BEATING THE BADDIES

HOW TO WIN THE WAR AGAINST HACKERS

INCLUDING: OUR TOP

5

RECOMMENDATIONS

ACU IT Solutions

Managing the technology powering your business

BEATING THE BADDIES
HOW TO WIN THE WAR AGAINST HACKERS

The internet is brilliant. It enables us to communicate in real time with friends on the other side of the world, find the answer to pretty much any question and work more efficiently than ever before.

But all that convenience and opportunity comes at a cost.

The speed and anonymity provided by the online world has made it easy for a new wave of criminals to steal our money and data with surprisingly little skill or effort. Hackers stole more than £130 billion in 2017, of which £4.6 billion came from British victims, according to a recent report.

Cyber-crime is now the number one threat to businesses everywhere. But that doesn't mean a devastating attack is inevitable. There are plenty of ways to stay one step ahead of the internet baddies and stop your business becoming yet another statistic.

When it comes to staying safe online, complacency is the real killer. So never underestimate the importance of internet security or assume that hacking is something that only happens to other people. The brutal truth is that it can - and does - happen to anyone who takes their eye off the ball.

Modern businesses are finding themselves in a virtual war zone, battling a new wave of criminals who will stop at nothing to steal valuable data and cause long-lasting damage.

Like any war, strong leadership and a great strategy will significantly reduce casualties and improve your chances of victory. Although it was written way back in the 5th Century BC, Sun Tzu's The Art of War is still influencing business leaders around the world – and it applies to perfectly to the war against cyber-criminals.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles"

Staying one step ahead of the enemy means having a deep understanding of your own organisational flaws and weaknesses, as well as an acute awareness of your opponent's dirty tricks. When you know what you're up against you'll be much better equipped to fight back. Sure, they can still attack you, but they can only cause real damage if you're not properly prepared.

So, let's first understand the enemy by taking a look at the most common types of cyber attacks threatening businesses today.

MALWARE

Malevolent, malignant and malicious, Malware is a generic term to describe all kinds of nasty software specifically designed to cause pain and disruption. Often still referred to as computer viruses, they do their damage by infecting the host with something that makes them sick – just like a real-life biological virus. And in the same way bugs are spread among living creatures, malicious code is used to generate multiple copies of the virus that spread across entire organisations.

Once it's found its way into the system (usually when a user clicks on a dodgy link) malware can cause chaos and huge financial losses in an alarmingly short space of time. Within hours systems can become completely inoperable, devices can be spied on and huge amounts of data can be stolen and sold to the first available bidder.

RANSOMWARE

The modern-day equivalent of "your money or your life", ransomware attacks take users completely by surprise by threatening them will major data loss unless they pay up fast. This particularly nasty form of malware has the power to completely block an organisation's access to their own information until they pay a ransom.

Ransomware attacks were at an all-time high in 2017, but thanks to an increased number of corporations investing in robust security and back-up solutions, fewer victims are paying up today.

There were still plenty of attacks last year though (2018), and hackers are still constantly on the look-out for organisations with a more lackadaisical approach to data protection.

BOTNETS

The Internet of Things (IoT) has revolutionised the way we work, live and play, with everything from our mobile phones to doorbells connected via the internet. And of course, hackers have been more than happy to exploit this new-found connectivity.

Constantly creating new ways to infiltrate personal and business data, cyber-criminals have been using a variety of internet-connected devices called botnets to perform a variety of attacks. From denial of service (DDoS) and ransomware to spying and cryptocurrency mining, botnets are on the rise and they're wreaking havoc on devices all around the world.

One of the biggest reasons cyber-criminals are targeting IoT devices is that attacks can go undetected for weeks or even months. It's often only when something goes seriously wrong that the victim notices their device has been compromised.

PHISHING SCAMS

Phishing has been around for ages now, and it's not looking likely to disappear any time soon. Criminals rely on a combination of good nature and ignorance among their victims, and both are surprisingly common even in today's tech-savvy workplace.

Phishing scams work by sending targets emails that have been carefully crafted to look like they come from a trusted source, and they're often sent later on in the day when staff are less likely to be alert to threats.

A common tactic is to send an urgent email from what looks like the big boss needing an important job – like a bank transfer – done urgently.

Whilst that might sound like an obvious trick that only a fool would fall for, tens of thousands of victims take the bait every single day.

Never underestimate a human's ability to make mistakes when the pressure's on.

MAN-IN-THE-MIDDLE (MITM) ATTACKS

A bit like a nasty nosy neighbour, MitM attacks eavesdrop on transactions and conversations between two or more parties. Once the attacker has made their way into your personal or professional business, they're perfectly positioned to steal your data and destroy your reputation.

The most common way cyber-criminals use MitM attacks is through unsecured public Wi-Fi, which is why working remotely from your local coffee shop can be a really bad idea. It only takes a few minutes for an attacker to intercept a device and install malicious software that processes and duplicates the victim's data.

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS

Ever suffer with information overload? When there's so much stuff you have to take in and remember that your brain simply gives up and you find yourself incapable of intelligent thought? That's basically what a DDoS attack does to computer systems, networks and servers by flooding them with so much traffic that they're no longer able to perform simple tasks.

