‘Towards a safe, connected, digital society’

Recommendation on the cybersecurity of the Internet of Things (IoT)

CSR

Cyber Security Council

Cyber Security Raad

‘Towards a safe, connected, digital society’

Recommendation on the cybersecurity of the Internet of Things (IoT)

Addressed to:

The Minister of Justice and Security
The State Secretary for Economic Affairs and Climate Policy
The State Secretary for the Interior and Kingdom Relations

CSR
Cyber Security Council
Cyber Security Raad

In addition, support and advice was requested from
the President of the Confederation of Netherlands Industry
and Employers (VNO-NCW)

CSR recommendation 2017, No. 3

Your Excellencies,

The Netherlands is in an outstanding starting position to exploit the economic opportunities of the digital future to the full. The level of digitalisation, the business climate and the available infrastructure are all factors that put the Netherlands in a leading position in Europe. This makes ensuring the conditions for economic success even more important: the security, trust in and the reliability of the digital infrastructure. New technologies are being developed at a meteoric pace and are a significant driver of innovation and economic growth. One of those technological developments is the Internet of Things (IoT).

The IoT is a network of 'smart' appliances, sensors and other objects (often connected to the internet) that collect data on their environment, can exchange this data and make (semi) autonomous decisions and/or take actions that affect their environment based on it.

The IoT will play an increasingly prominent role in daily life. The physical and digital worlds will become further interwoven. This will affect job opportunities, healthcare, mobility and prosperity among other things. There are many uses for the IoT, ranging from eHealth, smart homes, smart industries and smart cities to digital infrastructure. Examples include pacemakers, smart vacuum cleaners, self-driving cars, solar panels and locks on rivers and canals.

Opportunities and threats

The IoT is not a separate domain. It is part of the wider task of urgently improving the cybersecurity of our online services and systems, as has already been discussed in the Verhagen report[1]. However, the IoT does bring certain problems more urgently into focus because security problems are now manifesting themselves outside of the conventional IT domains.

The technical and economic opportunities presented by the IoT go hand in hand with digital threats to economic growth, security and freedom. This is why the Cyber Security Council (CSR) commissioned the Research and Documentation Centre (*Wetenschappelijk Onderzoeks- en Documentatiecentrum, WODC*) to conduct exploratory research[2]. This research revealed that the IoT could have far-reaching consequences if measures are not taken. Currently, IoT applications are often poorly secured and therefore form a threat to our security and privacy. The Mirai botnet, comprising hacked IoT devices, shows that the impact can already be severe and that this will only increase in the future. It is therefore important that the security and privacy risks are tackled to mitigate and prevent damage as far as possible. Targeted action is needed to secure our prosperity and well-being now and in the future.

Most significant challenges

The most significant challenges that the IoT brings with it are:

Vulnerability is increasing due to the scale at which insufficiently secured devices are connected to each other and the internet.

The problem is the explosive proliferation of insecure devices and applications that are connected to each other. This is not only new devices, older –and by definition insecure –devices are already connected to the internet. This concerns technologies that are connected to each other which lack cohesion, the result being that network security is almost impossible to achieve. The quality of the

[1] The economic and social need for more cybersecurity: Keep "dry feet" in the digital era', Herna Verhagen, September 2016

[2] '(Mis)connected in a smart society. The Internet of Things: opportunities, threats and measures', WODC, June 2017.

current software often leaves a lot to be desired and new devices lack or have very limited update-capabilities.

The amount of data that can be collected is enormous. Data security is difficult to arrange.
The basis for many (economic) opportunities lies in the fact that the IoT makes large quantities of data available. However, the data and/or applications that are available can also be used for unwanted criminal purposes. Consumers and businesses are insufficiently aware of the risks and do not implement adequate measures.

Enforcing the duties of care and liability for the products and services that are supplied is extraordinarily complex.

The IoT playing field is large, without borders and has a complex international composition. It is often the case that numerous parties are involved in the production and use of IoT products. Manufacturers combine or ‘rebrand ’different hardware and software from other manufacturers. There is lack of oversight due to the multiplicity of players, often foreign, in the IoT market. This makes it unclear who bears final responsibility and can be held to account. The problem is exacerbated by the fact that countries employ different standards and regulations. For the time being, there are few incentives to produce and maintain secure hardware and software. For the majority of manufacturers, the time-to-market and a low cost price are more important than the quality of a product. Businesses put too little effort into meeting their obligations and cybercriminals make grateful use of this. In addition, legislation with regards to duties of care within the EU (and globally) is not or is scarcely coordinated.

