Addressing Intentional Threats Using Risk Assessment

The Case of Ransomware and Eavesdropping

Disponibile anche in Italiano
www.isaca.org/currentissue

Cyberspace must be considered a hostile environment. Although it has enormous potential, threats are always present, even in the most protected virtual worlds or within home networks. One very insidious threat is ransomware. Ransomware is not satisfied with eavesdropping, which is a serious threat in itself; ransomware inflicts the additional damage of making data unusable, with the tenuous hope of recovery after paying the ransom. Many share the opinion that it is best not to pay, ever. When the risk of a ransomware attack cannot be avoided, action must be taken to ensure that the impact is manageable. Risk assessment can be used as a tool to deal with the most representative classes of intentional threats: ransomware and eavesdropping.

Risk Assessment

When navigating in cyberspace, there must be constant awareness of the risk involved. The risk is not necessarily related to what one does in cyberspace. It is related to what others are doing without the knowledge of users who have devices connected to the Internet. As the number of connected devices grows, the likelihood that illegal activities can cause harm, whether directly or through engagement with others, increases. The damage can go beyond an enterprise's sustainable risk capacity and, therefore, must be avoided to the extent possible.

A low level of risk means that the impact of a harmful event—the likelihood of its occurrence and the extent of the impact if it does occur—is kept as low as possible. In risk analysis, the approach must be holistic, evaluating the internal factors and the repercussions outside the enterprise resulting from mistakes or ineffective actions. It is hard to tell whether one security standard or framework is better than another, but a number of considerations can serve as a baseline for improving a defense system.

A risk event is something that happens at a specific place or time (possibility). A threat is anything (real) that is capable of acting against an asset in a manner that can cause harm. With respect to threats, it is important to:

LUIGI SBRIZ | CISM, CRISC, CDPSE, ISO/IEC 27001 LA, ITIL V4, NIST CSF, UNI 11697:2017 DPO

Is a lead auditor and a senior consultant on risk management, cybersecurity and privacy issues and has been the risk monitoring manager at a multinational automotive company for more than seven years. Previously, he was head of information and communications technology operations and resources in the Asia and Pacific Countries (APAC) region (China, Japan and Malaysia). Before that, he was the worldwide information security officer for more than seven years. He developed an original methodology for internal risk monitoring, merging an operational risk analysis with a consequent risk assessment driven by the maturity level of the controls. He also designed a cybermonitoring tool and system integrating a risk monitoring, maturity model with internal audit. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn at *https://www.linkedin.com/in/luigisbriz* or *http://sbriz.tel*.

- Maintain awareness of the threats that exist and understand their potential severity so that appropriate decisions can be made.
- Know the potential adversaries and their motivations so as to effectively counter them.
- Balance the costs and benefits of defense solutions when making data protection decisions.
- Avoid becoming passive and falling prey to decision-making inertia.
- Constantly evaluate, with pragmatism, the enterprise's defense capacity, avoiding unnecessary risk, acting in compliance with the rules and, if attacked, reacting to offenses.

It is also important to remember:

- Not to focus on the technological component alone, but to consider how to organize a correct defense perimeter, balanced by business objectives.
- Not to automatically accept assurances that everything is in place, and not to assume an unlikely event will never happen.

Although it is simple to create risk analyses, perform cost and benefit assessments, search for known vulnerabilities, plan installations, or acquire hardware and software, it is more difficult to properly design or configure systems according to the real security required by business needs or to predict threat agents' moves. This means accepting the probability that, sooner or later, an attack will be successful. Of course, it is impossible to know with certainty either the time of the attack or the extent of the damage.

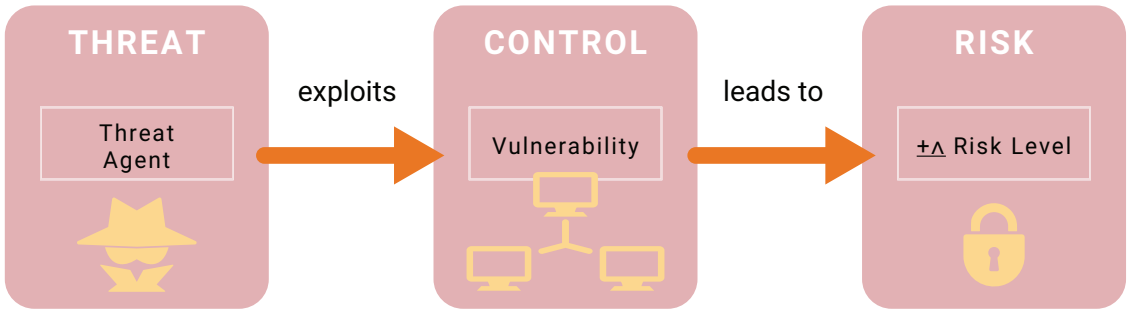
These two uncertainties are not the only constraints in building an information protection system.

