REVISTA DE GESTÃO E SECRETARIADO
MANAGEMENT AND ADMINISTRATIVE PROFESSIONAL REVIEW
ISSN: 2178-9010

Revista GeSec
São Paulo, SP, Brasil
v. 14, n.4, p. 5102-5122, 2023

DOI: http://doi.org/10.7769/gesec.v14i4.XXXX

Application of the threat modeling method in an operating system

Aplicação do método de modelação de ameaças num sistema operativo

Rodrigo Yokoyama [1]
Carlos Hideo Arima [2]

Abstract

Due to the increase in professionals adopting the home office model due to the COVID-19 pandemic, the threat to company information and assets has become more evident. This work aims to identify, describe and evaluate the impacts of applying the threat modeling method, using risk management standards, on corporate computers with the aid of a monitoring system. The proposed method for application suggests the adoption of processes and a system for updating, controlling and managing the Windows Operating System to reduce the threats faced. The research identified security using the STRIDE and DREAD methods and the ISO and NIST security standards. It verified 14 types of threats found in an operating system that can be properly identified and mitigated with the threat exploitation method.

Keywords: Threat Modeling. Stride. Dread. Risk. Security.

Resumo

Devido ao aumento de profissionais que adoptaram o modelo de escritório em casa devido à pandemia de COVID-19, a ameaça à informação e bens da empresa tornou-se mais evidente. Este trabalho visa identificar, descrever e avaliar os impactos da aplicação do método de

[1] Mestre em Gestão e Tecnologia em Sistemas Produtivos, Centro Estadual de Educação Tecnológica Paula Souza, São Paulo – SP, Brasil. E-mail: rodrigo.yokoyama@cpspos.sp.gov.br
Orcid: https://orcid.org/0000-0002-6421-7984

[2] Professor, Doutor em Gestão e Tecnologia em Sistemas Produtivos pelo Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza, Centro Estadual de Educação Tecnológica Paula Souza, São Paulo – SP, Brasil. E-mail: charima@uol.com.br
Orcid: https://orcid.org/0000-0001-7922-0943

modelização da ameaça, utilizando normas de gestão do risco, nos computadores das empresas, com a ajuda de um sistema de monitorização. O método de aplicação proposto sugere a adopção de processos e um sistema de actualização, controlo e gestão do sistema operativo Windows para reduzir as ameaças enfrentadas. A investigação identificou a segurança utilizando os métodos STRIDE e DREAD e as normas de segurança ISO e NIST. Verificou 14 tipos de ameaças encontradas num sistema operativo que podem ser devidamente identificadas e mitigadas com o método de exploração de ameaças.

Palavras-chave: Modelação de Ameaças. Stride. Temido. Risco. Segurança.

Introdução

According to a study prepared by Administration Institute Foundation (FIA), in April 2020, information collected from 139 small, medium and large companies operating throughout Brazil, in the period 2019 and 2020, 41% of company employees were placed in home office regime, almost all those who would have the possibility of working remotely, which amounted to 46% of the total staff. In the commerce and services sector, 57.5% of employees switched to teleworking, in small companies the percentage was 52%. (agenciabrasil.ebc.com.br, 2020)

Almost all systems face a variety of threats, and more are constantly being added as technology changes. These threats can come from outside or inside organizations, and their impact can be devastating. Systems can be prevented from fully functioning or confidential information can be leaked, which would affect consumer trust in the system provider. (Shevchenko et al., 2018)

The home office experiences revealed the general level of unpreparedness of software vendors, particularly about the security of their products. (Lallie et al., 2021)

Threat modeling is proposed as a solution for secure application development and system security assessments. Their aim is to be more proactive and make it more difficult for attackers to accomplish their malicious intentions. (Xiong and Lagerström, 2019).

Threat modeling methods are used to create an abstraction of the system; profiles of potential attackers, including their goals and methods; and a catalog of potential threats that may arise. (Shevchenko et al., 2018).

There is a lack of academic articles applying threat modeling with a focus on the computing environment used by end users. (Yokoyama and Arima, 2022).

As stated above, the research question is: how can threat modeling be applied in a computing environment at the operating system level?

To answer this question, the objective is to develop the application of threat modeling using the methods established in the literature in a computational environment, especially in the operating system.

Methodology

The present threat modeling was conceived based on the STRIDE and DREAD models, based on their application aiming at improving the security of the analyzed environment. This proposal uses some concepts of information security standards aimed at risk management that will be briefly explained below.

2.1 Threat Modeling

Threat Modeling can be defined as a strategic process designed to consider potential attack scenarios and vulnerabilities in a proposed or existing application environment in order to clearly identify levels of risk and impact. (Ucedavelez and Morana, 2015).

Good threat models can help verify the need for some requirements, for example, does the system need to be secure against someone who has physical access to the device? Apple said yes to the iPhone, which is different from the traditional PC world. As threats are found and triage is made to decide what to do with them, requirements are clarified. With clearer requirements, you can devote energy to a consistent set of security features and properties. (Shostack, 2014).

There is an important interaction between requirements, threats and mitigations. When using threat modeling, you may find that some threats do not align with business requirements and, as such, may not be worth addressing. With other threats, solving them would be too complex or expensive. It will be necessary to make a link between partially addressing them or accepting that these threats will not be addressed. (Shostack, 2014).

Threat modeling aims to greatly revitalize the data protection effort through a strategic and collaborative process. (Ucedavelez and Morana, 2015).

