7 Ways to ensure a data breach does not happen to you

By Fortinet global security strategist Derek Manky

143 million. The number of US consumers potentially affected by the recently announced credit services data breach is staggering. It's nearly half the US population. And as a credit reporting service, this data includes names, addresses, financial histories, social security numbers, banking information, and even driver's license numbers. It may take years to fully understand and resolve all of the potential personal and financial implications.

The data that was stolen in this attack is especially valuable. Credit cards are cheap and easy to replace, and subsequently have little resale value on the DarkNet. But the data targeted in this case is different. It includes everything a criminal enterprise would need to establish a lucrative identity theft operation, like the one that Fortinet's FortiGuard team helped Interpol uncover last year in Nigeria. In similar cases that FortiGuard has followed, we have seen such data used for things ranging from identity theft to money laundering, and even the financing of terrorism.

For the company hit by this attack, the financial impact will be equally massive. Within hours of the announcement a class action lawsuit was filed. More will likely follow. Their reputation will also likely be affected, and banks and lending institutions that rely on – and pay for – their credit services may be reluctant to touch potentially corrupted information. There are already a number of cybercrime bills working their way through US legislation. Because this is a hot topic, elected officials are likely to be outraged and demand stricter regulations and oversight that could affect the entire industry. And consumers who may potentially end up paying billions for services to help them resolve identity theft issues are likely to hold the company accountable.

Breaches like this often happen when network security is focused on the perimeter, but doesn't adequately protect the network interior. Security professionals have long referred to such perimeter-focused security – whether at the physical edge of the network or data centre, deployed to defend web-based services and applications, or protecting the cloud – as "hard and crunchy on the outside, soft and chewy in the middle." In such a scenario, attackers who are able to crack the hard candy shell surrounding the data have free and often undetected access to the tasty nougat inside.

Meanwhile, in addition to wondering whether or not people were individually affected, the other question being asked in board rooms across the country today is what can organizations do - right now - to make sure this doesn't happen to them? Here are seven critical places to start:

1. Prevent Compromise By Practicing Good Hygiene

Far too many organizations have neglected their basic patch and replace security hygiene. Networks are growing rapidly and span a variety of ecosystems, from IoT to the cloud. Establishing and maintaining an inventory of devices can be challenging. Given the number of successful attacks over the past few months that targeted vulnerabilities for which patches were readily available, and the millions of organizations that were affected as a result, regardless of how hard this may be, patching isn't optional.

It is imperative that every organization establishes and maintains a formal patching and updating protocol. Ideally, this would be automated, tracked, and measured. In addition, a process needs to be implemented to identify and either replace or take offline those systems that can't or that can no longer be patched.

2. Protect Your Network By Creating And Using Signatures

While new attacks are a real risk, most breaches are actually caused by attacks that have been around for weeks, months, or sometimes even years. In fact, the vast majority of attacks we see target known vulnerabilities for which a patch has been available for an average of three years. And many target vulnerabilities as much as ten years old. And because these vulnerabilities are known, attacks and exploits targeting those vulnerabilities can be detected using signatures. Signature-based detection tools allow you to quickly look for and block any attempted infiltration, or the

execution of an exploit targeting known vulnerabilities.
Signature-based tools are also increasingly effective against complex issues like zero-patch environments, such as IoT and other interconnected devices that are increasingly being adopted by organizations and that have been shown to be highly vulnerable to attack.

3. Detect And Respond To Zero Day Threats By Using Behaviour-Based Analysis

Of course, not all threats have a recognizable signature. New sophisticated attacks utilize a number of techniques to circumvent protections and evade detection. Behaviour-based security tools are designed to look for covert command & control systems, identify inappropriate or unexpected traffic or device behaviour, disable things like zero-day malware variants via detonation chambers/sandboxing, and correlate data to identify and respond to advanced threats.
As attacks become more sophisticated, and attackers begin integrating things like AI to improve their ability to penetrate defences while evading detection, security will need to continue to evolve as well. Advances in intent-based security, for example, will not only check and inspect data and applications crossing into the network for malware, but will provide deep inspection. They will look for patterns and then continuously monitor that traffic in order determine intent, allowing intelligent security systems to proactively intervene and thwart an attack before it has even begun.

