On the Cyber Security of Lebanon: A Large Scale Empirical Study of Critical Vulnerabilities

Yasser Fadlallah
Computer Science department
University of Sciences and Arts in Lebanon
y.fadlallah@usal.edu.lb

Mohamad Sbeiti
Cyber Defense and Internal Security
Deutsche Telekom AG, Germany
mohamad.sbeiti@tu-dortmund.de

Mohamad Hammoud
Computer Science department
University of Sciences and Arts in Lebanon
mwh018@usal.edu.lb

Mohamad Nehme
Cybersecurity Empowering Research Team (CERT)
Beirut, Lebanon
mohamad.nehme@gatewall.net

Ahmad Fadlallah
Computer Science department
University of Sciences and Arts in Lebanon
a.fadlallah@usal.edu.lb

***Abstract*—In this paper, we uncover 1645 critical vulnerabilities in the perimeter of Lebanon affecting the majority of its sectors, including critical infrastructure. Given the enormous economic and personal damage imposed by critical vulnerabilities, we use a novel framework to regularly identify these vulnerabilities in time on a large scale. We show that the root cause of the uncovered vulnerabilities is the lack of a core security best practice, namely, patch management. All the 1645 vulnerable systems had a patch offered by the vendor at the time they were found vulnerable. In addition to that, the poor reaction to our notification efforts to the owners of vulnerable systems underlines another lack of a proper incident handling process. To this end, this research shall be considered as a first step towards continuous attack surface evaluation of Lebanon, which shall involve different parties from public and private sectors in order to better perform risk analysis and mitigation.**

I. Introduction

It is beyond dispute that security is a core need for digitization, Industry 4.0 and Internet of Things (IoT), and with 5G – the digital life – the attack surface is to become larger due to the new dimensions of connected entities. According to [1], there have been 16 billion IoT connected devices in 2016 while 29 billion devices are forecast by 2022. Meanwhile, the number of successful large-scale cyber attacks is rising, e.g., Emotet and WannaCry, and the asymmetry in the cyberwarfare is increasing. Here, skilled hacker ability increases to harm enterprises, organisations and even states despite more investments in the defense line [2]. Thereby, fundamental questions the driver of digitization and 5G needs to answer are:

1) How adopters of digitization and 5G could be well equipped against security threats?
2) Does it pay off to implement the corresponding measures, i.e., how much more security does this offer?

Unfortunately, currently recommended security best practices have often shown to fail in practice [3]. These can be categorised in proactive and reactive measures.

- Proactive: This is a front-line defense to prevent/mitigate attacks. Measures applied are such as security awareness, security-by-design processes, patch management processes, threat intelligence, penetration testing, and other tools e.g. firewalls and intrusion prevention systems.
- Reactive: This is an additional defense line whenever front-line defenses fail. Measures applied are such as attacks/anomalies detection and reaction systems, security auditing, digital forensics and incident response.

While the aforementioned points are self-explanatory and are deemed to offer high level of security, the research in [3] showed that despite those best practices, critical long-aged vulnerabilities were still available across industries. This could be rooted in several issues. For instance, an internet-facing application could have a dynamic nature (features are often added) resulting in some changes not being (pen)tested due to the lack of resources and due to other priorities. Other example is the patch management being interval-based with relaxed intervals, as such vulnerabilities remain open without further countermeasures until the next patch interval. Yet another example is the lack of real-time detection of attacks in a segment of the IT infrastructure due to improper configuration/integration of relevant data sources in that segment – mostly because of the lack of detailed overview of the IT infrastructure. In general, one could say that as long as there is no practical process to regularly measure the overall effectiveness of the implemented security best practices, the two questions raised at the beginning cannot be answered.

As a result, organizations like the North Atlantic Treaty Organization (NATO) [4] and many top fortune companies like Facebook [5] and Google [6] have adopted couple of years ago an approach termed red teaming. According to NATO's definition, red teaming is an element that conducts vulnerability assessments, a) in a live environment, b) with an adversarial point of view, c) on the whole target scope, and d) without advising security staff. That is, the added value of red team activities can be found in:

- Assessment of the overall effectiveness of the implemented proactive and reactive security measures in the live environment.

