DELL Technologies

Malicious Insider: Strengthening Cybersecurity and Resilience with Dell Technologies

The Rising Threat of Malicious Insider Attacks

Malicious insider attacks have become one of the most pressing cybersecurity threats in today's business landscape. Unlike external threats, malicious insiders already possess a degree of trust and access within an organization, making their actions particularly damaging and harder to detect. From accessing sensitive data to sabotaging systems, insider attacks can cripple critical operations and cause severe financial and reputation repercussions.

Dell Technologies recognizes the growing danger posed by these attacks and develops innovative, scalable solutions to empower businesses in identifying, preventing, and mitigating the risks of malicious insiders. By combining state-of-the-art technology with expert-led services, Dell is helping organizations stay ahead of these internal threats.

What Are Malicious Insider Attacks?

A malicious insider attack occurs when an individual within an organization misuses their access to compromise data, disrupt operations, or extract sensitive information for personal, financial, or competitive objectives. This individual could be an employee, contractor, partner, or anyone with legitimate access to the company's systems and networks.

How Malicious Insider Attacks Work

Malicious insiders exploit their trusted position to bypass traditional security defenses. Common techniques include:

1. **Data Theft:** Exfiltration of confidential customer data, intellectual property, or financial records.
2. **Sabotage:** Purposefully damaging IT systems to disrupt business operations or tarnish reputation.
3. **Credential Abuse:** Using stolen or misused credentials to escalate access privileges or create dummy accounts.
4. **Collaboration with External Attackers:** Sharing access or sensitive knowledge with outside cybercriminals in exchange for financial gain.

This dual advantage of trust and inside knowledge makes malicious insiders exceptionally dangerous compared to external attackers.

The Impact on Businesses

The toll of malicious insider attacks is far-reaching, causing damages that extend beyond financial loss. Businesses may face consequences such as:

Financial Loss

Theft of sensitive information, fraud, or sabotage leads to revenue and recovery expenses that can amount to millions of dollars.

Operational Disruption

System sabotage or data destruction can halt operations, resulting in delays, missed opportunities, and reduced productivity.

Reputational Damage

A breach or attack by insiders erodes client and stakeholder trust, affecting customer loyalty and market perception.

Regulatory Non-Compliance

Depending on the industry, insider attacks can lead to hefty fines and penalties if sensitive data such as healthcare or financial.

Real-World Example

In 2020, an IT contractor working for a major financial institution intentionally deleted critical system configurations, causing network outages for over **10 hours**. This act of sabotage led to **millions** of dollars in financial losses, extensive recovery costs, and reputational harm. Such incidents illustrate the destructive potential of insider threats and emphasize the urgency of robust detection and prevention measures.

Estimated Costs

The average cost of an insider-related incident is estimated at **$4.99 million** and make up almost **55%** of all breaches, according to a 2024 Ponemon Institute study. This figure accounts for detection, recovery, and mitigation expenses, revealing the critical need for organizations to invest in preemptive defenses against insider risks.

83%

of organizations reported at least one insider attack in the past year

Source: 2024: Cybersecurity Insiders' Report

Combating Malicious Insider Attacks with Dell Technologies

Dell Technologies offers a comprehensive ecosystem of tools and services to combat malicious insider threats, ensuring your organization is prepared for the unexpected.

Secure Endpoints with Dell Trusted Workspace

Endpoints often serve as the entry points for insider threats. Dell Trusted Workspace integrates cutting-edge security features into hardware to fortify endpoints and safeguard sensitive data.

- **Dell SafeBIOS** ensures firmware integrity, thwarting attempts to manipulate system operations at the hardware level.
- **SafeID** protects credential data, preventing unauthorized access and credential abuse.
- **SafeData** encrypts sensitive data end-to-end, ensuring that intercepted or extracted information remains unreadable to malicious insiders.

By deploying these solutions, organizations can ensure their endpoints are protected, regardless of whether the threat originates internally or externally.

