A Survey on the Status of Cyber Security during COVID-19 Pandemic

KIPKEBUT ANDREW[1], CHEBOR JOHN[2]

[1, 2] Department of computer science and I.T Kabarak University-Kenya.

Abstract- Cyber security today has never had a more crucial role to play than keeping mission-critical organizations and agencies safe from cyber-attacks especially during the COVID-19 pandemic. The rapid, prevalent adoption of work-from-home has put considerable strain on cyber security from both security experts and employees. In this paper we survey cyber security status based on three major study points: First are the tools that enable work from home secondly Cyber Security threats during pandemic and lastly is Security measures for maintaining security requirements such as confidentiality, integrity, availability and privacy. This study also longitudinally looks at the new normal technology adoptions for, employee-employer engagement approaches, and digital business process changes that are profoundly effective for business continuity after the COVID 19 pandemic.

Indexed Terms- Cyber-security, Covid -19, Pandemic Threats, and Measures.

I. INTRODUCTION

Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, recovery policies and activities, including computer network operations, information assurance, law enforcement among others[1]. Cyber-attack is now an international concern and has given many concerns that hacks and other security attacks could endanger the global economy. In typical day to day activities organizations transmit sensitive data across networks and to other devices as they conduct businesses. Cyber security strives to protect this information and the systems used to process or store it.

Recently, deceitful computer users have continued to use the computer to commit cyber-crimes; this has greatly fascinated people and evoked a mixed feeling of admiration and fear [2]. The expansion of the internet has led to increase the hacking space in the Cyber world. Cyber security involves protecting information and systems from cyber threats [2]. With the recent COVID -19 pandemic that has spread to most countries in the world, Cyber threats has taken a different dimension since most employees are working from home, customers are also buying products from the comfort of their homes as per their government directives, and as a result, keeping pace with cyber security threats, technology strategies and operations has become a challenging task.

II. RELATED WORK

According to CSO Pandemic Impact Survey, 61% of the security and IT leader respondents are concerned about an increase in cyber-attacks targeting their employees who are working from home. According to this survey, 26% have seen an increase in the volume, severity, and/or scope of cyber-attacks since mid-March 2020. The Center for Internet Security's (CIS) Security Operations Center (SOC) has seen an increase in remote desktop protocol (RDP) exploitation, due to malicious attempts to exploit teleworking capabilities. There has also been a significant shift to using COVID-19 styled phishing and malspam campaigns. Forbes magazine between January and March 2020, reported that the firm, spam and opportunistic detections increased by 26.3%, while impersonation was up 30.3%, malware by 35.16% and the blocking of URL clicks by 55.8%. Overall, detections were up by a third [3].

Most of these increases undoubtedly reflect the increased opportunity presented by current circumstances, with isolated employees and the potential lack of suitably robust verification processes, which threat actors will hope to heavily exploit under the present lockdown, quarantine measures in many countries. World health organization has declared COVID -19 a pandemic that has caused huge impact on people's lives, families and communities. It has changed organization structures, the way employees work and bringing with it new cyber risks.

The U.S. Health and Human Services (HHS) Department recently suffered a cyber-attack on its computer system, this incident was known as campaign of disruption and disinformation that was aimed at undermining the response to the coronavirus pandemic believed that the act was orchestrated by a foreign actor [4]. This attack jammed the HHS servers with millions of hits over several hours, fortunately didn't succeed in slowing the agency's systems. Another study from the University of Maryland found that hackers attack every 39 seconds_(umd edu). On average, data breaches cost $3.92 million. Cybercrime schemes evolve quickly and attackers don't discriminate. That's why companies of every size need to stay up to date on cyber security trends. Cybercrime schemes evolve quickly and attackers don't discriminate. That's why companies of every size need to stay up to date on cyber security trends. New schemes, more remote workers and the move to cloud-based systems all require organizations to take cyber security more seriously than ever. Failure to do so can be devastating to both your company and those whose data you hold [5].