A good model helps to deal with classes or groups of attacks, in short, threat modeling is the use of abstractions to help think about risks. (Shostack, 2014)

2.2.1 STRIDE

Among a wide variety available that are considered methods for applying threat modeling, the STRIDE method is the most used method in the last 5 years for applying threat modeling. The results of the STRIDE approach are more meaningful, easily understandable, and comprehensive enough for system designers to develop appropriate security solutions. The STRIDE result can feed into risk analysis processes to establish the most critical threats and, in addition, the development of the most appropriate mitigation measures that should be applied. (Yokoyama and Arima 2020)

A good model helps to deal with classes or groups of attacks, in short, threat modeling is the use of abstractions to help think about risks. (Shostack, 2014). STRIDE is currently the most mature threat modeling method among other existing methods, developed by Loren Kohnfelder and Praerit Garg in 1999 and adopted by Microsoft in 2002. This method has evolved over time to include new threat-specific tables and variants. STRIDE by Element and STRIDE by Interaction (Shevchenko 2018).

STRIDE per element is more complex as it analyzes the behavior and operations of each component in the system. STRIDE by interaction, enumerates threats against system interactions considering origin, destination and interaction (Shostack, 2014).

STRIDE Per-element makes STRIDE more prescriptive by noting that certain threats are more prevalent with certain elements of a diagram, for example, one data store is unlikely to spoof another data store, by focusing on a set of threats against each element, this approach makes it easier to find threats (Shostack, 2014).

According to Shostack (2014) STRIDE is a mnemonic for things that go wrong in security, meaning: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. Each letter that makes up the name STRIDE is a category. The definition of each category, in Portuguese, is explained below:

- S: Spoofing is pretending to be something or someone you are not.
- T: Tampering is modifying something you shouldn't modify. It can include packets on the network, bits on disk, or bits in memory.
- R: Repudiation means claiming that you didn't do something (regardless of whether you did it or not).
- I: Information disclosure is about exposing information to unauthorized persons.
- D: Denial of Service are attacks designed to prevent a system from providing service, including crashing it, slowing it down excessively, or filling up all its storage.

- E: Elevation of privilege is when a program or user is technically capable of doing things they shouldn't do.

STRIDE analyzes vulnerabilities against each system component that could be exploited by an attacker to compromise the entire system (Khan et al. 2017). Based on STRIDE's 6 classifications, it is then possible to classify threats, entering each threat found in its appropriate classification in STRIDE.

After classifying the threats, it is necessary to evaluate the treatment for each threat found, choosing whether the threat will be mitigated, if responsibility will be transferred or if the risk will be accepted. The option of mitigating the threat is always the most favorable, other options should be considered only if there is risk tolerance.

Scandariato et al. (2015) in their descriptive study of the Microsoft threat modeling technique, show that the STRIDE method has a moderately low rate of false positives and a moderately high rate of false negatives. STRIDE has been successfully applied to cyber and cyber-physical systems (Shevchenko, 2018).

2.2.2 DREAD

DREAD can be leveraged to assess and rank the severity of threats. The DREAD and STRIDE methods can be used together for comprehensive cybersecurity and service lifecycle assessments (Zografopoulos et al., 2021).

STRIDE and DREAD are well-established threat modeling models for evaluating the security of products and services throughout their life cycle (Zografopoulos et al., 2021).

DREAD provides a blueprint by which threat vectors identified using STRIDE or other methodologies are evaluated and prioritized. Each individual threat vector is scored on five elements and an average taken, which can be used to compare its severity and probability with those of other threat vectors. Thus, DREAD goes beyond threat modeling to risk assessment. (Bodeau, Mcollum and Fox, 2018)

According to Seifert and Reza, (2016) The DREAD model classifies each threat into five different areas and then produces an overall classification based on the scores. DREAD analysis is based on determining answers to the following questions for each attack.

D – Damage potential: How much damage would result?

- High (3) – The attacker can gain full control of the system and/or perform tasks with administrative privileges.
- Medium (2) – Loss of sensitive information.

• Low (1) - Loss of trivial information.

R – Reproducibility: How difficult is the execution?

• High (3) - The attack can always be performed with ease.

• Medium (2) – The attack can only be performed with a specific time window and/or with a particular condition.

• Low (1) – The attack is extremely difficult to reproduce, even with extensive security knowledge.

E – Exploitability: How easy is it to reproduce the attack?

• High (3) – an inexperienced user can perform an attack in a short time.

• Medium (2) – An experienced user can perform the attack.

• Low (1) – The attack requires an extremely skilled person to accomplish the attack.

A – Affected users: How many people would likely be affected?

• High (3) – All users, default configuration and major clients are affected.

• Medium (2) – Some users and non-default configuration are affected.

• Low (1) – Small percentage of users are affected.

D – Discoverability: How difficult is it to find the vulnerability?

• High (3) – Vulnerability is easily noticeable and public sources explain the means of attack.

• Medium (2) – The vulnerability is contained in a functionality that is not very accessible on the system and requires a lot of analysis to find it.

• Low (1) – The bug enabling the vulnerability is obscure, users are highly unlikely to discover potential harm.

DREAD calculates the risk of threats encountered using various factors, including potential for harm, reproducibility, exploitability, affected users, and discovery. These individual ratings are then averaged to determine an overall threat score. DREAD is one of the most complete mechanisms to assess threat risk (Seifert and Reza, 2016).

2.2 ISO/IEC 27000

The ISO/IEC 27000 series of standards provides an overview of information security management systems (ISMS). The ISO/IEC 27001 standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system in the context of the organization.

