International Journal of Computer Applications (0975 - 8887)
Volume 183 - No.17, July 2021

A Methodology for Network Security Infrastructure according to the New Brazilian General Law for Personal Data Protection

Luis Fellipe Castro Silva
Federal University of Maranhao (UFMA)
Computer Science Postgraduate Program
Av. dos Portugueses, 1966 Bacanga – CEP 65080-805
São Luis – MA – Brazil

Samyr B. Vale
Federal University of Maranhao (UFMA)
Computer Science Postgraduate Program
Av. dos Portugueses, 1966 Bacanga – CEP 65080-805
São Luis – MA – Brazil

ABSTRACT

The General Law on Protection of Personal Data - LGPD (Law No. 13,709/2018) is a new Brazilian law that deals with the management of personal data of third parties, carried out by people, companies, and institutions. This legal provision requires that these data be protected by all necessary technical means, imposing a set of sanctions on the Organization. Due to the lack of a reference methodology for implementing the protection requirements defined in the Law, this work proposes one that provides a basis for constructing the network architecture supported by the most common models and applying a security policy to computer network infrastructures.

General Terms

Computer Networks, LGPD

Keywords

Methodology, Security, Firewall, GDPR, Data Protection

1. INTRODUCTION

The constant flow of data on the Internet catches the attention of malicious users looking for breaches to capitalize on this information. Considering the need to protect people's personal data, governments create laws and regulations such as the General Data Protection Regulation (GDPR)[9], the United Kingdom Data Protection Act (UK DPA)[21], the California Consumer Privacy Act (CCPA)[5], and the General Law for Personal Data Protection (from Portuguese, *Lei Geral de Proteção de Dados Pessoais*) or LGPD in Brazil[3].

Varonis[22] presented some data on risks about obsolete and unprotected data, inadequate management of permissions and passwords, and based on a sample of 130 companies, where 6.2 billion files were analyzed, some interesting data related to security are:

(1) 21% of company files are not protected;
(2) 41% of companies have more than 1000 confidential files[1] open to anyone;
(3) 88% of companies with more than 1 million files have more than 100,000 of them open to anyone;
(4) 65% of companies have more than 500 employees whose passwords never expire.

CERT.br[2][6] points out that in 2019 there were 875,327 cybersecurity incidents in Brazil (representing an increase of 29% in relation to 2018) among which: scans that made up 46.81% of the attacks, denial of service attacks with 34.42%, attacks on Web servers with 2.55%, fraud attempts with 4.5% among others.

In response to these facts, within the Brazilian scenario, in 2018 the LGPD was created based on the European. Among its indications, article 46 of LGPD establishes that: "The treatment agents[3] must adopt security, technical and administrative measures capable of protecting personal data from unauthorized access and accidental or illicit situations of destruction, loss, alteration, communication or any form of improper or illicit treatment".

Failure to comply with this law can result in fines of up to 2% of revenue (limited to 50 million BRL) for infringement, daily fines, publicity of the infraction, data blocking, data deletion, suspension of the database operation, and total or partial prohibition of activities related to data processing.

According to information from Serpro[20], 53% of Brazilian companies are not prepared to apply the new law, where 19% of the administrators of these companies do not even know what the LGPD is about, moreover, the same article points that 85% of the companies are not ready to guarantee the rights and duties related to data processing required by it. Because they are not prepared at the moment and there is no methodology to assist in this adaptation, companies are at risk of reaching the term in which the

[1]Files containing sensitive information such as: credit card numbers and other personal information

[2]Center for Studies, Response and Treatment of Security Incidents in Brazil

[3]Comprises: the Controller, someone who handles decisions regarding the processing of personal data, and the Operator, someone who performs processing of personal data on behalf of the controller

law will have legal efficacy, even without having their infrastructure ready and without guidance, which may result in sanctions before cited.
Given this, it is necessary to develop a methodology - based on the LGPD - that, when providing guidelines for the application of a security policy in the network infrastructure, presents itself as a mean of proving the application of all the necessary technical requirements for data protection of third party data. The methodology presented in this work seeks to serve as a reference point for treatment agents for network infrastructure, to meet the requirements of the law that point to the use of technical methods of network protection, focusing on the scope of data traffic in means of transmission acting at the level of the network architecture.
This work is structured as follows, in section 2, all topics considered essential for the understanding of the theme and the proposal are treated. Section 3 presents recent works that have an affinity to the topic of information security. Section 4 presents the proposed methodology, its phases, and the activities involved. Finally, section 5 gives an overview of the results and future work.

2. THEORETICAL FOUNDATION

This section discusses some works that conceptualize important topics within computer security.

