PRIVILEGED ACCESS MANAGEMENT

Dave Adamson *reports on security from within and what's required to take the next great cyber-security step*

In today's age of technology pervasion, news headlines are rife with stories of data breaches, the actions of opportunistic cyber criminals and the financial implications of poor security hygiene. The threat landscape is constantly getting wider and the ever-increasing amount of data that businesses are tasked with holding means that – theoretically at least – there are more holes in a company's cyber security net than ever before.

The vast majority of business and IT leaders are well aware of the spectre of the hacker, and how there are countless individuals and groups endowed with the skills and experience required to infiltrate modern systems. Keeping these characters at bay is obviously of paramount importance, but organisations often fail to realise that one of the biggest dangers to the security of their data can come from their own employees. This could be one of two different types of person: a scorned employee bearing a grudge and wishing to exact revenge or, more likely, an individual who lacks the adequate knowledge of how to keep sensitive data safe.

With all of this in mind, building a water tight cyber security strategy is about not just shielding a company's assets from the outside, but also making sure that internal access to the most sensitive data is tightly governed so that only the most highly trained personnel are allowed to handle mission-critical information. This is where privileged access management (PAM) will play a major part, by automatically shutting off data to those that are not supposed to access it. A recent report by Gartner recognising PAM as the top cyber security priority for 2018 is indicative of its growing importance.

Coupled with a philosophy that embraces regular training for employees at all levels, businesses stand the best possible chance of making sure that their internal cyber security strategies are just as thorough as their external ones.

One of the biggest threats to data can come from a company's own members of staff

COVERING THE BASES

With the advent of the General Data Protection Regulation (GDPR) earlier this year, organisations are under greater scrutiny when it comes to adequately protecting sensitive customer information. Plenty has already been said on these pages about the financial implications of GDPR non-compliance, so the next phase of the discussion needs to focus on the many things that businesses need to do to make sure they cover all the bases.

Many debates so far have centred on data sovereignty and making sure the location of stored data doesn't contravene GDPR rules, as well as the need to step up efforts to fend off the advances of cyber criminals. However, it is just as important for companies to approach GDPR compliance with their own employees in mind; this should encompass working out ways to ensure each and every worker is accessing and managing data in the right way, adding further weight to the argument that measures such as frequent training and PAM technology are essential components of the cyber-frequent training security mix.

To highlight the scale of the challenge facing businesses, it's important to take a look at some key statistics covering the number of recent data breaches. According to Symantec's *Internet Security Report* for 2018, there was a 92 percent increase in new malware downloader variants in 2017 compared with the previous year, and a 600 percent increase in attacks against IoT devices.

While these figures largely encompass external threats, they represent concrete proof of the fact that businesses have their work cut out when it comes to building a comprehensive cyber security strategy. Certain threats may be snuffed out by effective reactive or proactive security measures, but new phishing techniques or malware strains will inevitably be ready to take their place before long.

INTERNAL FACTORS

From an internal perspective, these figures only strengthen the case for taking affirmative steps to ensure those within an organisation are prevented from compromising sensitive data. The success of a phishing campaign or malware intrusion is often dependent on human error or a lack of cyber security awareness, so it is crucial that not only do those without this level of security expertise receive the training that they need, but also that the technology is in place to closely govern access to certain data.

Alongside everything that is going on outside the business, it is crucial to measure just how prevalent the insider threat has become. Recent research has shown that more than half of IT professionals believe that insider threats are one of the greatest security dangers facing their organisation, indicating just how seriously people within the IT department are taking the issue. Despite this, the same research revealed that organisations are giving administrative privileges to more employees, with the proportion of workers granted such privileges increasing sharply, from 62 percent in 2016 to 87 percent in 2018.

Businesses can do little to control what is going on in the cyber crime world beyond the boundaries of the organisation, but what is well within their control is the ability to decide who should have permission to access the most sensitive data. Insider threats are a real danger and IT staff are recognising this, but there is still much more to be done to nullify these dangers. Internal cyber security policies need to be much more comprehensive than they currently are, and should embrace an approach that clearly and consistently differentiates between who can access certain data and who cannot. Without this, companies run the risk of having their information compromised by their own employees.

> PAM TECHNOLOGY CAN PROTECT DATA SO THAT ONLY THE RIGHT PEOPLE HAVE ACCESS TO IT

If the problem of insider threats is to be addressed, maintaining a programme of frequent cyber security training and guidance for staff is essential, in order to increase their overall awareness and plug any gaps in their knowledge. However, a recent survey by Mimecast has shown that this is somewhat lacking within UK businesses.

SPOTTING THE THREAT

According to the poll, only 7 percent of organisations regularly train employees to spot phishing emails, despite the same respondents also reporting a 54 percent increase in email-based phishing attacks. This is a common method through which cyber criminals may aim to gain access to a company's systems, so the fact that very little is being done to train employees in this area points to a need for specialist technology to be put in place to fill this void. Training may eventually catch up, but businesses should not be banking on this being their most reliable line of defence in the meantime.

Governing who has access to specific data cannot be effectively done on a manual, case-by-case basis. The time required by the IT department to undertake such an endeavour would make it an impossible task in itself, and working out how best to isolate the use of privileged accounts can be a major administrative headache for IT staff.

Privileged access management technology can go a long way towards achieving these objectives with minimal hassle to the IT department and wider business. Such software works by automatically separating privileged user accounts and data from a company's main environment, essentially creating a new environment for this data that is much less

likely to be susceptible to the threat of a data breach. PAM technology can then protect privileged user credentials so that only the right people have access to specific information, and can immediately flag suspicious activity so that appropriate action can be swiftly taken.

CREATING A SAFE PLACE

In effect, it's about creating a safe place within an IT system where the most mission-critical data can be kept, well away from staff that could either deliberately or inadvertently expose it to malicious eyes. PAM software is able to automate this process and monitor the situation on an ongoing basis, meaning the IT department has more time to focus on other activities.

Creating and maintaining a healthy, well-functioning cyber security strategy is about making sure that any threats coming from both outside and inside of the business are taken care of. The danger of cyber criminals operating on the outside is well known and organisations are well aware of it, but it is vital that insider threats are given equal attention if cyber security policies are to be as comprehensive as they can be.

The value of training cannot be understated, as a vigilant, cyber-aware workforce can be hugely influential in keeping sensitive data safe. Organisations should look to step up their efforts in this area, especially given how hackers are increasingly choosing to target businesses through email phishing campaigns.

However, where companies can make a lasting difference to how they manage insider threats is by making sure the technology they have in place is adapted to tackling the risks attached to employee activity. Privileged access management has the potential to be a crucial cog in this machine, by simplifying the process of who has access to what data. By making best use of PAM, businesses will be in the best possible position to reach a point where access is governed automatically, intuitively and in a way that does not affect the smooth running of the organisation ●

INTERNAL CYBER SECURITY POLICIES NEED TO BE FAR MORE COMPREHENSIVE THAN THEY ARE NOW

Dave Adamson has over a decade of technical experience as an IT professional, and brings a passion for articulating public, private and hybrid cloud concepts to both business and technical audiences.

The advent of GDPR means organisations are under increased scrutiny to protect customer information