Cyber Security Risk Final Assessment Report

Court Clerk Smart Working

# 

# EXECUTIVE SUMMARY (max 250 words)

This report is produced for clerks of the civil and small claims courts of the Tribunal of Bengodi.

The below cyber security assessment regards on the possibility that the court clerks could work remotely from home due to the pandemic situation given by Covid-19. The qualitative and quantitative analysis are attached to this report in order to define the possible risks introduced by the smart working. First of all, it is reported the actual network infrastructure, then the proposal for the new one considering some adjustments for security reasons. After that, it is descripted the qualitative report with the main threats and vulnerability recognized. At the end, the quantitative report is summarized in order to show what has been analyzed and the overall costs. Moreover, any below schema is attached to be inspected better.

A summary:

1. Threats and risk and the worst possible impact: the analyzed threats concern on the confidentiality, integrity and availability on the supporting asset. An example of threat is the disclosure of information on the communication channel between clerk’s home and court internal network. The worst possible impact is the fact that a clerk can not work from home.
2. Mitigations and what changes in the risks with mitigations: the mitigations considered are useful to protect the possibility of the clerk to work from home safely. The overall risk is substantially decreased with the introduced mitigations.
3. Overall costs: the costs are principally for hiring security specialist and equipment to assure a correct and safe work environment. For example, it is considered the possibility to assume a network security engineer to configure critical functions of the network.

Work submitted in partial fulfillment for the course of Cyber Security Risk Assessment - University of Trento - a.a. 2020/2021

*This work is original work, has been done by the undersigned students and has not been copied or otherwise derived from the work of others not explicitly cited and quoted. The undersigned students are aware that plagiarism is an academic offence whose consequence include failure of the exam.*

Group 11: Nicolò Vinci, 220229

Cyber Security Risk Final Assessment Report

Court Clerk Smart Working

# TARGET OF EVALUATION

The entire scenario has been analyzed with the main purpose to offer a safe possibility to work remotely for the clerks. Below two schemas are reported and they represent the actual network infrastructure. Some assumptions are made to develop them, because the attached papers in the file BuildingScan-Smart-Court.xlsx have ambiguous data.

Network assumptions:

1. two routers to separate public VLANs (visitors and lawyers) from tribunal VLANs. One router to access external world.
2. “scanner location” gateway means the gateway where network scanning was started.
3. “Multimedia” network with IP address 10.186.6.1/23 under the VLAN 53 is considered with the IP address 10.186.6.0/23.
4. To resolve blank gateway of some networks:

* “Wifi lawyers waiting rooms” networks are attached to a gateway called Gateway Lawyers.
* “Wifi visitors” networks are attached to a gateway called Gateway Visitors.
* “Civil court judges” network is on the same gateway of the VLAN 18 that is 125.44.16.37.
* “Civil court clerks” network is on the same gateway of the VLAN 17 that is 125.44.16.37

|  |  |
| --- | --- |
| Immagine che contiene testo, nero, schermo, screenshot  Descrizione generata automaticamente | The actual networks in the building are reported for each floor in order to have a real view of where they are placed. |

**Figure 1** – Networks considering the Floors

|  |  |
| --- | --- |
|  | The actual network infrastructure is reported following the above assumptions. The VLAN are divided by colors. |

**Figure 2** – Network Infrastructure

# SUMMARY OF FINDINGS

The most security problems in the actual scenario concern on outdated softwares. Instead, for the smart working approach the security problems concern on the confidentiality, integrity, availability and authentication for the various network channels.

First of all, the subnet should be reorganized in different VLANs. It means that for each VLAN should be only one subnet and not more subnets in the same VLAN. After that, some internal firewalls are added to improve security and isolation between subnets. Moreover, an Intrusion Detection System is configured to monitor the incoming traffic and detect malicious flows. Two VPN servers have been planned in order to provide a secure network communication between clerk’s home and the internal network. There are two, because one is the backup VPN for emergency. Then, a data centre is used to keep the storage servers and logs. A room should represent this data centre. The room should be isolated from the other floors. At the end, a backup of the servers and log has been planned in a cloud infrastructure in order to face drastic situation and retrieve sensible data.