2.1 Network Invasion Techniques

Due to the inclusion of increasingly consolidated technology in daily life, more and more sensitive data are disseminated on the Network, causing the interest of malicious users in obtaining such data to acquire some kind of advantage (financial in most cases). To combat them, you need to know how your methods work, below is an overview of network attacks:

2.1.1 Network Attack. Initially, it is necessary to have an overview of the attacks, it can be seen when analyzing the attacks that malicious users follow a methodology to apply them, according to Hoque et al. [11], the attacker follows the following sequence of steps:

(1) Information collection - In which the attacker tries to collect information about network vulnerabilities in order to use them to assist in the attack;
(2) Vulnerability assessment - Based on the vulnerabilities found in the previous step, the attacker tries to compromise some nodes within that network;
(3) Launching the attack - In this phase, the attacker effectively launches the attack on the victim using the compromised nodes obtained in the previous step;
(4) Cleanup - Finally, the attacker tries to erase his tracks by cleaning up log files.

To categorize the attacks and their tools, the work also proposes a taxonomy model that can be adjusted as follows: Information Acquisition Tools and Techniques (e.g., sniffing and scanning) and Attack Launching Tools and Techniques (e.g., trojans, package spoofing, fingerprint attacks, and others)

2.2 Application of Security Techniques

In this section, the main technologies when it comes to securing a network will be covered.

2.2.1 Firewall. Duan and Al-Shaer [8] define that Firewalls are important security devices that protect the network by blocking unwanted traffic based on filtering policies. This component is usually positioned on the border between two networks. Figure 1 shows a classic example of a corporate network architecture showing the location of a Firewall in this type of network.

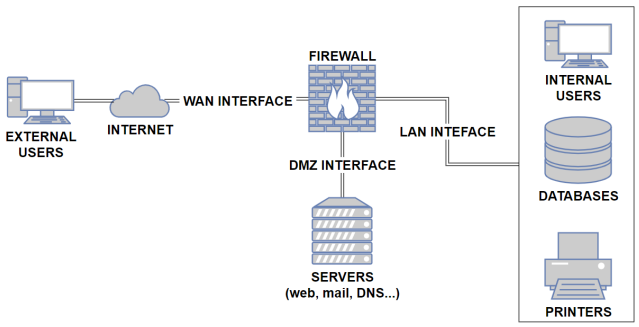

Fig. 1. Example of a Corporate Network Architecture.

A standard firewall consists of 3 network ports: one that gives access to the public internet, generally known as a WAN port, one that connects to the internal network, known as LAN, and a third that gives access to a subdivision of the internal network called DMZ (Demilitarized Zone). Usually medium-sized or large companies and any company that has e-commerce should have a DMZ in its network architecture, in this zone are servers that must, by business rule, be accessed by users outside the company, differently from the LAN that deals with the internal network that contains files that should not be publicly accessible.

2.2.2 IDS (Intrusion Detection System). According to Moustafa and Slay [16] IDSs are tools that monitor the flow of the network to identify and alert about attacks, which can be classified into:

(1) Signature-based - These contain a database of known attacks used to compare with traffic and can thus identify attacks based on their signature[4];
(2) Anomaly based - These create a profile considered "normal" by the daily functioning of the network. Any deviation from such behavior will be considered an attack.

Figure 2 shows an architectural model for the placement of an IDS on the network right after the Firewall. When identifying a suspicious flow according to its type of analysis, IDS will generate alerts that will be forwarded to a management system.

2.2.3 IPS (Intrusion Prevention System). In addition to the IDSs, there is an additional concept of defensive tool that can be analyzed, the Intrusion Prevention Systems - IPS. Bhuyan, Bhattacharyya and Kalita [2] suggest that the IPSs are a refined firewall capable of denying access to hostile traffic while legitimate traffic continues to have access. One form of classification for IPSs (which can also be applied to IDSs) is:

(1) Host Based - Where the IPS is placed as an agent on each host in the network to prevent an attacker from entering.

[4]When talking about attacks, signatures are bits of common bytes between samples of them

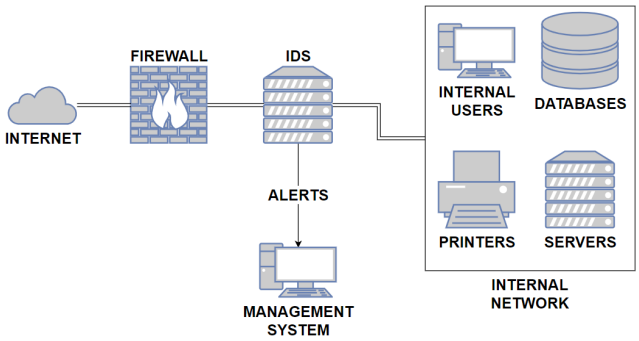

Fig. 2. Network Architecture Example with IDS.

(2) Network-based - Where IPS is placed on the network to monitor traffic and identify possible attacks and prevent them from entering. The network must be configured so that all traffic passes through the IPS.

2.3 Vulnerability Analysis

The vulnerability analysis is one of the phases of a rapid test process in which techniques or tools are used to identify possible "loopholes" to be exploited in an attack on a system or network. Samtani et al. [18] define in his work that there are two categories of techniques or tools for vulnerability analysis:

(1) Passive - where the objective is to cross-reference specific characteristics of the reference system with a database of known vulnerabilities;
(2) Active - where the device is actively investigated

2.4 Standards

In this section, the standards that are cited and adapted to the methodology proposed in this work will be treated

2.4.1 ISO 27001. ISO (International Organization for Standardization) is an international organization that covers unions focused on standardization in various areas of interest. The ISO 27000 family deals with Information Security management, in the paper of Hsu, Wang and Lu [12] the authors conceptualize that ISO/IEC 27001: 2013, official name, is a standard that provides specifications for Information Security Management System (ISMS).

