Supply Chain Security: Key Risk and Control Focus Areas

Yannick Herrebaut
Cyber Resilience Manager - CISO

Port of Antwerp Bruges

Who we are

Port of
Antwerp
Bruges

Who am I?

Yannick Herrebaut – Cyber Resilience Manager / CISO – Port of Antwerp-Bruges

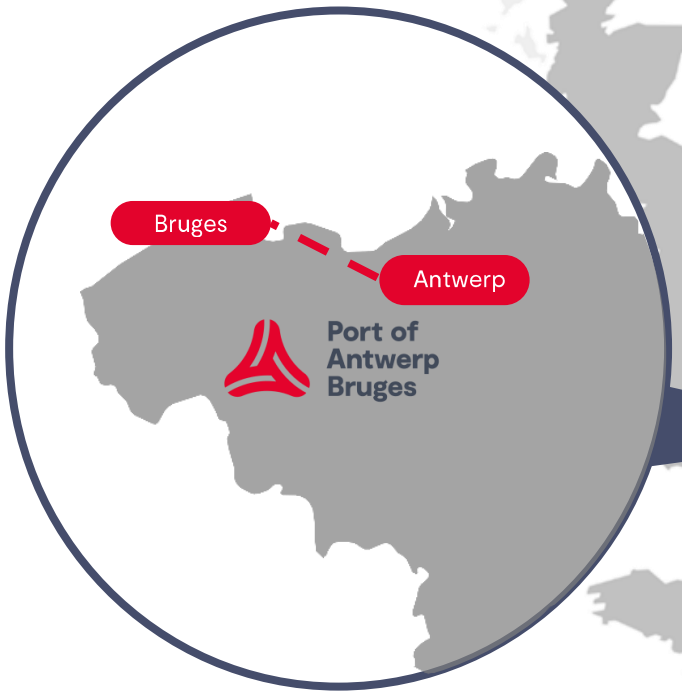
Education:

- Bachelor Multimedia & communication technology at Howest, Kortrijk
- Master IT risk & cybersecurity management at Antwerp Management School

Career:

- 2010 – 2018: Network administrator at Port of Antwerp
- 2018 – Now: Cyber Resilience Manager / CISO at Port of Antwerp-Bruges

Port of Antwerp Bruges



A global port in the heart of Europe

One port
Two sites

Port of
Antwerp
Bruges

2nd largest port in Europe

Transport

20,236
seagoing vessels/year

49,223
barges/year

42,000
loaded **cargo trains**/year

1,000 km
pipelines

166 **cruise** vessels
1 mio passenger movements

Cargo

Main **chemistry** hub in Europe

15% of the EU **gas** market

Largest **car handling** port in Europe

3.34 mio new cars/year

Second **container** port in Europe

Expertise in **breakbulk**

Port of Antwerp Bruges

14,322
Hectares

1,400
Companies

€ 20.8 billion
Added value

4.5%
GDP

164,000 **jobs**
Direct and indirect

Belgium's most important economic driver

Port of Antwerp Bruges

Daily operations

Frontrunner in four roles

Port Authority as a driver for Port of Antwerp-Bruges

Regulator

Operator

Landlord

Community builder

Port of Antwerp Bruges

Supply chain security, why bother?

Port of Antwerp Bruges

BBC

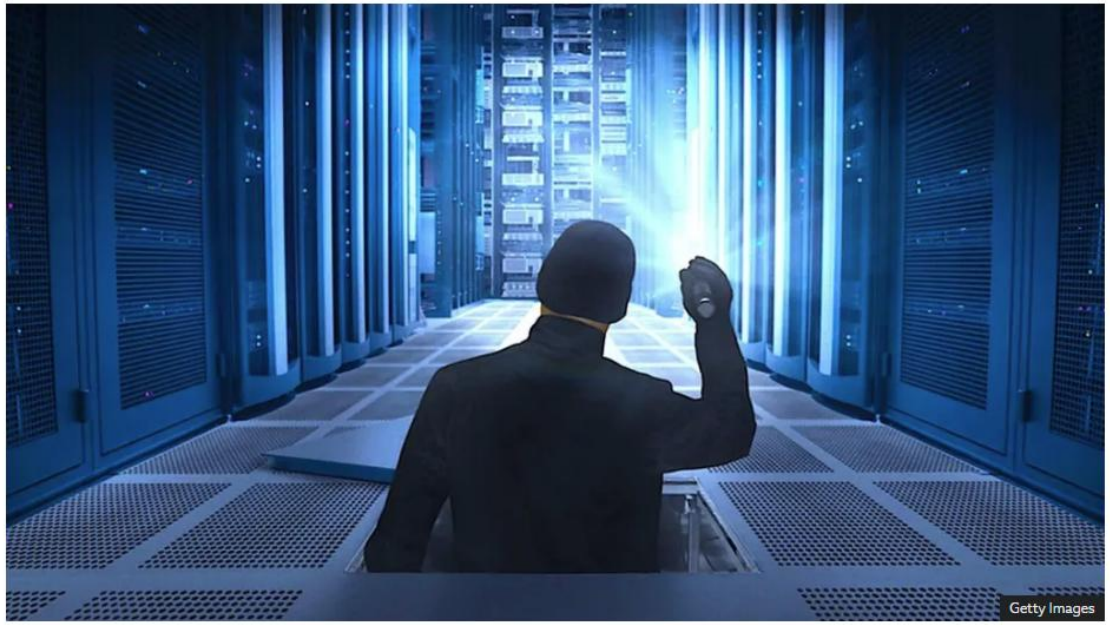
Home News Sport Business Innovation Culture Arts Travel Earth Video Live

SolarWinds: Why the Sunburst hack is so serious

16 December 2020

Share Save

Joe Tidy
Cyber reporter



We've all seen the pop-ups on our laptops or phones: "Update is available, click here to download."