Another study by Kenny Trinh (2020), Managing Editor of Netbook news hackers are creating videos of "CEOs asking employees to transfer money or give away other personal information" and "as this technology grows, it will become increasingly difficult to detect." [6]. This decision to keep employees home in order to follow social distancing guidelines happened so fast, many companies did not properly prepare. Cyber security wasn't a top priority at the beginning of the crisis, but now remote work poses one of the year's biggest threats

III. METHODS

The following methods are important in handling cyber security during pandemic. First of all the organization need to identify the technologies and tools that will support employees to work from home in order to maintain business continuity(figure 1), secondly is to identify the possible threats to this tools rolled out for remote working and thirdly identify the possible solutions to the vulnerabilities and threats that may affect this tools . Another very important task is reducing patch cycles for systems, such as virtual private networks (VPNs), end-point protection, and cloud interfaces that are essential for remote working will help companies eliminate vulnerabilities soon after their discovery.

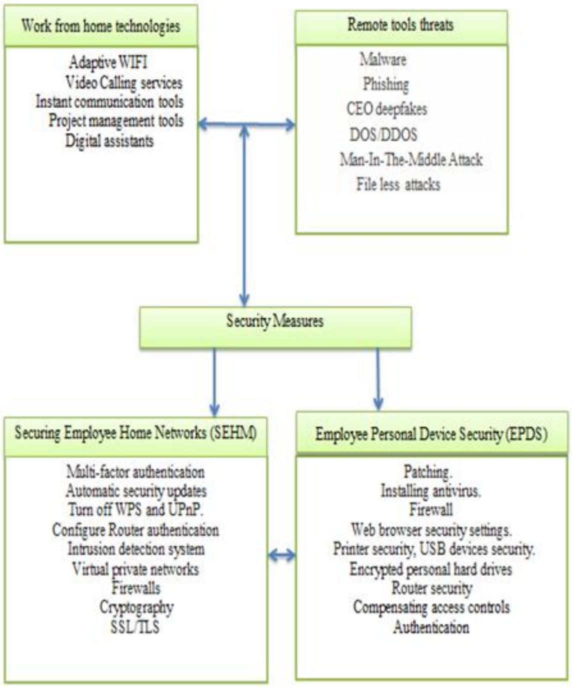
Work from home technologies
Adaptive WIFI
Video Calling services
Instant communication tools
Project management tools
Digital assistants
Remote tools threats
Malware
Phishing
CEO deepfakes
DOS/DDOS
Man-In-The-Middle Attack
File less attacks
Security Measures
Securing Employee Home Networks (SEHM)
Multi-factor authentication
Automatic security updates
Turn off WPS and UPnP.
Configure Router authentication
Intrusion detection system
Virtual private networks
Firewalls
Cryptography
SSL/TLS
Employee Personal Device Security (EPDS)
Patching.
Installing antivirus.
Firewall
Web browser security settings.
Printer security, USB devices security.
Encrypted personal hard drives
Router security
Compensating access controls
Authentication

Figure 1 the cyber security landscape (source, researchers)

A. Work from home technologies

With new pandemic Covid-19, working from home has been the most preferred method by organization in order to achieve their business processes and objectives, some of the technologies and tools adopted for this purpose include: Adaptive WIFI, Video Calling services, Instant communication tools, Project management tools, Digital assistants among others

i) Adaptive WIFI

Adaptive WFI allows networks to automatically switch between Wi-Fi and mobile data automatically to maintain strong network connection, for example if your Wi-Fi signal becomes weak or unreliable, your phone will switch to mobile data automatically. This makes collaboration more reliable.

ii) Video Calling services

Face Time, Messenger, Skype, Zoom, Google meeting and Hangouts, lets users to make video calls using a computer, phone and tablet. Users have options to use videos, mute or unmute .Figure 2 gives a UNAIDS and We Doctor organized a webinar bringing together health practitioners from China, Uganda and South Sudan to share experiences and knowledge in COVID-19 prevention and treatment. Figure 3, shows the analysis on video call services used during Covid -19 pandemic in different countries. Other video conferencing tools such as Google meeting and zoom has been used for the same [7].

Figure 2 Video conferencing (Source Unaids, 2020)

Instant messaging (IM) technology is a type of online chat that offers real-time text transmission over the Internet [8]. The most popular project management solutions are cloud-based, designed for the needs of virtual teams looking to access information from any location or device such as the use of mobile project management [9].

