Cybercheck: Beware of supply chain risks!

A guide for mapping and controlling supply chain risks for products and services from countries with an offensive cyber programme

Target audience

This guide is intended for public and private organisations that have Protectable Interests (*Te Beschermen Belangen*, TBB) with regard to National Security. Organisations can determine for themselves whether they have one or more Protectable Interests with regard to National Security (hereinafter abbreviated to PI-NS, the acronym is 'TBB-NV' in Dutch) by using existing frameworks.[1]

This guide was compiled for individuals working at the tactical level who have a role in controlling digital risks with regard to the deployment of products and services from countries with an offensive cyber programme.[2] These roles are primarily Chief Information Officers (CIOs), Chief Technology Officers (CTOs), and Chief Information Security Officers (CISOs). This guide can also be used by procurement departments, cybersecurity specialists, and ICT and security architects.

The following organisations contributed to this guide:

Bluebird & Hawk BV, the Dutch Banking Association, ICT Group, NS Nederlandse Spoorwegen, and Technolution

---

[1] Protectable Interests are also known as 'Digital Crown Jewels'. For more information, please refer to the *National Risk Assessment of the Kingdom of the Netherlands 2022* (*Rijksbrede Risicoanalyse Nationale Veiligheid 2022*), *Risk Assessment Guideline* (*Leidraad Risicobeoordeling*), or *Digital Crown Jewels: Data, Document and Registries of National Interest* (*Digitale Kroonjuwelen: gegevens, documenten en registraties van Nationaal Belang*) to determine whether your organisation has Protectable Interests with regard to National Security. Rijksbrede Risicoanalyse Nationale Veiligheid 2022 | Rapport | Rijksoverheid.nl, https://www.rivm.nl/nationale-veiligheid or Digitale Kroonjuwelen: Gegevens, documenten en registraties van Nationaal Belang | Rapport | Rijksoverheid.nl.

[2] The AIVD and MIVD have classified China, Russia, Iran and other countries as nations with an offensive cyber programme. AIVD Annual Report 2022 | Annual Report | AIVD, page 29.

Content

Introduction

The increasing digitalisation of Dutch society has many benefits but also comes with risks. One of these risks has been drawing increasing attention in recent years and involves the deployment of products and services[1] from countries with an offensive cyber programme that targets the Netherlands or its interests.

Countries with an offensive cyber programme may affect the supply chain during the development and maintenance of products and services.[2] These countries may coerce companies and citizens in their territory to cooperate on the basis of legal requirements, forcing them to build digital backdoors into their product or service.[3]

This strategy offers countries with an offensive cyber programme the opportunity to gain unauthorised access, via such products and services, to parts of the technical infrastructure of a target organisation. Such access can then be exploited for espionage and/or sabotage purposes.

Today, products and services are imported into the Netherlands from all over the world. If deployment of such products and services leads to an incident within organisations that support vital processes, it has an impact not only on the organisation itself but potentially on the Netherlands' national security as well. Therefore, mapping and controlling supply chain risks is essential for the digital functioning of both the organisation and of Dutch society.

Getting started: Gain insight into supply chain risks for products and services from countries with an offensive cyber programme

The Dutch General Intelligence and Security Service (AIVD), Chief Information Office-Rijk (CIO-Rijk), National Cyber Security Centre (NCSC), and National Coordinator for Security and Counterterrorism (NCTV) have released this joint publication to raise awareness of supply chain risks deriving from the deployment of products and services from countries with an offensive cyber programme.

[1] In this guide, a product is understood to mean the entire combination of digital components. A smartphone consists of physical hardware but also firmware, a specific type of Operating System (OS) and software in the form of applications, for instance. A service provides for a specific defined need of the organisation, and any service may make use of multiple products.

[2] The supply chain covers all suppliers of components, (partial) products and services that are part of the supply chain for product or service development and maintenance.

[3] AIVD publication *Offensive Cyber Programme, a perfect business model for states* (in Dutch) | Publication | AIVD.

This guide offers some concrete starting points for:

- Mapping potential supply chain risks with the aid of the Cybercheck[4]
- Conducting an additional risk assessment to manage and control potential supply chain risks. This is clarified with the aid of a fictional example.[5]

The results of the additional risk assessment cover a specific supply chain scenario and supplements the broader, existing risk management process of your organisation. If your organisation does not have a risk management process, we recommend setting up this process first.[6]

Please note: this guide does not offer advice as to whether products and services should be deployed within your organisation or not. Your organisation's management bears final responsibility for the decision to deploy specific products and services from countries with an offensive cyber programme. The Cybercheck in this guide is intended as a tool and offers your organisation a structure for mapping potential risks relating to a specific supply chain scenario.