From the quantitative point of view, all the costs to add the above network components are considered in the document CVSS-worksheet.xlsx. For example, the costs for the cloud infrastructure depend on various factors such as the CPU and the memory of the virtual instance or the geographic position of the instance. Other costs depend on the quality of the product. Then, there are costs per hour for professional figures.

|  |  |
| --- | --- |
|  | The new network infrastructure with an Intrusion Detection System, internal firewalls, 2 VPN servers, data centre with inside storage servers and logs, cloud infrastructure for the backup and one subnet for each VLAN. |

**Figure 3** – Network infrastructure with the proposed security mitigations to be deployed

# RISK ANALYSIS

## Preliminary Qualitative Analysis

The complete summary of results can be found in the document SecRAM-worksheet.xlsx submitted as integral part of the current report.

At Step 1, the primary assets are identified and their impact is assessed (see table 1.1 and 1.2 in the document SecRAM-worksheet.xlsx). The primary assets founded concern the smart working scenario and it means that the main purpose is to make available the possibility for the clerk to work from home safely. The main primary assets are Enable the smart working, Ensure secure remote connection and Store data securely.

At Step 2, the secondary assets for the list of primary assets are identified (see table 1.3 in the document SecRAM-worksheet.xlsx). For example, for the primary asset Ensure secure remote connection, the secondary assets are Personnel, Company PC, Secure network communication between clerk and court internal network with VPN and Cryptography. The criticalities of those supporting assets principally are the human factor and the confidentiality, integrity and availability of the VPN. Another example concerns the primary asset Store data securely, where the secondary assets are Personnel, Secure network communication between clerk and court internal network, Secure court internal network communication, Storage servers, Data centre and Cryptography. The criticalities of those supporting assets principally are the human factor, the confidentiality, integrity and availability of the storage servers and the integrity of the data centre.

At Step 3, threats and vulnerabilities are identified for the supporting assets from the Step 2 (see table 2.1 and 2.2 in the document SecRAM-worksheet.xlsx). The impact and likelihood of each threat are estimated. For example, the main threats for supporting asset Secure network communication between clerk and court internal network with VPN are:

1. Disclosure of information
2. Denial of communication
3. Tamper communication
4. Lost communication

It has been assumed that the supporting asset may have weak protection against the confidentiality (someone could read in clear the communication), the integrity (someone could modify the communication data), the availability (someone could make unavailable the communication) and the unexpected events that could cut the communication. Then, vulnerabilities are identified for each threat. For example, for the previous threat Disclosure of information, it has been considered the vulnerability Misconfiguration of the VPN. Another example, the main threats for supporting asset Storage servers are:

1. Information leakage
2. Unauthorized access
3. DDoS attack
4. Tamper data stored
5. Lost data Stored.

It has been assumed that the supporting asset may have weak protection against the confidentiality (some information can be leaked and read in clear), the integrity (someone may modify the stored data), the availability (someone may try a DDoS attack to make unavailable some servers), the authentication method (someone can exploit a weak authentication method to access illegally into the server) and the wrong action (a clerk can delete data by mistake).

At Step 4, after that the threat impact and likelihood are founded at Step 3, the risk level can be estimated as impact times likelihood (see table 3.1 and 3.2 in the document SecRAM-worksheet.xlsx). First of all, the table used to evaluate the risk has been reported. Then, the threat impact and likelihood have been reported for each threat and the risk has been computed. The main threats can be identified after the risk computation. Each threat has a risk High, because actually there are no mitigation against the considered threats. However, the most important threats are:

1. Human mistakes: someone can always exploit human mistakes.
2. Disclosure of information: regarding the remote connection via VPN, because the clerks work with sensible data.
3. Unauthorized access: regarding the court internal network, because someone can access to a critical subnet and perform a malicious attack.
4. Tamper logs: someone can modify the logs in order to hide malicious actions.
5. Disclosure of cryptography keys: with them, someone can decrypt every data on the storage and log servers. Reading them in clear.