We're constantly urged to do as we're told because these software updates improve our apps by boosting cyber-security and removing glitches.

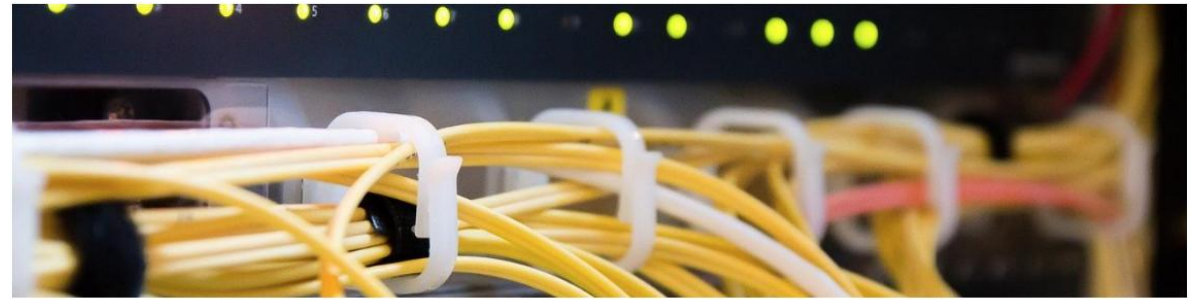
So when, in the spring, a pop-up message hit the screens of IT staff using a popular piece of software called SolarWinds, around 18,000 workers in companies and governments diligently downloaded the update for their offices.

What they couldn't have known was that the download was booby-trapped.

CENTRE FOR CYBERSECURITY BELGIUM

Search

Home News Organisation Regulation Sectors Vacancies Contact



PRESS RELEASE "DEACTIVATE KASEYA VSA : YOU ARE AT RISK OF A RANSOMWARE ATTACK FOLLOWING THE 'SUPPLY CHAIN' ATTACK ON THE SOFTWARE COMPANY KASEYA"

News

Are Belgian government agencies and companies in danger?

Kaseya VSA software is used worldwide, including in Belgium. The CCB does not know all of its Belgian clients and to date has not received a report of a Belgian victim. However, it is still important to monitor this threat and to seek out and help potential victims.

What has the Center for Cybersecurity Belgium (CCB) done?

The CCB has taken this threat seriously from the start. On July 3, CERT.be, the CCB's operational department, sent a warning and advice to Kaseya VSA users.

- A supply chain attack is an attack against an external partner, such as a vendor or supplier, who has access to your network.
- Kaseya, a computer software provider, was the victim of a supply chain attack. The hackers managed to compromise Kaseya VSA, a software that allows remote management of systems, to attack users of this software.
- Kaseya customers using the VSA product could be targeted by a variant of the REvil ransomware.

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Alert / OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160)

ALERT

OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160)

Last Revised: October 05, 2016

Alert Code: TA14-098A

Systems Affected

- OpenSSL 1.0.1 through 1.0.1f
- OpenSSL 1.0.2-beta

Overview

A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension.

National Cyber Security Centre

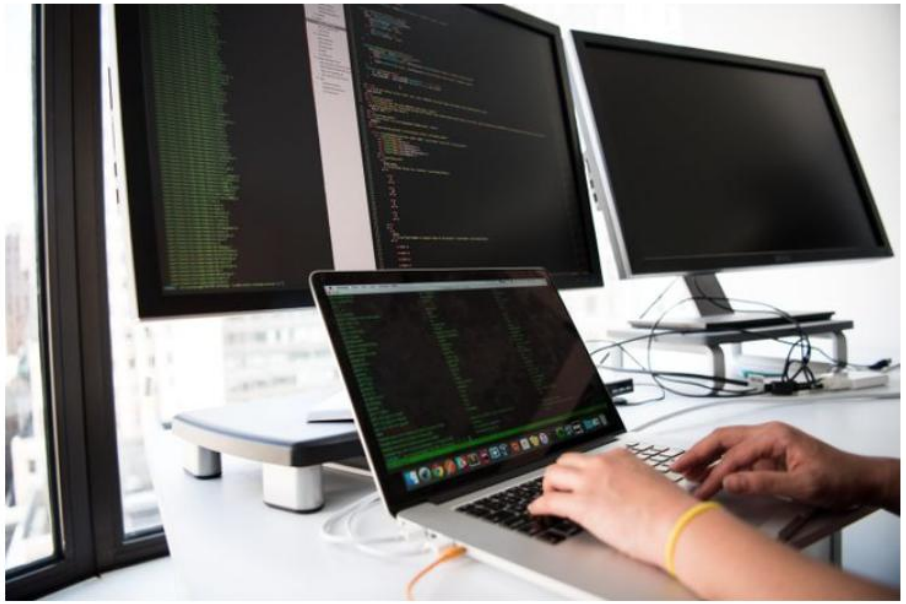
ABOUT NCSC | CISP | REPO

Home | Information for... | Advice & guidance | Education & skills | Products & services | Res

INFORMATION

Log4j vulnerability – what everyone needs to know

Information about the critical vulnerability in the logging tool, who it could affect and what steps you can take to reduce your risk.