978-1-7281-6939-2/20/$31.00 ©2020 IEEE

- Demonstration of the impact of cyber-attacks and removing uncertainty for decision makers.
- Improving the ability of cyber security staff and users as well as identifying gaps.

Thereby, red teaming would lead to a confident answer for the two questions raised at the beginning of this section. As such, red teaming is not yet another security process, it is rather a core pillar of the concept of security.

Here, a core challenge that is still to be addressed in order to be able to efficiently and regularly perform red teaming, is to automate the information gathering phase. This is the very first phase of red teaming and it deals with identifying and getting a detailed overview of the target, especially, that of the IT infrastructure (i.e., finding all corresponding IP addresses and domains, and gathering all relevant information about the services, products, applications, websites and vulnerabilities). To the best of the authors' knowledge, there is no commercial off-the-shelf tool or an open source framework that addresses this issue yet. Thereby, in this paper, we are going to introduce a project initiated in a collaboration between the USAL university and several researchers under the umbrella of a Lebanese Cybersecurity Empowering Research Team (CERT) NGO to tackle this challenge. The main idea is to continuously evaluate the attack surface of the Lebanese perimeter in order to a) capture critical vulnerabilities in the Lebanese perimeter and report these in time, and to b) pave the way for government-supported red teaming activities in Lebanon.

The rest of this paper is organized as follows: Section II presents the novel information gathering framework used, hereafter named the CERT framework. Section III provides an in-depth look at the vulnerabilities that were identified using the CERT framework in the Lebanese perimeter. An attack surface evaluation is performed in Section IV. Here a classification of vulnerable systems per sector is performed, information about the security budgets in Lebanon is presented for a better analysis, our notification process is elaborated and the impact of this notification is discussed. Finally, section V concludes the paper and states our next step in order to improve the current situation.

II. The CERT Information Gathering Framework

The CERT information gathering framework is a novel combination of systems for identifying and evaluating the attack surface of Lebanon in real time. It automatically retrieves a comprehensive inventory of the IT infrastructure of Lebanon. Based on an innovative approach, the framework easily interconnects different systems to efficiently collect all in-scope information. Moreover, its in-time semi-passive vulnerability analysis of Lebanon's IT infrastructure makes the CERT information gathering framework an attractive solution for risk management of Lebanon and of contractual partners, e.g., of companies operating in Lebanon. The framework is composed of three core blocks:

- **Passive IT Infrastructure Inventory**: Based on a target name as input (e.g., .lb / Lebanon), the framework crawls whois databases [8] to collect IP addresses belonging to Lebanon's Internet service providers. It uses passive domain inventory tools such as RedAsset [9]–[11] and massdns [12] for an automated inventory of sub-domains of Lebanon's IT infrastructure and their IPs. To feed RedAsset with the (main) domains, in addition to gov.lb, com.lb, net.lb, edu.lb and org.lb, the main domains were gathered from the Lebanese yellow pages [13]. Apart from IPs and domains, the CERT framework passively gathers a list of common open ports in the target perimeter by consulting Internet scanning engine like Shodan [14], Censys [15], Zoomeye [16] and Fofa pro [17].
- **Semi-Passive Vulnerability Analysis**: The framework connects different semi-passive vulnerability analysis and other OSINT tools in a fully compatible way so that they can interact harmoniously. This bundles the strengths of the different systems and saves manual work. Here, Shodan, Zmap, Zgrab, Webanalyze, CVE-Search [14], [18]–[20] as well as Proof-of-Concepts (PoCs) of critical vulnerabilities [21] are combined to efficiently identify and verify critical vulnerabilities in time.
- **Security Dashboard**: The framework fosters a simple and self-explanatory security dashboard, which includes both statistics and managerial charts dedicated for decision makers as well as detailed technical view for security experts. The security dashboard is implemented using Kibana for aggregations and visualizations and using Elasticsearch as a result database [22].

