Strengthening Cybersecurity:

A Deep Dive into the Digital Operational Resilience Act (DORA)

Table of Contents

Contents

Introduction

In an era where digital transformation drives business operations, cybersecurity is paramount. The rise in cyberattacks necessitates robust measures to reduce attack surfaces and respond swiftly to threats. Compliance with regulations like the Digital Operational Resilience Act (DORA) is essential to prevent severe penalties and ensure business continuity.

Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554, will take effect on January 17, 2025, for all EU member states. It aims to fortify the cybersecurity frameworks of financial entities and digital products within the EU, ensuring they can handle ICT-related incidents and operational disruptions.

Scope

DORA covers various financial entities, including banks, investment firms, credit institutions, insurance companies, crowdfunding platforms, and critical third-party service providers such as Cloud service vendors and data centers.

Penalties for Non-Compliance

Failure to comply with DORA can result in severe penalties, including daily fines of up to 1% of the average daily global turnover for up to six months, issuance of cease-and-desist orders, and public notices. These stringent penalties underscore the importance of adherence to DORA's requirements.

Key requirements and how WatchGuard supports them

1. ICT Risk Management: Financial entities must establish a comprehensive ICT risk management framework to ensure operational continuity during cyber incidents.

WatchGuard Solutions:

- **Firewalls:** Features like Gateway AntiVirus, IntelligentAV, DNSWatch, Application Control, WebBlocker, spamBlocker, and Network Access Enforcement in VPN detect and block network-based attacks.
- **Endpoint Protection Platforms (EPP, EDR, EPDR, Advanced EPDR):**
  - **Risk Dashboard:** Displays security risk levels on network computers.
  - **Vulnerability Assessment:** Performs automated scans on all endpoints.
  - **Software and Hardware Inventory:** Lists unauthorized software and versions.
  - **Device Control:** Manages removable or mass storage device behavior.
  - **Policies in Advanced EPDR:** Monitors or denies execution of system applications used by threats.
  - **EDR, EPDR, Advanced EPDR:** Continuously monitor endpoint activity while ThreatSync+ NDR monitors network traffic for anomalies and threats, correlating insights to mitigate risks.
  - **Patch Management:** Sets up policies and applies patches to keep systems updated, ensuring continuity by managing the entire patch life cycle.
  - **Full Encryption:** Provides centralized management of full disk encryption, securing sensitive data.
  - **Advanced Reporting Tool:** Offers visibility into network applications, identifying unauthorized or harmful applications.
- **AuthPoint MFA:** Enhances security by requiring multiple verification forms, reducing unauthorized access risk and attack surface.

2. Incident Management: Entities must monitor, manage, and follow up on ICT-related incidents, identifying root causes and taking preventive measures.

WatchGuard Solutions:

- **Firebox, EDR Core, EDR, EPDR, and Advanced EPDR** continuously monitor threats, implement automatic responses, and send incident data to ThreatSync.
- **ThreatSync (XDR)** consolidates all detections, automates incident response, and manages the entire process. It is included at no extra cost in all WatchGuard products.
- **WatchGuard Advanced Endpoint Security Solutions (EDR, EPDR, Advanced EPDR)** feature anti-exploit, contextual detections, and automated services like Zero-Trust Application Service and Threat Hunting Service.
- **WatchGuard Patch Management** automates patch identification and deployment.
- **WatchGuard MDR** offers 24/7 monitoring, threat hunting, detection, investigation, and guidelines for efficient incident response and attack surface reduction.
- **AuthPoint SSO portals** ensure that only authenticated users access critical systems, preventing unauthorized access.
- **AuthPoint** provides real-time monitoring and alerts for authentication attempts, allowing quick responses to suspicious activities.

3. Resilience Testing: DORA mandates rigorous resilience testing, including vulnerability assessments, penetration testing, and scenario-based testing, to ensure financial entities can withstand and recover from cyber threats.