Log4shell is a critical vulnerability in the widely-used logging tool **Log4j**, which is used by millions of computers worldwide running online services. A wide range of people, including organisations, governments and individuals are likely to be affected by it. Although fixes have been issued, they will still need to be implemented.

WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

The XZ Backdoor: Everything You Need to Know

Details are starting to emerge about a stunning supply chain attack that sent the open source software community reeling.

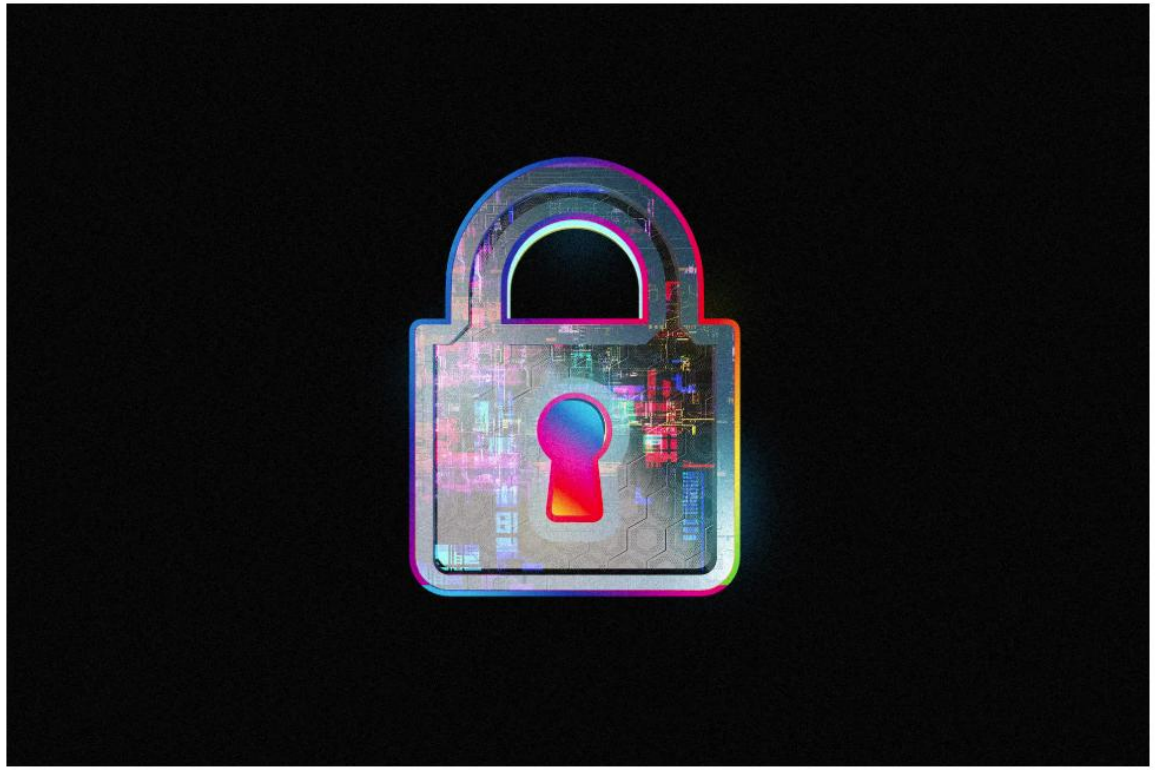


ILLUSTRATION: DA-KUK/GETTY IMAGES

If you buy something using links in our stories, we may earn a commission. This helps support our journalism. Learn more. Please also consider subscribing to WIRED

