Multi-stakeholder roadmap for implementing consumer vulnerability management.

Cyber Security Academy
Executive Cyber Security Program

Hinko Bastiaanse
S1942530
E-mail: Hinkob@gmail.com
Cybersecurity academy
Date of submission: 25 December 2018

Supervisors:
Prof. dr. ir. Jan van den Berg
Dr. Els de Busser

Executive summary.

The broadband access availability and bandwidth for the in-home domain have increased over 500% between 2000 and 2010. This, together with other technological innovations, has led to a situation where connected devices in the in-home domain increase both in numbers and in complexity. Consumers want to take advantage of the possibilities these devices offer but are unable to cope with the risks that accompany the usage of these connected devices. The cyclic execution of vulnerability discovery, classification, reporting, and remediation, called VM, could be part of the answer. Although VM in the in-home domain can theoretically be executed by the consumer, this research concluded that most Dutch consumers lack the technical skill and knowledge to do so. Therefore, this thesis proposes a solution in which the Dutch government, the connected device manufacturer, the internet service provider, and the VM solution provider assist the consumer in doing VM in his or her in-home domain. The end-result of this research is a roadmap which defines the steps per stakeholder, needed to build and run VM in the in-home domain in the Netherlands.

When VM is implemented in an organisation, determining the roles, responsibilities, and the risk appetite within the organisation is centralised. The size of the organisation also allows for acquiring people with vulnerability knowledge and IT skills, and for making a monetary or legal fist against connected device manufacturers and suppliers. In the in-home domain, the individual consumer cannot make this fist. A clear governance structure must be set up for VM to work in the in-home domain. The roles and responsibilities of stakeholders must be defined, and adhered to, and costs and benefits must be balanced.

The consumer plays an important role in reducing the number of vulnerabilities in the in-home domain. He or she needs to understand the risk of connected devices, must find it important enough to invest in security, and must know what measures are at his or her disposal to remediate the risks. This gives the device manufacturer an incentive to develop secure devices.
Resolving is part of the duty of care of the connected device manufacturer or software supplier. Security patches need to be issued, or configuration best practises supplied to keep the usage of connected devices safe. Implementation of patches, when not automated, must be as effortless to the consumer as possible to be effective. Law regarding this duty of care at this moment is too vague and ambiguous. Dutch government is working with the E.U. to remediate this. Starting with creating law for the home-router would be advisable from a risk perspective. A last resort for resolving high risk vulnerabilities, that cannot be patched or reconfigured, is to disable connectivity for only those devices via for instance mandatory updates.

When remediation is arranged, the ISP can, with explicit consent from the consumer, start discovering known vulnerabilities in the in-home domain. From a risk perspective, VM starts with detecting vulnerabilities in the home-router, which in the solution design is “phase 1”. Vulnerabilities of connected devices in the in-home domain can be discovered by scanning from the home-router, which is “phase 2”.
Most of the costs of doing VM lie in the discovery phase: Scanning software which can be used on the home-router needs to be developed, vulnerability signatures need to be updated, and to be able to run this scanning software, many home-routers currently deployed must be upgraded. In the solution design discovery is done by the ISP because of its information position, but securing the in-home domain is not the responsibility of the ISP. Therefor the substantial investments for these upgrades, run costs, and developments must be redistributed to the organisations responsible for the vulnerabilities.
Detected vulnerabilities, which exceed the acceptable risk threshold are reported, and can then be resolved. For the consumers that are unable to interpret the findings in the report, help needs to be arranged by the stakeholders.

Vulnerability management is implemented when all stakeholders do their part and all steps in the roadmap are realised. By adhering to the VM solution design described, the risk posed by connected devices in the in-home domain can be lowered to acceptable levels.

Keywords: Cyber security, vulnerability management, in-home, roadmap, connected device, IOT

Acknowledgement

This thesis forms the completion of my executive master at the Cyber Security Academy. I have enjoyed following this interesting programme and learning from knowledgeable lecturers, as well as from great fellow students.

I would like to thank my first supervisor Jan van den Berg, for allowing this paper to be my own work as well as steering me in the right direction whenever I needed it, and second supervisor Els de Busser for her advice and critical view. I am gratefully indebted to them for their very valuable comments on my research and am honoured to have worked with them.
I would like to thank all the experts who contributed to this research through the interviews. Without their views, and ideas, this research would not have been possible. Special thanks to my colleagues for their help and advice, and for making it possible for me to follow this master programme.

Finally, I want to express my profound gratitude to my partner Daniëlle de Roos, my children Yannick and Tycho, my parents, and my mother in law for their endless support and patience throughout my years of study and throughout the process of writing this thesis.

Hinko Bastiaanse, Den Hoorn 2018

Contents

Abbreviations

AT	Agentschap telecom
AP	Autoriteit persoonsgegevens
CBS	Centraal bureau voor de statistiek
CMNT	Cable modem termination point
CPE	Customer premise equipment
CSA	Cybersecurity act
CSAN	Cyber Security Assessment Netherlands
DDOS	Distributed denial of service attack
DSL	Digital subscriber line
ECS	European certification scheme
ENISA	European Union agency for network and information security
EU	European Union
FCC	Federal Communications Commission
FNT	Fiber network termination point
GDPR	General Data Protection Regulation
ICT	information- and communication technology
IoMT	Internet of medical thing
IoT	Internet of thing
IP	Internet Protocol
KPN	Koninklijke PTT Nederland N.V.
MPOE	Main point of entry
NCSC	National cybersecurity centre
NT	Network Termination point
ONT	Optical termination point
OS	Operating system
PAC	Private alarm central
PC	Personal computer
PLM	Product lifecycle management
PSTN	Public Switched Telephone Network
RED	Radio equipment directive
Tw	Telecom wet (Telecommunications law)
VM	Vulnerability management
WIFI	“Wireless Fidelity”, the synonym for a wireless communication network

List of Figures

List of tables

1 Introduction

1.1 Prologue

The usage of the Internet by home consumers is forecasted by Gartner[1] to take a flight in the upcoming years. One of the more significant innovations here is standard home appliances fitted with an IoT interface which allows for remote control over the internet. The refrigerator keeping track of its contents and ordering groceries online is an often-heard example, but one can also think of remotely controlled stoves, connected (smoke) alarms, smart in-and outdoor lighting, and even just-in-time delivery of pizza. According to McKinsey, *"The Internet of Things has a total potential economic impact of $3.9 trillion to $11.1 trillion per year in 2025"[2].*

These examples indicate that consumers and thus society grows more dependent on the correct working of communications services. Consumers use communication services for business as well as pleasure. Most businesses use communication services in their primary business processes, and vital services[3] would stop to function without communications services. In the past communication services were resilient because services would use separate infrastructure, whereby a crash of one type of service would not hinder the workings of another; an operator could switch to a landline when the mobile network was down. With the push on connected device manufacturers, Internet service providers[4] and businesses to become more (cost) efficient, the different types of communication services like telephony, data and mobile services become aggregated at the most basic communication layers, creating a more significant dependency on these underlying layers.

Criminals, on the other hand, have also discovered this dependence on business processes on communication services. Criminals abusing communications networks for illicit gain have proven[5] to be an increasing problem to the correct working of communication services and thus to Society. One of the reasons that the abuse problem is increasing can be explained, on the one hand, a profitable business model of criminals and, on the other, by the explosive increase in devices connected to the open communication[6]. The design of these connected devices often focuses on functionality and cost instead of security, thereby posing an easy target for criminals and thus increasing the "opportunity" factor for malicious use.

Multiple organisation recognise that this increasing risk is real: the "Cybersecurity Raad"[7], the "NCSC"[8], and "Agentschap Telecom"[9] advice to act on lowering risks posed by connected devices together with industry, where the "Rutte 3 akkoord" even mentions measures like installing IoT quality marks[10].

Within the space of private organisations, ISPs play a unique role because ISPs supply the connectivity between the customers' domain and the internet domain. Because of this intermediary role, the ISP is suited to secure the traffic flows between the Internet and customer domain. This intermediary function of the ISP also makes it ideal for governmental organisations to enforce regulation of these traffic streams from one central point. Just by making the ISP responsible for the enforcement of regulatory measures, governments do not have to deal with enforcing every internet user individually.

A good example is the "Pirate Bay blockade", in which Dutch governments in 2017 ordered the Dutch ISP's to block access for their internet users to the pirate bay (a website allegedly offering access to illegal content). The problem here was that Dutch internet users were not allowed to visit this

[1] Ganguli and Friedman, "IoT Technology Disruptions : A Gartner Trend Insight Report What You Need to Know."

[2] Manyika et al., "The Internet of Things: Mapping the Value beyond the Hype."

[3] overheid.nl, "Aanwijzing van Aanbieders, Producten En Diensten Vitale Diensten."

[4] techopedia, "Definition: Internet Service Provider."

[5] NCSC-NL, "Cybersecuritybeeld Nederland 2018."

[6] Abuse01, "Interview with Abuse Specialist."

[7] cyber security raad, "' Naar Een Veilig Verbonden Digitale Samenleving ' Advies Inzake de Cybersecurity van Het Internet of Things (IoT)."

[8] Nationaal Cyber Security Centrum (NCSC), "Cyber Security Assessment Netherlands 2017."

[9] Telecom, "Staat van de Ether 2017: Onveilige IoT-Apparatuur Risico Voor Samenleving."

[10] "VVD, CDA, D66 En ChristenUnie: Vertrouwen in de Toekomst."

website, but instead of prosecuting every single user, the justice department decided that it was more effective to block the site at the ISPs.

One of the most basic security controls is to remove the weaknesses in connected devices which, when left untreated, would be used by the criminal to gain unauthorised access or have the device perform unwanted or even criminal activities.
This so-called Vulnerability Management[11] (VM) is based on a three-step process: First, the known vulnerabilities in the connected devices and software are identified, then the found vulnerabilities must be resolved, and the process finishes with verification to confirm whether the vulnerabilities were successfully resolved.
These VM procedures are currently mandatory for all Dutch governmental organisations[12] and as part of well-known standards[13] deployed by many private organisations. Organisations perform VM primarily for increasing security for their online services benefiting their customers and themselves[14], which in turn also benefits society.
The tools to do VM are available to consumers as well. Most consumers, however, do not do VM in their in-home connected devices. Common reasons named are: the knowledge gap; should may grandmother of 104 understand vulnerabilities? Costs; professional vulnerability managers are not cheap, or even just a lack of caring; I have had no problems yet![15]. This takes place while past attacks have proven that connected home devices can be a real problem/risk to consumers and society.

In this thesis, an exploratory review is described on how VM can be done on connected devices in a consumer’s in-home environment and which barriers stakeholder must overcome. The research concludes by presenting a roadmap on how VM can be implemented for the in-home domain.

1.2 Research goal

While VM has been a standard in good internetworking hygiene in the business world, in the world of consumers and in-home equipment, measures to detect and control vulnerabilities are generally not present. In the Netherlands, several institutions have alarmed industry and government to intervene in the expanding risks posed by connected devices.

This thesis describes which steps must be taken to implement VM for the in-home domain. The solution plotted in time is the *deliverable of this thesis*:

> *A multi-stakeholder roadmap describing the steps needed to implement vulnerability management in the in-home domain of consumer households in the Netherlands.*

Especially in households, the expected increase in connected devices, and consumers paying little attention to IT security is a risky combination.
There are several (multi) stakeholders involved when performing VM for consumers; government is overall responsible for safety and security. Connected device manufacturers own the code and knowledge to secure connected devices present in the in-home domain and have a duty of care over their product. ISP’s are the intermediary between the consumer's internet connection at home and the worldwide internet and therefore have a duty of care over their network and services but can play a role in detecting vulnerabilities. Laws and regulations influence how these stakeholders work together, so lawmakers and law enforcement agencies form another group of relevant stakeholders.

[11] Nyanchama, “Enterprise Vulnerability Management and Its Role in Information Security Management.”
[12] Rijksoverheid, “Bir 2017.”
[13] ISO/IEC, “ISO 27002 Control 12.6 Technical Vulnerability Management”; NIST, “Security and Privacy Controls for Federal Information Systems and Organizations”; ISF, “Standard of Good Practise: IR2.7 Vulnerability Assessment.”
[14] Gartner, “IT Security Spenditure.”
[15] Altena, “Exploring Effective Notification Mechanisms for Infected Iot Devices.”

1.2.1 Research methodology

From a methodological viewpoint, this thesis follows a design science approach[16]. The focus is on "how to solve a problem" instead of "understanding why" as mostly used in classical science. The structure of this thesis will follow the reasoning line as depicted in Figure 1.

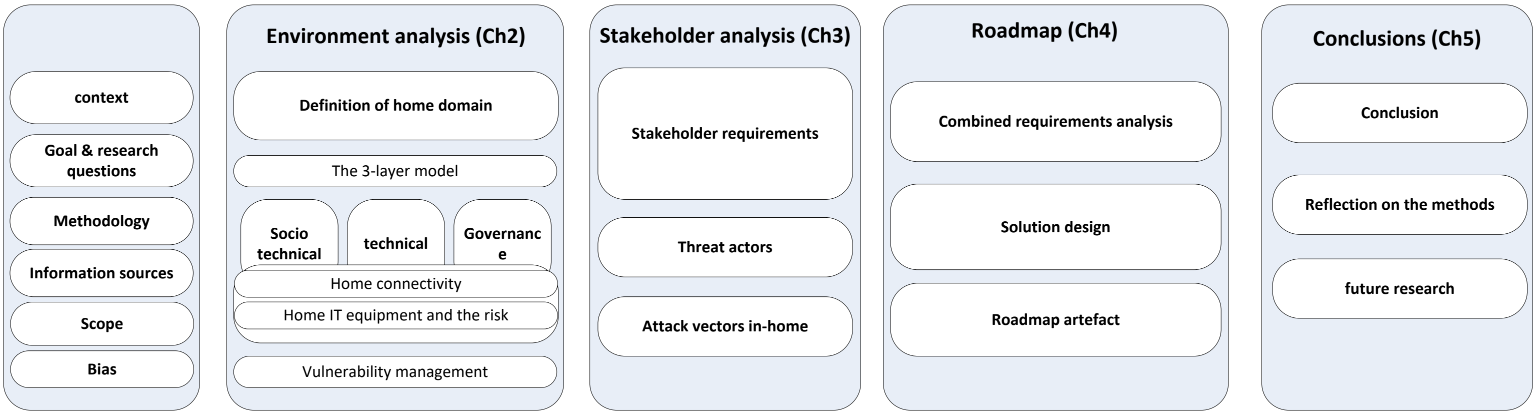


Figure 1: thesis structure

To produce the roadmap, first, a definition and analysis are done of the in-home environment and the relationships between stakeholders. The structure chosen for this research is the 3-layer model as described in chapter 2.2. By applying this 3-layer model, a breakdown is constructed to define and analyse the in-home domain from a technical, a social-technical and governance perspective (chapter 2). The environment analysis is used to identify the stakeholders relevant for designing the roadmap artefact. In chapter 3, Literature review and Interviews, done with relevant stakeholders, are used to come to a set of requirements of the VM solution. These requirements are combined and used to create the solution design in chapter 4. The steps needed to come to implementation are then plotted over time using gross estimations by Dutch stakeholders to come to the deliverable of this thesis in chapter 4.3: the roadmap.

This thesis ends with a conclusion and reflections on method and recommendations on future research (chapter 5).

1.2.2 Research design

The main structure of this research roughly follows the three steps of the fundaments of technology road mapping[17]. First, an establishment of the sense of urgency and a reconnaissance of the environment and the stakeholders was done. A simplified model of the in-home domain was constructed from the information of the reconnaissance. The environment and simplified model were then validated and used for drafting the questions for the initial interviews.

From the environment section and stakeholder answers, requirements were then gathered by browsing the text for essential criteria with the defined VM process and models in mind. Whether or not something is a requirement can be arbitrary, and limited time of stakeholders allowed for only one interview. Therefore, the gathered requirements were used to evolve the models and interview questions which were then validated in each following interview and let to the stakeholder sections. In the text, these requirements are mentioned by a letter followed by a sequence number which is enumerated in Appendix D Roadmap requirements.

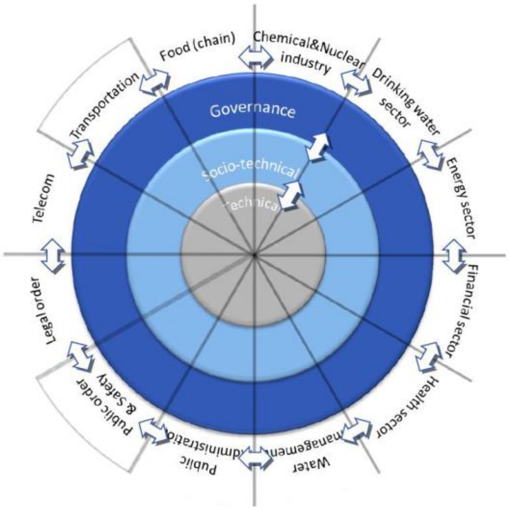


Figure 2 3-Layer model

Berg et al., "On (the Emergence of) Cyber Security Science and Its Challenges for Cyber Security Education."

[16] Hevner et al., "Design Science in Information Systems Research."
[17] Release et al., "Fundamentals of Technology Roadmapping."

In the analysis section, these enumerated requirements are combined into a solution design. From the interviews, timelines were distilled which, together with the requirements, are used to build the roadmap artefact. This thesis ends with the conclusions and reflection on approach and method.

The challenges associated with the implementation of VM require the analysis to be broader than just traditional technical analysis. Therefore, the analysis described in this thesis is based on the 3-layer model[18] introduces by Jan van den Berg. This 3-layer model introduces a socio-technical layer, which focuses on the cyber activities users undertake, i.e., the IT-enabled activities. A governance layer, which focusses on governance aspects, and the traditional technical layer. In this thesis, the word "lens" is used to indicate that a specific 3-layer focus is used.
The extension brought by introducing the 3-layer model allows the analysis also to include incentives, law, regulation and of course the "human element" which are further described in the next chapters.

Because law and best practices change over time, the 1st of September 2018 was taken as the "snapshot moment" which is seen as "present day" in this thesis.

1.3 Information sources

The information sources used to write this thesis were mainly literature study using freely available literature to create a view of the environment and possible solutions to the research objective. Interviews were then done with stakeholders in the field, in part to verify the findings and in part to gather the opinions and motivations of the stakeholder.

1.3.1 Literature study

Information found through literature study was used to form the basis of the VM solution. However, most literature and information sources discovered were focused on specific malware or mitigative techniques and in particular to (specific) business and governmental organisations. Not many literature sources were found that focus on consumers and how to mitigate the risks present in the in-home domain. The objective of this research is based on building a generic roadmap on how to implement VM in the in-home domain. Therefore, the information sources were expanded to vendor papers and presentations. Relevant exhibitions and conferences were visited to be able to have bilateral discussions with field experts which could fill in the knowledge gaps and gather the information needed to specify further and complete the research products. Interviews were done to gather the views and requirements of Dutch stakeholders who can play a role in implementing VM in the in-home domain.

1.3.2 Interviews

The goals of the interviews are twofold: First to verify the outcomes of the literature review, and second to gather the requirements of stakeholders needed to build the artefact.
The interviews were done in a semi-structured way. The reason being is that most interviewees have different expertise and backgrounds and therefore reasoned on different abstraction levels which required tailored interview questions to be able to gather the information needed to answer the research questions. The topics of the interview questions were fixed and communicated to the interviewees beforehand, but the order and questions themselves were open. All interviews were preceded by the interviewer giving a short introduction of the topic, scope and used models. The interviews were not recorded because most interviewees mentioned only wanting to talk without audio equipment, or the interviews took place in buildings where recording equipment was not allowed. Notes were taken by the interviewer which were later transcribed and sent to the interviewee for confirmation. These written records were made available to the first and second reader of this thesis.

[18] Berg et al., "On (the Emergence of) Cyber Security Science and Its Challenges for Cyber Security Education."

Doing the interviews in the desired order was a challenge because the interviewees of the ISP’s were only available during the summer break while the Dutch government interviewees stated that they could only deliver a significant contribution in the Autumn.
Therefore, the interviews with the industry were done first and the interviews with the Dutch governance organisations are used to validate and improve the analysis and artefact.

Informed consent

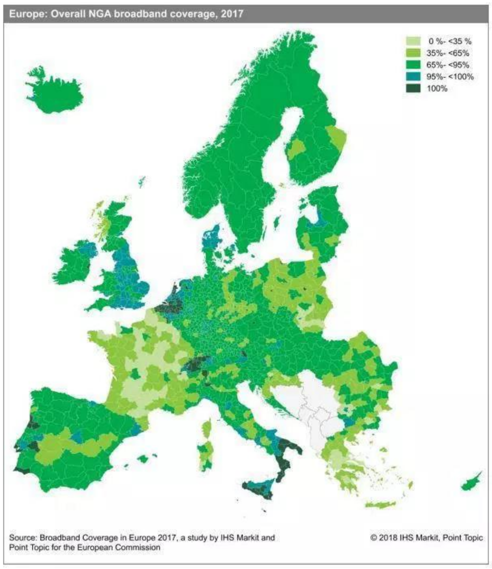
All interviewed persons were made aware that the research outcome is presented in a university publicly available thesis repository system. Several participants asked that specific information was not linked to their company in a possible publication in the media. Also, persons were asked at the start of the interview whether they as persons and company wanted to stay anonymous. These wishes were granted.

2 The in-home domain

This chapter starts with some history to better understand how, ISP's, communication services, and connected devices, in general, came to be. Then the in-home domain is described as seen through the three lenses of our methodology. Starting with the socio-technical lens to define the what ICT-enabled activities consumers undertake, followed by the technical lens to determine what technical measures underlie these ICT-enabled activities and what risks are involved. The chapter ends with what governance is in place for the in-home domain and what VM can bring to bring to secure connected devices in this in-home domain.

2.1 Global overview of the in-home domain

"Telecommunications is a technology that eliminates the distance between continents, between countries and between persons"[19]. It allows entities to communicate through a medium, which removes the need to be physically present to the entity receiving the communication. This medium evolved from a mechanical telegraph in 1794, to copper wires in 1837, to electromagnetic waves in 1896 to optical fibers in 1973[20]. Companies were established that offered telecommunications services like telegraphy and later telephony, commercial radio and television services. In Europe, these so-called service providers started as being state-owned companies like the PTT in the Netherlands and RTT in Belgium. Around 1980 a lot of European service provider companies were liberalised, and the state took a more regulating role[21]. 1980 was also the period where European service providers started delivering Internet communications services to people's homes. First, the internet was connected using, for modern standards, slow modem connections over the telephone network (also called fixed-line or PSTN) and which were charged by the minute or second. Between 2000 and 2010 these service providers increased the connection by 500%[22] using technologies like DSL (which used the PSTN) or Fiber (which demanded a whole new fiber-based infrastructure). In that same period Cable network operators, which up to then only delivered one-way television, started delivering two-way internet connectivity services to home users over their already existing Cable infrastructure[23]. In France, where the cable penetration rate is less than 15%[24], the fixed-line is used predominantly, but in the Netherlands, where the cable penetration rate is higher than 90%, the competition is fierce. In Europe, 87% of all households in 2017 had a broadband internet connection, and in the Netherlands, even 98% of all homes are connected to the Internet through a broadband connection[25]making it the country in Europe with the highest broadband penetration rate in 2017.


Europe: Overall NGA broadband coverage, 2017

Source: Broadband Coverage in Europe 2017, a study by IHS Markit and Point Topic for the European Commission

© 2018 IHS Markit, Point Topic

Figure 3 Broadband Penetration Europe 2017

The difference between internet access and broadband access is that broadband access according to the FCC is *"access that is always on and faster than traditional dial-in access[26]".* The term "faster" in this definition is not a fixed bandwidth. This can be observed in the FCC's communications, wherein 2010 the requirement was 4Mbit/s downstream and 1Mbit/s upstream, and in 2015 the requirement had grown to 25 Mbit/s downstream and 3 Mbit/s upstream[27]. The European Union has the ambition to connect all citizens to 30Mbit/s in 2020 and 50% of all households to 100Mbit/s in 2025.

[19] Huurdeman, *The Worldwide History of Telecommunications*.

[20] Huurdeman.

[21] Gentzoglanis, *Regulation and the Evolution of the Global Telecommunications Industry*.

[22] Nielsen Norman group, "Nielsen's Law of Internet Bandwidth."

[23] Esbin, "Internet over Cable: Defining the Future in Terms of the Past."

[24] IHS, "Cable Penetration."

[25] Statistiek, "Huishoudens in EU Met Internet Thuis."

[26] Federal communications commission, "National Broadband Plan."

[27] Federal communications commission, "Broadband Progress Report and Notice of Inquiry of Immediate Action to Accelerate Deployment."

Connectivity of the home domain via the mobile network is also sporadically used to connect the home domain to the internet. Some consumers have two ISP's or have integrated mobile connectivity into the home-router for redundancy purposes. This is not delivered as the standard by Dutch ISPs and is estimated by the interviewee's to be an insignificant part of the install base. The second use-case for mobile connectivity is when consumers who are in the process of getting a landline, or home users where a landline is not available, often connect through the mobile network. The number of users which use mobile broadband is less than 1% of the total in-home connections. Mobile connectivity, sometimes called mobile broadband is out of scope for this research because mobile connectivity, according to our interviewees, is not used often to connect homes and with the current 4G technology in most use cases does not reach the bandwidths needed to fit the EU broadband definition[28]. With the introduction of the 5G Mobile standard, this might change due to the higher bandwidths this 5G standard enables[29].

For connectivity to be put to good use, devices are needed that enable a function for the user. Therefor connected devices have been around since the birth of the internet because connected devices are the endpoints which use the communications technologies to allow users to communicate. In the 1970s and 1980s, these endpoints were mainly computers[30]. In the 1990s and 2000s, this focus on computers shifted towards connecting people. Nowadays the shift is towards connecting (nearly) everything to the internet of things[31] to be able to allow combining the data and enable remote controlled functions based on real-time machine analytics and learning[32]. Devices that have been around since before communication services like lighting or heating are enabled to communicate to all other connected devices, thereby enabling new applications. Fields of deployments of IoT are smart environments, domestic applications, industrial applications, security & emergencies, and logistics and transport[33]. To enable these new connectivity functions, extra hardware and software must be added to the already existing devices to allow them to connect to the internet. Adding extra hard- and software introduces new vulnerabilities[34] and by connecting the devices to the internet allows for a whole new group of attackers to remotely try and exploit these vulnerabilities. "Resolving" the vulnerability before it is abused, stops the attacker from exploiting the connected device. The periodic scanning and resolving of vulnerabilities is called vulnerability management (VM)[35]. The result of this thesis is to propose a roadmap on how to implement VM for the in-home domain.

2.2 The 3-layer conceptualisation

Traditionally, when speaking of cybersecurity, data, information and tangible assets are the assets that need to be protected[36]. This is often done using the C.I.A. approach; securing confidentiality, integrity, and availability. Although this C.I.A. concept has been the de facto standard over time, it mainly focusses on the technical aspects of security. When imposed on the scope of this thesis, a quick scan revealed that only a technical focus would be too narrow to cover the relevant aspects. To be able to deliver a feasible roadmap, the quick scan showed that social as well as legal and governance aspects had to be considered. Therefore the 3-layer model as described by Jan van den Berg[37] et al. was used as the basis for a holistic conceptualisation of the in-home domain.
The conceptualisation of Van den Berg et al. is an addition to the traditional C.I.A. approach on the traditional assets and defines "*securing the ICT-enabled activities*"[38] as the goal of cybersecurity.

[28] European Union, "Broadband Strategy & Policy."
[29] Sapakal and Kadam, "5G Mobile Technology."
[30] Taivalsaari, Technologies, and Mikkonen, "Software Engineering for the Internet of Things: A Roadmap to the Programmable World Software Challenges."
[31] Suresh et al., "A State of the Art Review on the Internet of Things (IoT) History, Technology and Fields of Deployment."
[32] Suresh et al.
[33] Suresh et al.
[34] Nyanchama, "Enterprise Vulnerability Management and Its Role in Information Security Management."
[35] Foreman, *Vulnerability Management*, 2009.
[36] ISO, "ISO/IEC 27000 Information Security."
[37] Berg, "Cybersecurity for Everyone."
[38] 3-layer model. See chapter 1.2.2

Technology in this conceptualisation is defined as the enabler of these "*ICT-enabled activities"* and governance is needed to steer the securing activities towards their intended goal.
This sequence is used in the following sub-chapters to explain the in-home domain, starting with the "*ICT-enabled activities*" or IT activities as seen through a Socio-technical lens.

2.3 The In-home domain as seen through a Socio-technical lens. (S)

This chapter starts with a short explanation of the socio-technical layer. After this introduction on the model, it follows up with an overview of the in-home domain as seen through a socio-technical lens.

The socio-technical layer is described by Van den Berg et al. as being the layer where the ICT-enabled activities take place. In the in-home domain, these activities are mainly undertaken by human actors interacting with ICT equipment like connected devices. Within the household, different persons deploy different activities. Adults work from home, children use social media and watch Netflix, and even seniors increasingly interact with ICT.
To start with the latter, seniors usually are a group of people with a low adoption rate of new technology. However, studies show that even seniors increasingly adopt ICT[39]. Research by Tsipi Heart[40] shows that ICT activities deployed by elderly can be of a fun nature by playing some bridge online, communication, or using email and Skype to interact with relatives and friends abroad. However, also applications like health services increasingly depend on connected devices placed at elderly homes to enable seniors to keep living on their own for as long as possible[41]. Hearts research also showed that seniors do have difficulties (S3) with understanding these new ICT technologies(S2), so fathoming security of connected devices will for most elderly be a bridge too far (S1).
Young people are generally more adept to ICT and its innovations then elderly. Research by Kent & Facer[42] in the UK in 2004 showed that 80% of tested children from the age of 6 already use ICT equipment like computer, tablets, phones and game consoles daily at school as well as at home. A more recent UK study by Stephen[43] concluded that children, in general, see ICT as a tool to be used. A few children in the research became interested in the ICT technology itself. Most "used" the device without a desire to gain in-depth knowledge of the technology itself.
Most studies of adults are specific to target groups in specific contexts. To still get a general picture of this group, the interviewees were asked for a description of this group with regards to adopting ICT technology. Their opinion was based on market research (which could not be shared) and personal experience. The interviewees agreed that this group comprehensively uses in-home ICT. Many office workers use the home network to work from home and connect to the office using an office laptop. For pleasure, this group commonly uses tablets, phones and televisions as in-home connected devices.
Securing these activities is possible on different layers. On the Social-technical layer, consumers can, for instance, get security awareness training to get to know the risks and consequences (S4 & S5) of not practising IT hygiene and to learn to buy connected devices with security seals(S2). Since the scope of this thesis is to give insight into technical vulnerabilities, the next chapter describes the in-home domain as seen through a technical lens. The reason for this focus is because technical equipment is underlying of the ICT related activities.

