Blog Post for SOURCE: (1700 words)

Three ways to Improve Preparedness for Cybersecurity—and Ethical Issues

Cybersecurity is part of *societal security* ("the ability of a society to persist in its essential character under changing conditions and possible or actual threats"). Potentially, cybersecurity concerns all of us; we can all become victims. Cyberattacks can come from a wide range of sources, ranging from a state and non-state groups to criminals, and can be aimed at a wide range of targets, ranging from individual citizens and businesses to infrastructure. Furthermore, the risks of cybersecurity are not always easy to grasp. And even if we understand the risks and know possible solutions, we can fail to prepare properly. Moreover, cybersecurity is not only a technological and economic phenomenon, but also a societal phenomenon; it involves citizens, companies and government agencies.

Focus on Preparedness for Cybersecurity

In order to better understand the role of citizens, companies and government agencies, we organized a workshop that focuses on *preparedness, prevention and resilience*: all the things that citizens, companies or government agencies can do to better prepare against cyberattacks, e.g., measures to better sustain a cyberattack, reduce the damage, or to keep things going as much as possible. We focused on preparedness because this theme often receives relatively little attention and because it raises a lot of questions: How much do we want to invest in preparedness? Compared to, e.g., cyberattack crisis management? And who should be responsible: citizens, companies, state agencies?

We can draw parallels to measures to promote preparedness in other domains, e.g., for flooding or for industry incidents. The Dutch government, e.g., advises (https://crisis.nl/wees-voorbereid/tips/): to have an emergency kit ready (with a radio, torch, spare batteries, first aid kit, matches, small candles, blankets, water bottles, tools and an alarm whistle) and to be informed about specific risks, depending on where you live, and to know what to do when the sirens sound, etc.

Do you have such an emergency kit? With spare batteries and enough water bottles? Do you know the risks for your region, and what to do when the sirens sound? And what about the equivalent preparedness for cybersecurity? Do you know the risks? What's your cybersecurity emergency kit?

Workshop Findings

We invited several experts for our workshop: to explore and discuss possible measures to improve ***preparedness*** for cybersecurity. Moreover, we identified various ***values that are at stake***, and ways to cope with these values, e.g., when different values conflicts with each other, like usability (not using passwords or using easy-to-guess passwords) versus security (using hard-to-guess passwords):

- Johan van Wilsem, manager of research into Criminality, Law Enforcement and Sanctions of the Research & Documentation Office (WODC) of the Dutch Ministry of Justice and Security
- Rolf van Wegberg, PhD candidate at Delft University of Technology, and Principal investigator of the cybercrime research program at TNO
- Rick van der Kleij, senior researcher of Cybersecurity & SMEs Research Group at The Hague University of Applied Sciences, and senior scientist human factors in cybersecurity at TNO
- Marc Steen, senior scientist of responsible innovation at TNO—SOURCE project team member and workshop facilitator—the workshop was prepared together with Kristoffer Liden, of PRIO.

Below are some of the ideas that we generated and discussed—including some remarks on freedom and equality, key values that we will want to uphold and protect in our society.

A Quality Mark for Internet-of-Things Devices

People are putting IoT devices in their homes and businesses, from robot vacuum cleaners to baby watching cameras. These devices introduce many vulnerabilities. People do not change the default password ("00000") or update the firmware. And manufacturers have little incentives to improve cybersecurity (they often compete on price, not on cybersecurity). The danger lies in these devices being hacked, and then being used as 'stepping stones' into a home or business network, or being deployed within a larger botnet, which can be used maliciously, e.g., for DDoS attacks.

For example, there was an incident in which a casino got hacked through its internet-connected fish tank thermometer: https://thehackernews.com/2018/04/iot-hacking-thermometer.html

From: https://commons.wikimedia.org/wiki/File:Fish_Tank_@_Honolulu_Aquarium_(4671604664).jpg

A potential solution would be a Quality Mark for IoT devices, overseen by an independent government agency. A Quality Mark would require people to use strong password and ensure automatic firmware updates for five years into the future. Such a Quality Mark would involve a trade-off between usability and security.

Freedom and equality

Moreover, it would involve values like freedom and equality. Producers and vendors of IoT devices can perceive such a measure as infringement of their freedom. There is, however, a history of successfully introducing measures for safety, like safety belts in cars. If everybody needs to comply, they do not disturb the market.