III. Selected Vulnerabilities for Experimental Study

To investigate the added value of the CERT info gathering framework, an experimental study to assess the attack surface of Lebanon's perimeter was performed. Relevant information about $612,608$ IP address and $24,382$ domains were gathered in May 2019 as a first step. Afterwards, critical unauthenticated remote vulnerabilities (see Table I) were selected based on which the security posture of Lebanon's IT infrastructure was explored. These vulnerabilities were selected for the following reasons:

- The severity of the vulnerability (its Common Vulnerability Scoring System (CVSS) score [7]) and the fact that it is remotely exploitable. All the selected vulnerabilities have a CVSS v3.0 score corresponding to high or critical.
- The availability of a corresponding exploit or Proof-of-Concept (PoC) online. This fact allows any malicious user with basic knowledge in networking and security to exploit the affected systems.
- The high number of potentially affected systems or the criticality of these (e.g., governmental or financial), which is delivered by the statistics of the CERT framework.
- The timeliness of the vulnerability.

The study was performed from May 2019 until the end of December 2019. The goal is twofold: first, to evaluate the attack surface of the Lebanese perimeter, and second to assess whether the CERT framework fulfills its red team goal in

TABLE I: Selected Critical Vulnerabilities

Vulnerable Product	Vulnerability Number	Vulnerability Disclosure Date	Vulnerability Advisory	Vulnerability Description
Citrix Application Delivery Controller (ADC) Gateway	CVE-2019-19781	27/12/2019	[23]	**Unauthenticated Remote Code Execution (RCE)**: This is an RCE application vulnerability affecting Citrix ADC Gateway versions: 10.5, 11.1, 12.0, 12.1, 13.0, among others. By exploiting this vulnerability, a remote unauthenticated attacker is able to perform arbitrary code execution, which could lead to a full compromise of the system.
Microsoft SharePoint	CVE-2019-0604	02/12/2019	[24]	**Unauthenticated RCE**: This vulnerability is an RCE that exists when the Microsoft SharePoint software fails to check the source markup of an application package. A remote attacker who successfully exploits the vulnerability can run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability does not require credentials, as such it is an unauthenticated RCE. Example of affected versions are SharePoint server 2019 and SharePoint enterprise server 2016.
MikroTik Router Operating System (OS)	CVE-2019-3978	29/10/2019	[25]	**DNS cache poisoning**: Any MikroTik router with an OS of versions 6.45.6 and below is vulnerable to unauthenticated remote DNS cache poisoning, which could lead to an unauthenticated RCE.
Windows Remote Desktop Service (RDP)	CVE-2019-0708	16/05/2019	[26]	**Unauthenticated RCE, known as Bluekeep**: This is an RCE vulnerability that takes advantage of the windows RDP service before authentication happens where an attacker sends specially crafted requests, and leads to a full compromise of the system. Example affected versions are Windows Server 2008 R2, and Windows Server 2008, and Windows Server 2003.
Pulse Connect Secure SSL VPN	CVE-2019-11510	08/05/2019	[27]	**Arbitrary file reading**: Multiple vulnerabilities were identified in Pulse Connect Secure SSL VPN in April 2019 among which ”unauthenticated arbitrary file reading”, which allows an attacker to read any file on the file System of the VPN including the file */data/runtime/mtmp/lmdb/data/data.mdb* that contains cached plaintext credentials of recent login, and the file */data/runtime/mtmp/system* that stores VPN users and admin, and associated hashed password. Example affected versions are Pulse Connect Secure 8.2 before 8.2 R12.1 and 9.0 before 9.0 R3.4.
Oracle Weblogic Server	CVE-2019-2725	26/04/2019	[28]	**Unauthenticated RCE:** This is a java deserialization vulnerability in the oracle weblogic server. It allows unauthenticated attacker to compromise the server via a crafted HTTP request (example endpoint */_async/AsyncResponseService*). Successful attacks of this vulnerability can result in takeover of the server. Example affected versions are 10.3.6 and 12.1.3.
Atlassian Confluence	CVE-2019-3396	25/03/2019	[29]	**Unauthenticated RCE:**: This vulnerability concerns the widget connector macro in Atlassian confluence Server before version 6.6.12, from version 6.7.0 before 6.12.3, from version 6.13.0 before 6.13.3, and from version 6.14.0 before 6.14.2. It allows remote attackers to achieve path traversal and RCE on a confluence server via server-side template injection.
MikroTik Winbox	CVE-2018-14847	02/08/2018	[30]	**Arbitrary file reading**: This vulnerability allows an unauthenticated attacker to connect to the Winbox port and request the system user database file in MikroTik RouterOS through 6.42. That is, the attacker can gain control of the username and password strings, and then use these credentials to gain access to the underlying system, which could lead to a full compromise.
Fortinet FortiOS SSL VPN Web Portal	CVE-2018-13379	06/07/2018	[31]	**Arbitrary file reading**: The implementation of the FortiOS SSL VPN web portal is affected by several vulnerabilities, among others, path traversal. By exploiting the latter, an attacker will be able to read contents of the *sslvp_websession*, a session file that contains a username and a plain-text password on a vulnerable system, and to reset passwords without authentication, which would lead to a full compromise of the system. Example of affected versions are FortiOS 6.0.0 to 6.0.4.
Liferay Portal	TRA-2017-01	09/01/2017	[32]	**Unauthenticated RCE:** This is a java de-serialization vulnerability in the TunnelServlet and other components of the Liferay portal. It is remotely exploitable via a crafted HTTP request (example endpoint */api/liferay*), leading to arbitrary code execution. Example affected versions are Liferay Portal EE 6.0 and Liferay Digital Enterprise 7.0.