At Step 5, pre-controls and post-controls have been proposed to mitigate the threats identified at Step 3 (see table 4 in the document SecRAM-worksheet.xlsx). For example, to mitigate the threat Disclosure of information, the pre-control considered is to Configure correctly VPN in a secure way, because if the VPN is correctly configured it is difficult for someone to decrypt on the fly the data through it. Instead, the post-control considered is to check the logs to find the responsible, cut the communication, use a backup link, understand the damage and patch the VPN vulnerability. So, the attacker should be identified with this control. Moreover, thanks to a backup link the clerk is able to work while the network link is down to be fixed.

At Step 6, residual risk has been reported (see table 5 in the document SecRAM-worksheet.xlsx). The residual impact and likelihood founded at Step 5 are multiplied together to compute the residual risk. With the considered mitigation, the risk of all threat is decreased from High to Medium or from High to Low.

## Quantitative Analysis

The complete summary of results can be found in the document CVSS-worksheet.xlsx submitted as integral part of the current report.

First of all, some assumptions have been considered in order to develop the quantitative analysis (see paper Assumptions in the document CVSS-worksheet.xlsx). For example, to compute the cost for a security expert per hour, in a day have been considered 8 working hours, then 5 working days in a week and 52 working weeks in a year.

At Step 1, the vulnerabilities present in the actual network and the possible vulnerabilities present in the smart working scenario have been identified and reported (see table 1 in the CVSS-worksheet.xlsx). Then, the affected machines by the actual vulnerabilities have been also reported (see table 3 in the CVSS-worksheet.xlsx). In particular, 9 machines are affected by OS end of life detection vulnerability which has a CVSS score of 10. Most of the affected machines are in the Prosecutor – Head and Assistants subnet. Another example concerns on 41 machines that are affected by SSL/TLS: Report weak cipher suites vulnerability which has a CVSS score of 4,3. However, this is a critical vulnerability given the large amount of machines affected and the importance to have strong cipher suites in the internal network, because they are used to establish secure connections for various protocol such as Remote Desktop Protocol (RDP). The actual vulnerabilities considered in the network are:

1. Dropbear SSH Multiple Vulnerabilities
2. OS End Of Life Detection
3. Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
4. SSH Brute Force Logins With Default Credentials Reporting
5. Dropbear SSH CRLF Injection Vulnerability
6. SSL/TLS: Report Weak Cipher Suites

At Step 2, the power of attackers has been considered in order to establish which are the most important vulnerability in the actual network to be patched immediately. In the smart working scenario, it is appropriate to distinguish between network, adjacent and local attack, because there is a WAN link (from clerk’s home to internal network via VPN) and a lot of subnet in the internal network (LAN). Also, an attacker can exploit the machine locally. So, it has been considered to reconfigure the network infrastructure to have more isolation between subnets. Moreover, it has been considered to add some internal firewalss for more safety.

At Step 3, the priority and the risk are computed for the actual vulnerabilities present in the network. It has been considered the impact from the quantitative point of view based on [1] that reports the salary for a court clerk and [2] that reports the salary for a police officer. Also, the likelihood is reported from the quantitative point of view considering how many malware attacks have been performed in the 2019 from the article [3]. All the details are reported in the table 4 in the document CVSS-worksheet.xlsx.

At Step 4, the various costs of proposed countermeasures are identified in the table 5 and 6 in the document CVSS-worksheet.xlsx. The costs are taken from [4] to [20]. All costs are reported in Euro. There is not an overall cost, because some costs are considered per hour or per piece. For example, a network security engineer costs 50€ per hour. So, if the company does not assume this working figure, he will be paid per hour. Here, there are some professional roles which are considered:

1. Cyber security expert
2. Network security engineer
3. Application security engineer
4. Pentester
5. HR senior/junior
6. IT technician

At Step 5, the residual risk is defined for the actual vulnerabilities. The mitigations proposed are considered and they decrease the impact and the likelihood. For example, for the vulnerability OS end of life detection, a prosecutor loses only 1 hour instead 8 hours in a day with the post-control mitigation. Moreover, with the pre-control the probability is decreased by a factor of 4. At the end, also the benefit is computed in order to show hoy much money is saved per day with the proposed mitigations.

