Cyber security essentials for boards and senior management

I have had many conversations with board members and senior executives on the subject of information security (or cyber security). One of the more common sentiments I have come across is the view that “if someone wants to get in they will” or “they are probably already in anyway”. It’s understandable that the sensationalised and high profile attacks can make us feel a little helpless sometime, however the reality is that regulators, investors and customers will pass judgement and if senior management and boards were lax, then the company will suffer.

Yes, if someone has the resources and the incentive, it can be hard to stop them hacking in, but this level of attack is reserved for the select few. Such an attack, also known as an advanced persistent threat (APT), is usually the realm of nation states or other high-profile organisations. These attacks will be perpetrated by skilled hackers, using secret vulnerabilities, known as zero day exploits, and involve significant research about the target to make the attack successful. These targeted attacks are expensive to conduct and when discovered generate sensational news stories, such as the US NSA recent hack.

However, for the rest of us, including the majority of commercial enterprises, we are far more likely to fall victim to a simpler, opportunist attack. These more generic attacks can be just as devastating in their impact, but the good news is that preventing them is quite feasible with relatively simple good practices and management prioritisation. For the criminals perpetrating these opportunistic attacks, it’s a numbers game. They want to spend as little as possible, for as much return as possible. This often involves distributing their malware widely to unsuspecting targets using email or websites. This malware, once activated by the recipient will exploit vulnerabilities on the host computer to take control - at which point the attackers have won. However, in an opportunist attack, the critical difference compared to an advanced attack is that the attacker does not have or does not want to pay for the secret vulnerabilities and they will exploit vulnerabilities in the public domain.

Since these vulnerabilities are in the public domain, the likelihood is that system vendors will have patches or updates available to block the attack. Ensuring all your systems stay up to date on patches will drastically reduce your chances of being hacked. Is it really that simple? Well yes and no. Depending on the size of your company, the numbers of patches could run into hundreds per year, across hundreds or thousands of devices. Often the patches need testing to ensure compatibility with older systems such as an old accounting system. Frequently, other business priorities exist for your IT teams, such as new projects – and patching drops down the priority list as nobody is asking for it. So, patches get delayed and backlogged and the task of catching up becomes ever more daunting. It’s not uncommon for a company to be 6-24 months behind with patching and this is what the attackers are hoping for.

The recent ransom-ware that hit the NHS among others is a prime example, the attack exploited a vulnerability that was fixed by a patch 2 months prior. Yet many systems were as much as 2 years out of date.

In the case of an advanced (APT) attack, using secret vulnerabilities, a board could reasonably claim it was beyond the company’s ability to prevent it. However, for an opportunist attack, using a vulnerability in the public domain for 6 months, then it is likely to be seen as a management failure and the board culpable if they were not putting the relevant level of challenge and monitoring on the management.

To bring a more rounded approach to cyber security and further improve your chances of resisting attack then a board also needs to be able to probe the areas of: organisation (eg delegation and reporting), processes (eg backups and policies), people (eg staff training and awareness) and technology.

However, the bottom line is that most attacks are opportunistic and preventing them is generally within management and board control providing the right questions are asked and the right priorities set.

If you require further information on how to approach this with your company, then please contact us. We may be able to offer an internal briefing with your management or board or assist with a preliminary survey.