Companies wrestle with growing cyber security threat: their own employees

Businesses deploy analytic tools to monitor staff as remote working increases data breach risk

By Hannah Murphy - May 12 2020

As cyber criminals and hackers ramp up their attacks on businesses amid coronavirus-related disruption, companies are also facing another equally grave security threat: their own employees.

Companies are increasingly turning to Big Brother-style surveillance tools to stop staff from leaking or stealing sensitive data, as millions work away from the watchful eyes of their bosses and waves of job cuts leave some workers disgruntled.

In particular, a brisk market has sprung up for cyber security groups that wield machine learning and analytics to crunch data on employees' activity and proactively flag worrying behaviours.

"We're seeing people say, 'I need better visibility into what my employees are doing with all of our data at home'," said Joe Payne, chief executive of cloud security group Code42, which tracks and analyses employees' activity on work devices. The group examines factors including when an employee typically works, what files they access and how much data they download.

" [Employers can ask] — if we have 10,000 employees, can you tell us who the most high-risk people are?" he said, adding that his company was handling a rise in cases of data theft among clients.

Insider threats

According to Mordor Intelligence, the $1.2bn data loss prevention market is set to balloon to $3.8bn by 2025, as many businesses migrate their data to the cloud.

So-called insider threats encompass employees unintentionally sharing private data outside of workplace networks, but also the deliberate stealing of data, typically motivated by financial opportunity or a grudge against an employer. Rarer, but a growing issue, is intellectual property theft and espionage on behalf of foreign governments.

Already more than a third of data breaches involve internal actors, according to a 2019 Verizon analysis of more than 40,000 incidents. At an exclusive meeting of top corporate cyber security heads at RSA, one of the largest cyber security conferences earlier this year, delegates labelled insider threats as their number one concern, according to one person in attendance — above nation state activity and threats from cyber criminals.

Traditionally, groups such as McAfee have offered tools that detect and block the exfiltration of sensitive data automatically. But there are also newer groups that seek to proactively alert employers to anomalous activity through behavioural analysis of data — which can involve screenshots and keystroke logging — and then place the onus on those employers to act in a way they see fit.

Falling under this category, Code42, Teramind, Behavox and InterGuard all told the Financial Times that they were seeing a rise in interest from potential clients under lockdown.

"There is an increase [during this pandemic] in people trying to steal intellectual property — reports or valuable HR data, client lists," said Erkin Adylov, chief executive of artificial intelligence group Behavox, which in February raised $100m from SoftBank's Vision Fund 2.

Its software analyses 150 data types to produce insights about employees' behaviour, including using natural language processing of email and workplace chats to assess "employee sentiment", he said. "Maybe there is uncertainty about [whether] the people are going to [keep] their job," Mr Adylov added.

"The market is moving very fast. I would say it's probably growing at a clip of 100 per cent a year. The demand is outstripping supply," he said.

State adversaries The risk of nation states opportunistically grooming employees for cyber espionage purposes is also a growing threat, several experts said. The issue was thrust into the spotlight recently when US officials last year charged two Twitter employees with mining data from the company's internal systems to send to Saudi Arabia.

"If I were a nation state actor [involved in cyber espionage] . . . certainly this is an opportunity to exploit some realities that exist. This is a heightened environment," said Homayun Yaqub, a senior security strategist at cyber group Forcepoint.

Executives at Strider Technologies, which wields proprietary data sets and human intelligence to help companies combat economic espionage, said it was seeing more recruitment of foreign spies, particularly by China, take place online under lockdown, rather than at events and conferences. "We're providing [customers] with the capability to respond to that [changing] adversary tactic," said chief executive Greg Levesque.

Nevertheless, critics argue that the technology is still nascent and further investment is needed to develop a more accurate understanding of what risky patterns of behaviour look like.

And while employers have long been able to legally monitor emails and web activity for signs of external cyber security threats, for some there is a discomfort about the privacy and trust implications of using such tools on staff.

"It's intrusive, it's not very culturally palatable," said former US army intelligence sergeant and former Palantir executive Greg Barbaccia. "To me, the insider threat is a cultural human problem. If someone wants to be malicious . . . you need to solve the human problem."

Omer Tene, vice-president of the International Association of Privacy Professionals, said: "Data breaches have been a huge issue. It's understandable why businesses would want to protect against that. I wouldn't be alarmist.

"But you need to be aware as a business and a technology of the creepy line," he added. "Are you doing anything . . . unexpected that will trigger backlash?"

I - Defining vocabulary. Write a personal definition for these words.

Breach : _____

Leak: _____

Migrate: _____

Insider threat : _____

_____

II - True or False? Correct the false statements

	True	False
Some companies are facing a security threat from their own employees under lockdown		…… …… ……
There is a growing market for cybersecurity groups that process data on employees' activity		…… …… ……
Cloud security group Code 42 tracks and analyses employees' activity on their home computers.		…… …… ……

The data loss prevention market is predicted to increase its revenue from $1.2bn to $3.8bn by the end of 2020.		…… …… ……
People who steal data are usually doing it on behalf of foreign governments.		…… …… ……
Typically, employees steal intellectual property such as reports, HR data and client lists.		…… …… ……
Under lockdown, the recruitment of foreign spies takes place at events and conference rather than online.		…… …… ……
Critics of cyber security say the technology is still new and needs more investment.		…… …… ……

III - Expression

1. Is it right for companies to spy on their own employees? Give reasons for your answer.

_____
_____
_____
_____
_____

2. What methods could and should companies use to protect sensitive data ?

_____
_____
_____
_____

3. You are the IT specialist of a medium structure. Present a do's-and-don'ts' list for your colleagues in the framework of your cybersecurity policy.

