Cyber Security Risk Final Assessment Report
Remote working of Tribunal of Bengodi

EXECUTIVE SUMMARY

This report was created to analyze and assess the Remote working of Tribunal of Bengodi, a mid-sized town in the North of Italy which needs to face the COVID -19 pandemic. The President of the Tribunal proposed the remote working of courts by suggesting few changes in regular scenario such as making some Court Clerk (Cancellieri) remotely available from home with a laptop so that it limits the visit to the office.

The remotely operated courts will work with Windows 10 locked down computers and will use a VPN software by using Juniper Junos Pulse to connect to their office computer with the same privileges. Other softwares will be used for remote communication like TightVNC or TeamSpeak.

This proposed report will analyze all the possible threats, risks and impact and then there will be detailed information about the mitigation and overall cost for all proposed new features and installations.

The main threats identified are caused by Denial of Service attack and unauthorised access to sensitive data, affecting the Clerks' ability to work on the assigned cases and communicate with the necessary counterparts.

However, most of the vulnerabilities can be mitigated by either updating the systems or setting up firewalls, whose cost (€ 500.000/3 years) is significantly lower compared to the risk of a successful attack as seen by the benefit (€ 80 million/3 years)

After the mitigations, the system is not endangered by major attacks and there is no likelihood of major data or financial loss.

Work submitted in partial fulfillment for the course of Cyber Security Risk Assessment - University of Trento - a.a. 2017/2018

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 consequences include failure of the exam.

NAME, SURNAME, STUDENT-ID ANISH KAUSHAL, 213870

NAME, SURNAME, STUDENT-ID ANISIA SPYROLARI, 213312

NAME, SURNAME, STUDENT-ID ZSOLT LEVENTE KUCSVAN, 213546

Cyber Security Risk Qualitative Assessment Report
Remote working of Tribunal of Bengodi

1. TARGET OF EVALUATION

As it was mentioned before, this assessment is done to evaluate the potential threats, risks and overall cost to implement a new secure remote setup for the Tribunal of Bengodi. The main focus is on the Clerk court and the modes of Communication.

During the making of this work, we mainly focused on the servers, architectures, softwares used and the remote communication channel.Hereafter we have listed all the necessary assumptions made in order to evaluate the future architecture to be built. The data flow and network architecture of the tribunal has been depicted in the below figure.

