



Tenable and the NIS Directive For Banking, Finance, Health and Digital Infrastructure Sectors

Directive (EU) 2016/1148 (NIS Directive) requires Operators of Essential Services (OES) and Digital Service Providers (DSP) to take “appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems. OES and DSP entities are responsible to determine the specific measures (security controls) to implement. The directive does not require specific measures nor security control frameworks. However, the NS Cooperation Group, composed of representatives from Member States, the European Commission and ENISA has published security measure guidance¹ to help organizations select appropriate measures.

Challenges

Defining “Appropriate and Proportional Measures”

Responsible entities are challenged to define and implement a defensible set of measures. The NIS Directive intentionally did not define “appropriate and proportional measures” because appropriate measures vary by entity and will evolve over time. Fortunately, ENISA² has stepped into the void and has suggested that responsible entities base measures on existing international standards.

Meeting Multiple Member State’s Requirements

Trans-national OES entities may be required to comply with very specific local standards. The challenge is to implement a common set of measures that can be readily adapted to support multiple standards.

Applying Appropriate Measures Across the Attack Surface

Technical measures must address the full range of network and information systems which may include servers, desktops, laptops, network devices, mobile, virtual infrastructure, web, containers and cloud. These diverse technologies make measuring and managing the entire attack surface very challenging. The challenge must be met by cost-effectively implementing technical measures across the attack surface, without deploying and maintaining a multitude of narrowly focused products.

Key Benefits

- **Inventory the Entire Attack Surface**
Gain visibility of all traditional IT, web, containers and cloud assets that comprise critical network and information systems
- **Identify Weaknesses**
Identify vulnerabilities, misconfigurations and other weaknesses that require remediation
- **Prioritize Remediation**
Vulnerability prioritization based on factors such as asset accessibility, availability impact, exploitability and threat intelligence efficiently focuses remediation/mitigation
- **Measure Exposure over Time**
Chart progress over time and highlight possible trouble spots
- **Streamline Reporting**
Provide evidence to National Competent Authorities of effective implementation of security measures.

¹ [Reference Document on Security Measures for Operators of Essential Services](#), CG publications 01/2018

² [Improving the Recognition of ICT Security Standards](#), Version 1.0, December 2017

How Tenable Can Help

Inventorizing the complete attack surface and then removing vulnerabilities and misconfigurations is foundational to any programme to manage the risk posed to the security of network and information systems. It requires Cyber Exposure, an emerging discipline for measuring and managing cybersecurity risk in the digital era. Tenable delivers the capabilities described below to help entities manage risk across their complete attack surface.

Discovery

Knowing what assets you have is foundational to protecting network and information systems. The days of traditional IT are gone. Today's modern the attack surface requires security leaders to consider not only traditional IT assets, but web, container and cloud assets. A comprehensive asset inventory is likely to include network devices, desktops, servers, databases, web apps, virtual machines, containers, mobile, and the cloud.

Assessment

Understanding the cyber exposure of all assets requires frequent assessment of which components are affected by new security vulnerabilities, insecure configurations and other security health indicators.

Analysis

Issues discovered during assessment must be Prioritized to identify vulnerabilities with the highest

impact to your organization. Through a combination of threat intelligence and machine learning the Tenable **Vulnerability Priority Rating (VPR)** ensures remediation efforts are focused on what matters most.

Remediation

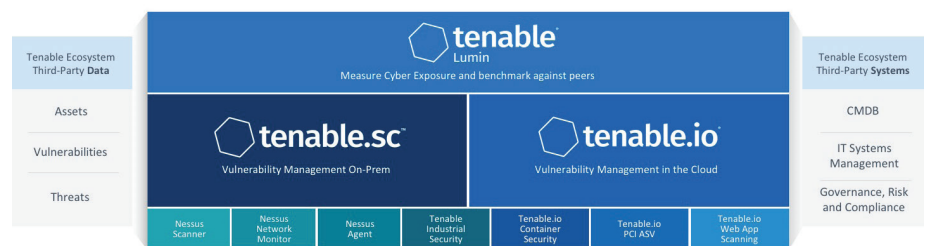
Remediation typically involves rolling out updates and patches. Alternatively, compensating controls may be implemented or the risk may be accepted; and reasons to justify the decision must be documented.

Measurement

Measurement and status reports are essential for self-assessments and for National Competent Authorities to determine whether an organization has met the NIS requirements. For example, reports will help answer the question, "Have the systems supporting essential services been regularly subjected to security scans?"

Tenable Solution

Tenable Cyber Exposure platforms assess, manage and measure cyber risk across the entire network and information system attack surface. Tenable uniquely provides the breadth of visibility into cyber risk across the modern attack surface and the depth of analytics to measure and communicate cyber risk in business terms.



Tenable Cyber Exposure Platform

More Information

Please visit: tenable.com

Contact us: please email us at sales@tenable.com or visit tenable.com/contact

COPYRIGHT 2019 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.