Know your vulnerabilities as cyber-attacks continue

Submitted by: PR Artistry Limited
Thursday, 30 March 2023

Given the state of the world today it is no surprise that there has been no let-up in the number and variety of cybersecurity hacks in recent times. All sizes and types of organisations continue to be targets. Nick Denning of Policy Monitor discusses what small and medium-sized enterprises (SMEs) can do to better defend themselves. Starting with knowing their vulnerabilities.

The variety of hacks, digital scams, data breaches and ransomware attacks have continued unabated as covered in the press by Wired Magazine (http://wired.com/story/worst-hacks-breaches-2022/) and Sky News (https://news.sky.com/story/businesses-urged-not-to-give-in-to-ransomware-cyber-criminals-as-authorities-see-increase-in-pay
If the biggest organisations are vulnerable, how can smaller organisations hope to stay safe?

The SME Advantage
It is true that larger organisations have more cybersecurity experts and resources to help protect them from attack than SMEs, but having in-house knowledge is only part of the story. Research can show ‘what’ the threat might be but not ‘where’ your organisation could be vulnerable. The good news is that SMEs by their nature are likely to have a smaller attack surface. Therefore, it is potentially easier for an SME to assess risks and to take an inventory of the assets that need protecting and how they may be vulnerable. However, if a business does not have even the basic skills and deployed technologies to access this type of information it can leave huge gaps in its defences, or lead it to invest in the wrong kind of security.

It is like leaving your house, locking all the doors and turning on the expensive burglar alarm you installed after a previous break in, but forgetting to close the bedroom window or secure the shed where your expensive power tools are stored.

Take an inventory of ALL your IT assets
Just as it is important to have a register of your physical assets for accounting and maintenance purposes, an important element of effective protection against cyber threats also requires an ongoing process of cybersecurity asset identification and management. This has two dimensions. Companies need a register of traditional physical IT assets such as PCs, servers and the increasing number of devices used to access systems remotely. Increasingly, organisations have items connected as part of the Internet of Things such as medical sensors, fire alarms and smart security devices. You need to have an inventory of all these assets as they make up the attack surface of an organisation.

The second dimension of IT asset management is that these assets can provide a vulnerable entry point and have great value in themselves, they may also be the ultimate targets of cyber-attacks. For example, an inadequately protected public application might provide a way-in for cyber criminals to download or corrupt your data or a path to enter your systems then move on to other targets. Customer data and employee records held in databases can help cyber criminals perpetuate identity theft and financial fraud. If there is a data breach an organisation can be hit by direct financial fraud, an inability to perform daily business processes, reputational damage and heavy data protection fines from regulators and the cost of forensic investigations.

What does Cyber Essentials say?

The NCSC has recently launched the Cyber Essentials Readiness Tool, which was developed by IASME. It asks organisations a series of questions related to the main Cyber Essentials criteria to help prepare them for certification. The first task is to define what is in scope and what is out of scope for certification.

As the tool says; “Assessment and certification should cover the whole of the IT infrastructure used to perform the business of the applicant, or if necessary, a well-defined and separately managed sub-set. The requirements apply to all the devices and software that are within the boundary of the scope and that meet any of these conditions:

- can accept incoming network connections from untrusted Internet-connected hosts
- can establish user-initiated outbound connections to devices via the Internet, or
- control the flow of data between any of the above devices and the Internet.

A scope that does not include end-user devices is not acceptable.”

NCSC has expanded its advice to cover the increase in home working and bring-your-own-device (BYOD). Traditionally, user devices were managed and controlled through centralised IT administration. The CE Readiness Tool notes that, “BYOD complicates matters, as users are given more freedom to ‘customise’ their experience making consistent implementation of the controls more challenging.” It also states that, “The default approach is that all corporate or BYOD home working devices used for applicant business purposes within the home location are in scope for Cyber Essentials.”

Know where you might be vulnerable

All devices, resources or services that are part of your ever-expanding IT landscape could be subject to risks or vulnerabilities that lead to a cyber breach or act as a bridgehead into your environment as a whole. It is important that your organisation not only creates an asset register of physical IT assets, which it may already have for depreciation purposes, but the register should also include more intangible assets like software and databases, plus employee devices used in a home-working or a BYOD context. This complete asset register will help you assess your vulnerabilities, ie the issues in code across all your IT assets which can be exploited to gain access to your data resources, syphon off funds, inject malware, or block or take control of entire systems and networks.

Policy Monitor’s CSPM solution can help you build a comprehensive IT asset register and then ensure you put in place the policies and processes that meet industry standards to reduce vulnerabilities and minimise cyber threats. We do this by integrating with industry standard technologies such as Qualys to scan networks and to deploy Qualys agents onto every computer to monitor all organisation assets deployed remotely such as where people are working from home. We plan to integrate with similar technologies where they are already deployed by customers. The key point of our approach is to include this information in a consolidated risk dashboard available to the Director of Security. So, not to replace the excellent third-party technology, but rather to get the data out of the IT department and to an informed board who can then direct the IT team managing the estate.

To find out more visit Policy Monitor (https://policymonitor.co.uk/cspm/)

-ends-

About Policy Monitor

Based in London, Policy Monitor is a cyber security company founded by experts with extensive experience in operational and risk management. We evolve safety procedures and protocols, providing security policy management solutions and services to Measure, Manage and Monitor cyber risk and guard against cyber-attacks.

Our flagship solution, Cyber Security Policy Manager (CSPM), is a cyber security policy management system that incorporates GDPR, US NIST and UK CE cyber security standards to guide organisations through complexity. It is a simple and cost-effective cloud-based solution that helps measure, manage and monitor an organisation's cyber security workflows and compliance. Cyber Essentials and IASME templates are pre-loaded to help reference cyber security best practice, define and implement a security policy and monitor compliance.

Press contact:

Mary Phillips
PR Artistry Limited
T: +44 (0)1491 845553
E: mary@pra-ltd.co.uk