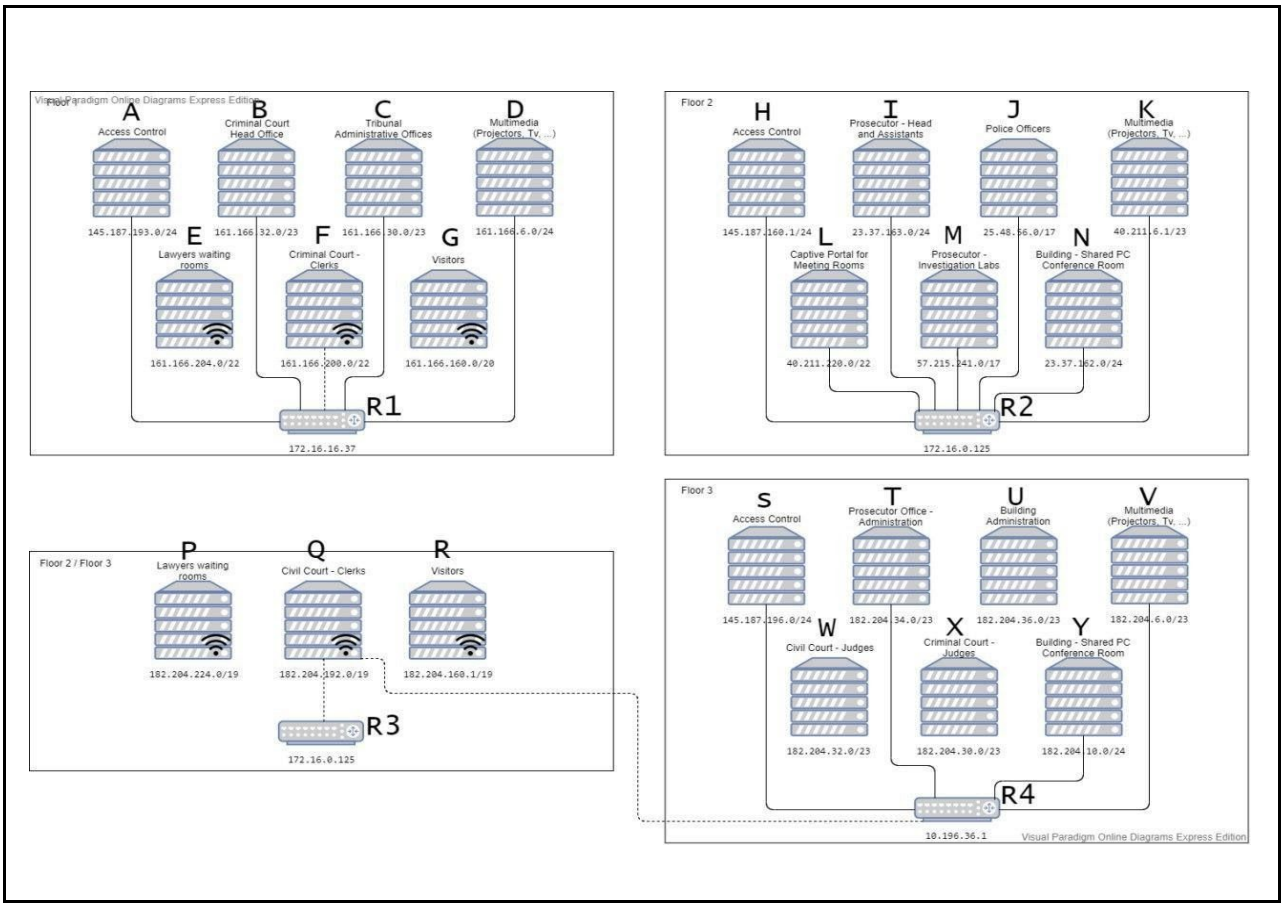

Figure 1 – Architectural Description of the Target of Evaluation

- We assumed that all the remotely operated computers will be running on Windows 10 with the same user privileges.
- Remote machines will use VPN software by using Juniper Junos Pulse to connect to their office computer.
- All the courts have their own way of working and their own schedules to manage their staff and budget.
- Each case is uniquely assigned to an individual clerk who will take care of its digital representation and updates.
- Clerks can help others clerks of the same court that means the digitals files can be transferred within the same court network.
- TightVNC and TeamSpeak softwares are used for remote management.
- In the given scan report, there were many vulnerabilities with different CVSS scores but for this report we have considered all the vulnerabilities which have CVSS more than or equal to 5.
- There were many different Systems/ Machines having the same CVE, so we considered them together as fixes/ controls are the same for all of them.

2. SUMMARY OF FINDINGS

The attack scenario includes all the threats which involve the disclosure of sensitive information about Clerk Courts, network architecture, controlled user privileges in remote scenarios and remote mode of communication. When these threats were assessed together in majority, they resulted in high and critical threats with high impacts on our primary assets. But when all the supporting assets of considered primary assets were assessed, it was found that these exploits have low impact on the proposed infrastructure.

For mitigation and to have a more secure infrastructure, we have proposed to have firewalls in the modified environment.

