Cyberespionage
Are you aware of the risks?

A publication by the AIVD and MIVD

Are you aware of the risks of cyberespionage?

The information and communication systems of Dutch businesses and institutions are under assault from cyberspies, on a large scale. Attacks are launched by, or on the orders of, other countries. That is the finding of investigations by the national intelligence services, the AIVD and MIVD.

Two-thirds of the organisations affected do not even know they are victims. In some cases, intruders have been accessing their systems undetected for years.
Relatively few organisations realise that they are potential targets, making many fail to protect themselves adequately.

This brochure is about attacks on the Dutch government and business community by foreign cyberspies. Their aim is to obtain confidential information. Not only do such operations damage companies' reputations and earning potential, in the long term they can undermine the military and geopolitical position of the Netherlands and its allies.

The first part of the brochure describes how cyberspies go about their work, and explains what basic countermeasures you can take to frustrate them. The second part is intended for your IT specialists and provides a number of recommendations to increase your organisation's resilience in the face of cyberattacks.

"Two-thirds of the organisations affected do not even know they are victims."

Cyberattacks – the risk is high

The so-called "digitalization" of our society has inevitably increased the risk of cyberattacks carried out on behalf of foreign governments. These are technically advanced and hard to trace. Many organisations are unaware that they have been targeted until third parties, often the intelligence services, alert them to the fact. Because of this, and also because of its wide geographical reach and the limited risk involved, cyberespionage has become an attractive activity. Its extent and diversity have grown massively in recent years. Around the world, thousands of public and private organisations come under attack each year.

"Around the world, thousands of public and private organisations come under attack each year."

Dutch businesses and government organisations are regular victims

Dutch businesses and government organisations are targeted on a regular basis. A number of ministries and vital industries have already been affected, including defence contractors and the high-tech, chemicals, energy, life sciences, health and water sectors.

The confidential governmental information obtained by cyberspies is used by foreign powers to exert undue influence over other countries. This can be done by exploiting sensitive material about political decision-making and strategies, political, economic and military planning and Dutch negotiating positions.

Valuable technical and scientific information enables foreign powers to reduce their dependence on know-how and products from other countries. And so improve their own economic competitiveness or geopolitical power – by accelerating the modernisation of their armed forces, for example.

Cyberattack sows damage and distress in German parliament

In 2015, espionage software was discovered on the computer network of the Bundestag, the German federal parliament. For weeks, members were left in a state of uncertainty. What data had been stolen? What communications had been tapped, and by whom? Apart from the political upheaval caused, the renewed debates about the internet as a vital infrastructure and the implications of possible interference in the democratic process by foreign intelligence services, the material damage was also great. Because the attackers had managed to gain access to the entire network and could have installed hard-to-find "back doors" in its software and hardware, about 20,000 computers and their peripherals (printers, telephones, routers and the like) had to be replaced.[1] This was necessary to be absolutely sure that the intruders would be unable to regain access to the Bundestag's confidential information and communications in the future.

1 *Verfassungsschutzbericht (Annual Report on the Protection of the Constitution), 2015.*

Do not underestimate the consequences

Dutch organisations, commercial and public, are often unaware of the scale, duration, impact and consequences of cyberattacks. Too many regard the costs of recovery as an acceptable business risk, assuming that these are better affordable than investing in structural preventive measures.

However, this attitude overlooks the potential financial and other consequences in the long term: a tarnished image, loss of market share and a weakened competitive position.
The number of cyberattacks observed by the Dutch intelligence services and the extent of the damage they cause, economic and non-economic, prove that this form of espionage poses a genuine threat to our nation's businesses and government.

Loss of intellectual property and investments

Research has shown that the cost of overcoming a typical cyberattack can range anywhere between 200,000[2] and 4 million US dollars.[3]

These amounts are higher than the average IT security budget of many companies. Of course, the actual costs vary per attack and per organisation.

For many firms, the loss of intellectual property and investments in research and development are even more damaging than the direct financial toll of recovering from a cyberattack. The fact is that the average cost of an attack rises every year.

2 *"Examining the costs and causes of cyber incidents", Journal of Cybersecurity, 25 August 2016.*
3 *2016 Cost of Data Breach Study; Global Analysis, Ponemon Institute, June 2016.*

In what way are you attacked?