The Intelligence of the Threat Agent

Natural threats or unintentional ones are quite predictable and, therefore, present the possibility of effective solutions. However, more dangerous are intentional threats conducted for fraudulent purposes—that is, threats that exploit vulnerabilities to acquire an illicit benefit with harm to others. This type of threat involves a threat agent (e.g., a hacker, who could be a person, a criminal enterprise or an artificial intelligence [AI] program) that consciously works to achieve a malicious end (**figure 1**). The agent's ability to exploit a vulnerability grows in proportion to the resources it has available. These resources include technical skills, technological means, will to act, predisposition to take risk, ability to improvise, knowledge about the target entity, and exogenous factors such as the time available, the attacker's culture, the attacker's malicious intent, the defender's inadequacy or, simply, luck.

The attacked entity defends itself with contrast controls,[1] such as searches for anomalous presences or the identification of internal weaknesses following a risk analysis, but it is reasonable to expect these defenses to have limited effectiveness. Vulnerability assessments[2] and penetration testing[3] are useful, but they operate on known vulnerabilities and attack techniques. Monitoring the severity of threats over time, testing the effectiveness of controls, and maintaining a realistic list of risk factors supplies information that is necessary, but not sufficient to

FIGURE 1
Risk Related to the Threat



provide an exhaustive picture of the scenario. There is always the possibility that the attacker is aware of an unidentified vulnerability.

How the Threat Advances

During an intentional attack, the threat agent is typically patient and often uses the algorithmic technique of backtracking[4] to achieve its goals, assuming the hacker does not already know how the targeted system is built. The hacker usually has extensive knowledge of the different types of vulnerabilities and makes targeted use of them based on the characteristics of the attack front. When a hacker begins the action of penetrating the protected perimeter of an enterprise, all possible attack options are available, but as the attack progresses, room for maneuvering is reduced (**figure 2**).

Once the hacker is inside the perimeter, the functional peculiarities of the environments, combined with the different defense methods, limit both the ability to access new resources more suitable for the offense and the ability to directly govern the resources previously introduced. In exploring the environment to be attacked, the hacker requires two distinct elements:

1. Appropriate knowledge of the vulnerabilities present
2. Appropriate means to exploit the vulnerabilities discovered

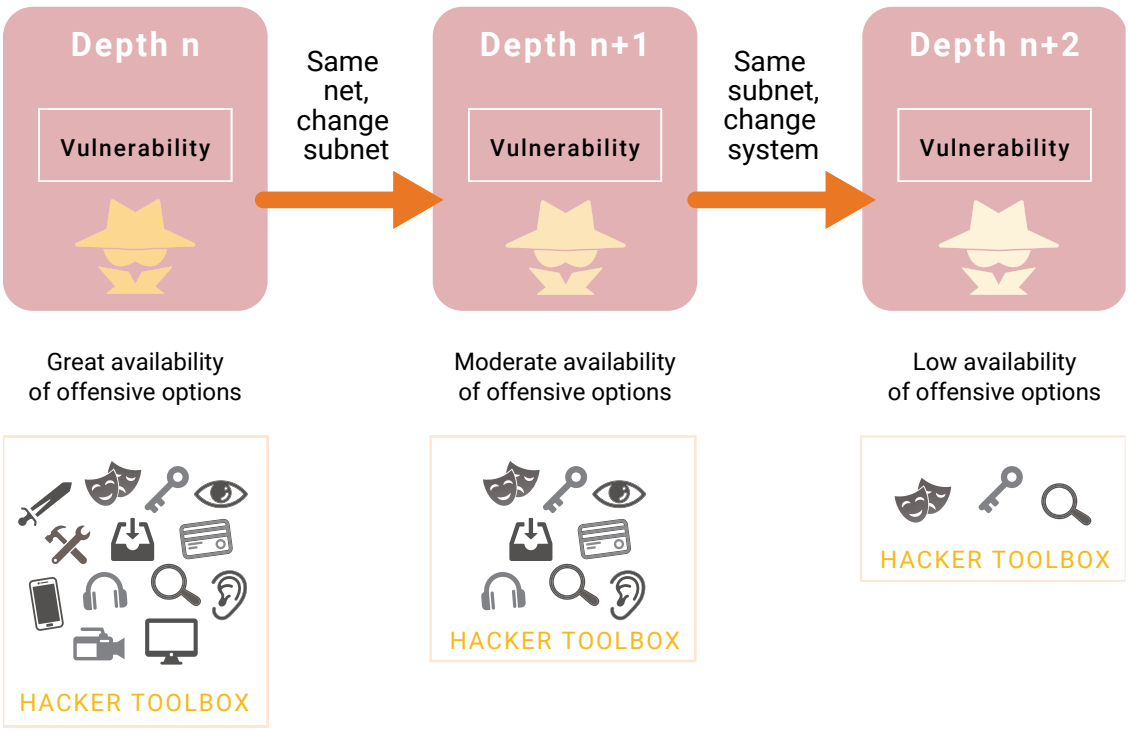
Mapping of the environment is achieved by exploring it, but this does not involve zero risk for attackers because they could be intercepted during the act.

