

WHAT IS RANSOMWARE AND WHY SHOULD MAINFRAMES CARE?



Ransomware has emerged as one of the most pervasive cybersecurity threats of the digital age, targeting organizations of all sizes and industries. This malicious software encrypts files and systems, demanding payment to restore access. While businesses often focus on protecting their servers, workstations, and cloud environments, a critical yet overlooked target remains at risk: the mainframe. Traditionally regarded as secure bastions of enterprise data, mainframes are increasingly vulnerable to the evolving tactics of cybercriminals.

In this blog, we explore the fundamentals of ransomware, its implications for mainframes, and why organizations must prioritize mainframe security in their ransomware resilience strategies.

What is Ransomware?

The US Cybersecurity and Infrastructure Security Agency (CISA) defines ransomware as "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable." Attackers then demand a ransom, often paid in cryptocurrency, to decrypt the affected files.

The consequences of ransomware attacks are severe and can include:

- **Operational shutdowns:** Businesses may be forced to cease operations, as seen in cases where retail chains and public services experience complete downtime.

- **Financial losses:** Costs include ransom payments, legal fees, lost revenue, and recovery expenses.
- **Reputational damage:** A ransomware attack can erode customer trust and tarnish an organization's reputation.
- **Compliance risks:** For industries with strict regulatory requirements, failing to protect data could result in fines and other penalties.

The myth of mainframe invulnerability

Mainframes are often considered immune to ransomware attacks due to their robust security architecture and isolation from traditional attack vectors. However, this perception is dangerously outdated. Modern enterprise environments integrate mainframes with other systems through interfaces like Microsoft Open Database Connectivity (ODBC) and REST APIs, increasing exposure to ransomware threats.

Consider these facts:

- **Proof of concept attacks:** Security researchers have demonstrated how ransomware can target mainframes, proving their vulnerability.
- **Integration risks:** Mainframes often serve as hubs for critical enterprise data. Attackers can leverage compromised systems connected to the mainframe to launch attacks.
- **Enterprise traffic:** The high volume of data flowing through mainframes makes them attractive staging grounds for distributing ransomware across an organization.

Real-world impacts of mainframe ransomware

Ransomware attacks on mainframes can have devastating consequences. For example, in 2022, [Miller County, Arkansas](#), experienced a ransomware attack where the mainframe was used as a platform to distribute malware across the enterprise. This incident underscores the potential for ransomware to compromise not only the mainframe but also interconnected systems and data.

Organizations relying on mainframes for critical operations in finance, healthcare, retail, and government cannot afford to underestimate these threats. A successful attack could disrupt supply chains, delay financial transactions, or jeopardize sensitive customer data.

Why mainframes must be part of the ransomware strategy

Ignoring mainframes in a ransomware defense plan creates a significant security gap. Here are key reasons why mainframes should be included:

1. **Critical role in operations:** Mainframes handle some of the most sensitive and mission-critical workloads, making them prime targets.
2. **Evolving threat landscape:** Cybercriminals are increasingly sophisticated, leveraging automation and AI to exploit vulnerabilities in interconnected environments.
3. **High stakes:** The potential consequences of a successful ransomware attack on a mainframe extend far beyond data encryption, impacting business continuity and compliance.

Conclusion

Ransomware is no longer a peripheral threat; it's a business-critical issue that demands comprehensive, enterprise-wide strategies. While mainframes have long been considered secure, their integration into broader enterprise ecosystems makes them vulnerable to ransomware attacks.

By acknowledging the risk and taking proactive steps to secure mainframes, organizations can strengthen their overall ransomware resilience. In the next blog, we'll delve into how ransomware targets mainframes and explore the tactics cybercriminals use to exploit these systems. Stay tuned.

Learn more about protecting your mainframe from ransomware attacks in the white paper, "[Mainframe Under Attack: Essential Measures for Ransomware Resilience](#)."