Investigations by the Dutch intelligence services show that cyberattacks by state actors are often successful because businesses and government agencies simply do not know how to protect their IT networks against them. Implementing proper safeguards and good security awareness are therefore vital first steps in building cybersecurity.

To take adequate countermeasures, it is important to understand how cyberspies work and what methods – technical and otherwise – they use. With this knowledge you can make it far harder for them. Even a few basic security precautions will increase your resilience in the face of their attacks.

In general terms, cyberattacks are divided into three phases.

1. Gain access.
2. Maintain access.
3. Steal or sabotage.

Throughout an attack, the cyberspies repeat these three phases again and again in order to extend or restore their access to your systems. They are constantly exchanging data with the target network, to steal data and install malware (malicious software). This process often requires access over a long period, so the intruders make every effort not be discovered.

Phase 1

Gain access

Cyberattacks are not random exercises. Foreign intelligence services draw up "shopping lists" of targets, depending on what information the state in question is interested in and what it wants to do with it. Its cyberspies then investigate how they might gain access to the organisations on the list. This could be through its employees, its suppliers or its poorly protected systems.

The internet and social media have made it easier than ever to identify and exploit vulnerabilities. As well as conducting so-called "port scans",[4] attackers use Google and social media to gather as much information as they can about their target. Most organisations are penetrated with the unwitting help of an employee, through "spearphishing": he or she is persuaded by a personal e-mail to open an attachment or a web link infected with malware. This and "social engineering" are the most common methods used because they are so successful, but the intelligence services are also witnessing more and more advanced attacks targeting hardware, for example.

4 Remote probes to see if any of a computer's ports are accessible by intruders.

Phase 2

Maintain access

Once inside a network, attackers install a so-called backdoor – another access point – to ensure that they maintain permanent access. As part of this process, they often attempt to extend their penetration of the network by mapping all its systems. And they look for additional user names and passwords which give them access to different systems and network segments.

In many cases, extra backdoors are installed to maintain the continuity of the attack. Intruders are careful in their approach, trying to fit in with the regular activity on the network so as to avoid detection.

Usually, cyberspies install malware on your systems. This allows them to trawl the network, automatically or manually, for the information they want. And for more user names and passwords, so that they enhance their rights and so gain access to even more data. The ultimate prize is the highest level of rights, such as those held by the system administrator. These provide full access to every part of the network and all data on it.

Having mapped the network, the attackers infect other linked computers, servers and devices such as printers, and sometimes even telephones, cameras and doors. The "backdoors" ensure that they do not have to keep relying on their original means of penetration, enabling them to maintain access even after security updates or the closedown of systems known to be infected. The use of proxies (intermediate servers) and encryption makes it harder to identify their origin and the nature of their activities.

Phase 3

Theft or sabotage

Once they have secured permanent access, the cyberspies are ready to instigate the actual attack. They are now in a position to collect data and to operate infected systems remotely. They can also lie dormant in a system, waiting to act on a later date.

In this phase, the intruders look for relevant information. Once they have found it, they copy it to temporary files. These are then sent to their own systems, often encrypted and

disguised as regular network traffic so as to keep their activities and intentions undetected. In many cases the stolen information is routed through a number of intermediate points in different countries – servers, proxies or satellites – to conceal the identities of those responsible. The temporary files and other traces are now deleted, so that many victims have no idea that their data has been compromised.

PlugX is a good example of cyberespionage malware. Since 2012, several different variants have been identified as responsible for attacks on defence contractors, other companies and government agencies. The program combines a number of the functions needed for phases 2 and 3 of an attack.[5] It could be described as the "Swiss army knife" of malware, because it incorporates multiple components which can be activated remotely as and when they are needed. Individually, these are difficult for virus scanners to detect.

What can you do?

Fighting cyberespionage is an unequal battle. The price of good protection is high, compared with the cost of mounting an attack. An intruder only has to find one weak point in your network, after all, whereas you have to find and secure them all. Nonetheless, it is quite easy to make things much harder for cyberspies. In just four steps, you can significantly enhance the basic security of your IT infrastructure.

