Photo: Pxhere

The enemy within

by **Mark Rodbert**, *CEO, idax Software*

It seems that the peak of data breaches is upon us, with a different story hitting the headlines each day – although I've been saying that every year since 2015. When imagining where the threat is coming from, most people picture a hooded hacker in a dark room or a state-sponsored covert operation. As a consequence, most organisations are focussing their defence on implementing solutions to prevent intruders from getting in, relying heavily on solutions such as firewalls or antivirus protection. But what about the people who are already in and pose a threat to the internal security of the organisation?

It turns out that the real threat lies a lot closer to home, with 66% of organisations considering malicious insider attacks or accidental breaches more likely than external attacks, according to the 2018 edition of the CA Technologies' *Insider Threat* report. Whether they are the result of bad actors attempting to sell sensitive company data, collusion, or unwitting accomplices using a work laptop on a Starbucks Wi-Fi, most breaches are simply a matter of access and opportunity.

Ultimately the outcome is the same, whether the intent is malicious or not. But, if we can identify who has access to what data and applications, and which of these are out of the ordinary, maybe there is a way to prevent internal threats after all.

An inside job

Clearly, an external threat is still a priority for businesses, and it's no surprise with many well-known enterprise businesses, like T-Mobile, Facebook, and Google, all facing damaging external cyber breaches last year. Yet, this shouldn't distract companies from the internal threat, which can be just as damaging; *Insider Threat* reported that 90% of organisations feel vulnerable to the insider threat, and the majority of employees have access to data they shouldn't. However, an insider threat becomes an external threat when compromised access is used by unscrupulous attackers. By tightening up the internal security vigilance, controls, and access processes, external hackers will find it harder to break through and entice staff with a phishing email.

So what can businesses do to start building their cyber defence to insider threat? Unfortunately, the answer is not as easy as simply implementing a new security system or process. Companies need to recognise the need for a cultural

idax
identity analytics

Using identity analytics, idax is the world's leading company in automatically analysing the access rights for an organisation, quantifying the risk, and determining who has excessive access requiring adjustment. Protecting digital information is critical for modern companies. Most cyber fraud is committed by employees. As technology becomes more complex, knowing whether or not someone should have access to systems is beyond the capability and knowledge of managers and traditional systems. What is required is a new approach. Using proprietary algorithms, idax enables organisations to manage access changes in real-time, making it possible to dynamically enforce the principle of 'least privilege'. For more information, please visit www.idaxsoftware.com

INSIDER THREAT

PRESENTED BY: ca technologies

Scan the QR code to directly access the 2018 edition of the CA Technologies' Insider Threat *report*

shift and change in attitude, to the point where everybody in the organisation understands that cyber security is their responsibility. In order to change the culture around protecting assets, organisations need to make everyone – from the CEO to the person at the door – feel responsible, involved, and empowered, putting employees at the front of the fight. This requires building tools not just available to the IT security department but targeted at the whole organisation.

However, we're discussing a transformational change which won't take place overnight but over a significant period so that each individual comes to recognise the part they play. The first phase of this is access management being the job of specific security teams. The issue here is that employees feel as though it's a job for the security or IT team, and has nothing to do with them.

The next phase, which is becoming increasingly widespread among organisations, is steering away from having just the security team tackle the cyber issue and instead putting line managers in charge of access rights. Currently, this often involves the line manager having to deal with a highly complicated, confusing access details spreadsheet, with no context or explanation about what in the list refers to what data and what files are required for a role. Moreover, the risk with reviewing access to assets is asymmetric. If access to something that an employee does need is taken away, there is a very high chance of a small issue. However, if somebody keeps access to something they shouldn't have, there is a very small chance of a huge breach. Human beings need help comparing these risks.

In the long run – the eventual third phase of this shift – companies can look to become part of the security revolution that will see everyone in a company self-certificating their own access rights, with oversight and ultimate approval from line managers. With an engaging, end-user-friendly user interface, employees are encouraged to take responsibility for their own actions and aim to be as secure as possible.

Step your cyber skills up now!

2019 is looking like it may be the year for organisations to finally take a step back – or in fact, step *up* – and analyse their own internal security measures. The internal threat is and always has been overlooked as a significant cyber threat. Why wait any longer to crack down on your internal security? By implementing software to manage access rights, employers can start their journey to change company culture towards security immediately. ■