Ransomware: Protecting Your Business from an Evolving Enemy

In our previous blog, we looked at the evolving threat of ransomware, so now let's take a look at how to meet this threat head on. Here's how to avoid becoming a threat actor's next target, and what to do if an attacker seizes your systems.

At this point, ransomware is nothing new. This malicious software's impact on businesses is just as devastating as ever, but the techniques that threat actors utilise to target organisations has grown in sophistication, particularly over the past 5 years. Nefarious parties are becoming ever more advanced in their efforts to hold your organisation to ransom, but the good news is that your business can adapt too.

Don't Be Held Hostage by Hackers

Having a plan in place for if the worst occurs is never a bad idea, but surely prevention is better than cure. In order to protect your business from possible ransomware attacks, you'll need the following:

A Software Patching Policy

Most cyber-criminals are not utilising zero-day exploits in order to infiltrate your systems, they're taking advantage of known vulnerabilities. When software vulnerabilities are found, the provider will release updates to fix the issue. This is simultaneously a good and a bad thing: it means there's a quick fix to solve the issue, but it also alerts malicious actors to the existence of a vulnerability, and if they can exploit it before you patch it, then they have a gateway into your environment.

Enforcing a complete software patching policy should be high up on the agenda if you want to keep hackers at bay. The policy must apply all system patches as soon as they're released, and include all 3rd party software too. You'll also want to pay close attention to internet facing software – Adobe Reader, web browsers, plugins, etc – and ensure it's regularly updated.

Robust Security Protection

This goes without saying, but all devices need to be protected by an anti-virus solution – this includes company owned devices *and* BYOD. At present, a lot of your workforce may be carrying out their daily tasks from home, but the threat of ransomware doesn't go away once your staff are no longer in the office; if anything, being outside of your corporate perimeter puts your workforce more at risk.

Your security protection must be kept up-to-date with daily signature updates, and you'll need active file scanning, web page inspections, and memory scans too. We'd recommend vulnerability scanning here too – it's a 24/7 automated service that gives you a full overview of your current security posture, allowing you to spot vulnerabilities, track remediation, and immediately identify any areas of risk.

Security Awareness Training

Security shouldn't just be the concern of your CISO, or even just your IT team; security is everyone's responsibility within your business. Cyber-criminals often exploit the human factor – utilising phishing scams or taking advantage of weak security practices within your workforce in order to gain access to your systems and wreak havoc. Having fully clued-up employees who can spot a sophisticated phishing email, understand the importance of regular updates, and practice good password management can go a long way towards preventing a cyber-attack.

Effective security awareness training needs to go beyond "don't click on any suspicious emails" and "use a password that includes a capital letter and a number" – it needs to properly address the threats of today. Our training sessions are designed to first impart an understanding of different types of threat actor and their motivations, so that your teams know what exactly they're up against. We also cover the damage that hackers can do to an organisation, and provide an up-to-date overview of the techniques they use – from exploiting insecure wireless, to physical access, and sophisticated social engineering scams. By learning to identify these types of attacks, your workforce can become your organisation's strongest line of defence against cyber-criminals.

While our awareness training sessions are aimed at non-technical staff, we also provide advanced hacking & defending courses for the system administrators and developers in your business, where we demonstrate exactly how an attacker could penetrate a network, and how to mitigate that risk. These sessions are designed to teach your technical teams how to code with security n mind, ensuring that your web applications and networks are fortified against threats. Going beyond that, you can also invest in an asset security review which will assess the security of domains, software, and networks that have already been built, and how to make them more resilient to attack.

Offensive Security Testing

This list wouldn't be complete without penetration testing, which should be part of any modern security strategy. A penetration test utilises human intelligence and the latest ethical hacking methods to gain access to your organisation's networks, apps, and devices. By simulating a cyber-attack, our testers are able to locate vulnerabilities in your systems, but instead of injecting ransomware or trying to negatively impact your environment in another way, we review your security posture from the inside and help you make it stronger.

Penetration testing is embraced by forward-thinking organisations who want to test the strength of their security posture and develop their cybersecurity maturity level.

Sophisticated threats require sophisticated defence strategies; think of it as a way of double checking that your systems are secure, and if they're not, it's better to know about it. That way, you can work alongside us to fix issues and mitigate risks – long before a malicious actor can find and exploit them.

Brace for Impact

Cyber-criminals rely on their ransomware attack causing anxiety within your organisation, because the more panicked business decision makers are, they're more likely to make hasty choices that could lead to additional negative impacts. Instead, what you need is an incident response plan; you need to prepare for the attack in advance, so that if one does occur, you can carry out the steps in your plan with a cool head. It should include:

Backing That Thing Up

Take regular backups and send the results offsite to multiple locations so that if your office environment is compromised (online, or physically) the hackers can't access and destroy your backups. It's also worth using physical media that's not always connected to your network to store your backups, as this will also make accessing and corrupting backup data more difficult for the hacker. Verify the success of this process by regularly restoring devices using your backups – the last thing you want is to have the success of your business recovery depend on a process that doesn't actually work.

Preparing Your Workforce for a Ransomware Attack

You need to have an incident response plan in place that covers all bases. For example: are your teams prepared for ransomware attacks that occur outside of office hours? Unsurprisingly, threat actors tend to strike when there's less chance of resistance, so deploying ransomware and fully infecting a system while the cat's away is a strategy they often use. To mitigate this possibility, you'll need a list of tech staff that you can contact quickly to deal with the problem, and you should order that list so that if your first choice doesn't pick up, you have another expert as your second best option, and so on.

Incident Response Scenario Testing (aka Wargaming) is a great way to develop your incident response strategy by testing its effectiveness. We typically develop scenarios that are based on real-world attacks that have previously taken place, and with ransomware, there are plenty to choose from. We'll take you through the common stages of a ransomware outbreak to test how well your teams can identify, contain, eradicate, and recover from an attack.

Fighting Back

So what happens when the worst does occur and your organisation falls victim to ransomware? First of all – **do not pay the ransom.** It might seem like the quickest and easiest way to get your data and systems back, but you might be playing directly into the hacker's hands. Submitting to their demands now only tells them that you'll be willing to pay up again in the future, so what's to stop them infecting your systems again in a week's time?

Here's what you need to do:

1. Immediately enact your incident response plan.
2. Notify the relevant parties: your senior management team, your directors, and your staff. Keep everybody in the loop so that there's no internal confusion about what's going on.
3. Notify the authorities: contact ActionFraud and the ICO and make them aware of the situation.
4. Contact your organisation's lawyers and cyber insurance providers.
5. If possible, isolate any affected workstations to stop them from communicating with other hosts and spreading the infection, this may include disconnecting them from your network entirely and removing access to Wi-Fi.
6. Restore your devices using your backup.
7. Address the vulnerabilities that were exploited – this may require an incident response team to help you get to the bottom of it.

Since first gaining increased mainstream attention over the past few years – partially due to the devastating WannaCry and NotPetya attacks that hit the headlines a few years ago – ransomware hasn't slowed down. Every day, a new organisation falls victim to this particularly nasty software, but hopefully this blog post has proven that there is a way to turn the tide. A sophisticated adversary requires a sophisticated defence, so by investing in security, preparing for the worst, utilising the right tech, and – most importantly – keeping a cool head, you *can* defeat this enemy.

If you'd like to know more about how Secarma's offensive security and consultative services can help you protect your organisation against cyber-attacks, contact a member of our team today.