The accidental hacker

While malicious employees generate more press, error and negligence are the real insider threats

There was a time when IT security's main preoccupation was to build an impenetrable barrier around corporate systems.

Keep hackers out. Keep data in. Perpetually patch and fortify to ensure that systems, users, and intellectual property stayed safe.

The problem security professionals face today is the creeping rise of vulnerabilities occurring inside the wall.

We tend to associate insider threats with malicious employees who steal information, sabotage IT systems, or manipulate data. But just as significant is the damage done by negligence and error.

As powerful as headline-grabbing breaches can be in terms of focusing minds, their spectacular nature may also make insider threats seem exceptional. In fact, it's the mundane, day-to-day nature of the issue that CISOs need to focus on. Much less exciting perhaps, but potentially just as damaging.

The danger within

While hacks and attacks tend to drive most discussion around IT vulnerabilities, breaches enabled by negligent employees and suppliers pose the more persistent threat. With their access to systems and assets, insiders can wreak more serious damage than outsiders. This can include loss of intellectual property, disruption to operations, sinking customer confidence, reputational damage, and leaks of sensitive information to third parties, including the press.

Awareness of the issue is growing, but many organizations – nearly a third in a study by the SANS institute[1] – still don't have adequate safeguards to detect or prevent attacks involving insiders.

If anyone is still in denial about the magnitude of the threat, consider that of the 57 percent of global organizations that have an information security policy, and while 81 percent of them have communicated it to their employees, only 39 percent believe those employees understand it, according to NTT Security's Risk: Value 2018 Report.[2] Freedom of Information requests sent to UK data protection watchdog, the ICO, reveal that staff mistakes accounted for almost half of all breach incidents reported over the past couple of years.

39%

Only 39 percent of global organizations believe employees understand their information security policy

[1] *SANS Institute: Insider Threats and the Need for Fast and Directed Response, 2015*
[2] *NTT Security Risk: Value 2018 Report*

Perhaps an indicator of how seriously some companies are taking the insider threat is the emergence of Zero-Trust Networking. It's an approach that assumes trusted zones have become a legacy concept in information security that is no longer fit for purpose.

Zero-trust may however be a difficult concept for some companies to implement, since organizations have to trust employees at some level. It may well conflict with an organization's ethos, employer branding, or pace of digital transformation.

Types of insider threat

The type of threat posed by employees or other privileged insiders differs according to a number of factors. There are three main categories — all of them potentially damaging:

1. **Accidental insider threat**
   Even the most loyal employee is capable of making a mistake. Accidentally cc'ing a competitor on your organization's P&L statement could easily happen when autofill is left on, and ten contacts in your Outlook list have similar first names. Accidents will happen. The question is, how do you deal with them and what steps can you take to decrease their likelihood?

2. **Negligent insider threat**
   Negligent insider threats are often the result of trying to work both efficiently and at speed, a combination that can result in skirting established IT security protocols. We've all seen the dialogue boxes from corporate IT telling us to download new software; or install new browser versions, and security patches. How many colleagues ignore these? How many others wouldn't hesitate to install software from unauthorized sources, primarily to help them be more efficient at work?

3. **Malicious insider threat**
   Safeguarding the company's assets against a highly-motivated malicious inside actor is difficult. Exfiltration of proprietary company information to a new employer is an increasingly common practice. The more senior the employee, the more access they are likely to have to sensitive company information, and the more damage they can do.

An emerging twist in this category is the rise of malicious cooperation between outside actors and employees. According to researchers at threat intelligence firm IntSights,[3] hackers are now actively trying to recruit employees – effectively weaponizing them for crimes related to insider trading and bulk theft of credit card numbers. Worrying as that development is, negligence and error remain the most prevalent forms of insider threat. Since the beginning of 2016, only a quarter of the insider breaches supported by NTT Security's Incident Response Team have been from overtly hostile activity. The rest were accidental or the result of simple negligence.

For more on common insider threat profiles and associated risk mitigation techniques, see **NTT Security's Global Threat Intelligence Center (GTIC) Quarterly Threat Intelligence Report, Q3 2017.**

Creating a culture of insider threat awareness

Given the scale of the threat posed by simple negligence, it is essential to create and sustain a culture of insider threat awareness across the organization – that is - a set of normative security behaviours that persist even when no one is looking.

According to NTT Security's Global Threat Report (GTIR), phishing has become one of the most popular ways for malicious actors to launch advanced info-stealing attacks, which could suggest poor levels of user security awareness.

Executive leadership is needed to drive cultural change, as is HR's ongoing involvement. A top-down approach demonstrates the importance of security for the organization's strategic, long term, overall well-being. HR's role is to embed security-awareness in recruitment, training, and professional development.

