Tackling cyber security risks in your organisation

Cyber security is a complex and continuous battle. Whenever an organisation identifies and addresses the tactics criminal hackers use, the crooks move on to a new strategy.

Spotted a new phishing email doing the rounds? Better warn your employees, although the next campaign will hit soon. Found a vulnerability that can be used to inject malware? Another one will emerge after you've patched that one.

This can make fighting cyber crime feel like an impossible task – but you'd be surprised at how much easier it gets when you look at the big picture rather than focusing on each threat as it arises.

That's because, as rapidly as criminals' attacks evolve, they all follow the same basic principles. If you create a holistic and adaptable defence strategy, you can keep pace with risks as they emerge.

But what exactly would that strategy look like? We explain everything you need to know in this blog.

Vulnerability testing

When you picture cyber crime, you probably see a hacker typing rapidly as they meticulously break down an organisation's defences.

Indeed, criminal hacking is the most common way organisations are breached, but most hacks don't involve complex coding or manually probing systems. They are simple intrusions that use automated tools that look for known vulnerabilities.

That means your organisation's weaknesses aren't tucked away in some crevice that will only be found after hours of searching. Criminals simply need to run a program and wait for it to reveal every possible point of entry.

This explains why analysis from Beaming revealed that UK businesses faced an average of 146,000 attempted cyber attacks in the second quarter of 2019 alone.

Although this sounds alarming, the good news is that organisations can use similar automated tools to identify weaknesses before cyber criminals exploit them.

These vulnerability tests are paramount to your organisation's security. No matter how diligent you are, your systems will always contain weaknesses, but by analysing your software, firmware and operating systems, you can root them out quickly and at a relatively low cost.

If you do this every three months, or whenever there are major organisational changes, you'll be in a strong position to stay one step ahead of cyber criminals and keep your systems secure.

This is a great start, but unfortunately, you probably won't have the budget to tackle every threat, or you'll find that there is no simple fix for certain vulnerabilities.

Written by Luke Irwin

That means you either need to spend money finding a workaround, removing the flawed system or accepting the risk and estimating that the cost of a breach will be less than the cost of rectifying the problem.

These are often difficult problems to solve, which is why you need cyber security experts in your team to advise you – something we look at more next.

Cyber security and your employees

According to Verizon's 2020 Data Breach Investigations Report, almost a third of all security incidents are caused by employees.

This might involve misconfiguring a database stored on the Cloud, disposing of files improperly, losing a storage device or a countless array of other mistakes.

The threat is even more pronounced as a result of COVID-19 and the rise in remote working. Employees rely on the Internet to communicate with colleagues and share documents, introducing new security risks.

For example, there is an increased risk of sending sensitive information to the wrong people, organisations making information available to unauthorised employees, exposing confidential information during video calls and employees using work laptops to visit dubious websites that might install malware.

But these problems will not necessarily go away after the coronavirus pandemic. An O2 survey has found that 81% of respondents expect to work from home at least one day a week even when their offices reopen, and 33% hope to work from home at least three days a week.

Whether tackling the risks introduced by remote workers or staff in general, your first task is to conduct a risk assessment to identify and evaluate your weaknesses.

From there, you should create relevant processes and policies that can mitigate these risks. Introducing strict requirements on password creation and management, for instance, will greatly reduce the likelihood of unauthorised access – as will implementing access controls.

Likewise, any organisation with remote workers should consider the security of employees' devices. You should create strict acceptable use policies, and mandate that staff work on company computers and phones and that they take appropriate measures to keep those devices secure when in public.

Staff awareness

It's only by teaching employees about the threats facing them and the ways their organisation deals with them that you can effectively tackle cyber threats on all fronts.

After all, technological defences and processes only work if your employees use those technologies and follow those processes responsibly.

Take phishing as an example. It's one of the most dangerous forms of cyber attack, in which criminals, masquerading as a legitimate person or organisation, trick victims into handing over sensitive information or downloading an attachment that contains malware.

