Cyber security: where to start?

And what else is there to do?

CEG Information Security, an updated version for Alert Online 2019

September, 2019

INHOUDSOPGAVE

1 CYBER SECURITY: WHERE TO START? AND WHAT ELSE IS THERE TO DO?

Within the CIO Platform Nederland, various knowledge sessions are organized throughout the year for and by the Information Security Officers of our member organizations. At these sessions we repeatedly discuss each other's best practices. For example, there has been a lot of discussion about the 10% of IT investments to be dedicated to cyber security, that was mentioned in Herna Verhagen's report[1]. The discussion was mainly about how to determine what to do in the area of (cyber) security and what costs are acceptable. In addition, the implementation of the General Data Protection Regulation (GDPR) on May 25th, 2018, has also provided the necessary activity.

The CIO Platform Nederland decided to summarize and share our learnings around safety measures as a contribution to, or inspiration for, organizations that have less capacity to think about security, but do want to get started with it. For this publication we've used the Cyber Security Framework of the American National Institute of Standards and Technology (NIST Framework) as an instrument to become more resilient in five steps. These steps are as follows: Identify, Protect, Detect, Respond and Restore. In the following article you can read the recommended measures, which we've placed in the context of the NIST Framework for clarity where possible.

Definition Cybersecurity:

"Cyber security is the freedom from danger or damage caused by disruption or failure of ICT or by misuse of ICT. The risk or damage caused by abuse, disruption or loss can consist of limiting the availability and reliability of the ICT, breach of the confidentiality of the information stored by the ICT or damage to the integrity of that information."

1.1 Where to start?

Keeping an organization, its data and systems, secure is a continuous process. It starts - as the NIST Framework suggests - in **identifying** the systems, data and other valuable assets that the organization needs to achieve its objectives. Subsequently the possible risks to the availability, integrity and confidentiality of those assets are determined. In the risk impact assessment, the organization places the

[1] H. Verhagen, 'Keeping "dry feet" in the digital era: The economic and social need for more cyber security' The Hague, October 2016. English summary: https://www.cybersecurityraad.nl/binaries/Keeping_dry_feet_in_the_digital_era_summary_tcm107-318154.pdf

identified risks in a context; how serious is it when a certain risk occurs? By defining the probability and impact of each identified risk, measures can be devised and proposed to manage this risk.

This makes it possible to make a rational assessment between the risk, impact and costs of the measures. This consideration is always the responsibility of the owner of the system for which the risk applies. If a plan is made based on this assessment to secure the organization, it's data and systems, you then have to implement the plan, check if the implementation was carried out correctly and has the required effects and then adjust the plan where necessary when during the operational phase issues arise and are dealt with (PLAN-DO-CHECK-ACT cycle).

1.2 How to keep data safe?

In other words, the 'protect' part of the NIST Framework. Below are some practical details of the protective measures that can, and sometimes must, be taken.

1.2.1 Access management

Access management has an important role to play in keeping data and information systems safe and is therefore specifically mentioned in the GDPR. Access management starts by determining who needs access to which data and systems, and then setting up access controls so that only the people who have the rights can access those systems and data. This limits the chance of activities, accidental or deliberate, with far-reaching unpleasant consequences for the organization. An up-to-date HR process, with clear in-, through- and outflow of employees, is crucial to keep the rights up-to-date with the right employee groups (role-based). This ensures that people can get to work quickly using their rights and prevents people who have a new role with other rights, or who leave the employment, from having access to data and systems with their previous rights. If this is combined with a password policy that enforces strong passwords and logging access, your access management is well on its way. In combination with virus scanners, intrusion detection and data leakage prevention, you keep your data and systems optimally secured.

1.2.2 System management

In addition to having access to data and systems under control, it is important to keep an eye on the development of the system itself and to set up a process to deal with security incidents. As for the first mentioned aspect, the development of the system, it makes sense to set up a Configuration Management Database (CMDB). This helps you keep track of how the system is set up and which settings are required to make it function properly. Changes in the system and experience with incidents that occur offer input for the risk assessment and may lead to adjustments of the measures to be taken.

1.2.3 Encryption of data

Because it can never be entirely ruled out that an unauthorized third party can gain access to a system, or can intercept data during transport between systems, it is necessary to provide data storage and data streams with encryption. This is also required for personal data in the GDPR. Encryption of the data makes this data useless for the third party who gets access to it. Encryption makes the loss of data less problematic for your earning capacity, as no one can use it to compete with you, and it can mean that a data breach does not have to be reported to the regulator.

1.2.4 Monitoring is important

In addition to all the preventive and protective measures you encounter, you should also make sure that you keep a close eye on what is happening with your data and systems. You should be able to check whether the persons and systems are used correctly by authorized persons. According to the NIST Framework, we are talking about '**detecting**'. This makes it easier to respond quickly and effectively when something goes wrong, in the '**response**' and '**recovery**' phases of the NIST Framework.

