NIS2

Revised EU Cyber Rules for Critical Infrastructure

On November 28th, 2022: The NIS 2 Directive was adopted by the Council of the European Union, replacing the NIS Directive (Directive 2016/1148/EC) in order to **improve cybersecurity risk management**.

Key points of the NIS2 Directive

The directive mainly applies to public and private entities in seven specific sectors (energy, transport, banking, financial market infrastructures, healthcare, drinking water supply and distribution, and digital infrastructures) and across three digital services (online marketplaces, online search engines, and cloud computing services).

One of the key items that the NIS 2 directive highlights is the importance and **requirement** for vulnerability assessment and patch management.

Article 6 of the directive states *"ENISA shall develop and maintain a European vulnerability registry… The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services, and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches, and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated."*

GFI LanGuard can assist organizations in complying with this requirement.

For over a decade, GFI LanGuard has been enabling thousands of businesses across the globe to manage and maintain end-point protection across their network, providing visibility into all the elements on their network, helping assess where there may be potential vulnerabilities, and providing the ability to patch them. The patch management and network auditing solution is easy-to-use and easy to deploy.

Some of the key operations that you can perform through GFI include:

- Automatically **discover all the elements in your network**, including computers, laptops, mobile phones, tablets, printers, servers, virtual machines, routers, and switches.
- Scan your network for **missing patches**.
- Find gaps in common **operating systems**. Identify missing patches in **web browsers** and **third-party software**.
- Identify **non-patch vulnerabilities** by using a regularly updated list of 65,000+ known issues as well as items such as **open ports and system information** about users, shared directories, and services.
- Automatically **deploy patches centrally**, or deploy agents on individual machines. Don't rely on individuals to keep your perimeter patched.
- Control which patches you install and **roll back any patches if you find problems**.
- Install **security patches** not just to fix bugs, but to help applications run better.
- Run automated **network security reports** to help you demonstrate compliance with multiple requirements such as PCI DSS, HIPAA, ISO 27001/27002, and SOX.

For a more detailed overview and free 30-day trial, we encourage you to visit the GFI LanGuard Product page.

GFI Software™