**Cybersecurity**

Cybersecurity is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. Cybersecurity is becoming a larger issue as there is increased reliance on computer systems, the internet, wireless communication such as Wi-Fi and Bluetooth and the increasing use of the internet of things devices. The increasing reliance of these technologies means that there is an increasing number of systems and therefore more potential areas of vulnerabilities (Itgovernance.co.uk, n.d.).

The most common tactic for network protection is a firewall. Firewalls can exist either as a software tool or a hardware device that is physically connected to the network (Oaic.gov.au, n.d.).

Where an intruder has managed to circumvent the firewall and network security, the next element to the defence of the system is the antivirus tools which are designed to scan hardware for malicious code. The aim is to, at worst, quarantine the malicious code and, at best, remove it before it can spread (Oaic.gov.au, n.d.).

Backup management is also an important piece of defending against cyberattacks. Backups allow organisations or individuals to mitigate risks with ransomware or other malicious code which may destroy data or software. Backups allow for the ability to recover quickly from an outage or data breach (Oaic.gov.au, n.d.).

Training is possibly the most value defence against cyberattacks. The most successful organisations protecting themselves from cyberattacks are usually those who run regular sessions on how staff can mitigate risks to their systems (Cyber.gov.au, n.d.).

Common areas where cybersecurity is prevalent:

* Financial systems

Financial systems are seen as an ideal target for hackers as the possible financial return for being able to compromise a system makes it an enticing target. There are many ways to compromise financial systems, ranging from access personal customer data to create identity fraud, to actually transferring funds or using stolen credit card details to gain a direct financial benefit. There are also attacks designed to disrupt the services of financial institutions such as denial of service attacks. Financial institutions have been continuously developing ways to counter the attacks. This includes a wide range of measures such as two-step authentication for online transactions, being able to instantly pause stolen credit cards and detecting unusual transactions and notifying customers via email or SMS text messaging that an unusual transaction has occurred. (Lin, 2017)

* Utilities and industrial equipment

Computers control functions at many utilities, including coordination of telecommunications, the power grid, and valve opening and closing in water and gas networks. Cyberattacks can disrupt essential services which depending on the length of time they are out, can be catastrophic (Zetter et al., 2016).

* Consumer devices

Desktop computers and laptops are commonly targeted to gather passwords or financial account information, or to construct a botnet to attack another target. Smartphones, tablet computers, smart watches, and other mobile devices such as quantified self devices like activity trackers have sensors such as cameras, microphones and may collect personal information. (Shahani, 2014)

* Businesses

Businesses are common targets as they can hold financial and personal data. Sometimes the data breaches can give hackers a large windfall for example Home Depot (Backman, 2014) and Target Corporation (Staff, 2013) in the United States of America having millions of customers’ credit card details breached. Furthermore, some cyberattacks are ordered foreign governments with the intent to spread their propaganda, sabotage targets.

Not all attacks are financially motivated however; for example in the Sony Pictures attack of 2014 the motive appears to have been to embarrass with data leaks, and cripple the company by wiping workstations and servers (Pagliery, 2014).

* Government

Government and military computer systems are commonly attacked by activists and foreign powers. Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records and financial systems are also potential targets as they are now all largely computerised (BBC News, 2012). Passports and government ID cards that control access to facilities which use RFID can be vulnerable to cloning (Liptak, Sciutto and Schleifer, 2015).

* Internet of things and physical vulnerabilities

The internet of things provides opportunities for misuse as the downside to creating more ease of use and connectivity. In particular, as the internet of things spreads widely, cyberattacks are likely to become an increasingly physical rather than a virtual threat. If a front door's lock is connected to the Internet, and can be locked/unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers in a world controlled by internet of things devices (Vermesan and Friess, 2013).

Currently most cybersecurity tools require human interaction or configuration. As an example, an IT team has to set up the antivirus system and backup schedules for an organisation and ensure that they are maintained. Artificial intelligence is expected to grow in the cybersecurity space (Secureworks.com, 2017).

In the future, we should be able to rely on smart tools to handle the bulk of event monitoring and incident response. The next generation of firewalls should have machine learning technology built into them, allowing the software to recognise patterns in web requests and automatically block those that could be a threat (Bocetta, 2019).

It is expected that the natural language capabilities of Artificial Intelligence will be the future of cybersecurity tools. The theory is that by scanning large portions of data across the internet, Artificial Intelligence systems can learn how cyberattacks originate and suggest solutions for decision makers within the organization (Bocetta, 2019).

