Cybersecurity Trends and Threats Towards Businesses

Incidents of cybercrime and hacking were a fundamental component of 2018's security landscape. Many international companies and prolific brands were victims of significant and costly breaches, from employees swindling nearly $1.8bn from the Punjab National Bank in India[1] to the Coca Cola insider breach that stole 8,000 employee's data[2]. Often, organisations are unaware of a breach until it has caused substantial damage. Falling victim to a cyber-attack can lead to the exploitation of employee and customer data, reputational damage, loss of revenue and the exposure of sensitive company information. This bulletin is the first in a series highlighting cyber security tips and trends. Below are some of the main cyber threats that are likely to affect businesses over the coming year:

State-Sponsored Cyber Attacks

Although many states are heavily investing in bolstering their cyber-security defences, the weak national and international response to last year's hacks have highlighted critical infrastructural vulnerabilities. The increased accessibility of spying tools has enabled states to proliferate these technologies on a larger scale. Cyber-espionage, surveillance, cyber-sabotage and cyber warfare are increasingly being utilised as an offensive and defensive strategy. Both public and private organisations are at risk, particularly companies involved in major infrastructure projects, defence and weaponry contractors and organisations engaged in international trade. Cyber warfare is progressively transforming into the preferred method of attacking other states, given the low cost of launching an attack and reduced risk compared to traditional warfare. It is likely that state-sponsored cyber-attacks will escalate in 2019.

Ransomware as a Service (RaaS)

Ransomware, or malware, is a type of malicious software that restricts people from accessing their files. Attackers then exploit this position and extort money from victims by holding their devices or data to ransom and threatening to leak or erase data. The services industry is most affected by ransomware, accounting for 38% of reporting infections.[3] The most common delivery systems are phishing scams.

Insider Threats

In terms of data security, the most prominent threat to businesses is not from external forces, but inside threat actors. The majority of the most successful attacks last year were via malicious insiders. Insiders work closely with business IT systems and have access to crucial company data. Whether they intend to leak data or access privileged accounts, any exploited data can cause major damage. Often, large portions of data leaks from insiders are not deliberate. Employees are routinely targeted in spearfishing attacks or can unwittingly give access to sensitive information to an unknown third-party. The severity of attacks has increased over the past couple of years, and the trend is likely to continue.

Cloud Insecurity

Cloud insecurity is predicted to continue to grow in 2019. Single-factor passwords are one of the most easily exploited tools for threat actors. Despite the risk, they remain the primary security solution for the majority of organisations despite readily available multi-factor authentication strategies. Password-based breaches are set to continue on a daily basis in 2019.[4] Banking Trojans, crypto mining and ransomware are likely to continue to present malware challenges that will threaten businesses and consumers in the coming year. There is a high chance that traditional anti-virus software will not be able to provide effective protection. It would be valuable for organisations to revisit their cybersecurity strategies, investigate malware-focused solutions, and keep track of network activity.

[1] https://www.bbc.com/news/business-43110085

[2] https://www.scmagazineuk.com/coca-cola-hit-insider-breach-8000-affected/article/1472617

[3] https://www.ajg.com.au/ransomware%20risk

[4] https://securityboulevard.com/2018/03/welcome-to-the-era-of-cloud-insecurity-7-threats-unveiled/

If you would like any further information on any of the elements mentioned in this bulletin, please email the Securitas Intelligence Unit at:

soc.intelligence@securitas.uk.com