ISO/IEC 27002 is the renamed ISO/IEC 17799 standard and is a code of practice for information security. Basically, it describes hundreds of potential controls and control mechanisms that could be implemented, in theory, subject to the guidance provided in ISO/IEC 27001.

ISO/IEC 27005 is the name of the main standard in 27000 series covering the management of information security risks, the standard provides guidelines for information security risks in an organization, specifically supporting the requirements of a security management system of the organization. information defined by ISO/IEC 27001 (Jeyaraj and Zadeh, 2010).

2.3 NIST 800-30

The purpose of NIST 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations. provides guidance to organizations in identifying specific risk factors. Risk assessment is a key component of a holistic risk management process across the organization. NIST 800-30 provides guidelines similar to the guidelines provided by the ISO/IEC 27000 standard for the treatment of risk.

The risk assessment process consists of four steps:

1. Preparation for the assessment.
2. Conduct the assessment.
3. Communicate the evaluation results.
4. Maintain the assessment.

Each step is divided into a set of tasks. For each task, the supplemental guidance provides additional information for organizations performing risk assessments.

The application of threat modeling was developed based on the steps explained below. Threat modeling perspectives and security standards were used to increase the protection of an operational environment.

Threat Modeling Development

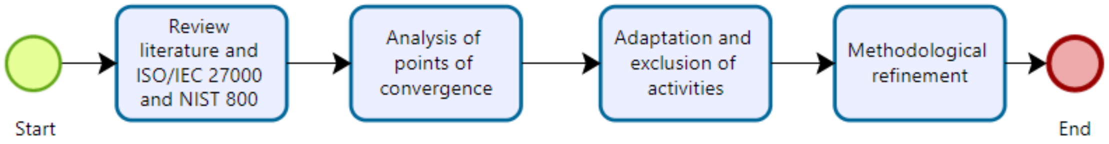
The application of threat modeling was developed based on the steps explained below. Threat modeling perspectives and security standards were used to increase the protection of an operational environment.

3.1 Definition of Expected Results

The expected result of this work is an application of threat modeling in existing processes with a focus on security and updating of programs for endpoints, using the STRIDE method based on the ISO/IEC 27005 standard and existing controls that can contribute, contained in the ISO/IEC 27002 and NIST 800-30 standards.

The main activities used to develop the solution proposed in this work are shown in Figure 1, they are: literature review and ISO/IEC 27000 and NIST 800 standards; Analysis of points of convergence; Adaptation and exclusion of activities; and Refinement of the methodology.

Figure 1:Methodology development process


Start
Review literature and ISO/IEC 27000 and NIST 800
Analysis of points of convergence
Adaptation and exclusion of activities
Methodological refinement
End

Source: Search result.

3.1.1 Review Literature and ISO/IEC 27000 and NIST 800 Standards

It was necessary to understand what concerns the main current threat modeling methodologies and standards ISO/IEC 27002, ISO/IEC 27005 and NIST 800-30. From the observation of the literature and suggestions contained in the ISO/IEC 27002, ISO/IEC 27005 and NIST 800-30 standards, we sought to identify and understand the activities involved in the proposed modeling process.

3.1.2 Analysis of Points of Convergence

As a strategy for presenting a methodology applicable to the standardization of security in an operational environment, we sought to identify the points where the methodologies analyzed converged. In other words, to define a base methodology, the activities that are present in ISO/IEC 27002 and in the application of STRIDE were mapped. Based on this strategy, a methodology was defined based on the activities of ISO/IEC 27002 and on the STRIDE methodology.

3.1.3 Adaptation and Exclusion of Activities

The main objective of this activity was to analyze the activities that made up the initial threat modeling methodology in terms of their suitability for the proposed objective. For this, the activities were contrasted with the properties inherent to the threat modeling paradigm and were targets of two strategic decisions: adaptation of the activity or exclusion of the activity.

3.1.4 Methodological Refinement

After searching the literature on possible solutions to the problem presented, the development of an artifact was defined as a potential solution that will help in a systematic approach to control and identify the threats found.

3.2 Design and Development

This activity defines the solution (artifact) that is a research contribution and the actual creation of the artifact. The processes below define the systematic approach to identifying and treating threats posed by the environment or asset.

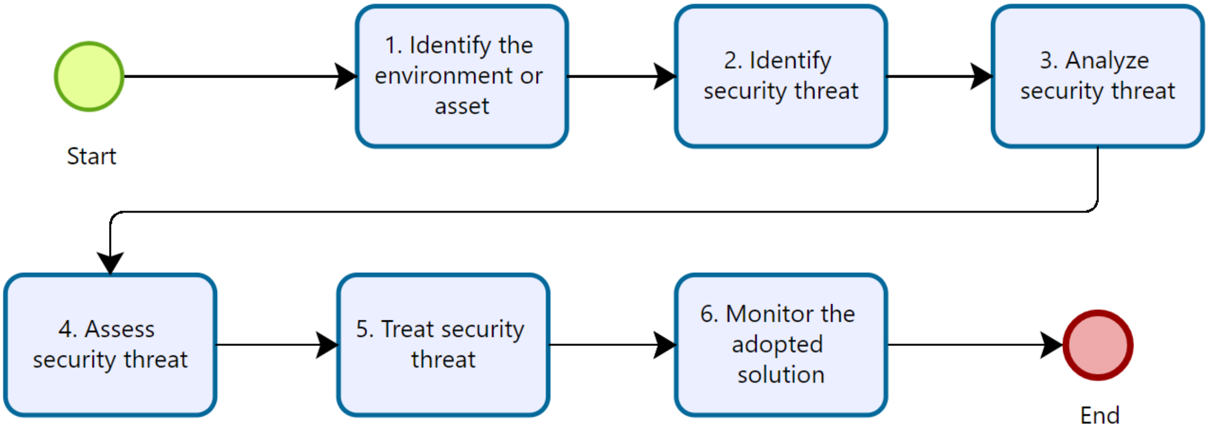
3.3 Processes

The applicable methodology for the proposed objective can be understood from the following processes and activities, prepared based on the controls contained in ISO/IEC 27005 and the use of the threat modeling method:

