What is an Insider Threat?

The security risk posed by an enterprise’s employees, associates, partners, contractors, and service providers with access to enterprise resources and data is classified as an Insider Threat. Insider activity is one of the biggest security concerns to enterprise data because perpetrators already operate past the first line of defense.

34% of all breaches involve internal actors.

Negligent insiders compromise enterprise security by neglecting to follow cybersecurity policies. They often fall prey to social engineering attacks.

Inadvertent insiders are employees whose accounts are compromised by external actors. They are unwitting participants in security incidents.

Malicious insiders willfully use their legitimate access to critical data to steal, delete, tamper with, or leak it for revenge or personal gain.

2.9 million records of PII were exposed by a vengeful Desjardins employee.

According to the Data Breach Investigations Report, the primary motivators of data theft are:

- 71% Financial gain
- 25% Espionage
- 4% Other (Negligence, revenge, etc.)

Huge monetary losses: The cost per Insider attack is between $100,000 and $2 million.

Operational disruption: In 2020, the number of exposed personal data records increased 141%, with a loss of $1.2 billion.

Loss of credibility: In 2020, 70% of consumers would stop doing business with a company if it experienced a data breach.

Why are Insider attacks difficult to combat?

- Maximized damage potential: 59% of insiders had credentialed access to the organization’s network and software.
- Extended detection time: On average, insider threat detection and containment takes 77 days.
- Privileged smoke screen: 63% of organizations think that privileged users pose the biggest insider risk.

How to mitigate Insider threats:

- Consolidate user activity reports: The more visibility you have into your Active Directory environment, the better your chances of detecting insider threats.
- Track data usage and movement: Audit all data accesses, including permission changes and data transfers to external storage devices, to detect anomalies quickly.
- Monitor privileged users: A critical component of insider threat detection, monitoring privileged users will help you keep a close eye on users who can cause the most damage.
- Deploy user behavior analytics: Detect, investigate, and mitigate threats like malicious logins, lateral movement, privilege abuse, data breaches, and malware.
- Automate security incident responses: Execute responses such as shutting down machines and disconnecting user sessions to mitigate data breaches.
- Lack of effective detection tools: 17% of organizations do not monitor user behavior at all.

Combat Insider Threats with ADAudit Plus

ManageEngine ADAudit Plus is a UBA-driven change auditor that continuously monitors user activity and provides detailed reports to enhance your insider threat detection strategy.

Explore the insider threat detection capabilities of ADAudit Plus using a free, 30-day trial.

Write to us at support@adauditplus.com to schedule a personalized demo.

Data sourced from: