The Unusual Cyber Attack Routes You Need to Consider

The threat of a standard cyber-attack is increasing by the day and businesses across the world need to be aware that it's quickly become a case of 'when' not 'if' an attack will happen. When it comes to attack routes most people will be aware of the issues that surround weak passwords and the dangers of phishing attacks. But are you thinking about the more unusual cyber attack routes these threat actors use when considering your security?

With that in mind we outline five unusual attack routes you may not have considered and give you some tips on how to protect yourself.

1. When cyber becomes physical

Cybersecurity may seem like a technology issue and your company will most likely have a number of security measures in place to help prevent an attack via email or through your website. But one unusual cyber attack route that businesses often fail to consider is a physical attack.

That's right, a cyber-attack doesn't have to be conducted via a computer, it could be just as easy for an unauthorised person to enter your premises and plug an infected USB into a laptop.

There's plenty of tales out there, from attackers faking a CV mishap in an attempt to get front of house to print a new copy, to attackers leaving infected USBs near company premises in the hope that an employee will plug it in to discover the identity of owner. Even attackers using fake blood capsules whilst inside an organisation's server rooms to divert attention. It sounds like it's something out of a spy film, but it really does happen and organisations need to be aware.

So, how do you protect yourself against this threat? It's all about having robust processes in place in terms of visitors and ensuring that processes are consistently followed, no matter how plausible the story. Get reception to challenge people they don't recognise from entering the building, never plug in a USB from someone you don't know and never allow access to a visitor without checking with the people they say they're there to meet. If in doubt deny access.

2. Being too social

In this list of unusual cyber attack routes, is this type of attack so unusual? We all know about being safe on social media for personal reasons, but oversharing on Facebook, Instagram, and Twitter could lead cyber criminals to attacking your employer too.

Sometimes attackers research targets for months in an attempt to gain a nugget of information they can use to attempt access, in other cases they don't even have to try. Employees are more than willing to give the information away.

Social media, for example, can provide a treasure trove of information and oversharing employees may provide attackers with key information that they can use. Pictures of work ID badges, selfies of people at desks with passwords on post it notes in the background, tagged photos providing your location.

People may also overshare when it comes to public places. We've probably all overheard a confidential phone conversation on a train or in a coffee shop. It may seem like nothing, but to an attacker it could provide a way in.

Educating staff and putting in place the correct processes is vital. Employees need to be regularly trained on the consequences of leaked information and policies such as social media usage need to be enforced as much as possible.

3. Secure your IoT

The Internet of Things (IoT) is growing at pace and connected devices can now be found throughout the home, the office and within industry. From connected light bulbs and heating to CCTV and smart fridges. In the excitement of these new innovations are we considering security?

It's generally accepted that you should assess the security of your new website before it goes live. But, would you consider doing the same when you're adding a new smart coffee machine to your breakout area or before plugging a printer into your network? Not many would.

But are IoT devices really secure? A review of IoT security stories from last year suggests that many aren't and common vulnerabilities have been exposed time and time again. Default passwords, the inability to update firmware or install patches, unnecessary web facing features.

Yet, people are still happy to plug these devices directly into their networks and therefore provide a potential route in for attackers. So, how do you secure your IoT devices in your business? We've created a guide to help you.

Download your IoT security checklist today

4. Are your suppliers providing attackers a way in?

In 2013 the American retailer Target was breached and malware installed on store payment systems. This meant that attackers had access to the details of 40m credit cards used at the company's stores. But how did they get in?

It turns out they didn't hack Target at all, well not at first. Attackers gained access to Target's air conditioning supplier via stolen credentials and using the remote access privileges they were able to gain a foothold on the retailer's network.

This highlights the importance of third-party supplier security and companies need to ensure that the companies they work with have robust security measures in place to stop a similar situation happening.

5. Is your guest wi-fi just only for guests?

How far does your guest wi-fi extend and how secure is it? If your guest wi-fi is on the same router as your corporate network then there's a good chance that hackers can use guest access to pivot their way into your systems and to your vital information.

They don't have to be on your premises to do it either. If your wi-fi extends beyond your premises then attackers could be in a car outside, or the coffee shop next door.

The key here is to segregate your guest wi-fi from your main company router and to ensure that passwords are enforced on all connections.

How do you protect your business?

These are just a few of the ways hackers can gain access to your network and the techniques used are constantly evolving. It's therefore important that organisations consider a host of unusual cyber attack scenarios when thinking about the overall security of their company.

Testing is a big part of this security effort and it's essential that organisations are testing the effectiveness of their own security measures. But testing isn't a one size fits all process, there are a variety of different tests available to companies from vulnerability scans through to penetration tests or even a full red team exercise.

To learn more about the testing options available to your company and the benefits it can bring visit our testing information page to find out more.

Find out more about testing

Improve your security with Secarma

At Secarma we're here to support your security improvement efforts and to help you protect your business from constantly developing attack techniques. Whether that be through our Estate Discovery service, penetration tests or a full scale red team exercise, our experienced security consultants will work with you throughout the process to ensure you are employing the most effective security solutions for your company.

To find out more about the different kinds of unusual cyber attack, contact a member of our dedicated team.