The attack techniques are generally based on software that can identify and exploit vulnerabilities and, consequently, either act autonomously (with logic wired in) or be controlled directly by the hacker. Direct control is much more powerful, but also much riskier because it requires an open communication channel that could be intercepted. When the search for vulnerabilities leads to no further possibilities to advance along a path, the hacker returns to the previous environment and tries another path not yet explored. The search can be exhaustive and continues until predefined conditions are reached (i.e., the resource sought is found or the research is abandoned).

There is a clear need to act at this stage to weaken the effectiveness of the attacker's actions, both by

FIGURE 2

Resources Available to the Hacker During the Attack



hindering the advance and by reducing the attacker's ability to communicate backward to gain new strength. The objective is to prevent the hacker from accessing new resources to improve the consolidation of its position. The goal is not technological confrontation, but loss of the hacker's competitive advantage represented by its ability to govern the target's vulnerabilities. If those vulnerabilities cannot be eliminated, the best option is to prevent the attacker from exploiting them easily or in full.

How to Counter the Threat

One way to counter a threat is to use the divide and conquer[5] method to reduce the power of the attack. In general, the method is used to counter the attacker's backtracking by integrating false resources into the environment to increase the complexity of the mapping. Increasing the number of search nodes with artificial nodes increases the search time, and using fake nodes with known vulnerabilities increases the visibility of the intrusion action. In other words, the divide and conquer method increases the number of nodes in the search. False nodes are placed strictly under monitoring by intrusion detection system (IDS). This method acts by artificially complicating the defended environment to confuse the advancing agent—that is, a path of passive and active obstacles is created with the aim of reducing the capacity for offense.

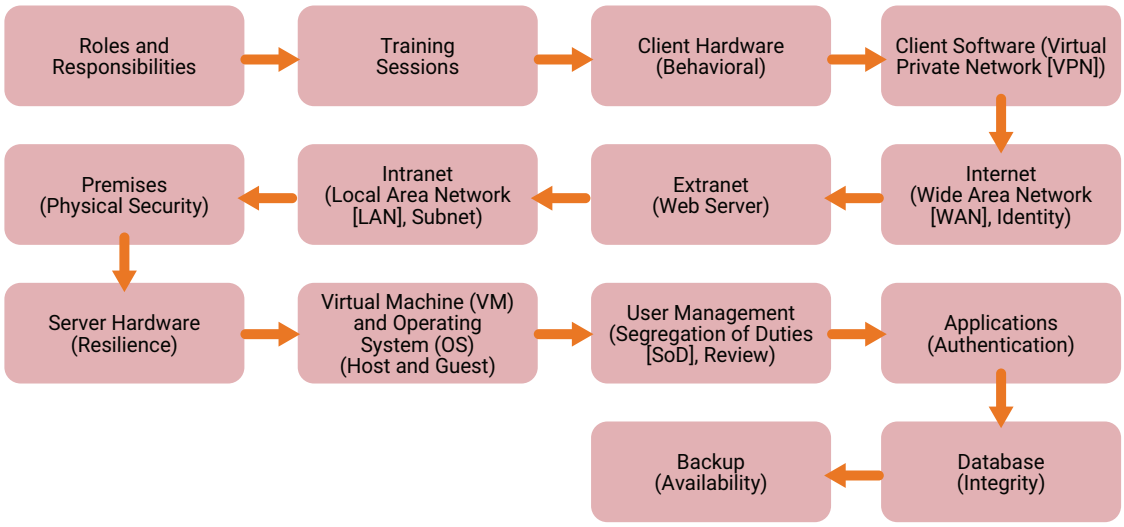
An obstacle is passive if it places barriers that must be bypassed or destroyed. This category includes mainly components in the field of networking, such as segregated subnets, traffic filters and closed doors. Resource authentication systems and encryption systems on communication channels and data are also in this category. These systems do not operate on specific malware, but act against entire classes of potential attacks or in response to control requests from the main data protection frameworks.

