Uptime Security

Cyber Security Checklist

How well-protected are you against cyber crime?

In recent years, cyber security has become increasingly important for organisations all over the world. As many industries undergo intensive digitization, there is a growing need to adequately protect your business and data from an expanding number of malicious actors.

Defending your organization against the increasing threat of cyber crime can be a daunting task as it involves implementing an overall strategy with numerous security measures and action plans. Where should you begin? What should you focus on? And what are you already doing right?

Grab this free checklist by the hand and discover which cyber security measures are already in place.

Identify

	Yes	No
Your organisation has a full inventory of assets associated with information and information processing facilities. The inventory is documented, reviewed and updated when changes occur.	☐	☐
You have an established cybersecurity policy, which is communicated throughout the organisation.	☐	☐

Protect

	Yes	No
Your company data is encrypted*.	☐	☐
Access and authorisation to company data is well managed, incorporating the principles of least privilege and separation of duties*.	☐	☐
Backups of data are conducted, maintained, and tested.	☐	☐

Uptime Security

Detect

	Yes	No
Your organisation's protection and detection hardware/software (e.g. firewalls*, anti-virus) has an activity logging functionality, which is not only enabled, but also backed-up and reviewed.	☐	☐
Anti-virus, -spyware, and other -malware* programs are installed and updated.	☐	☐
Vulnerability scans are performed.	☐	☐

Respond

	Yes	No
You have a readily available incident response process, with clearly defined roles, responsibilities, and authorities. The process is executed during or after an information security event on your organisation's systems.	☐	☐
You have implemented vulnerability management processes and procedures that include processing, analysing and remedying vulnerabilities from internal and external sources.	☐	☐

Recover

	Yes	No
You have developed a recovery process (DR) for disasters and information security incidents. When needed, the process is executed.	☐	☐

Need help protecting your organization?

Getting all elements in place may be challenging. That is why our mission is to help you protect yourself in a world that is rapidly evolving. At Bow Tie Security, you can rely on a committed group of cyber security experts with a profound understanding of the new NIS2* Directive, who are ready to offer you the necessary guidance in protecting your organisation against cyber threats. Want to learn more about NIS2?
Get in touch straight away.

Have you heard about the new NIS2 Directive?

In November 2022, the European Union adopted a new Network and Information Systems (NIS) Directive. NIS2, as this directive is called, is aimed at enhancing cyber security in a number of critical sectors across the EU and could very well be a game-changer for a lot of Belgian and international companies. NIS2 will be implemented nation-wide by the end of 2024.

NIS2 is an improved version of the Network and Information Security (NIS) Directive that was implemented back in 2018. NIS was the first piece of EU-wide legislation on cyber security and it was aimed at creating a common level of digital security across the Member States. Although NIS had some obvious merits, its implementation proved difficult, and the success was fragmented. As cyber-attacks and hacks are a growing threat, the Commission proposed to replace NIS by a stricter and more committing directive: NIS2. By strengthening security requirements, streamlining reporting obligations, and introducing more stringent supervisory measures and harmonized sanctions, NIS2 is focused on creating safer and more resilient digital environments and increasing the level of cyber security across all European member states.

What does NIS2 mean for Belgian companies? **Read it in our blog!**

Glossary

CCB

The CCB is the Belgian Centre for Cyber Security. In other words, the national authority for cybersecurity in Belgium. It supervises, coordinates and monitors the application of the Belgian cyber security strategy. As such, it is the organisation that will mould the NIS2 Directive into a new federal law on cyber security prevention and digital safety. The CCB will also be one of the authorities that will exercise supervision on the regulations set forth by NIS2.

Firewall

A firewall is a network security tool that monitors and filters incoming and outgoing network traffic based on a set number of security policies. Essentially, a firewall acts as a barrier between your internal network and the public Internet. A firewall's main purpose is to keep dangerous activities out.

Malware

Malware is an umbrella term for many types of malicious software, designed to infect or damage digital environments or gain access to them. Although all malware compromises the security and privacy of computer systems, each type works in its own intrusive way. Ransomware is a type of malware.

NIS2

In November 2022, the European Union adopted a new and improved version of the Network and Information Systems (NIS) Directive. NIS2, as the new directive is called, is aimed at enhancing cyber security in a number of critical sectors across the EU and could very well be a game-changer for a lot of Belgian and international companies. By strengthening security requirements, streamlining reporting obligations, and introducing more stringent supervisory measures and harmonised sanctions, NIS2 is focused on creating safer and more resilient digital environments and increasing the level of cyber security across all European member states. NIS2 will be implemented in Belgium by October 2024.

Ransomware

Ransomware is very common type of malware, that cyber criminals use to extort their victims. By hacking into an organization's digital environment, the malicious software corrupts entire computer systems and the criminals either threaten to publish sensitive data or to block business continuity, unless a ransom is paid.

VPN

A VPN or virtual private network is a software application that is designed to protect your devices against cyber criminals and unauthorized access. VPNs conceal your IP address and encrypt your internet traffic, making it very difficult for people to monitor your activity and access your information.

Encrypted

Encryption is a way of scrambling data so that only authorized parties can understand the information. Readable data is altered to appear random. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext.

Principles of least privilege and seperation of duties

Separation of duties has to do with splitting tasks among employees to reduce the chance of one employee committing fraud. Least privilege is when you only provide employees with the account privileges they need to complete their work. The principle of least privilege can support the separation of duties.

Bart Renard
Practice lead

bart.renard@uptimesecurity.com