Are These Top Insider Threats Lurking Behind Your Doors?

vivitec

www.vivitec.net

The Dangers of Insider Threats

Many business owners - and the IT professionals they rely on - focus on protecting their companies from external threats – the lone hacker out for a large ransom, the industry competitor pilfering secrets, or organized cyber-criminals with sophisticate phishing schemes, etc. But what about internal threats?

Organizations sometimes fail to consider the true risks that insiders pose to their cybersecurity. Yet, internal risks are every bit as dangerous and damaging as the external ones, even if there is not malicious intent.

The 2019 IBM Cost of Data Breach survey revealed that 24 percent of all data breaches in the past five years were the result of negligent employees or contractors.[1] Another report, Insider Data Breach Survey, found that 60 percent of executives felt employees who made mistakes while rushing to complete tasks were the primary cause of internal breaches. Another 44 percent pointed to a lack of general awareness as the second most common reason, and 36 percent cited inadequate training for their organization's security tools as a close third.[2]

To drive home the full harm of insider threats, we've compiled five actual case studies of internal actors who've wreaked financial and reputational damage when they got careless, or abused their knowledge and positions for personal gain.

[1] Cost of a Data Breach, IBM, 2019

[2] Insider Data Breach Survey 2019, egress, 2020

Case 1: The Careless Employee

Sometimes employers don't do enough to educate their workers about cybersecurity best practices, and sometimes employees fail to heed recommended security protocols:

> A report by a company's chief security officer discovered that one of the organization's techs was using duplicate credentials across multiple accounts and failed to set up two-factor authentication on at least two of his accounts.
>
> Though the company recommended these two security best practices – do not use the same log-in for more than one account and apply two-factor authentication for additional protection – the employee neglected to do so.
>
> This weak security enabled hackers to easily infiltrate the company's network where they disabled and deleted all data backups – local and cloud. After sabotaging the organization's backups, the hackers then installed ransomware and demanded payment. Without a usable backup, the company was forced to pay the ransom to recover its data.

What You Can Do

Set up automatic scans to check each clients security settings on each machine to ensure that your IT security policies are being enforced. Generate an automatic alert when two-factor authentication is not turned on where it should be.

Case 2: The Sneaky Former Employee

The knowledge that trusted employees gain about your business doesn't get turned in with their resignation. Employees can become threats after they move on:

> An engineer quit his job to start his own business that would be in direct competition with the company he left. According to court documents, the engineer hacked his former company's server using a former co-worker's stolen credentials. Once inside the network, he was able to retrieve AutoCAD files, design schematics, project proposals, and budgetary documents – all information that could provide a competitive advantage over his former employer. The value attributed to proprietary information he stole was between $250,000 and $550,000.
>
> For his efforts, the engineer was sentenced to 18 months in prison and two years of supervised release.

What You Can Do

Establish "exit procedures" for employee turn-over that includes the immediate removal of ex-employees from Active Directory. Scan the network daily for suspicious log-in attempts by ex-employees and others, and generate an alert for each incident.

Case 3: The Compromised Third-Party Vendor

An “insider” doesn’t have to be located directly within your walls to become a threat to your network. Trusted third-party vendors may have enough access to your network and data to be unknowing conduits for external hackers and do damage to your network:

> A hacker infiltrated a billing collections agency and gained access to patient information that belonged one of the agency’s clients: a healthcare laboratory. Almost 12 million patient records were compromised, including credit card numbers and other personal identifying information.
>
> A security firm that tracks compromised data found 200,000 patient payment details from the billing company for sale on the dark web. Fortunately, the lab had insurance in place to cover some of the potential cost and liability as a result of the breach.

What You Can Do

Set up internal IT security policies that limits storage of credit card and other personal identifying information, and includes additional security levels for access. Regularly scan the network for any suspicious log-in attempts and generate alerts to investigate.

Case 4: The Deceptive Spouse

Spouses share as much information as business partners, maybe even more. When those relationships turn sour, the secrets shared in private can be used for personal gain:

> When a business owner's spouse began an affair with the owner of a competing business, the spouse sought to use insider knowledge to benefit the competitor. The spouse attempted to log into the company computer with the intent of downloading the client database.
>
> Fortunately, the network had an insider threat detection program that identified this uncharacteristic behavior and sent out an alert regarding the anomalous login. An internal investigation occurred, revealing the attempted hack as well as the affair. Divorce followed shortly afterward.

What You Can Do

Scan the network regularly for anomalous log-ins and generate alerts to examine any suspicious activity. An insider threat protection system that uses machine learning to establish baseline end-user behavior trends can help determine when investigations are necessary.

Case 5: Unsupported Legacy Software and Devices

Sometimes insider threats are caused by failure to act, rather than an employee doing something bad. Out-of-date devices and software typically do not receive critical security updates and patches, rendering them open doors for hackers:

> A massive cyberattack penetrated a software vendor's IT management systems through a legacy IP scanner tool and compromised an unknown number of end-user client servers.
>
> Some clients had administrative superuser accounts created within their Windows active directory, so unidentified intruders had full access to their systems and data long before detection.
>
> The vendor admitted, "We still have no way to know what sort of malicious software or gateways may have been left behind nor what data has been stolen, which absolutely could lead to additional problems and liability concerns for us in the future."
>
> More than two months after the attack, the full extent of the damage was still unknown.

What You Can Do

Scan all networks daily, looking for software that is missing the latest security patches, and generate alerts for machines that need updating.

The Internal Protection You Need

As a reputable MSP, we understand cybersecurity and its significance to today's small businesses. Looking for internal cybersecurity threats is more challenging than managing threats from the outside.

We offer formidable insider threat detection and issue alerting that can accommodate any budget and networks of any size. We have specialized security software that runs a daily non-intrusive check of each computer on your network, and alerts us when it detects these kinds of insider threats, and more.

Contact us today to get protected.