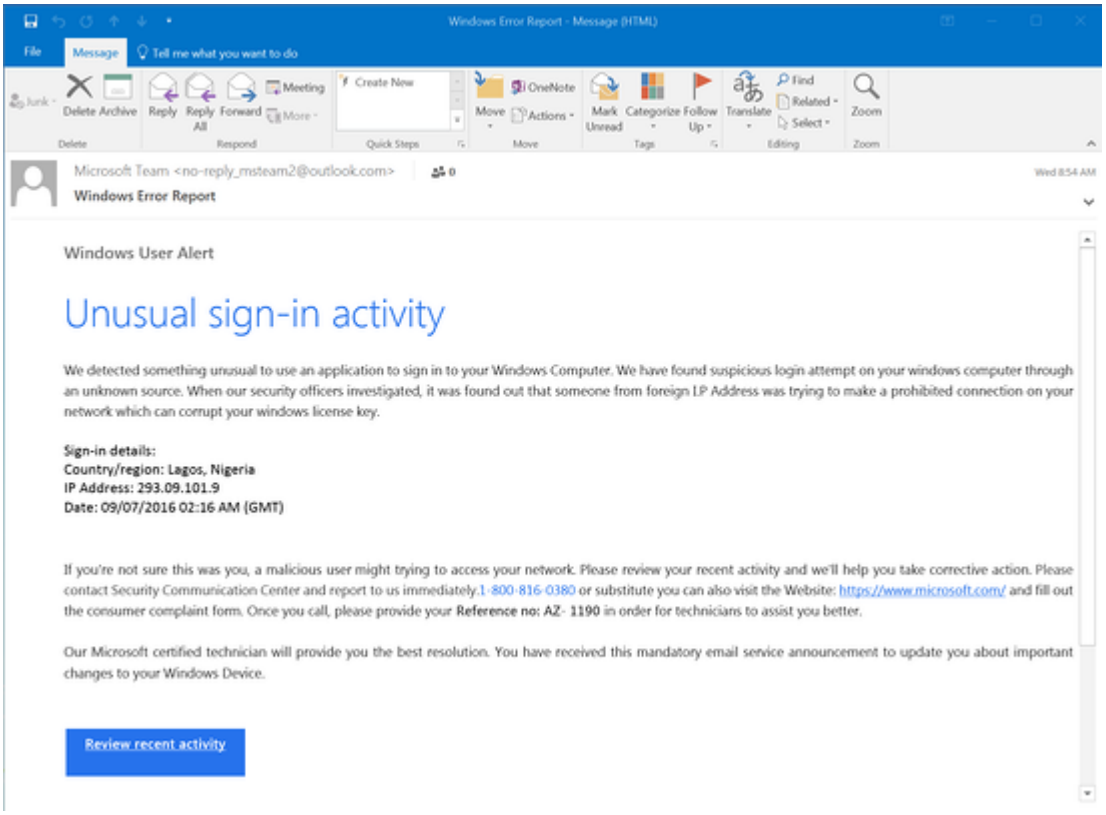

Image source: KnowBe4

Action Fraud warned people about a phishing scams capitalising on the disruption caused by the coronavirus pandemic.

As evidence of how perilous these scams are, Beaming's Five Years in Cyber Security report found that close to one in ten organisations fell victim in 2019.

In these circumstances, it's not just the victim whose account is compromised. The fraudster can use their access to launch further attacks and access a host of sensitive information.

According to a KnowBe4 report, the construction industry is most susceptible to phishing emails among small and medium-sized businesses, and second most susceptible among large businesses.

Almost 40% of employees in the construction industry fell for the researcher's bogus email. However, after three months of training, the percentage of people who fell for scam messages halved.

This shows the power that staff awareness alone can have – and when you pair it with technological defences, such as spam filters, and processes that instruct employees on what to do when they receive a suspicious email, you can greatly improve your resilience to attacks.

Of course, this lesson doesn't just apply to phishing. Almost every threat you face can be tackled across all three aspects of cyber security: technology, processes and staff awareness training working together to protect your organisation.

 Written by Luke Irwin

It may be tempting to think that one security control will do the trick – particularly if you are one of the many organisations working with a tight cyber security budget.

However, the threat of cyber crime and data breaches isn't going away, and the costs of security incidents can be huge, so you're better off investing now than waiting until it's too late.

IT Governance have a wealth of security experience and have helped hundreds of organisations prevent and respond to security incidents worldwide.

Discover how they can help you get cyber secure.

Written by Luke Irwin