[4] This refers to the risks that may result from the use of products and services where vendors from countries with an offensive cyber programme play a part in the supply chain of these products and services.

[5] We recommend conducting a risk assessment on the basis of the component's 'threat', 'protectable interests', and 'resilience'. Cf. page 11.

[6] Assessing risks in an organisation-wide and interrelated manner allows you to decide on security choices that match the organisation's objectives and make a positive contribution to the desired resilience. For more information, please refer to the factsheet *Controlling Risks: The value of information as a starting point* Factsheet *Controlling Risks: The value of information as a starting point*. | Factsheet | National Cyber Security Centre (ncsc.nl) or NEN-ISO 31000:2018 – Risk Management Guidelines.

1 The Cybercheck

The Cybercheck is a tool to map whether deployment of a specific product or service from a country with an offensive cyber programme may result in a heightened security risk and as such is cause for conducting an additional risk assessment.
This chapter explains how and for what purpose you can use the Cybercheck in your organisation. It also provides a glossary of terms to answer the questions in the Cybercheck.

What value does the Cybercheck add for your organisation?

The questions in the Cybercheck have been formulated based on a number of technology layers, the so-called technology stack. In this guide, the layers are the software, the operating system (OS), the firmware, and the physical hardware. Countries with an offensive cyber programme can use the supply chain to exploit the products of services on one or more of these layers. By answering a number of questions for each of these layers, you can analyse whether the technology in any one layer can possibly be exploited.

What products and services should you select for the Cybercheck?

This guide is intended for organisations who have one or more Protectable Interests with regard to National Security. Your risk management process should have already helped you establish what interests are at stake or will allow you to do so within a short amount of time.

The Protectable Interests are the starting point for selecting specific products and services for the Cybercheck. Determine on what products and services these interests depend or what products and services are themselves a Protectable Interest. For instance, because they must always be available. We recommend prioritising products and services based on its importance for the functioning of the Protectable Interest.

The selected products and services are the starting point for the Cybercheck in this guide. An example is a business-critical service for processing sensitive information or operational technology that supports production processes, such as a Programmable Logic Controller (PLC) or Human Machine Interface (HMI) in an OT environment.

Who should perform the Cybercheck?

The Cybercheck is intended for persons in your organisation who play a part in controlling digital risks. The management is the owner of these risks (for example, the process owner). The management bears final responsibility and is accountable. The management generally receives support from the Chief Information Security Officer (CISO), who usually is responsible for the execution. The CISO may also call upon a trusted partner to map the risks. The trusted partner does not have to be an expert on the subject matter but must be knowledgeable about the primary process and which persons can supply the right information for answering the questions of the Cybercheck. This might involve internal interviews with subject matter experts or external suppliers of a specific product or service.

When to use the Cybercheck

The Cybercheck can be implemented for products and services that are already in use as well as for those under consideration for procurement.[7] We recommend using the Cybercheck well ahead of time whenever you consider buying new products or services. This allows you to make a procurement decision in a timely manner. It is important to gain and maintain a good understanding of the origin of such products and services in terms of parties in the supply chain. Changes due to takeovers or new ownership constructions may be reasons for your organisation to conduct another Cybercheck.[8]

Select products and/or services for the Cybercheck

To begin with, establish the scope of the products and services that should be assessed in the Cybercheck

Conduct the Cybercheck and answer the questions

If the Cybercheck results in a 'yes', do an additional risk assessment

For the Dutch central government the existing cabinet policy applies that risks with regard to, for instance, espionage, undue influence or sabotage by state actors relating to digital products or services are assessed on a case-by-case basis with the aid of the so-called C2000 criteria.[9] Central government organisations can use the Cybercheck as part of the assessment that the C2000 criteria requires them to do.

