BLACK CELL

OFFSEC WHITEPAPER

TARTALOMJEGYZÉK

WHY DID REMOTE WORK BECOME INEVITABLE?

In order to stop COVID-19 from spreading, a significant number of organizations have ordered their employees, where possible, to work remotely or in Home Office.

In many organizations, systems deployed to provide mass remote access for employees and often had to make these solutions available as quickly as possible to the detriment of security. In many cases, protection is not developed and tested due to a lack of time or skills, or possibly due to the scarcity of the financial resources.

Despite the greatest effort and expertise, because of the short time available, there may be inadequacies, sudden adjustments, which can pose a serious security risk to companies and their employees.

Aside from human error, it is often noted that the simplest, cheapest (even free) solutions are preferably chosen in such situations. This not only worsens availability chances, but it also carries critical security risks (data loss, low level of prestige, loss of customers, severe corruption of the systems). In most cases, home networks do not meet the security standards required in the enterprise environment, thus the privacy of both the company and the user may be seriously threatened, as the corporate target for malicious attackers currently coincides with the home environment.

The current situation raises important safety concerns for both employers and employees. A successful cyberattack against an organization can not only cause data loss and lesser production, but can also result in access to the organization's accounts, intellectual property (data, source codes), personal and financial information, which the attacker can upload/sell on the Darkweb, channel it to a rival company. In addition, a successful attack can cause serious reputational loss for the organization, especially if the organization stores sensitive data about its clients. Forensic investigations, restoration, vulnerability detection and repair require a skilled, usually external team, more time, and much more resources than preventing an attack does.

Why is security so important now? Due to the panic caused by the pandemic and the unpreparedness of employees and employees' accessories, successful cyberattacks are expected to multiply and are expected to double the damage caused by attacks. Thus, it is strongly recommended that a preventive

approach and safety recommendations are taken into account when designing remote access, to minimize exposure.

How is it implemented?

Using RDP: In many cases, your organization provides remote desktop access over the Internet. Although its operation is user-friendly and easy to manage, opening this service to the Internet is not recommended, as RDP has numerous vulnerabilities and is likely to be exposed almost immediately, and may also disclose sensitive information about users or the operating system you are running on.

Using VNC: just like RDP, using VNC can provide remote access. The most common problem with accessing is that a password is usually not set to connect to, or even if it is, often weak, hence it is easy to brute force it.

By establishing an SSH connection: typically users are using Windows based systems, but they might want to remotely access a Unix based system which can be done via SSH. The most common mistake is that inappropriately configured privileges are provided, such as root SSH access, the successful attacker will have immediate authority over the system.

VPN is highly recommended when setting up remote access, because of its many features that are user-friendly, easy to use, and do not require professional knowledge of the protocol. Most VPN providers have multifactor authentication and the VPN connection established is also via an encrypted channel. Thus, much more resources are required to intercept and brute-force user data by unauthorized parties.

POTENTIAL DANGERS OF REMOTE ACCESS WORKING

The most common types of attack

As the vast majority of employees have never worked remotely or from home, they are significantly more exposed to individual cyberattacks. Taking advantage of the psychological pressures of closure and the pandemic, attackers increasingly target employees with phishing emails, which may come from senders mimicking trusted organizations or employees, suggesting that they are collecting donations or providing information about the coronavirus pandemic.

Phishing emails come in two main versions: the first version links the victim to an infected page by clicking on the link, requesting user information or credit card information and, in many cases, encouraging to download a document that installs a dangerous executable onto the victim's computer. The second type contains an attachment, which is most often an Office document (e.g. .xmlx, .doc, etc), a PDF, in rarer cases and executable program (.exe). Opening these on one's machine may cause either leaking sensitive information or granting access to the attacker.

Attacks on home routers, networks, machines, IoT devices have also multiplied with Home Office employees gaining access to the corporate network. A successful breach onto these home environments could allow an attacker to gain access to the internal systems. In many cases, an employee is connected to a public WiFi network where an attacker can intercept unencrypted data, including passwords and usernames used to log on.

