Ten Ways to Defend against Insider Threats

Overview

Cyberthreats aren't limited to hacks and ransomware attacks. An estimated 25% of all enterprise cybersecurity incidents originate inside an organization, according to Forrester. And these threats can come in a variety of forms, ranging from rogue administrators and disgruntled employees with access to sensitive information to poor data hygiene, human error, and even unmonitored, non-human accounts serving as attack vectors. Distributed workforces only add to the complexity by creating endpoint vulnerabilities outside of a network's four walls.

What Can CISOs and IT Leaders Do to Minimize These Threats?

1

Gain Visibility into Systems and Log Data

You need to know what is happening and have forensic readiness if and when the worst occurs. This means having the solutions in place to monitor and analyze your IT infrastructure and applications to troubleshoot issues, identify and prevent threats, data breaches, and downtime.

2

Automate Software Patches and Updates

This practice, commonly called data hygiene, ensures that structured and unstructured data inside of databases or file shares is "clean," meaning it's accurate, up to date, and error free. This can help mitigate human error while driving security, productivity, regulatory and compliance adherence, and efficiency.

3

Prioritize Education about Company Policies and Best Practices for Security

Ongoing, updated education about company policies and best practices for security is critical. This should be role-based and relevant. Let employees know the power they wield in allowing something bad to happen. They should ask themselves "How am I a vector?" to understand what behaviors are acceptable to the company and what social engineering (phishing) attempts look like.

4

Run Data Discovery Exercises and Tailor Security Controls Based on Findings

This can help you understand the level of security that each class of data needs and lessens the need to have all data secured at the maximum level, which can be costly. Increase the security measures on data that's classified (whether personal, critical, or industrial data), then have encryptions or other techniques that can increase the access level to that data when needed.

5

Implement Robust Security Controls

Limit access from regions that you don't have operations in or that are considered high-threat or high-risk. Layer a stack of tools across the environment, so if one control fails, another can compensate. For example, block personal emails to prevent the sending of data at the email level. The same can be done at the network level. Limit employees' access to data from company-owned devices or managed devices at the storage level only.

6 Increase Identity- and Role-based Controls on Sensitive Data

Adopting a zero trust approach to security will limit application access to only confirmed-safe users, systems, and processes. Multi-factor identification can reduce reliance on trust or authentication.

7 Monitor Log Data for Behavior Analytics

Organizations are highly vulnerable without security logs. These can be used to raise alerts on unusual employee activities. By creating a baseline for each user's typical behavior, behavior analytics programs make it easier to spot an anomaly (such as geolocation changes) as a potential compromise.

8 Deploy Threat Prevention Monitoring and Anomaly Detection

Threat prevention monitoring and anomaly detection can continually analyze traffic flows for anomalous signatures that could indicate the presence of malware or the flooding of host computers to cause a denial of service (DoS) or distributed DoS attack.

9 Ensure Users Know How to Report Issues

Make internal security a mandate, and make sure all users understand how they can report issues. A more formal "consequence management" approach may be an option. If users know the policy and know the standards but still go around them, they'll face consequences.

10 Bring High-access Users to the Security Conversation

This is all about sharing responsibility. For engineers, who have higher privilege or higher levels of access across systems, make security part of their remit. Bring them to the table and request they walk you through what they do normally. What is the normal day-to-day process? Based on what they're doing at the moment, introduce security controls and work with them.

Resilience: Make Security Events Non-events

Despite these best efforts, security experts agree that every company's number eventually comes up. What matters most is resilience. How well prepared you are can minimize the damage and speed recovery.

Render attacks non-issues with immutable backups like SafeMode™ Snapshots. and the Pure Storage Cyber Recovery SLA, which guarantees clean arrays shipped, a detailed recovery plan, and support team members to help.

PS2661-01-en 08/24