Rocket® software

Rising Cyberattacks Lead to Regulatory Changes — like DORA

A ransomware attack successfully breached just one of a software company's data centers, impacting a large customer base and pausing a sizeable number of services across Europe. With 91% of mainframe organisations having sustained data breaches or compromises over the last five years — and the regulatory changes mandated by the Digital Operational Resilience Act (DORA) — financial services companies are being required to upgrade, evaluate, and implement innovative systems and protocols to safeguard their data.

Fortify your mainframe with the most pinpointed vulnerability management technology and penetration testing services available in the market.

DORA has decreed that financial services organisations must routinely report and assess their risk. This incites the following:

- Organisations will need to prioritise vulnerability management on the mainframe, issuing regular vulnerability reports and risk assessments to ensure optimal risk management
- The European Central Bank is already administering a cyber resilience stress test — the first of its kind — on 109 directly supervised banks in 2024, preceding DORA's regulation amendments
- Organisations will need to ensure appropriate division of responsibilities and rights for mainframe users, crucial for effective risk management

Safeguard your open-source languages and tools with the fastest and most current support, in line with the NIST National Vulnerability Database and reported CVEs. Securing open-source languages and tools is vital, particularly on the mainframe. Unobserved open-source code can make significant room for cyberthreats, necessitating robust and current support. By utilising technology and support aligning with the NIST National Vulnerability Database, organisations can ensure the swiftest response to potential vulnerabilities.

Preserve critical business data to guarantee business continuity. The mainframe demonstrably needs to be addressed when introducing data recovery processes and technology:

- In January 2025, DORA will mandate organisations to revive their operations within a two-hour window
- It's crucial to have top-notch resources ready to rapidly recover particular datasets from a specific moment in time — and to effectively lessen the impact of an attack or data loss
- With the DORA deadline swiftly approaching, amidst an increasingly complicated regulatory landscape, now is the moment to establish a robust foundation in response to cyberthreats

When collaborating with industry leaders like Rocket Software, you can be confident you'll have the technology, know-how, services, and support required for digital operational resilience and effective risk management oversight. **Speak to a Rocket Software security specialist on how to build a robust foundation for your operational safety and resilience.**

Act now

Rocket® software