1) Identify the environment or asset
a) Identify technologies adopted
b) Identify system processes
2) Identify security threat
3) Analyze security threat
4) Assess security threat
5) Treat security threat
6) Monitor the adopted solution

Figure 2 presents the processes that represent the methodology:

Figure 2: methodology process


Start
1. Identify the environment or asset
2. Identify security threat
3. Analyze security threat
4. Assess security threat
5. Treat security threat
6. Monitor the adopted solution
End

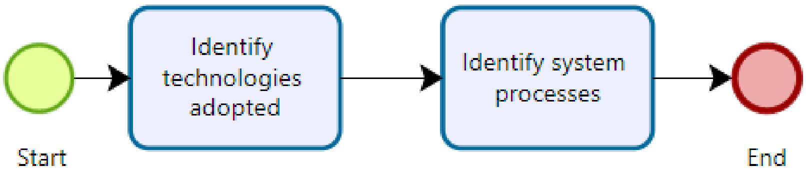
Source: Search result.

3.3.1 Identify the Environment or Asset

The first process is intended to gain an understanding of the system under analysis. For effective identification of security threats, it is necessary to understand the system assets, their processes and interactions. To carry out the architectural modeling step of the environment or asset, it is recommended to consult the documentation that technically describes the environment.

Thereby, the methodology proposed in this work defines the following activities to be carried out: Identify system assets and identify system processes. Figure 3 shows the representation of this process:

Figure 3:Environment or asset identification processes



Source: Source: Search result.

a) Identify technologies adopted

This activity aims to identify the different technologies adopted by the system. In this activity, it is necessary to identify which technologies are used or implemented for the use of the system and its product. You must identify the manufacturer, operating system, product version etc. allowing specific program-related threats to be scanned.

The technology adopted for this work was Microsoft's Windows 10 Operating System, where only its operating system will be analyzed, not considering the use of other third-party programs. Programs that interfere with the functioning and protection of Windows may be analyzed in future works.

b) Identify system processes

This activity aims to identify the processes performed by the system and processes that affect or modify the system.

These processes can include manual tasks by technology professionals, as well as automatic processes, which aim to modify something in the system itself or in the product that will be generated by the system, such as an update or the addition of some functionality. For example, in the case of this study, changing a process that involves updating a program or system contained in the image, the Windows operating system, will affect a critical process of the system deployment device and, consequently, the final product, which will have this system updated.

3.3.2 Identify Security Threat

This activity aims to identify the points of risk, threat or vulnerability of the system, in the case of this study, the operating system and its programs. This process seeks to identify risks, security threats and vulnerabilities in the analyzed environment, as a result, a list of security threats found in the assets that were analyzed is generated.

3.3.3 Analyze Security Threat

This step aims to analyze the threats found in the previous step. The analysis of risks, security threats and vulnerabilities are the main core of threat modeling, in this step the DREAD method was used to define the degree of threat of each item contained in the list of threats found in the previous step.

3.3.4 Assess Security Threat

In this step, the objective is to evaluate the threats highlighted in the previous steps. This activity aims to quantify the degree of danger of the threats found to show the magnitude presented by each threat, consequently helping to prioritize the treatment of each threat.

3.3.5 Treat Security Threat

This activity proposes reasonable solutions to the security threat found. According to ISO/IEC 27005 (2019), it is recommended that controls to modify, retain, avoid or share the risks are selected and that a plan for the treatment of the risk be defined.

3.3.6 Monitor the Adopted Solution

This step proposes continuous monitoring of the solution and analyzed environment, thus avoiding possible new security incidents and keeping the environment safe and up-to-date. It is recommended that the risks and their factors be monitored and critically analyzed to identify, as quickly as possible, any changes in the context of the organization and to maintain an overview of the risks.

For monitoring the adopted solution, it is currently not possible to prescribe a possible automatic solution due to the need to approve software updates provided by manufacturers before replication to the environment. Due to this limitation, a proposal was made for a system to aid in the approval control of operating system updates.

The proposed system will implement the process of continuous improvement in the verification of threats, which consists of improving the maturity of the product, as it will make the threat verification be done in an organized way and on defined dates, allowing threats to be found that were not mapped in a previous check. It will also make the update process a controlled task, no longer a reactive task, where the update only happens when a need is presented.

3.4 Control System Development

For system development, the PowerApps platform was used and for the development of triggers for sending emails to those responsible, the PowerAutomate platform, both from Microsoft. The PowerApps system has its own database stored in the Sharepoint cloud, using a standard format provided by Microsoft, with automatic backups being made at periods chosen by the tool manager.

The idealization of the system was made aiming at the internal functioning of the Microsoft “Teams” application, thus facilitating the interaction of the responsible analysts with the application.

Due to the purpose of the system, the following fields were considered essential for the system to work: ID, Software Title, Criticality, Modified by, Modified, Application Version, Approval Version, Verification Date, Approval Deadline, Periodicity, ID GMUD, Responsible Team, Focal point, Responsible manager, Threat modeling date, Current threat, Threat homologation version, CVE, Update site, Notes and Attachments, as shown in Table 1.

