Maturity guides for digital service builders

05 September 2023, 15:28

Tatiana Galibus

How to be ready for the NIS2 directive

It is no secret a major shift is expected for digital service builders with the new NIS2 directive. Upcoming regulations will oblige many digital providers and data centers to be considered as essential or important entities. The belts will be tightened for almost everyone: as soon as a service provider has an important customer falling under NIS regulation, he automatically has to be trusted, answer the security questions and conduct an audit. Software companies, even start-ups and scale-ups, need to look closer at regulations and often they are urged to do so by their customers.

What are the standards to follow in Belgium?

NIS2 directive does not specify step-by-step guidelines for companies. Member states adjust the general rules to their own situation, to assure compliancy. In Belgium, this work is being led by Center for Cybersecurity Belgium within the Cyberfundamentals framework. Cyberfundamentals is quite generic in its turn, although it is adapted to SMEs, it is not specifically for software companies, developers, testers, data centers, digital service builders etc.

What are the cybersecurity standards for software builders?

The good news is that there is a well-defined trusted framework of guidelines and tools for the digital service security. It is supported by OWASP - a nonprofit foundation that works to improve the security of software. OWASP provides and develops several important standards to be followed by the digital companies.

Why software builders should look at these standards? They are usable, understandable, pragmatic and widely adopted by software companies security experts.

- OWASP ASVS
- OWASP DSOMM
- OWASP SAMM

OWASP ASVS

The OWASP Application Security Verification Standard (ASVS) provides a basic list of requirements for secure development. We recommend this standard for developers and testers. ASVS proposes three maturity levels:

LEVEL	FOR WHOM
ASVS Level 1	A baseline level of assurance that can be assessed with less interaction between the ass
ASVS Level 2	A level of assurance for most applications i.e. containing sensitive data.
ASVS Level 3	Reserved for the most critical applications, that requires significant integration between t application team.

OWASP DSOMM

The OWASP DevSecOps Maturity Model provides opportunities to harden DevOps strategies and shows how these can be prioritised. It provides requirements and implementation levels for automation pipelines, software building and infrastructure hardening. We recommend this standard for automation operators, testers, solution managers and project leaders. DSOMM proposes five maturity levels (we overview the first three):

LEVEL	FOR WHOM	CONTROLS
DSOMM Level 1	Basic understanding of security practices	23 controls
DSOMM Level 2	Adoption of basic security practices	47 controls

DSOMM Level 3 High adoption of security practices	45 controls

OWASP SAMM

The Software Assurance Maturity Model (SAMM) is an open framework to help organisations formulate and implement a strategy for software security that is tailored to the specific risks facing the organisation. It helps to evaluate an organisation's existing software security practices and build a balanced software security assurance program.

We recommend this standard for CEOs, project leaders, and project owners. The foundation of the model is built upon the core business functions of software development with security practices tied to each (see diagram below). The building blocks of the model are the three maturity levels defined

How Sirris can help?

On **18 October 2023**, Sirris is organising a **knowledge exchange expert session**. It will be focused on NIS2 directive and other upcoming cybersecurity needs for digital services.

The session is completely free of charge. In this online meeting you can hear the expert opinions about the new regulations and cyber-security challenges and exchange with the alumni of our masterclass on their journey towards cyber-security maturity.

You can register here.

This session will also kick off our **Cybersecurity bootcamp for SaaS and digital services**, subsidised by VLAIO for Flemish companies. The bootcamp is designed as a learning journey, with in-depth theory and tailor-made practice sessions. We partner up with cybersecurity providers all over Flanders to deliver the best lesson learnt and networking experience, as well as individual micro-coaching sessions for your individual concerns.

Interested to know more about the bootcamp and register? Browse to our agenda!

Authors

Tatiana Galibus