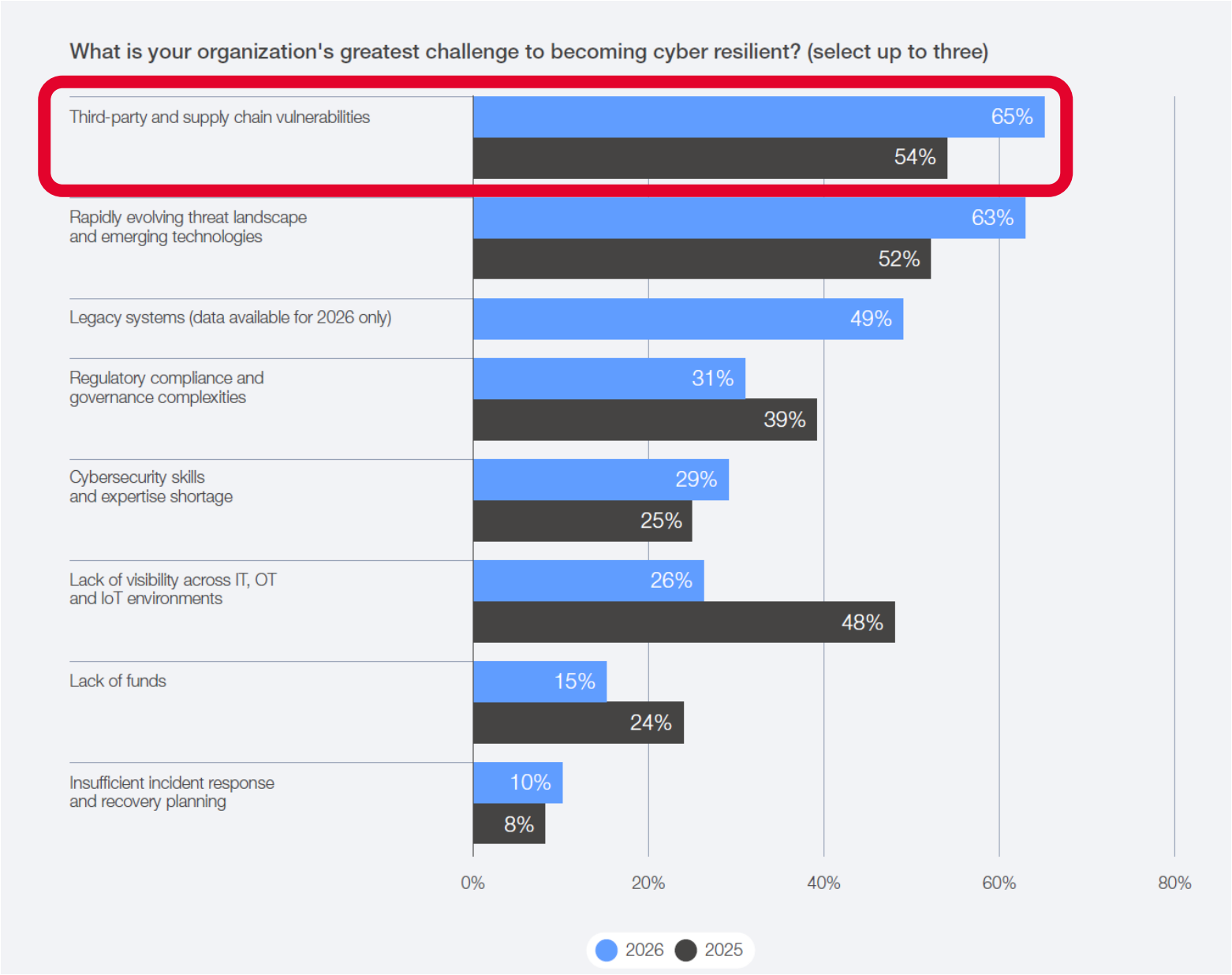
On Friday, a lone Microsoft developer rocked the world when he revealed a backdoor had been intentionally planted in XZ Utils, an open source data compression utility available on almost all installations of Linux and other Unix-like operating systems. The person or people behind this project likely spent years on it. They were likely very close to seeing the backdoor update merged into Debian and Red Hat, the two biggest distributions of Linux, when an eagle-eyed software developer spotted something fishy.

Don’t forget!

Open source

≠

Secure



Port of Antwerp Bruges

Source: WEF Global Cybersecurity Outlook 2026

CENTRE FOR CYBERSECURITY BELGIUM

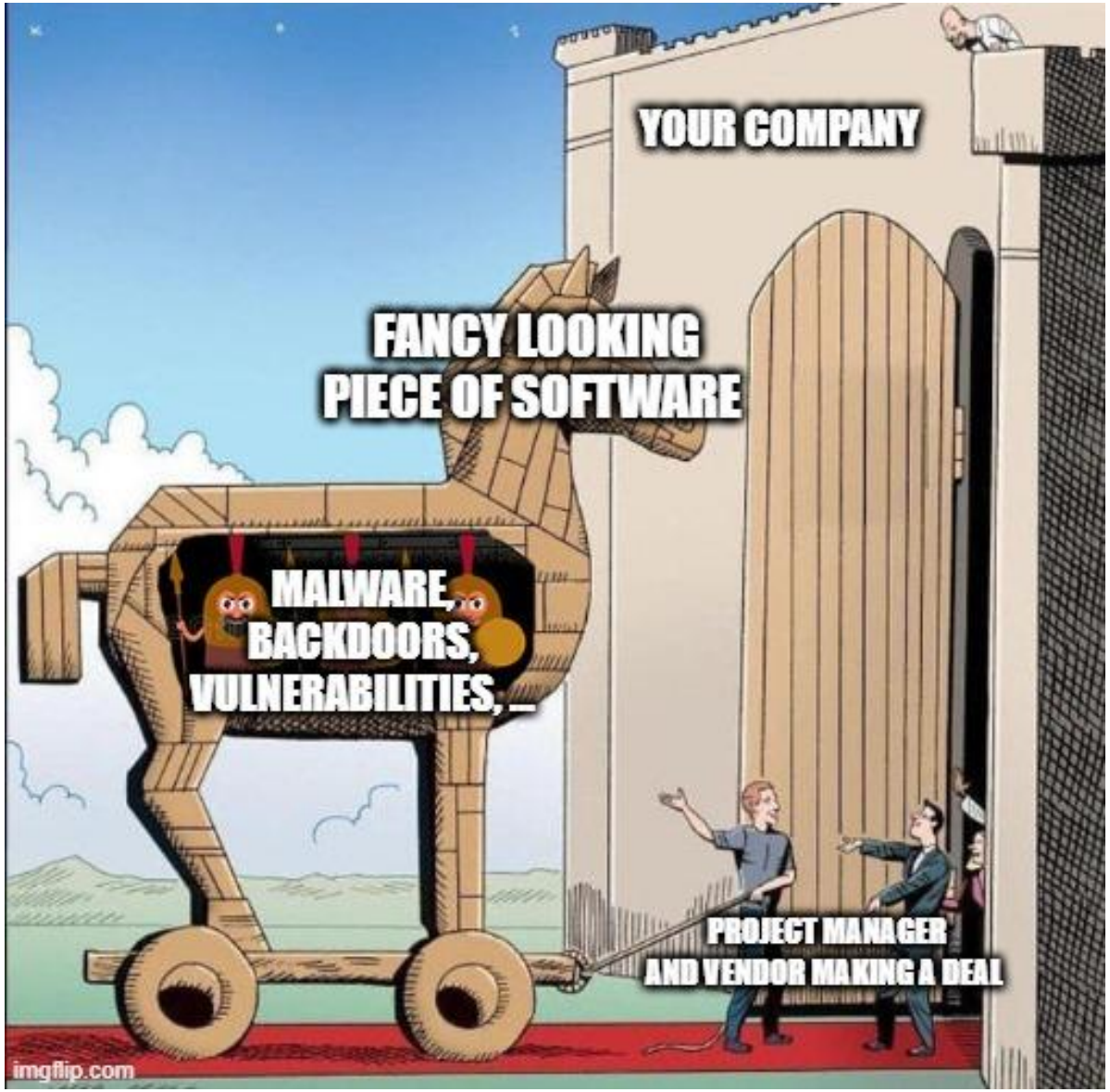
THE CYBERSECURITY MEASURES TO BE IMPLEMENTED