---

[7] We recommend consulting the 'Secure Procurement Toolbox 2024' in addition to the Cybercheck when initiating a procurement procedure. The NCTV, the Ministry of Economic Affairs and Climate, and the Ministry of the Interior and Kingdom Relations developed the Secure Procurement Toolbox to detect specific risks to national security in procurement and tendering processes: Secure Procurement Toolbox (2024) | Economic Security | National Coordinator for Counterterrorism and Security (nctv.nl).
Government bodies can use the ICO wizard to compile a set of information security requirements for procurement/tendering and contracting. Organisations outside the central government can use this tool for inspiration: ICO Wizard - bio-overheid.

[8] Acquisitions or new ownership constructions are not within this guide's scope but should be incorporated into the broader risk management process and considered to ensure the most comprehensive and well-justified decisions about the deployment of products and services from countries with an offensive cyber programme. For more information, please refer to Wet veiligheidstoets investeringen, fusies en overnames (35.880); Memorie van toelichting (TK, 3) - Eerste Kamer der Staten-Generaal (Act concerning security checks for investments, mergers and acquisitions (35.880); Explanatory Memorandum (TK, 3) - Senate of the Netherlands). If you have further questions concerning economic security, you can also check EV-loket (Economic Security Desk for Entrepreneurs): Ask a question | Ondernemersloket Economische Veiligheid

[9] The C2000 criteria are as follows:

1. Is the party supplying the service or product based in, or controlled by a party from, a country with legislation that requires commercial or private parties to collaborate with that country's government, in particular with state bodies that have an intelligence-gathering or military task, or is the party a state-owned enterprise?
2. Is the party supplying the service or product based in a country with an active offensive intelligence programme targeting the Netherlands and its interests, or a country with such a tense relationship with the Netherlands that actions affecting Dutch interests are conceivable?

A. Will the party supplying the service or product have extensive access to sensitive sites, sensitive ICT systems and vital infrastructure systems or works, with regard to which exploitation may represent risk to national security?

B. Is it possible to implement control measures providing adequate protection with regard to the national security risks at stake?

Getting started with the Cybercheck

We recommend proceeding with the Cybercheck in accordance with the following steps:

1. Select products and/or services for the Cybercheck[10]
2. To begin with, establish the scope of the products and services that should be assessed in the Cybercheck[11]
3. Conduct the Cybercheck and answer the questions[12]
4. If the Cybercheck results in a 'yes', do an additional risk assessment

Below is a glossary of terms used in the Cybercheck.

What is a product or service?

In this guide, a product is defined as the entirety of physical and digital components. For instance, a smartphone consists of physical hardware but also firmware, a specific type of Operating System (OS) and software in the form of applications. A service provides for a specific need of an organisation. A service often makes use of multiple products. Antivirus solutions or Identity and Access Management (IAM) solutions are examples of services.

A product in this guide is understood to mean not only a physical product with which users interact, but also the digital environment with which the product is connected. Security cameras are an example. A security camera consists of the physical security camera but can also be connected to a cloud environment to which it transfers the security footage. In this example, the cloud environment is therefore also a part of the product and must be included when answering the Cybercheck questions.

When investigating a service, you must determine what underlying products or services that service uses. These products and services are a part of the service and as such, they are relevant in answering the Cybercheck questions. Be aware that components may consist of several components and services may consist of multiple services for which products are used. It is up to the organisation itself to determine the scope and depth of the analysis of the supply chain.

Software

Software is the combination of programmes that enable computers or other devices to execute a task. Software can have many forms, such as the applications on your phone, office automation such as accounting software packages, or games.[13]

The operating system

The Operating System (OS) is the layer between the applications and the firmware controlling the hardware. The OS is loaded to the RAM after the system is started up. Microsoft Windows, Android, iOS, Linux and UNIX are familiar examples of an OS. OS extensions, such as Ubuntu for Linux or One UI for Android, are also included in the definition of an operating system.

[10] For more information, refer to the section 'What products and services should you select for the Cybercheck' to achieve a first selection.
[11] Refer to the section 'What is a product or service?' for more information.
[12] See 'Who should perform the Cybercheck?' for more information.
[13] For more information on protecting the software supply chain, please see: Factsheet Open Source Security | Factsheet | National Cyber Security Centre (ncsc.nl).

Firmware

Firmware is specific software programmed into hardware that facilitates the operating system in controlling that hardware. The firmware ensures that hardware can execute specific basic functions, such as starting up and shutting down. The Basic Input Output System (BIOS) is an example of firmware.