2.4.2 ISO 27002. The ISO/IEC 27002 contains guidelines that describe examples of information security applications by using particular control forms to attain control targets. The control forms cover 11 areas of security as laid out in ISO/IEC 27001. ISO/IEC 27002 does not dictate certain control forms but lets users choose and apply the type of controls that best serve their needs, by taking into account their risk assessment results [14].

2.5 Laws and Regulations

This section brings the introductory concept regarding the main regulations cited in the paper.

2.5.1 General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR) (EU) 2016/679 is a European law regulation on privacy and protection of personal data, applicable to all individuals in the European Union and European Economic Area. It also regulates the export of personal data outside the EU and EEA[9].

2.5.2 General Law on Protection of Personal Data (LGPD). Law governing the processing of personal data, including digital media, by a natural person or a legal person under public or private law, to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person[3].

3. RELATED WORKS

This section presents the main works dealing with adaptation to new information security laws. In their work Lopes, Guarda and Oliveira [15] seek to discover to what extent the implementation of ISO 27001[5] that provides specifications for Information Security Management Systems (ISMS) can be a facilitating factor for companies to comply with GDPR. Initially, the authors make a brief history about the development of GDPR and point out the main innovations of this regulation. After that, the authors describe the ISO 27001 standard, listing advantages that the adoption of this standard brings to Organizations.
In their discussion, the authors claim that there are many similarities between GDPR and ISO 27001, and demonstrate based on GDPR topics where ISO can be applied, however, this does not guarantee full coverage and should be seen as a facilitator. According to the authors, GDPR is a global standard that provides a strategic view of how organizations need to ensure data privacy. ISO 27001 is a set of good practices with a limited focus on information security and does not cover problems associated with data privacy as described in chapter 3 of the GDPR:

(1) Consent;
(2) Data Portability;
(3) The Right to be Forgotten;
(4) The Right to Restriction of Processing.

They conclude that based on their research, any Organization that has already implemented or is implementing ISO 27001 is in an excellent position to comply with GDPR requirements.
In the work Diamantopolou, Tsohou and Karyda [7] the authors identify synergies between GDPR and ISO 27001 and propose practices for their exploration. Initially, a scenario is given contextualizing the GDPR and its history, then the responsibilities of the data controllers are cited, who must apply measures to guarantee an acceptable level of security, although the law does not specify exactly what the methodologies or techniques would be.
Next, GDPR is conceptualized and highlights the greatest advances made with it, which are items such as Definition of personal data, Definition of special categories of personal data, Responsibilities of data controllers, Jurisdiction, Consent management, Notification of violation.
The authors also conceptualize ISO 27001 and point out its composition, then, an analysis is made extending an existing ISMS (obtained through the application of ISO) to suit GDPR based on the PDCA cycle used by the standard including actions to be taken.
In conclusion, the authors state that the application of ISO supports the organization in creating better business efficiency,

[5]It is an international standard published by the International Organization for Standardization (ISO)

protects valuable assets, protects the team's reputation, and facilitates compliance objectives. Several GDPR requirements are not covered by the ISO, however, the ISO provides a means to take organizations a step closer to achieving the regulation by minimizing effort.
The first work tries to relate the use of ISO 27001 in the adequacy to GDPR and it is shown that it does not guarantee full compliance with the law, but it is seen as a good gateway. The second work assesses the security of sharing security alert information by identifying risks in the DPIA report. Finally, no studies were found that applied LGPD in Brazil.

4. DEFENSIVE ARCHITECTURE METHODOLOGY (DAM)

The LGPD requires that the Organizations, apply technical and administrative security measures to protect data from unauthorized access under penalty of sanctions. This new law does not specify the means to be used to achieve what is required, therefore, a methodology facilitates the process because based on it, techniques, methods, tools, and formal activities can be defined based on scientific literature.
The objective of this work is to develop the Defensive Architecture Methodology (DAM), which aims to operate at the level of network architecture, seeking compliance with the LGPD where it refers to the technical means for the defense of data. In addition, this methodology presents means by which the network will be constantly monitored for flaws that cause vulnerabilities and also has the generation of reports that can serve to attest that the defense policies were in correct operation during the occurrence of a claim thus avoiding the application of sanctions on the Organization for negligence regarding data security.
There were no existing methodologies for LGPD because it is a recent regulation and there are no such artifices with an exclusive focus on its requirements. Taking into account the levels of protection such as protection in databases, file systems, access terminals, and networks connected to the internet for traffic and data service, in which the latter is the core of this work. In other words, the methodology built here does not offer complete data protection, being more focused on the level of network traffic.
The protection of network infrastructure involves the protection of data in the data traffic layer and for that, it is necessary to apply security models to ensure the correct application of the security guidelines, defined by Brazilian law, and to assist network administrators in correct applying security policies, through the correct implementation and configuration of the technological resources available and normally applied in network security, that will involve the application of security techniques such as Firewall, Detection and Intrusion Prevention System and Vulnerability Analysis.
As shown in Figure 3, the DAM consists of 3 main phases: building the wall, looking for cracks, and structural reporting. In phase 1, it will be necessary to create a security model that includes the use of tools such as Firewall and IDPS, the purpose of this phase is to form a solid defense at the architectural level. In phase 2, the monitoring activity will use a new tool this time focused on vulnerability analysis to find flaws that put the network at risk. In phase 3, a report will be generated, the vulnerabilities will be ranked (by a method purposed in this work) and will be applied the countermeasures (techniques and tools) recommended, among the most common that may be mentioned, is the closing of specific firewall ports that may have been left open due to misconfiguration.