[39] Näsi, "ICT Activity in Later Life."
[40] Heart and Kalderon, "Older Adults: Are They Ready to Adopt Health-Related ICT?"
[41] Heart and Kalderon.
[42] Kent and Facerw, "Different Worlds ? A Comparison of Young People ' s Home and School ICT Use."
[43] Stephen et al., "Learning from the Children: Exploring Preschool Children's Encounters with ICT at Home."

2.4 In-home domain through a technical lens (T)

The ICT enabled activities from the Socio-technical chapter can be seen as the "8th layer" of the OSI model and connects to the highest layer: "*Layer 7 of the Open Systems Interconnection (OSI) networking model, which defines standards for interaction at the user or application program level; for example, formatting electronic mail messages, reading and writing files, and file transfer. It is the highest layer of the protocol stack.*"[44]
This chapter describes the Socio-technical activities enabling network technology of the home domain. It starts with a short description of a typical home connected with broadband to an ISP. Using the OSI model[45] as a guideline, the home domain is then used to build the simplified model, which is used as environment setting for the stakeholder analysis.

Historically all equipment, including cables and phone, used for the telecommunication service were owned by the service provider[46]. With the introduction of customer-owned equipment like the fax machine and telex and with deregulation of the ISP's, a demarcation point had to be introduced which terminated the connection coming from the ISP towards the house, which is called the local loop[47]. This new demarcation point was called the "Network Termination point" (NT) or "Main point of entry" (MPOE). All ISP's with a presence in the home have their own Termination point. Therefore, in Dutch households, one can often find a Network termination point (NT) for the telephony network next to the Cable NT. There are some differences between operators and technologies with regards to the NT, they, for instance, call them Optical NT(ONT), Fiber NT(FNT), or Cable Modem NT(CMNT) but the main similarity is that these are all passive handover points from ISP to the customer.

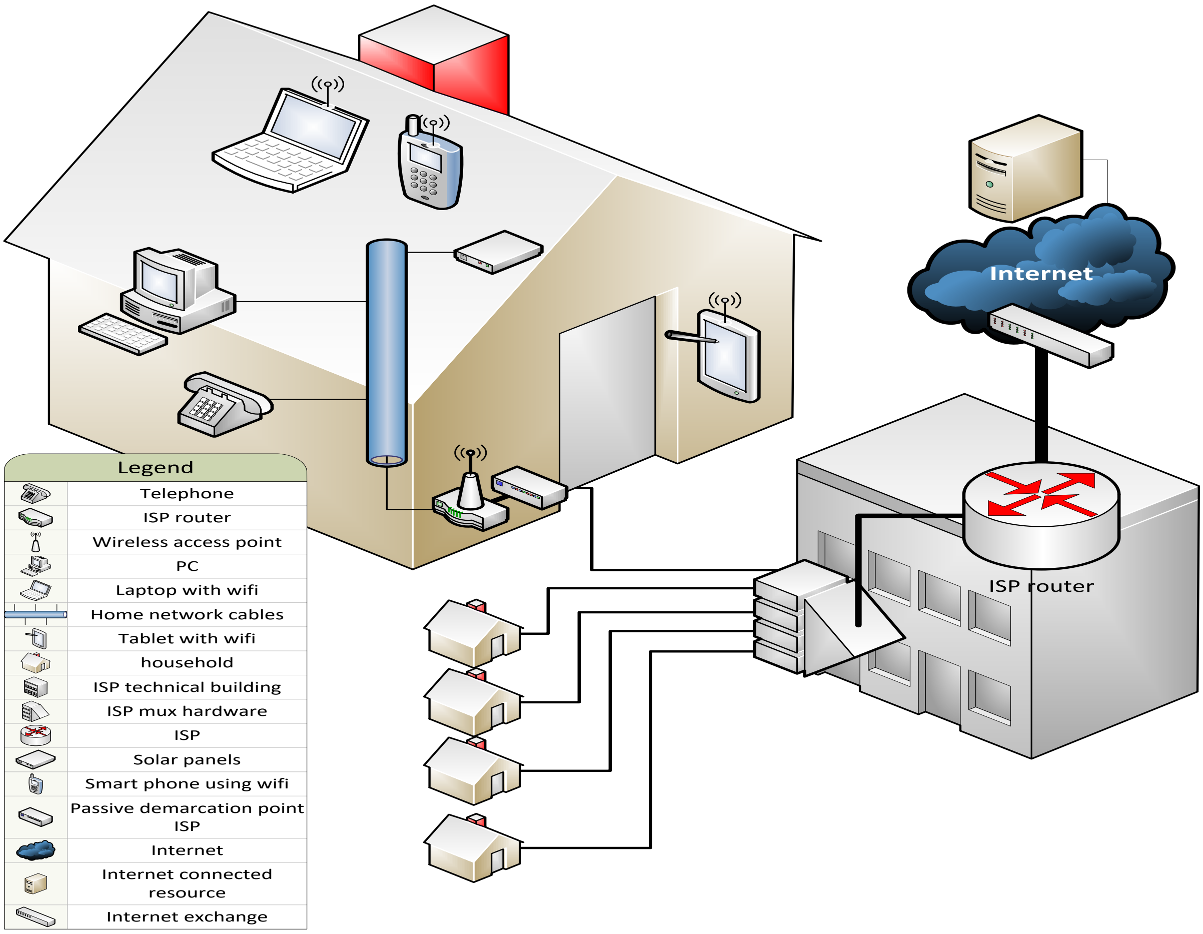


Figure 4 The in-home model

[44] SANS Institute, "Understanding Security Using the OSI Model."
[45] International Telecommunication Union, "X.200: Data Networks and Open System Communications."
[46] Huurdeman, *The Worldwide History of Telecommunications*.
[47] The network encyclopedia, "Local Loop."

This NT (OSI layer 1) is only a passive device which does not deliver an internet connection by itself. To connect to the internet, a CPE (customer premise equipment) must be connected to the NT. This CPE usually is a modem (OSI layer 2) with router functionality (OSI layer 3). This modem within the CPE is tasked with facilitating that packets from the devices in the home are sent to the central equipment of the ISP and vice versa. The router function in the CPE takes care that packets are routed towards the right device using the IP protocol[48]. The important thing to note is that the link between the home domain and the ISP only supports packets encapsulated in the IP protocol (T1) because IP is the standard protocol used on the internet. All non-IP traffic is either encapsulated in IP before it is sent to the CPE, or non-IP traffic is converted using an IP-gateway before the traffic is sent to the CPE which in turn forwards it to the internet through the ISP.

Within de home several different techniques can be deployed to distribute the connectivity through the house, we name the top 3. Traditionally "twisted pair ethernet" physical network cabling[49] is used with OSI layer 2 Ethernet encapsulation[50] on top, but with the arrival of internet-connected mobile devices, WIFI[51], both OSI layer 1 and 2, quickly gained ground. Connectivity using the already existing home power grid is the last in the top 3 line-ups. Powerline connectivity is not an IEEE standard and is made up of several underlying products and standards, all based on creating an OSI level 2 ethernet bridge between connected points within the home. The devices connected to these distribution methods are described in chapter 2.4.2.

The ISP receives the traffic on a OSI layer 2 network device (like a DSL multiplexer, or optical node) that aggregates (multiplexes) the traffic streams coming from the homes for scalability purposes and sends it to the ISP's main routing platform (layer 3) which handles the correct routing to the internet exchange[52].

2.4.1 Simplified in-home model

From an ISP perspective, layer two devices are essential for delivering the connectivity service. From a consumer in-home perspective these devices, however, are just part of the black box which starts at the NT and forms up the internet and service provider network. In the simplified model, these elements are therefore left out. Combining the service provider network and internet would lead to confusion regarding responsibilities. The ISP is responsible for the continuity of the connectivity network from home to the combined systems called the internet. However, the ISP is not responsible for these internet systems because they are not part of the ISP and his network.

On the in-home side, the different kind of internet devices, like smartphones, smart toys, tablets, and game computers are combined into "internet device". Although these devices perform different functions and may have different risk-profiles, all are seen as connected devices by the VM scanner if they are connected using the IP protocol. The only exception here is the Home-router because of its unique function of unlocking the home-domain towards the internet. This will be further explained in chapters 2.4.5 and 3.3.5.

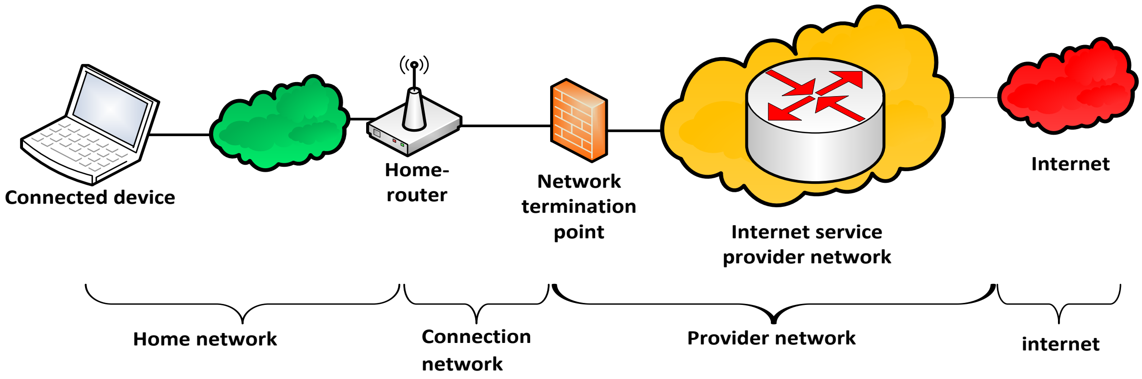


Figure 5 Simplified in-home model

[48] Darpa internet program, "RFC: 791 Internet Protocol Specification."

[49] cablek, "Network Cabling."

[50] IEEE, "802.3 Standard."

[51] IEEE, "802.11 Wifi Standard."

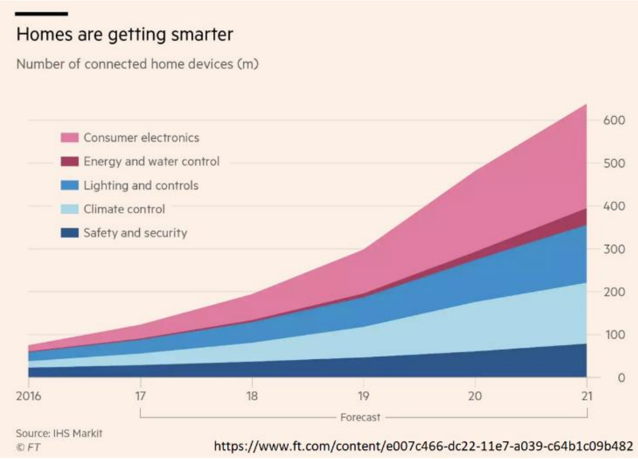
[52] TNO ICT and Dialogic, "Vraag En Aanbod Next-Generation Infrastructures 2010-2020."

2.4.2 IT equipment in the home domain and the ways in which they pose a risk. (R)

Risk is calculated by multiplying likelihood and impact[53]. This chapter describes some of the challenges with connected devices and the risk they pose to their owners as well as to Dutch society to give the reader some idea of the challenges and why the solution proposed in this thesis is opportune.

IT equipment in the home domain originally consisted of computer-related equipment with somewhat standardised software and protocols, connected to the CPE. Last ten years many more computer related devices were connected to the internet through the home internet connection, like mobile phones, tablets, microcomputers and many more. Trends like IoT, IoMT, home entertainment and smart homes make devices like the doorbell, which until now fulfilled its function without connectivity, connect to the home network and internet to improve upon its original function[54]. (R1)

Connecting devices like the doorbell to the home network may seem trivial to security because it does not protect an asset like for instance a camera, which handles private information. However, by connecting the doorbell to the home network, it can be used by criminals to remotely invade the home network, steal passwords stored within the doorbell, recover privacy-sensitive information about the owner, or use the doorbells ability to send traffic to use it in an attack[55]. Figure 6 shows the scale of growth that is expected with smart homes alone.



Source: IHS Markit
© FT
https://www.ft.com/content/e007c466-dc22-11e7-a039-c64b1c09b482

Figure 6 IoT growth expectance

2.4.3 Incidents and their possible impact

This increase in numbers also increases the impact in case these devices are compromised and used in a Distributed Denial Of service attacks[56]. A real-life example showing that this threat is real is the attack by the Mirai botnet in August 2016. In this attack, many IoT devices formed a DDOS attack which together took down several large websites.[57] Two aspects that made Mirai different to earlier DDOS attacks was the scale of the attack, 1.2 Tbps was unheard of before, and that zombie consumer devices, like connected CCTV camera's, home routers and connected tv set top boxes, were used. This raises the question whether these compromised home devices could also trigger a DDOS against vital services. An example often used is when thermostats or electric furnaces in Dutch homes altogether turn on at maximum power, would the electrical grid be able to handle that?[58]. The typical answer is that the electrical grid is built resilient enough to cope with such a DDOS attack, this is also the conception in the Netherlands[59].

Vital services like Dutch emergency services, however, are expected to be less resilient because they rely on physical measures like fire trucks, cars and personnel to physically act. Imagine that frequently used connected in-home device like a CPE or a solar panel is hacked[60]. That device can then initiate telephone calls from the in-home domain[61]. Only 47 calls in the night in Amsterdam lead to a disruption in the correct functioning of the emergency number 112[62], imagine what would

[53] ISACA, "Security Risk."

[54] Gubbi et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions."

[55] Brightsight, "Assessing the Security of ' Simple ' IoT Devices."

[56] Mirkovic and Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms."

[57] Kolias et al., "DDoS in the IoT: Mirai and Other Botnets."

[58] CSO, "Is Critical Infrastructure the next Ddos Target."

[59] contact the author personally, "Information Gathered through Anonymous Interview."

[60] NCSC-NL, "Cybersecuritybeeld Nederland 2018."

[61] AD, "Telephone Hacked through Vulnerable Solar Panel."

[62] Ministry of safety and justice, "Onderzoek Naar de Stroomstoring Amsterdam En Omstreken van 17 Januari 2017."

happen if all CPE's or hacked solar panels placed calls 112 at the same time. This same example goes for medical services and IoMT[63] with a panic button. Burglar alarms and police is a different story because the Dutch police only react when a person verifies a burglar alarm. However, in this case, the private alarm central is the victim of the DDOS, but PAC's are not part of emergency services. The impact to Dutch society of these physical world "DDOS" attacks, however, is apparent.

2.4.4 Likelihood

The second part of the risk calculation is likelihood. The lack of standardisation of protocols and software is one of the main factors why connected devices have an increased likelihood of being misused. In the world of IoT alone, 14 different wireless protocols are used, each with its vulnerabilities[64]. Under the strain of efficiency, several of these protocols are expected to be phased out in the foreseeable future, which means that hardware running those protocols will still be in use, but the support and patching of newly found vulnerabilities will stop. This also goes for the software running the connected device. Many devices are fitted with software which was written by a hardware company focusing on functionality and where writing code is a cost centre. These companies are unlikely to provide lifetime software support with updates and bug bounty programs[65]. Without support, these devices will become vulnerable over time without security updates which in turn increases the likelihood of the device being compromised and be used for illicit gain.

The other factor increasing the likelihood of misuse is that connected home devices and especially IoT at home often contain vulnerabilities and have default passwords and that by connecting them to an open network like the internet, the attack surface and thus the likelihood of malicious use is increased dramatically[66]. An example for this is the attack on a connected heating system in Finland where in November 2016, criminals used a vulnerable IoT heating system to shut down the heating on two buildings leaving the inhabitants in the cold for more than a week.[67] This example also shows that when home devices like heating, fridges and toasters are en-mass connected to the internet, that the impact on the owner's daily lives when abused is increased compared to the risks when a pc or laptop is hacked.

2.4.5 A special notion: the home-router.

There are multiple reasons why the home-router deserves special attention when securing the in-home domain:

Firstly, because the home-router handles all traffic between the home domain and ISP, it is the ideal place for criminals to intercept traffic from the home domain. The intercepted data can, for instance, be used to intercept passwords or spy on user data which is often part of higher level protocols in the OSI-stack. Apart from intercepting traffic, altering the user traffic can also be done from the home router. Altering traffic, for instance, is used when a criminal redirects home device to a malicious online banking site by altering the DNS[68]. Usually, a firewall installed on the home-router prevents attackers from the internet from connecting to devices in the home domain, but when the CPE is compromised, the attacker can easily bypass the firewall.

Secondly, add-on services like telephony and tv services are also delivered through the home-router. These add-on services create extra complexity which in turn introduces more risks to different levels of the OS and management of the home router[69]. Coming out of the box, home-routers are usually configured most functions active. This goes against security hardening best practices[70] because more services mean a bigger attack surface of the home-router(R4). Another hardening best practice is the use of malware protection like virus scanners or spyware protection. (R2) The home-routers

[63] Lysecky and Ott, "Security Challenges for Medical Devices."

[64] Pradeep et al., "IoT and Its Connectivity Challenges in Smart Home."

[65] Rossi, "The Internet of Old Things: Protecting the Future of IoT Devices."

[66] Farooq et al., "A Critical Analysis on the Security Concerns of Internet of Things (IoT)."

[67] Chirgwin, "Finns Chilling as DDoS Knocks out Building Control System."

[68] Khrais, "Highlighting the Vulnerabilities of Online Banking System."

[69] Trend micro, "Protecting Home Networks: Start by Securing the Router."

[70] coursera, "Network Hardening Principles."

delivered by Dutch ISP's do not run anti-malware protection. A quick scan of home-router vendors reveals that only a few models support anti-malware software.

Thirdly home-routers typically run software that is years behind of modern secure programming standards and vulnerability hunting efforts[71]. (R3)

To summarise, home-routers are an interesting target for criminals because they are the hub between home and internet, and home-routers form a relatively easy target because of no anti-malware protection and running older software.

Lastly, consumers neglect to perform security best practices for the home-router. Some examples are the installation of security updates, changing of the default password on the administrative interface or changing the Wi-Fi password.

2.5 Home domain through a governance lens (G)

This section gives an overview of the formal institutional environment of the in-home domain[72]. Apart from the formal institutional environment, governance also included informal norms and values like how stakeholders cooperate based on their own incentives, and how that is formalised into arrangements like alliances and contracts. These norms and values are stakeholder specific, where the formal institutional environment, based on formal rules, laws and regulation applies to all stakeholders. Therefore, the stakeholder dependent governmental aspects are analysed in the stakeholder section of this thesis (chapter 3).

Since governance of the in-home domain is comprehensive, this thesis narrows down its focus to the functional area of telecommunications and connected device manufacturers. The E.U. law that sets the requirements for the safety of a connected device is still under development. Therefore, on that part, we mention the relevant expected notions as explained by the interviewees[73].[74]

The snapshot revealed that four laws apply to the in-home domain as described in chapter 0. The snapshot was verified by interviewees specialised in telecommunications law. In this chapter, these laws are shortly explained, and the corresponding article and law texts can be found in Appendix C:

- Telecommunication law [75]
    - Privacy & GDPR
    - Electronic commerce law (2000/31/EC)[76]
- Net neutraliteits verordening[77]
- Computer criminaliteit II[78]

On the side of the connected devices, no specific law on security of connected devices exists for manufacturers. However, the interviewees referred to the following two directives:

- Radio equipment directive
- Duty of care principles

2.5.1 The telecommunications law

The telecommunications law(Tw) in the Netherlands is a dedicated law that has its roots in the postal and telegraphy law of 1904 and has evolved ever since. Significant changes to the Tw were for instance made in the time of liberalisations of the Telecommunication market (the '70's), but also in 1997 when the regulatory organisation OPTA was founded. The focus of the OPTA (nowadays called ACM) was to regulate all parties with significant market power and make it possible for new ISP's to

[71] "European Cyber Security Perspective 2018."

[72] Koppenjan and Groenewegen, "Institutional Design for Complex Technological Systems."

[73] DP01, "Interview with Policy Officer Dutch Parliament"; Reg01, "Interview with a Dutch Regulatory Policy Specialist"; Reg02, "Interview with a Regulatory Policy Specialist."

[74] The main language for legal texts in the Netherlands is Dutch. Therefore relevant texts are translated by the author. In case of dispute the Dutch law text is leading.

[75] overheid.nl, telecommunicatiewet.

[76] European Parliament, "Directive 2000/31/EC."

[77] European Parliament and Council, "Regulation 2015/2120."

[78] Overheid.nl, "Computer Criminaliteit II."

enter the Dutch telecommunication market. In the 21st century, the Tw was also amended with legislation coming from the European Union. Some examples are the ban on spam in October 2003[79], the cookie law of 2013[80]. The net neutrality amendment of 2013[81], where the Netherlands, together with the US and Chili, was the first to install net neutrality legislation (Since November 2015, net neutrality law is installed as a directive by the European Union[82]). Net neutrality is covered in a separate chapter from the Tw because it was removed from the Tw after it was installed as a directive by the EU[83].

Privacy & GDPR

In May 2018 the GDPR replaced the EU Data Protection Directive. The GDPR demands all companies to adhere to strict processes and procedures while collecting, storing and processing personal data of EU citizens. Although applicable to all organisations including ISP's, for the scope of this thesis the protection of personal data by the Personal Data Protection Act as included in the Tw chapters 11.1 – 11.13 is sufficient[84].

These privacy notions describe that the confidentiality of the communications and associated data must be ensured. The implication for the ISP is that when the ISP wants or needs to use the customers' data, explicit consent must be given by the consumer to the ISP. The ISP must specify which data will be used at what time and for what purpose.

An exempt can be made by the Dutch government which neglects this "explicit consent" notion. An example is the Lawful intercept article which obliges ISP's to deliver customer data for criminal investigations without asking for consent or notifying the customer in any way.

Regarding VM the data gathered by the VM scanners is categorised by the ISP as personal data[85]. The scan returns information regarding the in-home domain, connected devices and software used by the consumer in that domain, and vulnerabilities in those devices and software.

Continuity

ISP's deliver connectivity services that are categorised as vital for Dutch society[86]. Therefor ISP's are obliged by law to take appropriate measures to ensure continuity of their connectivity services.

The TW article 11a contains provisions stating the duty of care that ISP's have towards the delivery of their services. These provisions impose obligations on the ISP on the one hand but, on the other hand, allows him to take measures that go against provisions mentioned in other articles of the Tw. An example is the abuse process which is used by ISP's to place consumers, which have a malware infected system in their domain, into a confined network to prevent the malware from spreading. This example is further explained in chapter 3.4.2.

Electronic commerce law

ISP's in the Netherlands do not actively monitor customer traffic but are obliged to react when alerted to abuse activities by third parties. This is stated in the "Mere conduit" article of the 2000/31/EC directive of the European Parliament[87]. This rule voids ISP liability for illegal traffic transported over the ISP's network if the ISP does not alter or store the data and only transports traffic without knowledge of the content.

2.5.2 Net neutrality

Net neutrality is a directive issued by the EU, which ensures consumers free and open connectivity to the internet without ISP's imposing a bias on which services can and cannot be used. The net neutrality directive contains rules for the ISP to ensure the end-users get access to the open internet

[79] European commision, "SPAM: European Commission Goes on the Offensive."

[80] European commision, "The EU Internet Handbook: Cookies."

[81] ICT recht, "Nederlandse Netneutraliteit Voorbeeld Voor Europa, Handhaving Aangescherpt Met Boetes."

[82] European commision, "Open Internet Policy."

[83] European commision.

[84] Leg01, "Interview with a Telecom Legal Specialist"; Priv01, "Interview with an ISP Privacy Officer."

[85] Leg01, "Interview with a Telecom Legal Specialist."

[86] overheid.nl, "Aanwijzing van Aanbieders, Producten En Diensten Vitale Diensten."

[87] European Parliament, "Directive 2000/31/EC."

without any limitations. For the scope of VM, the following subset of technical principles from the EU net neutrality law is applicable.

A	Safeguarding open internet access
1.	End-users can receive and distribute information without ISP setting restrictions to location, origin, content or application. (Art 3.1 shaping principle)
2.	All information and traffic are treated equally and without discrimination. (art 3.3 equality principle)
3.	Any traffic management measure may entail the processing of personal data only if such processing is necessary and proportionate (art 3.4)
4.	The ISP will not monitor the specific content of the traffic. (Art 3.3 monitoring principle) (G7)
5.	*"End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service".* (Art 3.1 CPE choice principle) (G8)

Table 1 Net neutrality principles regarding VM

Apart from the provisions mentioned above, the ISP is still obliged to adhere to the duty of care principles as stated before. When measures are taken that influence the transparency of the internet service, the ISP must clearly state and explain these measures to the customer before signing the contract. The interviewees mention having incorporated these measures on their website and in their Terms and conditions[88].

However, as with most regulations, net neutrality law has side effects. Especially in the United States[89] the debate around net neutrality has focused on the argument that net neutrality law requires ISPs to treat all traffic equally, but that not all traffic is equal. A good example is the need to prioritise emergency calls. Imagine a situation where a family member has a cardiac arrest, and one wants to call the emergency services. At that same time, a neighbour is having a friendly telephone call with her mother and her son is streaming the newest Marvel movie causing congestion in the network. According to the Net neutrality fairness (equality principles) principle, all traffic should be treated equal, but most people would agree that in this situation prioritising the 112 call over the other traffic is the most sensible and humane thing to do. Equality and fairness may therefore not be the solution to the Net neutrality problem. As F.A. Hayek in 1945 wrote; *"The economic problem of society is not merely a problem of how to allocate "given" resources ~ It is rather a problem of how to secure the best use of resources known to any of the members of society, for ends whose relative importance only these individuals know"*[90].
To give providers and governments room to prioritise and differentiate with the best interest of Dutch society in mind and to ensure continuity of the connectivity services, an exemption is in place. Apart from allowing the Dutch government to set some priorities by directive, this exempt also allows traffic shaping to preserve the integrity of end-user devices, which is relevant in the case of VM.

2.5.3 Computer criminality law II

Computer criminality law II[91], in 2019 to be replaced by III, is criminal law that enables combating criminal offences connected to electronic networks. Although the in-home domain as such is not named in the computer criminality law, all devices which are connected to the in-home domain using IP fall under the term "geautomatiseerd werk". At the moment of writing, only equipment under lease by the consumer from the ISP, like a managed home-router, or a managed tv set-top box can legally be accessed by the ISP.

[88] KPN BV, "Algemene Voorwaarden Voor Vaste En Mobiele Telecommunicatiediensten D"; VodafoneZiggo, "Algemene Voorwaarden Ziggo."
[89] Open Secrets, "Net Neutrality."
[90] Hayek, "The Use of Knowledge in Society."
[91] Overheid.nl, "Computer Criminaliteit II."

Doing an automated VM scan to gather information on vulnerabilities is the first stage of hacking devices[92] in the in-home domain. Scanning for default passwords, a common vulnerability scan part, is seen as gaining access because when the default password matches, entry to the system is established. Therefor VM can only be done with "explicit consent".

2.5.4 The duty of care principle

The law on Product liability for IT and connected devices at the moment of writing is not as detailed as the Telecommunications law. However, IT and connected devices do fall under the general product liability rules[93]. These liability rules are based on whether errors in the software or device can lead to damage-costs being recovered.
The current regulation for liability of producers of products is regulated in section 3, book 6 of the Dutch Civil Code[94]. Recovering damages based on this product liability law has three limitations:

1. As can be read in Appendix C, the defect as explained in defective product criteria is based on a product which is delivered with a defect. In the case of software and connected devices, vulnerabilities can be unknown (article 6:185 d) at the moment of sale and can be discovered later. This would void product liability at least to some extent. (G11)
2. Product liability is based on tangible goods (including electricity). In the case of connected devices, the device is tangible, but the non-tangible software holds the vulnerability. In case of downloaded software, it is even more difficult to prove that the product is a tangible good. (G12)
3. A minimum amount of € 500 applies, and damage can only be claimed based on death or bodily injury or property damage suffered in the private space (article 6: 190 Dutch Civil Code). Damage to digital files is excluded and damage in the professional sphere as well. These provisions severely limit the use of product liability. (G13)

The second possibility to reclaim damages caused by vulnerabilities in connected devices and software is to appeal to product liability due to an unlawful act. In case of an unlawful act, the minimum amount of € 500 or damages outside the personal space are irrelevant. However, in this case, an unlawful act must be proven; the producer must have committed an attributable unlawful act. The expectation is that a mere coding error that was left unseen would not be seen as an unlawful act. Only a court case can give a definite answer and will be case specific[95].

2.5.5 Radio equipment directive

The Radio equipment directive Is an EU directive that was installed in 1999 and last updated in 2014. *"The Radio Equipment Directive 2014/53/EU (RED) establishes a regulatory framework for placing radio equipment on the market. It ensures a Single Market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects. These include technical features for the protection of privacy, personal data and against fraud. Furthermore, additional aspects cover interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software."*[96]
Essentially the RED does for radio equipment, what the EU also wants for cybersecurity. A single market through mandatory security certification, a set of minimum requirements for security, and good standards for efficient interworking. Therefore, the EU is exploring how to extend the RED also to incorporate cybersecurity requirements. The EU wants to do so by "activating" optional provisions which are already in place in the RED directive. The European Commission can activate these provisions for specific product groups also to incorporate network security[97]. Setting the exact

[92] Skoudis and Liston, *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses*.
[93] Ejure, "Product Aansprakelijkheid En Software."
[94] wetten.overheid.nl, "Product Aansprakelijkheid."
[95] Min01, "Interview with 2 Ministerial Cybersecurity Policy Officers."
[96] Commision, "Radio Equipment Directive."
[97] Reg02, "Interview with a Regulatory Policy Specialist."

baseline for acceptable risk would be done through self-regulation by industry, because of the diversity of devices, and technologies. (G15) (G16)

At the moment of writing the idea of the European Commission was to start a “proof of concept” with activating these provisions for the product groups “smartwatches”, “smart toys”. The effort of the European Union to secure connected devices will most likely start with the introduction of voluntary standards in which the connected device manufacturers themselves will set the baseline for acceptable risk. Only when voluntary fail, then the EU will switch to mandatory standards. (G17)

The RED, at the snapshot moment, is applicable for devices with some radio interface. Although many connected devices use WIFI, not all are devices are connected over the air. (G18) Therefor appending the RED to incorporate security demands is just one of the steps taken by the EU. Other directives will also be amended to incorporate cybersecurity demands. The reason for amending existing laws is that an overarching cybersecurity directive would take long to be implemented. Another reason is that a large number of EU lobby groups surrounding this topic might influence the lawmakers to the point that the cybersecurity law would not do justice to why it was drawn up[98].

