Six Essential Pillars of a Ransomware Prevention Strategy

By Rafeeq Rehman

Ransomware remains a pervasive and profoundly disruptive threat, capable of disabling critical organizational functions through the encryption of vital data and systems. According to the Verizon 2025 Data Breach Investigations Report (DBIR), 44% of all breaches showed ransomware was present making a notable rise from the previous year. This is a 37% increase from last year's report. Ransomware is also disproportionally affecting small organizations. In larger organizations, Ransomware is a component of 39% of breaches, while small- and medium-sized businesses (SMBs) experienced Ransomware-related breaches to the tune of 88% overall.

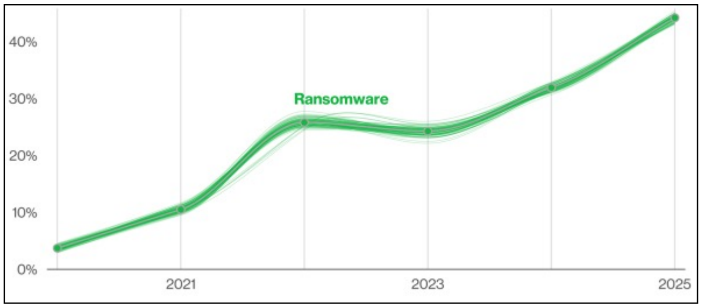


Figure 1: Ransomware action over time in breaches (source Verizon DBIR)

A truly effective defense necessitates a multi-faceted, layered approach that comprehensively addresses both technical vulnerabilities and the human element. Our point of view is that this six-pillar strategy, shown in Figure 2, provides a holistic framework, engineered to build organizational resilience and help significantly mitigate both the risk and impact of ransomware incidents.

1	**Timely and Comprehensive Patching** to fix old a new vulnerabilities
2	**Education awareness** as social engineering remains a primary entry vector
3	**Multi Factor Authentication (MFA)** to defend against stolen credentials
4	**Endpoint Detection Respond (EDR)** as first and last line of defense
5	**Backup and Recovery** capability with multiple copies and immutable backup
6	**Using Network Segments** at macro, micro, application and user level

Figure 2: Six essential pillars of ransomware prevention strategy.

1. Timely and Comprehensive Patching

Patching is foundational to sound cyber hygiene. Recent data indicates a substantial increase in attackers leveraging vulnerabilities for initial network access. The DBIR shows that, despite diligent remediation efforts, perimeter devices often remain susceptible, with a median vulnerability remediation time of 32 days, presenting a critical window for exploitation.

Recommendations

- Establish Robust Asset Management: Begin with a comprehensive inventory of all assets, including devices, applications, third-party libraries, APIs, and mobile applications.
- Implement a Holistic Vulnerability Management Program: Develop and execute a rigorous program for identifying, assessing, and prioritizing vulnerabilities.
- Prioritize Coverage and Timeliness: Emphasize the breadth of patching across the entire environment as critically as the speed of remediation.
- Integrate Third-Party Risk Management: Incorporate vendor security assessments, specifically inquiring about their vulnerability management practices.

2. Cybersecurity Education and Awareness

This pillar directly addresses the inherent human factor in cybersecurity. Social engineering, phishing, and impersonation persist as primary initial entry vectors, particularly prevalent in financially focused industries.

Recommendations

- Acknowledge Human Susceptibility: Recognize that achieving a zero-click rate on malicious links is virtually impossible, with approximately 1.5% of individuals consistently clicking (DBIR).
- Conduct Regular Training and Simulations: Implement frequent, realistic training exercises and simulated phishing campaigns to help reduce user susceptibility.
- Empower User Reporting: Provide intuitive and accessible mechanisms for users to report suspicious emails and potential phishing attempts. This allows an organization to use the power of the human population to catch phishing attacks early and block them before they show up in the inbox of all users.

3. Multi-Factor Authentication (MFA) Implementation

MFA is an indispensable component of modern Identity and Access Management (IAM) frameworks. It helps provide a critical defense against stolen credentials, a pervasive issue highlighted in numerous breach analyses. MFA typically combines multiple authentication factors, such as “something you know,” “something you have,” and “something you are.”