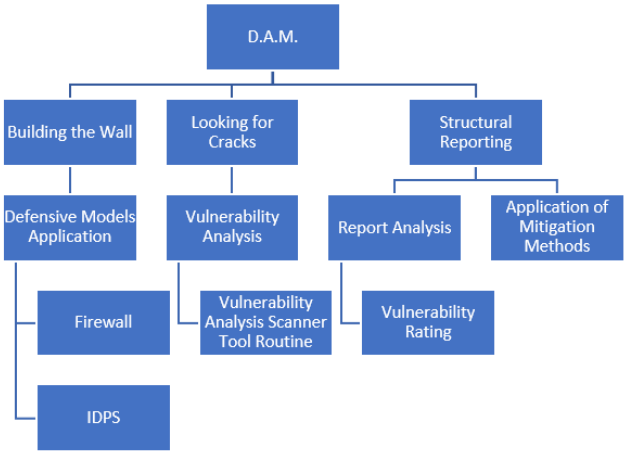

Fig. 3. DAM Details.

Then, the activities of each phase will be presented in the subsections, providing details of their operation, objectives, main outputs, methodologies, techniques, and tools involved in the process, such as the scientific basis for their use.

4.1 Building the Wall

Initially in the "Building the Wall" phase, in its activity "defensive models application", will be used the standards of the ISO 27000 family, more specifically ISO 27001 and ISO 27002, to adapt its controls to the DAM. According to the work of Diamantopolou, Tsohou and Karyda [7] and Lopes, Guarda and Oliveira [15] the use of such ISOs in the suitability for GDPR can be seen as a starting point that will put Organizations in a good position.
Considering the similarities between the GDPR and the LGPD, especially when it comes to Article 32 of the GDPR, which states that controllers and data processors must implement technical and organizational measures to ensure a level of security appropriate to the risk, this article is similar to Article 46 of the LGPD already mentioned in this work, demonstrates that the new Brazilian law allows the development of security models.
So specifically within this phase where there is the preparation of a solid defense when it comes to the level of network architecture, can be associated with the controls mentioned in annex A.13 of ISO 27001 that deals with communication security. In this domain, its controls try to guarantee the protection of information on the network and its facilities for processing support information [13].
Thus, Rianafirin and Kurniawan [17] when identifying physical security devices using ISO 27002 as a reference associates IDS as an item in the domain of network security management control, this work also relates the firewall with the domain of communication security. Achmadi, Suryanto and Ramli [1] divide the ISO into 4 categories, when talking about the software category, network security tools are mentioned, such as Firewall, IDS, and IPS.
In the case of the Firewall, the best practice model shown in Wack, Cutler and Pole [23], a guide prepared for NIST, points out that it must be positioned immediately before traffic enters the router allowing it to analyze all incoming and outgoing traffic, thus being able to apply the filters more efficiently.
In addition, will be taken into account three architectural models to demonstrate the necessary configurations about security policies, the models are infrastructure without DMZ,

infrastructure with DMZ, and infrastructure with DMZ and corporate application.

4.1.1 Infrastructure without DMZ. This is the simplest model in which there are only the WAN and LAN interfaces and is used in environments that do not provide any corporate network services, only for companies that connect to the web, also encompassing residential models. It is important to say that the following tables come with configuration suggestions, as there is no obligation to provide (allow) all of these services.

Table 1. Security Policy Rules Table for Infrastructure Without DMZ

Services	Ports	Status	Direction	Origin	Destiny
HTTP/HTTPS	80/443	allow	both	any	any
Telnet	23	allow	inbound	specific ip	specific ip
SSH	22	allow	inbound	specific ip	specific ip
FTP	21	allow	inbound	any	any
DNS	53	allow	both	specific ip	any
SMTP	25	allow	outbound	any	any
POP3	110/995	allow	inbound	any	any
IMAP	143/993	allow	both	any	any

In Table 1 the rules related to this architectural case, and the zone direction considered is LAN ⇒ WAN. Justifying, the HTTP and HTTPS ports must be allowed in both directions from any source to any destination (except for cases that require specific configurations) thus allowing LAN client access to the internet. Telnet and SSH services must be allowed in the direction of inbound, from a specific address to another specific internal address, allowing network administrators to have remote access. The FTP service must be allowed, in the inbound direction, with any source and any destination so that LAN stations can download via FTP, from the internet. The DNS service must be allowed in both directions, originating from a specific IP and any destination allowing the stations to resolve domain names as DNS clients of a specific server (provided by the internet provider). The SMTP service must be allowed in the outbound direction from any source to any destination, enabling the sending of email. The POP3 service must be allowed in the direction of inbound allowing the receipt of emails. Finally, the IMAP service must be allowed in both directions to enable the use of webmail.

