BIZCOMMUNITY

Why are CIOs and CISOs positions becoming more challenging?

By Pieter Engelbrecht

31 Oct 2018

CIOs and CISO's across industries are regularly moving between positions and companies because of a common mistake.

Source: pixabay.com

It's your worst possible nightmare. A hacker has breached the company's network and shut down its operations. Millions in revenue is being lost. And the even worse part – you're blamed.

This is becoming an all too familiar scenario for CIOs and CISOs tasked with securing their companies' networks. No sooner have they entered an organisation and put security systems in place, then they find themselves blamed for a successful breach of the company.

So, where does it all go wrong?

Network visibility is not a nice-to-have

Most CIOs or CISOs allocate their funding towards securing their data centre. However, when it comes to implementing a system that provides them with full visibility of their network, they consider it simply a nice-to-have.

So they implement basic security elements like a firewall and assume they'll be OK. But, in reality, should an attack happen at the edge of the company's network, they only way they can possibly know is by doing a deep dive to investigate each and every occurrence that might indicate a breach.

The DNA of cybersecurity failure

Martin Potgieter 8 Oct 2018

We all know this simply isn't possible though. When a user is locked out of their account, the IT department will rarely ever take the time to investigate why. They simply unlock the account and move on to the next problem.

It's true that when a user is locked out, it might be because they forgot their password, but it could also be an indication of something far more sinister.

Every lock-out is a potential attack

Aruba recently had a case, for example, where a client kept on getting locked out of their system. Not realising there was a problem, they kept unlocking the system and moving on.

Recognising and preventing modern cyber scams

Doros Hadjizenonos 22 Oct 2018

That is until one Sunday morning when around 1000 lock-outs occurred simultaneously. On taking the matter up we discovered that these lock-outs were a direct result of hackers attacking the network in order to access sensitive information.

And, the most concerning part of all this was that the devices being used to launch the attacks were, in fact, the company's own devices. When we investigated further, we found that these devices had actually been stolen some time ago.

Your greatest vulnerability is unguarded

So while CIOs essentially have no idea if and when attacks are happening at the edge, this is exactly where an organisation's greatest vulnerability lies. Think of the average digital environment today – thanks to IoT, there are more connected devices than there have ever been before.

Each device is a potential gateway for a major breach. And think of the consequences of the massive data breaches which have been occurring across the world. Millions are being lost on a regular basis.

One only needs to take a look at the statistics to see the odds of escaping one of these attacks are not good. In fact, according to the 2016 Global Megatrends in Cybersecurity report, 67% of companies with critical infrastructure suffered at least one attack during the course of those 12 months.

How can CIOs and CIS's secure their positions?

The only way a business can possibly remain secure under these circumstances is if the CISO or security team receives notifications as soon as something occurs on the network that is deemed to be out-of-the-norm.

Essentially an end-to-end system that can detect attacks and respond rapidly is vital. And it needs to cover the entire network from the data centre to the edge.

Aruba, for example, has an end-to-end solution comprised of ClearPass and IntroSpect. ClearPass provides companies

with proper network access control and is device agnostic, which means it can cover everything from a company's vending machine to industrial IoT equipment.

On the other hand, IntroSpect is an analytics solution that sits on top of a company's security solutions, for example its firewall. Based on its analyses of these solutions IntroSpect creates profiles for individual users. Then if activity takes place on the network which is outside of a user's typical profile, it immediately alerts the security officer.

Say for example, a particular user typically logs into the company network from South Africa between 08h00 and 22h00, but then one day that user logs in from Russia at 02h00, IntroSpect will immediately know something is wrong. And it can take this analysis as far as detecting when a user is typing more slowly to how they would normally.

Then once IntroSpect identifies a network intruder, ClearPass automatically kicks them off the network.

Combined these two technologies effectively ensure CIOs have, not only visibility, but also complete control of their entire network.

It's the only way to truly ensure you aren't the next CIO a network breach sends packing.

ABOUT PIETER ENGELBRECHT

Pieter Engelbrecht is the business unit manager at Aruba, a Hewlett Packard enterprise company.
- How autonomous IT and security solutions will enable proactive IT departments - 11 Apr 2019
- Creating a GDPR Compliance Framework with security tech - 26 Mar 2019
- Why are CIOs and CISOs positions becoming more challenging? - 31 Oct 2018
- Mitigate WAN complexity with SD Branch - 18 Sep 2018
- Securing the enterprise network with artificial intelligence - 21 Nov 2017

View my profile and articles...