e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-12, Issue-1 (February 2022)
https://doi.org/10.31033/ijemr.12.1.13

Cybersecurity Risks in Remote Working Environment and Strategies to Mitigate Them

Dr. Vivekananth.P
Senior Lecturer ICT, ISBAT University, Kampala, UGANDA

Corresponding Author: Vivek.jubilant@gmail.com

ABSTRACT

Remote work is popular these days around the world although remote work provides flexible routine and work life balance, remote work also comes with huge cyber security threats. This paper analyzes the types of cybersecurity threats such as unsafe Wi-Fi networks, weak passwords, unencrypted file sharing, phishing schemes,cyber-attacks. This paper also discusses the ways of mitigating these risks such as formulating a work-from-home security policy, investing in zero trust model,multi-factor authentication,VPN,firewall and strong Endpoint Detection and Response(EDR).

***Keywords*—** Cybersecurity, Remotework, Cyber-Attacks, Cyberawareness

I. INTRODUCTION

The world has rapidly gravitated towards computer technology in the past few decades, and currently, organizations make computers part of their daily operations. Computer technology has made work easier for most organizations on various fronts, such as effective communication between departments and employees, leading to high efficiency. The availability of the internet has improved connectivity, allowing employees to work remotely and deliver regardless of their location. However, the benefits of working from home come with various risks associated with cyber security. Employees working from home are the weakest link to the organization, and intruders can easily use them to obtain a firm’s confidential data, leading to significant damages. Even though remote working poses numerous security risks, organizations can use various strategies to mitigate the risks and protect their data, as discussed in the following paragraphs.

II. SECURITY THREATS

Working from home requires employees to access work systems from home. These systems use internet connections, which allow employees to connect, and access company servers based on the nature of their work. Nevertheless, a single security mistake by an organization security system or an employee can see these connections interrupted, leaking critical information to the wrong people. The following are some cyber security risks associated with working from home.

Unsafe Wi-Fi Networks

Employees working from home need the internet to connect to the company’s servers. They mostly use home networks and public unsecured connections, which expose them to malicious individuals who can spot their links and harvest personal and confidential data (Borkovich&Skovira, 2020). For example, information sent in an encrypted form on plain text can easily be intercepted and land in the hands of cybercriminals. Park et al. (2014) state that home Wi-Fi networks remain easier for hackers than typical business networks. They are less likely to use firewalls and more likely to depend on low-cost consumer-grade internet routers that might have weaker security. Home users also make frequent password mistakes for their modems and Wi-Fi networks. These networks are usually shared with gaming or Internet of Things devices vulnerable to hacks, leaving the entire network vulnerable to remote hacks.

Weak Passwords

Many organizations have weak passwords with remote workers, but having employees working from home makes the passwords even more vulnerable. Help Net Security (2020) states that a recent survey determined that approximately 75% of individuals working from home use identical passwords across most of their online accounts. This unsafe behaviour could have detrimental consequences for organizations considering the recent increase in fraudulent activities and hacking. Help Net Security. (2020) highlights that approximately 42% of employees still have their passwords written down physically, and 34% save them on their smartphones, while about 27% of employees save their passwords on computers. Even though most employers create a safe working environment for their employees, workers seek simple methods, especially when working from home, meaning insecure passwords, putting the company and more significant risks.

Unencrypted File Sharing

Even though organizations might think of encrypting data kept in their networks, some might not consider encrypting when sharing from one place to another. Employees share a lot of confidential information daily, ranging from client account information to files and many more that a firm cannot afford not to protect from being attacked by cybercriminals (Škiljić, 2020). Sensitive information finding its way into the wrong hands could lead to identity fraud, theft, and ransomware cyberattacks.