1. Identify your crown jewels.
2. Establish your threat scenarios.
3. Take measures.
4. Check your IT systems regularly

Step 1 Identify your crown jewels

First establish what the digital "crown jewels" in your network are, and where they are. These could be confidential or sensitive information, or perhaps systems holding personal data. You know better than anyone where the value of your organisation lies and what data and processes create that value.[6]

5 *PlugX – The Next Generation, Sophos, June 2014.*
6 *As an aid in doing this you could, for example, use the Handleiding Kwetsbaarheidsonderzoek Spionage' (Guide to Espionage Vulnerab lity Reviews, available in Dutch only) at www.aivd.nl/onderwerpen/cyberdreiging/documenten/publicaties/2011/02/17/handleiding-kwetsbaarheidsonderzoek-spionage.*

It is also important that you collect current threat information, as issued by the government, commercial providers and industry sources (ISAC information sharing and analysis centres). This is essential in building a clear picture of relevant threats and appropriate security responses.

Step 2 Establish your threat scenarios

Once you have charted your crown jewels, devise a number of realistic threat scenarios. What is the easiest way for cyberspies to gain access to this confidential material? Every threat scenario in every organisation is unique, and technical know-how is essential. So involve your IT department in the process. Industry partners, the government and commercial provider can provide support, too.

Step 3 Take measures

Once you have established the most likely threat scenarios, you can take effective countermeasures. These can be divided into three categories.

1. Preventive measures
   These reduce the chances of an attack on your systems succeeding.
2. Detective measures
   These reduce the chances that an attack will go undetected, enabling you to respond.
3. Mitigating measures
   These limit the effectiveness of malware and reduce the risk of damage in the event of a successful attack.

The second part of this brochure explains in greater detail how your IT department can implement these countermeasures.

Step 4 Check your IT systems regularly

Cybersecurity is a continuous process. The countermeasures described in step 3 will substantially enhance the resilience of your network, but they cannot provide total protection against determined, patient and well-equipped cyberspies. It is important that you always remain one step ahead of the attackers by checking your IT systems on a regular basis. For example, by launching a simulated attack based on one of the scenarios from step 2. These checks can help you to refine your processes and response in the event of a real attack. And they might also reveal one which is already under way.

IT countermeasures

This part of the brochure provides specific instructions for your IT department or provider to help them improve system security. The precautions described in the table below are listed in order of importance, as determined by the Dutch intelligence services.

The items listed are not specific countermeasures against cyberespionage, but rather standard precautions to enhance the security of IT systems. Nonetheless, they will improve your resilience to cyberattacks instigated by state actors and so it is important that they be implemented.

IT countermeasures

	Ref.	Precaution	Overall effectiveness	Impact on work rocesses	Initial costs	Ongoing costs
Essential precautions						
1	3.1	Compartmentalise and segment networks and systems.	Very high	Low	High	Low
2	1.1	Strengthen basic security of servers and workstations.	Very high	Low	Average	Average
3	1.5	Introduce “whitelisting” of trusted applications.	Very high	Low	High	Average
4	1.4	Apply end-to-end encryption on public infrastructure.	Very high	Low	Average	Average
Important precautions						
5	3.2	Minimise use of enhanced rights.	High	Average	Average	Average
6	2.1	Apply intrusion detection and prevention to known indicators of compromise (IoCs).	High	Low	High	Average
7	1.2	Scan incoming e-mail for security risks.	High	Average	Average	Low
8	3.3	Enforce use of strong authentication.	High	High	High	Average
9	1.3	Improve users’ security awareness.	High	Average	Low	Low
10	2.2	Conduct security tests regularly (penetration tests, vulnerability scans, red teaming and so on).	High	Low	Average	Average
11	2.3	Check websites visited by staff for malware.	High	Low	Average	Low
12	2.4	Use anomaly detection in the “crown jewels” compartment.	High	Low	High	Low
13	2.5	Use “honeypots” and “honeytokens”.	Average	Low	Average	Low

On the next few pages are more details of the preventive and detective precautions your IT department or provider can take to counter cyberattacks more effectively. The reference numbers in the table above refer to the section numbers of these specific descriptions.

1. 1. Prevention

The following preventive measures will increase your resilience against cyberespionage.