B. Remote tools threats

According to the results of the CSO Pandemic Impact Survey, 61% of the security and IT leader respondents are concerned about an increase in cyber-attacks targeting employees who are working from home , The survey further reported 26% increase in the volume, severity, and/or scope of cyber-attacks[10]. Some of these threats and attacks include:-

Malware: Cybercriminals are taking advantage of the *coronavirus* crisis to spread *malware*, disrupt operations, sow doubt and make money. Many organizations have tried to take steps in ensuring that employees are well-equipped to work remotely in a secure manner, threat actors of all types are taking advantage of the COVID-19 situation by spreading malware using Covid -19 thematic emails, chats and even social media.

Phishing: Digital Shadows reported of dark web markets that are advertising COVID-19 using a poisoned email attachment disguised as a distribution map of the virus's outbreak for prices ranging from $200 to $700, example of these themes include analyst's reports, health advice. Mime cast's 100 Days of Coronavirus report found that on average globally, RAR files were the most common form of delivering malware threats within emails during the pandemic, followed by ZIP files, with lesser trends around delivering malware through macros and ISO/image file formats present throughout this crisis[11].

CEO deep fakes: Criminals are using artificial intelligence (AI) -generated audio to impersonate a CEO's voice and con subordinates into transferring funds to a scammer's account. The Wall Street Journal reported that the CEO of an unnamed UK-based energy company thought he was talking on the phone with his boss, a CEO of a German parent company, who asked him to urgently transfer €220,000 ($243,000) to a Hungarian supplier. These kinds of threat are going to be common in the coming future [12].

DOS/DDOS: A downtime from an attack is even more disastrous especially with remote workforce. False negatively a larger remote workforce can even act as an unintentional DDoS attack by itself, simply because more remote users are trying to access services concurrently.

File less attacks. Cyber criminals don't need to place malware on a system to get in. File less or zero-footprint attacks use legitimate applications or even the operating system to launch an attack.

C. Security Measures

There are many measures to these threats afore mentioned, some the measures can be achieved at the client level or the network level.

i) Securing Employee Home Networks

The use of virtual private network (VPN) can add a layer of security, there are many simple steps employees can take to secure their home networks are a safe , some of these steps include:-.

- Practicing smart password management and enable multi-factor authentication (MFA) wherever possible.
- Enabling automatic updates for all routers and modems.
- Turning off WPS and UPnP.
- Configure the router or modem’s firewall with a unique password and enable the firewall.
- VPNs
- Cryptography
- Intrusion detection systems(IDS)

ii) Employee Personal Device Security (EPDS)

During this pandemic most employees use personal equipment instead of, or alongside, company-issued hardware. For employee EPDS the following measures needs to be observed: - Patching, Installing antivus, Firewall and web browser security settings. Employees should also secure their printers, USB devices, and maintained encrypted personal hard drives among others

iii) Secure Video Conferencing

Video conference capability has become common in helping employees continue to meet virtually. Keeping meetings private and password-protected, with a unique password for each meeting, is essential for enforcing security in order to avoid intrusions and thwart man in the middle attacks that may lead to impersonations or even loss of communication links.

D. Security analysis during pandemic

During the COVID 19 pandemic several video conference app were downloaded to facilitate virtual meetings as shown in figure 3.

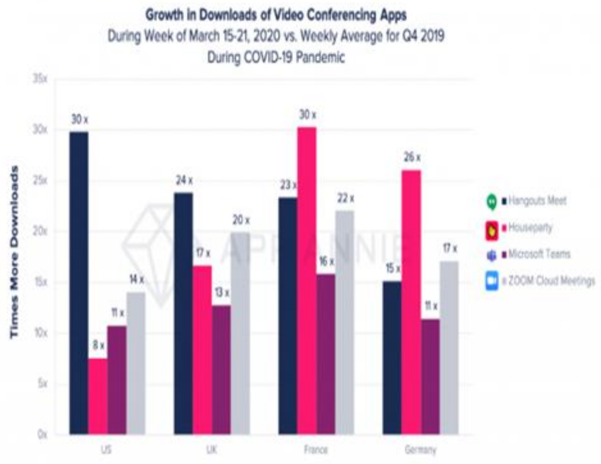

Figure 3 Growth of in downloads of video conferencing apps (source, techrunch.com).