4.1.2 Infrastructure with DMZ. As already seen in this work, this architecture contains a special zone that, as a rule of business, should contain servers that can be accessed by external users, it is a useful model for Organizations that provide a web page and email service.

Table 2. Security Policy Rules Table For Infrastructure with DMZ (LAN ⇒ WAN)

Services	Ports	Status	Direction	Origin	Destiny
HTTP/HTTPS	80/443	allow	both	any	any
FTP	21	allow	inbound	any	any
SMTP	25	allow	outbound	any	any
TELNET	23	allow	both	specific ip	specific ip
SSH	22	allow	both	specific ip	specific ip
POP3	110/995	allow	inbound	any	any
IMAP	143/993	allow	both	any	any

In Table 2 there is the first set of rules, in this case considering the list of LAN ⇒ WAN zones (there will be 2 more sets with different relations). For this relationship, HTTP, HTTPS, SMTP, FTP, IMAP, and POP3 services will work in the same way and for the same purposes as described in the previous infrastructure model. On the other hand, SSH and Telnet services must be allowed in both directions with the specific origin and specific destination, which allows network administrators to access a station on the internal network (LAN) of a device on the external network (WAN) and vice versa.

Table 3. Security Policy Rules Table For Infrastructure with DMZ (WAN ⇒ DMZ)

Services	Ports	Status	Direction	Origin	Destiny
HTTP/HTTPS	80/443	allow	both	any	specific ip
FTP	21	allow	inbound	any	specific ip
DNS	53	allow	both	specific ip	specific ip
POP3	110/995	allow	inbound	any	specific ip

Now in Table 3, the set of rules this time for the WAN ⇒ DMZ relationship. For this relationship, must be allowed the HTTP and HTTPS service in both directions, starting from any source but to a specific destination (which should in most cases be access to the web page hosting server), enabling access by external users to the available service. The FTP service must also be allowed only in the inbound direction from any source and arriving at a specific destination allowing remote stations (WAN) to download via FTP from a Web server (DMZ). The DNS service must be allowed in both directions from a specific source (DNS server of the internet provider) to a specific destination (Web server, for example) enabling the synchronization of primary and secondary DNS (ISP - Internet Service Provider). Finally, the POP3 service must be allowed inbound from any source and with a specific destination (email server) enabling the receipt of emails.

Table 4. Security Policy Rules Table For Infrastructure with DMZ (DMZ ⇒ LAN)

Services	Ports	Status	Direction	Origin	Destiny
HTTP/HTTPS	80/443	allow	both	specific ip	any
FTP	21	allow	outbound	specific ip	any
DNS	53	allow	both	specific ip	any
SMTP	25	allow	inbound	specific ip	any
POP3	110/995	allow	inbound	specific ip	any
IMAP	143/993	allow	both	specific ip	any

In Table 4, for this infrastructure model representing the DMZ ⇒ LAN relationship, where HTTP and HTTPS services must be allowed in both directions from specific sources with any destination within the Lan enabling the internal network to access services provided in the DMZ (with the specific IPs being of Web, DNS, and Email Servers). The FTP service must be allowed in the outbound direction from a specific source and with any destination allowing LAN stations to download via FTP from the DMZ server (Web server, for example). The DNS service is allowed in both directions from a specific address (DNS server) to any destination, enabling name resolution for LAN stations. SMTP and POP3 services must be allowed in the inbound direction of a specific IP (email server) to any destination enabling the transmission of corporate emails (SMTP) and the receipt of emails (POP3). Finally, the IMAP service must be allowed in both directions, starting from a specific source (email server) for any destination station, enabling the use of Corporate Webmail.

4.1.3 Infrastructure with DMZ and Corporate Application. In this model, a web server is located in the DMZ while the application and database servers are located on the LAN. Thus, when an external user makes use of the service he interacts with the webserver and it is the one who communicates with the application server and the latter communicates with the database server. Therefore, the user does not have direct access to the application server or the database.
In this infrastructure model, the operation is similar to the previous model, so the focus will remain only on what is different because there are two new services, SQL (1433) related to the database and a service of its own value that is related to the corporate application informed by the organization, therefore, in table 5 there are:

(1) the corporate application service in the WAN ⇒ DMZ direction open in both directions in the case of the need for remote access, via the web, of the presentation layer implemented in the DMZ;
(2) the corporate application service in the DMZ ⇒ LAN direction open in both directions so that the presentation layer (web server, in the dmz) of the application can access the services of the implementation layer (lan);
(3) the SQL service in the DMZ ⇒ LAN direction open in both directions to enable the web server to access the services provided by the Database layer implemented in the corporate network (lan).

