Privileged Users And Cyber Risk

cyber security risk management

Summary: The exploitation of privileged users' access to a network is typically the main root cause of most large-scale breaches. Do you have a well-developed PAM to mitigate this big risk?

We wanted to share a survey by Adobe on email usage. When asked how long people wait before checking email after they wake up, most wait until they get into the office (39%), but others do so while getting ready (27%), while still in bed (23%) or when about to leave home (11%).

As you think about which one of these buckets you fit into, it is worth noting that clearly different people have different ways of working with email. The same is true when it comes to ensuring proper network security. After all, not all data is important or critical, not all jobs have access to sensitive stuff and not all users are created equal from a risk footprint perspective at least.

Indeed, the exploitation of privileged users' access to a network is typically the main root cause of most large-scale breaches. System administrators and top executives tend to be among the privileged users, who have a higher and wider level of access to the bank's data and systems than other employees. Increasingly maturing cyber-attackers are more likely to target these privileged users' accounts for compromise, since they realize it will give them better and broader access to valued information.

Reinforcing this issue, a survey of attendees at last year's Black Hat cybersecurity conference found almost 33% said accessing privileged accounts was the best way to get critical data.

This problem is exacerbated by the fact that 43% of banks do not have any board members with professional technology experience, and another 30% have only one tech-savvy board member, according to the Accenture research.

Security experts say a well-built privileged access management (PAM) program can considerably mitigate the intentional or unintentional misuse of breach at all levels in a bank.

Limit access rights to a reasonable minimum. Banks should operate on the principle of "least privilege", meaning they should allow all users the bare minimum of permissions needed to do their jobs effectively. If an employee has access to data and systems that they do not need, there is a greater chance they will be targeted for compromise. By destroying the access bridges to the data, bad actors cannot cross.

Educate board members and executives. As they say, "To whom much is given, much is required." Since privileged users (especially those at the top of the organizational chart) have greater access to systems than other employees, they also have a greater obligation to customers, regulators and the bank itself to manage their access. Community banks may consider offering "deep-dive" briefings to privileged users, led by qualified third parties, to help extend a better understanding of online threats and cyber-hygiene.

Inform top leaders of security issues that affect the bank and industry peers. Despite the daily headlines decrying massive cyber-breaches, many privileged users at banks do not always connect the dots between their level of access and their potential to be targeted by attackers.

To do better, weave cybersecurity news and advice into regular gatherings. These can include such things as board meetings, executive events, newsletters, emails or social media. Doing so incorporates it into daily culture for all users.

DEPOSIT OPPORTUNITY YIELDING 2.55%

In an effort to expand our relationships, PCBB is pleased to offer community banks a money market deposit account rate of 2.55%, subject to availability. Contact operations@pcbb.com.

Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.