INSIDER THREATS

A guide to understanding, detecting and preventing insider security incidents

BomberJacket NETWORKS
651-448-9900 | www.bomberjacket.net
3260 163rd LN NW, Greater Minneapolis-St. Paul Area, Minnesota 55304

INTRODUCTION

Insider threats are a growing concern for business owners and IT experts today. A traditional defense and detection system is highly ineffective at identifying and mitigating these threats. Security threats that originate from within an organization are often the hardest to detect and prevent, especially since an insider has the trust and knowledge of infrastructure systems and data assets as well as authorized access to both.

EVEN THOUGH INSIDER THREATS ARE ON THE RISE, MOST COMPANIES DON'T HAVE PROPER SECURITY SYSTEMS IN PLACE TO DETECT OR PREVENT INSIDER INCIDENTS.

The goal of this eBook is to help you understand what insider threats are and explain the severity of the risks, costs and consequences these threats can inflict on your business. You will also get guidance on how to identify common indicators and warning signs as well as the security controls and strategies you need to prevent or mitigate the risks and impacts of insider incidents.

WHAT IS AN INSIDER THREAT?

An insider threat is a security breach risk situation posed by people from within an organization. An insider can be a current or former employee, or a third party such as a business partner or contractor, who has authorized access to sensitive information and can divulge, modify or delete data records.

Based on the insider's intent, insider threats are often broadly classified into malicious or criminal insiders and unwitting or negligent insiders. Malicious insider threats are intentional, where the insider misuses privilege, trust and knowledge to disclose information for financial or personal gain. Negligent insider threats are unintentional in nature and are caused due to carelessness or human error.

WHO ARE POTENTIAL INSIDERS?

ANYONE WHO HAS AUTHORIZED OR PRIVILEGED ACCESS OR INSIDER KNOWLEDGE ABOUT A COMPANY'S INFRASTRUCTURE, OPERATIONS, CYBERSECURITY PRACTICES OR DATA IS A POTENTIAL INSIDER THREAT.

They could be, current or former:

- Business owners or employees
- Contractors/subcontractors
- Partners
- Vendors

TYPES OF INSIDER THREATS

MALICIOUS INSIDER

The perpetrator could be a disgruntled employee or anyone with malicious intent who exploits their position and privilege to disclose sensitive information for personal or financial benefits, or to deliberately sabotage the company.

COLLUSIVE INSIDER

This type of insider has links with external bad actors whose motive is to compromise sensitive data or steal trade secrets or intellectual property by gaining access into the organization.

NEGLIGENT INSIDER

A regular employee or an unintentional participant whose carelessness leads to a security incident. Many organizations fail to recognize this threat until it's too late.

THIRD-PARTY INSIDER

This type of insider could be a business associate, contractor or vendor who has some level of access to an organization's network and information. They may not be a direct threat but have access to unsecure systems or devices that could easily be exploited by cybercriminals.

COMMON MOTIVATIONS BEHIND INSIDER THREATS

THE REASONS BEHIND INSIDER THREATS VARY. HERE ARE SOME COMMON MOTIVATIONS BEHIND THESE THREATS

MONEY/GREEDSTRATEGIC/COMPETITIVE ADVANTAGE

Financial gain can be a huge motivator for malicious insiders. Whether it's customer information or trade secrets, data is an asset. For a malicious insider with access to an organization's network and information, this is an easy opportunity to make a quick buck.

ESPIONAGE

Sometimes referred to as industrial espionage, economic espionage or corporate spying. It is the act of obtaining sensitive information or trade secrets and sharing it with another party for commercial or financial purposes.

REVENGE

A disgruntled employee or a former employee who joins a competitor can deliberately disclose trade secrets.

An organization could plant a mole in its competitor's company to obtain proprietary or customer information to gain a competitive edge. It could also be an insider sharing classified information to another competitor for personal gain or a departing employee taking confidential documents or customer lists to impress a new employer.

IDEOLOGICAL/POLITICAL/ RELIGIOUS AGENDA

These insiders can be influenced by emotions or extremist moral or religious beliefs. They could also be primarily driven by national pride or have unique political objectives.

WHY YOUR ORGANIZATION NEEDS TO TAKE INSIDER THREATS SERIOUSLY

Since insider threats originate from within an organization, they are hard to detect and defend against, making them very dangerous. Unlike external actors who need access to penetrate an organization, an insider has legitimate access to a company's network and systems. An insider with bad intent can exploit these authorizations and easily bypass security measures to expose confidential information and compromise an organization.

PRIMARY ASSET TARGETS FOR INSIDERS

An insider can divulge sensitive data either deliberately or accidentally, which can be damaging and costly for an organization if it falls into the wrong hands.

Some of the primary asset targets for insiders include:

- Critical operational or programming data for business
- Private customer or employee data
- IP or trade secrets
- Financial data

MANY BUSINESSES ARE UNAWARE OF HOW SERIOUS INSIDER THREATS CAN BE. THEY HAVE A MULTITUDE OF SENSITIVE FILES ACCESSIBLE TO EVERY EMPLOYEE, WHICH SIGNIFICANTLY RAISES THE RISK.

