BITS OF FREEDOM
Voor jouw internetvrijheid

Datum:
January 29, 2018

Bits of Freedom
Prinseneiland 97hs
1013 LN Amsterdam

Rejo Zenger
+31 6 39 64 27 38
rejo.zenger@bof.nl

bitsoffreedom.nl
IBAN: NL73 TRIO 0391 1073 80
KVK: 34 12 12 86, Amsterdam

Position paper regarding some aspects of the Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[1] and the proposal for the regulation Cybersecurity Act[2]

About our reliance on disruptive technologies

Much of the technology we use today is said to be disruptive. What is usually meant is that these technologies are capable of turning entire fields of business upside down in no time. The reality, of course, is that these technologies can disrupt all of society at once. Not because the technology forces us to rethink business models, but because our reliance on our digital infrastructure has grown exponentially while our attention for the security of that infrastructure has not kept pace at all. The consequences for our democracies, freedoms, economies, prosperity and safety are immense. Bits of Freedom would like to raise the attention of the European legislators to two aspects in particular.

First of all, we have noticed that many attacks are enabled due to the vulnerabilities that exist in much of the software on which our digital infrastructure is build. These attacks are often based on known vulnerabilities for which the update to remove that vulnerability wasn't deployed. These attacks do not only impact the user of the hard- or software, but also has external implications when the device is used in an (DDoS-)attack against other devices. There are quite a number of reasons why security updates aren't deployed, such as updates that unexpectedly change the behaviour of the vulnerable product, complicated certification processes, and the lack of security-by-default-settings. The solutions to this problem range from absurdly simple to rather complex, but all must be actively explored in order to optimise the security of our digital systems.

Secondly, the freedom to use encryption, to secure the digital communications and information of users, companies and governments, is under attack regularly. Some governments of member states think that, in order to secure our societies, it is acceptable to weaken the security of our hard- and software. However, as noted before, an insecure digital infrastructure will lead to a disrupted society.

[1] JOIN(2017) 450 of September 13th 2017

[2] COM(2017) 477 / 2017/0225 (COD) of September 13th 2017

Here's what needs to be done

Ensure security-by-default

The European legislator should ensure that all digital products on sale on the market are optimized for security. Manufacturers should be required to provide timely security updates for the entire lifetime of a product, to enable automatic installation of security updates whenever possible, to make a distinction between security-related and other updates and to make sure security updates are cryptographically signed to allow for verification of their authenticity and integrity. We also need to change the way some types of certification of industrial infrastructures work, as requiring a full re-certification of the entire system after patching a small security updates deters companies from deploying such an update.

Create a harmonized and mandatory certification framework

Because we care about the safety of the children, we have a framework regulating the minimum requirements for toys on the European market. For example, manufactures are not allowed to develop toys built from toxic material. Small parts of toys have a minimum size to prevent children from suffocating. We do not have similar minimum requirements when it comes to products which potentially negatively impact the security of our digital infrastructure. Bits of Freedom urges European legislators to introduce a certification framework, which will enforce minimum security standards for hard- and software on the European market. This certification framework should be harmonized and mandatory. A voluntary system would not help as it would not prevent manufactures, often from outside the European market, to sell cheap but insecure products.

Introduce liability for vulnerabilities in hard- and software

In nearly every business the manufacturer is liable for defects and damage caused by those defects. If you have house build for you, and the roof is blown away with the first mild storm, the architect or construction company can be held liable for the damage that has been caused. This is not the case for damage caused by vulnerabilities in hard- and software. These issues are often caused by low quality of the software, partly due to market pressure. When a critical vulnerability has been identified, it sometimes still takes months before an update to resolve the vulnerability is made available. Customers, oftentimes end-users with no means to protect themselves are left alone. This needs to change and this can be done by introducing or ensuring liability for hard- and software manufacturers and vendors.

Support development, production and use of encryption

The availability and use of high-grade encryption is essential for the protection of our digital infrastructure and communications. It is not only important for our democratic freedoms, but also vital for innovation and economic growth. Therefore, European legislators must stimulate further development of encryption, stimulate the application of encryption and should not undermine the development, production or application of encryption in any way. By extension, the legislator should not set limits on the maximum length of encryption keys, compel the installation of vulnerabilities for use by the government (such as backdoors), require the creation and/or handover of master encryptions keys, restrict the export or import of encryption technologies, or take any other step that hampers development and use of encryption.