kriativ.tech

Edition No. 9 – 11-10-2021
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
DOI: 10.31112/kriativ-tech-2021-10-60

CyberSecurity - Risks of Telework

Pedro Ramos Brandao
Coordinator Professor at ISTEC – pedro.brandao@istec.pt
Manuel Martins
Master's student in Computing at ISTEC - manuelantonio.martins@my.istec.pt

Abstract

Nowadays, telework is increasingly seen as an issue that must be addressed importantly and that solutions are found to enhance and strengthen it. As a result, organizations are increasingly relying on hybrid models of telework and presential work. The purpose of this paper is to assess whether an objective approach in the correlation between the tools made available and employee training and awareness for good use practices will reduce the risks associated with telework.

Keywords: Telework, Cybersecurity, Professional Qualification

Abstract:

Nowadays, telework is increasingly seen as an issue that must be addressed importantly and that solutions are found to enhance and strengthen it. As a result, organizations are increasingly relying on hybrid models of telecommuting and presential work. The purpose of this paper is to assess whether an objective approach in the correlation between the tools made available and employee training and awareness for good use practices will reduce the risks associated with telework.

Keywords: *Telework, Cybersecurity, Professional Qualification*

I. Introduction

The evolution of the business world as well as the technological world that follows it, in which several constraints have emerged over time that put pressure on organizations to evolve and grow so that they can keep up with business trends, but also in constant evolution in their IT and communications infrastructures to optimize their resources and human capital. It becomes crucial to address the digital security of all existing traffic, both within your infrastructure and outside of it. This aspect gains weight when we have a growing number of professionals in production or telework outside the corporate infrastructure using other providers and services where their good security practices are not ensured by the IT department of the organization they belong to. In addition, organizations allowing their employees to continue their tasks and projects from home to maximize productivity [1] are also allowing the risks associated with the organization's digital security to be jeopardized. Organizations must be aware of the dangers that they are allowing. Still, it is also necessary that they can equip themselves with tools and proactive approaches to make this new reality safe for all parties involved.

II. Literature Review

In recent studies, we see the identification of workplace risks to understand the dangers between corporate networks [2] and home networks. It turns out that the risk of malware triples, whereby the risk of exposure to different

malware families increases by a factor of seven as well as more than twenty-five percent of the equipment used in home networks are exposed to the Internet and that in seven IP addresses, one is exposed and that allows access to their routers making real the fragility that we are all exposed and that we can be the target of a possible cyber attack.

The exponential increase in the number of employees who will be teleworking also increases, to the same extent, the exposure of these same IP's to the organizations and their associations, both in terms of hardware infrastructure and in terms of all the applicational structure necessary for the execution of the most varied tasks assigned to the organization.

According to Tangjiliang *et al.* [3], Privacy and security are the primary concerns for most users of social networks and the vulnerabilities that may be exploited.

According to the European cybersecurity agency ENISA in the 2018 report, it points out that information leakage has consecutively risen in the ranking of threats as the consequence of the lack of internal training for the dangers of social engineering [4].

In a 2018 global survey (Cyberedgegroup), 50.6% of healthcare organizations and 47.3% of small and medium-sized businesses reveal that insider threat is their most significant and primary security concern.

According to CyberEdgeGroup, [5], in research conducted in 2020, the main security obstacles that inhibit IT departments from defending themselves against cyber-attacks are lack of personal training, too much data for analysis, low-security awareness on the part of employers as well as employees.

According to BITSIGHT [2], It is widely recognized that employee training should be the best approach to maintaining security appropriate to each organizational paradigm.

In an identified study that covers vulnerability exploitation such as sending commands on the TR-069 and TR-064 protocols [2] which will allow, among other instances, the implementation of honeypots [6] to get as much data as possible through the failure in accesses made from home networks to corporate networks.

In another paper on telework, he also points to a new paradigm imposed by CoVID-19 regarding a new normal [7]. Thus, a new paradigm and adaptation of organizations emerge in being able to get the most out of their employees due to the worldwide CoVID-19 pandemic.

III. Approach

In the day-to-day life of users as professionals in their organizations, the focus is on their productivity and relationship to achieve goals and objectives set for them. The computer and digital tools that are at their disposal only provide the path for them to use. Cybersecurity is not presented to them as a concern that should go hand in hand in their daily lives unless that same employee is an integral part of an IT department and hierarchy. IT departments already have software solutions that allow them to aggregate, analyze all the activity of different resources across the entire IT structure of the organization through SIEM [8] however, at this phase, it cannot yet allow them to have the same kind of control over home networks as teleworking employees. Therefore, it turns imperative that the business strategies are to make their entire infrastructure as resilient as possible, as well as providing their employees with adequate training and adequate knowledge to minimize the impact of all the risk factors that put an entire structure at stake, thus making the whole organizational structure as robust as possible. Such robustness could be implemented by the following:

a) Virtual Private Network (VPN) - VPNs have become the most widely used tool for most organizations to address the massive increase in teleworking employees by extending encrypted corporate networks to their homes. However, the implementation of VPNs in the home environment may already present a risk in its early stages since, at the time of execution, they may already be compromised with malware or even exploit these vulnerabilities. When the Back-End is already compromised, the VPN will be used by those who want to use it with malicious intent. Therefore, a

parameterization that checks the integrity of the endpoint and a Multi-Factor Authentication (MFA) implemented is crucial. Furthermore, VPN solution providers themselves, with this growing need for VPN, also have to adapt, innovate, and evolve the infrastructures they provide to their customers, making it even more crucial to have exemplary implementation planning to detect vulnerabilities and planning their patching and failover.