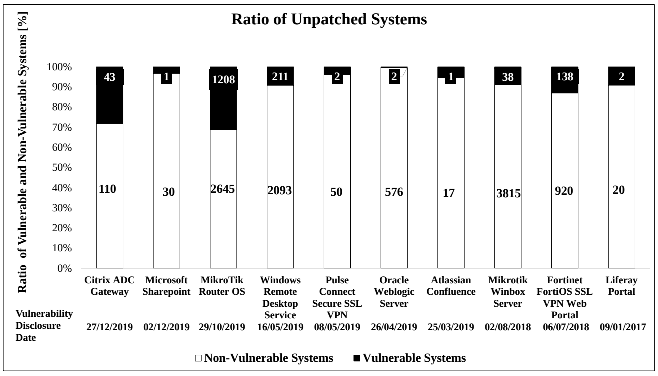

Fig. 1: Ratio of Vulnerable Systems in the Perimeter of Lebanon

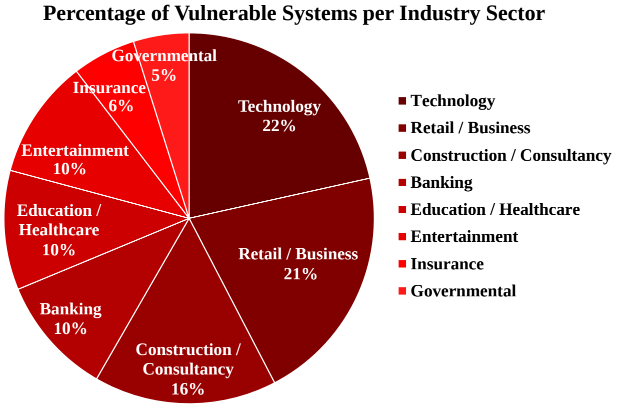

Fig. 2: Classification of Vulnerable Systems per Sector

terms of automatically gathering info about a large scope and efficiently identifying attack entry points.

