The need for zero trust in cybersecurity

By Graeme O'Driscoll

30 Aug 2019

Cybersecurity in an age of such rapid technological advancement has brought one incontrovertible fact to the fore: it's now a case of when a cybersecurity breach will happen rather than if. With this certainty comes another non-negotiable - that the industry requires a paradigm shift towards a zero trust model.

Graeme O'Driscoll

I recently participated in a roundtable with Theo Watson, commercial attorney for Middle East and Africa at Microsoft, and Shaun Durandt, general manager of HMD Global (Nokia), and although we shared a healthy debate about key issues affecting cybersecurity, we did agree that as technology and security advances, so do cybercriminals and attackers who find more innovative and sophisticated ways to crack it.

This means that end-users, organisations, vendors and regulators effectively need to get ahead of these cybercriminals – and the best way to do so is to start by adding layers of security that make it significantly harder for these criminals to breach.

Multi-factor authentication, for instance, is already gaining traction as a viable solution. Combined with the implementation of different levels of protection – from requiring a user name and password to needing facial recognition or a fingerprint for access right through to encryption of data – and this forms the foundation of securing a consumer's or company's data and devices.

These layers, while absolutely critical, should be accompanied by a zero trust model, where users trust nothing and

aggressively verify other people's and company's identities. Businesses and consumers alike should be vigilant about being lulled into a false sense of security – they should see it as inevitable that they will get compromised.

The trick to surviving a breach is making the amount of time between breach and detection as short as possible. This, together with the multiple layers of security measures that have been put in place to monitor and correct breaches, will serve as the differentiator between those who are able to recover from the cost and reputational implications of an attack and those who don't. This means ensuring the ongoing upgrading of the latest security measures.

Bringing all players around the cybersecurity table together

Regulations of course also play an important role in minimising the damage caused by cyberattacks. Legislation like the GDPR (General Data Protection Regulation) has been introduced to protect the data privacy rights of the ordinary man in the street and reshape the way organisations use data.

Regulations like these are intended to minimise the risk of a crisis like the Cambridge Analytica scandal, where millions of people's personal data were harvested without their consent to target them with political adverts.

In order for regulations to successfully prevent such episodes or any of the breaches that appear so regularly in the headlines, there is a need for multi-stakeholder engagement and commitment to cybersecurity. Technology typically outpaces legislation, so it is essential for multiple players – from regulators to vendors to business and consumer end-users – to play their roles to ensure security is a priority.

Central to ensuring that each stakeholder is able to play their role is education: consumers and companies tend to only consider security when they have been breached, so they need to be educated to change their behaviour through the zero trust model.

Vendors and regulators, on the other hand, need to be educated about what the security needs of the end-user are so that these can be built into the applications and systems. This becomes even more important in the age of the cloud, where location doesn't matter. Applications and systems simply need to work well in the cloud era – and be as secure as possible.

Even with security built-in – and in layers comprising multi-factor authentication, facial recognition, fingerprint access and encryption – enterprises and consumers alike need to take responsibility for their security.

Ultimately, this brings the crux of the cybersecurity issue back to the zero trust model. Zero trust, together with the latest security measures and regulations is the crucial weapon in the evolutionary arms race that is cybersecurity.

ABOUT THE AUTHOR

Graeme O'Driscoll, Head of R&D - Cyber Security at Internet Solutions