2.5.6 Industry certification & connected device security standards

The previous chapters entail measures which are pushed by the government. Industry themselves can also make agreements on standards together with government, standardisation institutions, or autonomous. Many standards on connected devices exist. Most focus on a specific market or product group. Connected devices used by financial institutions, for instance, make use of the following standards:

1. EMVCo[99] is a certification that is mandatory for electronic payment terminals, and chip payment cards, that process transactions for Europay, MasterCard and Visa (EMV)
2. Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard which sets requirements for the processing of payment card data.

The card branch or payment providers mandate these standards. Supervision ranges from formal audits by Qualified security assessors, via internal security assessors down to self-assessment questionnaires depending on the risk (number of transactions, monetary value). (G19)

ENISA[100]

Regarding setting cybersecurity standards for connected devices, ENISA plays a prominent role in the EU. ENISA was founded in 2004 by the EU to contribute to network and information security in the Union. ENISA does this by making recommendations on laws, regulations, and standards. ENISA has created a standard for IoT[101] when used in critical information infrastructures. Although the risk profile of the in-home domain is different to the risk profile of critical infrastructures,[102] many security measures can be used in the in-home domain. The ENISA baseline defines recommendations on several areas ranging from harmonisation of initiatives to low-level technical best practices. Because some requirements were gathered from the ENISA baseline, the security measures relevant to the in-home domain are displayed in Table 19 in appendix C.

[98] reg03, “Q&A Session with Regulatory Advisor on ‘Dag van de Apparatuur.’”
[99] EMVCO, “EMV Technologies.”
[100] ENISA, *Baseline Secur. Recomm. IoT Context Crit. Inf. Infrastructures*.
[101] ENISA.
[102] Nationaal Cyber Security Centrum (NCSC), “Cyber Security Assessment Netherlands 2017.”

2.6 Vulnerability Management (V)

This chapter gives a short overview of the vulnerability management (VM) process, followed by how this process can help in securing the in-home domain. The chapter ends with the pro's, and cons on using VM in the in-home domain.

2.6.1 What is Vulnerability Management

There are several ways to cope with security risks. One of these ways is to control the attack surface for a possible cyber-attack. This can be done by analysing and then remediating the vulnerabilities which are present in an IT domain and which can be exploited by an attacker to gain unauthorised access to this domain[103]. Vulnerabilities by themselves are not dangerous. However, they play a role in enabling steps of the kill-chain as described by Lockheed Martin[104]. Vulnerabilities in network design also enable lateral movement of the malware/attacker to other devices in the same network segment. The control of vulnerabilities in a continuous manner is called vulnerability management.
VM (Figure 7) is the cyclical practice of planning, discovering, classifying, reporting and remediating vulnerabilities.

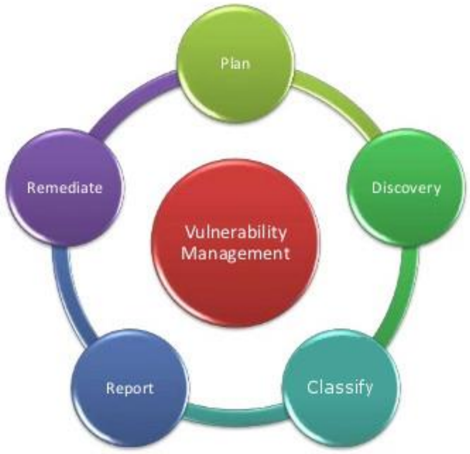


Figure 7 Vulnerability management

https://www.slideshare.net/sobca/qualys-intro

Discovering vulnerabilities is done by analysing the devices, their software, and in some cases their relation. Connected devices in the domain to be scanned are usually first discovered by scanning the network segment on some well-known IP ports (V1). After this discovery scan, the vulnerability scan is performed. The vulnerability discovery can be done in several ways. Some examples are RED or blue team penetration testing, automated vulnerability scanning, Fuzz testing, manual assessments, and by doing security walkthroughs in knowledge groups[105]. For periodic testing of large groups of devices, automated testing is preferred over manual assessment because of the economy of scale. (V2). Automated testing is done by comparing signatures of software with a known vulnerability, to the device under testing. The Quality of the automated test is based mainly on the number of signatures in the comparison database and the comparison method.

Classification is done to arrange the discovered vulnerabilities based on the severity and rank them using a standard like CVE[106](V3). Standards work well with stock software, but with self-made software, a self-made structure must be devised[107]. The discovered vulnerabilities are then compared to the acceptable risk standard which is set as a threshold/baseline (V4). This threshold defines which vulnerabilities need to get priority. This priority is set because solving all vulnerabilities is not economically viable. Also setting priority establishes focus on vulnerabilities with the highest risk factor.

Reporting is done to inform the owner of the devices under scanning on the vulnerabilities found. The report names the vulnerabilities with their ranking and which shows which vulnerabilities exceed the acceptable risk threshold(V5). Because the reporting is on known vulnerabilities, standard solutions must be suggested to the device owner on how to resolve the vulnerabilities(V6). The report must only contain the vulnerabilities applicable to that particular user(V7).

Remediation of vulnerabilities can be done in many ways and is dependent on the discovered vulnerability. The vulnerabilities that are found to exceed the acceptable risk threshold must be mitigated. Most technical vulnerabilities in connected devices can be resolved by patching or upgrading (V8). However, in situations where a vendor, for instance, cannot supply a patch to resolve

[103] DOD, "Https://Www.Spi.Dod.Mil/Tenets.Htm."
[104] Martin, "Http://Www.Lockheedmartin.Com/Us/What-We-Do/Aerospace-Defense/Cyber/Cyber-Kill-Chain.HtmlNo Title."
[105] Foreman, *Vulnerability Management*, 2009.
[106] "Https://Cve.Mitre.Org."
[107] Seacord and Householder, "A Structured Approach to Classifying Security Vulnerabilities."

a vulnerability, installing heuristic virus scanner or increasing the detection and reaction capability of the network can be effective to limit the risk posed by the vulnerability(V9). The last resort is to uncouple the connected device or software from the network (V10). “Human vulnerabilities” like phishing can be remediated by educating consumers or by doing sessions to increase consumer security awareness. (V11)

Planning is done to signify that when the vulnerabilities exceeding the acceptable risk threshold are resolved, a new discovery must be planned. The reason for planning a new discovery is twofold: the first is to determine whether the mitigation was successful and the second is to scan for new vulnerabilities. New vulnerabilities in existing hard- and software are discovered continuously. Another source of new vulnerabilities is the introduction of new hard- and software into the network domain which contain their own vulnerabilities which must be discovered and possibly resolved. Therefore, the VM process must be run in a continuous manner(V12).

2.6.2 Vulnerability Management in the in-home domain

Vulnerability management is already common practice in corporate IT environments, but not in the home environment. There are however products on the market with which a consumer can scan the in-home domain. The point from which the in-home domain is scanned determines the amount of insight in the in-home domain. Shodan[108] , for instance, is an online product which scans the internet for devices vulnerabilities. It allows users, for instance, to get an overview of all IP camera’s in a specific area with a particular vulnerability. Another function is for Shodan to do a scan of the IP address of the in-home domain of a particular consumer. Because this scan is performed from the internet, it will not scan beyond the home-router (see Figure 8). The home-router, when properly configured, will not allow the scan from Shodan to pass beyond the home-router into the in-home domain unless specific traffic is configured to be allowed into the in-home domain from the internet.

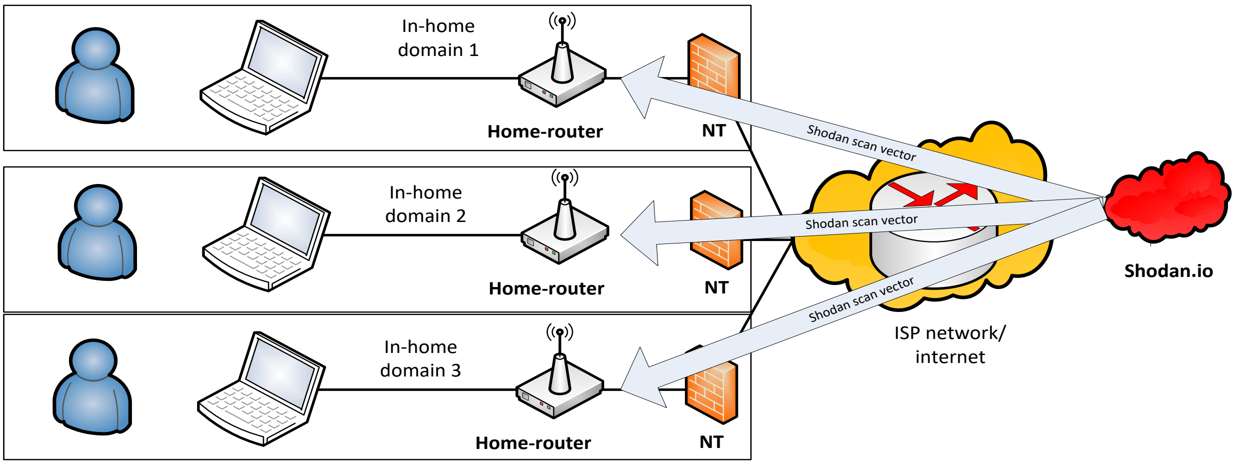


Figure 8 Shodan VM scan vector

The scan will therefore only report vulnerabilities which are found on the home router. This scan vector resembles the attack vector of most attackers. (which attack over the internet/Isp network) (V13) For a more in-depth view, market leaders in enterprise Vulnerability management like Qualys[109] and Tenable[110] each have a (free) version which can be used to scan a limited number of devices. The scan is initiated from a computer located in the in-home domain (see Figure 9) and will scan all devices it has connectivity to(V14). The output of such a free scan consists of the devices that were found and scanned in the in-home domain, the vulnerabilities which were found according to their latest known vulnerability list and the severity value according to the MITRE model[111].
The downside of this model is that the scan vector does not resemble the vector for attackers (which usually is coming from the internet/ISP network).

[108] shodan, “Https://Www.Shodan.Io/.”
[109] Qualys, “Qualys Freescan.”
[110] Tenable, “Nessus Licenses.”
[111] “Https://Cve.Mitre.Org.”

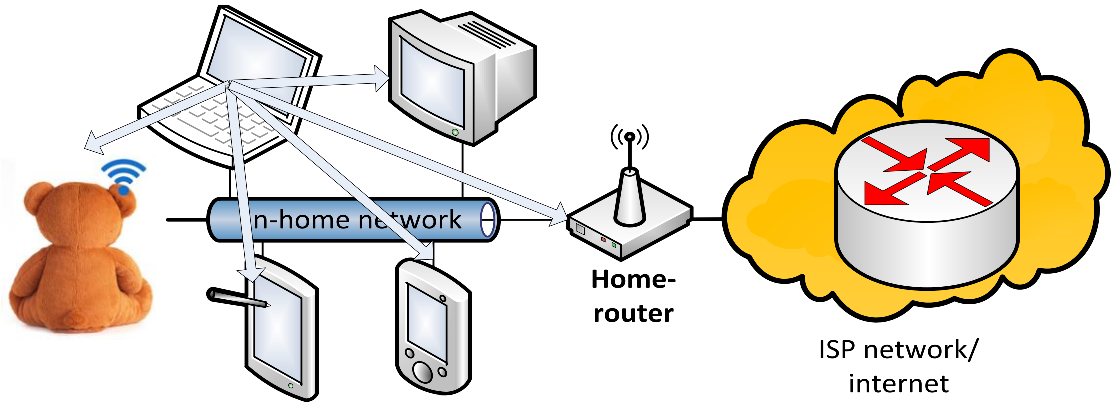


Figure 9 VM scan vector from a computer in the in-home domain

Automation

As seen in the discovery paragraph, several methods can be used to discover vulnerabilities. One can go really in depth on one device or software version by doing a full code review with all kinds of fuzzing techniques to discover old and new vulnerabilities[112]. This is resource intensive, requires much skill and is mainly used on "new" software where vulnerabilities are unknown. (V15)
The other possibility is to go broad by automatically scanning many (different) devices and looking for known vulnerabilities in the discovered devices. This is automatic, so scales to large numbers of devices and device types. This type of scanning requires little knowledge and works best with devices running "stock software". Automated scanning only works on technical equipment, so will not report on "human vulnerabilities" (V16). A mixed set of security measures is therefore prudent.

Installing the scanning software or for using Shodan, initiating the scan, interpreting the finding, and resolving the vulnerabilities requires IT and some networking knowledge.

Asset management

IT Asset management[113] in automated VM is essential because the virtual IP address discovered by the vulnerability scan and used to report vulnerabilities needs to be linked to the correct device. In the in-home domain, automatically assigning dynamic IP addresses to connected devices using the DHCP protocol is standard. Using DHCP would mean that an IP address, assigned to the connected bear toy at moment A, can be assigned to a parental laptop at moment B. Although the VM scan output does give some pointers to the type of device scanned, especially with more protocol standardisation, finding the correct connected device to be patched might become a challenge. The home-router in standard in-home deployments is the device supplying the dynamic addresses and therefore has the most knowledge on which device at what time had which IP address.
The home-router itself also has a dynamic address which is configured on the outgoing interface towards the ISP network. This IP address is used by the home-router to communicate with the ISP network and allow for IP traffic to traverse between the internet and the in-home domain and vice versa. The dynamic address used by the home-router is supplied by the ISP and changes much less often than the IP addresses in the in-home domain[114].

Authentication

Automated or continuous VM is by default done using non-authenticated scanning technique[115]. Non-authenticated scanning means that no credentials are used to perform the scan for discovering vulnerabilities. By not using credentials, the scan can gather basic information about the system like Operating system name and version, which services are listening on which network port, and information leaked by the system like banners, open file shares and unsecured information. Using a list of default passwords does fall under the non-authenticated scan. Most VM solutions do allow for vulnerability scans using credentials, and this allows for more in-depth analysis of the vulnerabilities

[112] Foreman, *Vulnerability Management*, 2009.
[113] Sisco, "IT Asset Management."
[114] ISP01, "Interview with Dutch ISP Security Senior."
[115] Berkeley, "Continuous Vulnerability Assessment Authentication."

in the system. The downsides, however, outweigh the advantages for most standard deployments: Storing all credentials in one system (and altering these credentials on every password change) creates a very high-risk database. The risk of rendering systems, information, or accounts inoperable by using them for vulnerability scanning is usually seen as too high.

Home-router

In larger organisations, mostly dedicated scan equipment is used, but for scanning in-home domains individually, dedicated hardware is too expensive and cumbersome[116]. Therefore, in the in-home scanning solution, a computer already present in the in-home domain is used by the consumer to install the scanning software and run the VM scan. (V17)

In the standard in-home scenario, no network zoning is used to separate different connected devices. According to network and hardening best-practices however, zoning must be used to keep malware from spreading through the domain. When zoning is used, the vulnerability scan will only detect devices in the same zone as where the scan computer is located.

The solution would be to install the scanning software on the central home-router. The home-router is the central hub connecting all segments and internet. (V18) See Figure 10.

The downside of this model is that the scan vector does not resemble the vector for attackers (which usually is coming from the internet/ISP network).

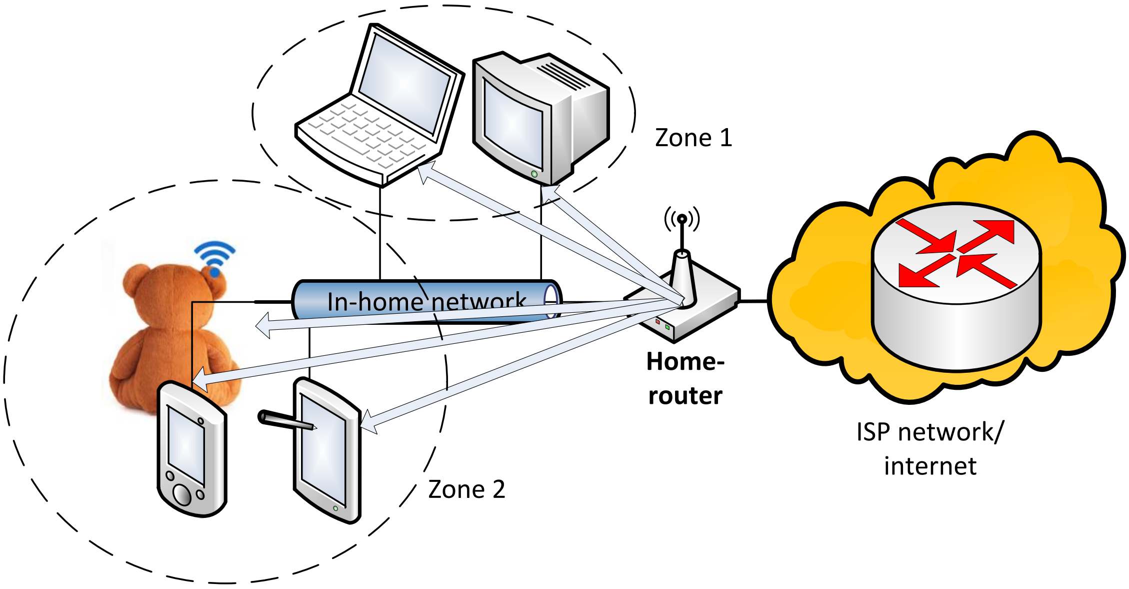


Figure 10 VM scan vector from home-router

Solutions to start VM scans from the home router are not widely available. When asked by telephone the before mentioned market leaders mention that they do not have home-router initiated VM software in the planning. F-secure has the “Sense” product[117] which is a home-router with the possibility to run Vulnerability scans. The SDK version can be used to run VM software on more vendor-agnostic hardware. Sense SDK will not run on home-routers currently deployed by the interviewed ISP’s because of limited IT resources on these platforms[118].

The interviewed suppliers state that at the moment VM is expensive because its use is mainly targeted at medium, large and enterprise business’. Also keeping the known vulnerability database up-to-date is resource intensive.

When introduced for a large population like the in-home domain, prices, however, would go down significantly. (V19)

[116] Supp02, “Telephone Interview with a Marketing Officer of a Security Products Vendor.”

[117] F-secure, “Sense SDK.”

[118] Supp02, “Telephone Interview with a Marketing Officer of a Security Products Vendor.”

2.6.3 Pros and cons

Like most security measures, VM has advantages and drawbacks. The three pros and cons 'from the book Vulnerability management by Park Foreman[119] , appended by the ones named in the interviews[120], are explained.

Advantage 1 is the scalability of automated VM. The possibility to automatically assess multiple devices from single or multiple locations simultaneously gives automated VM the edge when it comes to assessing multiple (different) devices.

Advantage 2 is the compatibility. All networked devices can be scanned without local actions or the need for compatible software on all devices under scanning.

Advantage 3 is the similarity of a VM scan to a real attack. Vulnerability scanning uses the same techniques as a hacker would do reconnaissance on which devices to attack. Hackers would also look for the weak points or vulnerabilities when scouting how to break into a specific domain or system. By mimicking this technique, the VM scan gives a representative view of the vulnerabilities open to attack.

Advantage 4 is the versatility of automated scanning. Vulnerability scans can not only scan for known weaknesses in software but can also detect the use of default passwords[121]. (V20) The scanner can mimic a user and try several combinations of passwords and report back on success or failures.

Advantage 5 is the ease of use regarding resolving. The knowledge of vulnerabilities does not benefit the safety of the in-home domain and is but the first step. After vulnerabilities have been found, they must be resolved. Because the vulnerabilities are known, standard resolving methods can be defined which help the consumer resolve the vulnerability with little IT knowledge.

Automated VM also has some drawbacks.

Drawback 1 is the visibility. The VM scanner can only scan devices which are connected and active on the network. When the scan, for instance, runs weekdays at noon, the chances are that devices that are not turned on during that moment (TV set top box, smartphones that are not at home) are not analysed for vulnerabilities.

Drawback 2 is the intrusiveness of automated scanning. The scanning process has an impact on the network and the device initiating the scan. (V21) When many devices are detected and scanned, the scan does pose a load on the network. Depending on where the scan is initiated from and the number of devices, this can slow the internet connection to a point where the scan results become erratic, and internet applications stop working. (V22). Some, mostly older, connected devices can temporarily stop working or even freeze when under aggressive automated scanning. (V24)

Drawback 3 are costs. With current prices, using commercial scanning solutions in the in-home domain is expensive to implement and maintain[122]. A significant cost component is the continuous process of making searching for new vulnerabilities and creating signatures which can then be used to scan for. When these costs are spread over an install-base like the in-home domain, prices are expected to go down[123].

Drawback 4 is the limitation of known vulnerabilities. Signature-based scanning methods like traditional virus scanning and VM depend on already discovered malware, and vulnerabilities. "behaviour" based methods like heuristic scanning[124] and network anomaly detection[125] can also detect attacks on unknown vulnerabilities by unknown malware. (v23)

Although no jurisprudence exists on doing VM in the in-home domain, VM could be considered as being intrusive according to the law computer criminaliteit 2", "net neutrality' and "GDPR" when the consumer gives no consent. More on this can be read in chapter 2.5

[119] Foreman, *Vulnerability Management*, 2010.

[120] Supp01, "Interview with a Security Products Chief Research Officer"; Supp02, "Telephone Interview with a Marketing Officer of a Security Products Vendor"; ISP01, "Interview with Dutch ISP Security Senior"; ISP02, "Interview with Dutch ISP Security Senior."

[121] Minsterie van economische zaken en klimaat, "Roadmap Digitaal Veilige Hard- En Software (Bijlage Bij 26643,Nr.535) - Parlementaire Monitor."

[122]"Http://Searchsecurity.Techtarget.Com/Feature/Comparing-the-Top-Vulnerability-Management-Tools"; Supp02, "Telephone Interview with a Marketing Officer of a Security Products Vendor."

[123] Supp02, "Telephone Interview with a Marketing Officer of a Security Products Vendor."

[124] Ször and Ferrie, "Hunting for Metamorphic."

[125] Ahmed, Naser Mahmood, and Hu, "A Survey of Network Anomaly Detection Techniques."

2.7 Summary

This chapter starts with the historical background of how the in-home IT domain came to be. The massive increase in bandwidth and availability of broadband for Dutch consumers resulted in a situation where the number of connected devices is forecasted to grow exponentially.

Next to the increase in numbers, ICT-enabled activities also integrate further into our daily routines, increasing the impact of failing connected devices to our lives. Consumers cannot keep pace with securing this increasing number of connected devices, and the complexity of connectivity between them, in their in-home domain.

The technical chapter explains the technical aspects of the in-home domain and proposes a model which reduces that complexity. This simplified model is used throughout the rest of this thesis.

Next to complexity, there is the increased risk introduced by a large number of devices connected to an open connectivity infrastructure which is the internet. This risk is explained using tangible examples.

To fill the void of consumers not being able to keep pace Dutch government together with stakeholders like the ISP have stepped in to help consumers secure the in-home domain. However, many different governance boundaries exist regarding consumers and their in-home domain, which complicates the helping efforts.

Through initiatives like setting standards, creating, or refining law, and educating users, stakeholders are trying to bring back the right balance between risk and security.

VM is one of the measures which could help with restoring this balance.

This raises the question whether VM can be executed in the in-home domain, and how this can be implemented. In the next chapter, the stakeholders are analysed which can play a role in doing VM in the in-home domain. Requirements are then gathered from this in-home environment analysis as well as the next stakeholder chapter. From these requirements a solution design is created, which results in the multi-stakeholder roadmap.

3 Stakeholders and actor analysis (A)

This chapter assesses which stakeholders have a role in doing VM in the in-home domain. This assessment is performed by first doing a literature analysis of the stakeholders and verifying this by doing interviews with representatives of most stakeholders. Only the stakeholders directly involved in doing VM in the home domain are mentioned.

The stakeholder groups are analysed and described in sub-chapters. These subchapters start with a brief description of the role that stakeholder group plays in securing the in-home domain, their behaviour, the responsibilities the group has, their incentives, and what is already being done by this group to secure the in-home domain. The second part of this chapter examines the behaviour and incentives of the threat actors that pose a risk to the connected devices located in the in-home domain. Requirements are derived from the stakeholder and actor analysis, which are used to design the roadmap in chapter 4. As mentioned in the research design, in the text, these requirements are mentioned by a letter followed by a sequence number. The requirements are enumerated in Appendix D Roadmap requirements.

3.1 Stakeholder overview

In the stakeholder overview, the simplified model, as designed in chapter 2 is used as a basis to determine the relevant stakeholders.

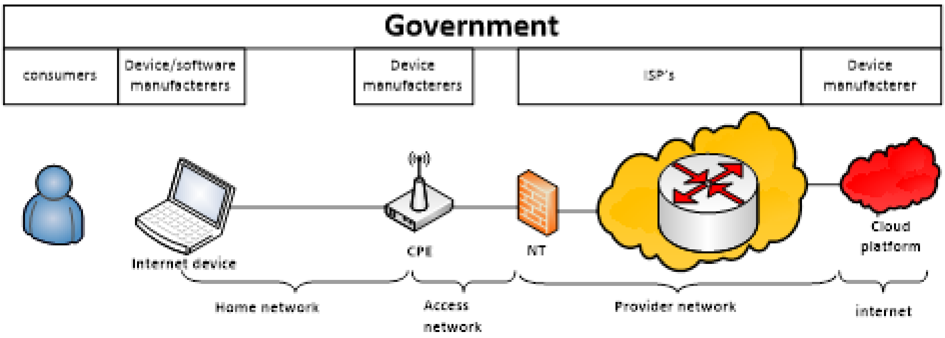


Figure 11 stakeholders in simplified in-home model[126]

Figure 11 shows the simplified model including the relevant stakeholders.

In short, consumers perform ICT-enabled activities with internet devices. The devices fall under the duty of care of the manufacturer[127]. In the case of internet devices, software and device can be uncoupled with regards to the duty of care. The Internet device is connected to the home-router which falls under the duty of care of the manufacturer. In most cases in the Netherlands, the home router is supplied by the service provider[128] based on lease-lend. The home-router is connected to the provider network, where the ISP has a duty of care[129]. In some cases, a cloud platform located on the internet provides services for the internet device to function[130]. Cloud services serving autonomous functions like google drive are not seen as being part of the in-home domain but can be used to attack the home domain, see Attack vectors 3.6.2. (A1)

[126] The stakeholder overview is based on Spriggs and Spriggs, "PDXScholar Survey of Security in Home Connected Internet of Things By." And interviews with stakeholders themselves.

[127] Cyber Security Raad, Wolters, and Jansen, "Ieder Bedrijf Heeft Digitale Zorgplichten."

[128] ISP01, "Interview with Dutch ISP Security Senior"; ISP02, "Interview with Dutch ISP Security Senior"; TNO ICT and Dialogic, "Vraag En Aanbod Next-Generation Infrastructures 2010-2020."

[129] Overheid.nl, "Telecommunicatie Wet"; Cyber Security Raad, Wolters, and Jansen, "Ieder Bedrijf Heeft Digitale Zorgplichten."

[130] SandersTamer, Mohammad A. Noureddine, Ahmed Fawaz, "A Game-Theoretic Approach to Respond to Attacker Lateral Movement."

3.2 The consumer (C)

The consumer is the physical person using and responsible for the connected device(s) in the home domain. As the person performing the ICT enabled activities, the consumer is the first line of defence in securing the in-home domain. Without the consumer practising some security hygiene, securing the in-home domain will be an almost impossible endeavour. Using a home analogy: no amount of locks or alarms will help if the door is left wide open.

As seen in chapter 2.3, the consumer group consists of individuals who use connected devices in a variety of ways. The home domain is often used by several physical persons each owning one or multiple connected devices in the home domain[131](C1). In this chapter, these different users of the in-home domain are simplified to 1 person (per household) which has the contractual agreement with the ISP and is responsible for all connected devices in his home.

3.2.1 Consumers & IT security awareness

Consumers, according to research done for Alert online[132], generally think of themselves as having sufficient to good cybersecurity skills. The most significant exception to this belief are the skills for the use of internet connected devices. (see Figure 12 Self-assessment cybersecurity skills. This belief on skills regarding connected devices is consistent with the literature[133] and the answers of the interviewees[134]. These sources state that consumers, with regards to connected devices, can generally be characterised as persons who are not security savvy[135]. Consumers are generally unaware of the risk introduced by connecting devices and do not adhere to security best practices like hardening, installing updates and changing the default password[136]. The CBS report states that consumers do upgrade their software when upgrading is automated by the vendor[137]. (C2)

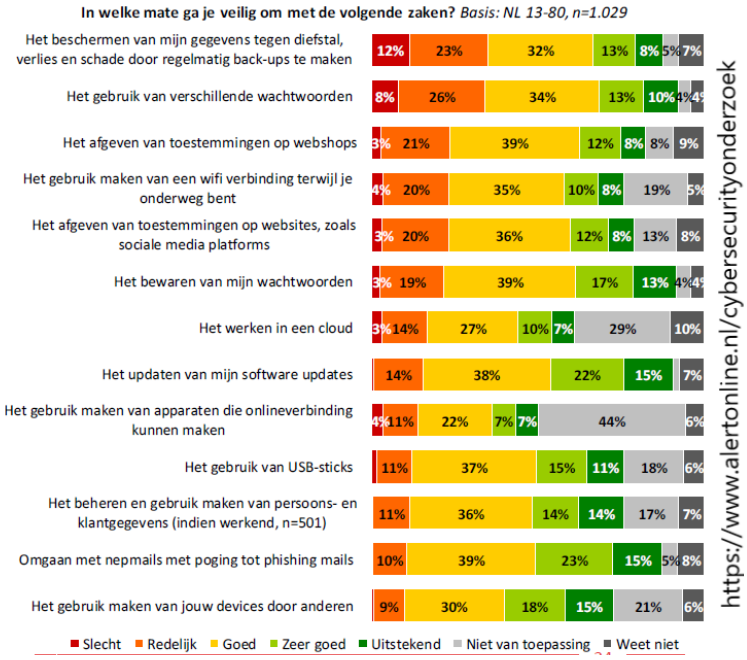


Figure 12 Self-assessment cybersecurity skills

43% of Dutch consumers are worried about their security which is also shown in figure 8. An interesting thing to note is the finding that people worry more about security in their in-home environment than in their work environment. One of the explanations can be found in the responsibility people feel. 71% of consumers feel responsible for being able to roam the internet from their private computer at home. At work, 16% feel responsible for being able to use the internet safely, where 64% of respondents think this responsibility lies with the employer.

[131] statista, "House Hold Distribution the Netherlands"; Kritzinger and Von Solms, "Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement."

[132] Online, "Alert Online."

[133] Schneier, "The Psychology of Security"; Centraal bureau voor de Statistiek, "Mobiele Telefoon Minder Vaak Beveiligd Dan Computer."