WatchGuard Solutions:

- **ThreatSync+ NDR** can be used to simulate attacks to test network defenses and identify weaknesses.
- **Endpoint Security Solutions (EPP, EDR, EPDR, Advanced EPDR):** Facilitate vulnerability assessments, resilience testing, and forensic analysis.
- **Patch Management:** Continuously identifies and remediates vulnerabilities.
- **MDR:** Provides 24/7 detection, response, and periodic security health reports.
- **Advanced EPDR:** Helps teams simulate attacks, detect weaknesses, and enhance security.
- **Secure Wi-Fi:** Simulates wireless attacks to test network resilience and provides detailed reports.

4. Third-Party Risk Management: DORA mandates managing third-party ICT service providers through contracts addressing security, data protection, and service availability to mitigate risks.

WatchGuard Solutions:

- **Firebox Access Controls:** Limits third-party access to essential areas.
- **ThreatSync+ NDR:** Monitors network traffic for anomalies from vendors.
- **Endpoint Security Solutions (EPP, EDR, EPDR, Advanced EPDR):** Detect threats from third-party suppliers using behavioral detection.
- **MDR and WatchGuard SOC:** Hunt for and detect potential supply chain threats.
- **Orion:** Creates custom hunting rules for supply chain threats.
- **AuthPoint:** Ensures MFA across all third-party services, managing third-party access risks.
- **Secure Wi-Fi:** Provides isolated guest Wi-Fi access, preventing unauthorized access to sensitive resources.

5. Information Sharing: DORA encourages financial institutions to share threat intelligence to enhance collective cyber resilience.

WatchGuard Solutions:

- **Advanced Reporting Tool, SIEMFeeder, IoC Search (Advanced EPDR and Orion):** These tools provide detailed logging and reporting for sharing threat intelligence.
- **ThreatSync (XDR):** Consolidates and correlates threat data for efficient sharing.
- **WatchGuard Cloud:** Centralizes management and generates reports for auditors and supply chain entities.
- **Audit Logs and Event Data Lake:** Maintain detailed logs of network and authentication activities for one year.
- **Reporting:** WatchGuard's Unified Security Platform and products (ThreatSync+ NDR, Endpoint Security Product, Incident reports in Orion, and MDR) provide comprehensive reports for compliance officers and regulatory authorities, supporting compliance and collective security efforts.

In addition to helping comply with the Digital Operational Resilience Act (DORA) with its products and services, WatchGuard's Unified Security Platform strictly adheres to the ISO/IEC 27001:2013 certification audits (view certificate). This certification provides a robust and structured foundation for information security management, which is crucial for DORA compliance. By integrating this certification into its platform, WatchGuard ensures that its solutions meet the highest security standards and facilitate financial institutions' adherence to the stringent regulatory and operational resilience requirements imposed by DORA.

Conclusion

WatchGuard's products are designed to exceed industry standards and help to comply with evolving regulations. Our Cloud-native Unified Security Platform and SaaS products support regular updates and security patches, which are essential for maintaining compliance and securing digital infrastructure.

Key capabilities include:

- **Comprehensive Security:** Covers network, endpoint, and Cloud environments for holistic protection.
- **Simplified Management:** The Cloud platform simplifies security policy management, aiding compliance.
- **Proactive Threat Management:** Automated response and continuous monitoring help prevent cyber threats.
- **Attack Surface Monitoring and Reduction:** Features like ThreatSync (XDR), Application Control, Gateway AntiVirus, and IntelligentAV monitor networks and block threats, while endpoint security and network access enforcement ensure only secure devices connect.

WatchGuard's Unified Security Platform products and services support compliance with DORA requirements, ensuring financial entities maintain a robust and compliant ICT environment through risk management, incident handling, resilience testing, third-party risk management, and information sharing.

Reference Links

- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC)
- The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554
- More information on WatchGuard products

bako tech®

BAKOTECH® is an international group of companies that occupies a leading position in the field of Focus Value Added IT distribution and supplies solutions from the world's leading IT manufacturers. Positioning itself as a True Value Added IT distributor, BAKOTECH provides professional pre- and post-sales, marketing, technical support for partners and end customers. Geographically, the group of companies operates in 26 countries in the markets of Central and Eastern Europe, the Balkans, the Baltic States, the Caucasus, Central Asia, with offices in Prague, Krakow, Riga, Kyiv, Baku and Nur-Sultan.