3 MIN READ

6 CYBER SECURITY THREATS THAT ARE OVERLOOKED BY BUSINESSES

Bleam Cyber Security | Janine Griffiths

Blog post ~ 6 cyber security threats that are overlooked by businesses

The cybersecurity threat landscape is constantly evolving, and attacks are becoming more complex. In the past 12 months ransomware attacks have increased 64% year on year (https://blog.barracuda.com/2021/08/12/threat-spotlight-ransomware-trends/) between August 2020 and August 2021. No business is completely immune to falling victim to a ransomware attack, however thankfully many businesses are investing time and money to protect their systems and networks to reduce this risk. A large component of a strong security posture is ensuring that employees and businesses are aware of cybersecurity threats, and most will be aware of the some of the common threats, however there are many other threats that businesses may be unaware of. In this article we will discuss 6 cybersecurity threats that are commonly overlooked by businesses.

Shadow IT

Shadow IT is the use of IT hardware or software used by a department or individual without the knowledge of the IT department or IT/security provider. This software may include cloud services or applications that d... increase productivity or to solve shortcomings of the provi... using unauthorised software is that it may have a vulnerab... an attack on a business's network or systems. Similarly, if e... unauthorised file sharing platforms, it makes it possible for customer data to be vulnerable to a data breach. An example of shadow IT hardware may include

employees using personal laptops or smartphones to access company data or networks. The risk of introducing this hardware to a company network is that it may be infected with malware that could spread to other devices on the network.

USB Drop Attacks

USB drop attacks are attacks whereby the cybercriminal leaves a USB infected with malware outside a business's office space or in a carpark. An employee then picks up the USB and plugs it into a work device in an attempt to find the owner, but at this point it is too late and the device is infected with malware. This attack method has been the cause of many large-scale cyberattacks. Thankfully, it can easily be avoided through educating employees about the risk of inserting unknown devices into work computers.

Social Media Phishing

Phishing attacks are some of the most common attacks and have been for many years. These are social engineering attacks where an attacker sends a fraudulent message designed to trick an employee into revealing sensitive information or clicking on a malicious link. Typically, these attacks are through email, and many employees are wary of this and think twice before opening an email from an unknown sender. However, these attacks also take place on social media, where employees are less likely to consider the consequences of opening a link from someone on LinkedIn. Employees should treat messages on social media, or SMS messages with the same level of scrutiny they do for emails.

Insider Threats

An insider threat is an individual with legitimate access to company systems and data, that use that access, either maliciously or unintentionally, to cause harm to the organisation. This may include employees that are manipulated into performing malicious activities, such as downloading malware or giving away login credentials. These attacks also include employees or ex-employees that purposely infect a computer with malware or sell company data. A key method of preventing insider threats is to follow the principle of least privilege access, ensuring that employees are only able to access the data they require and nothing more.

IoT

Any device that has access to an organisations network or internet is vulnerable to being exploiting and used to spread ransomware throughout a business. This includes internet of things (IoT) devices. These are any devices that are connected to the internet and may include heating and cooling systems, smart speakers, TVs, CCTV systems or even smart coffee makers. Although all these items make benefit an organisation, they are at risk of being the entry point for a hacker. Businesses should be cautious about using these devices in an office space, and at the very least the devices should be on a separate network to other business devices, such as computers and servers.

Malvertising

Malvertising is a method of spreading malware using legitimate advertising space on websites. Cybercriminals pay for the advertising space and embed a small piece of malicious code within the advert that once clicked will direct the user to a compromised or malicious website. This will infect the victim's device with malware that can then spread through a network leading to a widespread malware or ransomware attack. Due to the nature of this attack, the best way to avoid falling victim is to keep all browser up to date and avoid clicking on advertisements.

These are some of the cybersecurity threats that are commonly overlooked by businesses. Each year there are more threats that businesses face, and it can be difficult to stay up to date with the everchanging cybersecurity best practices. If you want to keep your business secure with a comprehensive cybersecurity solution, get in touch with us today.