MOST COMMON CONSEQUENCES AND COSTS OF AN INSIDER ATTACK

SOME OF THE COMMON CONSEQUENCES OF INSIDER ATTACKS INCLUDE LOSS OF CRITICAL BUSINESS AND CUSTOMER DATA

Apart from data and revenue loss, insider attacks can have a devastating impact on an organization.

An insider event can put critical business and customer data at risk, which can lead to lost confidence, negative reviews or credential theft.

DISCLOSURE OF TRADE SECRETS

Losing intellectual property, such as trade secrets, blueprints or designs, can lead to a competitive disadvantage. A business rival can leverage the stolen information to get ahead of the competition.

FINANCIAL COSTS AND LOSSES

Insider security incidents can result in significant revenue loss.

REPUTATION AND BRAND DAMAGE

Diminished reputation is a long-term consequence of an insider attack. One successful insider incident can damage even the best of brands and reputations.

WHEN YOUR EMPLOYEES, INDEPENDENT CONTRACTORS, EX-EMPLOYEES OR OTHER BUSINESS PARTNERS LEAK OR DESTROY CONFIDENTIAL DATA OR SABOTAGE IMPORTANT IT ASSETS, IT RESULTS IN SEVERE REVENUE LEAKAGE AND REPUTATION LOSS.

LOSS OF CUSTOMER TRUST AND BUSINESS

This is perhaps the worst consequence of an insider attack. Although organizations can physically or operationally recover from an insider attack, regaining the trust of concerned customers and partners can be difficult.

REGULATORY COMPLIANCE VIOLATIONS AND FINES

An insider threat leading to disclosure of personal information can have serious consequences, including government fines, legal fees, lawsuits and, in some cases, even imprisonment.

LOSS IN MARKET VALUE

An insider threat can have a direct impact on market value. For example, when a group of hackers claimed that they compromised the data of a digital authentication company, it's stock price dropped significantly in just one week.

LOSS OF PRODUCTIVITY

From identification to remediation, an insider incident consumes a lot of time, which can lead to downtime and impact an organization's productivity.

Spotting common indicators or warning signs

Although insider threats are difficult to identify and prevent, there are some common behavioral and digital signs that can help you recognize and stop them before they cause any damage:

Dissatisfied employees, change in attitude, declining performance

Ignores security practices or attempts unauthorized access to data

Frequently in the office during unusual working hours

Agitated or displays negative behavior towards colleagues

Violates company policies

Shows dissatisfaction towards work, talks about resigning or new opportunities

DIGITAL/NETWORK INDICATORS

- Downloads, accesses or transfers unusually large amounts of data
- Attempts to access confidential data that's not related to one's job role
- Makes constant requests to gain access to tools and resources not required or associated with one's job functions
- Uses unauthorized storage devices like USB drives
- Collects or copies files from classified folders
- Emails confidential information outside the organization

PREVENTATIVE DEFENSIVE STRATEGIES

To err is human. No doubt, human error is one of the most prevalent security threats that businesses face today. Therefore, an insider threat management strategy and regular employee training are the best defense against these threats.

Here is a list of security controls and best practices that can help prevent and detect insider threats:

01 Regular risk assessments: Organizations must identify and evaluate the potential dangers of a security incident, determine its critical assets and implement appropriate risk management measures to protect those assets.

02 Require identity authentication: Implementing two-factor (2FA) or multifactor authentication (MFA) will fortify security controls by verifying user identity via multiple unique factors before granting access to systems or sensitive data records.

03 Access and permission management: Granting only the bare minimum user permissions or systems and data access required to perform a job reduces the risks of unauthorized access, especially those that can result from exposed or stolen privilege credentials.

04 Security awareness and insider threat training: Organizations should periodically educate employees on data security, security policies and procedures, and common security threats.

05 Establish ‘baseline’ activities or behaviors: Establish this within your organization to take advantage of automation and machine learning.

06 Ongoing/continuous monitoring: Monitoring employee online activity as well as any suspicious behavior can help detect threats and prevent security incidents from occurring.

07 Data backup and recovery solutions: Organizations should implement efficient backup and recovery solutions to avoid costly downtime and severe consequences of insider threats.

PARTNER WITH AN IT AND CYBERSECURITY SPECIALIST

Insider threat incidents continue to rise, making every organization vulnerable. The unfortunate truth is that anyone with 'insider access or knowledge' poses a potentially serious threat to your business. This is why managing insider incidents all by yourself can be quite a challenge.

Your business can benefit greatly from partnering with a cybersecurity and IT expert. They have the experience and specialized tools to not only help implement necessary security controls and employee training measures, but also detect and mitigate your exposure to insider threat risks.

To find out how you can efficiently mitigate and prevent insider threats to secure your organization's data, network and employees, contact us today!

651-448-9900 | www.bomberjacket.net
3260 163rd LN NW, Greater Minneapolis-St. Paul Area, Minnesota 55304