Table 1: explanation about the fields in the system

Field name in the system	Explanation about the field
ID	Number automatically assigned to the software for control in the system
Title	Software display name
Criticality	Measurement of the criticality level of the software update to the business: Low, medium or high
Modified by	Last professional who made changes to the control
Modified	Date of the last modification made
Application version	Current software version in the production environment
Homologation version	Version under approval, which is being tested before being deployed to the environment
Verification date	Date that will start the approval of the new version of the software
Approval deadline	Deadline for completion of software approval
Frequency	Periodicity in which the verification of a new version or available patch is carried out: Monthly, quarterly, half-yearly or annually.
ID GMUD	GMUD number related to software update
Responsible team	Team responsible for the software
Focal point	Professional responsible for verifying and homologating the program
Responsible manager	Software responsible manager
Threat modeling date	Date of last threat modeling performed
Current version threat	Field displays whether or not there is a threat in the current program
Homologation version threat	Field shows whether or not there is a threat in the program under approval
CVE	CVE number related to the vulnerability found, if any
Update site	Website containing details about the availability and changes contained in the new version
Comments	Remarks, if any
Attachments	Attachments needed to perform the task, as well as the threat modeling performed.

Source: Search result.

Fields: ID, Modified by, Modified and Approval Deadline are controlled by the system, and cannot be modified by human actions.

Fields: Criticality, Responsible team, Frequency, Focal point and Responsible manager, are not editable in the operator's view, only managers can change this information in the Web access to the system.

Fields: Title, Application Version, Homologation Version, Verification Date, ID GMUD, Threat Modeling Date, Current version Threat, Homologation Version Threat, CVE, Update Site, Comments and Attachments can be edited by operators.

The creation of a Team in Microsoft Teams is necessary to control people authorized to access the system, thus restricting the access of other professionals and allowing access only to people who will be involved in using the system.

A history of updates done by operators showing what was changed and who made the change in the system was considered a necessary item, causing any change in the system to be recorded, for possible future verification regarding the change.

The periodicity of verification of the new version of the system will dictate the time that the system must allow for approval. It is not feasible to allow automatic updating of the application due to the need for tests and validation before being implemented in the environment.

The number of updates for each software will vary, depending on: the number of times the software is updated by the company per year, if the update is a major update or if the update is a security patch. The periodicity was established to ensure that the software is up to date and so that it is possible to apply the continuous improvement process, as shown in Table 2.

Table 2: frequency and period to homologate

Frequency	Period to homologate
Yearly	3 months
Semester	2 months
Quarterly	1 months
Monthly	15 days

Source: Search result.

Homologation groups were created to ensure that the Operating System does not conflict with existing programs on computers, two groups were created that will receive updates. The first group has only Technology professionals and the second group includes at least one professional from each area of the company.

Groups will receive updates on different dates:

- 1st Group will receive the update as soon as it is available;
- 2nd Group will receive the update after 7 days of the implementation carried out in Group 1.

The system flowchart should work as follows:

1) On the program update date, the system will send an alert to the person in charge to check for updates and threats of the analyzed software. The person in charge needs to perform the verification within the proposed period, if not, the immediate manager will be alerted.

a) If there is no new version of the program, the person in charge will finish the verification task and the verification cycle will be finished.

2) If a new update is available, tests related to software conflicts and verification of software changes contained in the update note are started, to verify if there are any new characteristics in the software that represent a threat.

a) After tests in the homologation group and threat verification, if the program is compatible and does not represent a threat to the company's existing systems, the program is updated.

3) If the available version represents a threat to the company, is incompatible or is not available for download, contact is made with the supplier to verify the points listed.

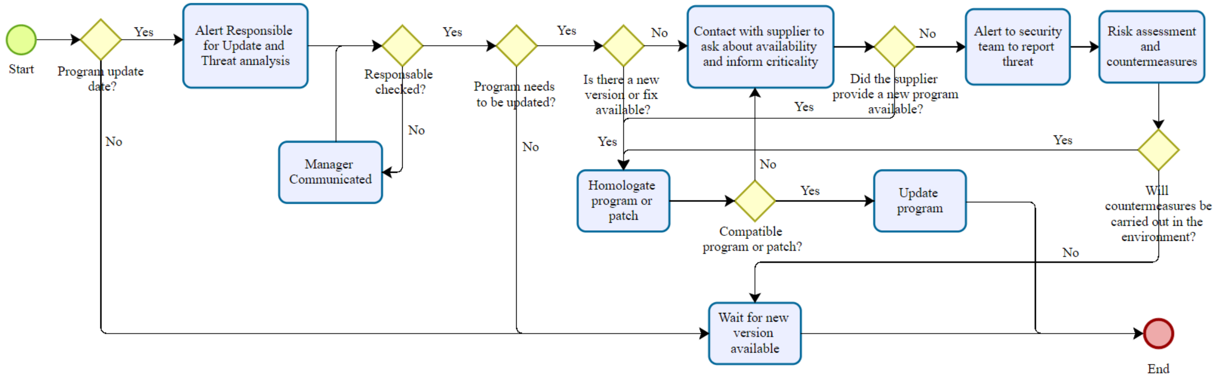
a) After homologation tests and threat verification, if the program is compatible and does not represent a threat to the company's existing systems, the program is updated.

