How to ensure your company doesn't suffer a disastrous third-party data breach

By Jody Brazil 3 days ago

Do you know who has access to your network?

Making headlines across the globe, security breaches have become a daily occurrence. As such businesses need to reassess the importance of ensuring the network is secure against potential third-party or supply chain partner data breaches, by understanding the level of access partners may have, without knowledge, into the network.

As a business, you may have done all you can to secure your information – but what happens when one of your partners is hit by a breach? Just because it is not your business that has been directly attacked, it does not mean hackers can't access your company's data if the correct security measures are not in place.

So how can organisations understand the risk of exposure, gain the insight into their network connections and effectively monitor the access levels awarded to their business and supply chain partners? Moreover, what can be done to mitigate this risk and ease the burden on the

IT and Network Managers whilst ensuring your business, and potentially your wider supply chain and partner network, is secure?

Learning from experience

We live in an increasingly interconnected world and, whilst it is natural for some organisations to allow their business partners access to certain aspects of its network, for example to improve collaboration between organisations, what happens when this goes wrong and leads to a data breach?

You need only look back to December of 2013 to gain an insight into the devastating ramifications of a major third-party data breach. American retailing giant Target was struck by what was one of the largest attacks in the retail industry's history when one of their supply chain partners, a provider of heating, ventilation and air conditioning (HVAC), was targeted by hackers.

Worryingly, the coding the hackers used to access the network was not an Advanced Persistent Threat (APT) attack, nor was it complex in nature. It was a piece of common coding available online. The attackers were able to utilise the HVAC's details to access Target's Point of Sale (POS) network undetected, resulting in 110 million payment card details being exposed.

This only happened because the supplier was granted access rights to more of the network than intended, which meant attackers were able to infiltrate the network through this backdoor before launching an attack that could have been wholly preventable. Target chose to allow a third-party access to its network, but failed to properly secure that access.

Understanding the risk level

Large-scale attacks, such as that experienced by Target, could have easily been prevented with the right care and the application of the right knowledge. There are a multiplicity of already existing methods and practices that would restrict business or supply chain partners from accessing systems and networks they have no need to access.

In the first instance, businesses need to critically look at their network maps and assess whether partners may have connected access to critical assets within the organisation. In all cases, it is important to understand how you are connected to each other to monitor and mitigate any further proliferation of the breach. Quick and effective response to these threats is critical to limiting the propagation and impact from a partner breach.

However, if an organisation doesn't have detailed information on the network paths between systems and the ability to proactively identify gaps in security, then preventing, mitigating and remediating security breaches will always remain a significant challenge.

Secondly, are the existing network defences configured correctly? The inability to properly configure existing defences remains, arguably, one of the most significant security challenges facing organisations today, increasing the risk of compromise and resulting breach incidents.

In the majority of cases, configuration issues arise due to an explicit action, or lack of actions, taken by network administrators in setting access rules, creating overly permissive configurations. Or even something as simple as leaving the device settings on default, which automatically puts the network at risk.

Conducting an audit of firewall access, rules and policies will also allow IT departments to see exactly what access people have, as well as identify potential gaps in security, thus allowing them to plug these holes and ensure the corporate network remains secure. The audit will not only identify these rules, but can also check the complexity and openness of rules, which can help to speed up traffic and reduce bandwidth consumption. In the past this process has been a tedious, manual one, but new security intelligence automation tools can now dramatically reduce the time required and increase accuracy.

In order to remain proactive and ensure the corporate network is fully protected, organisations should also conduct real-time analysis of access to their networks. As partners connect from external sites, IT departments need to see what is being accessed, who has access and what they are doing. Understanding what is happening on your network at any given moment can help to identify abnormal activity, enabling a business to immediately spot any problems, as and when they occur.

**Draw a line in the sand – and don't let your partners cross it**

As you would expect, since the revelations of these breaches, organisations have attempted to step up their security procedures by investing in expensive new systems in an attempt to safeguard their networks. But investing in all manner of security devices does not automatically grant immunity from these sorts of attacks.

Instead, security teams should be conducting tactical attack analysis and penetration testing on every device and pathway across their networks, which can identify systems that are vulnerable to attack. Moreover, businesses should be liaising with partners to properly identify gaps in security and ensure existing systems are installed and configured correctly.