NIS2 DIRECTIVE

NIS 2: an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents. The law requires appropriate and proportionate measures to be taken based on the entity's risk assessment. These measures include at least:

1. Policies on risk analysis and information system security
2. Incident handling
3. Business continuity and crisis management
4. Supply chain security
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
7. Cyber hygiene and cybersecurity training
8. Policies and procedures regarding cryptography and, where appropriate, encryption
9. Human resources security, access control policies and asset management
10. Multi-factor authentication solutions, secured communications and secured emergency communication systems within the entity, where appropriate
11. A coordinated vulnerability disclosure policy

These security measures can be implemented using the CyberFundamentals (CyFun®) or ISO 27001 reference frameworks.



CISO

Port of Antwerp Bruges

Okay you convinced me. How do I start?

Port of Antwerp Bruges

Key actions for supply chain cybersecurity

1) **Secure coding practices:** To mitigate internal development risk, it is key to implement foundational principles that minimize vulnerabilities and integrate security into the development process, making the software resilient against potential threats. Ensure that all open-source components come from trusted sources and set guidelines for their use. Clear responsibility for software security needs to be established, with mechanisms for accountability in place to ensure developers follow secure coding practices.

2) **Software bill of materials (SBOM):** To enhance transparency and visibility, SBOMs provide a comprehensive list of all components used in software, ultimately helping an organization to identify potential security risks.

3) **Continuous monitoring:** It is key to regularly scan for vulnerabilities and keep all software components up to date. AI can be a helpful tool in doing so, used for proactive monitoring, identifying vulnerabilities, detecting threats early, and reducing time-to-market pressures that often compromise secure development practices.

4) **Strengthened vendor management and risk assessment:** Organizations must implement robust vendor management practices, conduct thorough risk assessments, and ensure that third-party providers adhere to strong security protocols. Regular auditing and proactive assessment and monitoring are key for mitigating potential risks. Limiting access to sensitive parts of the software supply chain can further help to reduce the risk of unauthorized access.

Port of Antwerp Bruges

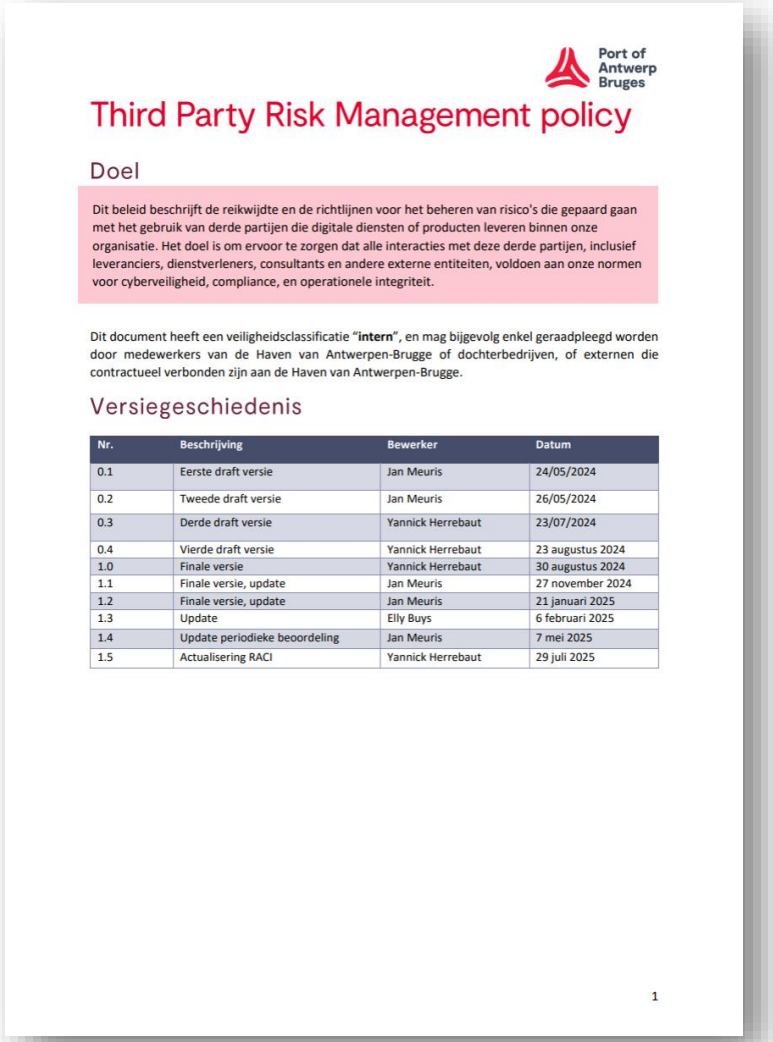
Source: https://www.weforum.org/stories/2025/01/software-supply-chains-cyber-resilience/

Disclaimer:

NIS2 compliance not guaranteed!