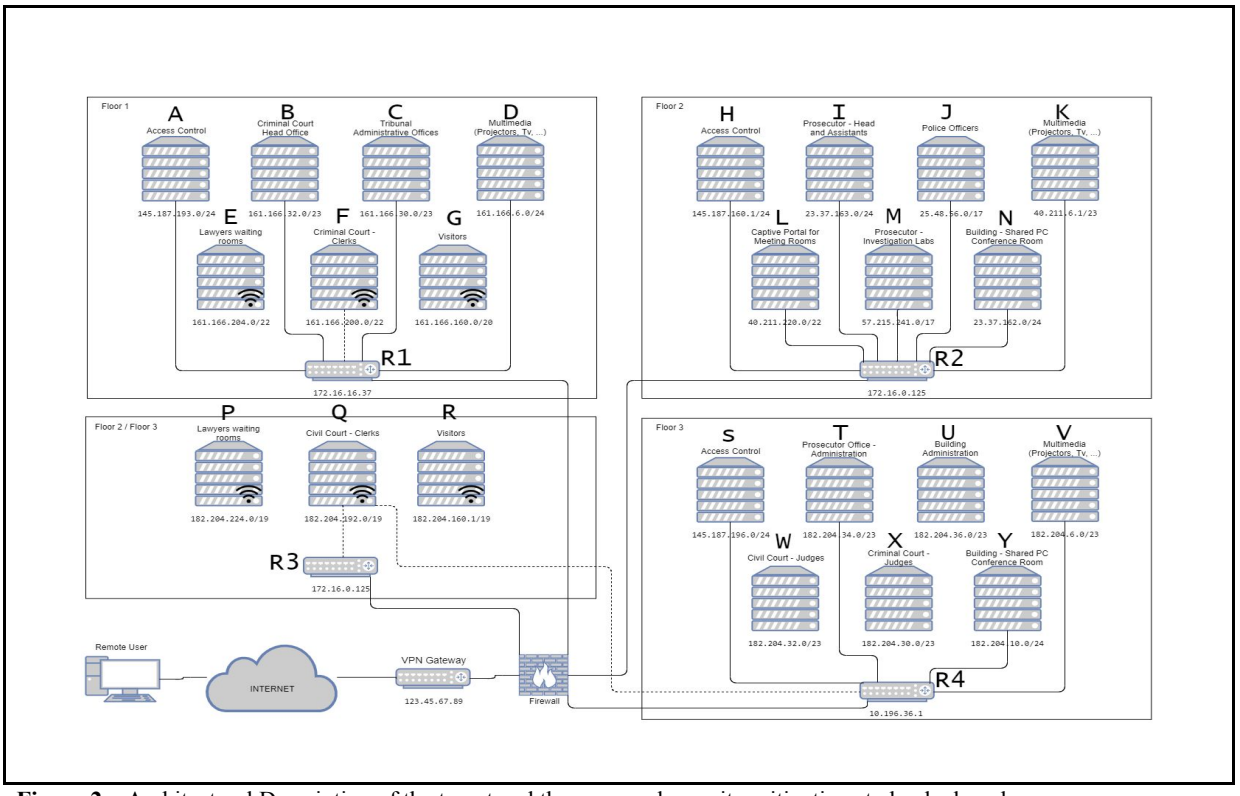

Figure 2 – Architectural Description of the target and the proposed security mitigations to be deployed.

Vulnerabilities: The Communication between different counterparts take place with the help of several protocols and one of them is MQTT. MQTT (MQ Telemetry Transport) is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks. An MQTT Broker is the glue that connects the devices that "publish" messages to the applications that "consume" them. There is a possibility of Man-in-the-middle attack where an attacker can read messages sent by other (genuine) devices, and inject its own false messages. At the same time, because of remote communication and remote operations, if server or protocol configurations are not done in an appropriate manner then it leaves a room for an attacker to intrude and steal the information and impact the integrity or can just perform DoS attack and impact the availability of the information or service.

And another vulnerability found was related to Escalated privileges and unauthorised access grant. For most of the assets it was found that if these two parameters are not taken care of, then they might result in high risk. For instance, If the TightVNC is not configured properly, it is very easy for an attacker to gain unauthorised access to all the sensitive information of the court cases.

And finally the most frequent vulnerability in almost all the supporting assets was related to their respective software updates given by vendors. If the softwares are not updated on time then any attacker can target the infrastructure resulting in many attacks like Denial of service attacks or man-in-the-middle attacks to affect the confidentiality, integrity and availability of services.

Mitigation: In order to counter the most frequent and high risk vulnerability present in different softwares and servers, we have proposed the updates and patches for all of the vulnerable assets which reduces the risk from high to low. For protocols like MQTT which results in leakage of data, we have proposed the correct configuration rules. For vulnerabilities like Brute force Logins and Anonymous logins, we have suggested to change the password frequently and give a strong password every time user changes it. The

number of login attempts should be fixed and an email update has to be sent to the user and head of the department whenever all login attempts are finished.

