THE 9 CYBER THREATS YOU NEED TO KNOW ABOUT NOW

net technical solutions

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 cybersecurity report, UK businesses are seeing an average of 146,491 attempted cyber attacks every day - that works out to around 100 every minute.

But despite increased awareness about criminal activity, the figure continues to rise every year, with 2019's stats up a huge 179% 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 criminals 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 which of the most commonly used tactics by hackers you need to be aware of. We're going to deal with some techy concepts, but we'll try to explain them in a non-techy way.

1

RANSOMWARE

Ransomware has become the icon of cybercrime, with hackers making millions by corrupting files and demanding a ransom for their safe return.

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

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

A new strain of ransomware referred to as LockerGoga was specifically created to target manufacturing and industrial companies; not only stealing data but physically harming machinery. With ransomware architects now able to bring production completely to a halt, a no-nonsense approach to security has never been more important.

Solution: **Anti-virus and mail filtering solutions are your first line of defence, followed by a strong firewall with UTM (Unified Threat Management). Staff education is also important as is locking down file permissions to only those who need it, to stop the potential spread. Finally make sure you have a secure, encrypted backup of data to the Cloud.**

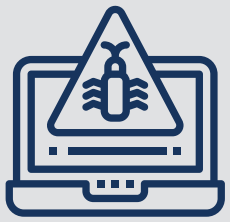
2

MALWARE ATTACKS

There are a host of different malware (malicious sofware) 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.

Solution: **Ideally you should have an acceptable user policy, ensuring staff know what software they should/should not be using/downloading. Anti-virus is important, along with regular malware checks using software such as Malwarebytes.**



Cloud computing offers a long list of benefits 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.

Solution: **Consider deploying MFA (Multi-Factor Authentication) and a strong password policy. Also consider introducing a company policy for BYOD (Bring Your Own Device).**

3

CLOUD ABUSE

4 INSECURE API ATTACKS

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 hot day.

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.

Solution: Ensure you only use mainstream software from reputable providers for line of business applications. Data should be encrypted and user access authenticated.

5 SUPPLY CHAIN ATTACKS

Supply chain attacks are a 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 acces 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.

Frighteningly, with NotPetya and its ilk 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 as 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 .

Solution: Again ensure you only use mainstream software from reputable providers and that software upgrades are managed carefully, ideally by your IT department. Always check you have a good restore point before actioning.

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 will be dead within the next few years and security conscious organisations will use 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)

Solution: Make sure your staff adhere to a clear password policy. This can be set at server level to ensure all staff follow the rules and can be put in place by your IT department if required.

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 viruses need a human 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 people are off-guard. So it's essential that everyone is educated in how to recognise unsafe messages.

You'll also need to implement a robust plan for managing personal devices if people work remotely. TFL reported a huge 34,322 lost mobile phones at the end of 2017, along with 1,078 laptops, 71 games consoles and 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. Unhappy ex-employees have been known to delete files, steal data and even acces company bank accounts. So it's important to disable all access the second they leave the building.

Solution: We can't emphasise enough the power of educating your staff to the pitfalls of IT security. Even a 10 minute staff meeting once a quarter, or a regular newsletter would help. It's also crucial to let your IT department know if staff leave, so that we can lock down account access. If your email is managed through 365, consider enabling the built in MFA function, which will stop hackers in their tracks.

8 BASIC DATA LOSS

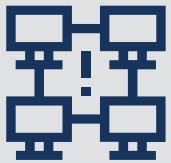
Cyberthreats aren't always the work of evil geniuses hacking into computer networks. Data goes missing for lots of reasons, and it's usually completely accidental. It's happened to the best of us; spending hours typing away on a document, only to delete it at the last minute. Without a reliable back-up 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 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 if the worst occurs, your business critical information will never be too far away.

Solution: We advise you to have at least two methods of backup in place, one local such as a tape drive, NAS box or removable media and one to the Cloud. We also have a solution from Datto that combines all of these neatly into one package.



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

Everything from heating and lighting to doorbells and CCTV can now be operated using our mobile devices when out and about. This has led to understandable concerns over security, and hackers are always on the lookout for weaknesses in new systems.

Solution: If you do invest in IoT technology for your organisation, ensure it is from a trusted provider and be sure to check what security measures are in place to prevent malicious access.

9 THE INTERNET OF THINGS - IOT

KNOWING YOUR ENEMY IS A START - BUT IT DOESN'T END THERE.

"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

net technical solutions

01252 235 235
sales@ntsols.com
www.ntsols.com

As technology continues to advance at record speed, so too do the cyber threats. Organisations 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 IT SECURITY HEALTH CHECK AND TO FIND OUT HOW WE CAN HELP YOU PROACTIVELY DEFEND AGAINST THE FAST CHANGING WORLD OF CYBERCRIME.