Attacks on remote access programs (e.g. VPN, RDP, SSH, VNC) have also increased. Organizations often use legacy free software or do not patch it due to aiming for cost efficiency. Using outdated software is a major problem, as exploiting these vulnerabilities can cause an attacker to suspend full access or even gain access to an internal network.

Ransomware attacks have also multiplied in recent years, most of which are delivered via phishing emails or targeted attacks. Ransomwares encrypt data on devices and can spread to more than one machine over the network. In case of a Ransomware infection, most of the data cannot be restored because the implementation of encryption used to lock the victims' data does not contain any serious

errors, or the virus may delete the data immediately. Even though an organization has backups, due to network segmentation and lack of antivirus, they can also be encrypted, making data recovery extremely costly and often impossible at all.

An attacker may not launch an attack on the organization for the purpose of obtaining information, but because being intended to impede the operation of the organization. Such attacks are called Distributed Denial of Service (DDoS) attacks. The essence of these attacks is that they overload the application, making it impossible for customers and employees to access it, and can cause errors that require the application to be restarted.

Zero-day attacks against Home Office access tools and programs are becoming more common too. These attacks exploit vulnerabilities that were previously unknown. By doing so these are the most dangerous attacks, as there are no fixes for vulnerabilities, and detection is cumbersome, achievable only by implementing and maintaining multiple layers of security.

Which vulnerabilities are exploited?

During the remote working and Home Office, all work is based on remote access services. These are currently considered to be the most important points in terms of information security. Poor access configuration and lack of monitoring and testing can also significantly contribute to the occurrence of incidents. Misconfiguration is one of the most commonly exploited vulnerabilities, which in many cases could cause access to sensitive data.

Many standards require data to be encrypted or anonymized, but many organizations do not stand in line, so in the event of an incident, an attacker may access critical data, such as usernames, passwords, sensitive banking information, source codes, clients, or even critical system access information.

Employees have way fewer and less secure devices at home than in a corporate environment because they often have to use their own equipment (non-updated programs, lack of antivirus, vulnerabilities in residential routers, use of default passwords, operating system, detection tools and group policies being obsolete) hence they provide an attack surface. By compromising an employee's device the

malicious actors might gain access to the mailing, install a keylogger or other malicious software that can even access the internal network.
The sophistication of phishing attacks and the lack of cybersecurity training and awareness of employees can also lead to successful attacks.

In many cases, employees do not report the suspicious events immediately, therefore an attacker may have more time to build resilience on internal systems and then continue to operate. By detecting and responding in a timely manner, most attacks that compromise the entire system, could be prevented.

A poorly configured VPN can cause overload, which may prevent some or even all the employees from connecting to the internal network.

Statisics

According to a survey conducted by Heimdal Security, the number of security incidents increased by 30% compared to the pre-COVID-19 era. In line with this, the number of successful attacks has also increased significantly.

These statistics also show that the number of phishing emails has soared, taking advantage of the panic caused by the pandemic. Employees are mentally overwhelmed by being locked up and are more likely to fall victim to a phishing email offering information on the topic.

According to statistics created by OpenVPN, every third organization has been affected by cyberattacks. As the study says 36% of interviewed organizations have already been successfully breached due to poorly configured remote access. According to experts, this situation is expected to increase significantly due to the exponentially increasing number of Home Office environments.

Numbers of malware detected by antivirus software has increased dramatically since the introduction of Home Office. However, it is important to note that antiviruses cannot detect sophisticated viruses, so it is advisable to implement a multi-step security policy.