Port of Antwerp Bruges

Third party risk management policy



Port of Antwerp Bruges

Third Party Risk Management policy

Doel

Dit beleid beschrijft de reikwijdte en de richtlijnen voor het beheren van risico's die gepaard gaan met het gebruik van derde partijen die digitale diensten of producten leveren binnen onze organisatie. Het doel is om ervoor te zorgen dat alle interacties met deze derde partijen, inclusief leveranciers, dienstverleners, consultants en andere externe entiteiten, voldoen aan onze normen voor cyberveiligheid, compliance, en operationele integriteit.

Dit document heeft een veiligheidsclassificatie **"intern"**, en mag bijgevolg enkel geraadpleegd worden door medewerkers van de Haven van Antwerpen-Brugge of dochterbedrijven, of externen die contractueel verbonden zijn aan de Haven van Antwerpen-Brugge.

Versiegeschiedenis

Nr.	Beschrijving	Bewerker	Datum
0.1	Eerste draft versie	Jan Meuris	24/05/2024
0.2	Tweede draft versie	Jan Meuris	26/05/2024
0.3	Derde draft versie	Yannick Herrebaut	23/07/2024
0.4	Vierde draft versie	Yannick Herrebaut	23 augustus 2024
1.0	Finale versie	Yannick Herrebaut	30 augustus 2024
1.1	Finale versie, update	Jan Meuris	27 november 2024
1.2	Finale versie, update	Jan Meuris	21 januari 2025
1.3	Update	Elly Buys	6 februari 2025
1.4	Update periodieke beoordeling	Jan Meuris	7 mei 2025
1.5	Actualisering RACI	Yannick Herrebaut	29 juli 2025

1

Port of Antwerp Bruges

Dividing vendors into different tiers depending on potential risk for the organisation

To make sure our policies are reasonable and appropriate, and are relating to the potential risk posed by a certain vendor, we divide them into 4 distinct categories:

- **Tier 1 - Very high risk vendors**: Problems have a serious impact and are difficult to manage, we must closely monitor that the necessary measures are implemented correctly.
- **Tier 2 - High risk vendors:** Problems have a significant impact but can be managed if the necessary measures are taken.
- **Tier 3 - Medium risk vendors:** Problems have a reasonable impact, but are well manageable.
- **Tier 4 - Low risk vendors**: Problems have a low impact and are well manageable.

Simply put, the supplier of printing paper does not have to adhere to the same rules as the vendor of our ERP system.

Port of Antwerp Bruges

The assigned tier depends on the risk estimation, which is influenced by different criteria

What is being implemented?

Criterium	Weight
The project involves **hardware** that will be connected to the Port of Antwerp-Bruges network *Examples: a module used to manage building systems like heating, ventilation, lights, … or a module that is connected to the onboard PLC of a tugboat to monitor fuel usage.*	8
The project involves the installation of **software on a server** within the network of Port of Antwerp-Bruges. *Examples: a web server in the Microsoft Azure cloud of Port of Antwerp-Bruges or a collaboration tool that's installed on a virtual server in the Port of Antwerp-Bruges datacenter*	4
The project involves the usage of software that is being hosted by a third party (**SaaS**). *Example: software that's being used to manage personnel planning*	2

Port of Antwerp Bruges

The assigned tier depends on the risk estimation, which is influenced by different criteria

What data is being processed?

Sensitive data (“confidential” or “limited distribution”) *Examples: information under NDA, data subject to a statutory retention period, security related information*	4
Data with a high requirement on **availability and integrity**. *Examples: operational personnel planning, asset information, CCTV, footage, shipping planning*	4
Personally identifiable information (PII, GDPR compliance) *Examples: simple data in large volumes (CRM), employee salaries, medical reports of accidents at work*	4

Port of Antwerp Bruges

The assigned tier depends on the risk estimation, which is influenced by different criteria

For what process will the supplier provide a product or service?

Essential business process: • Coordination of maritime traffic • Control of bridges and locks • Tugboat services • Berth management	8
Important business process *Examples: calculation and payment of salaries and port dues, collaboration tools, asset management*	4
Supporting business process: everything that's not essential or important	2

Port of Antwerp Bruges

The assigned tier depends on the risk estimation, which is influenced by different criteria

How does the user population look like?