4) If the supplier's update still poses a threat to the company or is incompatible with any other system used, the security team is alerted about the impossibility of updating and, if necessary, security patches are applied for the new version.

a) If there is no security patch for the new version, the security team is alerted to the threat and the risk assessment and countermeasure begins. The security team analyzes whether there is a need to apply a security patch for the old version or if the update to the new version will be carried out.

The system flowchart is represented in Figure 4:

Figure 4: system flowchart


Start
Program update date?
Yes
No
Alert Responsible for Update and Threat annalysis
Responsable checked?
No
Manager Communicated
Yes
Program needs to be updated?
No
Yes
Is there a new version or fix available?
No
Yes
Contact with supplier to ask about availability and inform criticality
No
Did the supplier provide a new program available?
Yes
Alert to security team to report threat
Risk assessment and countermeasures
Yes
Will countermeasures be carried out in the environment?
No
Homologate program or patch
Compatible program or patch?
Yes
No
Update program
Wait for new version available
End

Source: Search result.

For the purpose of the system, it was necessary to create three individual triggers, which will send communication with the responsible professionals:

• Sending an email to those responsible for checking the new version. The “verification date" field will inform when the e-mail should be sent;

- Sending an e-mail to the manager responsible for the application, if the person responsible has not carried out the new version verification task. The field "Approval deadline" will inform when the e-mail must be sent;
- Sending notification to the security team, if the supplier does not have a solution related to the threat found. When the field "Threat homologation version" is filled in with yes, the message on Microsoft Teams must be sent.

According to the processes and system flow, threats will be found by analyzing the update documentation made available by the manufacturer, where it will be possible to identify new features that may pose threats to the company. It will also be possible to keep the application up-to-date, avoiding vulnerabilities that have already been addressed but that made the environment vulnerable due to the absence of the patch.

Threat Modeling Application

Threat modeling application consisted of executing the steps explained in the previous section and threats present in ISO and NIST were considered using threat modeling methods.

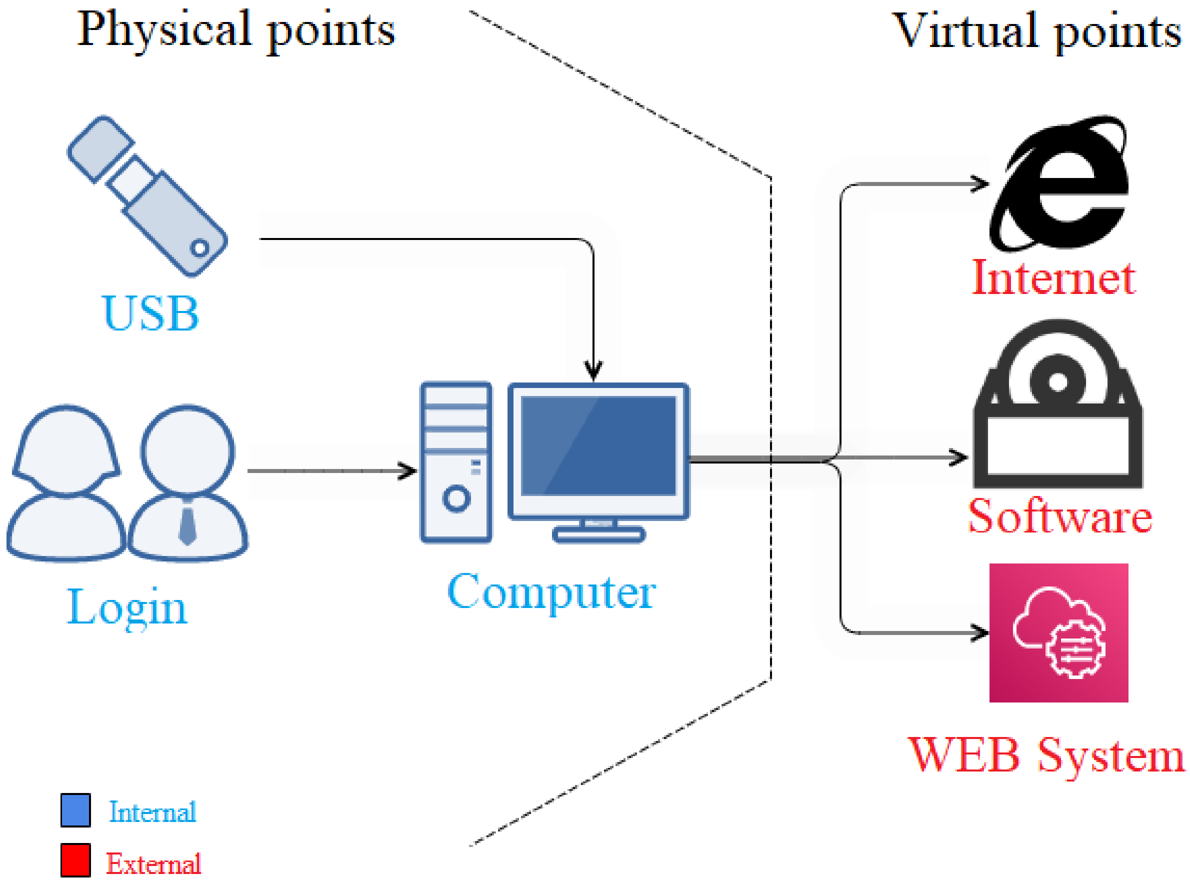
4.1 Identify Environment or Asset

Initially, it was necessary to verify the processes that are present in the environment, for a better understanding of the possible threats. The process points were divided between:

- Virtual points: which will present threats related to the native applications and functionalities of the Operational System.
- Physical points, where threats that can be exploited due to exposure of the computer to a physical environment will be presented, such as, for example, exploitation through a USB drive or alteration in the BIOS.
- Internal points, which are points presented by the company's own environment, without external influence.
- External points, where points of threats that come from an external environment, unrelated to the internal business environment, will be presented.

