CYBER SECURITY EXPLAINED

From phishing to ransomeware, companies are at risk from cyber criminals. Jason Connolly, director of Next Generation IT, explains how to guard against them

The islands are an attractive target to criminals across the globe. Whilst we live on a low crime island, online we are not protected by our geography.

So how do we protect ourselves from this evolving threat?

Good security is like an onion, with multiple layers of defences which ensure that even if a single measure is breached, all potential access points remain protected.

The main components of a security system are outlined in brief below:

Live protection

The first line of defence connecting any internal network to the internet is a traditional **firewall**. This device separates internal network traffic from the public internet and is analogous to a border control point. It is a fundamental and basic form of security protection.

The challenge with relying solely on firewalls is that it's not possible to block all network traffic - some ports need to be left open for emails to flow, staff to browse the internet and remote access to be allowed. This leaves potential vulnerable points for hackers, ransomware and malware. All other security measures aim to solve this challenge of detecting which traffic is official and which is bogus.

At the next level, **web security** monitors web traffic to detect and block any nefarious websites, code injected into kosher websites and botnets (vast zombie like networks of infected PCs used by criminals for attacks). It does this by examining website content. Recently, more advanced protection is provided by live reputation databases that filter out bad or compromised web servers. These databases are updated continuously by teams of security consultants who work 24/7 in labs around the world to examine, reverse-engineer and design countermeasures for new vulnerabilities in real time.

The last line of defence is **desktop antivirus, anti-malware** or **anti-ransomware software.** If an attack has got this far, then it is bad news. The type of attack and the victim's countermeasures will determine how much damage is done. Desktop software is designed to detect any infection, quarantine the infected machine to prevent spread to other devices on the network and with luck, clean up the infected PC or server.

Depending on the damage, it may be necessary at this point to revert to **backup** to restore the infected machine and any lost or corrupted data. It is absolutely imperative that good, regular backups are made, not just of the data, but also of any operating system and applications. A good backup will minimise the disruption by enabling infected systems to be restored quickly and with minimum data loss.

Other attack vectors

Web browsing is only one attack vector. Other vectors include email, which can be protected by **email filtering;** USB attached devices, which can be locked down to prevent access; and, web portals and remote access systems, which can be protected using a **reverse proxy service** and **two-factor authentication.**

Mitigation – security hygiene

However, these controls are only part of the story, as people are often the weakest link. Social engineering, using publicly available information, such as website or LinkedIn profiles, allows miscreants access to trick staff into inadvertently giving access to private systems through 'phishing' attacks. These approaches can be very sophisticated and convincing and therefore, regular and thorough **security training** is required to educate staff about fake or contaminated emails, links and attachments and learn good working practices to corroborate payment instructions.

There are also other security controls, such as **data encryption, mobile device management, penetration testing** and **security information and event management systems.** With the advent of the General Data Protection Regulation and increased penalties for data loss these advanced controls are becoming more prevalent.

Finally, arguably the most critical and often overlooked mitigation activity is regularly **patching and updating** desktop, server, application and security system software. It's often a race for software providers to develop and distribute patches to all affected systems before an exploit can be developed, deployed into the wild and spread to vulnerable systems. Whether your organisation wins this race or succumbs to the hackers very much depends on your security systems, people, processes and technology.