BIZCOMMUNITY

The DNA of cybersecurity failure

By Martin Potgieter

8 Oct 2018

Cybersecurity has become one of the most important aspects determining the safety of companies, governments and individuals in the modern age.

Martin Potgieter is technical director at Nclose

Headline-grabbing examples of major cybersecurity breaches have become increasingly commonplace, from the Sony Pictures hack in 2014 that points to a hostile foreign government to the exposure of as many as 110 million Target customers' credit card details due to sophisticated hacking techniques and inadequate response capabilities - not to forget on-going allegations and high-level investigations into Russia's influence over the 2016 US Elections.

Even South Africa's defence minister recently made a public statement that the government is aiming to improve and enhance its cyber defence capabilities in the wake of growing threats to public and private data and infrastructure. As pressure on public and private sector organisations grows to protect sensitive data more effectively, the chorus of vendors promising that their security solutions can just be plugged in and provide automated 100% security - a so-called "plug-and-protect" approach - grows.

But are plug-and-protect cybersecurity solutions truly effective at dealing with the growing complexity of modern cybersecurity? Unless they're being implemented effectively, I would argue a resounding "No".

Defining cybersecurity failure

In the case of Target, hackers gained access to sensitive customer credit card data through an elaborate scheme that was detected by its cybersecurity vendor's plug-and-protect solution. Failure occurred when the alerts pointing to the breaches were not acted upon.

As in most cases, cybersecurity failure is not in being breached – this is an inevitable part of doing business in the modern age, where you either have been breached or will be breached. Target's true failure was to not react to the alerts that notified them of a breach, which delayed their ability to respond, and left their systems - and their customers - severely exposed.

In the case of US consumer credit reporting agency Equifax, more than 145 million consumer credit records were exposed in what was later termed “possibly the worst leak of personal info ever”. Here, it took the company more than five weeks to disclose the breach, and even then the response was weak, with a website set up to help consumers understand whether their details were exposed having more in common with a phishing site than an official company response. Human error and inefficiency, more than anything, amplified the fallout from these breaches.

Plug-and-protect not a good bet

What these examples teach us is that possibly the biggest cybersecurity risk rests with companies’ and people’s complacency. Had Target not assumed that their boxed cybersecurity solutions would automatically protect them from threats, they would arguably have paid more attention to the alerts and have been in a better position to respond quickly. Today, vendors are claiming their “AI-enhanced” cybersecurity solutions take care of security while you take care of business. This is a dangerous falsehood.

Plug-and-protect solutions are appealing because the functionality the vendors are selling is expensive to develop in-house and, with a prevailing skills shortage, easier than sourcing the team of experts needed to do the same task. With the new wave of “AI-enhanced” solutions, companies are once again running the risk of putting their cybersecurity at the mercy of vendors instead of putting in the hard work to customise solutions for their IT environments, interpreting information from multiple sources and uncovering insights into risks and vulnerabilities.

The evolution of defence

Cyber defences have evolved greatly over the past two decades. In the 1990s, firewalls and anti-virus software were introduced, but provided little room for customisation, leaving companies at the mercy of vendors to ensure they were adequately protected. In the early 2000s, Intrusion Prevention Systems and Security Information and Event Management (SIEM) required companies to adapt the solutions to their specific needs, but arguably few companies did any customisation. The introduction of sandboxing (2008) and End-Point Detection and Response (2012) gave security professionals an additional information stream for analysis, which can reveal malicious behaviour or malware attempting to breach their systems.

While these technologies do improve cyber defences, what is needed to make them truly effective is something that ties all the elements together, what I term “defence engineering”. Defence engineering not only ties your cybersecurity solutions together, but it adds innovative inputs to your detection, brings response in as an integral part of your defence, and utilises the power of automation without negating the role of humans.

Managed Detection and Response (MDR), the latest and arguably most effective means of building powerful cybersecurity capabilities, is built to focus on threat detection instead of plug-and-hope-for-the-best. MDR brings next-generation detection capability and advanced analytics to actively seek out threats, and while some automation is used, it doesn’t exclude human intervention to monitor networks. What truly sets MDR apart though is its strong focus on response: remote incident response forms part of every MDR service agreement, and leaves room for on-site incident response during times of crisis.

Companies around the world are paying attention: Gartner predicts that 15% of midsize and large corporations will use MDR services by 2020, a major increase from the 1% currently using them. Isn't it about time you took a more effective

approach to detecting and responding to cyber threats?

ABOUT THE AUTHOR

Martin Potgieter is technical director at Nclose.