Hardware

Hardware covers the physical components comprising a digital product. Hardware can be deployed in both IT and OT environments. Examples of hardware include Random Access Memory (RAM), Central Processing Units (CPUs), Solid State Drives (SSDs), Printed Circuit Boards (PCBs) and Programmable Logic Controllers (PLCs). Printers, servers and network devices are also hardware.

Development

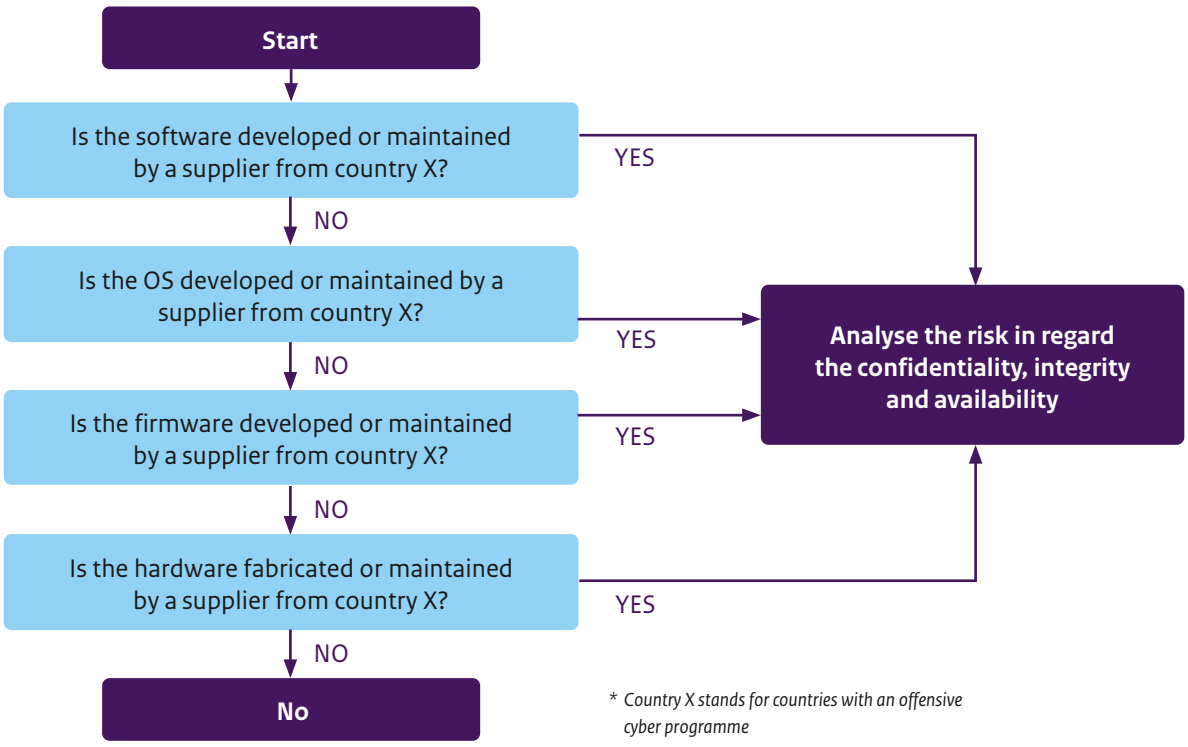
Products and services must be produced and/or developed before they can be deployed by users. For software, OS and firmware, this usually means designing and writing the program code. Mistakes can be made or inserted either intentionally or unintentionally during code development, which can be exploited by malicious actors. Hardware components are manufactured physically at plants, which means that digital backdoors can be incorporated into the product on purpose during production. These can then be exploited at a later time.

Maintenance

Products and services must be maintained/serviced after they are delivered. Software, OS and firmware are maintained by means of updates. An update often introduces new or improved features. They also patch vulnerabilities resulting from errors in the code. Malicious actors can exploit such updates to introduce vulnerabilities. A well-known example is the incident that occurred with a product of the company SolarWinds.[14]

Hardware and firmware sometimes require physical maintenance. In some cases, an organisation's administrator can handle this internally but often service and maintenance are outsourced to the hardware vendor. Malicious actors can exploit such physical access by asking or forcing the vendor to insert vulnerabilities.