Phishing schemes

Phishing denotes a type of online con targeting users by pushing them emails that seem to originate from a familiar source, such as internet service providers, banks, or a known individual in an organization (Federal Trade Commission, 2021). For instance, an email could be sent to an employee by an email address resembling the manager's, asking for specific information from an employee. Phishers use letter differences to create identical emails. For example, a company's email address could be using the single-story letter 'a' as one of the letters in the address. When creating the new email address, phishers change the letter to a double story. Most employees will not notice the difference and will willingly provide the information sought by the hacker. Sharma (2021) highlights that unsafe WI-Fi passwords allow hackers to access employee email addresses stored in individual gadgets, giving them a headstart on where to send their mails when seeking specific information. Therefore, employees working from home must be careful with any email they receive from "their colleagues" seeking personal of the company's crucial information.

Cyber-Attacks

Remote work operations blur the line between private spaces and organization security. Ikeda (2021) quotes a study by the HP Wolf Security department that working from home created security challenges to organizations, and sometimes firms had to compromise security for business stability. The majority of IT professionals interviewed in the study agreed that sometimes security takes a backseat to business continuity, especially if the situation demands that people work from home, such as during the pandemic. They agree that the circumstance has left most companies vulnerable to breaches of their networks, and it will not take long before a significant breach happens. As most people are expected to continue working from home past the pandemic, the situation is not temporary. Therefore, organizations must find ways to improve the security of their networks lest they have crucial information in the hands of the wrong people, costing them fortunes (Eian et al., 2020).Some employees use personal gadgetsunrelated to the company's security guidelines, while others feel that the security necessities slow work too much, hence ignoring them, leaving them susceptible to cyber-attacks.

III. RISK MITIGATION STRATEGIES

Even though working from home exposes organizations to cybersecurity risks, making them vulnerable to attacks that could negatively affect them, firms can develop and implement numerous strategies to prevent such breaches. Mitigating these risks requires that organizations develop policies guiding employee behavior regarding their operations from home and develop robust security infrastructure to prevent breaches.

Work-from-Home Security Policy

One of the most efficient strategies for remote working is to invest in a complete antivirus set for an organization and its personnel. Firms must insist on all devices used by employees working from home having an approved antivirus by the organization's information technology department. Malecki (2020) states that antivirus suites offer automatic remote work security against numerous threats, such as malware, spyware, viruses, Trojans, worms, and phishing scams sent through email. Another important policy that can save an organization is no sharing of passwords through mail even when requested. Family members should stay away from work and, finally, use a centralized storage solution as a policy to mitigate cybersecurity problems.

Investing in Zero Trust Model

Zero Trust denotes a security model used to secure infrastructure and data for the modern-day digital transformation. According to Ahmed, Nahar, Urmi & Taher (2020), the model addresses current business challenges, such as securing remote employees, hybrid cloud settings, and ransomware threats. Zero Trust addresses the following fundamental principles based on the National Institute of Standards and Technology (NIST) guidelines. It ensures continuous verification by ensuring all accesses are verified for all resources. It also limits the blast radius, thus reducing the effect of an internal or insider attack, should it occur. Finally, Zero Trust automates context collection and response, which entails behavioral information and the context from the whole IT stack for the most accurate responses.

Multi-Factor Authentication

Multi-factor authentication (MFA) defines security equipment that requires manifold authentication approaches from independent credential categories to ascertain a user's identity for any transaction using the company systems. Dasgupta, Roy & Nag (2017) highlights that it combines two or more independent credentials that a user knows, like passwords, what they have like security tokens, and their being, such as biometric verification methods. The primary goal of multi-factor authentication is to have multiple layers of defense, making it more difficult for unauthorized individuals to access their target.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-12, Issue-1 (February 2022)
https://doi.org/10.31033/ijemr.12.1.13

Firewall

Firewalls define network security tools that monitor and sieves incoming and outgoing information in a system based on a firm's established security policies. Roozbahani& Azad (2015) simplify this definition, stating that firewalls create barriers between private internal networks and the communal internet. Companies can use various firewalls, such as packet filtering, which analyzes a small amount of information and distributes it based on the filter standards. Proxy services protect systems by sieving messages at the application level, while stateful scrutinyscreens active connections to determine networks packages it should permit through the wall (Roozbahani& Azad, 2015). Finally, Next-Generation Firewall (NGFW) has a deep data inspection wall that inspects information at the application level.