The Computer and its Operating System, without the influence of other external factors that can be analyzed individually to check for other vulnerabilities, have the following native processes, as shown in Figure 5:

Figure 5: environment diagram



Source: Search result

4.1.1 Identify Technologies Adopted

It was necessary to verify the environment, in the case of this article, the Windows operating environment. For the survey of threats, the trivial login mode was considered, using username and password, for a better understanding of the suggestions that are made as solutions to mitigate the threats found.

4.1.2 Identify System Processes

The processes mapped by the environment that present potential threats are:

- Login on the physical computer.
- Use of external hardware for recording files.
- Physical unprotection of the hard disk content.
- Unprotection of the asset against virtual threats.
- Protection against loss of information contained in the computer.
- Disclosure of information to external entities.

4.2 Identify Security Threats

Based on the processes mapped by the environment that may present threats, using the STRIDE threat modeling by element, it was possible to identify the following threats:

01. Access to sites or systems not authorized by the company.
02. Improper access to the device using an external or third-party account.
03. Changing information on the corporate network.
04. Sharing enterprise login.
05. Disclosure or loss of business content.
06. Lack of physical protection for HD content.
07. Program installation that overloads the system.
08. Installation of programs not authorized by the company.
09. Program installation that overloads the enterprise network.
10. Loss of business information in event of disasters.
11. Outdated programs.
12. Asset protection against virtual threats.
13. Use of personal login in company programs.
14. Use of USB drive to record enterprise files.

Table 3: application of the STRIDE per element.

Windows						
STRIDE per element	**Spoofing**	**Tampering**	**Repudiation**	**Information Disclosure**	**Denial of Service**	**Elevation of Privilege**
External Entity:	Access to the device using an external or third-party account;		Access to websites or systems not authorized by the company;	Access to websites or systems not authorized by the company;		
			Use of personal login in company programs;	Use of personal login in company programs;		
Internal Entity:		Outdated programs;	Sharing enterprise login;	Disclosure or loss of business content;		
Physical:		Lack of physical protection for HD content;		Use of USB drive to record enterprise files;		
				Loss of business information in the event of disasters;		
Virtual:		Asset protection,			Program installation	Program installation

		against virtual threats;			that overloads the enterprise network.	not authorized by the company;
		Changing information on the enterprise network;			Program installation that overloads the system.	

Source: Search result.

4.3 Analyze security threats

To be able to assess threats, they need to be analyzed and classified correctly. For the classification of each threat, the DREAD method was used, as shown in Table 4:

Table 4:analysis of security threats using the DREAD method.

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability
01. Access to sites or systems not authorized by the company;	High	High	High	High	High
02. Improper access to the device using an external or third-party account;	High	Low	Low	Low	Low
03. Changing information on the corporate network;	High	High	Low	Medium	Low
04. Sharing enterprise login;	High	High	High	Low	High
05. Disclosure or loss of business content;	High	High	High	Medium	High
06. Lack of physical protection for HD content;	High	High	High	Low	High
07. Program installation that overloads the system;	Medium	Medium	Low	Low	Low
08. Program installation not authorized by the company;	High	High	High	Low	High
09. Program installation that overloads the enterprise network;	High	Low	Low	High	High
10. Loss of business information in the event of disasters;	Medium	Medium	Low	Low	Low
11. Outdated programs;	High	High	High	High	Medium
12. Asset protection against virtual threats;	High	High	High	High	High
13. Use of personal login in company programs;	Low	High	Low	High	Medium
14. Use of USB drive to record enterprise files.	High	High	High	High	High

Source: Search result.

4.4 Assess Security Threat

After each item found using DREAD, it was possible to assess the level of danger of each found, as shown in Table 5:

Table 5: DREAD score

	DREAD
01. Access to sites or systems not authorized by the company;	3
12. Asset protection against virtual threats;	3
14. Use of USB drive to record enterprise files.	3
05. Disclosure or loss of business content;	2,8
11. Outdated programs;	2,8
04. Sharing enterprise login;	2,6
06. Lack of physical protection for HD content;	2,6
08. Program installation not authorized by the company;	2,6
09. Program installation that overloads the enterprise network;	2,2
03. Changing information on the corporate network;	2
13. Use of personal login in company programs;	1,8
02. Improper access to the device using an external or third-party account;	1,4
07. Program installation that overloads the system;	1,4
10. Loss of business information in the event of disasters;	1,4

Source: Search result.

4.5 Treat Security Threat

After checking the threats presented by the system, it is necessary to prescribe a remediation plan for each threat found:

1. Access to sites or systems not authorized by the company.

• It is recommended to install a proxy on corporate computers and use a firewall to limit access to inappropriate sites and systems.

2. Improper access to the device using an external or third-party account.

• Domain login restrictions can be applied, thus preventing local accounts or accounts from other companies from being able to access the computer.

3. Changing information on the corporate network.

• Write restriction is suggested for most company professionals on network drivers or critical systems. You can restrict the reading and writing access of each professional according to their needs to perform their functions in the company.

4. Sharing enterprise login.

• It is recommended to use two-factor authentication and use system logs for login monitoring on all devices. This implementation may also prevent access to corporate e-mail via the WEB from being carried out without the user's knowledge and permission.