The Cybercheck



* *Country X stands for countries with an offensive cyber programme*

[14] Backdoor in SolarWinds Orion | News | National Cyber Security Centre (ncsc.nl)

The Cybercheck in practice: the TechnologyS case

The Dutch company TechnologyS is a manufacturer and vendor of high-end innovative digital components. Their components are unique and ensure TechnologyS' position as a global market leader. As such, TechnologyS makes an important contribution to the earning capacity of the Dutch economy, which consists not just of the direct revenue generated but also of an indirect contribution in the form of jobs, knowledge development, and the Netherlands' digital autonomy. A cyber incident could therefore adversely affect not just TechnologyS but also the economic and thus the national security of the Netherlands.

TechnologyS has set up a risk management process in which the principal Protectable Interests are defined. While TechnologyS has multiple Protectable Interests, one interest in particular has been established as being most critical: protecting the organisation's intellectual property. TechnologyS grew into the market leader through years of investment in developing high-end innovative components. It is currently the only company in the world that can produce these components. As a result, the market position of TechnologyS (and indirectly of the Netherlands) depends on the company's unique intellectual property. Protecting its intellectual property is therefore the highest priority of TechnologyS' management and its CISO.

TechnologyS is thinking about buying new laptops for the members of its executive board. The media have been reporting on risks around deployment of products and services from countries with an offensive cyber programme increasingly in recent months. It has made TechnologyS' CISO consider the ramifications. Have earlier risk assessments incorporated the specific supply chain scenario in which countries with an offensive cyber programme may gain unauthorised access to the organisation's technological infrastructure via products or services? The CISO wonders whether the planned procurement of laptops may involve security risks with regard to the availability, integrity and confidentiality of the organisation's intellectual property.

The CISO decides to use the Cybercheck to map whether procuring these laptops may represent a potential risk:

Is the software developed or maintained by a supplier from country X?	The CISO asks the internal IT department and experts on the subject matter for assistance and contacts a number of external vendors that developed specific software solutions for TechnologyS. The CISO asks these vendors to provide information about the software on which these solutions were built and who is maintaining it. This analysis shows that the software that was to be installed on the laptops, is not developed or maintained by a supplier from a country with an offensive cyber programme.	**NO**
Is the OS developed or maintained by a supplier from country X?	When buying the laptops, the organisation can select an OS type that is known not to be developed or maintained by a supplier from a country with an offensive cyber programme.	**NO**
Is the firmware developed or maintained by a supplier from country X?	The CISO presents this question to the internal IT department and relevant experts. They use device management tooling to determine what firmware version was to be used on the laptops and which supplier develops it. It becomes clear that the firmware is not developed or maintained by a supplier from a country with an offensive cyber programme.	**NO**
Is the hardware developed or maintained by a supplier from country X?	The CISO contacts the potential vendor via TechnologyS' procurement department. This shows that the hardware in the laptops and the associated driver are developed by a supplier from a country with an offensive cyber programme.	**YES**

The assessment above shows that the planned procurement of new laptops may lead to a heightened security risk for the organisation's intellectual property. The CISO decides to investigate further through an additional risk assessment.

2 Course of action for an additional risk assessment

If the Cybercheck shows that deployment of a product or service may lead to a heightened security risk, an additional risk assessment allows the organisation to further analyse these possible risks. The course of action presented in this chapter provides starting points to support your organisation in conducting the additional risk assessment.

We recommend doing the additional risk assessment on the basis of the components 'threats', 'protectable interests', and 'resilience'.[15] The information in the introduction of this guide provides a basis for the 'threats' component.[16] Your organisation generally already has gained insight into its principal Protectable Interests with regard to National Security (in Dutch: TBB's-NV) through the risk management process. The 'threat' and 'protectable interests' components then form the basis for analysing the 'resilience'.

Establishing a number of plausible supply chain attack scenarios creates a basis for assessing whether, and to what extent, your organisation is resistant to specific supply chain risks resulting from the deployment of specific products and services.[17] You can use examples of supply chain attacks that occurred in the past, for instance at SolarWinds, RSA and MeDoc. It is important to translate the examples and principles presented in this guide to the specific context of your own organisation to ensure that you create plausible and appropriate scenarios.[18]

You can use the outcome of the 'resilience' component to assess whether a heightened security risk exists and if so, its potential impact on the organisations Protectable Interests. Gaining insight into and assessing these risks is a necessary step before deciding on appropriate security measures.[19]