Moving to IDPS[6], DAM makes use of a network-based type since the objective at this stage is to protect the entire network from its point of entry. Here the guide to be used will be Scarfone and Mell [19] also published by NIST and it is indicated that for this type of IDPS the positioning is the same thought for the Firewall, being on the safer side of the network.
Once these protection tools are positioned and configured, the next phase will look for flaws in this previously performed configuration and proof of the obtained security level.

4.2 Looking for Cracks

The next phase, "Looking for Cracks", in your "vulnerability assessment" activity, will try to find flaws in the configurations through a vulnerability analysis routine made by some automated tool. This phase is also in charge of generating the input data for the following phases.
The Nmap[7] tool that will be used in this work, a service scanner created by Gordon Lyon, used to discover hosts and services on a network when sending packets and analyzing responses. Because it is possible to use it separately - thus improving performance - Nmap becomes the best option because it already fulfills what is necessary for this work (port scanning) in addition to the ability to generate logs (they will be important for the next phases in the generation of reports) in different formats.
Nmap uses the various port scanning strategies mentioned in the section 2. In this work, will be used the SYN Scan and UDP Scan methods to check all the ports, since the objective is to verify that the process done in Phase 1 of the DAM was correctly applied, testing the status of the ports and matching them with the appropriate architectural model (among the 3 presented in phase 1).
Another important aspect is the different types of responses that a scan can generate, in our case with Nmap, responses are not limited to open or closed ports. Therefore, there are 4 statuses in which a port can be classified:

(1) open - In this case, the port is accessible and there is a service "listening" to that port;
(2) closed - The port is accessible, there is nothing filtering the port (firewall) and there is no service "listening" to that port;
(3) filtered - Filtered ports are the result of applying a packet filter or Firewall in which case the port may still be open or closed, the scanner just couldn't get any response from the target;
(4) open—filtered - In some cases, the lack of response does not necessarily indicate that the port is filtered, it may still be open, so it ends up falling into that classification. An example, on a UDP connection, in most cases the destination system does not send a response when receiving a UDP packet. Thus, if the target system does not respond, the scanner categorizes it as "open — filtered".

In Phase 1, the three most common architectural models for applying sets of security configuration policy rules to the Firewall were separated, now, in Phase 2 it is time to test whether the application of the chosen model was executed correctly. For this, a Port Scanning tool will be used that will check each of the 65535 both for the TCP protocol, using SYN Scan, and for the UDP protocol, through UDP Scan.
SYN Scan operation starts with Nmap sending a packet with the SYN flag to the port to be checked, starting a three-way handshake protocol, so if the port is open, the next step in the protocol will be to respond with a packet with the SYN and ACK flags. In a normal connection, the last step would be for the "port scanner" device to respond with a packet with the ACK flag, but the information that the port is open has already been obtained and if a connection occurs, the concern will arise to close the connection, a reply must be given otherwise the target device would consider that the packet was lost and would be resending it, so a packet with the RST flag indicates to the target device to give up the connection. On the other hand, if after Nmap sends the SYN packet trying to start the verification/connection and the target device only responds with a packet with the RST flag, it indicates that the port is closed.
UDP Scan brings with it the complication of being a longer scan (depending on the ICMP response rate) working with sending empty packets or with specific payload depending on the port you want to analyze and waiting for a UDP response to define it as open, or an ICMP response unreachable to define it as closed.
The scanning process is started with the command (if done via CLI[8]) "nmap <target>", where, "target" can be an IP or a list of IP addresses (localhost and domain names can also be used). This command executed as a privileged user executes SYN Scan on the considered 1000 most popular ports by default. For this work, as previously mentioned, it will be necessary to perform the scan on all ports, therefore, will be used the "-p-" flag that will be responsible for this scope. Finally, we also want to store the results in a document that can be processed in software in the future, so we will include the flag "-oX <filename>", where "-oX" indicates that the output should be in XML format and if necessary a path for storing the file can be informed. In addition to specifying the scanning technique, other flags are used: for SYN Scan the flag "-sS" and for the use of UDP Scan the flag "-sU".
For all Scans, Nmap performs some tasks in the background, initially converting hostname to an IPv4 address using DNS name resolution. Subsequently, it performs a host discovery process to

[6]System that combines the functions of an IDS and IPS
[7]https:/ /nmap.org/
[8]command line interface like Windows CMD or Linux Terminal

Table 5. Security Policy Rules Table for Infrastructure with DMZ and Corporate Application