DEVELOPING OF REMOTE ACCESS WORKING

Safety solutions for creating Remote Access

When setting up remote access, it is recommended to use VPN, as by utilizing VPN data is sent over an encrypted channel and multi-factor authentication is also possible. VPN is highly user-friendly and can be monitored in many cases. However, it does matter what kind of VPN service provider the organizations use. One should choose a trusted provider that has verifiable references, even if it is a more costly solution, as these programs are constantly tested and improved, thus one can avoid utmost security incidents by having the correct patches and updates installed.

A critical point in the design is the proper setting up of the configuration. The preferences should allow for proper load balancing, should not contain sensitive data (neither configuration nor log files), and it is recommended that the user is getting logged off automatically after a period of time or in case of inactivity, along with being forced to re-enter the user credentials to reconnect.

Configuring logging is essential for both detection and forensic purposes. Monitoring the log files can help in identifying anomalies and malicious activity. The most effective way to do this is to connect them to a central system (such as SIEM) that can, after proper rules creation and configuration, alert the organization on potential incidents. In the event of a possible security incident, they provide information on how the attacker entered the system so repairing can be started immediately.

Providing corporate tools -where possible- are vital for users to deploy endpoint protection and to encrypt sensitive data.

It is important for the organization to be aware of the security risks of remote access and not only simply paying attention to securing but also maintaining the level of security is essential to minimize the attack surface. Thus, it is necessary to develop a policy alongside the system setup, based on the above points, which applies to all employees. It is recommended that this policy be reviewed and updated at least quarterly.

SECURITY TESTING OF REMOTE ACCESS DESIGN BY BLACK CELL

Description of the assessment

The purpose of the process is to uncover vulnerable services, leaked data that could lead to a successful attack

During the examination:

From public sources, we map remote access points to the organization (VPN, RDP, VNC, etc.) and search for leaked data (configuration files, username, email, password, open administrative domains, etc.) that could allow an attacker to gain access to the internal network.

Should the data not be available from a public source, then the pages or IP addresses provided by the organization will be scanned.

The next step in testing is the Black Box ('unauthorized') vulnerability testing of web logins and download interfaces that are accessible over the Internet, to determine whether they contain vulnerabilities that could allow an attacker to access sensitive information or gain remote access to the internal network.

The assessment also includes the testing the webmail interface.

The final phase of the operation is to set up a remediation and/or training package specifically for remote access, which can significantly reduce your organization's cyber security exposure to remote access.

Steps of the Remote Access Design testing

We investigate the relevant infrastructure and application following international methodologies (eg OWASP, NIST SP 800-15, OSSTMM) and innovative methodologies developed solely by Black Cell, to identify as many validated vulnerabilities as possible within the given timeframe.

The investigation begins with the exploration phase, which involves collecting data from publicly available sources (OSINT) and pre-evaluating the properties of the target. Subsequently, automated vulnerability testing and manual testing is performed to reveal the threat to the target (s).

Analysis and validation of the information collected to detect false positives. In the risk analysis phase, we list each vulnerability, outline the risks involved, and the consequences of exploiting it.

The result of the process is a summary report that includes a detailed description of the process, methodologies and tools used, the vulnerabilities discovered, their risk rating and evaluation, and suggestions for solutions to remediate them.

MONITORING REMOTE ACCESS OPERATION

STEPS OF THE MONITORING OF REMOTE ACCESS OPERATION

The following steps are required from operations team:

- One of the most important steps in operation is the proper implementation of Access Management, as most of the attacks are successful due to improper access management. Enforcing the "least access principle", granting only the privileges or accesses that are strictly necessary for the job to be performed (e.g., access only the network drives that the user must be able to reach, do not turn off the antivirus, network, do not run programs) and setting user privileges properly when an employee joins the organization are vital to maintain the security levels.

- It is necessary to keep a record of the permissions of users, and to periodically update and review this role-based access control matrix. Especially for users with higher access as these can be overlooked and get compromised in the event of an attack without being noticed. In many cases, when an employment relationship comes to an end, the account of the employee is not inactivated that poses a serious security risk. The above list is useful also for managing these scenarios.