b) Priority and Mobility - The concern of creating an ideal endpoint deployment scenario cannot be prioritized over the need to ensure the recovery of an organization's entire business process. So, after a roadmap with recovery management and implementation, it will comply with security standards and priorities that allow disaster recovery and failover situations to be aligned to an organizational control policy. After defining priorities, the issue of qualified and trained mobility for employees must align with an actual vision of the day-to-day professional situations, with the development of solutions that meet employees and their methodologies and adaptability in exploring solutions. We know that smartphones evolution has brought a window that employees will use to support themselves in the needs that arise in domestic contexts.

c) Home network location - From the moment the employee is no longer within the organization's network, there is a world of vulnerabilities that arise, from the entire home network with all kinds of equipment and gadgets to Internet of Things (IoT's) equipment are points that can be used in attacks.

d) Social engineering - It is essential and given the multifaceted universe that an organization can be composed of, to be able to add a layer of protection for attacks that may arise from afar, after all these same employees have an entire life mirrored in social networks in most cases, this same information can be used as a source to manipulate employees for the disclosure of privileged and confidential data.

IV. Discussion

We can identify several points regarding cybersecurity, so in this article, I will address the major risks, cybersecurity layers that are necessary to understand, tools or targeted solutions that should be implemented, making it a motivating and straightforward approach to drive a practical and functional implementation among employees, pushing them to explore, innovate, and undertake efforts to demystify cybersecurity and make the perspective of telecommuting a simple, helpful, and motivating model for both organizations and employees.

We can analyze several important points starting with the most significant risks found in cybersecurity for telework and how we can make organizations prevent and manage such situations.

The use of VPN is a crucial factor for encrypting communications, and thus, an IT department must ensure that all settings and policies are in place and carefully complied with them. It is as important to train employees regarding the mandatory use of VPN.

As for priority and mobility, it is also a focus of vulnerability that malicious players will potentially use to achieve their purposes.

Endpoint equipment must be provided with a centrally managed and up-to-date endpoint security system to mitigate potential attacks. If they occur, there is awareness of them for the IT team.

When using the home network, only proper training of employees on good practices can minimize their exposure to the Internet and potential cyber-attacks.

For instance, the organization might be sponsoring the implementation of a firewall so that the employee can more effectively protect his home network.

As for wireless network security, even in the home environment, security needs can and must be improved, like migrating the encryption protocols for wireless networks from WEP, WPA,

WPA version2 to WPAversion3 if the network allows it.

Passwords are considered a basic yet vital topic. It is up to the organizations to define standards and policies that encourage employees to adopt good and mandatory practices in the definition and constant renewal of their passwords. It is assumed that best practices and innovations in encryption and implementation are suitable for the latest technological innovations at the IT department level.

Regarding social engineering, the suggestion at the organizational level is to invest in training on safety protocols to detect these behaviors and adopt a proactive approach to prevent them.

Employees must be encouraged to use the equipment provided by the organizations, thus minimizing their exposure.

If they use their personal equipment, they should be equipped with tools to control security rules to prevent potential attacks.

Organizational investments must account in their planning for the evolution and constant change of the various environments that benefit from their structure to ensure that no vector that could be the target of a possible attack is left to chance.

V. Conclusion

This paper explored the confrontation of objectives, analysis of the object of study, revealing that creating ideal telework conditions is a path that can never be minimized or relegated to the background in contrast to the other priorities of organizations.

We conclude that it is crucial to implement technical security solutions and invest more and more in employee computer literacy to increase productivity and minimize the exposure of home networks to Internet vulnerabilities.

Security is never finalized. We can never give the topic closed, as cybercriminals will also always be innovative and adaptable to new trends and technological innovations. Most of all, a computer literacy training plan is created for all those involved in the entire process and collaboration within the organization. The next step that is intended to be taken following this article will be to explore the possibilities and innovations in computer illiteracy among employees and how we can evolve this area towards continuous improvement.

VI. References

[1] "Work from Home Cyber Risks – CyberExperts.com." [Online]. Available: https://cyberexperts.com/work-from-home-cyber-risks/. [Accessed: 19-Jul-2021].

[2] D. Dahlberg, "Identifying Unique Risks Of Work From Home-Remote Office Networks," p. 6, 2020.

[3] GundechaPritam, BarbierGeoffrey, TangJiliang, and LiuHuan, "User Vulnerability and Its Reduction on a Social Networking Site," *ACM Trans. Knowl. Discov. from Data*, vol. 9, no. 2, Sep. 2014, doi: 10.1145/2630421.

[4] L. Marinos and M. Lourenço, *ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends*, no. January. 2018.

[5] "CyberEdge 2020 Cyberthreat Defense Report Infographic | CyberEdge Group." [Online]. Available: https://cyber-edge.com/resources/cyberedge-2020-cyberthreat-defense-report-infographic/. [Accessed: 31-Jul-2021].

[6] " What's a honeypot? How do honeypots improve security | Kaspersky." [Online]. Available: https://www.kaspersky.com.br/resource-center/threats/what-is-a-honeypot. [Accessed: 21-Jul-2021].

[7] L. Bonacini, G. Gallo, and S. Scicchitano, "Working from home and income inequality: risks of a 'new normal' with COVID-19," *J. Popul. Econ. 2020 341*, vol. 34, no. 1, pp. 303–360, Sep. 2020, doi: 10.1007/S00148-020-00800-7.

[8] "IT Management Software & Remote Monitoring Tools | SolarWinds." [Online].

Available: https://www.solarwinds.com/.
[Accessed: 21-Jul-2021].