mobisec

GUIDE TO NIS2

HOW SECURITY MANAGEMENT PRIORITIES ARE CHANGING FOR COMPANIES WITH A MOBILE APPLICATION

mobisec.com

mobisec

OUR 8 POINTS

MENU

FOCUSED ON SECURITY

ABOUT US

Founded in 2015, Mobisec has dealt with **applicative cybersecurity** from the very beginning, in the knowledge that the responsibility for infrastructure security is increasingly passing into the hands of hyperscalers and cloud service providers; this makes data centres and networking particularly resilient, while leaving the logical-application world highly exposed.

We were born precisely to respond to the security needs of an increasingly connected world, developing unique skills and knowledge in ethical hacking and innovation. We offer tailor-made solutions to provide security and peace of mind to those who manage the cybersecurity of applications, mobile devices and IoT in the enterprise.

FOCUSED ON SECURITY

ABOUT US

In 2024 we became, the only Italian company among the 20 present worldwide, **official members of the ADA** (App Defence Alliance), the body of the Linux Foundation whose steering committee is Microsoft, Google, and Meta and whose mission is to guarantee the security and privacy of the app ecosystem by defining reference frameworks for testing and laboratories.

We are **firmly in the group of contributors to the OWASP** (Open Worldwide Application Security Project), the highest international body for defining security standards and procedures in the application world; in 2024 we will contribute directly to the mapping of Weaknesses, the new category introduced by the OWASP for Mobile Applications (MASWE).

Mobisec is included among the **Mobile Application Security Testing solutions within the Gartner Peer Insights**, with an average rating of 4.5/5.

Mobisec has obtained **ISO 27001:2022 certification for information** security management, and follows the standards of ISO 9001:2015 certification for quality management systems.

Introduction

NIS2

What it is - NIS2 (Network and Information Security-2) is the directive that came into force on 17 January 2023 and that EU Member States **must transpose by 17 October 2024**; it aims to establish common references within the Union on information security issues and operates synergistically with other regulations, such as the GDPR, the Cyber Resilience Act, and the DORA regulation.

To whom It applies - Although at first glance it may seem applicable only to a narrow base of companies, considered to be 'highly critical', in fact it extends to the entire supply chain, thus impacting a much wider number of companies.

Mobile Application Security - The regulation covers a wide range of requirements that companies must meet in order to be considered compliant, in this guide we focus on those points that specifically relate to Mobile Application security.

1. WHAT IS AN INFORMATION SYSTEM?

THERE ARE ALSO APPS

THE ARTICLE

Article 2 <<definitions>>, paragraph 1, letter E, 'information and network system':

1) *an electronic communications network within the meaning of Article 2, paragraph 1(vv) of Legislative Decree No 259 of 1 August 2003;*
2) *any device or group of interconnected or related devices, one or more of which performs, on the basis of a program, automatic processing of digital data*
3) *digital data stored, processed, retrieved or transmitted by means of networks or devices mentioned under (1) and (2), for their operation, use, protection and maintenance;*

The article highlights a crucial point: IT security is no longer an optional extra, but a categorical imperative. It is not just about protecting traditional infrastructure and software, but about extending security to everything that is connected and processes digital data. This includes smartphones and the countless apps we use on a daily basis.

Every app that is downloaded and installed is like a door or a window. The more you have, the more you have to make sure they are securely closed and protected. That is why NIS2 also includes these devices and their apps.

In short, the article reminds us that we live in an increasingly connected world and that security must be a priority, not only for large infrastructures, but also for portable devices.

2. RISK MANAGEMENT

ALSO IN THE AREA OF MOBILE APPS

THE ARTICLE

Article 23, paragraph 1 <<administrative and governing bodies>>:

The administrative and governing bodies of essential and important entities:

a) approve the manner of implementation of the cybersecurity risk management measures taken by those entities pursuant to Article 24;

b) oversee the implementation of the obligations set out in this Chapter and in Article 7;

c) they are responsible for the breaches referred to in this Decree.