IV. Attack Surface Evaluation

In order to gather information about the Lebanese perimeter with respect to the vulnerabilities depicted in Table I, a special focus was put on systems with the corresponding ports open, such as 7001 for oracle Weblogic, 8291 for Winbox and 443, 8443 or 9443 for the FortiOS and pulse secure connect VPN SSL vulnerabilities. This resulted in $44,501$ systems from the aforementioned $612,608$ systems in the Lebanese perimeter. From those systems, the per-vulnerability potentially affected systems were chosen and a proof-of-concept check was run on these to identify whether they are vulnerable or not. Once the vulnerable systems identified, the affected targets were notified per e-mail. The results are elaborated in the following.

A. Ratio of Critical Vulnerabilities in the Lebanese Sectors

The ratio of systems in the perimeter of Lebanon, that were exposed to critical vulnerabilities is depicted in Figure 1. The Figure shows that the number of vulnerable systems is significant with respect to the number of systems running the corresponding product or service, as described in Table I. For example, 1208 out of 3853 MikroTik routers are affected by the DNS cache poisoning vulnerability, i.e. almost 32%. This means that 1208 routers can be fully compromised and upgraded with a new firmware by the attacker. That is, the attacker can redirect all the traffic to himself as well as he can attack the internal network. Another result is the Bluekeep vulnerability found in the RDP protocol. It can be seen that 211 systems out of 2304 are exposed and can be easily compromised, especially, that several exploits have been published online. It is also worth noting that although some vulnerabilities are limited to a few number of organizations, however, these could cause a serious damage on the economy of the whole country, e.g., the Citrix ADC vulnerability. At the time the vulnerability was announced, it was found that sensitive systems in banking, insurance, healthcare, and business sectors (i.e., critical infrastructure) were affected. Looking at the Figure 2, we have classified the vulnerable systems above into 8 different sectors, using a sample of almost 150 systems[1]. One can observe that systems belonging to both sectors, **Technology** and **Retail and Business**, constitute around 43%. Other sectors such as **Construction and Consultancy** occupies around 16%, the **Entertainment** and the **Education-Health** sectors have a ratio of 10%, the **Governmental** sector is about 5%, and the **Insurance** sector lies by 6%. Yet, specially noteworthy is that the **Banking** sector has a ratio of 10% with 15 vulnerable systems. Given the criticality of this sector, this fact raises the question on the implemented security measures, especially with respect to their patch management processes and tools. Motivated by these initial results, and due the high ratio of short-aged and long-aged critical vulnerabilities in the Lebanese perimeter[2], we performed the following actions and analysis in an attempt to understand the root causes of this poor vulnerability handling.

B. Attack Surface Analysis: Review of Security Budgets

As security budget is key for patch management, which should lead to a low ratio of critical vulnerabilities, we interviewed private information security firms operating in Lebanon about the budget ratios of the various Lebanese sectors, which they have consulted over the last six years. Figure 3 illustrates the spending of these sectors on information security services[3]. Starting from 2017, the starting age of the vulnerabilities analyzed in this research, Figure 3 shows that the banking sector has decreased its budget to less than 40%. This could explain the relatively high vulnerability ratio of 10% in the Lebanese financial system over the last three years, as illustrated in Figure 2. Figure 3 also shows that the investment of the technology sector has increased starting in 2017 and then decreased, which could explain the result of a notably high

[1] The reason for which a sample of 150 systems is selected, is that not enough credible information is found for sector categorization for most of the remaining affected systems.

[2] See the ratio of FortiOS (08/2018, long-aged), Bluekeep (05/2019, medium-aged) and Citrix (12/2019, short-aged).

[3] Information security services includes information security consulting, information security assessment, information security training as well as forensic services. Budget spent on information security products and solution providers are excluded.