3. RISK ANALYSIS

3.1 Preliminary Qualitative Analysis

The complete summary of results can be found in the document **4_Kaushal_Spyrolari_Kucsvan_SecRAM-worksheet.xlsx** submitted as integral part of the current report.

At Step 1 we identified the primary assets and assessed their impact (see table **1.1** and **1.2** in the document **4_Kaushal_Spyrolari_Kucsvan_SecRAM-worksheet.xlsx**). The main primary assets that we identified are the ability for each Clerk to receive the assigned cases and their ability to communicate with the necessary counterparts which are the ones with the highest overall impact. More specifically, each Clerk is assigned a case, the details of which they receive in a document, through certified email with digital signature and they might need to notify or remind counterparts like judges and lawyers using a certified email with digital signatures. Losing the integrity and the availability of communicating with counterparts can highly affect the performance of the court, while the capacity of assigned cases will also be reduced if the integrity or availability of a Clerk's ability to receive cases is compromised.

At Step 2 we identified supporting assets for the list of primary assets from Step 1 (see table **1.3** in the document **4_Kaushal_Spyrolari_Kucsvan_SecRAM-worksheet.xlsx**). For the Clerk's ability to receive the assigned cases and their ability to communicate with the necessary counterparts, we identified the following main supporting assets: SMBv1 Server, Mailserver, SSL/TLS Certificate, a variety of protocols, Windows 10, JSON Web Signature (JWS), several web servers and Apache. For the latter, we also identified TeamSpeak. These supporting assets provide network communication protocol for providing shared access between systems, computer software which provides emails, cryptographic protocols for communication security, network protocol that transports messages between devices, standard for signing arbitrary data and a remote communication software between Clerks and their counterparts.

At Step 3 we identified threats to our supporting assets from Step 2 (see tables **2.1** and **2.2** in the document **4_Kaushal_Spyrolari_Kucsvan_SecRAM-exercise.xlsx**). The main threats for SMBv1 Server are elevated privileges and leakage of sensitive information because we assumed the existence of elevated command prompt vulnerability and its lack of support to encryption. The Mailserver is threatened by unauthorized access to sensitive data and Denial-of-Service Attacks, as personal computers can be left unattended and unencrypted email content may leak, while storage of more data than can be supported by the buffer may lead to overflow. The SSL/TLS Certificate is susceptible to session hijacking and cleartext leakage if "CSS Injection" vulnerability is in place and cryptographic protocols are not. Also, TLS, SSH, and IPSec protocols have a birthday bound if approximately four billion blocks allowing a "Sweet32" attack that provides access to sensitive information. Windows 10 is used by the computers used by Clerks to communicate with the courts' computers. End of Life of the OS will lead to the system not receiving any security updates from the vector. JSON Web Signature can allow access to arbitrary files though the existence of a .. (dot dot) in the HTTP GET request. Web Servers are threatened by SQL Injection and performance of dangerous HTTP methods such as PUT and DELETE given the allowance of execution of arbitrary SQL commands via the host name and misconfigurations of web servers. Apache is most threatened by the Web Server End of Life Detection through which the attacker can take control of the server via the non-updated security points. Lastly, TeamSpeak may provide access to attacker to sensitive data through the counterparts if the latter can be contacted via a logged in personal computer of a Clerk.

At Step 4 we evaluated the impact and risk level of the threats identified at Step 3 (see tables **3.1** and **3.2** in the document **4_Kaushal_Spyrolari_Kucsvan_SecRAM- worksheet.xlsx**). The predefined threats are of Medium or High risk severity. Hence, they need to be mitigated immediately. SMBv1 server threats have a combination of high impact and high likelihood which makes them of the highest priority as the affect the remote system, while TeamSpeak threats need to be mitigated as it interferes directly with the communication of the Clerks with their counterparts. Mailserver threats are a combination of the vulnerabilities caused by the physical presence of a direct link from the personal computers of the Clerks to the courts' computers, and lack of encryption on the content of the emails shared. The SSL/TLS Certificate and the various protocols implemented are closely connected to the safety of the system, making the mitigation of their threats highly necessary. Windows 10 is the basis for the remote model to work, so its uncompromised function is vital to the Clerks' ability to do their jobs remotely. Lastly, JSON Web Signature is vital for the authentication of the receive emails. Hence, any vulnerabilities modifying its functionality must be mitigated.