# ANNEX

An integral part of the report we attach the following documents:

1. Excel document reporting the application of SESAR SecRAM method (see file SecRAM-worksheet.xlsx).
2. Excel document reporting the application of CVSS Quantitative method (see file CVSS-worksheet.xlsx).

# REFERENCES

1. Prosecutor salary <https://it.talent.com/salary?job=pm#:~:text=Lo%20stipendio%20medio%20per%20pm,44%20750%20%E2%82%AC%20all'anno> . Checked on June 30, 2021.
2. Police officer salary <https://www.jobbydoo.it/stipendio/agente-polizia> . Checked on June 30, 2021.
3. Luca Zorloni, Responsabile economia e internet wired.it. <https://www.wired.it/internet/web/2020/03/05/cybersecurity-minacce-clusit/> . Checked on June 30, 2021.
4. Awareness training <https://nhlearninggroup.com/cybersecurity#:~:text=How%20much%20does%20cyber%20security,on%20the%20course%20you%20choose> . Checked on June 30, 2021.
5. Cost of cyber security expert, network security engineer, pentester, application security engineer: <https://mondo.com/blog-highest-paid-cybersecurity-jobs/> . Checked on June 30, 2021.
6. Cost of HR senior/junior: <https://www.tutored.me/it/hr-risorse-umane/> . Checked on June 30, 2021.
7. Cost of industrial electrician: <https://www.jobbydoo.it/stipendio/elettricista> . Checked on June 30, 2021.
8. RFID+biometric reader: <https://www.liberotech.it/it/lettore-biometrico-autonomo-per-controllo-accessi-lettura-impronte-digitali-e-rfid-anviz-t5pro.html> . Checked on June 30, 2021.
9. Cost of backup VPN: <https://www.usnews.com/360-reviews/vpn> . Checked on June 30, 2021.
10. Cost of Cisco firewall: <https://www.router-switch.com/Price-cisco-firewalls-security_c3> . Checked on June 30, 2021.
11. Security guard salary: <https://www.glassdoor.com.hk/Salaries/us-security-guard-salary-SRCH_IL.0,2_IN1_KO3,17.htm> . Checked on June 30, 2021.
12. Cost of camera: <https://itprice.com/cisco-gpl/civs-ipc-3050> . Checked on June 30, 2021.
13. Cost of fire system: <https://www.habitissimo.it/preventivi/impianto-antincendio> . Checked on June 30, 2021.
14. Cost of water detection sensor: <https://www.pcmag.com/picks/the-best-smart-water-leak-detectors> . Checked on June 30, 2021.
15. Cost of backup generator: <https://www.ernesto.it/prices/installare-un-generatore> . Checked on June 30, 2021.
16. Cost of electrical ground: <https://www.edilnet.it/guida/messa-a-terra-impianto-elettrico-quale-il-costo-289#:~:text=Messa%20a%20terra%20impianto%3A%20da,%E2%82%AC%20a%20700%2C00%20%E2%82%AC> . Checked on June 30, 2021.
17. Cost of circuit breakers: <https://campoelettrico.it/magnetotermico-differenziale-interruttori/magnetotermici-differenziali-abb/> . Checked on June 30, 2021.
18. Cost of cooling system: <https://www.cibsejournal.com/general/cost-model-data-centre-cooling/> . Checked on June 30, 2021.
19. IT Technician salary: <https://it.talent.com/salary?job=tecnico+informatico#:~:text=Tecnico%20Informatico%3A%20Qual%20%C3%A8%20lo%20stipendio%20medio%3F&text=Lo%20stipendio%20medio%20per%20tecnico,24%20500%20%E2%82%AC%20all'anno> . Checked on June 30, 2021.
20. Cost of retaining wall: <https://www.fixr.com/costs/retaining-wall-building#retaining-wall-cost-per-square-foot> . Checked on June 30, 2021.