Looking at equality, this could actually be improved by such a measure. There are currently (risks for) inequalities regarding cybersecurity between, on the one hand, people who *can* afford expensive devices (which are likely to be more secure) or who *have* cybersecurity skills (and, e.g., know about changing passwords), and, on the other hand, people who *cannot* afford expensive devices (and therefore have cheap and potentially less safe devices) or people who *lack* cybersecurity skills (and, e.g., forget to use strong passwords). Such inequalities will diminish with a Quality Mark, if it creates a minimum of cybersecurity for all IoT devices, regardless of prize or skills.

A Protection Service by Internet Service Providers, plus Basic Insurance (optional)

Another potential solution for the vulnerability of networked devices is that the Internet Service Provider (ISP; the company that puts the router in people's homes and businesses), monitors the addition of new devices to the network. If the ISP recognizes the device as safe, it allows it to connect fully. If, however the ISP recognizes the device as unsafe, e.g., because it has outdated firmware, than it only partly connects it to the network and gives a warning: "We detected a device with outdated firmware. We have put it in a walled garden; it can now only receive data, but not send any data. You need to update the firmware [instructions]; after that, it will be added to the network".

From: https://enterprisersproject.com/article/2016/2/internet-hackable-things-why-iot-devices-need-better-security

This measure is imagined as a Protection Service offered by ISPs. Additionally, ISPs can offer a Basic Insurance which will cover damages of cyberattacks (with an lower limit for own risk; and an upper limit of payment). This would be like booking a trip, plus a basic travel insurance.

Freedom and equality

If we look at freedom, ISPs will be free to offer these services (or not) and consumers will be free to choose it (or not). It is, however, likely that ISPs at the higher end of the market will offer such services, and that ISPs at the lower end will not, or only after these services have become commodities.

This may introduce inequalities. People with less disposable income may not be able afford such a Protection Service. Or people with less cybersecurity skills may be unable to follow the instructions of the Basic Insurance—and then fail to eligible for payments after an attack (there will be fine print saying that you need to follow instructions in order to be eligible for payment). This could exacerbate the digital divide regarding cybersecurity, where people with money and skills are safer than people with less money and less skills. ISPs may be accused of 'denying protection to less-paying clients'.

In order to reduce some of these inequalities, it may be needed that some independent or government agency sets minimum requirements for such a Protection Service and associated Basic Insurance. This would create a level playing field, and clarify what to expect of such a service and insurance; to protect citizens and businesses against having too high (or 'naïve') expectations.

Improved Communication and Motivation

Another way of improving preparedness for cybersecurity is to improve communication. Of course, there is basic information available. However, knowing the basics is often not enough. In addition, having information is not enough to change behaviour. Knowledge does not automatically translate into action. It is like living next to a river and knowing about the risk of flooding and about the need to have an emergency kit ready—but not having prepared such an kit.

From: https://www.itchronicles.com/security/cybersecurity-needs-a-human-firewall/

It would help if people receive personalised information about risks, plus instructions for how they can improve their preparedness. For example: “There was an X malware in email Y, which caused Z damage”, and instructions for what to do better in the future, like “If you see A, do B, and never do C”. Similar to the advice of a police officer after a home burglary: they look at the lock on the front door, show you how it was compromised, and advise to buy a better lock.

In addition, people need to be motivated to translate knowledge into action, e.g., by showing the positive/negative effects of safe/unsafe behaviour. Or they can be ‘nudged towards safer behaviour, e.g., by making safe behaviour simple—like putting the healthy food in the front, and the unhealthy snacks at the back; you are still free to choose, but you are nudged towards healthy eating.

A government agency can create a communication campaign. Such an agency can also provide instructions for, e.g., ISPs, how they need to inform their customers (“this happened; this you need to do better next time”). ISPs can then provide the personalised, detailed and practical information.

Freedom and equality

More information is likely to promote freedom, provide that this information is available, accessible and usable for all people. That is where a national government agency needs to play a role. If the information is not easily or universally available, accessible and usable, there are risks for inequality: the information would then be available for, e.g., only people with higher incomes or more skills.

Furthermore, measures for ‘nudging’ will need to be developed carefully, in order to protect people’s freedom. On the other hand, there are already all sorts of organizations and companies that attempt to influence people’s behaviour. The crux is probably to be transparent about the ‘nudging’.

Conclusions

There are various ways to improve the preparedness for cybersecurity. We explored three practical measures to promote preparedness in people and (small) businesses—measures in which government agencies, companies like ISPs and citizens have different roles and responsibilities. Moreover, we started to discuss key values, like freedom and equality, which will need to be taken into account carefully when designing and implementing such measures.

Further reading:

- Charter of Fundamental Rights of the European Union
- CANVAS White Paper 1: Cybersecurity and ethics
- Nederlandse Cybersecurity Agenda (in Dutch)
- National Cyber Security Research Agenda III