1.1 Strengthen basic security of servers, workstations, and network equipment

A lot of cyberattacks exploit vulnerabilities in the basic security protection of servers, workstations and network equipment. For example, the so-called EXTRABACON exploit requires read access to SNMP and network access to administrator services like Telnet or SSH.[7] Consequently, attacks of this kind can often be fended off by restricting this access to trusted systems. This is a basic security precaution. So too are the following counter-measures, which can also be highly effective.

a. *Patch software promptly and automatically*

Malware often exploits software vulnerabilities to infect systems. There are three possible scenarios in this respect.

1. The vulnerability is a known and a patch rectifying it is available, preferably from the original manufacturer of the software.
2. The vulnerability is a known but no patch is yet available. In this case, consider temporarily removing or disabling the software until a patch is released.
3. The vulnerability is not yet known (a zero-day).

The majority of attacks exploit known vulnerabilities and so are relatively easy to prevent. Applying software patches should be given a high priority as an integral part of system management. To ensure that all necessary patches are used, a good overview of all the software on all your systems is essential.

b. *Harden browsers and applications*

Make your browsers as robust as possible. This reduces the risk of infection when staff visit compromised pages. Always apply the latest patches to browsers and make sure that plug-ins known to be susceptible to attacks, such as Flash, Java, Javascript and Silverlight, are deactivated. Additional plug-ins are available for some browsers to reduce their attack surface. Also switch off the option to use Office macros, as these are often used to transmit malware.

7 *https://blogs.cisco.com/security/shadow-brokers*

c. *Use the security features supplied with your operating system*

Most operating systems are delivered complete with a firewall and memory-protection features such as EMET or ASLR. Make use of these integrated functions.

d. *Switch off unused functions*

If a server or workstation does not need certain services or applications, such as remote access or data supplied with the operating system, either deactivate them altogether or configure them as restrictively as possible.

e. *Keep your virus scanner up to date*

Virus scanners do not prevent all cyberattacks, but they help. Studies show a success rate of about 70 per cent, but to maintain that level of protection the scanner has to be kept up to date with the latest virus definitions. And this applies on all devices connected to the network. The real benefit of these scanners is that they stop most common, undirected malware infections, leaving you to focus the bulk of your specific detection and monitoring activities on threats being directed specifically at you.
To ensure that incoming malware can be analysed, it is important that the scanner place it in quarantine rather than destroying it.

f. *Use encrypted data storage and transmission.*

Cyberespionage is all about gathering information. To limit the amount of readable material an attacker can gain access to and steal, whenever possible encrypt your important data at rest and in transit.

g. *Minimise the use of removable media*

Institute as restrictive a policy as possible for the use of removable media, to prevent them acting as a conduit for malware infection or loss of data. For example, you can significantly reduce your exposure to attack by making it impossible to read from or write to USB media. If this is not feasible in your situation, then at least ensure that only registered USB media, issued by and under the control of your organisation, can be used.

Deactivate the autorun function on such media, too. And scan it regularly and automatically for indicators of known malware.

1.2 Scan e-mail on a mail proxy server

Because many cyberattacks begin with phishing, it is essential that you scan all incoming e-mail – and attachments – for malware and suspicious URLs before it reaches the recipient's mailbox. Cyberspies try to make their e-mails look as convincing as possible. For example, they use the real names of workmates, managers or business contacts to tempt you into clicking on a link or opening an attachment. A spam filter offers no protection against phishing.

Make sure that executable file types (.exe, .msi and the like) can never find their way into an employee's inbox as an attachment. The true origins of e-mails can be checked using techniques like DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF). If suspicious characteristics are found, it is important that the complete e-mail and its attachments be quarantined for further investigation.

1.3 Improve users' security awareness

A successful cyberattack often begins with an unwitting action, such as opening an infected e-mail attachment or web page. As well as implementing technical countermeasures, your staff need to know how to recognise various forms of attack. Cyberspies could target anyone in their efforts to penetrate your network, not just key accounts. So include such attempts in your own specific threat scenarios.

a. *Verify unexpected e-mail, even from known senders*

If they receive unexpected, unsolicited or unusual e-mail which seems to be from a known sender, it is advisable that your staff call or e-mail that person to verify its authenticity before opening any attachments or links.

b. *Set up a central reporting point for suspicious activity*

It is important that your staff have a central point of contact they trust to report suspicious incoming e-mails or messages, and to put any questions they may have. Even false alarms help to raise security awareness within the organisation, as long as they are taken seriously and dealt with respectfully.

