CYBERSECURITY & RISK MANAGEMENT SELF REPORT

Mohammed Shaad Mehboob Matcheswala (21065793)

CARDIFF UNIVERSITY

Index

RISK TO DATA 2
PHISHING AND MALWARE 2
DENIAL OF SERVICE 2
PUBLIC WIFI 2
LIMITATIONS TO EXISTING TECHNOLOGIES 3
VPN 3
ANTI-VIRUS 3
LIST OF RECOMMENDATIONS 4
GENERAL RECOMMENDATION 4
VPN 4
ANTIVIRUS 4
REFERENCES 5
CONTINUOUS ASSESSMENT MARKS 6

Since the pandemic, there has been gigantic development in work-from-home plans, and this doesn't seem as though this will at any point settle again, as plenty of organizations are planning their employees to continue with this scheme. However, since employees use a home public network while working from home, there is always a risk to data, employees or organizations can face. Most of the attacks which were experienced during the pandemic were phishing, malware, and denial of service(DOS) (Emenike 2021). The most common data risks are data-breach, data-loss, data-rot, data-corruption, compliance risk, privacy, deanonymization, dark-data, data-remanence, regulatory risk, personal data (Spacey 2017).

Data Risk

Three scenarios have been discussed based on the risks to data:

1. Phishing and malware

Mostly, the organizations provide devices to employees to work from home. Many attackers target mobile devices to send phishing emails and hyperlink attachments to carry out their malicious activities**.** If an employee accesses this kind of email and hyperlink attachments, their devices could be infected by malware and when they connect through their corporate network there is a high risk that they might infect the organization's devices, as cybercriminals are using websites to spread malware, spyware, and trojans. These types of malicious programs could be extremely lethal to the organization as this might lead to **data leakage** and **malfunction of the company's system** (Chigada and Madzinga 2021). This could further lead to **data breaches and data corruption**. For example, a virus named CoronaVirus was developed by hackers, which **corrupts the data** and cannot be later recovered. This was spread through software download links. It could work as a keylogger and could be also used for ransomware (Chigada and Madzinga 2021; Cook 2020).

2. Denials of service

In a DoS attack, an attacker tries to exhaust the resources of the server by sending junk requests, resulting in the **unavailability of servers** and later demanding a ransom to stop these attacks. Plenty of companies become victims of such attacks (Emenike 2021). A distributed DoS attack can also be performed through BlackNET RAT, a trojan that loads remote files on the victim's computer and converts the victim's device into a botnet (Dark Side Of BlackNET RAT - K7 Labs 2020). Viruses like BlackNET RAT could infect employees' devices if they click on any links which might contain malicious content.

3. Public Wi-Fi

Employees often use public networks like public Wi-Fi to connect with their companies. In this scenario, hackers could easily connect to this network and could infect the user with malware. Due to this, there will not only be a **risk to the personal devices** but also a huge risk to the **organization's data** (Chigada and Madzinga 2021). There are devices like Pineapple which acts as a hotspot honeypot (rogue access point) and through which the attacker could be able to capture all the traffic(Amity University et al. 2020). For instance, the **victim's credentials, organization's data which the victim is accessing, credit card details, etc. might be leaked.**

Limitations to existing technologies

VPNs

- Secure VPNs are one of the most important tools to connect to the organization in the WFH scenario. However, CVE-2020-5180 exposed a vulnerability in Viscosity open-source VPN, where authorized but unprivileged local users were able to escalate their privilege, by inserting a malicious library inside the memory of Open VPN.
- Employees might use their old and unpatched machines to connect to their corporate network through VPNs (Heath 2020) which might have plenty of vulnerabilities. If a hacker has infected that machine through malware and later the user tries to connect the corporate network, then there is a high risk that other machines inside the organization network could be infected (Bansode and Girdhar 2021).
- VPNs use encryptions to prevent malicious attacks by inspecting incoming traffic. This encryption should be free from known vulnerabilities. However, some VPNs use low-level encryption, due to compatibility issues. So may not be able to protect completely from some malware. (Heath 2020). for example, CVE-2015-7756 exposed vulnerability in Juniper ScreenOS through which the cipher-text was easily able to be decrypted.

Antivirus:

Using anti-virus provides risks to the organization's assets, even if the employees are working from home or working in an office environment.

- Due to many organizations' privacy policies of denying the complete analysis of the file data content, while transferring over the network, such privacy policies can render the effective scanning of cloud-based malware solutions. Moreover, malware solutions also query the cloud and store information about analyzed file contents, which can be a threat to organizations' privacy policies (Agrawal and Wahie 2016).
- N-version antivirus makes use of multiple malware detection engines, which may increase false-positive detection and can lead to an increase in redundancy, and overhead (Agrawal and Wahie 2016).
- Antivirus could sometimes fail to detect malware inside the system due to by-pass vulnerability. For example, CVE-2018-12238 and CVE-2018-12239 exposed the vulnerability of antivirus engines depending on patterns to identify malicious files and viruses. Due to the by-pass issues vulnerability, the scanning of infected files was skipped, so that they do not get detected.
- Most antiviruses are vulnerable to fileless attacks, as it is a new type of attack in which the attacker uses zero-footprint attacks, macro or non-malware attacks. In this type of attack, the attacker does not have to put malware on the system. (The Limitations Of Antivirus - A Guide. 2021).