4. Deploy Web Application Firewalls

While many attacks still leverage tried and true methods for infiltrating a network, such as email-based phishing or targeting known and unpatched vulnerabilities, many threats no longer enter the network through traditional avenues. Web-based attacks are increasingly common, often exploiting the exponential growth in applications – especially those designed to query and mine for information directly in the data centre.
Because the demand for homegrown and customized web applications has grown so rapidly, many organizations simply do not have the time or resources to adequately test and harden the applications and servers they are deploying. An effective way to close that gap is by implementing a Web Application Firewall (WAF). These security devices are specifically designed to provide deep, high performance inspection of web application traffic far beyond what is provided by traditional NGFW technology.

5. Leverage Threat Intelligence

Advanced threat intelligence enables organizations to shrink the time to detect threats and close the gap between detection and response. There are a number of threat feeds available that keep organizations up to date regarding the latest threat trends and detected exploits. The challenge is converting this data into usable intelligence and cross-correlating it with your local intelligence and infrastructure. And deploy tools such as SIEM and WAF technologies that can consume that data, convert it into actionable policies, and apply it to protecting your network.
At the same time, consider joining a local ISAC (Information Sharing and Analysis Centres), especially one designed for your industry or architecture, where you can receive relevant threat intelligence and share what you see with your industry peers.

6. Avoid Point Solutions

Given the rapid expansion of networks, their dynamic and elastic nature, and the shift from a single perimeter to dozens or even hundreds of potential access and data exchange points, the traditional security strategy of deploying point security devices or platforms at the edge of the network or data centre is no longer adequate. Further, traditional point security technologies tend to be isolated, which means they can only see and respond to the threats that pass in front of them.
But given the nature of today's advanced, multi-vector, and highly intelligent threats, security solutions need to be interconnected into a single, cohesive system that can span and adapt to elastic network architectures. This dynamic integration provides transparent visibility across the entirety of the network, which is critical because you can't defend against a threat you can't see. In addition, a system of integrated, orchestrated security solutions enables organizations to proactively and intelligently fight cyberattacks wherever they occur.
An integrated security framework, like the Fortinet Security Fabric, connects security tools so they

can share and correlate information, and enables centralized orchestration, single pane of glass management, and consistent policy distribution. More importantly, it also enables a coordinated response to attacks, automatically hardens security and access points, isolates affected devices and malware, identifies vulnerable or compromised systems, and initiates forensic analysis and remediation.

7. Segment Your Network

Given the fluid nature of device access, and the wide-ranging flow of applications and data across many of today's networks, it is more important than ever that you establish and maintain effective and secure network segmentation that prevents threats from spreading horizontally across your network. Organizations can dramatically improve their security by deploying Internal Network Segmentation Firewalls to prevent the proliferation of threats, regardless of whether they managed to breach the security perimeter or compromise an access point, or originated internally. ISFWs may sit in front of specific servers that contain valuable intellectual property, protect a set of user devices or web applications sitting in the cloud, or secure traffic moving between logical divisions of responsibility or lines of business inside an organization.

In the case of a data model where massive amounts of data are collected and correlated in a single environment, it is especially critical that segmentation controls be established that can detect threats that have managed to penetrate the perimeter of the data centre and are now moving laterally through that environment. Without segmentation and detection tools in place, such threats are free to collect, corrupt, and exfiltrate data. Internal segmentation, micro segmentation, and controls that track and monitor things like behaviours and workflows are essential for today's data-centric digital businesses.

While the scale of this data breach is alarming, the attack they suffered is not unique. Far too many organizations have adopted state of the art network designs and yet still rely on isolated second-generation security solutions and strategies to protect them. More than ever, security cannot be an afterthought. It requires planning, people, and processes combined with adaptive security technologies that can dynamically scale to today's digital networks and automatically respond as a single, integrated system to address the advanced cyberthreats targeting them.

/ENDS.