COVID-19
Cybersecurity Threats – Vulnerabilities and best practices to be secure

15 April 2020

Michael Ioannou

ELIAS
NEOCLEOUS
& Co LLC

COVID-19 Cybersecurity Threats and Vulnerabilities

Working from home has become the new norm for almost all organizations, due to the recent COVID-19 pandemic outbreak. Employees are now working from home using a range of devices, whether personal or provided by their organization. Many organizations are focusing on their business continuity plans allowing them to remain fit for purpose; thus, being able to continue offering their services without any disruption or delay. However, this prioritization of operational continuity may lead to the organization neglecting any security vulnerabilities that might have arisen during the implementation of contingency plans.

A vulnerability on a home device that acts as a medium to a corporate infrastructure (files, servers, emails, etc.) might lead to a security breach and cause significant damage to your organization, both in terms of finances as well as its reputation.

In these circumstances, the odds are overwhelming in favor of organizations experiencing a cyber security incident which may have dire consequences for the organization and/or its clients.

In this briefing we analyze the key threats and vulnerabilities created by the remote working environment, and then set out some best practice measures that can be implemented by organizations to mitigate those risks.

Threats

Confidentiality - Data Leakage / Data Theft:

Many organizations give employees the ability to access the corporate data remotely, which is akin to having "open doors" to the corporate data from anywhere and causes a headache for Security Officers on how to fortify the security posture of their organization.

Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. Data leakage threats usually occur via the web and email but can also occur via mobile data storage devices such as optical media, USB keys, and laptops.

Therefore, allowing the use of a home device, without the proper security controls, could easily give an advantage to attackers to gain unauthorized access to confidential data.

Availability - Malware/Ransomware:

A breach is not restricted to data leakage or disclosure of confidential information. Not being able to access your data, or any kind of destruction of data, are also considered breaches. Under the General Data Protection Regulation (GDPR) any kind of breach leading to the accidental or unlawful destruction or loss of data should be notified to the commissioner and data subjects without undue delay, but no later than 72 hours after becoming aware of it.

Such destruction of data could be caused by a type of malware called Ransomware. When executed, Ransomware encrypts all files in the network and usually the attacker demands ransom payment in order to allow the organization to regain access. There are several different ways that ransomware can infect your computer. One of the most common methods today is through emails, which will include a malicious attachment or links to a malicious website.

Integrity – Unsecure Connection:

Integrity refers to the process of ensuring the authenticity of information. Chiefly, ensuring that information is not altered and that the source of the information is genuine. An attacker could take advantage of an unsecure, unencrypted transmission and alter the information on its way to the organization.

Such transmission of data could be input in a system's database, email communication, payment process and any document file accessed by the user. By intercepting and altering the communication to any of the above-mentioned cases the attacker has the ability to cause the organization great financial losses.

Vulnerabilities

Endpoint Devices

For organizations that implement the BYOD (Bring Your Own Device) policy, which in most cases is a temporary solution as part of the measures enacted during the pandemic, employees are required to use their own personal devices. Therefore, organizations that had not previously been "fortified" in order to facilitate such a strategy, might find themselves exposed to great risks.

Moreover, contemporary studies by cybersecurity researchers indicate that attackers will continue to exploit vulnerabilities and issue threats to BYOD devices to disclose or destroy organizational data, primarily by using malicious software.

The main reason for this is that home devices are often unpatched, using an outdated operating system or software. Also, the lack of security controls such as basic antivirus software, access control and password policy enforcement on the device are additional factors that encourage attacks.

In addition, organizations should be vigilant and proactive not only towards outsiders, but also towards employees, who may attempt for any reason to exfiltrate confidential information or valuable assets that belong to the organization. Therefore, being able to access data from a BYOD without any controls in place might give the opportunity to a disgruntled employee to copy data for any malicious act causing damage to the organization.

Network

Remote working without a secure connection, such as a VPN encrypted tunnel, might lead to an interception of communication. In this instance, the attackers could maliciously alter the information on its way to the organization for their own benefit or steal information (e.g. bank transaction details, passwords, etc.).

Users

Employees are considered to be the weakest link in an organization in terms of cybersecurity. Studies have shown that more than 70% of data breaches are perpetrated through or by employees.

For example, unaware or uneducated employees might access a harmful website, click on a link or download an attachment included in an email. Subsequently a malicious software might be installed on their computers providing access to the attacker, in turn allowing the attacker to encrypt the data of the organization. Further, a breach or attack can also be facilitated through a social engineering method called phishing, in which the user may be tricked into willingly giving away their username and password.

Best Practices for mitigating Risks

Educate Employees

As mentioned earlier, the weakest link in an organizations' cybersecurity are the employees. Considering the threat of an unintentional incident due to an employee's lack of awareness or neglect, the best method to overcome this is by conducting employee awareness programs and by designing and implementing security policies and procedures.

An effective awareness program will help users to understand their role in keeping the organization's cyber space secure. After a successful awareness program, a user will think twice when presented with the decision of whether to open an email attachment, follow a link in an email or use a weak password. In addition, users will be able to distinguish a legitimate email from a phishing mail, as well as being aware of what rules need to be followed so as to not fall in the "trap".

VPN

Virtual Private Networks (VPN) are secure connections that protect information sent between employees working from home and the organization. They also encrypt data and prevent cyberthreats.

During the pandemic, a VPN can be a lifeline for companies, as it allows remote workers to access the same information they would at the office through a secure tunnel.

Multifactor Authentication

Multifactor authentication would be considered as an excessive security measure by most organizations, however, it is a crucially important feature. The importance of multifactor authentication is underlined when having to deal with remote workers using their own devices, which allows for the possibility of the device falling into the hands of a stranger.

There are three categories of multifactor authentication:

- "Something you know" i.e. Password,
- "Something you have" i.e. Phone, card, etc.
- "Something you are" i.e. biometrics, face recognition, etc.

By using multifactor authentication to login to the corporate network, there is supplementary security through the addition of more protection layers.

DLP Solution

Data Leakage Prevention (DLP) is a solution whose only purpose is to prevent data breaches from intruders. By analyzing and identifying the confidentiality level of all files of the organization, the DLP will block or send an alert whenever data is being moved within the network.

In addition to DLP, Data Encryption uses keys to encrypt and decrypt the data in the network. So even if a malicious individual was to gain access to the data, it would simply look like gibberish and would be useless to the attacker. Data Leakage Prevention and Data Encryption are more often than not distinct solutions but can be implemented at the same time.

Endpoint Security

The advantage of having antivirus protection is directly associated to the consequences of not having antivirus protection. It is considered the most basic security solution for end-user activities.

However, despite its rudimentary nature, using antivirus will at least protect computers from the most basic, well-known viruses. This is done by scanning the system against the known signatures of these viruses. It is essential to download and update the antivirus software systematically and be up to date with the latest virus signatures.

However, it should be noted that recent developments and cybersecurity solutions are introducing the Next-Generation Antivirus, also called EDR (Endpoint Detection Response), which identifies a threat through machine learning behavior analysis and helps prevent any zero-day attacks.

For more information related to any Cybersecurity or Data Protection matters please contact Michael Ioannou, the GDPR Department or your usual contact at Elias Neocleous & Co LLC.

Contact Us

ELIAS
NEOCLEOUS
& Co LLC

Elias Neocleous & Co. LLC, Neocleous House,
195 Makarios III Avenue 1-5th floor, Limassol,
CY, CY-3030, Cyprus,

+357 25110110

+357 25110001

info@neo.law

taskforce@neo.law