Creating supply chain attack scenarios

An important consideration: Attackers choose the path of least resistance

When creating the attack scenarios, we recommend keeping in mind that the scenario of supply chain exploitation by a country with an offensive cyber programme will generally require a greater effort in terms of costs, time and effort with a higher risk of damage in case of being detected. There are also more easily available attack vectors to achieve the same goal, such as sending a spear-phishing e-mail or exploiting a (known) vulnerability or configuration errors.[20] These attack vectors generally have a lower risk in terms of exposure because they can be implemented remotely or via the internet, making it harder to trace them back to the attacker.[21]

---

[15] You can determine and implement the order for the 'threat' and 'protectable interests' according to your own preferences. However, we recommend always tackling 'resilience' last since 'threats' and 'protectable interests' must provide the basis for the 'resilience' component.

[16] For more information, please refer to Cyber Security Assessment Netherlands 2022 | Publication | National Coordinator for Counterterrorism and Security (nctv.nl).

[17] You can find more information in Analytical methods and cybersecurity | Expert blogs | National Cyber Security Centre (ncsc.nl).

[18] You will have to call upon several stakeholders in your organisation to complete the different components of a risk assessment. These may include the management to determine the main Protectable Interests but also security experts who are able to help you establish plausible supply chain attack scenarios specific to your organisation on the basis of these PIs.

[19] You must always present the risks and available measures to the risk owners (usually the management). The risk owners bear final responsibility for making a decision about risk control measures.

[20] Cf. Basic Cyber Security Measures | National Cyber Security Centre (ncsc.nl) for additional recommendations regarding basic measures that can increase your organisation's resilience to lower-key attack methods.

[21] AIVD publication *Offensive Cyber Programme, a perfect business model for states* (in Dutch) | Publication | AIVD.

Think of a situation in which an attacker has discovered that certain software in your organisation contains a critical vulnerability that is relatively easy to exploit remotely. As a result, the effort to exploit this attack vector is relatively low. On the contrary, an attack on the supply chain through a supplier to achieve the same goal would require more effort in this example.

We therefore recommend selecting the most plausible attack paths for your organisation.[22] For instance, the consideration above may allow you to determine, even at the stage of the additional risk analysis, that a targeted supply chain attack does not always constitute the primary risk for your organisation.

A tool: The Cyber Kill Chain

The Cyber Kill Chain (CKC) is a useful Framework to establish attack scenarios.[23] This model describes the stages that attackers may go through to achieve their objective. The stages describe how an attacker attempts to penetrate the organisation *(in)*, how they gain permanent access and move digitally through the organisation *(through)*, and how they achieve their objectives *(out)*.[24] The Cyber Kill Chain provides starting points to establish attack scenarios and allows you to create specific supply chain attack scenarios.

An overview: examples of supply chain attack scenarios

The overview below offers examples of supply chain attack scenarios that your organisation can use when creating attack scenarios. It is not a comprehensive list of every possible scenario but provides a broad overview of the various supply chain attack methods that countries with an offensive cyber programme may deploy.[25]

The framework tells you, for each of the attack scenarios, whether it results in potential security risks for availability, integrity and confidentiality. It also classifies the attack stages of *'in'*, *'through'* and *'out'* as shown above.

Example of an attack scenario	Stage	Availability	Integrity	Confidentiality
1. Deliberately inserted backdoor or vulnerability	In	✔	✔	✔
2. Malicious software update	In	✔	✔	✔
3. Insider threat via service engineer	In	✔	✔	✔
4. Exploitation of a product or service to gain access to another product or service	Through	✔	✔	✔
5. Espionage on data that is transmitted to the supplier by default	Out	✘	✘	✔
6. Exerting covert influence on the operation of a product or service	Out	✘	✔	✘
7. Sabotage of a product or service	Out	✔	✘	✘

[22] What attack paths are plausible and relevant for your organisation depends on your existing security measures and the intention, capacity and activities of countries with an offensive cyber programme as established in the 'threat' component. As such, the 'threat' and 'protectable interests' components are an important basis for assessing your resilience.

[23] For more information, please go to AIVD/MIVD publication: *Cyber-attacks by state actors - seven moments to stop an attack* | Publication | AIVD.

[24] Unified Kill Chain: Raising Resilience Against Cyber Attacks.

[25] We recommend using the MITRE ATT&CK framework as an additional resource. It provides an extensive list of attack methods that have been detected in actual practice and can help you establish conceivable attack scenarios for your organisation. The framework also provides the associated mitigating measures. Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®.

