IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Solving the Problem of Insider Threats to Enterprise Cybersecurity

Ronald Sens

Ronald Sens
EMEA Director
A10 Networks

Biography

Ronald Sens is EMEA Director at A10 Networks (https://www.a10networks.com). A passionate B2B technology leader and marketing professional with over 20 years of technology industry experience in multiple international marketing disciplines, Ronald's main areas of B2B marketing and technology expertise are in Enterprise Mobility, Data Security and Compliance, Datacentre, Networks, Servers and Storage, End-user Computing, SaaS, Virtualization, Enterprise Software, Mainframe and UNIX, Professional and Managed Services.

Ronald blogs at https://www.a10networks.com/blog

Keywords Insider threats, Enterprise, Cybersecurity, Problem, Solution, Report, Malicious
Paper type Research

Abstract

There are many threats to enterprise cyber security with most coming from external threat actors. One of the most overlooked threats that companies are not safe from is insider threats. As the author of this article explains, security professionals are constantly being warned about insider threats and in A10 Networks AIR report[1] earlier this year almost half (48%) of IT leaders say they agree or strongly agree that their employees do not care about its security practices. With companies aware of the issue, what are enterprises doing to fight back against these threats and why is it such a major concern?

Introduction: How big is the problem of insider threats?

The simple answer is very big. Generally cyber threats present a big issue to many companies, but many can be dealt with by using the appropriate solutions and having trained employees. To tackle insider threats, managers and IT leaders need to take an entirely different approach which can vary depending on the business environment.

All insider threats can often be classified into two distinct groups: the malicious, criminal employee and the unknowing, ignorant, employee. Both of these groups have to be approached in different ways, whilst identifying which employee falls into which group is not simple. Employers have to figure out what motive its staff has to be acting in a malicious way, whilst identifying them from the clumsy employees.

It's a sabotage

The motive behind an employee looking to sabotage a business could be inspired from many sources like holding a grudge over a bad personal assessment, peer or management conflicts, differing ideological views or pressure from an outside force. Identifying a motive can be difficult but, favourably, desire alone will not give such employees a chance to act. There needs to be an opportunity as well and this is where those in charge can work to prevent sabotage.

Many opportunities can be reached simply by that employee having increased or existing access to delicate points of information and so it is important that managers ensure that all of their employees only have access to the minimum required for their role. Then there are more sinister attempts at disrupting businesses like social engineering tactics – setting up the right scenario for this malicious employee to get access through someone else's computer/network.

Additional actions that security professionals should take notice of are the unusual behaviors of some employees, such as arriving early or leaving after everyone else, recent changes in access, frequency of downloads or failed login request from a use system. Anyone of these could be a sign of an ulterior motive and are good places to start when trying to identify malicious employees in the business. Behaviour is the key and it is important to determine the behaviour patterns of individuals, whether it be done with technology, physical apparatus or digital monitoring tools.

Did I do that?

With the next group – the unknowing, ignorant, employee – a different approach is needed. The cyber threat from this group can come from many places but it all stems from one issue: they do not realize they are a risk. So, the simple solution to solving this problem is to properly educate staff, and not just the IT department but the entire business, as these risks can come from any department.

Research shows that 88% of IT heads say that employees need better education on the best security practices and while many companies do inform their staff of these practices, 29% of IT professionals noted a lack of corporate commitment to policies and enforcement. So, while enterprises know the best practices to stop insider cyber threats most of the employees don't care, so perhaps the area that needs fixing is the method in which enterprises explain these practices?

According to the *AIR report*[1], password policies are communicated to employees through email reminders (66%) followed by employee orientation (50%), internal meetings (48%), and communication from a manager (44%). E-mail reminders are highlighted here as the main way of communication and this should not be the case.

In today's busy work environment employees are receiving e-mails non-stop and, by distributing such vital security information to an already crowded information network, are bound to skip over it. Potentially, they have more pressing work to deal with and so the internal security information is not the priority. Eventually it will be forgotten.

The solution is simple. More direct communication with staff and more workshops around cybersecurity could bring these issues to the forefront of employees and make them more aware. Then, regarding passwords, it could be made mandatory to have them changed on a regular basis, with two-step authentication for extra protection. If password change isn't enforced, then employees are most likely going to be too busy to change them.

Passwords not being updated isn't the most pressing issue regarding insider threats. Every employee can bring with them a vulnerability to the mainframe. The most common threat an unknowing employee can bring with them is opening an entryway with unverified or unsecure apps, both on computers and on phones. Every employee has a mobile phone and most likely a smartphone with multiple apps that they may use throughout the day. Apps that require online connections may end up being connected to the office mainframe and allow a gateway for hackers. Then on computers some apps like Photoshop and Skype are common practice but there are other, less secure, apps that could bring malware with their installation.

To tackle this issue, a regulation should be placed on what can and cannot be used in the office, at least on laptops and PC. If an employee wants to install new software, they should need to be granted permission from an admin who can verify that the app is secure. For mobile apps this is harder to control as they aren't strictly for work but if employees are properly taught about these threats and regularly informed about how to avoid suspect apps themselves then they can stay more aware of potential threats.

Conclusion: is there hope?

Almost a quarter of IT decision-makers think there will be no improvement in security behavior at their company, but 75% are more optimistic. Cybersecurity is increasingly becoming more mainstream in the business world and many enterprises are beginning to shift more resources to fight back. Funding is going towards technology to deal with malware and other malicious outsider threats, but insider threats do not appear to be a focus yet. As more people take notice, hopefully this will change. Getting the balance between having a warm, open working environment versus a police state-esque look and feel is not easy, but with correct training and observation of employee behaviours there is hope for enterprises to deal with insider threats.

Reference

[1] http://get.a10networks.com/air/