Once the network has been completely overwhelmed with emails and requests it becomes completely inaccessible, resulting in significant losses and often irreparable reputational damage.

ZERO-DAY ATTACKS

This kind of cyber-attack happens on the first day a weakness is found in a piece of software. Usually when a user becomes aware of a potential security risk they have time to report it to their software provider, who will in turn develop a patch (a bit like a sticking plaster) until a more permanent solution is available.

But in the case of zero-day attacks it's too late for a quick fix. That's why cyber-criminals are always listening out for news about potential flaws so they can act before the user has a chance to do anything about it.

STRUCTURED QUERY LANGUAGE (SQL) INJECTION

Cyber attackers perform SQL injections by inserting code into database queries, giving them complete control over databases and websites. It requires very little skill or knowledge to initiate an attack, but the effects of the stolen and misused data are often devastating.

"The greatest victory is that which requires no battle".

It's often said that prevention is better than cure, and that's certainly the case when it comes to IT.

Businesses targeted by cyber-crime fall into two camps: those who have prepared and those who haven't.

It goes without saying that the ones who have always put IT security low down on their list of priorities find themselves in the hottest, deepest water. The effects of even a relatively small data breach can last for months, even years, with many organisations finding themselves completely unable to recover from the loss of revenue, reputation and customers.

It's not a matter of IF your organisation's going to be attacked, but WHEN. According to a report from Hiscox Group, a small business in the UK is targeted by cyber-crime every 19 seconds – that's 65,000 attempts every single day.

Scary statistics indeed, but they can only do real damage if you're not properly prepared.

Any cyber attack will be inconvenient and worrying, but if you've got all your ducks in a row it doesn't have to be devastating. When you have the proper plans, procedures, software and support in place you'll always have the upper hand.

So, let them fight, sweat and exhaust their troops while you sit back and smile, safe in the knowledge that you've done everything in your power to protect yours.

HERE ARE OUR TOP

5

RECOMMENDATIONS

1. Create a culture of awareness

Around 88% of data breaches are caused by unsuspecting staff members, so make IT education a priority in your organisation. Run internet safety awareness courses and ensure that you and your staff are always up to date with the latest threats and how to avoid them. Schedule regular reviews and refreshers into your diary, and lead from example. If you're seen with Post-it notes displaying multiple passwords, or you regularly share login details, you can't expect your workforce to take security seriously.

2. Use strong passwords

Sure, it's a pain having to have separate passwords for all your different applications, but it really is better to be safe than sorry. Hackers have been stealing passwords for years because people make it so easy for them by using them on multiple accounts or choosing codes that even a toddler could guess. Strong passwords include a combination of uppercase, lowercase, numbers and special characters, and they should be changed once a month.

There's some great software out there these days that enables you to create (and remember) new passwords without having to keep coded messages in your diary or phone, so there's really no excuse for the likes of "Password1" or "123456" any more.

Multi-factor authentication is even better. Before being granted access to data, users have to do something to prove it's really them logging in. This can be as simple as receiving a text on your phone, or for ultra security, using a specialist device.

3. Be careful what you (and your staff) post

We live in a society where it's become the norm to over-share. From A-list celebrities to friends you haven't seen since primary school, it seems that everyone is happy to divulge each moment of their waking day in detail. This constant stream of personal information has given cyber criminals the perfect opportunity to target victims through social media, quickly finding out where they live, what they do for fun and where they work.

To minimise your chances of becoming a victim think about how much information you really want to share with strangers and make it policy for employees never to divulge business details online.

4. Avoid public Wi-Fi

While it can be great to take a break from the office and work from the local café or train, using free Wi-Fi leaves you wide open to attack. It's the perfect opportunity for cyber-criminals to steal passwords, customer data and banking details, quickly spreading viruses between multiple devices. If you or your workforce are going to work remotely, use a VPN (Virtual Private Network) to secure your connection, and be sure to turn off sharing on your device settings.

5. Develop a multi-layered approach to IT security

The most important tools in your arsenal are robust, up to date anti-virus software and firewalls which should be constantly monitored and regularly updated.

It's also essential to ensure that all software is regularly updated to avoid any vulnerabilities hackers

could exploit. Old, outdated computers also pose a significant threat, so undertake regular inventories of your entire system and schedule licensing renewals.

Even with the best plans and precautions, disasters can still happen. The world of cyber-crime is so rapidly evolving that even hardened security experts can't guarantee that a hacker won't come up with a new way to break in. So you'll need a backup in place. When your data is properly backed up in a secure place and regularly tested for vulnerabilities, any disasters that do occur can be rapidly dealt with and you'll have peace of mind that any lost data can be quickly replaced.

"In the midst of chaos, there is also opportunity"

It can seem like a scary old world out there, but being faced with a threat is a good opportunity to take stock.

An overhaul of your IT system can breathe new life into your organisation; streamlining workflows, facilitating teamwork and – *here's the really great bit* – actually saving you money.

We can show you what risks are present in your business.
Get in touch – and let's talk cyber security.

ACU IT Solutions
Managing the technology powering your business

www.acu-it.co.uk 0141 255 1617