Services	Ports	Status	Direction	Zone	Origin	Destiny
Corp. App.	App. Port	Allow	both	WAN ⇒ DMZ	specific ip	specific ip
Corp. App.	App. Port	Allow	both	DMZ ⇒ LAN	specific ip	specific ip
SQL	1433	Allow	both	DMZ ⇒ LAN	specific ip	specific ip

verify that the host is active. Nmap then converts the IPv4 or IPv6 address back to a hostname using a reverse DNS query. Finally, it starts the chosen scan depending on the user's privileges [4].
At the end of the execution, Nmap generates a report indicating the analyzed ports, the status, and the corresponding service[9]. This report can be exported in several formats, among them the XML, which will be the format chosen so that in the later phase the results are processed by a tool that will make the comparison between the expected result and the result obtained generating a diagnosis.
As it does not present zones and direction in its port analyzes and in order to test all the possibilities presented here, it is necessary to carry out repeated analyzes starting from the zones involved. Therefore, in model 1, which involves only 2 zones (WAN and LAN), 2 port analyzes will be necessary, one from WAN⇒LAN and the other in the reverse direction. For the other 2 models, 6 port analyzes will be necessary because they involve 3 zones (WAN, DMZ, and LAN). Thus it can be inferred how the situation of a port is, for example, if port 80 appears open in the analysis WAN⇒LAN and does not appear open in the analysis LAN⇒WAN, it can be inferred that it is only open in one direction, if it appears in both analyses it means that it is open in both directions.

4.3 Structural Reporting

The "Structural Reporting" phase will give an overview, based on the configurations applied in the previous phases, about defensive structures and their state. This report should contain the vulnerabilities found by scanning the network, as well as its level of threat according to the scale proposed in this work, and finally possible solutions to eliminate or mitigate the vulnerability.
The port analyzes obtained in the second phase will be the basis for the execution of this phase, it also includes the use of the software developed for the analysis of such documents. The software named "Castor[10]", developed in the Python programming language, works in general, as shown in the following activity diagram (Figure4).
Initially, the person in charge of the network must inform the software through a menu about which model he designed the network and depending on the model selected, the following steps may have some differences, starting with the amount of analysis to be informed, for example, in the case of model 1 selection, only 2 analyzes will be necessary: one in the direction of the WAN to the LAN and the other in the reverse direction.
For the other cases, as there are 3 zones involved, will be necessary a greater number of analyzes (6) for the reasons already explained in the previous phase. There is yet another difference that appears in the third model, in this case, the Organization contains a corporate application that makes use of a personalized port, which means that it must be informed manually by the person in charge. After this initial process, a comparison is made between the input analyzes and the expected models.

[9]this refers to the basic scan, but more information can be added depending on the desired and the flags used at the time of the scan
[10]Beaver, in Portuguese

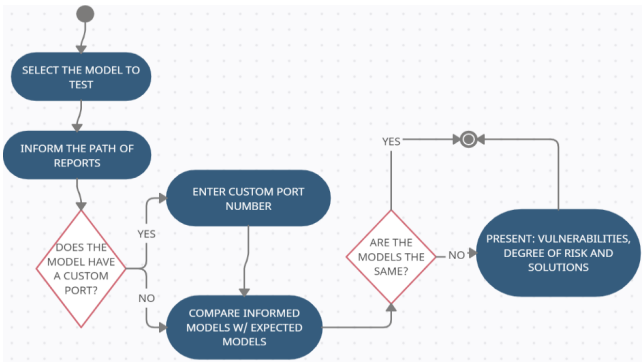

Fig. 4. Activity diagram.

This part of the process is done through lists, when the path of the result of the port analysis is informed, the software makes an analysis of the XML document and searches for the number of ports that are marked as "open", these numbers are stored in a list structure. In addition, internally for each model, zone, and direction, there are different pre-defined lists according to what is proposed in this work. When obtaining the lists originating from the informed port analyzes, the software makes a comparison, if the lists (informed and expected) are the same, it informs that the network has been configured correctly and ends the execution. Otherwise, the responsible person is informed that there are vulnerabilities, the level of risk, and the possible solution (Figure 5).

```
Lan->Wan analysis and recommended model are different
Vulnerability Level (DAM): Medium
we recommend that you close the following ports:
lan->wan:  [135, 139, 445, 554, 808, 2869, 5040, 5357, 5700
```

Fig. 5. Report.

The level of risk is based on the factors Zone and Direction of traffic as seen in the proposed models, and these are nominal levels (low, medium, and high), for this, the ranking is organized as follows:

(1) lan ⇒ wan - medium level of vulnerability;
(2) wan ⇒ lan - high level of vulnerability;
(3) dmz ⇒ wan - low level of vulnerability;
(4) wan ⇒ dmz - medium level of vulnerability;
(5) dmz ⇒ lan - high level of vulnerability;
(6) lan ⇒ dmz - medium level of vulnerability.

First, it was considered that all situations where there is inbound traffic to the LAN would be assessed as high risk because it is in this zone that the Organization's most sensitive files or the "trusted network" will be, according to Goodrich and Tamassia [10]. Then, it was considered that all incoming traffic to the DMZ would have

a medium level of risk, since, through elements of the DMZ, webservers, for example, there may be attacks such as Clickjacking, XSS, and others and that result in loss of third party data. Then, was considered outgoing traffic from the LAN to the WAN as a medium risk, because, despite being outgoing traffic, it still involves the most sensitive zone. Finally, outbound traffic from DMZ to WAN was considered a low-level risk because it is outbound traffic and involves only the DMZ.