This article highlights the important role of administrative and management bodies in ensuring IT security. It is not only a matter of approving risk management measures, but also of supervising their implementation and taking responsibility for any breaches, including in the area of mobile applications.

The proactive approach is not only about putting security measures in place, but also about constantly monitoring them and being ready to intervene in the event of problems. IT security requires constant commitment from everyone, starting with the management and governing bodies.

3. SECURITY OF SUPPLY CHAIN

RESPONSIBILITIES FOR SOFTWARE HOUSE AND CONTRACTING COMPANY

THE ARTICLE

Article 3, paragraph 10 <<scope of application>>:

Finally, this Decree shall apply, regardless of its size, to an undertaking connected to an essential or important entity, if it meets at least one of the following criteria:

a) *it makes decisions or exerts a dominant influence on decisions regarding the cybersecurity risk management measures of an essential or major entity;*
b) *owns or operates information and network systems on which the provision of services by the important or essential entity depends*
c) *performs IT security operations of the important or essential entity*
d) *provides ICT or security services, including managed services, to the important or essential entity.*

Section 3, paragraph 10 of the NIS2 Act broadens the scope of cybersecurity to include not only essential or important entities, but also companies connected to them. This has important implications for the security of mobile applications.

What does it mean? That mobile application security is no longer just a matter for individual developers or software development companies. Now, the companies that commission the development of these applications and use them for their own business must also take responsibility for their security.

All players involved, from development companies to user companies, must work together to ensure the security of mobile applications.

4. DATA PROTECTION

GDPR STRENGTHENS

THE ARTICLE

Article 3, paragraph 11 <<scope of application>> :

This is without prejudice to the rules on the protection of personal data set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Legislative Decree No 196 of 30 June 2003, as well as on combating the sexual abuse and exploitation of children and child pornography set out in Legislative Decree No 39 of 4 March 2014.

Data protection remains a priority. NIS2 does not override GDPR regulations, but reinforces them, further emphasizing the importance of keeping data protected.

More and more applications within smartphones convey and manage important fractions of users' lives. In order to make it standard for companies that use apps to do business, NIS2 brings attention back to the issue of personal data.

Carrying out specific tests to analyze the robustness of the structures is essential to be compliant with what is required by the regulations.

5. UPDATES AND MAINTENANCE

ESSENTIAL TO MONITOR DEVELOPMENT AND RELEASE CYCLES

THE ARTICLE

Article 24, paragraph 1, subparagraph 2 letter E <<Obligations in respect of risk management measures for information security>>:

Essential and important entities shall take appropriate and proportionate technical, operational and organizational measures [...] to manage the risks posed to the security of information and network systems [...], as well as to prevent or minimize the impact of incidents for the recipients of their services and for other services.

[...]

The measures referred to in paragraph 1 shall be based on a multi-risk approach, aimed at protecting information and network systems as well as their physical environment from incidents, and shall include at least the following elements: [...] (e) security of the acquisition, development and maintenance of information and network systems, including vulnerability management and disclosure;

NIS 2 speaks clearly: it is mandatory to take all measures to update, maintain and enforce the security of information systems, including mobile applications, and the proper management of vulnerabilities. Updates must be released promptly to fix security holes, and this is only possible through a procedure of continuous monitoring of vulnerabilities in applications with each release.

This is of paramount importance for mobile applications, which once released are effectively out of the company's control.

6. TRAINING AND AWARENESS

INTERNALISING BEST PRACTICES

THE ARTICLE

Article 23, paragraph 2, letters A, B <<Administrative and management bodies>> : *a) are obliged to undergo training in computer security; b) promote the periodic provision of training consistent with that referred to in paragraph a) to their employees, in order to foster the acquisition of sufficient knowledge and skills to identify risks and assess computer security risk management practices and their impact on the entity's activities and services.*

This NIS2 article reminds us that cybersecurity training is not just a duty, but an opportunity. It is not just about learning how to protect data or prevent attacks. It is about understanding how the digital world works, how the applications and mobile devices we use every day can be designed and developed with security in mind. Imagine courses such as ‘Security by Design’ or ‘DevSecOps’, where you learn how to programme securely from the start, not as a step-by-step implementation. And let's not forget training at management level, because security is everyone's responsibility.

