NIS2 DIRECTIVE – PART 2

How companies can achieve NIS2 compliance while driving digital growth

Five key considerations for CISOs, Data Protection Officers, and Compliance Leaders

MIKE FLACHE

NIS2 DIRECTIVE – PART 2

1. Identify, assess, and address your risks

NIS 2 requires management bodies of essential and important entities to take appropriate and proportionate technical, operational, and organizational measures to manage the risks posed to the security of network and information systems and the physical environment. Organizations would do well to identify their risks, assess their impact, and take steps to mitigate them.

NIS2 DIRECTIVE – PART 2

2. Evaluate your security posture

A risk and security evaluation can assist in pinpointing vulnerabilities, such as unmanaged passwords or misconfigured or inactive accounts that are susceptible to credential theft. Organisations would do well to conduct a comprehensive security assessment to evaluate their security posture and identify areas for improvement such as introducing phishing resistant authentication factors.

NIS2 DIRECTIVE – PART 2

3. Take steps to safeguard privileged access

Adversaries can exploit privileged accounts to orchestrate attacks, take down critical infrastructure, and disrupt essential services. NIS 2 advises critical entities to limit access to administrator-level accounts and to regularly rotate administrative passwords. Organizations would do well to take steps to safeguard privileged access by implementing best practices such as least privilege access, continuous authentication, and threat analytics.

4. Strengthen your ransomware defenses

Costly and debilitating ransomware attacks are a major concern for EU regulators and one of the primary drivers of the NIS 2 Directive. Organizations would do well to introduce security solutions and best practices to proactively defend against ransomware. This includes using endpoint privilege security solutions to enforce the principle of least privilege, control applications, and augment next-generation antivirus (NGAV) and endpoint detection and response (EDR) solutions.

5. Move to a Zero Trust strategy

Traditional perimeter-based security architectures, conceived to defend trusted enterprise network borders, aren’t suited for the world of cloud services and hybrid workforces. Organizations would do well to adopt a Zero Trust approach.

NIS2 DIRECTIVE – PART 2

What I learned from my insight into Okta?

- How Okta approaches the topic holistically
- What added value the company's solutions offer
- How Okta is helping to improve the cybersecurity of critical infrastructure across the European Union

Okta white paper

“Why Identity is Important”

Download here