The '*in*' attack stage

In the scenarios below, countries with an offensive cyber programme try to gain unauthorised initial access to an organisation's technological infrastructure (or parts thereof) via products and services.

1 *Deliberately inserted backdoor or vulnerability*

Countries with an offensive cyber programme can insert a digital backdoor into a product or service's hardware or software or force the manufacturer to do so.[26] They can also deliberately insert a vulnerability that acts as a backdoor or force the manufacturer to do so. Countries with an offensive cyber programme can use such a backdoor to gain unauthorised access to parts of the technological infrastructure and gain direct control of the product or service. This enables them to access the data processed by the product or service, for instance. The backdoor can also be exploited to sabotage the functioning of the product or service (cf. scenarios 6 and 7); or the product or service constitutes a so-called stepping stone into interfaced networks or devices (cf. scenario 4).

2 *Malicious software update*

Countries with an offensive cyber programme can use updates to gain access to a product or service. By installing a malicious update or deliberately weakening the implemented cryptography, they can insert a backdoor or vulnerability in a specific product or service (cf. scenario 1).

3 *Insider threat via service engineer*

For some products and services, organisations need to hire specialised maintenance personnel. Such service engineers are often hired via the vendor that delivered the product or service. In most cases, service personnel have comprehensive access to the product and sometimes they also have access to data centres or interfaced associated/connected products. Countries with an offensive cyber programme may force the vendor based in their territory to have their service engineer install a backdoor.[27]

The '*through*' attack stage

In the scenario below, countries with an offensive cyber programme nestle deeper into the organisation's technological infrastructure after having gained access in the '*in*' attack stage. This stage aims to determine what parts of the technological infrastructure attackers can exploit to achieve their underlying objectives.

4 *Exploitation of a product or service to gain access to another product or service*

In most cases, a product or service must be able to connect or interface with other products or services within the organisation, such as mobile phones connected to the organisation's mail server. When countries with an offensive cyber programme can gain initial access via a product or service (cf. scenarios 1 through 3), these connections and interfaces can be exploited to gain access to other products or services.

The '*out*' attack stage

The scenarios below are examples of how countries with an offensive cyber programme can realise their underlying objectives through products or services:

5 *Espionage on data that is transmitted to the supplier by default*

Nearly all modern products and services transmit data to the vendor or supplier. Such data may vary from sensor-generated data and site data to large volumes of user data. All of it is stored on the supplier's servers. Countries with an offensive cyber programme may gain access to this data, either covertly or through the use of legal instruments.

---

[26] The *Cybersecurity Woordenboek* (Cyber Security Glossary) defines a backdoor as a covert way to circumvent security measures to access a digital system. Such backdoors are often created intentionally in such a way that they are invisible to others.

[27] For more information on insider threats, please see *Dealing with Insider Threats* | Publication | National Cyber Security Centre (ncsc.nl).

6 Exerting covert influence on the operation of a product or service

Countries with an offensive cyber programme can exert covert influence on the way a product or service functions, causing it to stop (fully) executing specific operations or, to the contrary, execute additional operations without the organisation noticing. For instance, sensors can be manipulated to generate incorrect data or the attacker can deliberately prevent notifications or e-mails from reaching the organisation.

7 Sabotage of a product or service

After gaining access, countries with an offensive cyber programme may deliberately disrupt the way a product or service functions. Examples are manipulating the power supply of a product or remotely deactivating the product or service. They can also force a supplier to cease supplying parts or support products and services. Consequently, products or services can no longer be supported or stop working altogether.

3 The outcome: what is next?

An important last step after conducting an additional risk assessment is to register the findings and provide feedback to the people in your organisation who are responsible for controlling digital risks arising from the deployment of products and services from a country with an offensive cyber programme.

If the findings of an additional risk assessment are not incorporated into the organisation's broader risk management process, the responsible manager(s) cannot ensure that such risks are adequately controlled and mitigated. Nor can the risks be assessed as part of a coherent whole, which means that the management cannot come to a well-founded decision regarding the use of a product or service.

This chapter concludes with a reprisal of the earlier fictive TechnologyS example. Below we return to the TechnologyS-example to explain the principles described in the previous chapter and to show how your organisation can use the outcome of the additional risk assessment to take further steps in risk control and mitigation.