Do's	Don'ts

IV – Final Task (evaluated)

You will create an original poster or video-clip that must sensibilize your co-workers about your company's cybersecurity policy, what must be done and avoided.

V – Vocabulary

Authentication, Botnet, BYOD, Data Breach, Clickjacking, Deepfake, DDoS, Domain, Encryption, Exploit, Firewall, Hacker (Black Hat), Hacker (White Hat), Trojan Horse, Malware, MFA, PenTest, Pen-testing, Ransomware, Rootkit, Social Engineering, Phishing, Spoofing, Spyware, Virus, VPN, Worm.

	The process of identifying a user's identity, making sure that they can have access to the system and/or files. This can be accomplished either by a password, retina scan, or fingerprint scan, sometimes even a combination of the above.
	a network of computers that have been infected with a virus, and now are working continuously in order to create security breaches. These attacks come in the form of Bitcoin mining, sending spam e-mails, and DDoS attacks.
	The result of a hacker successfully breaking into a system, gaining control of its network and exposing its data, usually personal data covering items such as credit card numbers, bank account numbers, Social Security numbers, and more.
	a favourite Black Hat tool. Using multiple hosts and users, hackers bombard a website with a tidal wave of requests to such an extent that it locks up the system and forces it to temporarily shut down.
	A series of computers and associated peripherals (routers, printers, scanners), that are all connected as one entity.
	Coding used to protect your information from hackers. Think of it like the code cipher used to send a top-secret coded spy message.
	A means of attack on a computer system, either a series of commands, malicious software, or piece of infected data. Note that in this context, it is a noun, not a verb.
	Any technology, be it software or hardware, used to keep intruders out.
	Any hacker who attempts to gain unauthorized access to a system with the intent to cause mischief, damage, or theft. They can be motivated by greed, a political agenda, or simply boredom.
	A hacker who is invited to test out computer systems and servers, looking for vulnerabilities, for the purposes of informing the host of where security needs to be buffed up.
	describes a wide variety of bad software used to infect and/or damage a system. Ransomware, worms, viruses, and trojans are all considered this. It is most often delivered via spam emails.
	A scam where a hacker poses as a legitimate business or organization (especially credit card companies, banks, charities, Internet providers, other utilities) in order to fool the victim into giving them sensitive personal information or inducing them to click a link or attachment that ends up delivering malware
	A form of malware that hijacks your system and encrypts your files, denying you access to them until you send money to unlock everything
	when a hacker changes the IP address of an email so that it seems to come from a trusted source.
	A form of malware used by hackers to have an overview of your computer activities. If a mobile device such as a smartphone is infected, a hacker can read your text messages, redirect your phone calls, and even track down where you are physically located!
	Yet another form of malware, this one a misleading computer program that looks innocent, but in fact allows the hacker into your system via a back door, allowing them to control your computer.
	Malware which changes, corrupts, or destroys information, and is then passed on to other systems, usually by otherwise benign means (e.g. sending an email).

	a method of connecting a series of computers and devices in a private encrypted network, with each user's IP address being replaced. Users get Internet anonymity, making it difficult for hackers to attack.
	Malware that can reproduce itself for the purposes of spreading itself to other computers in the network. Particularly nasty, they can either be simply a means of slowing down a system by eating up resources, or by committing exploits such as installing back doors or stealing data.
	a collection of programs or software tools that allow hackers to remotely access and control a computer or network. Although they do not directly damage users, they have been used for other purposes that are legal, such as remote end-user support. However, the majority of them can open a backdoor on the targeted systems for the introduction of malware, viruses, and ransomware. Typically, it is installed without the victim's knowledge via a stolen password or by taking advantage of system flaws.
	company policy that permits, encourages, or mandates employees to access enterprise systems and data using their own personal devices, such as laptops, tablets, and smartphones, for work-related activities.
	An approach to security evaluation where manual exploitations and automated techniques are used by attack and security professionals. Only environments with a solid security infrastructure should employ this advanced kind of security evaluation with a mature security infrastructure.
	is a growingly popular way to access restricted resources, instead of breaking in or utilizing technical hacking techniques. This strategy relies on user manipulation and human psychology. An employee might get an email purporting to be from the IT department in order to deceive him into disclosing private information rather than trying to uncover a software weakness in a company system.
	when someone is tricked into clicking on one object on a web page when they want to click on another. In this manner, the attacker is able to use the victim's click against them. It can be used to enable the victim's webcam, install malware, or access one of their online accounts.
	A piece of audio or video that has been altered and changed to make it seem authentic or credible. The most perilous aspect of the prevalence of deepfakes is that they can easily convince individuals into believing a particular tale or idea, which may lead to user behaviour that has a greater impact on society at large, such as in the political or financial spheres.
	makes it more difficult for hackers to access your account by requiring you to provide at least two different credentials. It requires a second factor to confirm your identity in addition to your username and password, such as a one-time security code, a fingerprint scan, or a face recognition scan.
	simulates a cyberattack on your computer system to look for weaknesses that could be exploited. It involves attempting to get into any number of application systems (such as frontend/backend servers, APIs, etc.) in order to find security holes like unsanitized inputs that are vulnerable to code injection attacks.