Recommendations

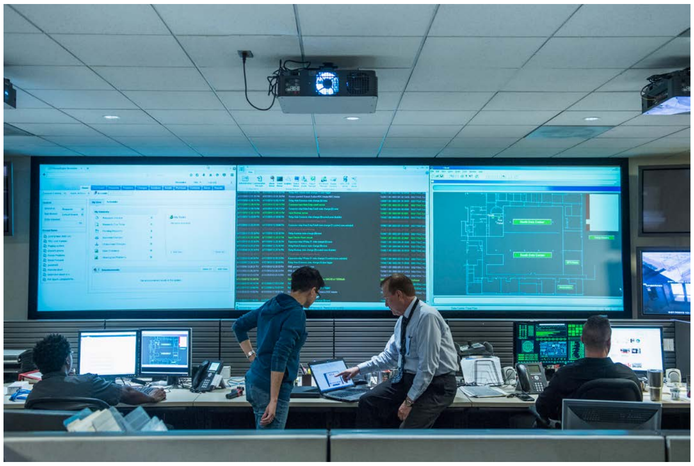
- Mandatory for Remote Access: Enforce MFA as a mandatory requirement for all remote users connecting via VPN or similar technologies.
- Prioritize Privileged Accounts: Leverage MFA to significantly enhance the protection of privileged accounts.
- Disrupt Attack Chains: Recognize MFA as a major impediment to both initial infection and subsequent lateral propagation within the network.

4. Advanced Endpoint Detection and Response (EDR)

EDR solutions serve as both the primary and ultimate line of defense for blocking malware across diverse operational environments, including on-premises, cloud, remote user devices, and mobile endpoints. It facilitates near real-time monitoring and blocking, helping to significantly reduce attacker dwell time.

Recommendations

- Foundation in Asset Management: A robust EDR strategy is predicated on comprehensive asset visibility and management.
- Maximize Coverage: Prioritize achieving maximum coverage across all endpoints within the organization.
- Select Modern, Integrated Solutions: Choose contemporary EDR solutions that seamlessly integrate with threat intelligence feeds, helping to protect against the latest ransomware attacks.
- Phased Deployment: For organizations deploying a modern EDR solution for the first time, begin with detection capabilities and progressively transition to automated blocking modes.
- Integrate with Network Access Control (NAC): Consider integrating EDR with NAC solutions to facilitate the isolation of non-compliant or compromised endpoints, potentially as part of a broader segmentation strategy.



5. Robust Backup and Recovery Capabilities

This pillar is fundamental to organizational cyber resilience. It helps provide the reliable and timely restoration of data and the complete reconstruction of systems following an attack.

Recommendations

- Implement Immutable Backups: Utilize immutable backups across diverse storage mediums, leveraging secure backup vaults.
- Comprehensive Backup Scope: Ensure backups encompass not only data but also applications and system software essential for a complete rebuild.
- Establish Virtual Air-Gapped Cyber Vaults: Create isolated cyber vaults, protected by stringent firewall rules and MFA, to serve as a last resort.
- Regular Validation and Testing: Conduct frequent table-top exercises, auditing, and recovery testing to validate the efficacy and timeliness of recovery processes.
- Align with Recovery Objectives: Ensure backup and recovery strategies are meticulously aligned with defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

6. Strategic Network Segmentation

Network segmentation is designed to limit the spread and blast radius of an attack. It helps effectively reduce the overall attack surface, contain malware, and significantly accelerate recovery efforts. Organizations can start with traditional layered network architectures to achieve macro segmentation as a first step. Micro Segmentation provides granular segmentation at the host, workload, and application levels. For Cloud-Native Applications the recommendation is to explore segmentation strategies tailored for microservices, service meshes, and containerized environments.

Recommendations

- Adopt a Phased Implementation: Begin with a comprehensive application discovery phase to map dependencies.
- Leverage Diverse Technologies: Utilize a strategic combination of network switches, firewalls, virtual infrastructure, distributed firewalls, Kubernetes, and service mesh technologies to achieve effective segmentation at different levels.

These six pillars collectively provide a robust, actionable, and adaptable framework for organizations to help fortify their defenses against ransomware, thereby enhancing their overall cybersecurity posture and ensuring critical business continuity in the face of evolving digital threats.

Conclusions

There is no single tool or technology to safeguard against ransomware. This article outlines a comprehensive, multi-faceted approach to combat the growing threat of ransomware. This strategy emphasizes a holistic framework addressing both technical vulnerabilities and the human element, built upon six key pillars: timely and comprehensive patching, cybersecurity education and awareness, multi-factor authentication (MFA) implementation, advanced Endpoint Detection and Response (EDR), robust backup and recovery capabilities, and strategic network segmentation. Each pillar includes specific recommendations to help enhance organizational resilience, mitigate risk, and significantly reduce the impact of ransomware incidents, ultimately aiming to fortify defenses and ensure business continuity.

To get the latest updates on real-world breaches and help safeguard your organization from cybersecurity attacks visit https://verizon.com/dbir

Rafeeq Rehman loves to write about Cybersecurity and share his experiences. He is the creator of CISO MindMap, a tool to elaborate on complexities of CISO's job. When not working on computers and networks, he enjoys reading classical poetry.