Roadmap for

Digital Hard- and Software Security

Ministry of Economic Affairs and Climate Policy
Ministry of Justice and Security

The Hague, April 2018

Summary

Digitalisation increases our dependency on ICT. Although there are many associated advantages, this also makes us vulnerable to threats such as data theft, business sabotage or extortion. Because interconnected devices are increasing in number, digital security is a concern not only for individuals, but also for society as a whole. Many parties, including the Dutch government, are currently taking measures to promote the security of digital products. However, due to poor cohesion as well as market and behavioural failure, these measures are still lacking in effectiveness.

The Digital Hard- and Software Security Roadmap offers a cohesive set of measures for eliminating security gaps in hard- and software, detecting vulnerabilities and mitigating their consequences. All stages of the product life cycle are covered; digital security must be promoted from beginning to end, from product design and production right through to use and disposal. Effective examples include strong passwords, timely updates and deletion of data at the end of a product's life. Joint responsibility is also important in this respect, as it is not only the suppliers of a product, but also the users who have a part to play in digital security. The Dutch government is investing in various instruments aimed at promoting hard- and software security, to which other parties, such as sector organisations and universities, can also contribute.

Whatever the stage, the aim is to strike the right balance between security, freedom and economic growth. A one-sided focus on security can potentially undermine other public values, such as human rights and innovation, despite the fact that innovative products can actually help reinforce security in the long term. This Roadmap aims to counteract these threats and protect fundamental rights and values, while also taking full advantage of the opportunities offered by digitalisation. It also leaves room for complementary measures in specific domains or sectors, as relevant risk assessments and associated measures can vary greatly.

This Roadmap proposes the following measures:

Standards and certification. The application of standards in both the design and use of a product is important in order to reduce vulnerabilities. Standards can also be used to increase the demand for secure products. Most efforts in this regard are aimed at coordinating various initiatives that seek to create standards for retaining cost/other effectiveness and make an active contribution to European negotiations in the field of standards and mandatory certification.

Monitoring the digital security of products. Detecting and sharing information on vulnerabilities allows manufacturers to modify non-secure products. Retailers can consider removing products from the shelves and users can decide to patch or deactivate their products. The Dutch government intends to cooperate with the private sector and other relevant stakeholders to develop a monitoring mechanism offering information on the digital security of products, with a specific focus on devices that are part of the Internet of Things. This monitoring will also include experiences in the international arena.

Cleaning up infected user products. Internet service providers can play a major role in increasing hard- and software security. The Dutch government plans to initiate discussions with Internet service providers, to explore how they can help combat non-secure IoT devices (analogous to their successful approach to mitigate botnets.

Testing for digital security. Testing for vulnerabilities is necessary at various stages of the product life cycle. To gain experience and find out what a shared testing platform has to offer, a pilot is under development using a range of sector-based use cases.

Cybersecurity research. Innovation is indispensable when it comes to hard- and software security, which is why the Netherlands invests in research on innovative solutions to tackle security problems.

Liability. Liability legislation enables users to claim damages resulting from a lack of digital security, which acts as an incentive for providers to keep their hard- and software secure. The Dutch government is currently in dialogue with stakeholders and specialists regarding areas for attention and improvement when it comes to liability for insufficient digital security of hard- and software. The Netherlands is also actively taking part in the expert group on liability and new technologies. In the EU negotiations on the European Commission's proposal for a directive on digital content and digital services, the Dutch government is proposing mandatory security updates for software products supplied to consumers.

Statutory requirements, supervision and enforcement. Setting minimum security requirements can serve to keep non-secure products off the market. The Dutch government is investigating which minimal security requirements can be made applicable to devices under the EU's Radio Equipment Directive.

Awareness campaigns and empowerment. As part of the cybersecurity awareness campaigns run by the website https://veiliginternetten.nl, the Dutch government will be launching one or more public campaigns to support policy-making for digitally secure hard- and software. Awareness campaigns will tie in with the above-mentioned measures where necessary, in order to raise awareness and increase resilience among consumers and SMEs.

National government procurement policy. National governments are major hard- and software users. They can include digital security criteria in their procurement policies, in order to both set a good example and foster demand for digitally secure products. The Dutch government will investigate which additional measures are necessary or desirable in national government procurement to ensure digitally secure hard- and software.