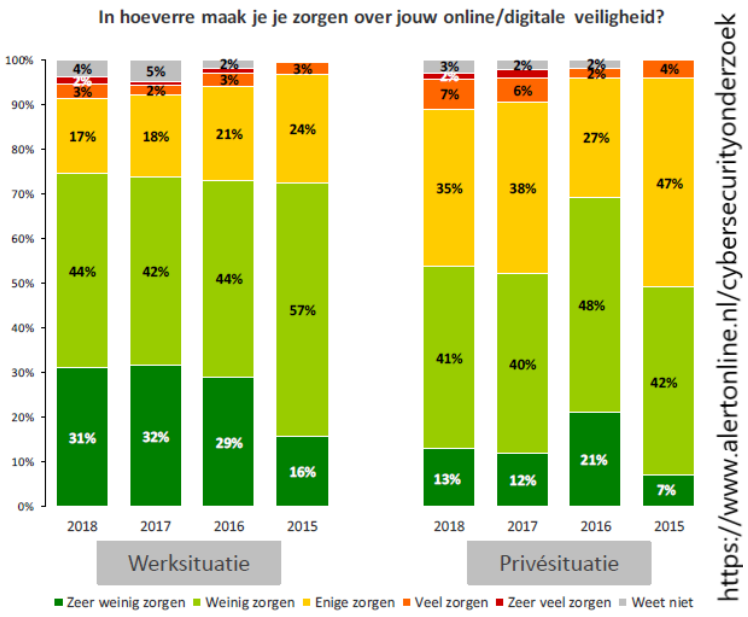
[134] DP01, "Interview with Policy Officer Dutch Parliament 19-10-2018"; Reg01, "Interview with a Dutch Regulatory Policy Specialist on 4-10-2018"; Reg02, "Interview with a Regulatory Policy Specialist on 08-10-2018"; ISP01, "Interview with Dutch ISP Security Senior 15-08-2018"; ISP02, "Interview with Dutch ISP Security Senior 19-09-2018"

[135] ISP02, "Interview with Dutch ISP Security Senior"; DP01, "Interview with Policy Officer Dutch Parliament."

[136] Schneier, "Schneier on Security"; Farooq et al., "A Critical Analysis on the Security Concerns of Internet of Things (IoT)."

[137] CBS, "Nederland Koploper in Gebruik van Veiligheidssoftware."

That people feel the responsibility to secure their in-home domain is also shown in figures from the CBS from 2011. These figures show that consumers in the Netherlands are among the highest in the EU with regards to the use of security software[138]. The researchers explain these figures by stating that Microsoft Windows, the OS used by over 80% of consumers[139], installs its security tooling automatically[140]. Research on awareness shows that only 43% of consumers install anti-virus software themselves[141]. Research done on connected devices running security software[142] shows that amongst connected devices, the number of devices running security software is even lower[143]. The security software vendors confirm this deduction[144] and explain this because security solutions for connected devices are in short supply compared to computers.



https://www.alertonline.nl/cybersecurityonderzoek

Figure 13 Consumer awareness research on digital safety.

In the alert-online survey 2018[145], with 36% of the respondents having a smart tv, and 31% having a wireless printer, these are the most often used connected devices in the in-home domain (apart from tablets, PC's, and smartphones). When asked for the risk that the tv gets compromised, ¾ of respondents' value that chance very small. The printer being compromised Is valued even less opportune with 80%. Security is seen by consumers as a commodity[146]. People want security but don't want to pay a premium for it (C3). Price and functionality are the main drivers for selecting the connected device. Even when security would be a criterion for consumers, no standards or tests are available to consumers who would allow for a good security comparison to make a well-weighted decision[147]. For consumers, the security of connected devices is a lemon market now[148]. (C4 & C5)
A way for consumers to react to his lemon market situation is to stand up for their rights in court. However, a lack of jurisprudence, legal uncertainty on duty of care principles, and far-reaching contractual obligations by connected device vendors make it almost impossible for individuals to go to court over a lack of security of a connected device[149]. De Consumentenbond started a court case against Samsung in 2015 for prolonging the time Samsung devices got security update, but this case was settled in favour of Samsung[150]. (C6)

[138] CBS. "Nederland Koploper in Gebruik van Veiligheidssoftware."
[139] Statista, "Global Operating Systems Market Share for Desktop PCs, from January 2013 to July 2018."
[140] Consumentenbond, "Windows Defender Worst Virusscanner of the Test."
[141] Alert online, "Nationaal Cybersecurity Bewustzijnsonderzoek."
[142] Farooq et al., "A Critical Analysis on the Security Concerns of Internet of Things (IoT)"; Brightsight, "Assessing the Security of ' Simple ' IoT Devices."
[143] Alert online, "Nationaal Cybersecurity Bewustzijnsonderzoek."
[144] Supp01, "Interview with a Security Products Chief Research Officer"; Supp02, "Telephone Interview with a Marketing Officer of a Security Products Vendor."
[145] Alert online, "Nationaal Cybersecurity Bewustzijnsonderzoek."
[146] Harald Bauer, Ondrej Burkacky, "McKinsey: Security in the Internet of Things."
[147] DP01, "Interview with Policy Officer Dutch Parliament."
[148] Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism."
[149] Wolters, "Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten."
[150] Rechtbank Den Haag, "Consumentenbond Tegen Samsung."

3.2.2 Organisations assisting de consumer

The following organisations focus on the security of consumers in the cyber domain:

“de Consumentenbond”[151] is active in helping consumers with the security of connected devices in several areas. On the Consumentenbond website tips and tricks are given to consumers on what actions to take[152]. Consumentenbond is active in testing security of connected devices and (security) software[153]. From the legal side, Consumentenbond has set minimum demands regarding security updates[154] and went to court with Samsung over the update terms of Samsung devices[155]. Occasionally Consumentenbond shares input and experiences with Dutch[156] and E.U.[157] governmental organisation on how to tackle security in the in-home domain.
The view of Consumentenbond, with regards to flaws in connected devices, is broader than security, Functionality reduction, like tv’s losing app support, are also covered by their actions. The solution to securing the in-home domain, according to Consumentenbond, mainly lies with the manufacturer taking responsibility for a duty of care for their products and vendors for not selling “crappy products”. The law currently offers insufficient possibilities for this. Consumers do play a role but can only be held responsible when he or she has been seriously negligent (C7 & C8). Awareness can play a role in educating consumers on the risks, but consumers now cannot recognise a well-secured product. Therefor Consumentenbond sees the manufacturer and vendor as the most critical players in resolving the vulnerabilities in insecure connected devices in the in-home domain[158] .

“Vereniging eigen huis”, when asked on their role in Vulnerabilities in the in-home domain, mentions[159] having written about the privacy of the “smart meter”[160]. “Vereniging eigen huis states that, regarding the in-home domain, they value freedom of choice and privacy. Security, however, is not touched upon in these statements.

Consumer organisations like “De nationale ombudsman”[161] and “De geschillen commisie”[162] responded not being part of the discussion around consumer IT safety. They only act on a more reactive basis to issues which arise from interactions between government and consumers. So, when the roadmap is implemented these organisations can assist the consumer, but only on an individual per-case basis. (C9)

“Bits for freedom” responded not being able to participate in this research[163].

[151] consumentenbond, “Phone and Mail Conversation Met Consumentenbond Augu.”
[152] consumentenbond forum, “Schandalig Privacy Beleid van Polar.”
[153] Consumentenbond, “Windows Defender Worst Virusscanner of the Test.”
[154] consumentenbond, “The 9 Demands Regarding Security Updates.”
[155] Rechtbank Den Haag, “Consumentenbond Tegen Samsung.”
[156] consumentenbond, “Phone and Mail Conversation Met Consumentenbond Augu.”
[157] BEUC, “Cybersecurity for Connected Products.”
[158] consumentenbond, “Phone and Mail Conversation Met Consumentenbond Augu.”
[159] vereniging eigen huis, “Mail Conversation.”
[160] Vereniging eigen huis, “Slimme Meter.”
[161] De nationale ombudsman, “Telephone Conversation.”
[162] Geschillencommisie, “Telephone Conversation.”
[163] Bits of Freedom, “Mail Thread.”

3.2.3 Interviewee's opinion on "the consumer".

The interviewees mention[164] that about 10% of consumers are ICT technology adept and early adopters of new technology like smart lighting and smart home equipment. This ICT adept group, the interviewee's expected, would, in theory, be able to detect vulnerabilities in most common devices and resolve them when a patch is available. (C10)

Overall the interviewees expect that most consumers install patches when the patch management is (semi-) automated which is confirmed by the CBS[165][166]. Consumers are reluctant to put much effort or money into securing the in-home domain although they know they are running a risk[167]. The interviewees expect the reasons to be:

- The lack of knowledge; consumers generally don't know how to secure their in-home domain.
- The feeling of low risk; Consumers assume that they as individuals will not be attacked.
- The externality[168] between the consumer bearing the security cost but not the effects. Banks, when attacked, lose money either directly or through a loss of reputation. When consumers are attacked they often lose little because lost money is often repaid by insurance or bank and stolen data is often of little value to the consumer. When the consumers' devices are used in a DDOS attack, the negative effects are felt by the target, not the consumer. (C11)

The interviewees expect that when the consumer would bear the negative effects of attacks on their ICT enabled activities, they would invest more time, money, and effort into securing their connected devices. Consumers, however, are not expected to be able to deal with all complexities surrounding securing their ICT enabled activities[169]. Therefore, organisations like the government and ISP's should help them secure these ICT enabled activities[170]. (C12)

Due to ISPs not being able to deliver 100% uptime, and incidents around 2010 in the media with deep packet inspection[171], consumers in the Netherlands experience some distrusts against the ISP sector in general[172]. The ISP's have since been working on an image to regain the trust of the consumer[173].
"Trust takes years to build, seconds to break, and forever to repair"[174] (C13)

[164] ISP01, "Interview with Dutch ISP Security Senior"; ISP02, "Interview with Dutch ISP Security Senior."

[165] Centraal bureau voor de Statistiek, "Mobiele Telefoon Minder Vaak Beveiligd Dan Computer."

[166] CBS, "Nederland Koploper in Gebruik van Veiligheidssoftware."

[167] NCTV, "Cybersecurity Bewustzijnsonderzoek 2018: Driekwart Getroffen, Helft Komt Niet in Actie Na Cybercrime."

[168] Herley, "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users."

[169] DP01, "Interview with Policy Officer Dutch Parliament."

[170] Romanosky, "Examining the Costs and Causes of Cyber Incidents."

[171] College bescherming persoonsgegevens, "Analyse Gegevens Mobiel Dataverkeer Kpn."

[172] ISP02, "Interview with Dutch ISP Security Senior."

[173] ISP02.

[174] Quote from unknown author.

3.3 The connected device manufacturers. (M)

Introducing connectivity to existing devices is performed by a wide range of industries. Manufacturers want to take advantage of the potential of the generated data and connectivity functions[175]. The drive of most manufacturers, however, is universal: Generating sustainable profit[176]. This drive has made increasing speed to market for functionality while lowering cost important.

One of the advantages for manufacturers of connecting devices is that by making a device connected, manufacturers can get valuable insights by collecting data generated by the connected devices. Location and movement, device usage, purchasing preferences, and health information are just a few of the data examples that can give valuable insights to manufacturers. The flipside to these insights is that they give insight into the personal environment of the consumer, which consumers do not want to be revealed, and which is therefor protected under privacy law[177].

The manufacturer has a duty of care to protect assets like the device, its functions and the data generated when stored on the systems of the manufacturer[178]. To protect these assets, security measures must be implemented. Manufacturers often see these security measures as a cost centre which also delays development[179]. Verbruggen and Wolters analysed that the lack of focus on security by manufacturers can be explained by Market failure, Legal uncertainty, far-reaching restrictive contract terms, and the complexity of the connected device product chains. These four factors will be explained in this section.

3.3.1 Complex product chains

Especially for the manufacturers new to connecting devices, like the manufacturer of home appliances, securing their devices proves to be a challenge[180]. The possible delay and costs of focusing on the broad spectrum of security make that newcomers often choose to buy an “embedded connectivity module” or “Cyber-physical module” from the 3rd party[181] like Google[182]. That way manufacturers do not have to develop a connectivity module but can buy the connectivity functionality and install this module in their device. Implementing a cyber-physical module, however, does not absolve the manufacturer of the connected device to implement security measures like hardening, and updates, default passwords must be changed. Unneeded services need to be disabled[183] and so on.

Updates from the embedded module supplier need to be implemented into the software together with the other software modules controlling other modules within the connected device. Then this new composite of software must be tested for correct functioning and interaction with other modules on the hardware. When multiple hardware versions exist, all must be tested with the software or different software versions must be maintained. When correctly tested, the software must be released by the connected device manufacturer.

The duty of care towards the customer is the responsibility of the manufacturer or vendor delivering the end product. However, due to the complexity of having multiple interacting modules, liability is shared with the module suppliers using complex contracts[184]. (M1) (M2)

[175] Lee and Lee, “The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises.”

[176] Berry, *Discovering the Soul of Service: The Nine Drivers of Sustainable Business*.

[177] Lee and Lee, “The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises.”

[178] Cyber Security Raad, Wolters, and Jansen, “Ieder Bedrijf Heeft Digitale Zorgplichten.”

[179] Wolters, “Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten.”

[180] AB01, “Interview with Abuse Specialist”; Gershenfeld, Krikorian, and Cohen, *The Internet of Things*.

[181] Friess, *Internet of Things - from Research and Innovation to Market Deployement*.

[182] Zhang, “IoT Security: Ongoing Challenges and Research Opportunities.”

[183] coursera, “Network Hardening Principles.”

[184] Wolters, “Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten.”

3.3.2 Legal uncertainty and restrictive contract terms

Right now, legal uncertainty still does not give sufficient incentives to the connected device manufacturers to take security adequately seriously[185]. Legal texts mentioning "correct technical and organisational measures"[186] without elaborating on "correct" make it hard for manufacturers to know what is expected from them. Without a specification in the law, Case law would for manufacturers be the next best thing in establishing the correct boundary for the type of security measures needed to abide by the duty of care as expected by Government. Unfortunately, almost no case law is available regarding correct implementation of duty of care by manufacturers. [187]

For consumers to go to law with a connected device manufacturer over vulnerabilities, the costs and duration of a lawsuit are not in proportion to the benefit for the consumer to have a vulnerability resolved. Consumers are therefore assigned to collective actions or public interest litigation cases. One example of such a public interest litigation case is the lawsuit where the Consumentenbond sued Samsung for not delivering a patch to recent Samsung Android devices which contained the vulnerability "Stage fright"[188]. The ruling, however, was in favour of Samsung because according to the judge, the Consumentenbond had not been able to clarify utility and necessity of Samsung issuing a patch sufficiently.

The clarity of duty of care is made even vaguer using exoneration clauses and other restrictive clauses in the general conditions of use. These clauses, which a user must comply with to be able to use the device or software, often[189] contain far-reaching obligations and restrictions for consumers and are used to exclude all forms of liability and temper expectations with regards to cybersecurity[190]. Although the legality of these notions goes against term 1a of the directive 93/13/EEG[191]: *"inappropriately excluding or limiting the legal rights of the consumer",* they do pose a hurdle for consumers before going to court. (M3)

To resolve the legal uncertainty, at the snapshot moment, the European Commission was working on a minimum set of requirements mandatory for connected devices. This minimum set includes patching requirements[192].

From the private side, Google in Mai 2018 announced that it would require integrators of their embedded modules to issue security patches regularly[193]. This means that manufacturers using Google's android hard and software will be contractually obliged to issue security updates at regular intervals. By clarifying and concretising the law on what a consumer can expect from a connected device manufacturer, exoneration clauses also lose a lot of their function in keeping consumers from going to court to stand up for their rights to secure connected devices and software. (M4)

3.3.3 Market failure

The market for connected devices has the potential to combine three markets: durable goods, software, and consumable goods[194]. The example of the connected refrigerator best explains this statement. In the non-connected world, a refrigerator is a durable good which is purchased by making a one-time payment. By connecting the device, the refrigerator can order consumable goods online without human intervention. By offering this as a service, companies like Amazon[195] combine the market for durable goods with consumable goods. These services can then be offered based on a subscription, which allows for monthly revenue. As software running on the refrigerator enables this service, Amazon could choose to run only proprietary software, or limit the shops the

[185] Wolters, "Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten."
[186] autoriteit persoonsgegevens, "Verantwoordingsplicht."
[187] Wolters, "Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten."
[188] Rechtbank Den Haag, "Consumentenbond Tegen Samsung."
[189] consumentenbond forum, "Schandalig Privacy Beleid van Polar."
[190] Wolters, "Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten."
[191] council of the european communities, "Directive on Unfair Terms in Consumer Contracts."
[192] Reg01, "Interview with a Dutch Regulatory Policy Specialist."
[193] Schoon, "Google Requires OEMs to Roll-out Regular Android Security Patches."
[194] Perera, A. Zaslavsky, Christen, "Context Aware Computing for the Internet of Things: A Survey."
[195] Amazon, "Amazon Fresh."

refrigerator can use. This amount of control over users' everyday life and new options for creating revenue attract business.
To be able to participate in the connected device market, large enterprises like Google, Amazon, Apple, and Philips make substantial investments to gain a first mover advantage on network effects[196] and platform economics[197]. Platform economics allows for several benefits to the device manufacture[198] from which information expansion is most lucrative to the in-home domain. Information expansions mean that the device manufacturers have access to the data generated by the connected device. In the historical situation, the devices and their data mostly resided in the in-home domain where functions were performed. With platform-based services data is transported to the cloud (and often stored there) to be able to perform actions. The downside in this situation is that the data in such a business model is vulnerable to attacks, even when the in-home domain is secured[199]. (M5)
The efforts to be a first mover to be able to benefit from a network effect means that manufacturers will go to market with a new product even when known vulnerabilities still reside in the software[200]. This behaviour is facilitated by consumers, because Consumers regarding connected devices often go for the lowest price, instead of valuing security thus creating a market failure.[201] An addition to this is that even when the consumer has security in high regard, he is not able to discern between well secured and poorly secured devices because standards are lacking.
Taking the first quote of this chapter, due to market failures where only price matters, connected device suppliers with poorly secured devices but quick go to market will prevail. (M6)

3.3.4 Protective measures by manufacturers in the in-home domain

Self-regulation by industry on securing connected devices did not yield the intended results[202]. This led the "Cybersecurity Raad"[203], the "NCSC"[204], and "Agentschap Telecom"[205] to advice the E.U. to act on lowering risks posed by connected devices together with industry. The E.U. together with member states decided to do a pilot on refining the duty of care of manufacturers by setting mandatory requirements on the security of connected devices[206]. Mandatory certification is also explored, but due to complex E.U. product law,[207] this might come slightly further away in time.

The most important way to protect connected devices is by employing proper IT hygiene. This is done by periodically installing software updates and security patches and complying to security recommendations and standards[208]. These updates and patches are made available by the software supplier or connected device manufacturer and remediate known vulnerabilities and defects in the software. By patching these security holes, attackers cannot use these vulnerabilities to compromise the device. The effectiveness of this solution is determined to a great extent by the ease of use of performing the update. When the patching process is automated, devices in the in-home domain are usually patched[209], but when manual actions are required by the consumer, then the patch-rate

[196] Waluszewski, "Hoping for Network Effects or Fearing Network Effects."
[197] Diana Farrell, "The Online Platform Economy: Has Growth Peaked?"
[198] Oxera Economics Council, "Benefits of Online Platforms: Technical Appendix."
[199] Sangiovanni-Vincentelli et al., "Benefits and Challenges for Platform-Based Design."
[200] Caulkins, "Sell First , Fix Later : Impact of Patching on Software H . John Heinz III School of Public Policy and Management Sell First , Fix Later : Impact of Patching on Software Quality."
[201] Wolters, "Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten."
[202] Reg01, "Interview with a Dutch Regulatory Policy Specialist."
[203] cyber security raad, "' Naar Een Veilig Verbonden Digitale Samenleving ' Advies Inzake de Cybersecurity van Het Internet of Things (IoT)."
[204] Nationaal Cyber Security Centrum (NCSC), "Cyber Security Assessment Netherlands 2017."
[205] Telecom, "Staat van de Ether 2017: Onveilige IoT-Apparatuur Risico Voor Samenleving."
[206] Reg01, "Interview with a Dutch Regulatory Policy Specialist"; Reg02, "Interview with a Regulatory Policy Specialist"; ISP02, "Interview with Dutch ISP Security Senior"; DP01, "Interview with Policy Officer Dutch Parliament."
[207] DP01, "Interview with Policy Officer Dutch Parliament."
[208] Herley, "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users."
[209] CBS, "Nederland Koploper in Gebruik van Veiligheidssoftware."

drops dramatically. It is also possible to install a personal firewall which blocks attacks on these and unknown vulnerabilities. The drawback of this measure is that the software needs to be available. Either the patch should be available to be able to update, or the “personal firewall” software needs to be available. The second drawback is that when the installation is not automated, Effort and skill are needed by the user to do the installation and possibly maintenance. (M7)

Safeguarding the endpoint device from malware is traditionally a task for the Virus scanner (or malware scanner). Virus scanners no longer compare every piece of data with a virus definitions database but also do anomaly detection and behavioural analysis. By detecting unusual behaviour, or certain patterns, a virus scanner can detect viruses that are not present in the database and alert the user or even prevent malicious action before it is executed. Virus scanners are present on almost 90% of all Dutch PCs, laptops[210] and even tablets and smartphones often have virus scanners installed[211]. On connected devices like smart-home equipment or other IOT however, virus scanners are almost inexistent and hardly viable[212]. (M8)

3.3.5 A special notion: the home-router manufacturer

Although a connected device, the home-router has a special role because it is the gateway for the in-home devices towards the internet. Because of its direct connectivity to the internet is poses a bigger risk, as discussed in chapter 2.4.5. However, also, from a manufacturer standpoint, it is a “special” because in the Netherlands most ISP’s deliver a home-router which is also managed. The software running on the home-router, which is managed by the ISP, is also security tested at regular intervals by the ISP and is hardened where possible[213]. With the implementation of the Net Neutrality notion A5 (users can choose their endpoint device), ISP’s are worried that security will be impacted for the worse because end-users will have to manage their home-router including security[214]. (M9)

Another risk when allowing the consumer to buy and manage their own router is that the market failure as discussed in chapter 3.3.3 could also impact the home-router. In the managed home-router situation, the ISP selects the home-router based amongst other things on quality of security[215]. Because the Dutch ISPs mainly supplies home-routers at the moment no bulk market exists in the Netherlands. Home-routers are mainly sold to tech-savvy consumers with high demands[216] which also includes security. When users can choose and manage their own router, ISPs expect that the reason of choice in most cases will be to lower costs. This will lead to the same market failure as discussed in chapter 3.3.3 where the security of the home-router will be negatively impacted by cost pressure. (M10)

3.3.6 Protective measures deployed on the home-router

The most basic defence here is the implementation of a firewall blocking unwanted traffic. This measure is activated by default on the routers supplied by the Dutch ISP’s who were interviewed[217]. Because the consumer traffic is dynamic, only from internet incoming traffic which was not initiated from the in-home domain is blocked. A more granular setting would improve the security of the in-home domain, but this requires skill and effort from the consumer. Attacks like email phishing[218] can bypass the firewall present on the router because it is seen as normal email traffic.

Another measure which can be deployed from the CPE is Antivirus software that vendors have available that can be implemented on the router to detect and block traffic streams to known malicious sites[219][220]. The downside is twofold: The costs of the software and updates make that this option is only available on routers in higher price segments. The second drawback is that these kinds of solutions only filter out the known malicious sites.

[210] CBS. “Nederland Koploper in Gebruik van Veiligheidssoftware.”
[211] Centraal bureau voor de Statistiek, “Mobiele Telefoon Minder Vaak Beveiligd Dan Computer.”
[212] Man01, “Interview with Manufacterer of Security Measures.”
[213] ISP01, “Interview with Dutch ISP Security Senior”; ISP02, “Interview with Dutch ISP Security Senior.”
[214] Economische, “Beleidsregel Netwerkaansluitpunt.”
[215] ISP01, “Interview with Dutch ISP Security Senior”; ISP02, “Interview with Dutch ISP Security Senior.”
[216] ISP02, “Interview with Dutch ISP Security Senior.”
[217] ISP01, “Interview with Dutch ISP Security Senior”; ISP02, “Interview with Dutch ISP Security Senior.”
[218] Krejčířová and Dvořák, “Phishing – the Threat of Internet Banking.”
[219] Asus, “AiProtection.”
[220] Man01, “Interview with Manufacterer of Security Measures.”

3.4 The ISP (I)

This chapter starts with the motivations of an ISP to help secure the in-home domain, followed by a short notion on what already is performed and what an ISP can contribute in the light of VM. Little literature exists on Dutch ISP's and their motivations to secure the home domain. Therefore, a qualitative analysis is done using literature on ISP's worldwide and interviews with CISO's and personnel of the two main ISP's serving home connections (market share in-home connectivity VodafoneZiggo (43.6%) and KPN (41.2%)[221]) in the Netherlands.

3.4.1 Motivations for the ISP to help secure the in-home domain

Within the scope of this thesis, the ISP is mainly tasked with supplying connectivity between the home domain and the internet. The ISP however also supplies the home domain with services like Television, mobile and fixed Telephony services, and often email and security services.
The ISP has a contract with the consumer to transport all-in and outbound traffic through the ISP's network to the internet. The ISP is legally[222] and contractually[223] obliged to protect the continuity of its network and ensure the continuity of the services delivered to its customers(I1). From the interviews, it can be deduced that ISP's are motivated to help protect customers from digital harm from an economic perspective[224]. The reasons mentioned by the interviewees:

- ISP's compete on customer satisfaction, and consumers often perceive security problems in the in-home domain as a connectivity problem, leading to dissatisfaction.
- ISP's must invest in security measures like Abuse to comply with the duty of care. Estimations by ISP's in 2009 were that an incoming abuse call costs around 8 euro, while an outgoing call, to for instance notify a user of a malware infected device, costs 18 euro[225].
- Increased social importance contributes to positive branding.

Additionally, the literature review showed that another reason is the fear for blacklisting by other ISP's. The Internet is based on networks being interconnected, and when "ISP X" is the source of lots of abuse traffic, then a repercussion by these other ISP's can be to blacklist and thus block all traffic from "ISP X". The direct and indirect costs for ISP X to lift the ban are an incentive to implement security measures.[226] (I2)

3.4.2 Security measures already deployed

The interviewees of both interviewed ISP's state that they have taken security measures to ensure continuity of service and to improve their customer satisfaction. These measures can be grouped into three main categories of implementation[227]:
Fully external: security measures that are delivered by the ISP for the consumer to secure the in-home domain.
The interviewed ISPs all mention delivering add-on security services like F-secure virus scanning[228]. These services are offered at a minimal cost and can be used to increase the security of computers, smartphones, and tablets in the in-home domain. These security services cannot be used on more dedicated connected devices like connected washing machines or home domotics.

Fully internal: security measures deployed by the ISP to secure the in-home domain. A good example is the Abuse mechanism.

[221] telecompaper, "Marktaandeel Analyse."
[222] overheid.nl, telecommunicatiewet.
[223] VodafoneZiggo, "Algemene Voorwaarden Ziggo"; KPN BV, "Algemene Voorwaarden Voor Vaste En Mobiele Telecommunicatiediensten D."
[224] SOC01, "Interview with SOC Manager"; ISP02, "Interview with Dutch ISP Security Senior"; ISP01, "Interview with Dutch ISP Security Senior."
[225] Bauer and Eeten, "Cybersecurity : Stakeholder Incentives , Externalities , and Policy Options."
[226] Bauer and Eeten.
[227] Rowe et al., "The Role of Internet Service Providers in Cyber Security Project Leads."
[228] KPN BV, "KPN Veilig"; VodafoneZiggo, "Internet Beveiliging."

All interviewed ISP's take part in the "Abuse information exchange"[229] This exchange is a foundation funded by government and most Dutch ISP's with the purpose of working together by sharing information on consumers who are known to have malware-infected devices. The abuse information exchange relies on sources reporting on known infected devices. These infected devices are mostly discovered by their connectivity to the command & control(C&C) server[230]. Malware and the C&C function are continuously evolving making it harder for the exchange to detect and report[231]. Eliminating the vulnerability used by the malware would eliminate the source instead of remediating the effects of the infection.

The Abuse information exchange passes the infection data to the ISP hosting the consumer owning the infected device. The ISP can then take measures to keep the infection from spreading while informing and helping the affected consumer to clean his or her equipment of the malware.

The most common reaction from Dutch ISPs, when alerted to a malware infection, is to validate the infection and then to inform the affected customer and restrict his or her connection to a confined Quarantine environment. This environment is specifically designed to help the customer clean his systems from infection without spreading the infection to other customers or the internet. In this case, the ISP uses the "risk control" exception, mentioned in the Net neutrality law chapter, as a reason to purposely not comply with the Net neutrality shaping and equality principles based on a known threat to the ISP's network[232].

Another measure deployed by the ISP is securing of customer premise equipment. These CPE's are delivered by the ISP's to be placed in the in-home domain for a specific function. Examples are the set top-box which transcodes the television feeds, or the home-router which is already explained in detail in chapter 3.3.5. These devices and their software are security tested before deployment and new software for these devices is also tested before being implemented.

ISP's in the Netherlands also deploy measures that are network based like port blocking of notorious spam abuse ports[233] or DNS based malware detection[234]. These measures are all implemented to safeguard the network. Not all ISP's deploy the same security measures. This is dependent on the network topology deployed by that ISP. Shared medium networks[235] , for instance, are secured differently than dedicated networks because of the crossover effects to other customers.

Upcoming technologies explored by ISP's[236] are the use of artificial intelligence to do network anomaly detection. Network anomaly detection[237] is already done in enterprise networks[238] but proves to be challenging to deploy in more heterogeneous data streams which differ continuously. Therefore, doing anomaly detection on the central ISP side might be challenging. Software vendors are working on decentralised systems[239] where the AI is performed on the home router[240]. This, however, comes at a cost both in hardware, where the home-router hardware must be upgraded and in development on the software and home-router manufacturer side.

Hybrid internal /external: Imposing policies on consumers which makes the consumer part of the securing effort.

