SC MEDIA

Don't be scared to go back to basics with your cybersecurity strategy

4 hours ago

OPINION by Andy Miles

Combatting day-to-day threats can be achieved by addressing basic core principles: password practices; email management; updating and testing security processes as well as ensuring a security-first culture.

The headlines around cyber-security often focus on advanced cyberattacks, the underground cyber-arms race and speculation of nation-state attacks. In reality, most cyber-crimes are more mundane. For businesses combatting day-to-day threats, protection can be achieved by following basic core principles.

This core comprises of practices related to passwords, email management, updating and testing security processes as well as ensuring a security-first culture. Whether an agile start-up or an established global corporate, these principles remain the same. A good place to start is the NCSC's (National Cyber Security Centre) Cyber Essentials. These guidelines provide those with a blank slate with a consolidated foundation from which to build out processes and procedures that work for their organisation's unique objectives, work practices and IT structure.

Know your weaknesses before the criminals find them for you

Regularly scanning and assessing networks for vulnerabilities should be a number one priority for all businesses. No matter how water-tight you believe your networks to be, new security vulnerabilities are discovered hourly and hackers are dedicated to finding them before you do. Hackers can take advantage of vulnerabilities in mere hours, meaning the quicker they are found and patched by you, the less time you risk having an open door for exploitation.

The first line of defence is a commitment to regular vulnerability scans. For example, Microsoft's Patch Tuesday, where the company issues patches every two weeks is a baseline frequency.

It should go without saying that once a vulnerability is discovered the priority should be to act immediately to prevent exploitation. One cautionary tale is that of WannaCry, which hit the

NHS in Spring 2017. The vulnerability exploited by this hack had been previously patched, but many organisations failed to treat it as a priority and update systems.

Regular patching will ensure protection against most attacks. However, the sprawling nature of modern IT networks means that even the most rigorous scans will occasionally miss vulnerabilities. Multiple systems interacting, software updates experiencing interoperability issues, not to mention the challenge of taking critical systems offline to perform patching. It can be difficult to manage security in an organisation that demands always-on services.

Consequently risk-management must include assessment of the impact of downtime, versus the risk of unpatched systems. This is a board-level discussion that requires IT and finance teams to work to work together to assess risk and work together to mitigate loss.

One way in which these teams can inform this risk assessment is through in-depth penetration testing of their systems. This allows for controlled testing of vulnerabilities and potential impacts of breach on the organisation.

Engage in ethical hacking

Penetration testing, also known as pen testing or ethical hacking, sees experienced security professionals taking on the role of hacker to uncover cyber-vulnerabilities. This is regarded as an essential security practice by the Information Commissioner's Office (ICO), which has handed down hefty fines to organisations who have failed to test their systems.

Ethical hackers will start with basic attacks, for example trying common password combinations (yes, teams are still guilty of using 'password' to protect key systems). This will expose the 'easy-fixes', before moving on to more sophisticated methods such as phishing attacks and SQL injection.

Each managed attack will test security measures and safely expose holes to be plugged and processes to be refined. This is an exercise that should ideally be undertaken every six months, or at least annually. If there are major changes to the network or structure of the organisation, ad-hoc pen testing should become a key part of the planning process.

Don't let email be an open door

Email is still the most common vector for conducting a cyber-attack; 90 percent of the attacks ThinkMarble investigates begin with a malicious email. These are sophisticated, coordinated campaigns designed to evade traditional Secure Email Gateway solutions.

Spear-phishing attacks impersonate a trusted contact and target specific employees, thereby bypassing attachments and keywords usually filtered by email security scanners. Alongside this, more advanced attackers will disguise their sender ID and mask their IP address. A lack of email security combined with poor patching practices makes a company a prime target for low level attacks.

Don't be the last to know

Although rare, even the most secure networks are still potentially exposed to zero-day exploits. These are vulnerabilities used in attacks before they can be reported and patched. In the face of the a zero-day exploit, every minute counts. That means having a robust system to detect attacks as they happen.

This requires an experienced security team, with 24-7 capability – an asset most companies do not elect to take in house due to expense and resource required to power such an asset.

https://www.scmagazineuk.com/dont-scared-go-back-basics-cybersecurity-strategy/article/1491797

Managed security services give access to security professional through an affordable regular fee, enabling organisations to have a team of experts on watch.

Back to basics

Unfortunately, no amount of security measures will guarantee full protection from cyber-crime. However, with a wealth of information, experts and tools at hand to help instil best practice there is little excuse not to take this issue seriously. Ensuring the basics are in place now will stand organisations in good stead to combat low-level attacks, while being alert for the vulnerabilities that could lead to more serious breaches.

https://www.scmagazineuk.com/dont-scared-go-back-basics-cybersecurity-strategy/article/1491797