Cybersecurity: Experience and best practices during COVID-19 pandemic

A. ROCHAIS, 6 July 2020, NETIA white paper

Table of contents

Introduction

With this white paper focused on the emerging cyber threat that we world is facing during the COVID-19 crisis, NETIA wish to share his experience, his initiatives and his knowledge on those topics.

Emerging cyber threat during COVID-19 pandemic

The cyber threat actors

The COVID-19 pandemic has radically changed the work habits of many companies, by forcing them to switch very quickly to remote work.

Some companies already had integrated some remote working habits but very rarely for their whole staff simultaneously.

This forced change resulted in uncontrolled cyber vulnerabilities.

The threat actors (people or entities who can cause, transmit or support a threat) have perceived this cyber weakness from companies and so are intensifying their activities during this period.

The state-sponsored groups

Many hacker groups sponsored by states have already used the COVID-19 topic to reach the targeted objectives (state actors or not) while using complex attacks:

- Vicious Panda (group suspected of being sponsored by the Chinese state) did compromise many targets from the Mongolian public sector using a text document in .rtf format send through spear phishing campaign (appearing to have been sent by the Foreign Affairs Minister of Mongolia).
- Hades Group (suspected of being sponsored by the Russian state) used the same entry point to deploy Trojan horses (through email appearing to have been sent by the Public Health Centre of the Ukrainian Health Minister) to attack Chinese targets.

There are many more examples and these states sponsored groups are deploying many resources to reach their target.

Attacks originated by state-sponsored groups are not the majority, but the media sector is particularly vulnerable.

Cybercriminal groups

Most of the attacks identified originate from cybercriminal groups (mostly motivated by financial gain).

According Proofpoint (USA), 80% of the current threats are using the COVID-19 topic to reach their targets.

A high risk level in the media sector

Media (audio, television and digital) are prime targets for state sponsored groups (cyberwar) or for non-state sponsored groups (cybercriminals, hacktivists, etc.). Controlling news and information is a strategic target for entities who seek to destabilize a country or an independent media. This well-known threat leads many states to protect information channels.

Specific recommendations have been made on this subject by the European Broadcast Union: EBU R143.

In 2019, we can find many examples following the TV5 Monde cyber-attack (suspected to be leaded by a group linked to the terrorist organization ISIS or by Russian hackers) : M6 Group, Sveriges Television (Sweden), Cadena Ser Radio (Spain), N1 TV (Serbia), etc.

The threats linked to remote working

The main threats linked to remote work are:

Threats on organizational assets

It means the destruction, the theft, the disclosure, the misappropriation or the blockage of assets which are critical for the company.

Those critical assets are vital assets for the activity of the company (production systems, source code, web site, brand image…)

Organizational assets mean every asset that is critical for external stakeholders.

Threats on personal assets

It means the theft, resale, disclosure, or fraudulent use of personal assets.

Personal assets could be the identity of the employees, or anything that can be linked to the identity of a person (bank account, social security number…)

In Europe, every company must protect those assets as part of GDPR.

The main types of cyber attacks

Phishing/Spear Phishing

The phishing is a process which permit to access to private information or to deploy a malicious software (like a ransomware) while pretending to be someone trustworthy

This happened generally by email send but can also be due to a malicious website.

The spear phishing is a highly targeted form of phishing involving social engineering (investigation to get detailed information on the targeted employees with the goal of deception).

Ransomware

The ransomware is malicious software that takes personal or organizational assets hostage, it can lead to a total block of a production system.

To be able to get the access to the system or data encrypted, the company will be asked to pay a ransom to the attackers. The last technology of ransomware is integrates data leaks (where attackers publicly disclose data if the ransom is unpaid).

Denial-of-service

Denial-of-service (DoS) attacks can be categorized by attempts from attackers to prevent access to legitimate users of a service (production system, web site, etc.).

This kind of attack can take several forms. Different types of protection can be used at the network level (Firewall, IDS…) or at the applicative level (WAF…). Free software solutions are usable on-site or in the cloud like the KEMP reverse proxy.

Another example: Project Shield is an initiative with the goal to protect news media from distributed denial-of-service (DDoS) attacks.

The vulnerabilities linked to the generalization of remote working

Vulnerabilities on the remote working tools

Many vulnerabilities that could be used to deploy ransomware or enable a data leak have been detected int the software solutions used for remote working (Citrix, Zoom, Fortigate VPN…).

The example of the videoconferencing platform Zoom is a concrete example (theft of 530,000 users account as well as links and meetings access credentials.