Endpoint Detection and Response(EDR)

Endpoint Detection and Response(EDR) denotes a combined endpoint safety solution that integrates real-time uninterrupted monitoring and collection endpoint data with rules-based automated responses and examination capacities. According to Arfeen, Ahmed, Khan & Jafri (2021), the main functions of an EDR security system entail monitoring and gathering activity information from endpoints that could show any danger. It also analyzes information, identifies warning patterns, and routinely responds to identified dangers to eliminate, contain, and alert relevant security departments and personnel. Finally, it has forensic and analysis tools to research any identified dangers and look for apprehensive activities.

VPN

Employees working from home can also use Virtual Private Networks, which would help them stay private. VPN establishes a secure and encrypted connection between a device and the internet, giving a private link for data and communication while users use public networks (Singh & Gupta, 2016). VPNs work at the operating system level and reroute all the traffic through other servers, making it difficult for intruders to hack the system.

IV. CONCLUSION

In conclusion, computer technology has snowballed in the past few decades, allowing companies to make computers part of their daily operations. Computers have improved productivity by making work easier and allowing employees to work from different places. However, they also come with various risks, such as external attacks, leading to data breaches. Some factors that allow breaches include unsafe Wi-Fi networks, weak passwords, phishing schemes, and cyber-attacks. These threats can be mitigated through work-from-home policies, VPN, firewalls, multi-factor authentification, and Endpoint Detection and Response(EDR).

REFERENCES

[1] Ahmed, I., Nahar, T., Urmi, S. S. & Taher, K. A. (2020, Jan). Protection of sensitive data in zero trust model. In: *Proceedings of the International Conference on Computing Advancements*, pp. 1-5.

[2] Arfeen, A., Ahmed, S., Khan, M. A. & Jafri, S. F. A. (2021, Nov). Endpoint detection & response: A malware identification solution. In: *International Conference on Cyber Warfare and Security (ICCWS)*, pp. 1-8.

[3] Borkovich, D. J. & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems, 21*(4).

[4] Creese, S., Hodges, D., Jamison-Powell, S. & Whitty, M. (2013, July). Relationships between password choices, perceptions of risk and security expertise. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 80-89. Springer, Berlin, Heidelberg.

[5] Dasgupta, D., Roy, A. & Nag, A. (2017). Multi-factor authentication. In: *Advances in User Authentication*, pp. 185-233. Springer, Cham.

[6] Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H. & Fatima, Z. (2020). *Cyber attacks in the era of covid-19 and possible solution domains*.

[7] Federal Trade Commission. (2021). *Phishing scams. Phishing scams and how to spot them*. February 22, 2022. Available at: https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/phishing-scams.

[8] Help Net Security. (2020). *Home workplaces introduce new risks, poor password hygiene*. February 22, 2022. Available at: https://www.helpnetsecurity.com/2020/05/12/home-workplaces-password-hygiene/.

[9] Ikeda, S. (2021). *Working from home brings new cybersecurity challenges as workers commonly bypass inconvenient measures*. February 22, 2022. Available at: https://www.cpomagazine.com/cyber-security/working-from-home-brings-new-cybersecurity-challenges-as-workers-commonly-bypass-inconvenient-measures/.

[10] Malecki, F. (2020). Overcoming the security risks of remote working. *Computer Fraud & Security, 2020*(7), 10-12.

[11] Park, M. W., Choi, Y. H., Eom, J. H. & Chung, T. M. (2014). Dangerous Wi-Fi access point: attacks to benign smartphone applications. *Personal and ubiquitous computing, 18*(6), 1373-1386.

[12] Roozbahani, F. S. & Azad, R. (2015). Security solutions against computer networks threats. *International Journal of Advanced Networking and Applications, 7*(1), 2576.

[13] Sharma, T. (2021). *Evolving phishing email prevention techniques: a survey to pin down effective phishing study design concepts*.

[14] Singh, K. K. V. & Gupta, H. (2016, Mar). A new approach for the security of VPN. In: *Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies*, pp. 1-5.

[15] Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats. *International Cybersecurity Law Review, 1*(1), 51-61.