ISP's nowadays put customers with devices participating in a botnet into a closed remediation environment as described in "Fully internal". The customer receives a standard mail informing him or her of the restriction and some standard tips on how to resolve standard infections. The ISP prevents blacklisting that way, but the technically incompetent person often cannot resolve the

[229] "Abuse Information Exchange."
[230] AB02, "Interview with an Abuse Specialist."
[231] Ali et al., "ZombieCoin 2.0: Managing next-Generation Botnets Using Bitcoin."
[232] ISP01, "Interview with Dutch ISP Security Senior"; ISP02, "Interview with Dutch ISP Security Senior"; Bauer and Eeten, "Cybersecurity : Stakeholder Incentives , Externalities , and Policy Options."
[233] ISP02, "Interview with Dutch ISP Security Senior."
[234] "Privacy-Friendly Threat Detection Using DNS."
[235] TNO ICT and Dialogic, "Vraag En Aanbod Next-Generation Infrastructures 2010-2020."
[236] KPN ventures, "KPN Ventures Provides Growth Capital to CUJO AI for International Expansion."
[237] Ahmed, Naser Mahmood, and Hu, "A Survey of Network Anomaly Detection Techniques."
[238] Darktrace, "The Enterprise Immune System."
[239] Supp01, "Interview with a Security Products Chief Research Officer."
[240] Supp02, "Telephone Interview with a Marketing Officer of a Security Products Vendor."

vulnerability or becomes re-infected. ISP's are researching how to inform the customer better, so the infection time is decreased, and customer satisfaction is increased. Although not directly responsible for remediating infections in the in-home domain, ISP's from a corporate social responsibility point of view want to invest more time and effort into informing customers when an infected device is discovered[241] by giving more actionable information to the consumer. Research by Altena[242] reveals that consumers only act on the infection when placed in Quarantine, but when Quarantined, sending actionable information shortens the infection time. Future research could be to deploy more granular quarantine measures. Instead of Quarantining the whole in-home domain, configuring the home-router only to disallow infected devices access to the internet might prove to decrease the impact of the Quarantine security measure on consumers. (I3)

Another example of a hybrid solution is where ISP's deploy spam scanners which label emails suspected to be spam. The users must make the conscious choice to open the email after acknowledging that they understand the risk and knowingly open the email.

3.4.3 ISP's and government

ISP's in the Netherlands are relatively heavily regulated by the Dutch government[243] and a shared belief between 2005 and 2011 was that ISP's should do even more[244]. The reasons named were that ISP's have more information and are more technically capable then consumers. Several ways to get the ISP to act were analysed: Legal incentives by; McCullagh (2005) et all, Lichtman and Posner (2004), Parameswaran et all (2007); or by monetary incentives: Huang, Xianjun and Whinston (2007), Rowe et all (2011).

Dutch ISP's, however, do not aspire to become the *"police officers of the in-home domain" and* feel responsible for delivering continuous and open connectivity for their customers[245] without knowledge or interference with what the customer does with the connection. The ISP feels responsible for ensuring that the service is delivered continuously and that customers do not obstruct the use of the internet for other users. (I4)

After interviewing consumer organisations, governmental organisations, and ISPs the focus of who should solve the vulnerabilities in the in-home domain seems to be shifting from an ISP focus towards having the manufacturer solve the vulnerabilities. This seems logical since the ISP can only mitigate some effects of an attack, but cannot resolve the root cause, which is resolving the vulnerabilities which are present in the software. On the other hand, vulnerabilities present in unsupported hard- and software nowadays will never be patched. Therefore, a proper balance must be established between measures deployed by the different stakeholders.

[241] AB02, "Interview with an Abuse Specialist."

[242] Altena, "Exploring Effective Notification Mechanisms for Infected Iot Devices."

[243] Rowe et al., "The Role of Internet Service Providers in Cyber Security Project Leads"; Reg02, "Interview with a Regulatory Policy Specialist."

[244] Rowe et al., "The Role of Internet Service Providers in Cyber Security Project Leads"; Bauer and Eeten, "Cybersecurity : Stakeholder Incentives , Externalities , and Policy Options."

[245] ISP01, "Interview with Dutch ISP Security Senior"; ISP02, "Interview with Dutch ISP Security Senior."

3.5 Dutch government (D)

The Dutch government observes that the digital and physical world are becoming more and more intertwined. As a result, the consequences of digital vulnerabilities become more intrusive for people in their normal life. Although 100% digital safety is seen as unfeasible, measures are needed to achieve the optimal level of digital safety. These measures are researched and defined in several Dutch governmental organisations. [246]

In the Netherlands, the safety and security of connected devices used by consumers is the responsibility of the Ministry of Economic Affairs and Climate (EZ & K). Regulation of consumer connected device manufacturers regarding security is the Agentschap Telecom (AT) for the more technical aspects while the Authority for consumer and markets (ACM) is focused on the legal aspects with regards to ISP's and consumer law.[247]

This section explains the role of the Dutch government in securing in the in-home domain. The chapter roughly follows the structure as set out in the Roadmap Digital safe hard-and software released by the ministry of EZ &K in April 2018[248]. The contents of the roadmap about implementing VM in the in-home domain are validated in interviews with employees working for ACM, AT, the Ministry of EZ &K, and a policy officer of a member of the Dutch parliament. Their views are also incorporated in this chapter to enrich the findings of the beforementioned roadmap.

3.5.1 The roadmap and its measures

The goal for the digital safe hard- and software roadmap, called roadmap in this chapter, is to define a balanced set of security measures to improve the digital safety of hard and software. The nine measures with a short explanation are:

Standards and certification: the use of standards for connected devices helps both security by design, and security when in use. Certifications and standards can lift the security lemon market principle[249] by enabling consumers to differentiate between safe and unsafe products. At the moment many standards exist on securing connected devices[250]. This diversity of standards leads to confusion amongst consumers who do not know what standard to look for in a connected device.

Another difficulty is that none of the security standards for connected devices is mandatory in the Netherlands.

To accomplish a wide acceptance and create enough leverage over manufacturers, The Dutch government works together with the E.U. on establishing a Cybersecurity Act (CSA) and European certification scheme(ECS). The CSA will be the overarching framework under which the ECS will be introduced. The ECS, when deployed, overrules all local certification schemes of E.U. members. This certification scheme will be gradually made mandatory starting with high-risk product groups. The requirements which must be met to become certified are established in working groups, which consist of relevant international public and private organisations together with standardisation bodies.

Monitoring digital safety of products: Even with mandatory standards, the introduction of insecure devices is possible. Manufacturers can go bankrupt or, given the international nature of the connected device market and the sampling methods of customs, devices can be imported and connected to the in-home network. Therefore, sharing information about vulnerabilities with consumers, manufacturers, and vendors is crucial. Consumers can decide not to buy connected

[246] Staten-generaal, "Antwoord Op Vragen van de Leden Van Toorenburg En Verhoeven over Het Bericht 'Experts: Overheid Moet Ingrijpen Bij Internetapparaten.'"

[247] DP01, "Interview with Policy Officer Dutch Parliament"; Min01, "Interview with 2 Ministerial Cybersecurity Policy Officers"; Reg01, "Interview with a Dutch Regulatory Policy Specialist"; Reg02, "Interview with a Regulatory Policy Specialist."

[248] Minsterie van economische zaken en klimaat, "Roadmap Digitaal Veilige Hard- En Software (Bijlage Bij 26643,Nr.535) - Parlementaire Monitor."

[249] Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism."

[250] ENISA, *Baseline Secur. Recomm. IoT Context Crit. Inf. Infrastructures*; TNO, "Tno: Dealing Securely With the Internet of Things."

devices, manufacturers can stop using an insecure embedded device, and vendors can stop selling insecure devices.
The Dutch government works together with industry and international parties on creating a mechanism to track insecure equipment.

Cleaning infected devices: although the roadmap says cleaning infected devices, this measure means that ISPs can contribute to fighting unsafe devices in the same way that ISP's are fighting botnets[251]. Dutch ISP's use different methods for notifying customers[252]. (D1) As described in chapter 3.4.2, the abuse mechanism locates infected devices participating in a botnet and quarantines the entire in-home environment of the customer. The ISP's cannot clean infected devices located in the in-home domain. Even if the ISP's offered consultancy services to clean the infection, it would be in the same manner as a tech-savvy customer would clean the infection him-or herself[253]. For resolving the vulnerability, the ISP would also be at the mercy of the manufacturer to supply a security patch of sorts which fixes the vulnerability. If not patched, the device will become infected again the same way it got infected before cleaning. The Dutch government wants ISP's together with the abuse hub to report infected devices, discovered on the internet, to the owner of the in-home domain. Table 2 shows the customer journey mapping[254] of a consumer being informed by an ISP on vulnerabilities in his domain:

ISP informs the non-technical customer on an infection in the in-home domain with Quarantine

Reporting method	Information from ISP to customer	Customer experience
Informational	Infection X has been detected in your domain which can be resolved by patch Y. Click the link in ISP notification to install the patch.	The customer will feel pleased because he can secure his domain without much effort.
The patch does not work	Infection X has been detected in your domain which can be resolved by patch Y. Click the link in ISP notification to install the patch. The link sends the wrong update rendering the device inoperable	The customer will feel displeased because his device is rendered inoperable. He will call the ISP and maybe claim damages
Current	Infection X has been detected in your domain which can possibly be remediated by following one of the following solutions, followed by a list of security vendors or long, detailed technical instructions	The customer will feel displeased because he must invest time and effort. There is a possibility that the proposed solutions will not work or that the infection cannot be cleaned.
VM scan	Infection X has been detected in your domain which can be remediated by following one of the following solutions, followed by a list of security vendors. By clicking the link, the ISP can scan your domain. More specific information to resolve the infection follows.	The feel of the customer will differ, but the extra choice to allow the ISP to help will appeal to some customers. This is also dependent on the incentive model (for instance: paid, unpaid) The ISP could limit the quarantine to only the infected device (future research)[255]
No patch	Infection X has been detected in your domain which at the moment cannot be remediated because a patch is not available.	The customer will feel displeased because he cannot remediate the infection without disconnecting the device.

Table 2 Customer journey map of a consumer being informed by an ISP

[251] Ministerie van economische zaken en klimaat, "Consumentenagenda: Houvast Bij Voortdurende Verandering."
[252] Altena, "Exploring Effective Notification Mechanisms for Infected Iot Devices."
[253] AB02, "Interview with an Abuse Specialist."
[254] Verhoef, "Understanding Customer Experience Throughout the Customer Journey."
[255] Supp02, "Telephone Interview with a Marketing Officer of a Security Products Vendor."

As can be seen from this customer journey map, only a combined approach of detection and resolving of a vulnerability leads to positive customer satisfaction. (D2) The impact of the Quarantine measure could be minimalised when only the infected device can be quarantined instead of Quarantining all devices in the in-home domain. This requires the development and deployment of segmentation and Quarantining on the home router[256]. When asked to verify, the ISP's responded that this would also raise the need for automation of the Quarantine measure, because the current (half)manual Quarantine processes do not scale to the volume of connected devices which are expected. (D3)

Testing for digital safety: With testing, vulnerabilities can be discovered in different phases of the product life-cycle. The roadmap mentions that manufacturers of connected devices can do penetration testing to discover vulnerabilities in their products. The second function named is to have business and organisations doing cybersecurity scans. Part of these "cybersecurity scans" can be done on consumers in the form of automated vulnerability scans, which is the result of the VM roadmap for the in-home domain as proposed in this thesis. (D4)

Cybersecurity research: Research must be done to create innovative solutions to cope with safety challenges.

Liability: Creating the possibilities for consumers to appeal to liability law can incentivise hard-and software manufacturers to invest in securing their products. The significant modification to already established liability law is to clarify and concretise vague terms like faulty, sufficient, proportionate measures with regards to software. This measure is complementary to the minimal security demands and mandatory certification for connected devices. (D5)

Legal requirements, supervision, and enforcement: By setting minimum safety requirements unsafe connected devices can be banned from the market. All interviewees from governmental agencies point to the Radio equipment directive as the legal vessel that is going to be appended by the E.U. to contain the rules regarding the security of connected devices. The interviewees expect the RED to be operational within a 2-year timespan. When operational, enforcement is needed to encourage vendors and manufacturers to abide by the law. Various supervisory bodies will help maintain the digital security of hardware and software in the Netherlands. The ACM will, for example, supervise consumer protection, the Autoriteit persoonsgegevens will supervise on privacy regulations, and Agentschap Telecom will supervise the technical standards and manufacturing industry in the Netherlands. The interviewees mention working on supervisory plans and preparing for their new role of securing connected devices to be able to fulfil their task as soon as the RED is appended. The governmental organisations mention wanting to establish the rules together with the industry by starting with self-regulation, because the industry has the most knowledge of the technology and how to secure them[257]. (D6)

Awareness and empowerment: Dutch government invests in Awareness campaigns like "veiliginternetten.nl" for safe hard- and software. Campaigns are aimed at making consumers and business organisations aware of the security risks and resilient when a risk materialises. The goal is to enable people to make purchase choices where they can include security as one of the aspects. (D7) (D8)

Purchasing policy of the national government: By only investing in secure products the Dutch government leads by example as well as stimulates, as large user of hard and software, the demand of secure hard- and software.

[256] Supp01, "Interview with a Security Products Chief Research Officer"; AB02, "Interview with an Abuse Specialist."

[257] Reg01, "Interview with a Dutch Regulatory Policy Specialist."

3.6 Threat actors and their attack vectors (T)

Risk alone does not bear adverse effects. A threat actor must exploit the risks for the risk to materialise into adverse effects to the device under attack. This chapter describes what malicious actors abuse the vulnerabilities present on devices in the in-home domain and what attack vectors are available to them. The chapter ends with the selection of attack vectors relevant to the scope of this thesis.

3.6.1 Malicious actors

On the criminal side, a multitude of malicious actors have a motivation to attack connected devices in the in-home domain. These actors benefit in several ways. Some steal data (IP or personal information[258]) or money (crypto mining[259]), some alter data for monetary gain (ransomware[260], bank fraud[261]) or pleasure (gaming DDOS[262]), or to fill their malicious toolkit for attacking better-protected targets or vital infrastructure (MIRAI[263]).
This chapter uses the new cyber threat actor topology of M de Bruijne et all[264] as a basis. In his paper, M. de Bruijne argues that a threat actor topology must be exhaustive and relevant. Since this thesis focusses on a method to gain insight into vulnerabilities in the in-home domain more than on the actors abusing them, this chapter is based on a simplification of actors as described in the Cybersecurity assessment of the Netherlands (CSAN) of 2018[265], published by the NCSC. The CSAN methodology for threats and actors is based on a direct attack by the actor on a target. From an NCSC perspective, the target of actors attacking the in-home domain is the consumer and his or her connected devices. The CSAN refers to consumers as members of the public. The term consumers is used due to consistency.
Table 3 Actors & threats is a list originating from the CSAN 2018[266]. The list shows by whom consumers are most likely to be attacked, followed by a tangible example.

The scope within which to fit the attacker in this thesis is broader than the definition of the CSAN. Where the CSAN only focusses on *"threats originating from various actors against various threats"*[267], this thesis and chapter also take into account the scenario where an attacker attacks the consumer in order to use the in-home IT equipment to mount an attack on other organisations, as justified in chapter 2.4.2. In the CSAN 2018, this threat of in-home equipment being used as a catalyst to attack other organisation is mentioned shortly as *"The use of third parties"*[268]. With this notion, the NCSC describes that vulnerabilities in consumer IT equipment are exploited without altering the functionalities as not to alert the owner/user of the equipment. The control of these so-called drones or zombies is then sold in batch as a DDOS service to malicious actors which use the drones in their attack of the organisation of their choosing.
With this widened comprehension of threat actors in relation to the consumer in-home equipment also becoming a "tool" for attackers to go after "bigger fish", the number of actors also increases to incorporate all other actors[269].

[258] Farooq et al., "A Critical Analysis on the Security Concerns of Internet of Things (IoT)."
[259] Azmoodeh, "Detecting Crypto-ransomware in IoT Networks Based on Energy Consumption Footprint."
[260] Azmoodeh.
[261] Khrais, "Highlighting the Vulnerabilities of Online Banking System."
[262] Richard A. Paulson; James a webber, "CYBEREXTORTION."
[263] Kolias et al., "DDoS in the IoT: Mirai and Other Botnets."
[264] Bruijne, van Eeten, and Pieters, "Towards a New Cyber Threat Actor Typology A Hybrid Method for the NCSC Cyber."
[265] "European Cyber Security Perspective 2018."
[266] NCSC-NL, "Cybersecuritybeeld Nederland 2018."
[267] "European Cyber Security Perspective 2018."
[268] "European Cyber Security Perspective 2018."
[269] NCSC-NL, "Cybersecuritybeeld Nederland 2018."

ACTOR	THREAT	MOTIVATION
STATE SPONSORED	*Espionage*; By accessing information in the in-home domain, the state actor is, for instance, able to gain personal information of the consumer for extortion purposes. Extraction of intellectual property through homeworkers is another example.[270]	*Gain intellectual property* *Gain control over persons* *Gain an anonymous platform of attack* *Gain intel on procedures and persons*
CRIMINAL	*Information/system manipulation*; Criminals try to manipulate banking transactions, performed by the consumer, to divert the money to their accounts.[271] *Information theft*; criminals, steal personal information which is sold on the black market.[272]	*Monetary gain through banking fraud* *Monetary gain by selling personal information*
SCRIPT KIDDIES	*Information theft*; Script kiddies steal information to conceal themselves in further attacks or just as a price to make a name for themselves.[273]	*Just for fun* *Gain an anonymous platform of attack*
UNINTENTIONAL ACT	*Leak*: A consumer copying personal information on a USB stick and loose that USB stick.[274]	

Table 3 Actors & threats[275]

3.6.2 Attack vectors

Vulnerabilities in connected devices in the in-home domain can be attacked using different attack vectors[276]. Figure 15 shows the locations from which an attack can occur as an icon of an unwanted person with a number. Each location is explained in Table 4 attack vectors. The "number" column corresponds to the attack vector in Figure 14, the "location" names the location where the attacker attacks from. Column "curable by VM" is filled by combining the technical simplification (Figure 5) with the attack vectors (Figure 14). These two figures are combined to make a deduction whether VM, in theory, can resolve vulnerabilities needed to exploit the corresponding attack vector successfully.

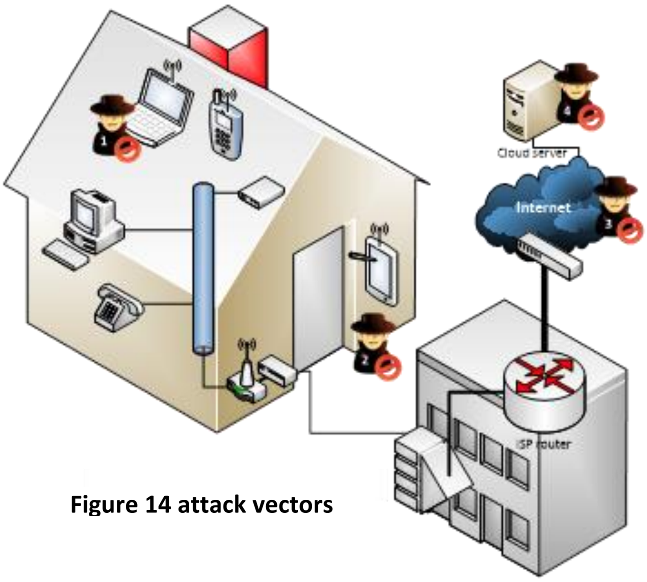


Figure 14 attack vectors

As can be deducted from Table 4, VM can account for reducing the surface of attack for most attack vectors. However, in some situations, using VM alone is not sufficient to secure the in-home domain entirely. For an attack to have a significant impact on Dutch society, generally they must be deployed en-mass. This makes attack vectors which need local access less likely to be used. Attack vector 4 (the cloud attack) can be deployed remotely but cannot be detected by VM. This shows that giving insight into vulnerabilities in the home domain is only part of a range of measures needed to secure ICT-enabled activities deployed by consumers.

[270] ZDNET, "Russian Hackers Are Attacking Home Routers, ISPs and Business Firewalls to Spy and Steal Data, Warns US, UK."
[271] Khrais, "Highlighting the Vulnerabilities of Online Banking System."
[272] "European Cyber Security Perspective 2018."
[273] McAfee, "7 Types of Hacker Motivations."
[274] Elmrabit, Yang, and Yang, "Insider Threats in Information Security Categories and Approaches."
[275] NCSC-NL, "Cybersecuritybeeld Nederland 2018."
[276] Hansman, "A Taxonomy of Network and Computer Attacks."

Nr	**Situation**	**Explanation**	**Curable by VM**
1	Attack from inside the in-home domain using an infected device	An attacker, using a compromised connected device within the in-home domain as a stepping stone, can attack another device without having to deal with the security measures on the outer shell of the domain.[277]	Partly, although the attacker already gained access to a device in the in-home domain, resolving of vulnerabilities on other devices, limits the attack footprint and thus can prevent the attacker from gaining access to other devices. Removing the malicious code from the infected device is dependent on the code and the measures already deployed by the attacker to maintain access.
2	Attack by being physically near the building and join RF traffic	An attacker or device physically located near the home breaks into a connected device by tapping into RF signals that radiate outside the physical house. This can be done by hacking the WIFI connection, but also by abusing other RF protocols like Bluetooth, ZigBee, or z-wave.[278][279]	Partly, by resolving vulnerabilities in the WIFI access points, the consumer can harden its WIFI network which makes unauthorised access much harder. Vulnerabilities on non-IP devices like Z-wave are in most cases not found since the IP gateway hides the z-wave devices from the being scanned.
3	Attack from anywhere in the logical transport path (man in the middle) of the traffic or with logical access to the home router	An attacker with access to equipment handling the connectivity between the connected device and for instance the supporting cloud server can control traffic by receiving, altering, and resending that to the destination.[280]DNS altering attacks and attacks using remote systems management attacks are part of this attack vector	Partly, some VM solutions can also scan communication types used and can report when vulnerable protocols like telnet and HTTP are in use. Even when informed, consumers would most likely not be able to change this into a secure transmission protocol. The home-router would be the ideal place for this attack so hardening the home router is important. (see chapter 2.4.5)
4	Attack from anywhere with logical access on a trusted service platform.	An attacker with access to the cloud service servicing the connected device can remotely change the parameters or extract information of the connected device without ever connecting to the in-home domain.[281]	No, the trusted cloud needed by the connected device to fulfil its function is located on the internet. From a VM viewpoint, this cloud is just one of the systems on the internet and is not part of the VM scope
#	Non-networked attack	An attacker can corrupt the firmware which is used to run connected devices or the CPE even when these devices are not connected. This will give the attacker access to the in-home domain even without network access. A famous example is Stuxnet[282]	No, when not networked, VM is unable to detect the attack. Installing security patches is still possible of course.

Table 4 attack vectors

[277] SandersTamer, Mohammad A. Noureddine, Ahmed Fawaz, “A Game-Theoretic Approach to Respond to Attacker Lateral Movement.”

[278] digicert, “Wi-Fi Is Hacked and so Are Your IoT Devices?”

[279] Ronen et al., “IoT Goes Nuclear: Creating a Zigbee Chain Reaction.”

[280] Gangan, “A Review of Man-in-the-Middle Attacks.”

[281] All, “The Design of Smart Home Platform Based on Cloud Computing.”

[282] Symantec, “W32.Stuxnet.”

3.7 Summary

In this chapter the stakeholders defending, and the actors attacking the in-home domain are analysed. The chapter starts with the defensive side, assessing the consumer, the device manufacturer, the ISP and Dutch government.

The consumer is the first line of defence but values his or her knowledge regarding the security of connected devices as low. Also, the consumer is not organised and omnifarious, which makes it difficult to make a fist against large manufacturers. Several requirements are deduced which show that this is a problem to be solved. Requirements set by the Dutch government on this topic are to set clear liability for securing devices and making manufacturers responsible for resolving these vulnerabilities. This could however contradict to the requirements most stakeholders have around measure being cost efficient. Balancing costs and benefits is important for VM to be successful.

The manufacturer's main incentive is to make a profit and moving into the connected devices market promises opportunities in network effects and platform economics. At the moment not many positive incentives exist to deliver secure products. Securing connected devices is often seen as a cost centre, which also slows down developments needed to take advantage of the opportunities.
Law that could make for negative incentives when lacking in security at the moment is too vague and cumbersome for the consumer to be used against manufacturers in a court of law. Several requirements show that these laws must be transparent and unambiguous for VM to work.

The ISP, although not responsible for securing the in-home domain, plays a role in securing this in-home domain because it is the intermediary between in-home domain and the internet. At the moment, ISP's already detect zombies in the in-home domain and do endpoint security testing. The incentive for the ISP to invest in these measures is, that adverse effects originating from infected connected devices, are often seen by consumers as a connectivity problem caused by the ISP, resulting in customer dissatisfaction. Requirements from the ISP not to become the police officer of the internet combines badly with the requirement of the Dutch government for the ISP to play a role in the in-home domain.

The Dutch government has made an overarching roadmap to increase the security of connected devices. The requirements in this roadmap can roughly be reduced to three points. Create and refine law to clarify the roles and responsibilities of stakeholders, create awareness and empower consumer to battle insecure connected devices, and make security transparent to consumers by introducing standards and seals.

From a threat actor viewpoint, many threat actors are interested in the home domain. Whether for attacking directly (banking fraud, crypto jacking) or for use as a tool to go after bigger targets (botnets). Attackers can use a number of attack vectors, and VM can help in reducing the attack surface of the connected devices in the in-home domain, as part of a balanced set of security measures. For VM to be able to do so, requirements were deduced which allow VM to detect vulnerabilities which pose the highest risk of being abused by threat actors.

In the next chapter the requirements are analysed and used to form the solution model. The steps needed to design and implement this solution model are then plotted in the multi-stakeholder roadmap.

4 multi-stakeholder roadmap for implementing consumer vulnerability management.

This thesis started with the sense of urgency of dealing with vulnerabilities in connected devices in the in-home domain. After this, the in-home environment was explained using the 3-Layer model followed by an analysis of the relevant stakeholders. Requirements were gathered in these chapters which are used to construct the multi-stakeholder roadmap and explain the actions in this chapter. These requirements are displayed in Appendix D for easy reference.

The multi-stakeholder roadmap to implement consumer vulnerability contains the steps per VM function which are needed to implement VM in the in-home domain.

The roadmap does not fill in all requirements because some requirements, for instance, contradict because of conflicting incentives. The timelines are based on the timelines gathered in the interviews and the literature study. These timelines can vary significantly due to technical and governmental complexities. Addressing vulnerabilities in the in-home domain is not yet at an advanced stage, and an unambiguous joint goal is not yet committed upon by all stakeholders. Therefore, the stakeholders' roadmaps start by defining roles and responsibilities.

4.1 Requirements analysis

4.1.1 Requirements mapped on the three-layer model

In Table 5 the requirements are mapped to the three lenses of the 3-layer model[283].

3-layer lens	Requirements
Technical	C2;D3,4;G3,5;I3;M5,9;R1,2,3,4;T1,2;V1,8,9,13,14,15,17,18,20,22,23,24
Socio technical	C8,9,11,12;D7,8;G6,20;M7;V11,16,21
Governance	A1,C1,3,4,5,6,7,10,13;D1,2,5,6;G1,2,4,7,8,9,10,11,12,13,14,15,16,17,18,19;I1,4;M1,2,3,4,6,8,10;V2,3,4,5,6,7,10,13,19,25

Table 5 requirements per 3-layer lens

Governance lens

The result shows that most requirements come from the governance lens. This could be due to an unbalanced set of resources; however, the interviewees confirmed that the list of stakeholders was complete. Therefore, a more likely explanation is that, at the moment of doing the interviews, the governance of connected devices in the in-home environment was being shaped. Law was being made on roles and responsibilities, the duty of care, liability, type of regulation. These governmental uncertainties also translated into the requirements for doing VM in that same in-home domain. Therefore, every roadmap for direct stakeholders starts with defining roles and responsibilities.

For the solution design, governance is also seen as the trigger to break the current market failure where security of a connected device is given insufficient priority in the purchase and use/maintenance phases. Clear rules on duty of care should lead to regular security updates which are a starting point for doing VM.

Another explanation is that most interviewees fulfil a governance role within their organisation. The reason for this governance interview focus is that, where VM is a standard best-practise in hardening hard- and software devices which are documented extensively, implementing this solution in the Dutch in-home domain is new.

Socio-Technical lens

The requirements with a socio-technical character can be explained in three parts:

Consumers must be helped by government and industry to increase knowledge and skill to a sufficient base level, so they can include security in their behaviour (buying, using). Of course, these requirements are backed by governmental requirements like setting reasonable security standards and seals.

[283] Berg et al., "On (the Emergence of) Cyber Security Science and Its Challenges for Cyber Security Education."

The second part is that consumers have to be helped in understanding their role in securing the in-home domain and also the threats and responsibilities that come with using connected devices. For instance, most home-routers at the moment are managed by the ISP. When a consumer claims his or her right to purchase and use a home-router, that consumer must know that from that point, he or she is also responsible for the security of that device. At the moment Dutch law does not provide for this, but apart from that, the consumer must be made aware of this before installing the freedom of choice for endpoints.

The third part is for consumers to know their right concerning the duty of care of connected devices. Consumers, whether or not helped by consumer organisations, need to know what their rights are concerning the security of connected devices and how they can claim these rights.

Technical lens

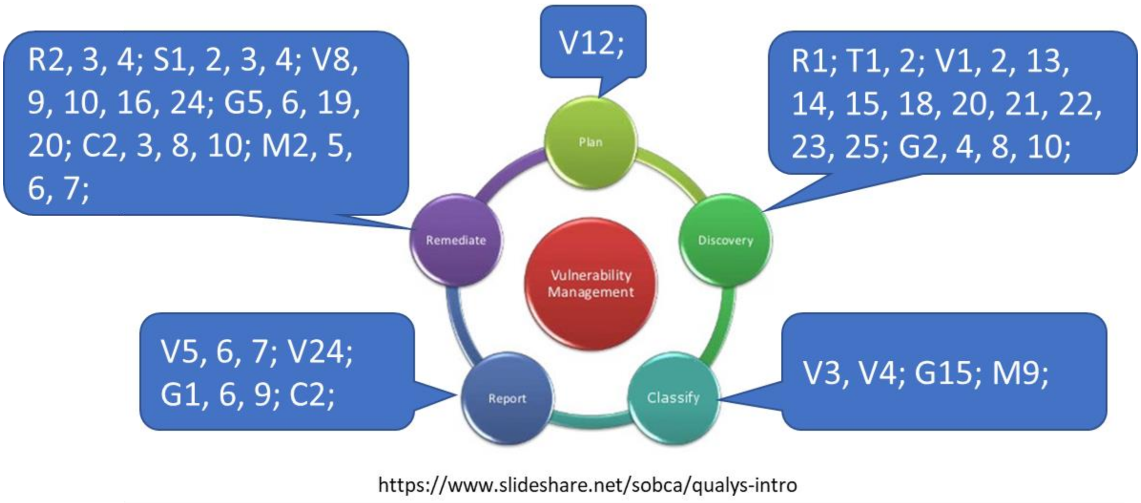
The requirements with a technical character roughly sort into three groups:

The first group consists of requirements for the remediation process. The availability of remediations methods, in particular, security patches, is paramount before controlling vulnerabilities is useful. Knowing which critical vulnerabilities are present without a way of dealing with them does not reduce the risk to acceptable levels. Therefore, the second step, after defining roles and responsibilities is for the manufacturer to start testing devices, which are in the field, and release security patches or other methods of remediating these known vulnerabilities. Important for successful remediation is that the method for deploying the fix to a vulnerability is easy to undertake for a consumer with little knowledge and skill of IT. Preferably the method is installed automatically, and only fixes the vulnerability without altering other characteristics.