The growing number of brute force attacks on the RDP (Remote Desktop Protocol) from the beginning of the pandemic, detailed by Symantec is another concrete example.

The structural vulnerabilities

- The multiplication of external access to the enterprise network.
- The lack of regular updates deployment on Operating Systems, applications and firmware.
- The users, at home, often facing a lack of tools and the overload of their IT Service are constrained to use software or services not adapted with the company security rules.
- Vulnerabilities on software used for production.
- Daily usage of a personal Wi-Fi network, not as secure as the company network.

The human risk

The employees themselves are risks for the company's and for their own personal data. The risk can come from the use of IT tools but also from the deception (phishing), highlighting the need of cyber awareness in all organisations.

NETIA@Home, return on experience

NETIA built solutions with clients during the COVID-19 pandemic

During this changing period, we want to enable our clients to continue production workflows while limiting the cyber risk introduced by those new practices. In March 2020, we launched the NETIA@Home initiative.

Kit@Home

This part is about solutions designed around simple use cases that permit users to replicate their workflows in the condition of remote working. Those developments are tested by our radio partners and their users for continuous improvement and delivery. Our goal is to combine the client experience with a secured software solution adapted to the environment of each radio.

The tools delivered are allowing users to work independently from their home and to securely integrate media assets to the central production system of the radio through FTPS.

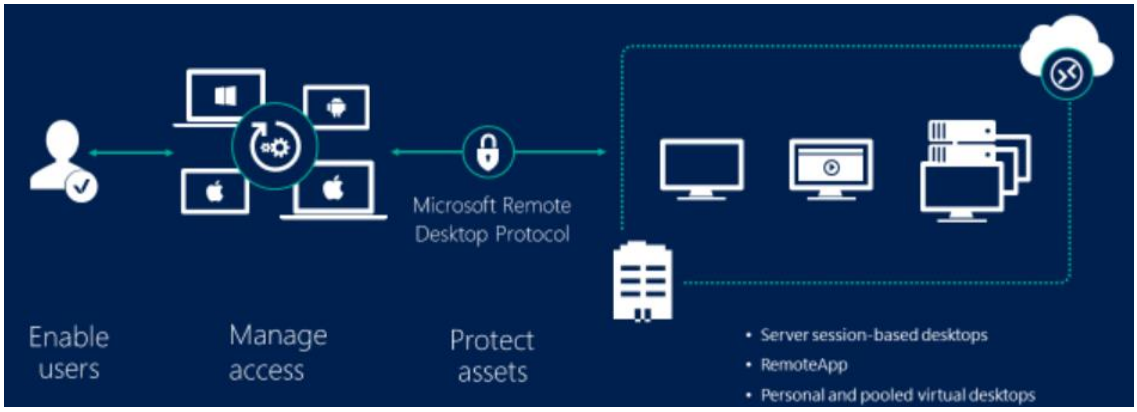
A web browser delivered as a web service to the clients permit them to connect securely with the central databases. This browser is reachable in HTTPS, is integrating modern authentication methods in conformity with the OWASP best practices. During the testing phase at NETIA we conduct Static and Dynamic security tests on the application.

Enterprise@Home

The solutions grouped under the name Enterprise@Home permit remote access to the entire RadioAssist application, as if you are at the office. We offer support to technical directors in integrating remote employees into production workflows.

We've accompanied clients in implementing solutions such as:

- Virtual machine installation
  - VMware, Hyper-V
- Usage of RDP
  - Access to the production software through secured Microsoft RemoteApp and reinforcement of operating systems.



- Cloud usage
    - Microsoft Azure, VMware Horizon…
- Utilisation of virtual private network (VPN) for access to certain parts of production tools.

To support our clients while ensuring the security of their company, NETIA is available to recommend reinforcement during opening of the web services to internet, during the implementation of remote access or in all other subjects that may represent a security risk for the company.

Risk reduction at NETIA during COVID-19 pandemic

With the objective to secure our employees and to defend the interests of our clients, NETIA did the following:

- Internal phishing campaigns simulation for awareness of the employees (using impersonation of sender's identity, malicious attachments and links to fake web sites)
- Security control and monitoring in remote access
- Usage of multifactor authentication for the sensitive accounts
- Automated and controlled OS and software updates
- Vulnerability analysis of the computers
- Security measures based on artificial intelligence and behavioural analysis
- Threat intelligence

In summary, you cannot deny risks in cyberspace, so NETIA invites you to consider the threats and risks mentioned in this document et to contact us for support you on:

- The protection measures
- The control adapted
- The tools delivered by NETIA to enable remote working