1.2.5 Incident response process

In the event of an incident, a **response** must be made. An incident **response** process must be in place, with clear tasks, procedures and escalation lines. The responsibility for carrying out these activities lies increasingly with a Security Operation Center (SOC). Several of our members have set up a SOC, where incident related data is analyzed to obtain a threat assessment with associated mitigation measures. If there is no (financial) room for an internal SOC, think at least of a Cyber Security Incident Response Team (CSIRT). This team acts as the Emergency Response officer in your organization in case of calamities in the field of information security.

1.3 Recovery after an incident

If there is a failure of systems, or loss of data, then it is important to get the operational processes up and running again as quickly as possible. A flawless backup and restore process, is indispensable. Do not just prepare this process on paper, but also test it regularly in practice. Also think about (internal and external) reports and communication on such incidents: who needs to be informed?

> **Most mentioned measures for each NIST category :**
> 1. **Identify: Have an external scan performed**
> 2. **Protect: Patch management plans**
> 3. **Detect: Install a CSIRT / SOC organization**
> 4. **Responses: Setting up the Security Incident Management process**
> 5. **Restore: Backup & Restore in order**

1.4 Safety in production chains

External communication is relevant from the perspective that organizations almost always have relationships with other organizations (third parties). You can think of suppliers and customers in the production chain, but also of regulators. For cyber security you almost always depend on parties outside your own organization. So you have to take that into account in your security policy. You can’t control security alone! That certainly applies in the increasingly complex chains in which we operate.

A very specific measure in this respect are the processor agreements that are mentioned in GDPR. These are mandatory if others have access to personal data for which your organization is responsible under the GDPR. This document contains agreements with these partners on the way in which personal data is handled. It also states how action is taken at the moment that an incident occurs in which personal data are (possibly) lost or have become available to third parties. Every organization will have to conclude a (substantial) number of processor agreements. To this end, you will have to discuss the issue of cyber security with these parties, but also with probably several departments involved within your own

organization, and put down on paper that what has been agreed upon. In addition to clarity about what contract parties can expect from each other, this also creates the necessary awareness for working safely with the data of or about others.

In any case, it is valuable to include safety aspects in purchasing and contract negotiations and to include these in the agreement as a so-called "Security Annex". Consider, for example, how to deal with risk assessments, measures to be taken, reports to be delivered and proof of compliancy of the partners and other third parties.

1.5 Keeping software and systems up-to-date

And once the assessments have been carried out, the agreements signed, the measures implemented, the specialists in a SOC are alert to incidents and their resolution, still more is involved to stay secure ....

The rapid developments in software and hardware ensure that it is necessary to keep up to date. Your systems must be checked continuously. Both against newly discovered vulnerabilities, and after every change in infrastructure and systems. Solutions for discovered vulnerabilities (patches) must be implemented quickly, before the vulnerabilities are exploited and without disrupting the operation of your organization. Virus scanners must be constantly updated and settings of software and hardware adjusted regularly.

The execution of an external scan or penetration test (for example by a formal audit authority) is also recommended. These scans can check whether the systems are vulnerable from the inside and/or from the outside. Or whether changing laws and regulations have an impact on your system. Such tests usually yield concrete proposals for dealing with vulnerabilities and thereby making the system safe and compliant.

1.6 Everyone has a role and responsibility

Safety will always need your attention, you are never 'done'. Because both your systems and the environment in which they operate are constantly changing, so is the vulnerability of the organization. It is not only about ICT, tools and systems and it is not only the (Chief) Information Security Officers and the Chief Information Officers who carry responsibility is staying secure: *Everyone within the organization and beyond (in the chain) has a role.* Communication about this in all sorts of ways - focused on the target groups - is necessary. And do not just do this incidentally, but take care of dosed activities during the year. For example by awareness campaigns and training for all staff, Dashboard Security Controls for the Executive Board, playful actions, serious games, exercises or Security talks. Whatever you do, ensure that security and everyone's role continues to receive attention!

Last remark

From security theory and various inventory rounds to get input for this article, we've identified 100+ measures that can be used to provide companies with greater security with the help of ICT. We certainly do not want to be complete in this story. If you want to brainstorm about the measures within your organization, please contact us so that we can introduce you to one of the CISO's in the network of the CIO Platform Nederland.

The CIO Platform Nederland in short:

CIO Platform Nederland is the association of large users of digital technology in the Netherlands. We are there for the CIO/CDO, his/her 'peers' and employees. We offer an easily accessible network, where the CIO/CDO can go to share ambitions, challenges, questions and concerns. We facilitate active collaboration and sharing practical knowledge at every level in the organization. All this on a confidential and upright platform.

Check out our website for more information: www.cio-platform.nl.

About this publication

Text & editing
CEG Information Security, CIO platform Nederland

Foto Cover
iStock

• info@cio-platform.nl
• www.cio-platform.nl