- Monitoring of suspicious user activity (e.g. firewall, IDS / IPS / SIEM) is recommended.

- Developing mobile device management and mobile application management to filter out suspicious activity related to business phones, and to remotely manage device security (encrypting data, running a malware scan, or completely erasing data from lost devices) is advisable.

- Configuring network segmentation and logging, similar to the Remote Access Point.

- Creating an incident response and recovery plan.

- Provisioning online and offline backups.

- Keeping programs up-to-date by patching and updating; monitoring and updating VPN for vulnerabilities is the most important of all, because at the moment, it is about ensuring the continuity of the company's production, along with security.

- Cyber Threat Intelligence solutions help prevent passwords and sensitive information - associated with email address - from being leaked. Also, using the CTI, we can get specific information about attacks on segments and zero-day attack codes in advance.
- Developing educational materials for users to ensure they get accustomed with new systems and manage them safely.

From the users' side, the following steps are required:

- Changing the default passwords for home routers is a top priority.

- It is recommended to use strong passwords and, whenever possible, setting two or more factor authentication to increase the security level.

- Disabling sharing with other hosts on the network.

- Keeping the tools and software up to date by updating and patching.

- Operating only sharing platforms used by the organization (internal file sharing, company mail)

- Separating private and work activities: it is necessary to prohibit or restrict social media, private mailing on the workstation, and to exclude the execution of unknown programs, which also pose a serious risk to the organization.

- It is recommended to force the screen lock on the computer to prevent unauthorized access (child, etc.), data loss.

- Restricting the sharing of Home Office selfies and meetup printscreens: employees may share these kinds of images on various platform, but they may contain sensitive data such as link to a document, web access or meeting room access, or even passwords. It is advisable to delete sensitive information and educate employees to ensure sensitive media is not shared with unauthorized parties.

- It is extremely important to educate employees on how to detect and filter out phishing emails, as 90% of attacks are successful due to opening such emails. It is important to create security awareness amongst employees as they are more exposed to cyber-attacks in the home environment.

Factors to consider, and to raise your employees' awareness to recognize phishing emails based on the following signs:

- The most striking feature is that these emails contain a link that leads to a website resembling trusted page. In the current situation, attackers often exploit panic around COVID-19 and promise information on these websites. In each case, drag and drop the mouse over the link to see what page it is pointing to. If the page is unfamiliar, you must notify the security department.

- Although phishing sites use certificates, it is increasingly common for phishing emails to lead to unauthorized pages. If the link starts with "http: //" instead of "https: //", we may suspect phishing.
- Disguised as a letter from a financial institution or utility company.

- They often contain spelling or grammatical errors.

- Sometimes they are written in English or another (previously unused) language. If the service provider has sent the letters in Hungarian before, this should give rise to suspicion.

- Phising emails in many cases contain attachments instead of links (most often Office or PDF filetypes), which either exploit vulnerabilities in the outdated program or run code when opened.
- In case of sophisticated phishing attacks, emails may appear to be completely legitimate (e.g. detecting suspicious login regarding the victim's account, incoming CV, job search etc). In this case, the sender's email address (or IP address) may be a point of reference. If the sender is suspicious, you should report as well.

- It is unlikely that one has won without registering anywhere and it is unlikely that one will receive free products. So, if an employee receives an email like this in their inbox, should never open the link in it.
- Most phishing emails rely on human psychology, hence they often threaten to close the account or restrict access to a site. Victims tend not to thoroughly check the emails due to pressure of time.
- Emails may come from a seemingly colleague or organization leader, suggesting that the content of the letter is important and confidential. If the letter comes with an attachment, it is worth checking the sender.

- Dangerous links are often disguised as automatic tracker links sent by parcel services. This is especially dangerous as they may not only arrive via email, but also via SMS or through some applications that may compromise the employee's business phone.

- Microsoft login page looks like this:
  https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response (…)
- If the login page is not similar in structure, do not enter login information.