List of recommendations

VPN

- VPNs should always be used by employees working from remote locations (Chigada and Madzinga 2021).
- Multifactor authentication should be used for authenticating the user when accessing the VPN. VPNs hardware should be updated with the latest version of firmware and security patches. Data transmission should use properly updated secure tunnels and their protocols. Sessions should be maintained with TLS encryption (Bansode and Girdhar 2021).
- A.14.1.2 Securing application services on public networks: information that is carried out on the public network must be protected from malicious activities, modification, and unauthorized disclosure ((ISO/IEC 27001:2013) 2017).
- Clients with older version software should not be allowed to access VPNs until the issue is fixed (Bansode and Girdhar 2021).

General recommendations

- A.12.3.1 Information backup: regular backup of software, information, and the system must be taken and tested in consideration with the backup policy of an organization ((ISO/IEC 27001:2013) 2017).
- For maintaining good cybersecurity, it is important that an organization follows proper cyber hygiene, must always verify the sources (files, software, etc), and stay updated (Chigada and Madzinga 2021; Abukri & Bankas 2020).
- A.12.2.1 control against malware: Organizations must make sure that the employees must be made aware of the risk related to cyber-attacks and in case of any cyber-attacks, measures should be placed to detect, prevent and recover from that ((ISO/IEC 27001:2013) 2017).
- Strict information security policies should be placed which should include data access control, extensive logging, and monitoring policies that must support remote access security (Chigada and Madzinga 2021).
- A.9.4.1 Information access restriction: access control policy must be defined to restrict access to information and application ((ISO/IEC 27001:2013) 2017).
- Additional security controls should be used for sensitive data, which are not allowed to be used generally when the employees are working remotely (Chigada and Madzinga 2021) to prevent risks related to data.

Antivirus

- Before opening any suspicious files, it is highly recommended to use virus-scanning tools. Moreover, scanning should be performed regularly through anti-virus software to catch malware. Protect the system through a proper firewall (The Limitations Of Antivirus - A Guide. 2021).
- Antivirus software should be updated regularly to reduce the chances of the system being infected by a new type of malware.

References

Chigada, J. and Madzinga, R., 2021. Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, 23(1).

Spacey, J., 2017. [online] Available at: <https://simplicable.com/new/data-risks>

K7 Labs. 2022. *Dark Side Of BlackNET RAT - K7 Labs*. [online] Available at: <https://labs.k7computing.com/index.php/dark-side-of-blacknet-rat/>

S. Alsehibani and S. Almuhammadi, "Anomaly Detection: Firewalls Capabilities and Limitations," *2018 International Conference on Computing Sciences and Engineering (ICCSE)*, 2018, pp. 1-5, doild: 10.1109/ICCSE1.2018.8374204

Emenike, S:., 2021. Data loss prevention in a remote work environment.

Bansode, R. and Girdhar, A. 2021. Common Vulnerabilities Exposed in VPN – A Survey. *Journal of Physics: Conference Series* 1714(1), p. 012045. doi: 10.1088/1742-6596/1714/1/012045.

Heath, M. 2020. *Four Risks to Consider with Expanded VPN Deployments*. [online] Available at: <https://www.f5.com/labs/articles/cisotociso/four-risks-to-consider-with-expanded-vpn-deployments> [Accessed 18 January 2022].

Anon 2021. Remote Working Changes Are Here to Stay-Are Your Network Vulnerabilities? [Online] Available at: https://www.netscout.com/blog/remote-working-here-to-stay [Accessed: 8 January 2022].

The Limitations Of Antivirus - A Guide. 2021. Available at: https://tucu.ca/small-business-guide-malware-viruses/ [Accessed: 10 January 2022].

A. Agrawal and K. Wahie, "Analyzing and optimizing cloud-based antivirus paradigm," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016, pp. 203-207, doi: 10.1109/ICICCS.2016.7542349.

Information technology— Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013) 2017. BSI Standards Publication.

Continuous Assessment

Date	Events	Grades
27/10/2021	Presentation Phishing during cyber security awareness week	Grade – A (out of 10)
9/11/2021	Discussion in class	Grade – C (out of 2)
24/11/2021	Discussion during group activity (week 8)	Grade – B (out of 2)
1/12/2021	Discussion during group activities	Grade – B (out of 2)
8/12/2021	CTF event	Grade – A (out of 2)