(//www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021)

The 6 worst cyberattacks of 2021 (//www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021)

Bleam Cyber Security (//www.bleamcybersecurity.co.uk/blog/author/bleam-cyber-security) : May 3, 2022 10:15:00 AM

2021 was a year of digital transformation for all businesses. The widespread adoption of remote and hybrid work has resulted in employees being more...

Cyber security (//www.bleamcybersecurity.co.uk/blog/tag/cyber-security)

Read More (//www.bleamcybersecurity.co.uk/blog/the-6-worst-cyberattacks-of-2021)

(//www.bleamcybersecurity.co.uk/blog/91-of-cyber-attacks-start-with-an-email)

91% of cyber attacks start with an email (//www.bleamcybersecurity.co.uk/blog/91-of-cyber-attacks-start-with-an-email)

 Bleam Cyber Security (//www.bleamcybersecurity.co.uk/blog/author/bleam-cyber-security) : Mar 21, 2022 2:01:59 PM

Email is the most common type of threat vector, and 23% of people click on malicious emails. It only takes one click for your whole network to be...

Cyber security (//www.bleamcybersecurity.co.uk/blog/tag/cyber-security)

Read More (//www.bleamcybersecurity.co.uk/blog/91-of-cyber-attacks-start-with-an-email)

(//www.bleamcybersecurity.co.uk/blog/an-exciting-update)

An exciting update... (//www.bleamcybersecurity.co.uk/blog/an-exciting-update)

Bleam Cyber Security (//www.bleamcybersecurity.co.uk/blog/author/bleam-cyber-security) : Feb 28, 2022 11:20:37 AM

Bleam Cyber Security has undergone an exciting acquisition. We are thrilled to announce that we have been acquired by Simpson Associates, (https://www.simpson-associates.co.uk/) a leading...

News (//www.bleamcybersecurity.co.uk/blog/tag/news)

Read More (//www.bleamcybersecurity.co.uk/blog/an-exciting-update)

SERVICES

Managed Services

- Managed Detection & Response for Email (//www.bleamcybersecurity.co.uk/email-detection-response)
- Managed Detection & Response (//www.bleamcybersecurity.co.uk/managed-detection-and-response)
- Managed Sentinel (//www.bleamcybersecurity.co.uk/managed-sentinel)
- Managed Secure Access
- Managed Private Access (//www.bleamcybersecurity.co.uk/managed-secure-access)
- Managed Internet Gateway (//www.bleamcybersecurity.co.uk/managed-secure-private-access)

Microsoft Security

- Managed Azure Sentinel (//www.bleamcybersecurity.co.uk/managed-sentinel)
- Azure Security Assessment (//www.bleamcybersecurity.co.uk/azure-security-assessment)

PROFESSIONAL SERVICES

Penetration Testing (//www.bleamcybersecurity.co.uk/penetration-and-security-testing)

Retained Incident Response (//www.bleamcybersecurity.co.uk/retained-incident-response)

Security Standard Readiness Services (//www.bleamcybersecurity.co.uk/security-standard-readiness)

Information Security Programme (//www.bleamcybersecurity.co.uk/virtualciso)

Cyber Essentials (//www.bleamcybersecurity.co.uk/cyber-essentials)

COMPANY

About Us (//www.bleamcybersecurity.co.uk/about-bleam-cyber-security)

Careers (//www.bleamcybersecurity.co.uk/careers)

FAQs (//bleamcybersecurity-25176453.hs-sites-eu1.com/frequently-asked-questions-1)

Blog (//www.bleamcybersecurity.co.uk/blog)

Events (//www.bleamcybersecurity.co.uk/events)

bleam (//www.bleamcybersecurity.co.uk)

(https://twitter.com/BleamCyber)

(https://www.linkedin.com/company/bleam-cyber-security)

Privacy Policy (//www.bleamcybersecurity.co.uk/privacy-policy)

Cookie Policy (//www.bleamcybersecurity.co.uk/cookie-policy)