Size of the total user population (> 1000)	2
Both **internal as well as external** users	2

Port of Antwerp Bruges

Every tier has a different set of measures a vendor has to adhere to

Tier	Measures

Tier 1
> 27
	- Non-Functional Requirements
	- Cybersecurity policy for third party contractors (if applicable)
	- Signed declaration for external access (if applicable)
	- Security rating score (quantitatively managed)
	- NIS2 compliant (ISO27001 certified or CyFun Important Verified)
	  ○ Extensive questionnaire (in case no certificate or no verified claim)
	  ○ Standard questionnaire (in case relevant certificate or verified claim can be presented)

Tier 2 > 17 < 27	- Non-Functional Requirements - Cybersecurity policy for third party contractors (if applicable) - Signed declaration for external access (if applicable) - Security rating score (defined) - Standard questionnaire
Tier 3 > 7 < 17	- Non-Functional Requirements - Cybersecurity policy for third party contractors (if applicable) - Signed declaration for external access (if applicable) - Security rating score (managed)
Tier 4 < 7	- Non-Functional Requirements - Cybersecurity policy for third party contractors (if applicable) - Signed declaration for external access (if applicable)

Port of Antwerp Bruges

Context

Our TPRM policy and all applicable measures are published on our website:

https://digitalspecs.portofantwerpbruges.com/non-functional-requirements/

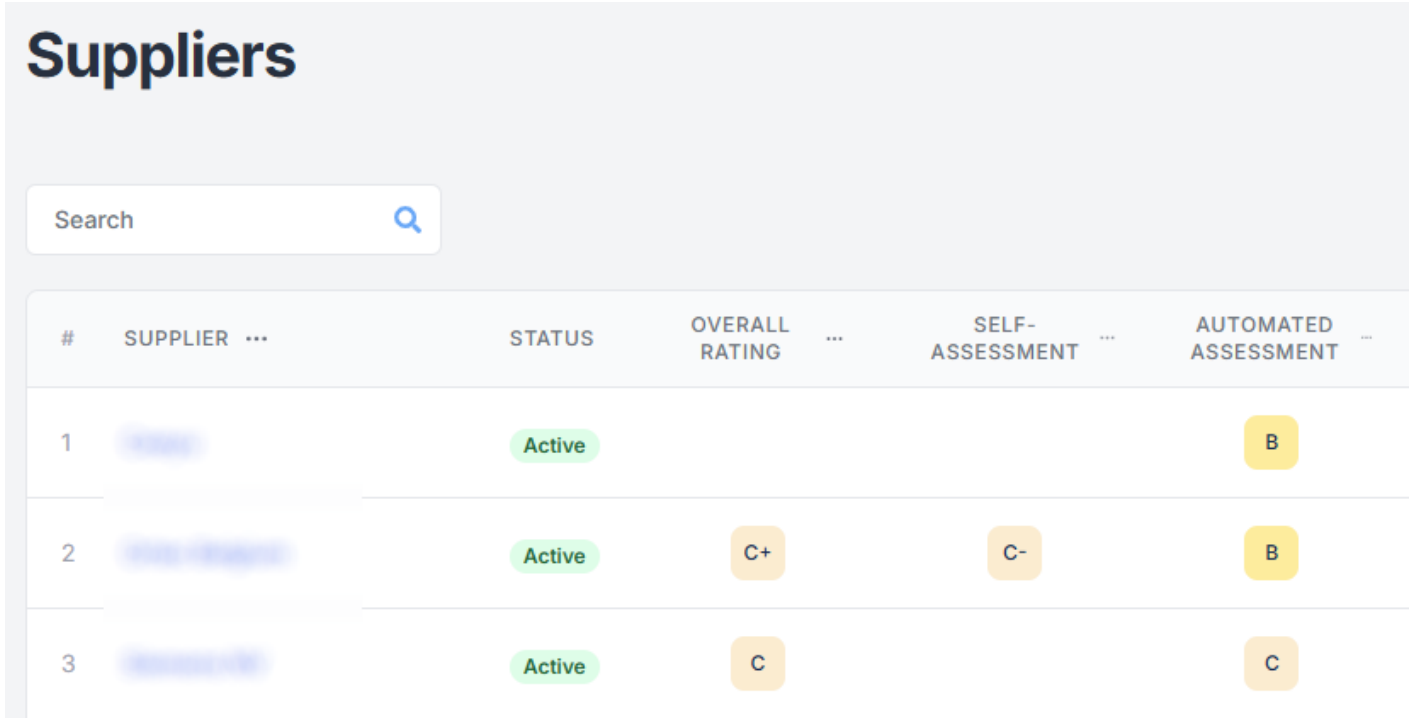
During the evaluation process, we take into account:

- Whether the vendor can be considered as “**unique**” (= even if the vendor doesn’t comply with our policy, there is no way around him)
- Whether doing business with this vendor is **prohibited** by regulation or he has received negative advice (= the vendor is compliant with the policy, but we can’t / don’t want to do business with him)

Port of Antwerp Bruges

Context

For the **security rating scores** and the processing of the **questionnaires**, we use Ceeyu:



Port of Antwerp Bruges

Ceeyu

Context

We deliberately kept the questionnaires (relatively) short, so the burden on the vendors is manageable. The extensive questionnaire has 39 questions in total, aligned with the NIST CSF and CyFun frameworks:

Port of Antwerp Bruges

Ceeyu

BZ: Business

IT: Information Technology department

PR: Procurement department

CR: Cyber Resilience department

SP: supplier

TPRM process overview

Evaluation & classification

- Determining the right tier
- BZ, IT & PR responsible
- CR reviews & gives approval

Engagement

- SP needs to accept relevant measures according to tier
- SP (T1, T2) needs to fill in questionnaire
- CR reviews questionnaire & gives approval

Remediation

- When SP does not meet the necessary requirements
- BZ, IT, PR and CR determine remediation timeframe & actions
- Contract will be terminated when SP does not comply within timeframe

Monitoring

- Security rating scores of T1, 2 and 3 SP will be monitored during the course of the contract by CR
- When SP does not comply anymore, remediation process applies