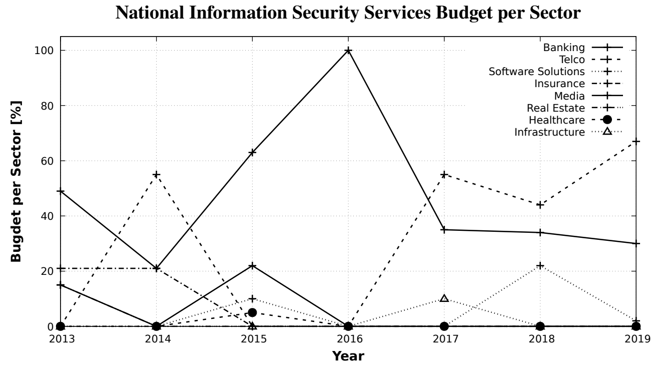

Fig. 3: Security Budgets of Lebanese Sectors between Year 2013 and 2019

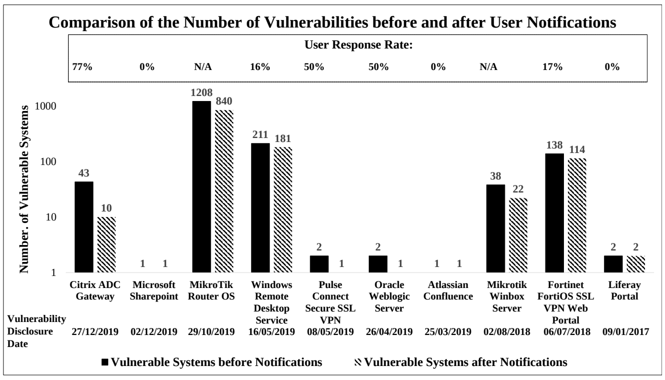

Fig. 4: Classification of Vulnerable Systems per Sector

vulnerability ratio of 22% in Figure 2. On the other hand, the investment of the telecommunication sector has increased starting from 2017 yielding in no detected vulnerability in this sector. Last but not least, Figure 3 reflects the poor (or no) security investment of the other sectors apart from the public and governmental sectors. The latter could not be captured in our interviews due to the lack of any contractual situations with the interviewed firms. These have expressed their struggles to offer their services and knowledge to the public sector. These facts criss-crosses with the high vulnerability ratios of all sectors in general in Lebanon.

C. Attack Surface Analysis: E-Mail Notification Handling

With the results obtained above, and in order to minimize the risk to be compromised on the exposed systems, it was indispensable to contact systems administrators so that they take the necessary actions to avoid any consequent damage. Here we mention that thanks to the CERT platform, in addition to the IP address of each system, the domain name is provided when available. These domains names were keys to help finding the contact email to inform the responsible/administrators about the vulnerabilities and the advisory to do the necessary patch. Therefore, we developed a smart script that looks for the targeted email at different stage. This script scans search engines, the domain's website, and the whois database for any email that can be found for the targeted systems. Once the emails found, we designed a well structured email with the goal to notify the users about their information system exposure. The email describes the CVE, the damage it could cause, and an advisory with a reference where the necessary patches can be found. Figure 4 illustrates how poor was the notification handling by the affected systems administrators/responsible. The results **before notification** are similar to those shown in Figure 1. Figure 4 shows that among the 211 users that have been notified, only 30 users have patched their systems against the Bluekeep CVE, and similarly, 22 systems in use of the Fortigate SSL VPN are patched after being notified. Systems based on Liferay and Confluence frameworks have shown no reaction to our notifications, whereas most of the systems (33 out of 43) that use the Citrix software have done the necessary patch within one week of the first scan. On the other hand, regardless of whether the patches were applied due to our emails or not, it is important to mention that we received no reply to our emails, which leads us to conclude that the notification handling was going to happen as expected, although some exposed systems to relatively old vulnerabilities that date more than one year, e.g. Fortigate SSL VPN, have done the patch just after our notifications.

Next, Figure 5 illustrates the per-sector closed vulnerabilities. Interestingly, it can observed that all banking sectors have closed their vulnerabilities that were in the Citrix ADC. As mentioned previously, the second scan was performed one week after the first scan. This means that the banking sector, which is most critical, can be seriously damaged during the few days until the patches are performed. All other sectors have poorly reacted and some did not react at all, such as the Retail-Business, despite our notifications.