- Most service providers do not require login information for links sent in emails, if login is required for password change or other reasons, it is advisable to do so on the official site.

In these cases, the information security department should be notified immediately and the letter should be investigated, the employees who received the email identified and notified. It is important that whenever an email or application asks you to click on a link, always be careful and check the source!

BLACK CELL SAFETY TESTING OF REMOTE ACCESS OPERATION

Description of the assessment

The purpose of testing is to evaluate the privilege level of the remote access and the vulnerabilities of the network, furthermore to develop remedial suggestions, in addition to examining the exposure of remote accesses over the Internet.

The process begins with a remote workflow security audit, followed by testing the network security, access configuration settings and permissions with provided user-level credentials.

During the examination:

We assess vulnerabilities in individual applications, services, servers and devices available on the intranet.

If needed, we will test the detection capabilities and responsiveness of SIEM / IDS / IPS systems in collaboration with the organization's information security department.

In the end we compile a remediation and training package specifically for remote access, which can significantly reduce an organization's cyber security exposure to remote access.

Steps of the Remote Access Design testing

During the assessment, we investigate the affected system using international methodologies (NIST SP 800-115, OWASP, OSSTMM) and Black Cell to identify as many validated vulnerabilities as possible within the time available.

The investigation begins with an analysis of the structure of the network. With the client we determine which part of the network could be tested, which devices and applications are critical points of the system, what kind of and level of access is provided during testing.

By automated scanning and manually running scripts, we identify applications and devices that are accessed through the secured connection, and detect vulnerabilities in the system.

As part of the process, we test individual accesses and settings that limit the ability of a normal user to circumvent and access or use services, information, that are outside the user's grant level. Vulnerabilities discovered in the network, OS and application layers, along with the results are then manually validated to filter out false positive results.

In the risk analysis phase, we classify each vulnerability according to its level of criticality and then outline the risks involved and the consequences of exploiting them.

The result of the operation is a summary report that includes a detailed description of the process, the methodologies and tools used, the vulnerabilities discovered, their risk classification and evaluation, along with suggestions for solutions to remediate them.

SOLUTIONS, SERVICES WE PROVIDE AND SUPPORT:

- MetaAccess
- Metadefender
- Sophos MDM
- Sophos UTM
- SIEM
- WAF
- Vulnerability Assessment
- Penetration Testing
- Phishing simulation

REFERENCES

https://cybersecurityventures.com/cybersecurity-ceo-dont-let-coronavirus-fears-distract-your-employees-from-phishing-scams/

https://economictimes.indiatimes.com/tech/internet/covid-19-cert-in-says-spurt-in-cyberattacks-on-personal-comps-since-work-from-home-protocol-began/articleshow/74849119.cms?from=mdr

https://finance.yahoo.com/news/cybercrime-damage-costs-may-double-172000803.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAgAbv2BTOvXyXlEaIIf4DFwscA7IlG1bLKEZ2Ie3BH1hEM8DrACUHNIgYK1jvuKfsTngkEmgH9k7vYB99-gtJc7eHTgCSE-Q32_isCcPK_ml-vbIyD7v1X0-wCOFRmqXuo0uJFjaiLEfjZmoTfDKFWOKjWcvibbmbdoFdMnAmLT

https://heimdalsecurity.com/blog/cybersecurity-guide-for-small-businesses/

https://heimdalsecurity.com/blog/malicious-websites-work-from-home/

https://openvpn.net/remote-workforce-cybersecurity-quick-poll/

https://threatpost.com/coronavirus-poll-cyberattacks-work-from-home/153958/

https://www.avantechit.com/cyber-security-tips-home-office/

https://www.hornetsecurity.com/en/email-security-in-the-home-office/

https://www.ifsecglobal.com/cyber-security/10-ways-to-protect-your-business-from-cyber-attacks/

https://www.ifsecglobal.com/cyber-security/10-ways-to-protect-your-business-from-cyber-attacks/