MIS Solutions

INSIDER THREATS

SPOTTING THE COMMON WARNING SIGNS

According to a recent study, **the human element is involved in over 80% of all breaches.**[1] To protect your business from insider attacks, it is critical that your entire organization understands what these threats are and learns how to spot or identify the common indicators and warning signs before it's too late.

WHO POSES AN INSIDER THREAT?

Anyone with privileged access to inside knowledge of your company's data or information assets, infrastructure and operational strategies could pose a potential security threat.

COMPROMISED OR EXPLOITED INSIDERS

A user whose authorized or privileged credentials were captured via a phishing email or any other breach and used to gain access.

MALICIOUS AND CRIMINAL INSIDERS

Insiders using authorized access to steal/expose sensitive data or deliberately damage/destroy critical systems to intentionally harm the business or for personal gain.

NEGLIGENT OR CARELESS INSIDERS

A user with no aim to steal or jeopardize the business but who unintentionally exposes the company to security risks for the sake of productivity or efficiency.

EXTERNAL OR THIRD-PARTY INSIDERS

Independent or third-party partners, vendors and contractors with access to internal systems and data assets, or those who have "inside" knowledge or information.

Cybercriminals stole login credentials in close to 20% of incidents.[2]

A negligent employee or contractor is the cause of over 50% of reported insider threat incidents.[3]

MOTIVATIONS BEHIND INSIDER ATTACKS

1 FINANCIAL / GREED

Over 80% of breaches are financially motivated.[4]

2 ESPIONAGE / COMPETITIVE ADVANTAGE

In over 20% of incidents, nefarious insiders gained unauthorized access to proprietary information.[5]

3 REVENGE / DISGRUNTLED EMPLOYEE

Disgruntled employees manipulating the company's tools, applications or systems accounted for over 40% of breaches.[6]

4 IDEOLOGICAL / POLITICAL OBJECTIVES

Insiders who oppose a business on political or ideological grounds have platforms like Wikileaks through which they can leak confidential company information that is at odds with their opinions.

PRIMARY BUSINESS ASSETS AT RISK

Business Financials & Account Details

Trade Secrets and IT & Network Systems / Infrastructure

Customer or Employee Data Records

Corporate IP or Program Code & Trade Secrets

CONSEQUENCES

Exposed Customer Data / Lost Trust

Financial Losses / Costs

Disclosure of Corporate IP or Trade Secrets

Brand and Reputation Damage

Regulatory Compliance Fines & Penalties

SPOTTING THE WARNING SIGNS & INDICATORS

While insider threats are often the hardest to detect, there are some common digital and behavioral indicators you should be monitoring for:

BEHAVIORAL INDICATORS

Repeated attempts to bypass security controls or hide or camouflage activities

Working or logging in frequently during "off hours" or the middle of the night

Displaying disgruntled behavior often or for a long period of time

Acting odd, withdrawn or anxious with colleagues or management

DIGITAL INDICATORS

Obtaining or hoarding large amounts of data

Searching for and saving sensitive or protected data

Accessing or requesting access to data assets not associated with their job functions

Using personal or unauthorized portable storage devices (USB, SD Cards)

PROACTIVE DEFENSE: SECURITY & RISK MANAGEMENT PROGRAM

Securing your IT environment from insider threats starts with securing your critical assets, enforcing clear IT security policies, increasing your IT visibility and promoting a culture of change. This is the only way to mitigate and prevent insider threat incidents.

Our team has the specialized tools and experience in IT, cybersecurity and data protection that can bring you peace of mind by securing your IT environment from both insider threats, unintentional or otherwise, and growing external threats.

CONTACT US TODAY TO PROTECT YOUR BUSINESS FROM INSIDER THREATS!

Sources: 1, 4 - 2022 Verizon DBIR
2, 3, 5, 6 - 2022 Ponemon Cost of Insider Threat Global Report

Sales contact information: 513-793-6222 Sales@missolutions.com