The second group consists of the vulnerability discovery method. Several requirements are set which determine the visibility of the scan: IP based devices must be detected, default passwords must be detected, and scan vector must mimic an attacker. Since the discovery scan can influence the behaviour of connected devices, the scanning method must be tuned to have as little effect on the devices under scan as possible.

The third group of requirements describes the demands regarding the data that is collected with the vulnerability scan. This data, which consists of customer devices and vulnerabilities present on those devices, can be regarded as very confidential. Apart from the VM use of presenting the customer with an overview of vulnerabilities in their domain, in the wrong hands, it may also lead to harm. A list of vulnerabilities could come in handy for an attacker when preparing for an attack on a specific person. However, also consider the scenario in which a detective can check by a smartphone from a criminal, to which other domain that smartphone has been connected to, which devices were in that domain and which vulnerabilities can be abused to gain access. Although some will see this as a functional step, others will abhor the privacy infringement.

4.1.2 Requirements mapped on the vulnerability management model


R2, 3, 4; S1, 2, 3, 4; V8, 9, 10, 16, 24; G5, 6, 19, 20; C2, 3, 8, 10; M2, 5, 6, 7;
V12;
R1; T1, 2; V1, 2, 13, 14, 15, 18, 20, 21, 22, 23, 25; G2, 4, 8, 10;
Plan
Discovery
Classify
Report
Remediate
Vulnerability Management
V5, 6, 7; V24; G1, 6, 9; C2;
V3, V4; G15; M9;

https://www.slideshare.net/sobca/qualys-intro

Figure 15 Requirements per VM step

In Figure 15 the VM specific requirements are also mapped to the steps of the VM model in the previous chapters. Since most explanations are given in the previous section, the three most noteworthy events are displayed below:

- Forty-one requirements could not be attributed to one of the steps of the vulnerability model. These requirements can roughly be divided into two groups. The first group one consists of mainly governmental, requirements about roles and responsibilities that have to be established and laws that “steer” stakeholders in adhering to those roles and delivering what is expected of them. The second group of requirements relate to both technical and governmental aspects of the VM solution itself. These requirements describe what kind of technical vulnerabilities must be detected, that the (personal) data has to be protected, and that home-router require special priority.
- Only one requirement can be attributed to “plan”. Probably this relates to the earlier comment that stakeholders mostly had a governance scope. Since VM is not introduced yet, the first scan takes the most effort to set up. After setting up the first cycle, replanning that cycle will take less effort.
- Most requirements can be attributed to remediate. This can be explained because several different possibilities exist to do remediation. Security patching is the most prominent measure to solve vulnerabilities, but also measures like incentivising tech-savvy consumers to assist others, Abuse measures, and awareness fall within this category.

In the following subchapters, these requirements are plotted in a roadmap. Because the actors performing the actions are not yet assigned, suggestions are made based on the analysis described.

4.2 Solution overview

In this subchapter, a generic overview is given of the VM scanning solution based on the requirements and the analysis described earlier. The structure follows the three lenses of the three-layer model.

4.2.1 Technical solution overview

The technical model mainly describes the “discovery phase” and the Remediation phase of the VM steps. The discovery phase is the phase where the connected devices are scanned for vulnerabilities.

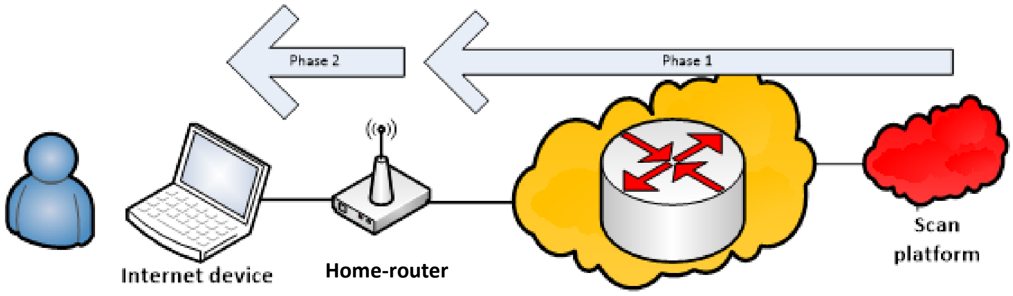


Figure 16 VM scanning model

The discovery in the solution design is split into 2 phases as can be seen in Figure 16, because of three reasons:

1. The discovery scan must be representative of the threat actors' attack vector. The threat actor in most cases attacks from the internet.
2. The Home-router is the optimum device to discover connected devices in the in-home domain. However, VM software has to be developed, before the discovery scan can be launched from the home router.
3. The Home-router is the gateway between the in-home domain and the ISP domain. Although at the snapshot moment, most home-routers are managed by the ISP, the home-router is an endpoint device which, according to net neutrality law, can be bought, employed, and managed by the consumer. In the case of a user-owned home-router, the ISP loses sight over the in-home domain and is thus unable to scan for vulnerabilities anymore.

Phase 1 discovery

Anyone on the internet can already deploy the discovery scan of phase 1 (see the Shodan scan in Figure 8). However, because of the dynamic use of IP addresses, attributing the vulnerabilities to the correct consumer would be very hard. Consumers can look up his or her IP address by visiting https://whatismyipaddress.com/ using a device in the in-home domain. An internet-based scanner can then scan the IP address shown. Considering the analysis of the consumer in chapter 0, these steps would probably go beyond the skills of many consumers with little IT skills.
The second organisation with knowledge of the consumer and the IP addresses is the CIOT because the ISP is obliged by law to hand over IP address and consumer information to the CIOT on a daily basis[284]. The CIOT, however, is only allowed to use this data for criminal investigations, which VM is not.
The third organisation is the ISP. The ISP hands out the IP addresses to the home-router dynamically and has a contract with the consumer. Handing over the consumer and IP data to a secondary party who deploys the scan would be troublesome from privacy and competitive perspective.

The ISP’s network is in the path between the internet and in-home domain so that the attack vector can be mimicked. The ISPs already do VM on the home-routers they manage, and from a technical perspective, they could also scan the home-router in the consumer-owned scenario.
Concluding: from a technical perspective, the ISP is best suited to deploy the VM scan of phase 1 and report the findings for the right consumer. From an attack vector and risk perspective, the home-router is one of the most critical devices on which to mitigate vulnerabilities.

[284] Ministry of justive and safety, “Telecomgegevens Voor Opsporing.”

Phase 2 discovery

The discovery scan of phase 2 can only be deployed from a device in the in-home domain, because the home-router stops most connections like discovery scans, coming from the internet.
As explained in chapter 2.6.2, the consumer has several possibilities to do the discovery scan in the in-home domain. The majority of consumers, however, are not able to deploy this scan because of the knowledge deficit.
From an ISP perspective, the only possibility is to do the discovery scan from the home-router. 2 main VM software vendors state that scanning from a home-router is possible[285]. However, the software would have to be designed and built (6 months), and most routers currently deployed by ISP's in the Netherlands would have to be upgraded. (see next subchapter).

Remediation

Technical remediation of vulnerabilities can be done in 2 ways. The first way is for the connected device, or software manufacturer issues a security patch which, when installed on the vulnerable device, eliminates the vulnerability.
The second way is to reconfigure the connected device, so the vulnerability is no longer active. An example is to disable a non-essential service, containing a vulnerability, in the configuration of the home-router.

As described in chapter 3.4.2, ISPs also protect devices in the in-home domain. Technically these measures do not fall under the definition of remediation because the vulnerabilities are not sanitised. Only the impact of the abused vulnerabilities is mitigated, or the vulnerabilities are "hidden" from the internet. Remediation has a preference because when the attacker gains access to the in-home domain or the device is connected to a non-secured connection (for instance: smartphone on the open network) then the ISP security measures are bypassed, and the vulnerabilities present in the connected device can still be abused.
With some alterations to the home-router, the current quarantine option to disable internet access for in-home domains with infected devices could be made more specific to disable network access for the infected device(s). This would reduce the adverse effects of the Quarantine option. This could be future research.

Future

The proposed VM solution is based on a situation where Ipv4 is used. IP version 6 (Ipv6) is the successor to ipv4 that is introduced sparsely. In the situation where ipv6 is deployed, other connection models might require a redesign of the scanning method. The sparse deployments, however, all us a connection models in which a home-router was used[286]. When this deployment is continued, this would suggest that the 2-phase approach could be used.
Security solutions like VM use signatures to track down vulnerabilities in software. Signature-based methods will in the near future become obsolete. Although vendors could not give a precise estimate, expectations[287] were that in a ten-year timeframe, artificial intelligence-based anomaly detection would take over from signature-based detection methods. This could be future research.

[285] Supp01, "Interview with a Security Products Chief Research Officer"; Supp02, "Telephone Interview with a Marketing Officer of a Security Products Vendor."
[286] KPN, "Meest Gestelde Vragen over IPv6"; VodafoneZiggo, "Vragen over IPv6 Beantwoord."
[287] Supp01, "Interview with a Security Products Chief Research Officer."

4.2.2 Governance solution overview

Roles

Key to a successful implementation of VM in the in-home is for all stakeholders do their part. At the moment the roles of stakeholders and what is expected from them, concerning vulnerabilities in the in-home domain, is insufficiently clear. Defining these roles and responsibilities for/together with the stakeholders is paramount. The European Commission has made a start by defining the RED directive as a vessel to carry the demands, but this does not cover all devices, and the mandatory demands have to be defined.

By appending the RED, the EU is aiming to make the connected device manufacturer responsible for solving vulnerabilities, which make the successful attack possible. The role of the consumer stays negligible because he can hardly be held accountable due to a lack of knowledge and expertise.

Classification

At the snapshot moment, most measures to secure the connected devices are defined by manufacturer or ISP.

For the ISP the cooperation through the abuse information exchange[288] helps determine which infection makes a device eligible to be placed in Quarantine. However, each ISP defines the requirements and process for placing someone in Quarantine. This “self-regulation” works because the ISP is obliged by the Tw to ensure the continuity of its network, and malware spreading through the ISP's network is terrible for the reputation.

Instead of manifested infection, which is abuse, VM focusses on lowering the risk of infection. Since lowering risks, in the end, costs money and 100% risk-free without losing functionality is impossible, a baseline of acceptable risk is needed. Standards are a way of setting this level of acceptable risk and enable cooperation between stakeholders.

The manufacturer can then determine in which vulnerabilities to invest resources; the consumer can determine which vulnerabilities are important based on easily understandable criteria.

Setting this base-line is finding an optimum for stakeholders. The Dutch government, responsible for safety, will want low risk. Manufacturers will want a higher risk baseline because solving vulnerabilities, with the current incentives model, cuts into their profits.

In an ideal situation, based on simple rational choice theory, the consumer would be able to determine the baseline on his own by changing his usage and buying behaviour based on his security level preference. However, due to a limited cognitive ability (most consumers do not have perfect information with regard to IT security to make a rational choice), the “choice under uncertainty” (There is only a risk of attack with negative results), and diffuse liability (why invest in security when one is unlikely to bear the adverse effects) the consumer is unable to determine the baseline. Therefore, an option is to have the baseline set by an organisation in which stakeholders have a vote. How to realise such an organisation could be future research.

Legal constraints

The previous chapter describes a role that would fit the ISP from a technical perspective. From a governance perspective, however, this brings up some challenges:

From a Tw privacy and computer criminality two perspectives (chapter 2.5), the ISP is not allowed to scan the connected devices without the explicit consent of the owner of those devices. Without incentives for the consumer to keep the in-home domain safe, he or she will probably not give consent let alone pay for the scans.

Market

As mentioned in “consent” the manufacturer must make costs to release updates which remove vulnerabilities. However, these are not the only costs. The government also makes costs to release and monitor law and regulate.

Implementing VM discovery also brings costs (chapter 2.6.3). Phase 1 could be established with current technological means and would require implementing and upkeep. Phase 2 however, will additionally need developing, implementing. However, also secondary expenditures like upgrading

[288] “Abuse Information Exchange.”

home-routers must be included. Without funds to compensate for these expenditures, ISP's are unlikely to cooperate.

An important notice is that only discovering without remediation would yield little benefits to security. One could deploy naming & shaming tactics with the found vulnerabilities. However, with the current incentives, the cost would probably stay the dominant factor for consumers compared to security, when buying connected devices.

4.2.3 Socio-technical solution overview

As can be read in the previous chapters, the view of consumers on security is fundamental. As long as consumers do not see the importance of safe devices, they will not sufficiently incorporate security in their purchase and usage behaviour. Apart from an incentive problem, a deficiency in knowledge of the dangers and how to prevent these is also a big factor in why consumers do not secure their connected devices. To solve this, private and public parties invest in awareness, educational, and empowerment campaigns to raise consumer awareness. Given the diversity of the consumer group, it might be prudent to assume that some will never reach the required technical level. These people can be helped by for instance a digital marketplace for helping out consumers with IT problems (like the Buuv initiative[289]).

Implementation strategy
A phased approach could be the most prudent way to implement VM in the in-home domain; Consumers get time to get used to the idea that they have vulnerabilities and that they have to do something to resolve their vulnerabilities. The stakeholders at the same time get time to perfect the VM governance, platform, and processes. This way strict liability can be avoided by utilising transparency. An example of an implementation strategy is:

1. Starting with nudging. By providing consumers with standardised reports on their high-risk vulnerabilities (on for instance the home-router) and information on what to do to mitigate these vulnerabilities. By not applying pressure, consumers can get to know the VM process, how to act on vulnerabilities, and getting used to the means at their disposal to rid their in-home domain from very high-risk vulnerabilities (Good Samaritan approach: no demands are set, only information and help is given).
2. Next phase is to extend the vulnerability reports by giving a comparison to the baseline. This step is based on the principle as articulated by Louis Brandeis *'sunlight is the best disinfectant'[290].*
3. The third step is demanding consumers to adhere to VM by for instance using the DMCA technique[291] by regulating that consumers must comply with 'notice-and-takedown' of vulnerabilities, for instance, accessible from the internet, within a prescribed time-frame.
4. The last step could be to quarantine devices with high-risk vulnerabilities, accessible from the internet, for some (baselined) time. At the same time, this consumer receives information on how to resolve the vulnerability (patches, focused help pages, consultancy).

The steps above are an example of an implementation strategy. Further research needs to be done to devise the most effective implementation strategy.

[289] "Buuv."
[290] Brandeis, *Other People's Money and How the Bankers Use It*.
[291] Stobbs, "The Digital Millennium Copyright Act."

4.3 The multi-stakeholder roadmap

In the roadmap, the phases of coming to VM are plotted using Product lifecycle management (PLM)[292]. PLM introduces many phases to come to a lifecycle of a product or service, which are also product dependent. For the roadmap in this thesis, the “design, build, run” approach is used as described by Dave Ingram[293]. Because Ingrams approach is focused on building and releasing a product, and the focus of VM is on running a process, an evaluation step is introduced at the cost of the design phase. This evaluation step stresses that the functioning of the VM process has to be monitored and adjusted if/when the circumstances require this. The reason to use only these three steps is that the abstraction level of the roadmap is too high and the estimates of the timelines too uncertain to build in more granularity by including design and build.

4.3.1 Dutch government roadmap

The Government shows the actions that the Dutch government needs to undertake to introduce VM in the in-home domain.

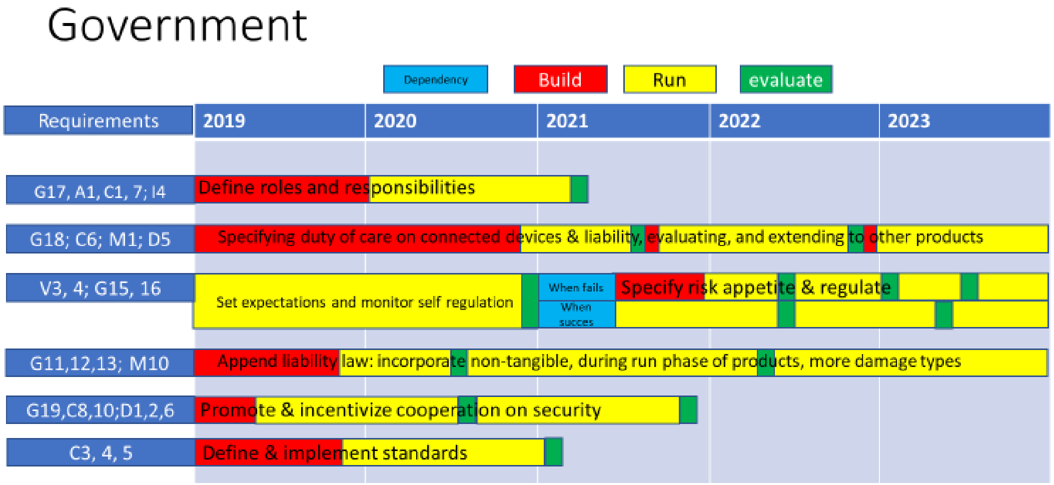

Government
Dependency
Build
Run
evaluate
Requirements
2019
2020
2021
2022
2023
G17, A1, C1, 7; I4
Define roles and responsibilities
G18; C6; M1; D5
Specifying duty of care on connected devices & liability, evaluating, and extending to other products
V3, 4; G15, 16
Set expectations and monitor self regulation
When fails
When succes
Specify risk appetite & regulate
G11,12,13; M10
Append liability law: incorporate non-tangible, during run phase of products, more damage types
G19,C8,10;D1,2,6
Promote & incentivize cooperation on security
C3, 4, 5
Define & implement standards

Figure 17 Roadmap Dutch government

The Dutch government is already active on taking steps to increase the security of consumer connected devices. Dutch government issued a roadmap on the safety of connected devices, awareness campaigns are given, and the Dutch government is in consultation with the European Commission to install and append laws to incorporate security. These actions form a sound basis for building VM.

Legislation like the RED is part of the European Union legal framework. Therefore changes in these laws have to be sanctioned by other E.U. members. This makes for a time-consuming process which, due to possibly conflicting incentives, might lead to endless debates and hollow laws. Appending these laws is however essential to break the current market-failure with regards to security. As a parallel step, the Dutch government can, together with industry, work on implementing self-regulation which, when proven successful, can be continued when the EU laws are ready. When proven unsuccessful, strict regulation can be installed backed by the new EU laws.

For VM to work, the legislation should also incorporate some form of risk appetite and incentives to adhere to the risk appetite. This might be positive incentives, for tech-savvy consumers assisting less IT knowledgeable consumer, or negative incentives for not resolving for vulnerabilities above the threshold.

Lastly, the Dutch government is tasked with balancing the costs of the stakeholders. Most notably are the costs for doing the vulnerability discovery in phase 2. The primary costs of building and running VM, but also the secondary costs of upgrading home-routers when applicable, have to be balanced over the responsible stakeholders.

[292] Stark, *Product Life Cycle Management*.

[293] Ingram, *Design – Build – Run: Applied Practices and Principles for Production-Ready Software Development*.

4.3.2 Connected device manufacturer roadmap

The roadmap for the connected device manufacturer describes the steps this stakeholder has to undertake to do his or her part in implementing VM in the in-home domain.

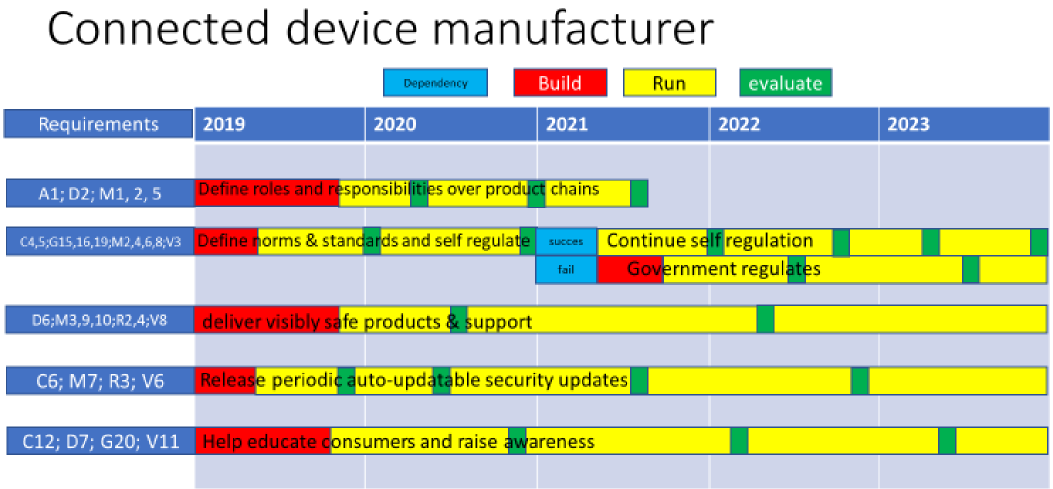

Connected device manufacturer
Dependency
Build
Run
evaluate
Requirements
2019
2020
2021
2022
2023
A1; D2; M1, 2, 5
Define roles and responsibilities over product chains
C4,5;G15,16,19;M2,4,6,8;V3
Define norms & standards and self regulate
succes
Continue self regulation
fail
Government regulates
D6;M3,9,10;R2,4;V8
deliver visibly safe products & support
C6; M7; R3; V6
Release periodic auto-updatable security updates
C12; D7; G20; V11
Help educate consumers and raise awareness

Figure 18 Roadmap Connected device manufacturer

The connected device manufacturer, with regard to VM, is tasked with supplying the solutions to vulnerabilities which exceed the risk-appetite. As described in the governance roadmap, a time-period exists in which the manufacturer can demonstrate that his industry can self-regulate the current security situation towards the set risk-appetite.

Another crucial task for the manufacturer is to contribute to standards which make it possible for consumers to comprehend the differences of security levels between different connected devices in order to incorporate this into his or her buying and run behaviour.

Special notion on the home-router manufacturer
As mentioned in the previous chapters, the home-router performs a critical function. As the gateway posing a high risk of being attacked, the home router could be a good choice for piloting new legislation with stricter security demands.
For enabling discovery phase 2, the home-router manufacturer has to cooperate with the VM solution provider in order to enable discovery scanning from the home-router.
The last quick-win is for the home-router manufacturer to adopt hardening best practices. Also, the development of methods to enable segmentation in the in-home domain could be worth exploring. Important to bear in mind when implementing security measures is that consumers with little IT knowledge and skill must be able to deploy and use them.

4.3.3 Consumer

The consumer cannot be addressed as one entity like the other stakeholders which makes the construction of a roadmap ineffective. This does not mean however that the consumer plays no role. The whole implementation of the solution design starts with the consumer. When the consumer does not give explicit consent, then VM detection cannot be done due to legal restrictions. For the consumer to be able to give consent, he or she must first understand what terms to agree to, and therefore some basic knowledge is required. When the consumer is more aware of the risks, he or she will more likely be inclined to give consent.

Especially when the consumer decides to use his or her home router, then VM the solution design phase 1 can only be performed. This means that the consumer then has to perform updates on the home router him-or herself as well as controlling the vulnerabilities in his or her in-home domain.

4.3.4 ISP roadmap

The roadmap for the ISP describes the steps this stakeholder has to undertake to do his or her part in implementing VM in the in-home domain.

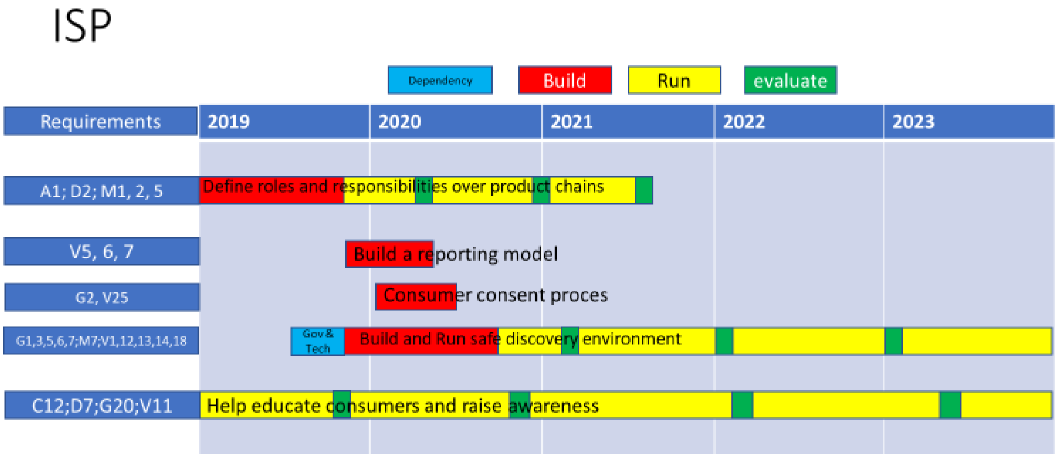

ISP
Dependency
Build
Run
evaluate
Requirements
2019
2020
2021
2022
2023
A1; D2; M1, 2, 5
Define roles and responsibilities over product chains
V5, 6, 7
Build a reporting model
G2, V25
Consumer consent proces
G1,3,5,6,7;M7;V1,12,13,14,18
Gov & Tech
Build and Run safe discovery environment
C12;D7;G20;V11
Help educate consumers and raise awareness

Figure 19 Roadmap ISP

Although the ISP does not have a responsibility in securing the consumers' in-home domain, the ISP can play a role in the VM process due to his or her role as communications provider with, at the snapshot moment, control over the home-router. The role for the ISP would be to perform vulnerability discovery for the in-home domain for both phases.

Before the ISP is allowed to do a discovery scan, consent by the consumer has to be given.

At the moment ISP’s check the home-router for vulnerabilities but with the instalment of the Net Neutrality freedom of choice for endpoints principle, consumers are allowed to choose their home-router. This would mean that:

- The home-router is not checked for vulnerabilities anymore. By doing a periodic scan from the ISP network or internet, vulnerabilities could still be detected on the consumers home-router. (phase 1 discovery). Resolving them would become a task of the consumer.
- Phase 2 discovery could not be executed by the ISP anymore. To enable phase 2 the consumer has to install and execute phase 2 him-or herself.
- The narrowed down Quarantine option as described in chapter 4.2.1 would not be possible anymore.

The ISP’s are already doing awareness campaigns, and this has to be continued to raise awareness of consumers on the security risks, what can be done to mitigate the risks and the role of the consumer in securing the connected devices in the in-home domain.

4.3.5 Vulnerability management solution provider roadmap

The roadmap for the vulnerability management solution provider describes the steps this stakeholder has to undertake to do his or her part in implementing VM in the in-home domain.

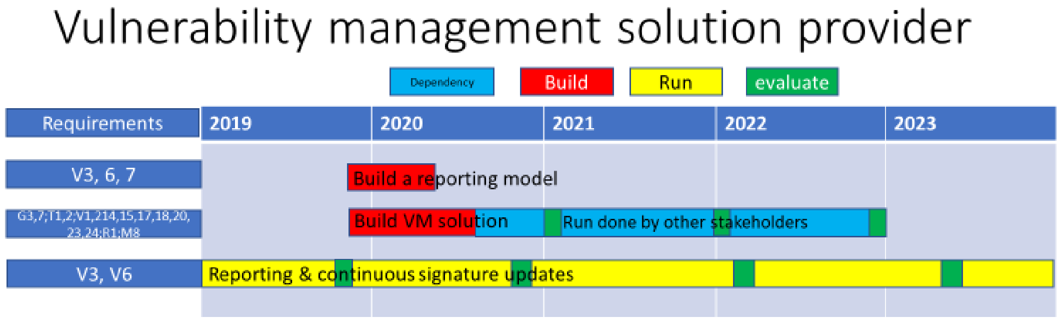


Figure 20 Vulnerability management solution provider

The vulnerability solution provider has the responsibility to design and build the solution needed to periodically run discovery scans from either the ISP network/internet for phase 1 and run scans from the home-router for phase 2. Also, the requirements regarding scaling, scan visibility and part of the requirements regarding the safekeeping of the vulnerability information fall within this scope. The reporting model incorporates what the consumer gets to see, but also incorporates the suggestions on how to mitigate the vulnerability when over the risk threshold.
During the run-time of the VM solution, the provider handles making signature updates on newly found vulnerabilities together with the connected device manufacturers.

4.3.6 Synchronisation of the roadmap

As stated in the requirement analysis (chapter 4.1), the roadmaps cover about half of the requirements. The rest of the requirements are either governance of the VM solution, or content based of the VM solution, and as such incorporated into the solution design. The roadmaps define the steps needed to realise and implement the solution design. Apart from some interdependencies mentioned below, stakeholder groups can develop the capabilities needed to implement their “VM step” autonomously. This is possible because each step in the VM model is assigned to only one stakeholder group, which limits the interdependencies. However, only by performing all the VM steps can an effective VM process be executed. The interdependencies that do exist are explained below:

Almost all roadmaps start with defining roles and responsibilities because every stakeholder has a role in the VM process. This means that when one stakeholder does not do his or her part, then the VM process will not work. Therefore stakeholders must come to a governance structure which can hold stakeholders responsible for doing their part, which can perform quality assurance, and which can balance the costs. When the roles from the solution design are used, and costs have to be beared by that specific stakeholdergroup, then the costs are disproportionately distributed.

At the moment the European Commission is working on appending the RED with security requirements. This would set patching requirements for the connected device manufacturers. The solution design is based on manufacturers wanting to cooperate with the VM implementations based on “self-regulation”. When self-regulation fails, risk appetite must be set by the government (local, but more likely E.U.)

The discovery in the solution design is performed by the ISP, creating, and maintaining the VM software, as well as the signatures is the responsibility of the VM solution provider.

The communication of the report and possible resolving methods must be a combined stakeholder effort, because multiple information streams need to be combined in the report.

5 Conclusions & further research

The conclusion chapter consists of three parts. The first part gives conclusions regarding the roadmap, the second part describes the methods used and how well they tailored to the building of the VM chapter, and this chapter concludes with making recommendations on future research.

5.1 Conclusions of the VM research

Connected devices are expected to increase significantly in numbers, as well as in impact on people's daily life's. This increase also introduces a risk. To improve the security of the in-home domain and the connected devices in it, this thesis proposes a multi-stakeholder roadmap to implement vulnerability management (VM) in the in-home domain of Dutch consumers.
Although VM in the in-home domain can theoretically be executed by the consumer, assisted by the manufacturer or software supplier, this research concludes that most Dutch consumers lack the technical skill and knowledge to do so. Therefore, this thesis proposes a solution in which the Dutch government, the connected device manufacturer, the ISP's, and the VM solution provider assist the consumer in doing VM in his or her in-home domain. The per stakeholder roadmaps define the steps needed to build and run this VM solution.