The downside of artificial intelligence is that it will not be cheap and it is likely that only large organisations will be the only ones who are capable of affording the first generation of security products.

Currently, the most common way for verification to access a system or identify an authorised user is via passwords. Internet users create passwords for each website or service that they subscribe to online. This system can be frustrating to maintain as well as vulnerable to attack if they rely on simple passwords or use the same one for multiple sites. (Espinosa, 2018) There have been improvements in password manager software performance in recent years, most of which aim to simplify and strengthen online security by removing a large portion of the manual effort from the task through algorithms that suggest and store passwords complex enough to reduce your chances of being hacked (Bocetta, 2019).

However, developments in Artificial Intelligence could mean that passwords become a thing of the past. The idea is that the Artificial Intelligence would track every user within an organisation based on roles, privileges, and common actions. Any deviation from the norm would be flagged and require the person to use a second form of authentication, such as biometrics that scan fingerprints or facial features. This process could also of second form authentication could also extend to individuals accessing the internet and may make passwords a thing of the past (Bocetta, 2019).

Bibliography

* BBC News. (2012). No early ruling in McKinnon case. [online] Available at: https://www.bbc.com/news/uk-19506090 [Accessed 11 Jul. 2019].
* Backman, M. (2014). Home Depot: 56 million cards exposed in breach. [online] CNNMoney. Available at: https://money.cnn.com/2014/09/18/technology/security/home-depot-hack/ [Accessed 11 Jul. 2019].
* Bocetta, S. (2019). Is AI fundamental to the future of cybersecurity?. [online] CSO Online. Available at: https://www.csoonline.com/article/3402018/is-ai-fundamental-to-the-future-of-cybersecurity.html [Accessed 11 Jul. 2019].
* Itgovernance.co.uk. (n.d.). What is Cyber Security? | IT Governance UK. [online] Available at: https://www.itgovernance.co.uk/what-is-cybersecurity [Accessed 10 Jul. 2019].
* Espinosa, N. (2018). The Five Laws of Cybersecurity | Nick Espinosa | TEDxFondduLac. [online] YouTube. Available at: https://www.youtube.com/watch?v=\_nVq7f26-Uo [Accessed 10 Jul. 2019].
* Oaic.gov.au. (n.d.). Information from the Australian Cyber Security Centre about preventing and mitigating data breaches| Office of the Australian Information Commissioner - OAIC. [online] Available at: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/information-from-the-australian-cyber-security-centre-about-preventing-and-mitigating-data-breaches [Accessed 11 Jul. 2019].
* Liptak, K., Sciutto, J. and Schleifer, T. (2015). Experts: China might be building database of federal worker info - CNNPolitics. [online] CNN. Available at: https://edition.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/ [Accessed 11 Jul. 2019].
* Pagliery, J. (2014). What caused Sony hack: What we know now. [online] CNNMoney. Available at: https://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/ [Accessed 10 Jul. 2019].
* Secureworks.com. (2017). Cybersecurity Programs of the Future: What Will ‘Bench Strength’ Look Like?. [online] Available at: https://www.secureworks.com/blog/cybersecurity-programs-of-the-future-what-will-bench-strength-look-llke [Accessed 11 Jul. 2019].
* Shahani, A. (2014). NPR Choice page. [online] Npr.org. Available at: https://www.npr.org/sections/alltechconsidered/2014/08/06/338334508/is-your-watch-or-thermostat-a-spy-cyber-security-firms-are-on-it [Accessed 11 Jul. 2019].
* Vermesan, O. and Friess, P. (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. [online] Internet-of-things-research.eu. Available at: http://www.internet-of-things-research.eu/pdf/Converging\_Technologies\_for\_Smart\_Environments\_and\_Integrated\_Ecosystems\_IERC\_Book\_Open\_Access\_2013.pdf [Accessed 11 Jul. 2019].
* Wallace, G., Pepitone, J., O'Toole, J,. Isidore, C., Pagliery, J., and Johns, J., (2013). Target: 40 million credit cards compromised. [online] CNNMoney. Available at: https://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html [Accessed 11 Jul. 2019].
* Zetter, K., Zetter, K., Dreyfuss, E., Barrett, B., Matsakis, L., Barrett, B., Newman, L. and Newman, L. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. [online] WIRED. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [Accessed 11 Jul. 2019].