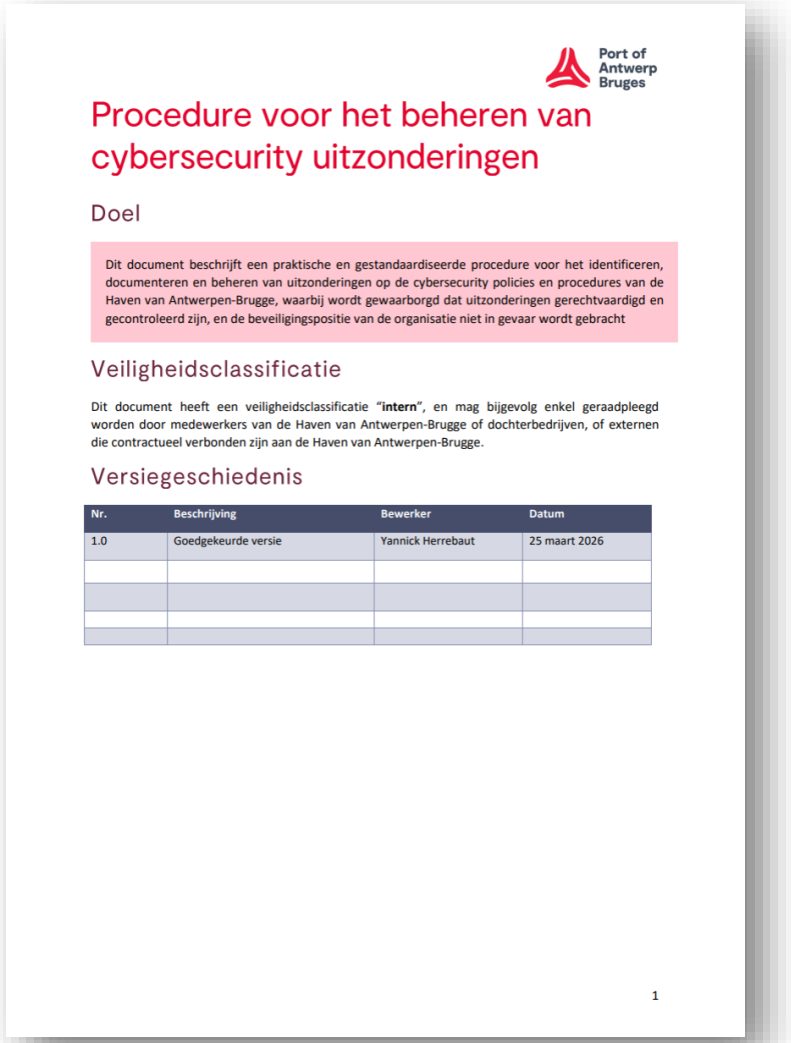
Port of Antwerp Bruges

TPRM is not a silver bullet though

- **Large projects**, where there is a main supplier and several subcontractors (ex. Construction projects). How to make sure that subcontractors also follow TPRM policy?
- **Frame agreements of other government entities**: PoAB does not write these tenders, so TPRM policy of the tendering entity applies (if there is one). How to make sure that purchases through these frame agreements comply with the TPRM policy of PoAB?
- There are **different ways to buy digital products and services**: purchases via creditcard, “purchasing orders” (< 30K€), and frame agreements of other government entites. How do we make sure nothing escapes our attention?
- What to do with **regular purchases**, like smartphones, laptops, servers, … Going through the full TPRM policy for every purchase order is not feasible. Maybe whitelist certain vendors for a specific period of time?
- **“Questionnaire fatigue”** is a real thing among vendors. Some kind of standardized questionnaire could come in handy…
- We will start with embedding TPRM in new contracts starting from Q1 2025, but there is of course still the **“💩 of yesterday”**

Port of Antwerp Bruges

Exception management



Port of Antwerp Bruges

Procedure voor het beheren van cybersecurity uitzonderingen

Doel

Dit document beschrijft een praktische en gestandaardiseerde procedure voor het identificeren, documenteren en beheren van uitzonderingen op de cybersecurity policies en procedures van de Haven van Antwerpen-Brugge, waarbij wordt gewaarborgd dat uitzonderingen gerechtvaardigd en gecontroleerd zijn, en de beveiligingspositie van de organisatie niet in gevaar wordt gebracht

Veiligheidsclassificatie

Dit document heeft een veiligheidsclassificatie "**intern**", en mag bijgevolg enkel geraadpleegd worden door medewerkers van de Haven van Antwerpen-Brugge of dochterbedrijven, of externen die contractueel verbonden zijn aan de Haven van Antwerpen-Brugge.

Versiegeschiedenis

Nr.	Beschrijving	Bewerker	Datum
1.0	Goedgekeurde versie	Yannick Herrebaut	25 maart 2026

1

In essence:

- The exception has to be provided to the Cyber Resilience Manager in writing, by a member of the Port Management Team
- The Cyber Resilience Manager assesses the risk of granting the exception
- If the Cyber Resilience Manager gives positive advice, the exception is granted and added to the exception register. If the advice is negative, the member of the Port Management Team can escalate to a member of the board of directors, who has the final say
- In all cases, the risk ownership is transferred to the requesting party, and he/she is responsible for taking appropriate risk mitigating measures
- Exceptions can be rescinded at any given time if the risk profile has changed significantly

Port of Antwerp Bruges

Thank you!
Questions?

Port of Antwerp Bruges