Complacency in supply chain cyber security – a hidden threat to SMEs

Small and medium sized enterprises are under pressure to protect themselves against cyber attacks to mitigate the risk of being excluded from supply chains.

LONDON, UK, March 20, 2019 /EINPresswire.com/ -- Joe Collinwood, CEO at CySure, takes a closer look at the implications of complacency in supply chain cyber security.

In a rapidly evolving landscape of cyber threats, many organisations are focusing efforts on protecting the confidentiality, availability and integrity of their networks and systems. While this is important, small to medium enterprises (SMEs) are typically falling to understand the wider risks and to implement basic cyber hygiene measures. This complacency compromises their own IT environment and that of suppliers and partners within their supply chain.

> It is time for SMEs to act and adapt their information security practices to the new landscape and demonstrate their cyber credentials."
>
> *Joe Collinwood, CEO, Cysure Limited*

New research conducted by the Federation of Small Business (FSB) identified that 65% of UK Small Businesses do not have plans in place to deal with potential supply chain disruption including cybercrime[i]. The threat is real and SMEs need to act or risk their business failing due to the lack of a robust cyber security strategy.

The weakest link

A number of big brand organisations have recently been exposed by data breaches and although their names may have made the headlines, in some incidences the security breach occurred due to flaws in third-party partners. High profile data breaches such as the attack on communications firm TalkTalk, which was fined £100,000 in 2017 by the Information Security Office (ICO) for a third party's misuse of data[ii], have been a wake-up call for organisations, whatever their size.

Like TalkTalk, many organisations often rely on a vast network of agile SME suppliers and partners. However, small companies can be easier targets for attackers if they don't have robust security measures in place. With information and security arrangements shared across a supply chain, the cyber-security of any one organisation within the chain is potentially only as strong as that of the weakest member.

Research firm Vanson Bourne[iii], surveyed 1,300 senior IT decision-makers and IT security professionals in organisations with 500+ employees. Respondents were selected from across major industry sectors and from the US, Canada, UK, Mexico, Australia, Germany, Japan, and Singapore. The study, conducted in 2018, revealed that two-thirds of respondents reported that their organizations had experienced a software supply chain attack, with 90%of those confirmed that they had incurred financial cost as a result. The average cost of an attack was over $1.1 million.

The survey also found that the majority of organizations aren't adequately prepared and feel vulnerable. Almost 90% of the survey respondents believe that they are at risk for a supply chain attack, yet companies are still slow to detect, remediate and respond to threats.

A determined attacker will stress test the cyber security of a supply chain, seeking to identify the weakest link and use any vulnerabilities present to gain access to other members of the chain. Whilst not always the case, it is often SMEs, with their limited IT expertise and resources, that have the weakest cyber-security arrangements. Once an attack has been successful against an SME supplier, attackers can then leverage their access as an entry vector into the larger network.

Securing the supply chain down the line

Following the introduction of the EU General Data Protection Regulation (GDPR) and the broader scope of fines available to the Information Commissioner's Office (ICO), large organisations are realising that it's no longer enough to ensure their own network is secure, they must now also pay attention to securing the supply chain.

Enterprises that are at the top of a supply chain will more and more require certification as proof of security and compliance, or will want contractual warrants and indemnification as protection for themselves. The increased risks of a data breach and GDPR enforcement are requiring companies to ensure they have cyber security as a part of their contract with processors, contractors or service providers. Larger organisations, which are risk adverse to reputational damage and business disruption, will choose to use only those suppliers that are certified as part of their due diligence and selection process.

The increased risk of cyber-attacks is not only a concern within the enterprise. The Department of Defense (DoD) has announced that all contractors that process, store or transmit Controlled Unclassified Information (CUI) must meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards by December 31, 2017 or risk losing their DoD contracts.

Effective cyber-security risk management with certification

SMEs can protect themselves against cyber-attacks and mitigate the risk of being excluded from supply chains by undertaking a certification process. Cyber Essentials is a UK government and industry backed scheme to help all organisations protect themselves against common attacks. In collaboration with Information Assurance for Small and Medium Enterprises (IAMSE) they set out basic technical controls for organisations to use which is annually assessed. The aim is to ensure that companies can understand their cyber risks, implement appropriate cyber defences and meet minimum cyber security standards without hindering business and share best practice.

With larger organisations increasingly validating that sufficient cyber-security standards are implemented across the entire supply chain, SMEs risk losing contracts should they fail to prove sufficient compliance and information security to meet the minimum expected by their partners. SMEs that are not prepared to take cyber security seriously will be weeded out by business failure, either due to a data breach or not being able to compete with certified businesses.

It is time for SMEs to act and adapt their information security practices to the new landscape and demonstrate their cyber credentials. By utilising an online information security management system (ISMS) that incorporates Cyber Essentials, SMEs can undertake certification guided by a virtual online security officer (VOSO) as part of its wider cyber security measures. This will help the organisation to coordinate all security practices in one place, consistently and cost-effectively, keeping them safe and competitive in 2019 and beyond.

[i] https://www.fsb.org.uk/first-voice/majority-of-small-businesses-unprepared-for-business-interruption

[ii] https://www.theguardian.com/business/2017/aug/10/talktalk-fined-100000-for-not-protecting-customers-personal-data

[ii] https://www.vansonbourne.com/client-research/24111701tc

Mary Phillips
PR Artistry
+44 1491 845553
email us here