At Step 5 we proposed a set of security controls to mitigate major threats identified at Steps 3-4 (see table **4** in the document **4_Kaushal_Spyrolari_Kucsvan_SecRAM-worksheet.xlsx**). To mitigate the threats on SMBv1 Server, SSL/TLS Certificate, Windows 10, JSON Web Signature, SQL Injection on Web servers and Apache, upgrades of the pre mentioned assets are required. The vulnerabilities that make these threats possible have been recognized by the vendors, which have issued upgraded version or upgraded packets with these vulnerabilities patched. Hence, an upgrade would be enough as a pre-control and would automatically remove the need for post-controls, as the threats would be no longer viable.On the other hand, for mitigating unauthorized access to sensitive data on the Mailserver, we proposed to implement od encryption of email contents combined with log out of the email server after each session and verifications of digital signatures before access to email content. Denial-of-Service of Mailserver can be mitigated by strictly defining the allocated memory spaces and by implementing a back system for emergencies. TLS, SSH and IPSec protocols' threats can be patched by leading SSL/TLS configurations to choose AES over DES and, upon detection of the threat, discarding the contaminated data and updating them with new ones. Also, threat from performance of dangerous HTTP methods such as PUT and DELETE can be avoided with the use role-based access restrictions to these dangerous HTTP methods or by disabling them completely. This mitigation can be supported through the creation of temporary backup of the material to handle

changes caused by the PUT and DELETE methods. The secure communication though TeamSpeak can be achieved by prompting Clerks to log out of the system the moment they need to leave the computer unattended while at the same time a two-way authentication between the communicating entities should be implemented.

3.2 Quantitative Analysis

The complete summary of results can be found in the document **4_Kaushal_Spyrolari_Kucsvan_CVSS-worksheet.xlsx** submitted as integral part of the current report.

At Step 1, we identified the vulnerabilities present in the network before the risk analysis and have identified the key streams. They are summarized in **4_Kaushal_Spyrolari_Kucsvan_CVSS-worksheet.xlsx.** In particular, System B (Criminal Court Head Office) and System I (Prosecutor- Head and Assistants) are vulnerable to same threats of "httpoxy", "Linux Home folder accessibility" and "http TRACE XSS attack" which has a CVSS score of 5.1, 5 and 5.8 respectively.

System B and System U (Building Administration) share many similar vulnerabilities such as "Windows SMB Remote Code Execution Vulnerability", Memory and CPU consumption resulting in DoS attack" and " Windows SMB Information Disclosure Vulnerability" which has a CVSS score of 7.8 and 9.8 .

System C (Tribunal Administrative Offices) and System I (Prosecutor- Head and Assistants) have many common vulnerabilities related to Dropbear SSH which leaves a room for execution of arbitrary code which has a CVSS score of 10.

There are vulnerabilities which were found in many different systems and we categorized them together such as SSL/TLS certificate expired was found in System B, C, T and U and it has CVSS Score as 5. Windows Elevation of Privilege Vulnerability was found in System B, F and T with CVSS Score of 7.8. Obtaining cleartext data via birthday attack (Sweet32) was possible in System B, C, I, T and U and its CVSS Score is 5. Another vulnerability these systems share is "CCS Injection" which allows man-in-the-middle attack and it has CVSS score of 6.8.

While analyzing the vulnerabilities and possible attacks, we found that the System B is the one which has more vulnerabilities such as vulnerabilities related to PHP (Buffer Overflow, arbitrary code execution, remote code execution, Denial of Services, stack-based buffer overflow, Directory Traversal, security bypass, man-in the-middle etc) and has CVSS score varying from 5 to 10.

System C is mostly vulnerable because of ZOHO WebNMS framework which has threats of weak password which can be obtained in cleartext by attackers, directory traversal and bypass authentication and all of them have CVSS score of 7.5. Joomla has also affected the system C as it has XSS vulnerability because of inadequate filtering of content and it has CVSS score of 5.

System I has all the vulnerabilities related to OpenSSL such as discovery of RSA key, denial of service because of memory consumption, application crash, Out-bounds read, false positive packet drop, Integer overflow, race conditions etc with CVSS score of mostly 10 and 7.8.

