NIS2

Überarbeitete EU-Cyber-Regeln für kritische Infrastrukturen

Am 28. November 2022 wurde die NIS-2-Richtlinie vom Rat der Europäischen Union verabschiedet und ersetzt die NIS-Richtlinie (Richtlinie 2016/1148/EU), um **das Management von Cybersicherheitsrisiken zu verbessern**.

Die wichtigsten Punkte der NIS2-Richtlinie

Die Richtlinie gilt hauptsächlich für öffentliche und private Einrichtungen in sieben spezifischen Sektoren (Energie, Verkehr, Banken, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und -verteilung sowie digitale Infrastrukturen) und für drei digitale Dienste (Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste).

Einer der wichtigsten Punkte, die in der NIS-2-Richtlinie hervorgehoben werden, ist die Bedeutung und das **Erfordernis** der Schwachstellenbewertung und des Patch-Managements.

In Artikel 6 der Richtlinie heißt es: *"Die ENISA entwickelt und unterhält ein europäisches Register der Sicherheitslücken... Register enthält insbesondere Informationen über die Sicherheitslücke, das betroffene IKT-Produkt oder die betroffenen IKT-Dienste, die Schwere der Sicherheitslücke im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, die Verfügbarkeit von entsprechenden Patches und, in Ermangelung verfügbarer Patches eine Anleitung für die Nutzer gefährdeter Produkte und Dienstleistungen, wie die Risiken, die sich aus den aufgedeckten Schwachstellen ergeben, gemildert werden können".*

GFI LanGuard kann Unternehmen bei der Einhaltung dieser Anforderung unterstützen.

Seit mehr als zehn Jahren unterstützt GFI LanGuard Tausende von Unternehmen weltweit bei der Verwaltung und Aufrechterhaltung des Endpoint-Schutzes für ihr gesamtes Netzwerk. Die Lösung bietet einen Überblick über alle Elemente des Netzwerks, hilft bei der Einschätzung potenzieller Sicherheitslücken und bietet die Möglichkeit, diese zu schließen. Die Lösung für Patch-Management und Netzwerk-Auditing ist benutzerfreundlich und einfach zu implementieren.

Zu den wichtigsten Funktionen, die Sie mit GFI ausführen können, gehören:

- Automatische **Erkennung aller Elemente in Ihrem Netzwerk**, einschließlich Computer, Laptops, Mobiltelefone, Tablets, Drucker, Server, virtuelle Maschinen, Router und Switches.
- Scannen Sie Ihr Netzwerk auf **fehlende Patches**.
- Finden Sie Lücken in gängigen **Betriebssystemen**. Identifizieren Sie fehlende Patches in **Webbrowsern** und **Software von Drittanbietern**.
- Identifizierung von **Schwachstellen, die nicht durch Patches behoben werden können,** anhand einer regelmäßig aktualisierten Liste von mehr als 65.000 bekannten Problemen sowie von Elementen
  wie **offene Ports und Systeminformationen** über Benutzer, gemeinsame Verzeichnisse und Dienste.
- **Verteilen Sie Patches** automatisch **zentral**, oder verteilen Sie Agenten auf einzelnen Rechnern. Verlassen Sie sich nicht auf Einzelpersonen, um
  Halten Sie Ihr Perimeter gepatcht.
- Kontrollieren Sie, welche Patches Sie installieren, und **nehmen Sie Patches zurück, wenn Sie Probleme feststellen**.
- Installieren Sie **Sicherheits-Patches** nicht nur, um Fehler zu beheben, sondern auch, damit Anwendungen besser funktionieren.
- Führen Sie automatische **Netzwerksicherheitsberichte** aus, um die Einhaltung verschiedener Anforderungen wie PCI DSS, HIPAA, ISO 27001/27002 und SOX nachzuweisen.

Eine ausführliche Übersicht und eine kostenlose 30-Tage-Testversion finden Sie auf der Produktseite von GFI LanGuard.

GFI Software™