Figure 3 shows the downloads made to video conferencing app during the week of march 15- 20, this shows an increase growth in US,UK ,france and Germany .Much of the growth is due to the increased adoption of apps like Google’s Hangouts Meet, Microsoft Teams and Zoom Cloud Meetings[13].

The March findings indicated that the food and beverage industry experienced more website attacks globally (+6%), especially in Germany (+125%). There were more attacks on the financial industry both globally (+3%) and in specific countries like Italy (+44%), UK (+21%), and Spain (+18%) [14].

A study performed by Google shows that many phishing attack escalated during March 2020, it during this period that pandemic was at its peak in most countries Jan, Feb and March months recorded 149195, 293235 and 522495 website phishing attacks respectively as seen in figure 4.

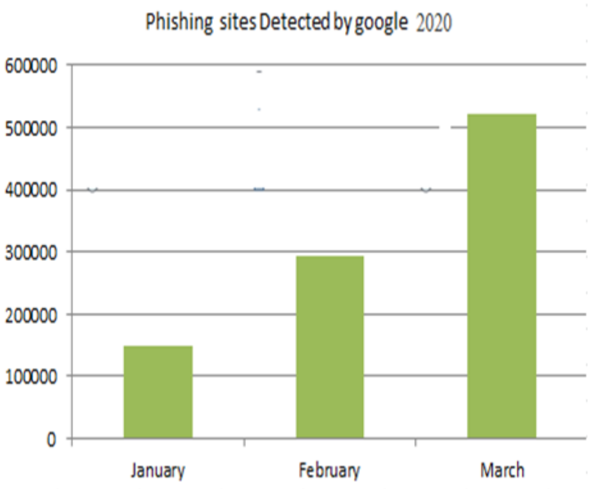

Figure 4 Phishing attacks on websites detected by Google between Jan –March 2020

Countries all across the globe are reporting an increase in cybercrime during the pandemic. For instance, in Italy, the Polizia Postale, which is the law enforcement branch in charge of the cybercrimes, reported several kinds of scams and frauds that came in the form of ads, emails, fake websites, but also through phone calls and messages [15]. Cybercriminals are capitalizing on the anxieties and fears triggered by the pandemic, using malware, such as viruses, worms, Trojan horses, ransom ware and spyware, to invade damage, steal or cancel personal data on personal computers.

CONCLUSION

The COVID-19 crisis has escalated the risk of malicious cyber-attacks as organizations large and small increase their reliance on remote working and online services. Conceivably most importantly, every organization should make sure workers have the right assets to remain productive, including tools to collaborate in teams and communicate efficiently with colleagues and suppliers. If secure tools aren’t provided, then users will find their own ways of working and connect on that are vulnerable, therefore compromising security. It is also important for organizations to upscale their cyber security during pandemic times to avoid data loss.

REFERENCES

[1] https://www.helpnetsecurity.com/2020/04/21/web-attack-traffic-trends/

[2] Jansweijer W Schreiber G, Wielinga B. IJCAI workshop on eradicating cybercrime in the world. In Towards Cybercrime Eradication, August 19-20th 1995.

[3] https://www.forbes.com/sites/emmawoollacott/2020/05/05/exclusive-cybersecurity-and-covid-19the-first-100-days/#7c52c53439d5

[4] https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

[5] https://i-sight.com/resources/11-cybersecurity-threats-for-2020-plus-5-solutions/

[6] Kelly, Jon (24 May 2010). "Instant messaging: This conversation is terminated". BBC. Retrieved 14 March 2018.

[7] https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[8] Kelly, Jon (24 May 2010). "Instant messaging: This conversation is terminated". BBC. Retrieved 14 March 2018.

[9] Margi Murphy, "Six free, mobile-friendly project management tools for your business", *techworld.com*, August 13, 2015

[10] https://www.cisecurity.org/white-papers/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/

[11] https://www.cio.co.ke/8-ways-attackers-are-exploiting-the-covid-19-crisis/

[12] https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#185170a62241

[13] https://techcrunch.com/2020/05/22/strategies-for-surviving-the-covid-19-series-b-squeeze/

[14] https://www.drizgroup.com/driz_group_blog/category/ddos

[15] http://www.unicri.it/news/article/covid19_cyber_crime