BIZCOMMUNITY

The White House ushers in a new era of cybersecurity

By Stephen Kreusch

8 Jul 2021

The United States has been reeling from several major and highly-publicised security breaches. Most recently, a ransomware attack prevented operations at the Colonial fuel pipeline. Last year, hackers believed to be directed by Russian intelligence services infiltrated SolarWinds, a popular IT management software vendor used widely by the US public sector and many private sector companies. Affected companies included Microsoft, Intel and Cisco. The US Treasury, Justice and Energy departments were also impacted. And earlier this year, Chinese-linked attackers targeted hundreds of thousands of Microsoft Exchange mail servers worldwide.

Source: Unsplash

These incidents represent the tip of the iceberg, and they occur everywhere, not just against the US. Fortunately, the security world isn't complacent. The cybersecurity industry has developed some excellent countermeasures such as multi-factor authentication (MFA), endpoint detection and response (EDR), and models like zero-trust security.

But whoever said: "Build it and they will come," was wrong, at least concerning cybersecurity.

Let me give an example. You likely use multi-factor authentication often, probably through your bank. It will send you an SMS with a unique code or ask you to accept a prompt on your phone. You'll notice MFA in many places, such as your Gmail account. It's very effective, but it's not used nearly as widely as it ought to be.

How CISO's should remediate a ransomware attack

7 Jul 2021

If I told you that your home would be safer with a security gate in front of your locked door, you'd see the value of that. Yet, we tend to become very picky in the digital world and justify why we don't need a seemingly obvious security feature. We

see that gate as an obstruction to us, not the characters we want to keep out.

I understand the reluctance. Cybersecurity can be complicated, and complicated can lead to high costs and low effectiveness. There are other considerations, such as ageing computer systems or how security measures could annoy users and dampen productivity. So organisations play it safe, and the free market doesn't push certain security features aggressively enough. If it isn't broken, why fix it? Except, it's very broken in terms of cybersecurity.

Two common but opposing mindsets adopted by organisations are to deal with a breach when it happens and try to survive vs proactively planning for compromise and adopting best practices, and deploying the right security solutions. Most companies opt for the former, hoping they won't be targeted - a terrible strategy. Cybercriminals are equal opportunists, attacking everything from governments to mom and pop shops. We have to be more proactive, and a new order from the White House puts some muscle behind that intent.

An executive order by the White House

In response to recent breaches, US President Joe Biden signed an executive order that determines best security practices for software companies wishing to do business with US federal departments and agencies. It mandates the use of MFA, endpoint detection and response and encourages zero-trust security - an approach that treats all data interactions with suspicious scrutiny. The order also removes barriers around sharing breach information, enabling the left and right hands to know what each is doing. It establishes a Cyber Safety Review Board to review significant incidents, similar to how the National Transportation Safety Board investigates aircraft crashes, leading to safer aviation.

Compared to previous orders and standards, this one is quite aggressive and prescriptive. It will have an impact. The US government is a large technology customer with considerable procurement power, and the security improvements that arise from the executive order will benefit other security customers.

South Africa should take note

I hope other countries, including South Africa, are taking notice. We've been very progressive with legislation such as the Protection of Personal Information Act (PoPIA). As our country rapidly adopts digital systems, clear guidance from the top will help our public and private sectors to make themselves and their users more secure.

Why should we take the lead and not wait for the US order to create change? The South African government uses many local companies that design custom software and might not have a reason to worry about what happens in North America. If we released a similar benchmark, it would help secure the public sector, the largest spender on ICT in the country, and influence the local tech sector to be more security conscious. Several state organs have a say on security, but a message from the top can provide clear benchmarks and expectations that others can strategise and implement.

Breaches in the USA make headlines. But cybercrime strikes everywhere. Hopefully, the White House's executive order will add clarity and direction to get the job done, helping secure our digital futures. If we do the same, South Africa will take

another step into becoming a leading digital society.

ABOUT THE AUTHOR

Stephen Kreusch is the cybersecurity director of Performanta.