The TechnologyS example: conducting an additional risk assessment
On the basis of the Cybercheck, TechnologyS' CISO has decided to conduct an additional risk assessment. This allows them to investigate potential security risks regarding the new laptops for the members of the executive board.

The Protectable Interests have been mapped and the management has determined that intellectual property is the primary PI. The organisation has also determined the possible impact for TechnologyS if the confidentiality of its intellectual property is violated. The PI assessment shows that this would affect not only TechnologyS itself but also the national security of the Netherlands. Based on a range of publications on threats, the CISO has concluded that TechnologyS owns high-value innovative knowledge, making the organisation an interesting target for countries with an offensive cyber programme that have the motivation and means to obtain its high-value innovative knowledge through espionage.

The CISO decides to organise a broad meeting with the ICT department and internal security experts to study the organisation's resilience with the aid of attack scenarios.

The 'in' attack stage
The CISO and his team create a plausible attack scenario for the 'in' attack stage. In this case, the laptops the organisation aims to buy are the starting point. The attack scenario assumes that a backdoor is built into the laptop hardware, granting initial access to TechnologyS' technological infrastructure.

One of the security experts notes that TechnologyS' network has multiple external interfaces with the internet, which might constitute entry points for attackers. The example of spear phishing e-mails or remote exploitation of configuration errors is also mentioned.

The CISO and his team consider the various attack methods and map the existing security measures. They conclude that the organisation has implemented a range of basic measures and additional measures that are geared towards dealing with attacks from the internet and will make it more difficult for attackers to breach the organisation's assets. Earlier scenarios did not take possible backdoors in the hardware into account. The CISO and his team determine that this is a plausible as well as a relevant supply attack scenario for TechnologyS and decide to focus on this possibility.

The 'through' attack stage
If attackers gain access via a backdoor, they will be able to search the organisation's internal network for TechnologyS' intellectual property. TechnologyS has implemented segmentation, which means that the intellectual property is stored in a secure environment that is not connected to the internet. The CISO and his team consider and map possible attack paths from a laptop into the environment containing the intellectual property. They investigate whether an attacker would have sufficient rights to gain access to the environment containing the intellectual property, for instance, but also whether a request for higher rights would be noticed, or whether lateral movement through the network would be detected. The CISO and his team note that security measures to keep attackers out of TechnologyS' network have been implemented but there are no adequate security measures to quickly and effectively detect suspicious behaviour within the internal network.

The 'out' attack stage
The actions in the 'in' and 'through' stages enable attackers to gain access to the secure environment containing the intellectual property. This enables them to access and exploit data. One of the security experts notes that data access constitutes a risk for espionage but that it would also be possible to copy data from the secure environment to a laptop, allowing attackers to obtain the data through that medium. The CISO and his team therefore map current security measures with regard to data exfiltration.

Outcome and what is next?
Based on the plausible attack scenario, the CISO and his team conclude that there is a security risk with regard to TechnologyS' intellectual property due to the laptops that the organisation wants to buy. The CISO and his team compile a report with their findings and recommendations. These findings and recommendations must also be incorporated into the broader risk management process to achieve the most comprehensive overview possible of the primary business risks for TechnologyS.

The report presents the following recommendations:
- A security measure that might be able to provide better security for TechnologyS is to select a preferred supplier that can offer additional guarantees concerning hardware integrity. It is also possible to have security testers assess the hardware's integrity before distributing the laptops to users
- TechnologyS can also consider detection and response solutions to detect and block suspicious behaviour on the internal network and laptops
- The rights to the secure environment can be restricted even further
- TechnologyS can implement additional solutions to prevent data exfiltration

The report and its recommendations are presented to the responsible decision-makers. This information allows TechnologyS' management to come to a well-founded decision concerning the procurement of new laptops. In the process, the level of risk acceptable will be determined. The report will serve as a starting point for selecting additional security measures that fit within TechnologyS' broader organisational objectives.

This brochure is a publication of:

Algemene Inlichtingen- en Veiligheidsdienst
aivd.nl
Postbus 20010 | 2500 EA Den Haag

CIO Rijk
Postbus 20011 | 2500 EA Den Haag

Nationaal Coördinator Terrorismebestrijding en Veiligheid
nctv.nl
Postbus 20301 | 2500 EH Den Haag

Nationaal Cyber Security Centrum
ncsc.nl
Postbus 117 | 2501 CC Den Haag