modern networks

The 9 cyber threats you need to know about now

The 9 cyber threats you need to know about now

It probably comes as no surprise to read that cyber crime is a topic that's not going away any time soon.

According to a 2019 cyber security report, UK businesses are seeing anaverage of 146,491 attempted cyber attacks every day -that works out to around 100 every minute.

But despite increased awareness aboutcriminal activity, the figure continues to rise every year, with 2019's stats up a whopping179% compared to the same time in 2018.

With no organisation proving too small or too boring (or too big and high profile) for hackers to attack, this is a threat that simply can't be ignored.

So how can you stay ahead of the cyber baddies without investing too high a proportion of your precious resources? It starts with understanding the threats. Like Sun Tzu wrote back in 512 BC in the classic book The Art of War, the starting point for winning any battle is to "know your enemy".

So let's take a look at hackers' most commonly used tactics that you need to be aware of. We're going to deal with some techy concepts, but we'll explain them in a non-techy way.

1. Ransomware

Ransomware has become the poster-girl of cyber crime, with hackers making millions by corrupting files and demanding a ransom for their safe return.

It used to be that they'd focus all their efforts on large organisations like healthcare providers and multi-national enterprises, but they're now regularly attacking small businesses too. In fact they use automated software to target all businesses, all the time.

All it takes is one click on an infected link... and all your valuable data is being used as a blackmail tool. Some people are prepared to pay big to ensure they don't lose that data forever.

A new strain of ransomware referred to as LockerGogawas specifically created to target manufacturing and industrial companies; not only stealing data but physically harming machinery.

With ransomware architects now able to literally bring production completely to a halt, a no-nonsense approach to security has never been more important.

2. Malware

There are a host of different malware (malicious software) attacks being deployed by cyber criminals these days, all of which are specifically created to cause as much harm as possible.

Common causes of successful attacks include file sharing through insecure sites, downloading media and signing up to free software programs, so strict security mechanisms are a must.

This is something Modern Networks can do for you.

3. Cloud Abuse

Cloud computing offers a list of benefits as long as your arm, but it's still easily abused. The fact that we can all work remotely from our mobiles and tablets increases the risk of devices being lost and data ending up in the wrong hands.

Plus, with everything stored in virtual servers accessible from anywhere, it's crucial to proactively defend against malicious activity and have robust back-ups in place.

4. Insecure API Attacks

This thing called an API allows different pieces of software to speak to each other.But if they aren't created with strict security processes in place, hackers will soon be buzzing around your data like wasps around an ice lolly on a hotday.

There's very little you can do about this unless you're a technological whizz who designs software alongside your day job, so the safety of your organisation is very much in the hands of your provider.To avoid getting stung, be sure that stringent data encryption and authentication software is included before you buy.

5. Supply Chain Attacks

Supply chain attacks are a particularly nasty weapon in the cyber criminal's arsenal, and they're becoming increasingly common. Also referred to as third-party or value-chain attacks, they happen when someone from outside an organisation has access to its data. What looks like a legitimate software update is pushed out, but instead of updating it spreads a fast moving and destructive virus that has the power to take whole companies out of operation.

The most high profile example at the time of writing is the NotPetya attack, a Russian-masterminded piece of malware that released the most devastating cyber event businesses had ever seen. The virus spread like wildfire, turning computer screens black and disabling entire networks within minutes.

The really terrifying thing about NotPetya and its ilk is that the viruses spread on their own, with no need for human interaction. Until recently it was safe to assume that as long as people knew how to recognise an iffy email attachment, cyber criminals wouldn't be able to cause much damage. NotPetya has changed the face of computer viruses because it can take out hard drives all by itself.

According to a 2018 survey conducted by the Ponemon Institute, over half of organisations had suffered breaches that were caused by a vendor -further proof that you need to pick your suppliers wisely.

6. Poor Password Management

Weak passwords are pointless and dangerous, but millions of people are still cutting corners with easy to guess codes like Password1 and 12345678.

The impact is so serious it's predicted that passwords as we know them will be dead within the next few years. Instead of single-factor authentication (using one password to access an account) security conscious organisations are using multi-factor authentication instead.

To dramatically reduce hackers' chances of success, this uses:

- Something the person knows (such as a password)
- Something they possess (such as a code sent to a mobile)
- And sometimes, something they are (a piece of biometric evidence like a fingerprint or retinal scan)

7. Your Own Staff

Unfortunately, the weakest link in many organisations is often well-meaning staff. With the exception of sophisticated attacks like NotPetya, the majority of computer viruses need a human being to enable them, by clicking on a link or replying to a phishing email.

These attacks often happen at the end of a busy day when defences are low and people are thinking about going home. So it's essential that everyone is educated in how to recognise dodgy messages.

You'll also need to implement a robust plan for managing personal devices if people work on the go. Transport for London reported a huge 34,322 lost mobile phones at the end of 2017, along with 1,078 laptops, 71 games consoles and -staggeringly -10 desktop computers. It only takes a second to leave a device on a train, but the repercussions last a lot longer.

Regular backups and data encryption are a must if you want to avoid the drama of a mislaid mobile device. And let's not forget previous staff, particularly if they left under a cloud. Disgruntled ex-employees have been known to delete files, steal data, spread rumours and even access company bank accounts. So it's important to disable all access the second they leave the building.

8. Basic Data Loss

Cyber threats aren't always the work of evil geniuses hacking into computer networks. Data goes missing for lots of reasons, and it's usually completely accidental. It's happened to the best of us; spending hours typing away on a document, only to delete it at the last minute.Without a reliable back-up method, that file is lost for good.

14% of data loss is caused by human error, 10% is down to software failure and the rest is caused by hard drive crashes and system errors.

Data losses like this don't just take a huge amount of time and effort to fix, but they can seriously damage reputations too. And with GDPR now in full swing it's never been more important to ensure that accidents like these don't happen.

You'll need regular backups, 24/7 data monitoring and SSL security encryption to give you peace of mind that even ifthe worst does happen, your business criticalinformation will never be too far away.

9. The Internet of Things - IoT

It's a fancy phrase that's become quite a trend over recent years, but the Internet of Things (IoT) is really just about different devices being connected online.

With everything from heating to doorbells now being operated by our mobile phones while we're out and about, there have been understandable concerns about security.

Hackers are always on the lookout for weaknesses in new systems, so if you do invest in IoTtechnology for your business, make sure it's from a trusted provider who takes security seriously.

Knowing your enemy is a start

"So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss. If you only know yourself, but not your opponent, you may win or may lose. If you know neither yourself nor your enemy, you will always endanger yourself." - Sun Tzu

As technology continues to advance at record speed, so too do the threats. Companies of all sizes, across all industries, need to employ robust data management practices and create a culture in which online security is the norm.

It's important not only to understand the risks and what to look out for, but also to recognise any weaknesses within your own organisation that could leave you vulnerable to attack.

Contact us today for a no-obligation security health check and to find out how we can help you proactively defend against the fast changing world of cyber crime.

modern networks

01462 426500 | modern-networks.co.uk