c. *Be cautious about sharing contact details on social media*

It can be incredibly easy to find the names, job descriptions and contact details of an organisation's personnel online. And all can be exploited to mount spearphishing

attacks. Staff should be taught to be more reticent about sharing exact details of their work, such as specific projects they are involved in, and to be alert when making new contacts on social media like Facebook and LinkedIn.

d. *Protect details of your IT components and configuration*

Any information a cyberattacker can glean in advance about your IT systems (for example, your network DMZs, proxy use, data-storage location and type, mail server location or internal DNS servers) makes it easier to probe and penetrate your network.

1.4 Apply encryption on public infrastructure.

By definition, transmitting sensitive information over public infrastructure without taking proper precautions is insecure. As the owner of the material, you cannot check what route it takes or who has access to it. It is therefore vital that confidential communications be adequately secured, preferably using end-to-end encryption.

For example, the online link between two trusted networks can be encrypted by means of a virtual private network solution like OpenVPN-NL. For traffic to your web and e-mail servers, SSL is an option. Alternatively, encrypt the information itself using a communication product such as PGP, LUNA or VeraCrypt.

1.5 Introduce "whitelisting" of trusted applications.

With application whitelisting, only explicitly trusted software can be run on a system. Any programs the organisation has not specifically added to its "whitelist" will be rejected, thus reducing the risk that malware can be installed or executed. In addition, application isolation can be implemented to keep a program's access to data to the absolute minimum necessary.

Whilst these measures are highly effective from the security point of view, however, one disadvantage is that they require very good system planning and precise configuration. But when combined with segmentation, despite the initial administrative burden this may well be a very worthwhile way to protect the network segment holding your crown jewels.

2 Detection

The following precautions will improve your chances of detecting an attack, so that countermeasures can be taken as quickly as possible.[8] But how effective they are very much depends on how good your incident response is. If you detect something and then do nothing about it, any precautions will be totally ineffective.

2.1 Apply intrusion detection and prevention to known indicators of compromise

The term "intrusion detection and prevention" covers a wide range of measures designed to recognise a cyberattack, successful or otherwise, on your infrastructure. These are based on known "indicators of compromise" (IoCs) – tell-tale signs of an attack in network traffic or on a computer system. A well-designed intrusion-detection process produces a substantial amount of information that needs to be analysed. In broad terms, intrusion detection and prevention can be divided into the following subprocesses.

a. *Actively scan systems for suspicious activity*

Apply so-called "host-based intrusion detection" (HIDS), scanning computer systems actively, comprehensively (both servers and workstations) and regularly in search of suspicious activity. That might include the activation of suspect processes, the running of unauthorised file types and the initiation of unusual network traffic, such as establishing a VPN connection to an external address. Also, check regularly that all accounts on the system are and need to be operational; this eliminates the presence of "ghost" accounts, belonging to former employees or created illegally.

b. *Scan both incoming and outgoing network traffic for suspicious activity*

Apply so-called "network-based intrusion detection" (HIDS), scanning incoming and outgoing traffic actively and regularly in search of suspicious activity. A number of programs for the real-time monitoring and filtering of this traffic is available on the open market. Always use a next-generation firewall (NGFW) with stateful inspection or deep-packet inspection (DPI). For user internet traffic, a proxy may be used. Ideally, the NGFW or proxy will support encrypted connections by means of, for example, SSL offloading.

8 *See also the publications Handreiking voor implementatie van detectie-oplossingen (Guide to the Implementation of Detection Solutions, ava lable in Dutch only) and How to Recognise Attacks from Advanced Persistent Threats.*

c. *Log relevant network connectivity – and check the logs*

Good logging of all connectivity – with the help of NetFlow or Bro, for instance – is important in order to keep a close eye on what is happening on your network, as well as for the investigation of past events. To monitor activity and connectivity effectively, establish proxies between your internal network and external ones. And check the resulting logs regularly, either manually or automatically. Abnormalities in, say, traffic volumes, connectivity times or specific DNS queries can then be reported immediately.