While the law article might seem austere, think of it as an invitation to explore, learn and innovate. After all, cybersecurity is a journey, not a destination. And what journey would it be without some learning along the way?

7. MONITORING AND INCIDENT RESPONSE

PREVENTION IS BETTER THAN CURE

THE ARTICLE

Article 35, paragraph 3 <<Monitoring, Analysis and Support>> :

The NIS Competent National Authority, for the purpose of the monitoring activity referred to in paragraph 2, may:

a) request from the subjects a report, also periodical, including self-assessments and implementation plans, on the state of implementation of the obligations set forth in this Decree, as well as the information necessary for the performance of its institutional tasks, stating the purpose of the request;

b) request from the subjects the performance, periodical or targeted, of security audits, in particular in the event of a significant incident or violation of this Decree by the subject;

c) require subjects to carry out security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, if necessary in cooperation with the subject concerned.

This article emphasises the importance of continuous and accurate monitoring to respond to security incidents, including those affecting mobile applications. Security cannot be left to chance: it is essential to perform regular, well-done pentesting to detect and correct vulnerabilities in a timely manner. The frequency and quality of these tests are essential to prevent significant incidents. If the company does not have the necessary in-house expertise, it is equally crucial to collaborate with partners who are experts in the field. Collaboration with external professionals ensures that security scans are based on objective, non-discriminatory, fair and transparent risk assessment criteria, as required by regulations. Maintaining a high focus on security and responding quickly to incidents is crucial not only to protect sensitive data, but also to ensure business continuity and user confidence.

8. COMPLIANCE AND AUDITS

CONTINUOUS MONITORING

THE ARTICLE

Article 34, paragraph 7 <<General principles for the conduct of surveillance and enforcement activities>>:

Periodic and targeted security audits and security scans ... shall be carried out by independent bodies (and shall be based on risk assessments by the NIS Competent National Authority or the auditee or other available risk-related information).

Article 35, paragraph 3, letter b) <<Monitoring, analysis and support>>:

The NIS Competent National Authority, for the purpose of monitoring activities ... may: require subjects to carry out periodic or targeted security audits, in particular in the event of a significant incident or violation of this decree by the subject.

Articles 34 and 35 of the NIS2 transposing legislation emphasise the crucial importance of comprehensive IT security. It is not enough to have a robust infrastructure and up-to-date software: organisations must also ensure that their applications also comply with current regulations. The NIS Competent Authority plays a key role in this process, requiring regular security audits, especially in the event of significant incidents or breaches of regulations. Taking a proactive approach not only helps prevent potential threats, but also ensures that organisations stay one step ahead of emerging risks. Ultimately, these articles are not just an obligation, but a valuable guide to keeping the beating heart of the business safe. Regulatory compliance should not be seen as a burden, but as an opportunity to strengthen cyber resilience and protect the business in the long term.

mobisec

conclusions

MOBISEC FOR NIS2

The implications of NIS2 on mobile application security are forcing a reorganisation of the agendas of those responsible for security in the company; these are issues that cannot be ignored and for which Mobisec offers valuable support in achieving compliance with a combination of key services: we carry out security assessments for your mobile applications, helping you to address vulnerabilities before they become a real compliance issue. By means of **Vulnerability Assessments and Pentesting documented by reports with targeted guidance on how to mitigate the detected weaknesses**, we help you comply with the most stringent security standards, while at the same time strengthening your company's internal mobile application security skills.

AIDA OWASP Gartner Peer Insights CSQA GESTIONE SICUREZZA INFORMAZIONI ISO/IEC 27001 – CERT. n° 7600B

mobisec

staysafe@mobisec.com

Mobisec

Viale della Repubblica 22/III
Villorba (TV)

4010 Moorpark Ave
San Jose, CA 95117

mobisec.com

Keep in touch.