Proactive Threat Detection with CrowdStrike

Identifying insider threats requires visibility and monitoring of user behaviors. CrowdStrike, integrated within Dell's solutions, utilizes artificial intelligence and behavioral analytics to detect anomalies indicative of insider threats.

For example, abnormal data transfers during off-hours or unauthorized access to critical areas of the network are flagged immediately, facilitating a rapid response. A U.S. healthcare organization recently leveraged proactive threat detection to identify and terminate an employee's attempt to exfiltrate patient data, preventing a costly breach.

Enhanced Data Protection with Dell PowerProtect

Dell PowerProtect provides a robust line of defense through secure backups, air-gapped storage, and immutable copies of critical data. By ensuring that sensitive information is protected from alteration or deletion, insider attacks targeting data integrity can be rendered ineffective.

An example is a manufacturing company that faced a disgruntled employee attempting to sabotage design files. Dell PowerProtect's recovery vault allowed the company to restore operations within hours, avoiding disruptions and maintaining business continuity.

Rapid Incident Recovery with Dell Professional Services

When an insider threat escalates into an incident, rapid recovery is essential. Dell's Professional Services, including Remote Data Recovery and Incident Response, ensure that businesses can recover data and systems quickly. Dell's experts lead the process to minimize downtime and mitigate impacts.

These are just a few examples within the Dell portfolio of solutions that can help with malicious insider threats.

Advanced Network Security and Micro-Segmentation with Dell PowerSwitch Networking & SmartFabric OS

Strengthens defenses against malicious insider attacks by delivering advanced network segmentation, strict access controls, and real-time traffic analytics across your infrastructure.

The Importance of a Multi-Layered Security Approach

An effective defense against insider risks requires more than one layer of protection. Implementing a multi-layered security strategy ensures no vulnerability becomes a weak point. Key steps include:

Key Steps to Enhance Defense

- **Zero Trust Principles:** Continuously verify all access requests and assume no entity is inherently trusted, even within the perimeter.
- **Role-Based Access Controls (RBAC):** Restrict employee access to only the systems and data necessary for their roles.
- **Advanced Encryption Solutions:** Encrypt data in rest and in transit, effectively neutralizing data theft.
- **Employee Awareness and Training:** Incorporate frequent security awareness programs to prevent accidental participation in malicious activity.
- **Regular System Testing:** Conduct penetration testing and vulnerability scans to ensure defenses remain reliable.

These practices, bolstered by Dell's solutions, create a formidable, holistic protection framework against malicious insiders.

Strengthening Defenses Through Strategic Partnerships

Dell partners with industry-leading cybersecurity providers, including **CrowdStrike** and **Secureworks**, to strengthen their solutions further. CrowdStrike enhances endpoint security and provides valuable threat intelligence on indicators of compromise, while Secureworks offers advanced threat detection and response services. These collaborations ensure that Dell's customers benefit from an ecosystem of integrated and cutting-edge technologies.

Why Choose Dell Technologies for Cybersecurity

Dell Technologies continues to set the gold standard for multilayered cybersecurity solutions. Businesses benefit from Dell's industry-leading expertise, deep partnerships, and innovative suite of products that adapt to today's evolving threat landscape. From endpoint security to insider detection to incident recovery, Dell provides a complete framework of resilience that inspires trust and enables growth.

Build a Resilient Future with Dell Technologies

Protect your business against malicious insider threats with Dell Technologies' comprehensive, scalable solutions. By partnering with Dell, you're not just securing your operations but also ensuring business continuity, fostering customer trust, and future-proofing your organization. Contact us to learn more about implementing proactive defenses today.

Dell Technologies is your trusted ally in combating insider threats, safeguarding your critical assets, and empowering your business to thrive in a dynamic digital environment. A future of security is a future of success, and it starts with Dell.

Learn how to address some of today's top cybersecurity challenges at **Dell.com/SecuritySolutions**

Learn more about Dell solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation with #DellSecurity

DELL Technologies