5. Disclosure or loss of business content.

• It is recommended to use software to concentrate business files created by professionals, a program for Electronic Document Management for example, thus preventing important information from being saved only locally on your computer.

6. Lack of physical protection for HD content.

• It is suggested to use encryption programs, for instance, the Windows solution for encryption, to prevent information from being accessed by third parties. This program can also prevent access to the equipment's BIOS, making data access difficult.

7. Program installation that overloads the system.

• Restriction of software installation is recommended, Windows User Account Control can help with this threat, making an administrator account necessary for installing programs.

8. Program installation not authorized by the company.

• Restriction of software installation is recommended, Windows User Account Control can help with this threat, making an administrator account necessary for installing programs.

9. Program installation that overloads the enterprise network.

• Restriction of software installation is recommended, Windows User Account Control can help with this threat, making an administrator account necessary for installing programs.

10. Loss of business information in event of disasters.

• It is recommended to use software to concentrate business files created by professionals, a program for Electronic Document Management for example, thus preventing important information from being saved only locally on your computer.

11. Outdated programs.

• It is necessary to verify and apply the update for the Operating System. This item can be difficult because programs depend on tests and validation before being updated. In case of incompatibility, the Operating System may malfunction or present new threats due to incompatibility with other programs.

12. Asset protection against virtual threats.

• It is suggested to use an antivirus program to protect the Operating System, one can consider using the Operating System's own antivirus, in the case of Windows, but an antivirus with more protection functions is recommended.

13. Use of personal login in company programs.

• Restriction can be applied to domain login, thus preventing local accounts or accounts from other companies from being able to access the computer. For access to other programs, it is recommended that a block be created, preventing the computer from being able to access other programs using personal or other company logins.

14. Use of USB drive to record enterprise files.

- To block file transmission, you must use a configurable rule on the computer to block the USB for reading and writing, as well as blocking data transmission via Bluetooth.

4.6 Monitor the Adopted Solution

After remediation of the threats faced, the proposed system can be used to monitor, control and store information about software updates. Tests, validations and evidence will be reported in a future article, in addition to this article.

Conclusion

This research identified threats in an operating system using the STRIDE and DREAD methods, and ISO and NIST Standards. There were 14 types of threats found in an operating system that can be properly identified and mitigated using the threat modeling method. Among the 14 threats identified, 10 have a score above 2, presenting greater risk and it is recommended to verify the indicated points according to their remediation.

It is noted that a systematic approach to control, identification and correction of threats found can collaborate with enterprise risk management, thus helping to verify new versions and homologation before being put into production.

Standardization and use of a single image for all company devices can help mitigate threats, making it necessary for adjustments to be made only once and replicated to all other computers. The proposed system for monitoring new versions will help control the versions available by the manufacturer. Together with the application of threat modeling, it will be able to help, and remedy presented vulnerabilities.

The proposed system has alerts for a customizable period aimed at the continuous improvement of the product, changing the verification from reactive and becoming a controlled verification, as well as triggers to alert managers and the security team, highlighting possible threats in real-time. The system has a history of updates, allowing the analysis of changes in the system and the individual approval process, allowing the customization of each task, including attachments necessary for the execution of the task. There is also the possibility of using the system result for compliance sampling in audits.

For development of future research, the development of a system to control, identify and apply new updates automatically can facilitate the process of verifying threats and carrying out risk management.

As future work, the complete development of the system, tests and internal and external validations must be carried out to verify the maturity and effectiveness of the proposed system.

As future benefits, we can mention the possibility of involving other areas for the application of the threat modeling method in other devices.

References

Agência Brasil. Home office foi adotado por 46% das empresas durante a pandemia. 2020. available at: https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia. Access on 05/07/22.

Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). *Cyber threat modeling: Survey, assessment, and representative framework*. MITRE CORP MCLEAN VA MCLEAN.

Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 361-380. ISO/IEC. ISO/IEC 27001: Information security management systems - Overview and vocabulary, 2013, available at: https://www. abntcatalogo.com.br/ Access on: 01/09/2021

ISO/IEC. ISO/IEC 27002: code of practice for information security management, 2013, available at: https://www.abntcatalogo.com.br/ Access on: 01/09/2021

ISO/IEC. ISO/IEC 27005: Information security risk management, 2019, available at: https://www.abntcatalogo.com.br/ Access on: 01/09/2021

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017, September). STRIDE-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)* (pp. 1-6). IEEE.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

MITRE CVE SEARCH LIST, available at: https://cve.mitre.org/cve/search_cve_list.html acessado em 14/04/2022

NIST 800-30 - Guide for Conducting Risk Assessments, 2012, available at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final Access on 14/04/2022

Seifert, D., & Reza, H. (2016). A security analysis of cyber-physical systems architecture for healthcare. *Computers*, *5*(4), 27.

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat* *modeling: a summary of available methods*. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.

UcedaVelez, T., & Morana, M. M. (2015). *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons.

Xiong, W., & Lagerström, R. (2019). Threat modeling–A systematic literature review. *Computers & security*, *84*, 53-69.

Yokoyama, R., & Arima, C. H. (2022). Análise textual e bibliométrica sobre modelagem de ameaça Textual and bibliometric analysis on threat modeling. *Brazilian Journal of Development*, *8*(1), 7678-7690.

Yokoyama R.; Arima C.H. (2022) Modelagem de ameaça, análise de risco e suas aplicações na literatura. *International Journal of Development Research*, 12, (04), 55049-55055.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*, *9*, 29775-29818.

Submetido em: 17.03.2023
Aceito em: 18.04.2023