5. CONCLUSION

This work aims to meet the demand for the new General Law for the Protection of Personal Data in Brazil that may cause sanctions to Companies that do not meet their requirements, through a methodology, the work seeks to be part of the "technical and administrative means" cited in the law for the defense of data, in this case, acting at the architectural level of the network.

The law did not regulate the technical security requirements to be applied, it only determines sanctions for those who do not protect the personal data of third parties. The DAM methodology provides a roadmap for data protection under the law.

The proposed methodology consists of 3 phases: Building the wall, Looking for Cracks, and Structural Report, which can structure, monitor, and report the state of the network architecture, being limited only to this level of security, not guaranteeing global security. However, still working to assist in compliance with Article 46 of the LGPD. The use of a methodology implies the application of techniques based on scientific literature and more widespread models.

With the proposed methodology, companies, public, and private institutions will have a technical procedure for applying data security measures at the network traffic level.

As future work, there is the expansion of the Building the Wall phase, adding more defensive models (such as new tools) and expanding the scope of the methodology as it currently works only at the architectural level of the network and can be extended to other levels, including the protection of File System and Database.

6. REFERENCES

[1] Dedy Achmadi, Yohan Suryanto, and Kalamullah Ramli. On developing information security management system (isms) framework for iso 27001-based data center. In *2018 International Workshop on Big Data and Information Security (IWBIS)*, pages 149–157. IEEE, 2018.

[2] Monowar H Bhuyan, Dhruba K Bhattacharyya, and Jugal K Kalita. Alert management and anomaly prevention techniques. In *Network Traffic Anomaly Detection and Prevention*, pages 171–199. Springer, 2017.

[3] Brasil. Lei nº 13.709, de 14 de agosto de 2018.

[4] Paulino Calderon. *Nmap: Network Exploration and Security Auditing Cookbook*. Packt Publishing Ltd, 2017.

[5] California. California consumer privacy act, 2018. Disponível em:`https://oag.ca.gov/privacy/ccpa`, Acesso em: 02/01/2020.

[6] CERT.br. Estatísticas dos incidentes reportados ao cert.br, 2020.

[7] Vasiliki Diamantopoulou, Aggeliki Tsohou, and Maria Karyda. General data protection regulation and iso/iec 27001: 2013: synergies of activities towards organisations' compliance. In *International Conference on Trust and Privacy in Digital Business*, pages 94–109. Springer, 2019.

[8] Qi Duan and Ehab Al-Shaer. Traffic-aware dynamic firewall policy management: techniques and applications. *IEEE Communications Magazine*, 51(7):73–79, 2013.

[9] European Union. Regulation (eu) 2016/679 of the european parliament and of the council of 27 of april 2016, 2016. Disponível em:`https://gdpr-info.eu/art-1-gdpr/`, Acesso em: 22/01/2020.

[10] Michael Goodrich and Roberto Tamassia. *Introduction to Computer Security: Pearson New International Edition*. Pearson Higher Ed, 2013.

[11] Nazrul Hoque, Monowar H Bhuyan, Ram Charan Baishya, Dhruba K Bhattacharyya, and Jugal K Kalita. Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40:307–324, 2014.

[12] Carol Hsu, Tawei Wang, and Ang Lu. The impact of iso 27001 certification on firm performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 4842–4848. IEEE, 2016.

[13] ISO. ISO/IEC 27001:2013. Standard, International Organization for Standardization, Geneva, CH, October 2013.

[14] Muhammad Taher Jufri, Mokhamad Hendayun, and Toto Suharto. Risk-assessment based academic information system security policy using octave allegro and iso 27002. In *2017 Second International Conference on Informatics and Computing (ICIC)*, pages 1–6. IEEE, 2017.

[15] Isabel Maria Lopes, Teresa Guarda, and Pedro Oliveira. How iso 27001 can help achieve gdpr compliance. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6. IEEE, 2019.

[16] Nour Moustafa and Jill Slay. Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In *2015 military communications and information systems conference (MilCIS)*, pages 1–6. IEEE, 2015.

[17] Kartika Rianafirin and Mochamad Teguh Kurniawan. Design network security infrastructure cabling using network development life cycle methodology and iso/iec 27000 series in yayasan kesehatan (yakes) telkom bandung. In *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, pages 1–6. IEEE, 2017.

[18] Sagar Samtani, Shuo Yu, Hongyi Zhu, Mark Patton, and Hsinchun Chen. Identifying scada vulnerabilities using passive and active vulnerability assessment techniques. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, pages 25–30. IEEE, 2016.

[19] Karen Scarfone and Peter Mell. Guide to intrusion detection and prevention systems (idps). Technical report, National Institute of Standards and Technology, 2012.

[20] Serpro. Empresas estão ou não preparadas para atender a lgpd?, 2019.

[21] United Kingdom. Data protection act 2018, 2018. Disponível em:`https://www.gov.uk/data-protection`, Acesso em: 22/01/2020.

[22] Varonis. 2018 global data risk report from the varonis data lab, 2018.

[23] John Wack, Ken Cutler, and Jamie Pole. Guidelines on firewalls and firewall policy. Technical report, BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2002.