The discovery step in the solution design is based on a 2-phased approach. The first phase is based on discovering the vulnerabilities present in the home-router, because the home-router, as the gateway to the in-home domain, poses the biggest risk. The second phase also discovers vulnerabilities in the in-home domain behind the home-router. Phase 2, however, can only be developed when the ISP has control over the in-home router, since the home-router is the basis for the discovery scan. With the Net neutrality principle of freedom of endpoint device, ISP control over the home-router is no longer evident.

Resolving vulnerabilities is mainly the task of the connected device supplier or manufacturer because they are responsible for delivering well-secured devices. Resolving can either be done by delivering a security patch which eliminates the vulnerability, or by reconfiguring the device so the vulnerability can no longer be abused. Ideally resolving vulnerabilities is automated, so that consumer do not have to carry out any actions. In cases where automation is not possible, non-tech-savvy consumers need access to help with resolving. A last resort for resolving high risk vulnerabilities, which cannot be patched or reconfigured is to disable connectivity for those devices.

A centralised approach to doing VM also leads to centralised storage of per consumer VM information. This personal information is valuable to multiple (malicious) organisations and requires adequate protective measures. The usage of this information must be on a strictly need-to-know basis, and the consumer must be able to easily understand what the information is used for.

From a stakeholder perspective, Setting the roles, responsibilities, and the risk appetite for VM within a corporate environment is centralised. The size of the organisation also allows for acquiring people with vulnerability knowledge and IT skills, and for making a monetary or legal fist against connected device manufacturers and suppliers. In the in-home domain, the individual consumer cannot make this fist. Organisations such as the Consumentenbond already help the consumer, but regarding security, this is still in its infancy.
Dividing the roles and responsibilities of the VM steps introduces difficulties. The organisation possibly able to do discovery in the in-home domain for instance is the ISP. However, this would require the ISP to make large investments, while the ISP has no responsibility for the in-home domain and the devices residing in it, and therefore is not prepared to bear these costs. Therefore, a solution is required to transfer these costs to other stakeholders based on responsibility.

Looking towards the future, technologies like virtualisation, A.I. assisted anomaly detection, and forced security patching are expected to bring new possibilities on automatically remediating vulnerabilities without loss of service might render the VM process obsolete.
However, until these technologies have fully matured, VM can fill the gap and attribute to a more secure internet for all to enjoy.

5.2 Reflection on the method

5.2.1 The 3-layer model

The 3-layer model worked well to illustrate the in-home environment from different perspectives.
With only the technical lens, VM would have been an excellent process to secure the connected devices in the in-home environment. By including the Socio-technical and Governance perspectives, knowledge gaps of consumers, laws, and incentives are included in the analysis. This lead to a much more refined view of the difficulties that can be expected with the introduction of VM in the in-home domain and how these difficulties can best be solved.

The initial plan for the requirements gathering phase was to determine the requirements based on the three layers. This proved to be difficult because gathering requirements is typically done by asking stakeholders. The method used for this thesis was to interview people. This led to a diversity of requirements across the 3-layers. Therefore the stakeholders were selected using the environmental analysis and, in the interviews, the 3-layer model was used to structure the interview. Using the 3-layer model for the requirement gathering with stakeholders worked well in the sense that most interviewees indicated that the differentiation into three layers helped them to answer the questions more clearly and that the model helped to structure the conversation. An observation by the author was that interviewees usually had 1 or sometimes two layers as a preference and lacked in-depth knowledge in the other layers.
Using the 3-layer model for the analysis proved especially useful to determine which stakeholders must cooperate to solve specific issues. Many requirements, mentioned by the interviewees, clustered into the requirement “setting roles and responsibilities”. Although one requirement, this must be filled by several stakeholders working together which led to a divergence in the roadmap phase. Creating the roadmap in the three phases of the 3-layer model also did not work. A roadmap must be attributed to dedicated stakeholders.

5.2.2 The simplified model

The first two interviews were done using the full in-home model (Figure 4). The interviewees needed too much time to understand the model and the level of detail also raised questions that were not directly relevant to the research. Therefore the simplified model was created (Figure 5). The interviewees in the subsequent interviews validated that the model was correct and indicated that the abstraction level of the simplified model contributed to understanding the situation and answering the questions. The second supervisor mentioned that using the simplified model as a basis for explaining the different scan vectors improved her understanding of the vectors a lot.

5.2.3 Methods and the reasoning line

Starting with the first layer of the 3-layer model (the technical layer) made for a very rough transition coming from the introduction. Starting with the ICT-enabled activities and then using the OSI model to come to the underlying technical layer made for a more organic reasoning line where less technical readers can also understand the technical aspects underlying the ICT-enabled activities.
The OSI model proved successful in making the transition from socio-technical to technical layer and explaining the technical aspects of the in-home domain. The OSI model, however, lacked the abstraction to make the transition to governance layer. For the transition to the governance layer, the 4-layer model of Koppenjan & Groenewegen was used. Their 4-layer model allowed for the formal law to be split off from the incentives. The formal law was explained in the general governance lens chapter, where incentives are stakeholder specific and thus are handled in the stakeholder analysis.

The Roadmap was constructed using Ingram’s “design, build, run” model. This model was appended with an evaluation phase at the expense of the design phase. The design and build phase in the roadmap are combined. The additional evaluation phase increases the usage of Ingrams model on a continuing process like VM instead of Ingram’s product focus.

5.2.4 Design science

The primary goal of the research described in this thesis was to build a roadmap as mentioned before this makes this research design science. Hevner[294] described seven steps of creating an artefact. These seven steps are used to evaluate the overall process of coming to the roadmap for implementing VM in the in-home domain.

Hevner phase	proof
Design as an artefact	The simplified model was created to come to analysis and requirements. These requirements together with the analysis of chapter 2 lead to the creation of the roadmaps per stakeholder.
Problem relevance	As described in chapter 1.1, several Dutch governmental organisations, as well as the interviewed private parties, state that vulnerabilities in the in-home domain are becoming a big problem. As described in the conclusion, a mix of security solutions is needed to tackle this problem. This roadmap can help in solving this problem.
Design evaluation	Demonstration of the success of a roadmap is only possible when the steps are fulfilled, and the working is successfully demonstrated. The evaluation is done by validating the steps proposed in the interviews. Especially the governmental interviews were used to validate the models and findings
Research contribution	At the snapshot moment, no references could be found of research looking into doing vulnerability management in the in-home domain. This while the interviewees see the problem relevance and the established way of controlling vulnerabilities in organisations is implementing a vulnerability management process
Research rigour	Several well-established models and methods were used to come to the artefact. These models are described in this chapter. Also, the findings on the three-layer model were discussed with the owner of that model to help improve upon the 3-layer.
Design as a search process	This artefact was created by taking a well-defined and established solution (vulnerability management) which proofed its worth in the security of public and private organisations. This thesis describes the analysis and how to implement in a domain new to vulnerability management (consumer in-home domain).
Communication of research	This thesis will be openly available through the Cybersecurity Academy website and searchable through ResearchGate.

Table 6 The 7 steps of design science by Hevner mapped on the roadmap artefact

[294] Hevner et al., “Design Science in Information Systems Research.”

5.3 Recommendations on future research

During the research, several subjects were identified that seem open to further research:

Governance
This thesis is based on exploratory research, and therefore the roadmap uses generic steps. The in-depth description of how to implement measures or law and their exact configuration is not incorporated. The first step in further research is how stakeholders have to be organised in order to get the right balance between security and the costs needed to provide this security. This can be part of research into institutional design[295] of security regarding consumers.
Questions this organisation has to answer are: How will the risk baseline be established and evolved, who will bear which costs, What role can the consumer play now and in the future regarding the Vulnerabilities in his domain.

During the interviews, it was found that decisions about liability, responsibility, and control Versus freedom were still ongoing or even just starting. These were noted in this paper, and where applicable advice was given, but settling these discussions was not part of this thesis. Research is needed in order to find the right balance.

Socio-technical
At the moment consumers have difficulty with understanding the risks connected devices in their in-home domain pose, and what they can do about that. Consumers, however, need to have some notion of risk in order to want to invest in the security of their connected devices, and for instance, give explicit consent for stakeholders to start performing VM. Information targeted to specific consumer groups might be more efficient than performing mass awareness campaigns and might trigger a VM snowball effect.

Technical
This research is focused on the in-home domain; mobile broadband is not incorporated because the connectivity, which is an essential element in this research, is supplied through different technical means. A roadmap on how to implement VM in the mobile domain might improve the economy of scale of the VM platform, making VM more lucrative for stakeholders to implement. This could be further researched.

At the moment, ISPs deploy Quarantine measures on the consumer connection. For the consumer, this means that one infected device ensures that all devices in his in-home domain no longer have access to the internet. By deploying the Quarantine measure on the home-router, technically one could disable internet access to the infected device. Whether this is feasible, desired, and what steps are needed for implementation could be further researched.

The interviews revealed that signature-based detection methods like VM in the future would be replaced by network anomaly detection methods based on Artificial intelligence. Contrary to VM, network anomaly detection inspects traffic and destinations which at the moment goes against Net neutrality law. How to implement Network anomaly detection in the in-home domain can be further researched.
At the moment VM still offers advantages, but discussions about roles, responsibilities, and liability could take long to be resolved in the E.U. Research can be done on whether investing in VM or betting for Network anomaly detection is most efficient.

[295] Koppenjan and Groenewegen, “Institutional Design for Complex Technological Systems”; Regulationbodyofknowledge.org, “Institutional Design.”

6 Bibliography

AB01. "Interview with Abuse Specialist." *17-07-2018*, n.d.

AB02. "Interview with an Abuse Specialist." *02-11-2018*, n.d.

"Abuse Information Exchange." Accessed October 11, 2018. https://www.abuseinformationexchange.nl/english.

Abuse01. "Interview with Abuse Specialist." *17-07-2018*, n.d.

AD. "Telephone Hacked through Vulnerable Solar Panel." Accessed September 21, 2018. https://www.ad.nl/gouda/telefoon-gehackt-via-zonnepaneel-rekening-van-7000-euro~a76f8239/.

Ahmed, Mohiuddin, Abdun Naser Mahmood, and Jiankun Hu. "A Survey of Network Anomaly Detection Techniques." *Journal of Network and Computer Applications* 60 (2016): 19–31. https://doi.org/10.1016/j.jnca.2015.11.016.

Akerlof, Geaorge A. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *ScienceDirect*, n.d.

Alert online. "Nationaal Cybersecurity Bewustzijnsonderzoek," 2018.

Ali, Syed Taha, Patrick McCorry, Peter Hyun Jeen Lee, and Feng Hao. "ZombieCoin 2.0: Managing next-Generation Botnets Using Bitcoin." *International Journal of Information Security* 17, no. 4 (2018): 411–22. https://doi.org/10.1007/s10207-017-0379-8.

All, Haijun Gu et. "The Design of Smart Home Platform Based on Cloud Computing," 2011. https://www.researchgate.net/publication/221333091_The_design_of_smart_home_platform_based_on_Cloud_Computing.

Altena, E M. "Exploring Effective Notification Mechanisms for Infected Iot Devices," n.d.

Amazon. "Amazon Fresh." Accessed October 22, 2018. https://www.amazon.com/AmazonFresh/b?ie=UTF8&node=10329849011.

Asus. "AiProtection." Accessed October 11, 2018. https://www.asus.com/Aiprotection.

autoriteit persoonsgegevens. "Verantwoordingsplicht." Accessed October 31, 2018. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht.

Azmoodeh, Amin. "Detecting Crypto‑ransomware in IoT Networks Based on Energy Consumption Footprint." Accessed October 18, 2018. https://link.springer.com/content/pdf/10.1007/s12652-017-0558-5.pdf.

Bauer, Johannes M, and Michel J G Van Eeten. "Cybersecurity : Stakeholder Incentives , Externalities , and Policy Options." *Telecommunications Policy* 33, no. 10–11 (2009): 706–19. https://doi.org/10.1016/j.telpol.2009.09.001.

Berg, Jan van den. "Cybersecurity for Everyone." In *Cybersecurity for Everyone*. Springer LTD, 2018. https://link.springer.com/book/10.1007/978-3-658-21655-9.

Berg, Jan Van Den, Jacqueline Van Zoggel, Mireille Snels, Mark Van Leeuwen, Sergei Boeke, Leo Van De Koppen, Jan Van Der Lubbe, Bibi Van Den Berg, and Tony De Bos. "On (the Emergence of) Cyber Security Science and Its Challenges for Cyber Security Education." *NATO STO/IST-122 Symposium in Tallin*, no. c (2014): 1–10.

Berkeley. "Continuous Vulnerability Assessment Authentication." Accessed November 24, 2018. https://security.berkeley.edu/continuous-vulnerability-assessment-remediation-guideline.

Berry, Leonard L. *Discovering the Soul of Service: The Nine Drivers of Sustainable Business*, 1999.

BEUC. "Cybersecurity for Connected Products." Accessed November 1, 2018. https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf.

Bits of Freedom. "Mail Thread." august 2018, n.d.

Brandeis, Louis. *Other People's Money and How the Bankers Use It*, 1914.

Brightsight. "Assessing the Security of ' Simple ' IoT Devices," n.d.

Bruijne, Mark De, Michel van Eeten, and Wolter Pieters. "Towards a New Cyber Threat Actor Typology A Hybrid Method for the NCSC Cyber," 2017, 71.

"Buuv." Accessed November 24, 2018. https://buuv.nu/.

cablek. "Network Cabling." Accessed September 5, 2018. http://www.cablek.com/technical-reference/cat-5---5e--6--6a---7--standards.

Caulkins, Jonathan P. "Sell First , Fix Later : Impact of Patching on Software H . John Heinz III School of Public Policy and Management Sell First , Fix Later : Impact of Patching on Software Quality," no. August 2003 (2004).

CBS. "Nederland Koploper in Gebruik van Veiligheidssoftware." Accessed September 21, 2018. https://www.cbs.nl/nl-nl/nieuws/2011/42/nederland-eu-koploper-in-gebruik-veiligheidssoftware.

Centraal bureau voor de Statistiek. "Mobiele Telefoon Minder Vaak Beveiligd Dan Computer." 21-09-2018. Accessed October 1, 2018. https://www.cbs.nl/nl-nl/nieuws/2018/38/mobiele-telefoon-minder-vaak-beveiligd-dan-computer.

Chirgwin, Richard. “Finns Chilling as DDoS Knocks out Building Control System.” Accessed June 10, 2018. https://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/.

College bescherming persoonsgegevens. “Analyse Gegevens Mobiel Dataverkeer Kpn,” no. November (2013).

Commision, European. “Radio Equipment Directive.” Accessed November 7, 2018. https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en.

consumentenbond. “Phone and Mail Conversation Met Consumentenbond Augu.” st & october 2018, n.d.

———. “The 9 Demands Regarding Security Updates.” Accessed November 1, 2018. https://www.consumentenbond.nl/acties/updaten/eisen-veiligheidsupdates.

Consumentenbond. “Windows Defender Worst Virusscanner of the Test.” Accessed September 21, 2018. https://www.security.nl/posting/412610/Consumentenbond%3A+virusscanner+is+zijn+geld+waard.

consumentenbond forum. “Schandalig Privacy Beleid van Polar.” Accessed November 1, 2018. https://community.consumentenbond.nl/consument-recht-28/schandalig-privacybeleid-van-polar-17021/index1.html#post74760.

contact the author personally. “Information Gathered through Anonymous Interview.” n.d.

council of the european communities. “Directive on Unfair Terms in Consumer Contracts.” Accessed October 31, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31993L0013&from=NL.

coursera. “Network Hardening Principles.” Accessed August 30, 2018. https://www.coursera.org/lecture/it-security/network-hardening-best-practices-T3lID.

CSO. “Is Critical Infrastructure the next Ddos Target.” Accessed August 30, 2018. https://www.csoonline.com/article/3141601/critical-infrastructure/is-critical-infrastructure-the-next-ddos-target.html?page=2.

cyber security raad. “‘ Naar Een Veilig Verbonden Digitale Samenleving ’ Advies Inzake de Cybersecurity van Het Internet of Things (IoT),” n.d.

Cyber Security Raad, P. Wolters, and C. Jansen. “Ieder Bedrijf Heeft Digitale Zorgplichten,” 2017, 30. https://www.cybersecurityraad.nl/binaries/20170405_CSR_Handreiking2017_CompleetDEFweb_tcm56-253718.pdf.

Darktrace. “The Enterprise Immune System.” Accessed November 1, 2018. https://www.darktrace.com/en/technology/.

Darpa internet program. “RFC: 791 Internet Protocol Specification,” 1981. http://www.ietf.org/rfc/rfc0791.txt.

Diana Farrell, Fiona Greig. “The Online Platform Economy: Has Growth Peaked?” *SSRN Electronic Journal*, 2017.

digicert. “Wi-Fi Is Hacked and so Are Your IoT Devices?” Accessed September 27, 2018. https://www.digicert.com/blog/wi-fi-hacked-iot-devices/.

DOD. “Https://Www.Spi.Dod.Mil/Tenets.Htm,” n.d.

DP01. “Interview with Policy Officer Dutch Parliament.” *19-10-2018*, n.d.

Economische, Ministerie Van. “Beleidsregel Netwerkaansluitpunt,” no. december (2017): 1–2.

Ejure. “Product Aansprakelijkheid En Software,” 2016. http://www.ejure.nl/2016/09/productaansprakelijkheid-en-software/.

Elmrabit, Nebrase, Shuang Hua Yang, and Lili Yang. “Insider Threats in Information Security Categories and Approaches.” *2015 21st International Conference on Automation and Computing: Automation, Computing and Manufacturing for New Economic Growth, ICAC 2015*, no. September (2015). https://doi.org/10.1109/IConAC.2015.7313979.

EMVCO. “EMV Technologies.” Accessed November 7, 2018. https://www.emvco.com/.

ENISA. *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures*. *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures*, 2017. https://doi.org/10.2824/03228.

Esbin, Barbara. “Internet over Cable: Defining the Future in Terms of the Past.” *7 CommLaw Conspectus 37*, 1999.

European commision. “Open Internet Policy.” Accessed October 18, 2018. https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality.

———. “SPAM: European Commission Goes on the Offensive.” Accessed October 18, 2018. http://europa.eu/rapid/press-release_IP-03-1015_en.htm?locale=en.

———. “The EU Internet Handbook: Cookies.” Accessed October 18, 2018. http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm.

“European Cyber Security Perspective 2018,” 2018.

European Parliament. “Directive 2000/31/EC,” 2000. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=NL.

European Parliament and Council. "Regulation 2015/2120." *Official Journal of the European Union* 2014, no. November 26th (2015): 1–18.

European Union. "Broadband Strategy & Policy." Accessed August 24, 2018. https://ec.europa.eu/digital-single-market/broadband-strategy-policy.

F-secure. "Sense SDK." Accessed November 9, 2018. https://www.f-secure.com/nl_NL/web/home_nl/sense.

Farooq, M., Muhammad Waseem, Anjum Khairi, and Sadia Mazhar. "A Critical Analysis on the Security Concerns of Internet of Things (IoT)." *International Journal of Computer Applications* 111, no. 7 (2015): 1–6. https://doi.org/10.5120/19547-1280.

Federal communications commission. "Broadband Progress Report and Notice of Inquiry of Immediate Action to Accelerate Deployment," 2015.

———. "National Broadband Plan." Accessed August 24, 2018. https://www.fcc.gov/general/national-broadband-plan.

Foreman, Park. *Vulnerability Management*. Auerbach Publications, 2009.

———. *Vulnerability Management*, 2010.

Friess, Ovidiu Vermesan; peter. *Internet of Things - from Research and Innovation to Market Deployement*, 2014.

Gangan, Subodh. "A Review of Man-in-the-Middle Attacks." *ArXiv Preprint ArXiv:1504.02115*, no. Mim (2015): 1–12.

Ganguli, Sanjit, and Ted Friedman. "IoT Technology Disruptions : A Gartner Trend Insight Report What You Need to Know." *Garter*, no. June (2017): 1–12.

Gartner. "IT Security Spenditure." Accessed June 17, 2018. https://www.gartner.com/newsroom/id/3836563.

Gentzoglanis, Anastassios. *Regulation and the Evolution of the Global Telecommunications Industry*, n.d.

Gershenfeld, Neil, Raffi Krikorian, and Danny Cohen. *The Internet of Things*. *Scientific American*. Vol. 291, 2004. https://doi.org/10.1038/scientificamerican1004-76.

Geschillencommisie. "Telephone Conversation." july 2018, n.d.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." *Future Generation Computer Systems* 29, no. 7 (2013): 1645–60. https://doi.org/10.1016/j.future.2013.01.010.

Hansman, S. "A Taxonomy of Network and Computer Attacks." Accessed September 22, 2018. https://www.sciencedirect.com/science/article/pii/S0167404804001804.

Harald Bauer, Ondrej Burkacky, and Christian Knochenhauer. "McKinsey: Security in the Internet of Things." Accessed October 21, 2018. https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things.

Hayek, Friedrich. "The Use of Knowledge in Society." *The Economic Nature of the Firm* 35, no. 4 (2018): 63–68. https://doi.org/10.1017/CBO9780511817410.007.

Heart, Tsipi, and Efrat Kalderon. "Older Adults: Are They Ready to Adopt Health-Related ICT?" *International Journal of Medical Informatics* 82, no. 11 (2013): e209–31. https://doi.org/10.1016/j.ijmedinf.2011.03.002.

Herley, Cormac. "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users." *Security*, 2009, 133–144. https://doi.org/10.1145/1719030.1719050.

Hevner, Alan R, Salvatore T March, Jinsoo Park, and Sudha Ram. "Design Science in Information Systems Research." *MIS Quarterly* 28, no. 1 (2004): 75–105. https://doi.org/10.2307/25148625.

"Https://Cve.Mitre.Org," n.d.

Huurdeman, Anton A. *The Worldwide History of Telecommunications*, n.d.

ICT recht. "Nederlandse Netneutraliteit Voorbeeld Voor Europa, Handhaving Aangescherpt Met Boetes." Accessed October 18, 2018. https://ictrecht.nl/2015/02/05/5/.

IEEE. "802.11 Wifi Standard." Accessed September 5, 2018. http://www.ieee802.org/11/.

———. "802.3 Standard." Accessed September 5, 2018. http://www.ieee802.org/3/.

IHS. "Cable Penetration," 2016. http://www.cable-europe.eu/wp-content/uploads/2015/12/graph-1.png.

Ingram, Dave. *Design – Build – Run: Applied Practices and Principles for Production-Ready Software Development*, n.d.

International Telecommunication Union. "X.200: Data Networks and Open System Communications" 4 (1994): 59. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items.

ISACA. "Security Risk." Accessed August 29, 2018. https://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/Security Risk Management.pdf.

ISF. “Standard of Good Practise: IR2.7 Vulnerability Assessment,” 2016.

ISO/IEC. “ISO 27002 Control 12.6 Technical Vulnerability Management,” 2013.

ISO. “ISO/IEC 27000 Information Security.” Accessed September 23, 2018. https://www.iso.org/isoiec-27001-information-security.html.

ISP01. “Interview with Dutch ISP Security Senior.” *15-08-2018*, n.d.

ISP02. “Interview with Dutch ISP Security Senior.” *19-09-2018*, n.d.

Kent, N, and K Facerw. “Different Worlds ? A Comparison of Young People ’ s Home and School ICT Use.” *Journal of Computer Assisted Learning* 20, no. SPECIAL SECTION (2004): 440–55. https://doi.org/10.1111/j.1365-2729.2004.00102.x.

Khrais, Laith T. “Highlighting the Vulnerabilities of Online Banking System.” *Journal of Internet Banking and Commerce*, 2015. https://doi.org/10.4172/2165-7866.1000120.

Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. “DDoS in the IoT: Mirai and Other Botnets.” *Computer* 50, no. 7 (2017): 80–84. https://doi.org/10.1109/MC.2017.201.

Koppenjan, Joop, and John Groenewegen. “Institutional Design for Complex Technological Systems.” *International Journal of Technology, Policy and Management* 5, no. 3 (2005): 240. https://doi.org/10.1504/IJTPM.2005.008406.

KPN. “Meest Gestelde Vragen over IPv6.” Accessed November 27, 2018. https://www.kpn.com/faq/17208.

KPN BV. “Algemene Voorwaarden Voor Vaste En Mobiele Telecommunicatiediensten D,” 2018.

———. “KPN Veilig.” Accessed November 1, 2018. https://www.kpn.com/service/internet/veilig-internetten/kpn-veilig.htm.

KPN ventures. “KPN Ventures Provides Growth Capital to CUJO AI for International Expansion.” Accessed November 1, 2018. http://www.kpnventures.com/2018/10/18/kpn-ventures-provides-growth-capital-to-cujo-ai-for-international-expansion/.

Krejčířová, Lívia, and Jiří Dvořák. “Phishing – the Threat of Internet Banking,” n.d., 51–66.

Kritzinger, E., and S. H. Von Solms. “Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement.” *Computers and Security* 29, no. 8 (2010): 840–47. https://doi.org/10.1016/j.cose.2010.08.001.

Lee, In, and Kyoochun Lee. “The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises.” *Business Horizons* 58, no. 4 (2015): 431–40. https://doi.org/10.1016/j.bushor.2015.03.008.

Leg01. “Interview with a Telecom Legal Specialist.” *22-08-2018*, n.d.

Lysecky, Roman, and Peter Ott. “Security Challenges for Medical Devices,” n.d.

Man01. “Interview with Manufacterer of Security Measures.” *10-10-2018*, n.d.

Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. “The Internet of Things: Mapping the Value beyond the Hype.” *McKinsey Global Institute*, no. June (2015): 144. https://doi.org/10.1007/978-3-319-05029-4_7.

Martin, Lockheed. “Http://Www.Lockheedmartin.Com/Us/What-We-Do/Aerospace-Defense/Cyber/Cyber-Kill-Chain.HtmlNo Title,” n.d.

McAfee. “7 Types of Hacker Motivations.” Accessed September 27, 2018. https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/.

Min01. “Interview with 2 Ministerial Cybersecurity Policy Officers.” *11-10-2018*, n.d.

Ministerie van economische zaken en klimaat. “Consumentenagenda: Houvast Bij Voortdurende Verandering.” *Ons Kenmerk DGETM / 18247539*, no. 41 (2013): 1–9.

Ministry of justive and safety. “Telecomgegevens Voor Opsporing.” Accessed October 4, 2018. https://www.justid.nl/dienstverlening/telecomgegevensenopsporing/index.aspx.

Ministry of safety and justice. “Onderzoek Naar de Stroomstoring Amsterdam En Omstreken van 17 Januari 2017.” Accessed September 21, 2018. https://www.rijksoverheid.nl/documenten/rapporten/2017/07/27/tk-bijlage-onderzoek-naar-de-stroomstoring-amsterdam-en-omstreken-van-17-januari-2017.

Minsterie van economische zaken en klimaat. “Roadmap Digitaal Veilige Hard- En Software (Bijlage Bij 26643,Nr.535) - Parlementaire Monitor,” 2018. https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vknsg3qvz5tb.

Mirkovic, Jelena, and Peter Reiher. “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms.” *ACM SIGCOMM Computer Communication Review* 34, no. 2 (2004): 39. https://doi.org/10.1145/997150.997156.

Näsi, Mati. “ICT Activity in Later Life,” 2012. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5547400/.

Nationaal Cyber Security Centrum (NCSC). “Cyber Security Assessment Netherlands 2017,” 2017. https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2016/1/CSBN2016.pdf.

nationale ombudsman, De. “Telephone Conversation.” *July 2018*, n.d.

NCSC-NL. “Cybersecuritybeeld Nederland 2018,” 2018, 1–88. https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html.

NCTV. “Cybersecurity Bewustzijnsonderzoek 2018: Driekwart Getroffen, Helft Komt Niet in Actie Na Cybercrime.” Accessed October 1, 2018. https://www.alertonline.nl/nieuws/2018/nederlanders-zetten-eigen-digitale-veiligheid-op-een-laag-pitje.

Nielsen Norman group. “Nielsen’s Law of Internet Bandwidth.” Accessed October 18, 2018. https://www.nngroup.com/articles/law-of-bandwidth/.

NIST. “Security and Privacy Controls for Federal Information Systems and Organizations,” n.d.

Nyanchama, Matunda. “Enterprise Vulnerability Management and Its Role in Information Security Management.” *Information Systems Security* 14, no. 3 (2005): 29–56. https://doi.org/10.1201/1086.1065898X/45390.14.3.20050701/89149.6.

Online, Alert. “Alert Online.” Accessed October 21, 2018. https://www.alertonline.nl/.

Open Secrets. “Net Neutrality,” 2017. https://www.opensecrets.org/news/issues/net_neutrality/.

overheid.nl. “Aanwijzing van Aanbieders, Producten En Diensten Vitale Diensten,” 2018. https://zoek.officielebekendmakingen.nl/stb-2017-476.html.

———. telecommunicatiewet (2018). http://wetten.overheid.nl/BWBR0009950/2018-05-01.

Overheid.nl. “Computer Criminaliteit II.” Accessed September 30, 2018. http://wetten.overheid.nl/BWBR0019934/2007-09-01.

———. “Telecommunicatie Wet.” 28-07-2018, 2018. http://wetten.overheid.nl/BWBR0009950/2018-07-28.

Oxera Economics Council. “Benefits of Online Platforms: Technical Appendix,” no. October (2015). http://www.oxera.com/getmedia/89afcf75-95f0-4b8f-ab3e-d463e81e5f46/The-benefits-of-online-platforms-technical-appendix-(October-2015).pdf.aspx.

Perera, A. Zaslavsky, Christen, P. and Georgakopoulos. “Context Aware Computing for the Internet of Things: A Survey.” *Arxiv*, 2013. https://arxiv.org/pdf/1305.0982.

Pradeep, S, T Kousalya, K M Aarsha Suresh, and Jebin Edwin. “IoT and Its Connectivity Challenges in Smart Home.” *International Research Journal of Engineering and Technology (IRJET)* 3, no. 12 (2016): 1040–43.

Priv01. “Interview with an ISP Privacy Officer.” *24-09-2018*, n.d.

“Privacy-Friendly Threat Detection Using DNS,” no. August (2018).

Qualys. “Qualys Freescan.” Accessed November 9, 2018. https://www.qualys.com/forms/freescan/.

Rechtbank Den Haag. “Consumentenbond Tegen Samsung.” *Ecli:Nl:Rbdha:2015:7145*, 2016, 1–16. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2016:1175&showbutton=true&keyword=consumentenbond+samsung.