'As HR practitioners, we play a vital role in helping create a secure-aware organization where integrity, diversity and collaboration are core values that shape our approach to security awareness,' says Heather Scallan, Senior Vice President of Human Resources, NTT Security.

'We do this by ensuring all our employees are engaged, making security part of their performance focus, so they understand the importance and feel empowered to act as secure-aware advocates who can re-endorse the right behaviours.'

Challenges to colleagues should be conducted in an engaging way. The objective would be to encourage and enlighten, rather than condescend or demean.

It's worth noting that board-level leaders are also being targeted in attempts at social engineering that aim to win their trust over time and trick them into providing sensitive information or access credentials. In new human vulnerability tests conducted by NTT Security on behalf of clients wanting to evaluate their risks from all angles, we found that senior management compromised organizational security in as little as ten minutes.

[3] *IntSights 2017: Monetizing the Insider: The Growing Symbiosis of Insiders and the Dark Web.*

'As HR practitioners, we play a vital role in helping create a secure-aware organization... ensuring all our employees are engaged, making security part of their performance focus, so they understand the importance and feel empowered to act as secure- aware advocates who can re- endorse the right behaviours.'

HR departments should work with CISOs, executives and management at all levels to lead by example, customize training and consider what kinds of insider threat workers in a particular operation might encounter, so they can be on the lookout.

'It's about partnering with the CISO to achieve the right balance between actual training and ensuring a culture where risk-aware behaviour is the norm rather than the exception,' adds Scallan.

Seeing is defending

The first thing any organization needs in order to catch an insider threat is visibility of risk indicators on the network. If we think of firewalls as tech sentries at the gate, visibility is the guard dog patrolling inside and sniffing for anomalies. Internal network traffic, access logs, and policy violations all need to be monitored continuously for suspicious activity.

Understanding what a regular day looks like on your network is a good place to start. Are there lists of people expected to access sensitive information as a normal part of their day-to-day duties? Do you have a clear idea which applications are normally used in regular operations? Anything that falls outside those bounds should be investigated. Network visibility of threat indicators means being able to identify anomalous behaviours: for example, unauthorized system or folder access, violation of security policies, data loss, or data hoarding.

Robust risk assessment is crucial

To effectively mitigate all the types of insider threat, you must understand your organization's level of susceptibility to them. Undertaking a robust risk and vulnerability assessment will determine how prepared you are to prevent, detect, and respond.

A foundational first step in IT risk assessment is to identify and locate the organization's key information assets - the most critical in terms of data, IP, and systems. This business context can be integrated into any detection tools and will enable companies to adopt a more mature, risk-based prioritization approach to incident response.

The next step will be to identify technical vulnerabilities, business process gaps, management issues, and honestly rate your ability to analyse the human behaviours that can signal a nascent or actual threat.

Our experience shows that the insider threat problem is complex; as such, you need to adopt an assessment methodology that encompasses people, policies, practices, and technologies.

Services and solutions worth considering

User behaviour is traditionally monitored via active directory, user logs and web proxies. Limiting an organization's insider threat defense to these controls, however, will not enable timely detection of vulnerabilities created by the wide range of errors and policy skirting that occurs every day.

In addition to cultural change initiatives, capturing the indicators of an insider threat will require advanced tools such as Endpoint Detection and Response (EDR) and User Entity and Behaviour Analytics (UEBA).

However, organizations are struggling to invest limited resources in the required people, processes and technology Designing a security-focused change initiative may also require skill sets not normally present in in-house teams.

One option to consider is a managed security service that can shorten the gap between detection and response and combine the use of contextualized threat intelligence and advanced analytics to improve accuracy. Methods and tools to detect insider threats could include anomaly detection techniques such as machine learning or behaviour modelling.

And if the worst does occur, having a critical incident response plan in place will enable the correct use of the right tools and techniques to mitigate the threat, regardless of whether the threat originates from an external or internal source. Worryingly, the NTT Security Risk: Value 2018 Report indicates that only just over half the companies surveyed (57 percent) have an incident response plan in place.

With this in mind, working with a managed security service provider (MSSP) can bring valuable real-world experience from other markets and technology environments.

Conclusion

When we think of insider threats, we inevitably imagine the likes of a Julian Assange or Edward Snowden, and spectacular leaks of confidential information with vengeful or ideological motivations. But while a WikiLeaks-type threat is well understood, an intense focus on malicious threats risks missing out all the other vulnerabilities which carry huge potential for harm. Gaining visibility of negligent human behaviours that inadvertently create vulnerabilities - and changing them - must move to the top of the CISO agenda for the foreseeable future.


NTT