System T (Prosecutor Office-Administration) has Directory traversal vulnerability, Boa server writes without sanitizing non-printable characters, SSH Brute force logins with default credentials, Default SSH Host key and Misconfigured Web Server have the CVSS score of 7.5, 5,5, 9, 5 and 7.5 respectively.

System U has vulnerabilities which perform incorrect free operations for multiple-value, Cross-site scripting vulnerability, error codes generated by UserDir directive and two of the vulnerability is related to network protocol (FTP and MQTT) with CVSS score of 10, 10,5, and 6.4 respectively.

At Step 2, we identified that most of the vulnerabilities require an update or upgrade by their respective vendors. These vulnerabilities have different CVSS scores (such as 7.8, 7.5, 5, 9 or 10). For vulnerabilities which don't have an update or vendor fix, we have proposed different mitigation based on the vulnerabilities.

For Linux home folder accessibility, we suggest to have restricted access or root privilege to access it. System Admin can disable the default pages within the server configuration to reduce the risk from missing 'httpOnly' cookie attribute and session hijacking (System B and C). Disabling HTTP TRACE requests and Dangerous HTTP methods (PUT and DELETE) will reduce the risk of cross-site tracing on systems B, I, U and will avoid the running of arbitrary code on the web server of system T, respectively. We have suggested some configuration changes by disabling few services like VRFY, EXPN on Mailserver (Systems C, I and U), ident service on IIS (System C), UserDir disable in Apache on Red Hat Linux system (System U) and at the same time configure WAF to overcome Microsoft IIS Tilde Character Information disclosure (System B), Close the TCP Port0 (System I), block access to hidden files (dot files) to restrict the permission to read the content of directories (System U)

Never disable AES based ciphersuites on server over DES/3DES as it might lead to sweet32 attack (Systems B, C, I, T and U) Another mitigation suggested by us is to generate new SSL/TLS certificates (System B, C, T and U) and new SSH host keys (System T). For systems B, C, F, I, N, T, U and Y add Firewalls or create VPN to protect the ZOHO WebNMS framework so as to avoid the

chances of upload and execution of arbitrary files (specifically for system C) and create a blacklist to deny the anonymous logins on FTP server to avoid data leaks (system U).

And the final suggestion from us was to encrypt the files (specially listed files) and restrict the access based on Roles and create a list based on which access will be granted. And Change the password to make it hard to guess, so as to reduce the risk for all brute force login attacks.

Based on above proposed mitigations, we have modified the exploitability and impacts of each vulnerability.

At step 3 we have calculated the overall impact and likelihood for a cyber attack.After the scan runs on the remote system, we decided to focus on the cyberattacks that can threaten our target. In order to measure the number of cyberattacks on court houses in Italy per year, we found that the number of cyberattacks in Italy during 2019 was 6.211 and 40.8% of those cases are aimed at Government bodies. The Italian Government is made from 3 branches, one of which is the Judicial Branch. Hence, every year 845 cyber attacks take place in Italian court houses every year in total. Depending on the type of attack, the number varies as represented in the assumptions table included with the data reported in Table 3 for the key assets. Attacks caused by hacking, malware or social engineering and they include XSS, SQL Injection and Denial-of-Service attacks, malware, ransomware, phishing and leaks of sensitive information. Hence their impact can be € 20.000, € 50.000 or € 200.000 depending on the affected assets. Taking into account the number of attacks, incidents and breaches we found that the likelihood of these vulnerabilities can range from 1% to 50% to over 350% making the risk of the attack vary from € 440, which is significantly lower than the expected impact to € 796.320, which is significantly over the expected impact. Full details are available in **4_Kaushal_Spyrolari_Kucsvan_CVSS-worksheet.xlsx**.