d. *Block network traffic with known C2 domains*

In the wake of malware infection, the affected system will often try to make contact with a command-and-control (C2) server operated by the attackers. Actively filter your network traffic for these efforts by scanning for the indicators described in reports about cyberattacks. Your traffic logs will then reveal attempts to contact malicious domains, enabling you to initiate an immediate follow-up investigation. An NGFW or proxy can be used to block traffic in this way.

e. *Analyse the information generated by your intrusion detection and prevention process*

Bring together all the information generated to detect suspicious activity on your internal infrastructure. An intrusion detection and prevention process usually produces too much data for manual investigation and analysis, and in any case interpreting it is a specialist task. Your HIDS and NIDS systems should therefore report to an automated security incident and event management (SIEM) system, which makes the high volumes of data generated easier to search, correlations easier to identify and statistics easier to produce. Employ qualified staff capable of interpreting the output.

2.2 Conduct regular security tests

An IT infrastructure changes all the time. New systems are connected, old ones are updated and configurations are modified. Every one of these changes affects the security situation.

For this reason, it is important to conduct regular security tests. With, of course, a particular focus on your crown jewels. Use the threat scenarios compiled for your organisation to help carry out the tests. When undertaking simulated cyberattacks, focus not just on detection but on the whole security picture: prevention, impact limitation, detection and response.

In general terms, there are three important types of security tests.

a. *Vulnerability scans*

A vulnerability scan or vulnerability audit tests all or part of a network for security weak points, such as obsolete versions of services and deficiencies in the configuration of components or systems. It generates an overview of these vulnerabilities.

b. *Penetration tests*

This is an audit which exploits detected vulnerabilities to actually attempt to gain access to a system. In other words, it realistically simulates an attack scenario.

c. *Red teaming*

The most realistic security test of all is the red-teaming attack. Whereas vulnerability scans and penetration tests are limited in scope and conducted with the knowledge of the system administrator, in this case no-one is told when the simulated intrusion will take place or what form it will take. The idea is to keep it as clandestine as possible.

2.3 Scan websites visited by staff

Log the websites visited by staff and scan them for malware. A good tool for doing this is Honeyspider; it allows you to check all sites visited, or a selection, automatically and regularly. Commercial products making use of the same "sandboxing" technologies are also available.

2.4 Use anomaly detection in the crown jewels compartment

All the intrusion-detection methods we have described so far are based on known indicators of cyberattacks. By contrast, anomaly detection aims to identify as-yet unknown indicators by analysing deviations from the "normal" situation. However, it is only really effective when applied to small, compartmentalised network segments where that normal situation is constant and relatively easy to map. With good compartmentalisation, the segment containing your crown jewels will probably satisfy these criteria. So anomaly detection there may be able to identify attacks with previously unknown indicators.

2.5 Use "honeypots" and "honeytokens"

A "honeytoken" or "low-interaction honeypot" (LIH) is a passive feature in a system or database, included specifically to enable the detection of attacks on it. Unlike active honeypots, which are often created for the purpose of analysing intrusions, a honeytoken is more like a tripwire: if someone does stumble over it, you are notified immediately. A series

of carefully chosen and positioned honeytokens can make it very difficult for an attacker to not stumble over at least one of them.

There are many different kinds of honeytoken and LIH, and various ways of monitoring them. Your specific situation and your reasons for deploying this tactic will determine which, if any, you choose. Common types include a characteristic of production data and deliberately created "fake" data. Or fictitious data-entry fields, websites, network shares, network services and so on.

To check that honeytokens are actually being used, relatively simple IoCs can be generated and registered in, say, an IDS or SIEM.

3.1 Compartmentalise systems and segment networks

A lot of IT networks are configured like a meadow, with a sturdy fence around the outside edges but a wide open field inside. This kind of structure is almost impossible to defend: once a cyberspy has gained access, they can roam unfettered around your network and any others linked to it. To prevent this, networks should be segmented and systems compartmentalised. Segmentation means dividing your network into separate parts, and in particular confining access to your crown jewels to those people, applications and computers with a genuine need to read or retrieve them. Such restrictions should apply especially to important core systems like domain controllers and the active-directory environment.

Your security investments can then be concentrated on your most sensitive segments, leaving your less confidential processes and data in a less heavily protected environment. Segmentation is relatively easy to achieve with the aid of virtual local area networks (VLANs) and firewalls. In the most confidential segments, you are strongly advised to disable internet access.