Reg01. “Interview with a Dutch Regulatory Policy Specialist.” *4-10-2018*, n.d.

Reg02. “Interview with a Regulatory Policy Specialist.” *08-10-2018*, n.d.

reg03. “Q&A Session with Regulatory Advisor on ‘Dag van de Apparatuur.’” *13-11-2018*, n.d.

Regulationbodyofknowledge.org. “Institutional Design.” Accessed December 15, 2018. http://regulationbodyofknowledge.org/regulatory-process/institutional-design/.

Release, Unlimited, Marie L Garcia, Olin H Bray, and Sandia National Laboratories. “Fundamentals of Technology Roadmapping,” n.d.

Richard A. Paulson; James a webber. “CYBEREXTORTION.” Accessed October 18, 2018. http://iacis.org/iis/2006/Paulson_Weber.pdf.

Rijksoverheid. “Bir 2017,” 2017. https://www.earonline.nl/images/earpub/d/d3/BIR2017_definitief_20171130.pdf.

Romanosky, Sasha. “Examining the Costs and Causes of Cyber Incidents.” *Journal of Cybersecurity*, 2016, tyw001. https://doi.org/10.1093/cybsec/tyw001.

Ronen, Eyal, Adi Shamir, Achi Or Weingarten, and Colin Oflynn. “IoT Goes Nuclear: Creating a Zigbee Chain Reaction.” *IEEE Security and Privacy* 16, no. 1 (2018): 54–62. https://doi.org/10.1109/MSP.2018.1331033.

Rossi, Ben. “The Internet of Old Things: Protecting the Future of IoT Devices.” Accessed August 29, 2018. https://www.information-age.com/internet-old-things-protecting-future-iot-123463549/.

Rowe, Brent, Dallas Wood, Douglas Reeves, and Fern Braun. “The Role of Internet Service Providers in Cyber Security Project Leads,” no. June (2011): 1–12. http://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf.

SandersTamer, Mohammad A. Noureddine, Ahmed Fawaz, William H. “A Game-Theoretic Approach to Respond to Attacker Lateral Movement,” n.d. https://link.springer.com/chapter/10.1007/978-3-319-47413-7_17.

Sangiovanni-Vincentelli, a., L. Carloni, F. De Bernardinis, and M. Sgroi. “Benefits and Challenges for Platform-Based Design.” *Proceedings. 41st Design Automation Conference, 2004.*, 2004, 409–14.

https://doi.org/10.1109/DAC.2004.240381.

SANS Institute. “Understanding Security Using the OSI Model,” 2002.

Sapakal, Reshma S, and Sonali S Kadam. “5G Mobile Technology.” *International Journal of Advanced Research in Computer Engineering & Technology* 2, no. 2 (2013): 2278–1323.

Schneier, Bruce. “Schneier on Security.” *Wwwschneiercom*, 2008, 336. http://www.amazon.com/Schneier-Security-Bruce/dp/0470395354.

———. “The Psychology of Security.” *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 5023 LNCS, no. 4 (2008): 50–79. https://doi.org/10.1007/978-3-540-68164-9_5.

Schoon, Ben. “Google Requires OEMs to Roll-out Regular Android Security Patches,” 2018. https://9to5google.com/2018/05/11/google-android-security-patch-requirement/.

Seacord, Robert C., and Allen D. Householder. “A Structured Approach to Classifying Security Vulnerabilities.” *Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst*, no. January (2005): 1–39. https://doi.org/CMU/SEI-2005-TN-003.

shodan. “Https://Www.Shodan.Io/,” n.d.

Sisco, Mike. “IT Asset Management” 1, no. C (2002): 0–1. https://doi.org/S0740-0020(10)00038-9 [pii]\r10.1016/j.fm.2010.02.008.

Skoudis, Ed, and Tom Liston. *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, 2005.

SOC01. “Interview with SOC Manager.” *17-07-2018*, n.d.

Spriggs, Benjamin, and Benjamin Spriggs. “PDXScholar Survey of Security in Home Connected Internet of Things By,” 2018.

Stark, John. *Product Life Cycle Management*, 2015.

Staten-generaal, Tweede Kamer Der. “Antwoord Op Vragen van de Leden Van Toorenburg En Verhoeven over Het Bericht ‘Experts: Overheid Moet Ingrijpen Bij Internetapparaten,’” no. 530 (2018): 2017–19.

statista. “House Hold Distribution the Netherlands.” Accessed September 28, 2018. https://www.statista.com/statistics/519863/total-number-of-households-in-the-netherlands/.

Statista. “Global Operating Systems Market Share for Desktop PCs, from January 2013 to July 2018.” Accessed October 21, 2018. https://www.statista.com/statistics/218089/global-market-share-of-windows-7/.

Statistiek, Centraal bureau voor de. “Huishoudens in EU Met Internet Thuis,” 2018. https://www.cbs.nl/nl-nl/nieuws/2018/05/nederland-koploper-in-europa-met-internettoegang.

Stephen, Christine, Joanna McPake, Lydia Plowman, and Sarah Berch-Heyman. “Learning from the Children: Exploring Preschool Children’s Encounters with ICT at Home.” *Journal of Early Childhood Research* 6, no. 2 (2008): 99–117. https://doi.org/10.1177/1476718X08088673.

Stobbs, Gregory. “The Digital Millennium Copyright Act.” *Multimedia Security Technologies for Digital Rights Management* 2860, no. 105 (2006): 457–82. https://doi.org/10.1016/B978-012369476-8/50020-8.

Supp01. “Interview with a Security Products Chief Research Officer,” n.d.

Supp02. “Telephone Interview with a Marketing Officer of a Security Products Vendor,” n.d.

Suresh, P., J. Vijay Daniel, V. Parthasarathy, and R. H. Aswathy. “A State of the Art Review on the Internet of Things (IoT) History, Technology and Fields of Deployment.” *2014 International Conference on Science Engineering and Management Research, ICSEMR 2014*, 2014. https://doi.org/10.1109/ICSEMR.2014.7043637.

Symantec. “W32.Stuxnet,” 2010. https://www.symantec.com/security-center/writeup/2010-071400-3123-99.

Ször, Péter, and Peter Ferrie. “Hunting for Metamorphic.” *In Proceedings of the 2001 Virus Bulletin Conference (VB2001)*, no. September (2001): 123–44. https://doi.org/10.1007/s11416-006-0028-7.

Taivalsaari, Antero, Nokia Technologies, and Tommi Mikkonen. “Software Engineering for the Internet of Things: A Roadmap to the Programmable World Software Challenges.” *IEEE Software*, 2017.

techopedia. “Definition: Internet Service Provider.” Accessed October 17, 2018. https://www.techopedia.com/definition/2510/internet-service-provider-isp.

Telecom, Agentschap. “Staat van de Ether 2017: Onveilige IoT-Apparatuur Risico Voor Samenleving.” Accessed June 6, 2018. https://www.agentschaptelecom.nl/actueel/nieuws/2018/juni/04/onveilige-iot-apparatuur-risico-voor-samenleving.

telecompaper. “Marktaandeel Analyse,” 2018. https://www.telecompaper.com/nieuws/breedbandmarkt-groeit-in-q1-met-03-kpn-verliest-licht-marktaandeel--1247259.

Tenable. “Nessus Licenses.” Accessed November 9, 2018.

https://www.tenable.com/products/nessus/activation-code.

The network encyclopedia. “Local Loop.” Accessed August 26, 2018. http://www.thenetworkencyclopedia.com/entry/local-loop/.

Tittel, Ed. “Http://Searchsecurity.Techtarget.Com/Feature/Comparing-the-Top-Vulnerability-Management-Tools,” n.d.

TNO. “Tno: Dealing Securely With the Internet of Things,” no. December (2016).

TNO ICT, and Dialogic. “Vraag En Aanbod Next-Generation Infrastructures 2010-2020,” 2010, 167. http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2010/03/16/next-gen-infrastructures/next-gen-infrastructures-v1-0-3-final.pdf.

Trend micro. “Protecting Home Networks: Start by Securing the Router.” Accessed August 30, 2018. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/protect-home-network-securing-router.

United States: US Army. “Cyberspace Operations Concept Capability Plan 2016-2028.” *TRADOC Pamphlet 525-7-8*, no. February 2010 (2010): 1–77. http://www.fas.org/irp/doddir/army/pam525-7-8.pdf.

vereniging eigen huis. “Mail Conversation.” july 2018, n.d.

———. “Slimme Meter.” Accessed October 18, 2018. https://www.eigenhuis.nl/besparen/energie-besparen/slimme-meter.

Verhoef, Katherine N. Lemon & Peter C. “Understanding Customer Experience Throughout the Customer Journey.” Accessed November 3, 2018. https://doi.org/10.1509/jm.15.0420.

VodafoneZiggo. “Algemene Voorwaarden Ziggo,” 2018, 1–18.

———. “Internet Beveiliging.” Accessed November 1, 2018. https://www.ziggo.nl/internet/internetbeveiliging/.

———. “Vragen over IPv6 Beantwoord.” Accessed November 27, 2018. https://community.ziggo.nl/over-de-community-210/vragen-over-ipv6-beantwoord-20327.

“VVD, CDA, D66 En ChristenUnie: Vertrouwen in de Toekomst,” 2017. https://www.tweedekamer.nl/sites/default/files/atoms/files/regeerakkoord20172021.pdf.

Waluszewski, A. “Hoping for Network Effects or Fearing Network Effects.” *The IMP Journal*, 2006.

wetten.overheid.nl. “Product Aansprakelijkheid.” Accessed November 7, 2018. http://wetten.overheid.nl/jci1.3:c:BWBR0005289&boek=6&titeldeel=3&afdeling=3&z=2018-09-19&g=2018-09-19.

Wolters, Mr. dr. P.W.J. Verbruggen* en mr. dr. P.T.J. “Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten,” 2017.

ZDNET. “Russian Hackers Are Attacking Home Routers, ISPs and Business Firewalls to Spy and Steal Data, Warns US, UK.” Accessed September 27, 2018. Korreweg 230, 9715AN Groningen.

Zhang, Z K. “IoT Security: Ongoing Challenges and Research Opportunities,” n.d.

Appendices

6.1 Appendix A the OSI model

The OSI model is based on the notion that network communication functions are divided into layers. Within these layers, actions take place needed to fulfil the communication function of that layer. Each layer only communicates with the adjacent layer. Because the interface between the layers is fixed, different protocols can communicate using this fixed interface. The OSI model uses 7 layers:

7.	Application	This layer communicates with the end-user
6.	Presentation	This layer transforms the data from the session layer into information that the application can process
5.	Session	This layer controls the connections between computers. It for instance handles the graceful closure of sessions
4.	Transport	Makes sure data is delivered error-free as to relieve the higher layers. This layer is also used often for encryption of the data path when higher layers are unable to encrypt.
3.	Network	Controls the operation of the subnet (logical network). Determination of the routed path data should take is determined here.
2.	Data link	Provides error free transfer of data frames between nodes (physical network) on the physical medium including addressing of local nodes
1.	Physical	manages the raw unstructured bit stream on the physical medium like fiber and copper wire

Table 7 OSI model

For the 2way transport of packets between the home domain and the internet, ISP's only the first 3 layers are used.

Many models are deducted from the 7-layer OSI model[296]. The TCP/IP model being the most used. However, for the abstraction level of this thesis, the OSI model is used, because most derivates have simplified or skipped the physical layer. This is logical from a technical networking perspective, but for the governance perspective, the physical NT hand-over point is important.

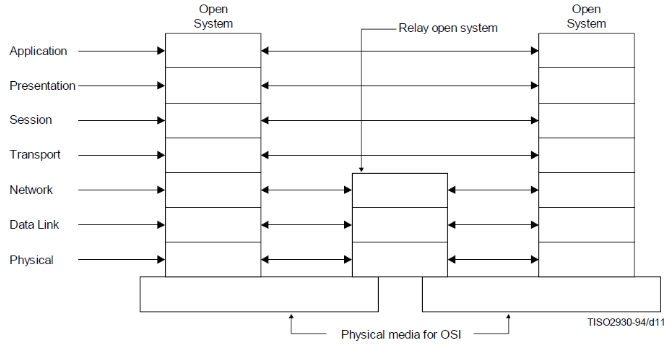


Figure 21 2-way IP transport

[296] International Telecommunication Union, "X.200: Data Networks and Open System Communications."

6.2 Appendix B The 3-layer model

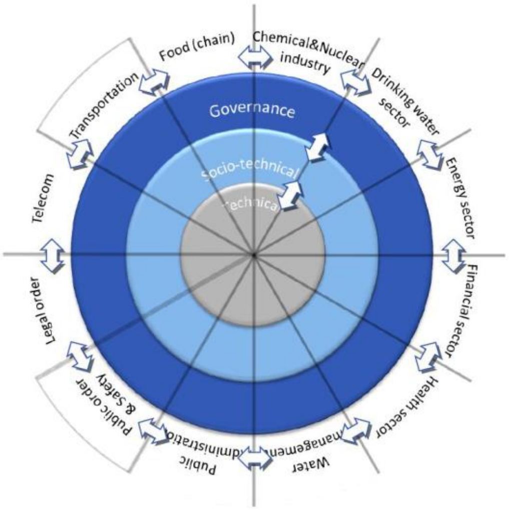


Figure 22 3-layer model[297]

The reason for using the 3-layer model in this thesis however was because it frays out especially the technical and governmental levels. A quick scan on the main subject revealed that just looking to either the technical or governmental aspects alone would not give a satisfactory analysis because the effects within the layers influence each other.

Other models reviewed were the 3-layer model of cyberspace from the U.S. army TRADOC[298] . This model however focusses more on the physical, logical location and persona instead of incorporating governmental aspects. This model was not chosen because physical and logical can be combined (see technical layer) and governmental is especially important in answering the research question.

Also, many models deducted from the 7-layer OSI model[299] were found, but on the abstraction level of this thesis, these 7 layers combined are regarded as the technical layer.

[297] Berg et al., “On (the Emergence of) Cyber Security Science and Its Challenges for Cyber Security Education.”

[298] United States: US Army, “Cyberspace Operations Concept Capability Plan 2016-2028.”

[299] International Telecommunication Union, “X.200: Data Networks and Open System Communications.”

6.3 Appendix C: Governance: Specific Law articles

6.3.1 Telecommunicatie wet[300]

Privacy

The principles relevant from a privacy perspective are:

Article 11.2a:	
1.	The confidentiality of the communication and associated data must be ensured. (G1)
2.	The consumer must give explicit consent for the actions of the ISP on his data after having received information on data type used, duration of use and the purpose of use. When a legislative provision is in place for the measure, no consent is needed. (G2)
3	The data which an ISP must store to be able to deliver the connectivity services shall be protected using appropriate technical protection measures. (G3)

Table 8 privacy notions Tw

Article 13.2a Lawful intercept	
1.	All organisations delivering telecommunication services are obliged to provide data, like location data, personal data, traffic data to identify users and their actions, when requested to do so for criminal investigations. This article enabled the ministry of justice and safety to install a procedure to oblige service providers to hand-over personal data like IP addresses to the CIOT on a daily base[301].

Table 9 Lawful intercept

Continuity

Article 11a.1 “duty of care”	
1.	*“Providers of public electronic communications networks and publicly available electronic communications services shall take appropriate technical and organisational measures to control the risks to security and the integrity of their networks and services.”*
2.	*“Our Minister may impose an obligation on a provider of public electronic communications networks and of publicly available electronic communications services to take technical or organisational measures within a given period regarding the security and integrity of public electronic communications networks and publicly available electronic communications services.”*

Table 10 Duty of care ISP

Service interruption	
1	An ISP delivering an internet access service can only stop delivery of the access service when necessary for protecting the integrity and/or safety of the network or services. The consumer being impacted must be informed before activating the security measure. *(article 7.6a 1g).*

Table 11 Service interruption

Duty of care exempt	
	The shaping principle and monitoring principle *“shall not prevent providers of internet access services from implementing reasonable traffic management measures. ~ such measures shall be transparent, non-discriminatory and proportionate~ Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.”* (Art *3.3)* These traffic-shaping measures **“***shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, to:*
A.	*comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;*
B.	*preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users; (G9)*

[300] Overheid.nl, “Telecommunicatie Wet.”

[301] Ministry of justive and safety, “Telecomgegevens Voor Opsporing.”

C.	*prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.*

Table 12 Duty of care exempt

6.3.2 Net Neutrality[302]

A	Safeguarding open internet access
1.	End-users can receive and distribute information without an ISP setting restrictions to location, origin, content, or application. (Art 3.1 shaping principle)
2.	All information and traffic are treated equally and without discrimination. (art 3.3 equality principle)
3.	Any traffic management measure may entail the processing of personal data only if such processing is necessary and proportionate (art 3.4)
4.	The ISP will not monitor the specific content of the traffic. (Art 3.3 monitoring principle) (G7)
5.	*“End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user’s or provider’s location or the location, origin or destination of the information, content, application or service, via their internet access service”.* (Art 3.1 CPE choice principle) (G8)

Table 13 Net neutrality technical principles

B	Transparency measures:
1.	Any traffic shaping (volume, speed, quality) performed is explained clearly by the operator. (explain principle) (art 4.1a) (G6)
2.	How to complain when NN is not followed by ISP. (complain principle) (art 4.2)

Table 14 Net neutrality transparency principles

6.3.3 Computer criminaliteit II[303]

Computer criminality law 2	
1	of the criminal code is applicable: “With a term of imprisonment not exceeding two years or a fine of the fourth category, the person who deliberately and unlawfully intrudes into an “geautomatiseerd werk” or part thereof shall be punished as guilty of computer intrusion.*”* (Article 138ab) (G10)

Table 15 Computer criminality 2

6.3.4 Manufacturer and Vendor duty of care [304]

Product liability section 3, book 6 of the Dutch Civil Code[305].article 6:185	
	The producer is liable for the damage caused by a defect in his product, unless
a	he has not put the product into circulation
b	in view of the circumstances, it is plausible that the defect that caused the damage did not exist at the time when it put the product into circulation, or that this defect arose later; (G11)
c	the product has been produced neither for sale nor for any other form of distribution for the economic purpose of the producer, nor has it been manufactured or distributed in the exercise of his profession or business;
d	the defect is because the product complies with mandatory government regulations;
e	based on the state of scientific and technical knowledge at the time when he put the product into circulation, it was impossible to discover the existence of the defect; (G11)

[302] European commision, “Open Internet Policy.”

[303] Overheid.nl, “Computer Criminaliteit II.”

[304] Cyber Security Raad, Wolters, and Jansen, “Ieder Bedrijf Heeft Digitale Zorgplichten”; Wolters, “Consument En Cybersecurity Een Agenda Voor Europese Harmonisatie van Zorgplichten.”

[305] wetten.overheid.nl, “Product Aansprakelijkheid.”

f	as far as the producer of a raw material or manufacturer of a component is concerned, the defect is due to the design of the product of which the raw material or component forms a constituent or to the instructions given by the manufacturer of the product.
2	The liability of the producer shall be reduced or cancelled considering all circumstances if the damage is caused both by a defect in the product and by the fault of the injured party or a person for whom the injured party is liable.
3	The liability of the producer shall not be reduced if the damage is caused both by a defect in the product and by the conduct of a third party.

Table 16 Product liability

Product defective criteria section 3, book 6 of the Dutch Civil Code[306]. article 6:186	
1	A product is defective if it does not offer the safety one can expect from it, taking all circumstances into account and in particular: A: The presentation of the product B: the reasonably foreseeable use of the product; C: the time when the product was put into circulation. (G11)

Table 17 Product defective criteria

6.3.5 Radio equipment directive[307]

Chapter 1 Article 3 Essential requirements	
3.a.	radio equipment interworks with accessories
3.b.	radio equipment interworks with other radio equipment
3.c.	connected to interfaces of the appropriate type
3.d.	not harm the network nor misuse network resources
3.e.	protection of personal data and privacy
3.f.	protection from fraud
3.g.	access to emergency services;
3.h	facilitate its use by users with a disability
3.i.	Only compliant software can be loaded

Table 18 Essential RED requirement

Provisions in red are optional and can be activated only by the European Commission on specific product groups.

6.3.6 ENISA Vulnerability management best practices[308]

ENISA VM best practices	
GP-TM-04	Sign code cryptographically to ensure it has not been tampered with after signing it as safe for the device and implement run-time protection and secure execution monitoring to make sure malicious attacks do not overwrite code after it is loaded.
GP-TM-05	Control the installation of software in operating systems, to prevent unauthenticated software and files from being loaded onto it.
GP-TM-18	Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), that it is signed by an authorized trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.
GP-TM-19	Offer an automatic firmware update mechanism.

[306] wetten.overheid.nl.

[307] Commision, “Radio Equipment Directive.”

[308] ENISA, *Baseline Secur. Recomm. IoT Context Crit. Inf. Infrastructures*.

GP-TM-20	Backward compatibility of firmware updates. Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.
GP-TM-09	Establish hard to crack, device-individual default passwords.
GP-TM-22	Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null, or blank passwords are not allowed.
GP-TM-28	Device firmware should be designed to isolate privileged code, processes, and data from portions of the firmware that do not need access to them. Device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code.
GP-TM-42	Do not trust data received and always verify any interconnections. Discover, identify, and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services.
GP-TM-44	Make intentional connections. Prevent unauthorized connections to it or other devices the product is connected to, at all levels of the protocols.
GP-TM-43	IoT devices should be restrictive rather than permissive in communicating.
GP-TM-47	Risk Segmentation. Splitting network elements into separate components to help isolate security breaches and minimize the overall risk.
GP-TM-48	Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set.
GP-TM-50	Ensure only necessary ports are exposed and available
GP-TM-52	Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.
GP-TM-56	Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors.
GP-TM-57	: Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.
NT1 (G20)	End users and consumers must be educated to be able to make informed decisions when buying IoT devices and systems. Campaigns raising awareness for IoT security are thus highly important, also to be able to maintain a basic level of cyber hygiene for the security of the “Things” that they have purchased or are operating. The role and initiatives of consumer rights associations should be highlighted in this respect.
NT2	trainings and courses at schools and universities (considering localization to reach a wider audience) will further promote a better understanding of IoT security among the younger generation and thus in the long-term contributed to raising awareness.
NT3	Moreover, market demands on cybersecurity are somewhat low because of the lack of consumer perception in the added value of cybersecurity. Consumer involvement is quite important, and it should be supported more. Communication campaigns should be implemented by the government (e.g., the Commission, member states) to increase and sustain said perception and thus inherently necessitate the adoption of further mechanisms to promote IoT cybersecurity.
NT4	a specific level of security and privacy before market deployment is encouraged. Defining security frameworks supported by baseline security measures can be a way forward in this direction.,
NT5	Use of other schemes such as certification and labelling can also encourage better understanding and transparency in terms of IoT security and thus should

	be considered (also benefitting end users and consumers in educating them and making them more aware of IoT security) albeit in a context and risk specific manner per use case/application sector.
NT6	Subject to such approaches, subsequently regulative efforts and initiatives could then be put in place to follow the same path.
NT7	A noteworthy aspect involves security updates that constitute a significant issue in the context of IoT. After deployment, security updates need to be provided where practically possible without special knowledge requirements or financial obligations on the end user/consumer within a defined term and conditions until “end-of-support”. The latter must be clearly defined by the manufacturer/provider of the IoT product and must be clearly communicated to the end user/consumer.
	As identified by the interviews with the experts, an important issue when IoT is considered is that of liability. It is of particular importance in the IoT domain since the cyber-physical nature of IoT relates and tightly binds security to safety. The question of liability needs to be addressed. The question of where liability may fall lies between the different and diverse stakeholders of the IoT ecosystem, such as developers, manufacturers, providers, vendors, aftermarket support operators, third party providers and the end users, to name a few.

Table 19 ENISA VM best practices

6.4 Appendix D Roadmap requirements

The table starts with the requirement number. This field starts with a letter which corresponds to the chapter (see index). The following number is the requirement number of that section. The second column is the requirement. The third column is the designation linking the requirement to the vulnerability management model (Discovery (D), Classify (C), Report (R), Remediate (S), Plan (P). The fourth column depicts whether the requirement maps to the 3-layer model (governance (G), socio technical (S), technical (T)). When the third column holds no value then, the requirement cannot directly be plotted on the VM model.
The following requirements for the roadmap were derived:

Nr.	Requirement rationale	VM	GST
A1	Accountability must be established end-2-end over the product chain		G
C1	Attribution must be clear (currently the contract holder is responsible for what happens in the home domain).		G
C10	Consumers with IT skills must be incentivized to help consumers with less skill	S	G
C11	Effects from an attack must be visible to the people responsible.		S
C12	Government and ISP's must help raise awareness with consumers.		S
C13	To be able to fill in C12, reputations of ISP and government must be increased		G
C2	Security patch installation must be automated.	S	T
C3	Security must be easily interpretable to consumers.	S	G
C4	Security standards must be devised so users can differentiate between products based on the security level.		G
C5	Provisions to empower the standard need to be in place to prevent a lemon market situation		G
C6	legal support must be created regarding security for connected devices for consumers to be able to stand up for their rights in court with a reasonable chance of success.		G
C7	Consumer liability regarding security of connected devices must be clear.		G
C8	Consumers must have sufficient resources available to live up to their liability.	S	S
C9	Consumer organisations must be able to play a role in raising awareness by also reporting on security of connected devices (like Consumentenbond).		S
D1	ISP's and industry must assist in cleaning the in-home domain.		G
D2	A combined stakeholder approach is needed to come to a solution to secure the in-home domain.		G
D3	The proposed solution must scale to cope with large numbers of devices		T
D4	Cybersecurity scans must be done by industry, and found vulnerabilities need to be resolved before releasing new software or devices to general public.		T
D5	Liability law must be unambiguous and clear for stakeholders to take their role in securing connected devices.		G
D6	Industry must work together with governmental organisations to set the right balance of security measures.		G
D7	Consumers must be made aware of the risks of connected devices		S
D8	Consumers must be made aware of their role and responsibilities in securing connected devices.		S
G1	Confidentiality of the personal data must be ensured		G
G10	The VM solution must not deliberate and unlawful intrude consumer owned equipment.	D	G
G11	Liability law is now based on "bring product in circulation", this should also incorporate the run phase of products.		G
G12	Product liability law is based on tangible goods. Software is not tangible. This should be appended.		G
G13	Liability law is only applicable to bodily injury and property damage in the private sphere. This scope must be widened.		G

G14	When the RED is installed as a baseline framework, then amendments must be made to incorporate minimum demands and risk appetite.		G
G15	When self-regulating, requirements must be set on which to self-regulate.	C	G
G16	When self-regulation is used, then an organisation must be appointed to keep oversight.		G
G17	When voluntary fails, then EU will switch to mandatory. Make smart. What is expected, when, who is accountable, what will happen when mandatory demands are not met.		G
G18	The RED is focused on radio connectivity. This should also incorporate fixed line devices		G
G19	Best practices which are discovered and tested by mature security organisations must be used by less mature organisations. Cooperation must be promoted or incentivized.	S	G
G2	Either consent must be given by the consumer or a legislative provision to scan the in-home domain must be implemented.	D	G
G20	Apart from technical vulnerabilities, human vulnerabilities must also be mitigated.	S	S
G3	Personal data must be protected using “appropriate technical protection methods”		T
G4	The VM solution must take care of personal data. When personal data is requested by Dutch government, this includes vulnerability data when in possession by the ISP, then this must be clear to the consumer.	D	G
G5	The ISP must take appropriate measures to control the risks to security and integrity of their services.	S	T
G6	Any traffic shaping is explained clearly by the ISP.	S	S
G7	ISP’s shall not monitor the specific content of the data.		G
G8	The consumer must be able to use terminal equipment of their own choosing	D	G
G9	Shaping and monitoring must preserve the integrity and security of the network or services provided via that network, and of terminal equipment of end-users.		G
I1	The ISP must ensure the continuity of its services and network.		G
I3	Negative impact of security measures must be as low as possible		T
I4	ISP must not become the “police officer” of the internet		G
M1	Standard contracts including liability must help solve the liability issues with security in complex product chains		G
M10	The required quality of security of end user devices must be predetermined and enforced before and during use and management by consumers.		G
M2	Standardisation in connectivity modules should help solve the security problems with the current diversity in modules	S	G
M3	Ambiguous contracts which limit rights of consumers must be actively combated.		G
M4	Security and their best practices must become mandatory in contracts between connected device parts suppliers.		G
M5	Security must be looked at in an end to end manner. Not only by securing the device, function, or local data. Cloud components must also be secured.	S	T
M6	Incentives for releasing secure products must be installed	S	G
M7	Security must be easy to “use” by consumers	S	S
M8	Standardized software /interfaces should be used which make it easier for security software providers to create matching security products.		G
M9	Vulnerabilities in Home-routers must be controlled especially		T
R1	The VM solution must be able to discover vulnerabilities in all in-home devices.	D	T
R2	The CPE poses a big risk to the in-home domain, hardening best practices must be followed	S	T
R3	Home-router software must be kept up-to-date	S	T

R4	Home routers should be shipped with unnecessary services turned off.	S	T
T1	The VM method supports IP connected devices.	D	T
T2	The VM method supports WIFI and powerline connected devices.	D	T
V1	The VM solution must be able to discover devices in the in-home domain	D	T
V10	Ground must be established on which to force uncoupling connected devices which cannot be secured.	S	G
V11	Consumers must be educated to improve security awareness		S
V12	The VM process must be done in a periodic manner	P	G
V13	The VM solution must scan with the same vector as attackers	D	T
V14	The VM solution must scan all connected devices in the in-home domain	D	T
V15	the scan solution must scan using a method that matches the expected products in the in-home domain	D	T
V16	Human vulnerabilities must be resolved	S	S
V17	Scanning must not require extra hardware (cost)		T
V18	When network zoning is used, devices in all zones must be scanned	D	T
V19	To be cost efficient, the install-base must be large		G
V2	The VM solution must support automated scanning	D	G
V20	The scan must scan for default passwords	D	T
V21	The scan must not negatively impact the user experience.	D	S
V22	The scan solution must be able to differentiate between devices to speed up scanning by only testing relevant signatures	D	T
V23	The scanning method should be able to detect new vulnerabilities	D	T
V24	A solution for older devices must be devised which either crash or which cannot be updated.	S	T
V25	Scanning must be done legally	D	G
V3	A ranking standard must be agreed upon to be able to rank vulnerabilities.	C	G
V4	An acceptable risk standard must be set	C	G
V5	The report must show the vulnerabilities which exceed the acceptable risk threshold	R	G
V6	Standard solutions must be suggested to the consumer	R	G
V7	The report must only contain the vulnerabilities applicable to that particular user.	R	G
V8	Security updates or patches for vulnerabilities above threshold must be available.	S	T
V9	When updating is not possible, other mitigative measures must be available	S	T

Table 20 Roadmap requirements