Recommendation

The CSR sees six strategic solutions to tackle the challenges posed by the IoT, partly based on the WODC report. As such, we recommend the following, concrete actions:

1. Certification, quality marking and access requirements
    - The State Secretary for Economic Affairs and Climate Policy explores how the proposed EU Cybersecurity Certification Framework[3] and, if necessary, CE marking can be used to keep unsecured IoT devices off the European market. Certification should be used to formulate minimum requirements in regard to the length of time that the supplier supports the product, the way in which security updates should be made available, the period during which the burden of proof of conformity rests with the supplier and the requirement that the device can be disconnected from the internet without the loss of 'normal 'functionality. If the European framework does not provide sufficient capabilities, the Minister should then draft a (legislative) proposal to guarantee these requirements, through the selling regulations for instance.
    - The State Secretary for the Interior and Kingdom Relations, in conjunction with central government and regional authorities, sets up procurement policy in such a way that standard digital security requirements are set for suppliers, including within the framework of smart cities.
    - The Minister of Justice and Security coordinates a proposal for including cybersecurity standards into existing binding sectoral security requirements in major sectors such as healthcare, transport and energy.

2. Transparency
    - The State Secretary for Economic Affairs and Climate Policy and the Minister of Justice and Security fund an independent monitor of hacked and vulnerable IoT devices so that information on which manufacturers and suppliers do not adequately secure their devices becomes available publicly.

3. Raising awareness
    - The State Secretary for Economic Affairs and Climate Policy and the Minister of Justice and Security request a clear commitment from the manufacturers and suppliers of IoT devices to use a 'labelling system '(e.g. stickers on the packaging) to provide customers with information about (i) the level of security of the device concerned; (ii) if the device can receive automatic security updates; (iii) the period during which the supplier will maintain the product; and (iv) if the device can be disconnected from the internet without loss of 'normal 'functionality.
    - The State Secretary for Economic Affairs and Climate Policy and the Minister of Justice and Security fund an information campaign and have a simple guide drawn up that informs consumers of the new labelling system and helps to deal with the risks of the IoT.

[3] Joint Communication to the European Parliament and the Council, 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Brussels, 13.9.2017 JOIN(2017) 450 final.

4. Product liability
    - The State Secretary of Economic Affairs and Climate Policy and the Minister of Justice and Security draft (proposed) legislation to tie-in the security of IT products and services more closely with the product liability scheme, whereby manufacturers can be held legally liable for economic loss also. This proposal should preferably tie-in with the measures that will be presented by the European Commission in June 2018.[4]
    - The State Secretary for Economic Affairs and Climate Policy and the Minister of Justice and Security identify which Dutch supervisory bodies, similar to the American Federal Trade Commission[5], can address manufacturers on basic security problems, such as not issuing security patches in a timely manner, based on existing duties of care. The Duties of Care Manual[6] and the FTC Directive[7], among other things, can serve as the basis for this.

5. The responsibilities of intermediaries
    - The State Secretary for Economic Affairs and Climate Policy and the Minister of Justice and Security together draw up industry guidelines for bringing the security of the IoT under the existing duties of care of intermediary suppliers.
    - The State Secretary for Economic Affairs and Climate Policy and the Minister of Justice and Security request a clear commitment from the internet providers to help remove infected IoT devices from their networks, similar to the successful approach to botnets (in AbuseHub for instance).

6. Improving enforcement
    - The Minister of Justice and Security coordinates a proposal from all of the Ministries concerned to create a proper mandate and sufficient capacity to structurally guarantee the enforcement of cybersecurity standards and rules in all sectors.

The Hague, December 2017

on behalf of the Cyber Security Council,

Jos Nijhuis
Co-chairman CSR

Dick Schoof
Co-chairman CSR

[4] Joint Communication to the European Parliament and the Council, 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Brussels, 13.9.2017 JOIN(2017) 450 final (p. 6).

[5] See: https://www.ftc.gov/about-ftc

[6] 'Every Business has duties of care in the field of cyber security, cyber security guide for businesses', CRS, February 2017.

[7] See: https://www.ftc.gov/news-events/press-releases/2017/06/ftc-offers-comment-process-aimed-improving-security-internet