At step 4 we identified the total costs of our proposed countermeasures (for NNN Euro in total) as well as the residual likelihood and therefore the residual risk after we have applied the countermeasure. The countermeasures suggested for the threats listed fall in three major categories: vendor fixes through updates, internal changes, like modifications of configurations, and firewalls. The vulnerabilities have been recognized by the vendors and they have generated updated versions with these vulnerabilities patched. Hence, the upgrade completely removes the vulnerabilities leading to no impact associated with them. If there are no vulnerabilities, attackers have no way to make an attack and without an attack there is no impact on the system. The cost of this type of mitigation is based on the payment of the employee responsible for keeping up with the updates for the system's software and the cost of the upgrade. As the upgrades needed for the vulnerabilities located are free of charge, the cost is limited to the system administrator's salary for a half to one month per year depending on the vulnerability. The same cost related approach is taken for the internal changes, making the cost affected only by the cost of the employees' salary, which is calculated to € 1.102,13 per month and the time the mitigation will require. For the implementation of the firewalls we need to consider the cost of the firewall as well, which comes up to € 1.333,3. The outcome of these measures leads to significantly lower risk. Specifically, for the updated parts of the system the risk is only viable for the initial period of delay until the mitigations are implemented, a is set to € 0 after that. As an outcome of that, the likelihood is viable only for that period as well, extremely reducing it. Hence, the benefits of fixing the vulnerabilities reaches a total of about € 80 million in total compared to the cost which is € 500.000 for three years.

The detailed costs and benefits for each threat and mitigation can be found in detail at Table 3 in **4_Kaushal_Spyrolari_Kucsvan_CVSS-worksheet.xlsx** while details about the calculations of the numbers and amounts used in the report can be found in the references.

ANNEX

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

1. Excel document reporting the application of SESAR SecRAM method (see file **4_Kaushal_Spyrolari_Kucsvan_SecRAM-worksheet.xlsx**).
2. Excel document reporting the application of CVSS Quantitative method (see file **4_Kaushal_Spyrolari_Kucsvan_CVSS-worksheet.xlsx**).

REFERENCES

[1]

'2019-data-breach-investigations-report.pdf'. Accessed: Jun. 29, 2020. [Online]. Available: https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf.

[2]

'2019-dbir-executive-brief.pdf'. Accessed: Jun. 28, 2020. [Online]. Available: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf.

[3]

'Apache :: How to update/upgrade Apache 2.4 to newer version'. https://www.apachelounge.com/viewtopic.php?t=5768 (accessed Jun. 28, 2020).

[4]

‘Changing your PHP version’. https://help.fasthosts.co.uk/app/answers/detail/a_id/1962/~/changing-your-php-version (accessed Jun. 28, 2020).

[5]

‘Choosing a Firewall’, *TechGenix*, Feb. 23, 2004. http://techgenix.com/choosing_a_firewall/ (accessed Jun. 29, 2020).

[6]

‘Cyber Security Specialist Salary in Italy’. https://www.erieri.com/salary/job/cyber-security-specialist/italy (accessed Jun. 29, 2020).

[7]

‘How long does it take to upgrade to the Windows 10 Fall Creators Update version 1709?’ https://answers.microsoft.com/en-us/windows/forum/windows_10-update/how-long-does-it-take-to-upgrade-to-the-windows-10/4c158f39-240c-4fe6-b530-52ac7f4be0b2 (accessed Jun. 28, 2020).

[8]

K. Robinson, ‘How Much Does a VPN Solution Cost? | AVOXI Cloud Communications’, *https://www.avoxi.com/*, Jun. 28, 2017. https://www.avoxi.com/blog/vpn-solution-cost/ (accessed Jun. 29, 2020).

[9]

‘Italy: cyber attacks number by method 2019’, *Statista*. https://www.statista.com/statistics/649297/cyberattacks-distribution-share-by-method-in-italy-timeline/ (accessed Jun. 28, 2020).

[10]

‘Le tendenze dei cyber attacchi in Italia: gli ultimi dati a confronto’, *Agenda Digitale*, Mar. 21, 2019. https://www.agendadigitale.eu/sicurezza/le-tendenze-dei-cyber-attacchi-in-italia-gli-ultimi-dati-a-confronto/ (accessed Jun. 28, 2020).

[11]

‘Public Administration | Interactive Verizon Data Breach Investigations Report’. http://verizon.datawheel.us/industry/public (accessed Jun. 29, 2020).

[12]

‘Systems Administrator Salary in Italy | PayScale’. https://www.payscale.com/research/IT/Job=Systems_Administrator/Salary (accessed Jun. 28, 2020).