In a network, there is often no need for workstations to communicate directly with one another. As a rule, they can be linked through one or more servers. In such cases, you should make direct connection impossible. This is compartmentalisation. Similarly, when there is no need to connect with an external network, that possibility should also be disabled.

3.2 Minimise use of enhanced rights

Among the crown jewels of your organisation are its network administrators. So protect them. Limit the number of admin accounts and shield their identities. Grant regular users the minimum possible rights, so that compromised accounts cannot be used by a cyberattacker to explore your system or network. Be reticent about issuing accounts with admin rights, and supervise them carefully. Users with system admin rights on a workstation do not necessarily need the same level of access to the network, and vice versa. Delete accounts as soon as they become redundant. And use different accounts and passwords for the administration of different compartments, especially those containing your crown jewels.

3.3 Enforce use of strong authentication

Cyberattackers go in search of credentials, such as passwords and keys, with which they can increase their rights on or access to your systems. If they manage to obtain "hashes" of passwords, for example, they will try to work out the actual passwords these are encrypting.

a. Use strong passwords and encryption

To stand up to the threat posed by automatic cracking tools, passwords need to be robust. So check actively and regularly that all passwords within your organisation are strong enough. For example, by running their hashes through a password-recovery tool. In particular, do this whenever a user configures a new password. Use only strong encryption algorithms, such as AES256.

b. Do not store cryptographic keys on the user system

If this is unavoidable, protect the keys with a very strong password. Preferably in combination with a second form of authentication.

c. Allow only strong forms of external access to your network

Once an intruder has compromised a system, they are very likely to go in search of user credentials in order to gain external access to your organisation's network. To counter this threat, you are advised to allow such access only through VPN tunnels with mandatory two-factor authentication.

d. Protect your Wi-Fi network

Equip the wireless connections within your network with a strong form of authentication as well, preferably one based on digital certificates.

Talk to your IT supplier

More and more organisations are outsourcing their IT and communications to third-party suppliers of hardware, software and support services. If you have done this, talk to your supplier about cybersecurity. Has it implemented all the above measures on your behalf? For example, can it provide you with the relevant logs if you need to investigate a possible cyberattack on your organisation? From our experience, that is not always the case – sometimes, for instance, suppliers do not differentiate their logs between individual clients. This makes it difficult to study the nature and extent of an attack.

Have you been the subject of an incident which might involve a state actor?

Where possible, the Dutch intelligence services share the results of investigations into cyberattacks by state actors with relevant third parties. For example, we may disclose technical details of an attack to chain partners or, bilaterally, to the victims. In so doing, we always protect the confidentiality of your information as well as that of our sources and methods. We also advise government departments and agencies on the protection of their sensitive information. In all of these activities, our primary aim is to help other organisations to improve their resilience against cyberattacks.

If you believe you have been the subject of an incident which might involve a state actor, you should report it to the intelligence services. Please contact the **General Intelligence and Security Service** (AIVD) on +31 79 320 5050 or, if the incident is related to the defence industry or military interests, e-mail the **Industry Security Bureau** (BIV) at indussec@mindef.nl.
For the Dutch national government and vital infrastructures, the National Cyber Security Centre (ncsc.nl) serves as the information hub and centre of expertise on cybersecurity.
Note that once the Data Processing and Cybersecurity Notification Act (Wet gegevensverwerking en meldplicht cybersecurity) enters force in mid-2017, it will become compulsory for government bodies and the operators of vital infrastructure to notify the NCSC of all cyberincidents of a disruptive nature. Moreover, the NCSC advises that such incidents always be reported to police.

There has been a similar notification requirement for data leaks since 1 January 2016. Specifically, any public or private organisation subject to an incident in which personal data has or may have been compromised must report it to the **Dutch Data Protection Authority** (Autoriteit Persoonsgegevens). This can be done through the special online notification function at autoriteitpersoonsgevens.nl.

Colofon

This brochure is published by:

Ministry of the Interior and Kingdom Relations of the Netherlands
General Intelligence and Security Service (AIVD)
aivd.nl

Ministry of Defence of the Netherlands
Military Intelligence and Security Service (MIVD)
defensie.nl/mivd.nl

Oktober 2017