On the other side, system administrators for 2 types of vulnerable systems that are: the MikroTik DNS cache poisoning and the MikroTik Winbox Server, could not be reached due to the difficulties in finding their contacts, especially, that such systems are not necessarily application systems but rather routers for probably private owners. This means that the damage extends to the private networks. That is, without being aware of such vulnerabilities, the risk that private networks can be exploited will be increasing, and this points out to the importance of spreading awareness among all the community in use of computing systems.

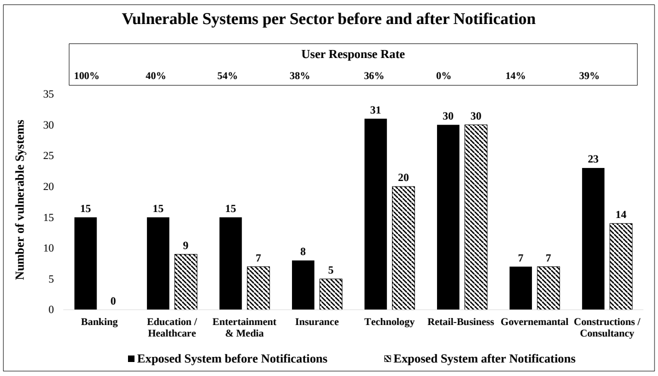

Fig. 5: Overview of Sector Reaction to E-Mail Notification

D. Attack Surface Analysis: Feedback of Affected Targets

Despite our attempt to notify all affected targets, either by sending them an e-mail directly when possible, or by informing their Internet Service Provider (ISP) when not possible, as well as by informing the Lebanese national Internal Security Forces (ISF) in both cases, we have not got any reply to our notification. Thereby, we contacted systems administrators and ISP to understand the reasons and asked them about the reasons of the presence of critical vulnerabilities in their targets and they can be summarized as follows:

- Reasons for the presence of critical vulnerabilities: Missing maintenance or update procedures, missing hardening guidelines and processes, missing security monitoring measures, missing security awareness, and missing security budgetary plans.
- Reasons for the poor reaction to notification: Lack of expertise to understand the email, lack of trust in the email notification process, and/or the email not received.

V. Conclusion

In a nutshell, this paper aims to shed the light on the security issues facing the information systems deployed in public and private Lebanese companies, associations, and institutions. We used a new platform that interconnects different data sources (mainly OSINT) to gather all in-scope information for an adequate security risk analysis and management. Many vulnerable systems were identified belonging to the different sectors including critical ones such as **Banking**. The conducted work and the obtained results revealed the lack of applying two core best practices in information security which are **patch management** and **incident handling**. Another crucial issue highlighted in this paper was that only few sectors have allocated decent budgets for security services. Given these facts, we perceive that a next step to enhance the cyber security level in Lebanon is to use this work as a foundation to involve international cyber security firms, lebanese ISPs, system administrators, research teams, and delegated staff from the public sector in the evaluation and remediation of Lebanon's attack surface, thereby, paving the way for government-supported red teaming activities in the future.

VI. Acknowledgment

This work would not have been possible without the experience gained at Deutsche Telekom, which is the leading European telco and with its T-Systems unit Telekom Security being the leading cyber security provider in Germany. As such, the reader is recommended to consult Deutsche Telekom / Telekom Security for professional security services at https://www.t-systems.com/de/en/security.

References

[1] Ericsson Mobility Report (2019, June). 5G uptake even faster than expected. Retrieved from https://www.ericsson.com/en/press-releases/2019/6/ericsson-mobility-report-5g-uptake-even-faster-than-expected

[2] Garrett M. Graff (2017, April). Chasing the Phantom: Inside the Hunt for Russia's Most Notorious Hacker. Retrieved from https://www.wired.com/2017/03/russian-hacker-spy-botnet/

[3] White Hat Security (2016). Web Applicayion Security Statistics Report. Retrieved from https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report-FINAL.pdf

[4] Dandurand, Luc. (2011). Rationale and blueprint for a cyber Red Team Within NATO: An essential component of the alliance's cyber forces.

[5] Facebook (2017, Feb 17). A Look at Facebook Security. Retrieved from https://www.facebook.com/careers/life/a-look-at-facebook-security

[6] Google Careers (last visited March 2020). Security Engineer, Information Security Assurance/Red Team. Retrieved from https://careers.google.com/jobs/results/111476636454396614-security-engineer-offensive-security/

[7] FIRST, Common Vulnerability Scoring System SIG. Retrieved from https://www.first.org/cvss/

[8] RIPE, Reseaux IP Europeens. Retrieved from https://ftp.ripe.net/pub/stats/ripencc/membership/alloclist.txt

[9] Redasset Tool (2019 April 26). Retrieved from https://github.com/rverton/redAsset

[10] Internet-Wide Scan Data Repository. Retrieved from https://scans.io/

[11] Certificate Transparency. Retrieved from http://www.certificate-transparency.org/known-logs

[12] MassDNS 0.3 (2020, March 31). A high-performance DNS stub resolver for bulk lookups and reconnaissance. Retrieved from https://github.com/blechschmidt/massdns

[13] Yellow Pages Lebanon. Retrieved from https://www.yellowpages.com.lb

[14] Shodan Search Engine. Retrieved from https://www.shodan.io/

[15] Censys Search Engine. Retrieved from https://censys.io/

[16] ZoomEye Search Engine. Retrieved from https://www.zoomeye.org/

[17] Fofa Search Engine. Retrieved from https://fofa.so/

[18] The ZMap Project. Retrieved from https://zmap.io/

[19] Webanalyze (2020 March 3). Port of Wappalyzer (uncovers technologies used on websites) in Go to automate scanning. Retrieved from Webanalyze. https://github.com/rverton/webanalyze

[20] CVE-Search (2020 March 17). Cve-search - a tool to perform local searches for known vulnerabilities. Retrieved from https://github.com/cve-search/cve-search

[21] PoC in GitHub (2020 April 03). PoC auto collect from GitHub. Retrieved from https://github.com/nomi-sec/PoC-in-GitHub

[22] Elastic. Open Source Search: The developer of Elastic Search. Retrieved from https://www.elastic.co

[23] Citrix (2020, Jan 24). CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway. Retrieved from https://support.citrix.com/article/CTX267027

[24] Microsoft (2019 April 25). CVE-2019-0604 Microsoft SharePoint Remote Code Execution Vulnerability. Retrieved from https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604

[25] MikroTik (2019 Oct 28). DNS Cache Poisoning Vulnerability. Retrieved from https://blog.mikrotik.com/security/dns-cache-poisoning-vulnerability.html

[26] Microsoft (2019 May 14). CVE-2019-0708 — Remote Desktop Services Remote Code Execution Vulnerability. Retrieved from https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

[27] Pulse Secure (2020 Jan 13). Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX. Retrieved from https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

[28] National Vulnerability Database (2018 July 18). CVE-2015-0204 Detail. Retrieved from https://www.oracle.com/security-alerts/alert-cve-2019-2725.html

[29] National Vulnerability Database (2019 April 22). CVE-2019-3396 Detail. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2019-3396

[30] MikroTik (2018 Mar 25). CVE-2018-14847 Winbox Vulnerability. Retrieved from https://blog.mikrotik.com/security/winbox-vulnerability.html

[31] FortiGuard Labs (2019 May 24). FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests. Retrieved from https://fortiguard.com/psirt/FG-IR-18-384

[32] Tenable (2017 Sept 01). [R1] Liferay CE Portal /api/liferay Java Deserialization Blacklist Bypass Remote Code Execution. Retrieved from https://fortiguard.com/psirt/FG-IR-18-384