An obstacle is active when it reacts to the malware's presence in some way; an alarm warns if abnormal activity is detected (e.g., security information and event management [SIEM], IDS), but blocking (e.g., intrusion prevention system [IPS]) or elimination (antivirus) are also possible. The creation of false resources (e.g., a database with low protection or a firewall with a vulnerability), especially if connected to an IDS or IPS, weakens the hacker by forcing it to focus attention on false targets. For effective counteraction, these resources are aimed at specific threats.

This approach can be classified as a defense-in-depth (DiD) technique (**figure 3**), which consists of dividing an environment into different layers and then further dividing them into homogeneous areas according to predefined criteria justified by the risk analysis. It is interesting to note that this is not a pure technological defense, as the first lines of defense are organizational. The first step in defense-in-depth—awareness of threats and their consequences—is achieved through a solid organizational structure that defines and communicates roles and responsibilities up to the point of operation. Everyone in the enterprise must have clear expectations of who should do what and why.

FIGURE 3

Elements of DiD



LOOKING FOR MORE?

- Read *Defending Data Smartly. www.isaca.org/defending-data-smartly*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Human behavior in connection with the use of physical devices and installed software plays a significant role in data protection. Security measures require that users' identities are known. The enterprise network's first line of defense relies on the extranet, while the internal network must be structured into homogeneous subnets as defined by the security classification. The most relevant technical principles for systems and devices are defined by measures such as:

- The servers and network equipment must be physically protected, and fault resilience must be guaranteed.
- Virtual machines should be used to disable all unused services, because they guarantee a safe and fast restart in the event of an incident.
- Operating systems and applications must be accessible only to authorized users.
- Databases must be on dedicated systems, separate from the web servers, and software must be tested.
- Backups must reside on the same subnet as databases; they should be maintained offline without remote access (control on local area network [LAN]).
- Every decision made in the design of the data protection system should be justified based on the risk analysis.

How to Reduce the Impact

Regardless of the effectiveness of a defense system, it is not possible to eliminate all vulnerabilities, which means that the probability of a risk event occurring cannot be reduced to zero. Consequently, there will be an impact; but the goal is to reduce that impact to one that is within acceptable limits. The effort should be made to ensure that the minimum impact is determined in the design phase, and that the implementation is checked to ensure that it complies with the risk analysis at all times.

The divide-and-conquer technique, already used to divide the processes of the protection system, is also fundamental in reducing the data or services exposed to a possible attack. Applying this technique on a computer system means separating the data querying, data modification and command execution operations and reviewing the user interface and data connections with respect to a logical division of the database, depending on the identified risk factors.

Virtual machines should be used to disable all unused services, because they guarantee a safe and fast restart in the event of an incident.

The logic of this technique involves fragmenting the data set and management applications on multiple virtual machines, each dedicated to a specific service. Thus, there will be a web server without data, master files on one database server, reporting data on another database server and so on. Each server contains only the minimum number of resources necessary to carry out a complete service.

Using this process, the final impact of an attack is minimized because the origin system has become a set of various minor environments, the sum of which, in terms of functionality and data, can replicate the origin system. If the system is well designed, it is highly unlikely that all machines will be compromised at the same time. This means reviewing the individual features is a function of risk containment. For example, the module for displaying and updating a master file could be revised in two separate functions: one for displaying data, which acts directly on the master file tables: and another for writing to a buffer, which is analyzed by a validation process before transferring a change to the registry.

The same database could be redesigned on different partitions, decoupled and synchronized by system processes. Then, in the event that a partition is compromised, the loss will never be as serious as the loss of the entire database. The production maintenance activity must take place on dedicated connections, be constantly monitored, and never be open simultaneously on production and backup environments. The division of each system into various components that can be easily replaced or adjusted creates resilience in the face of an incident. This goes a long way toward systematically reducing the impact of an adverse event.

Eavesdropping and Ransomware

If an attack is successful, DiD is achieved by subdividing the monolithic system into layers and divisions according to criteria based on the risk analysis. Each countermeasure is evaluated

holistically to understand the benefits and contraindications on an enterprisewide level. This approach is designed to prevent and manage incidents that compromise the confidentiality and availability of information. Two types of malware that are particularly insidious and share the same methods of intrusion but differ in purpose and consequences are eavesdropping, which sneaks inside systems to collect confidential information, and ransomware, which renders a system unusable and promises a hypothetical remedy in exchange for money.

Eavesdropping is a parasite, an unwanted intruder that lives off the host, while ransomware is a poison for which an unguaranteed antidote is needed. They both have the same goal of penetrating the host's defenses, and they use the same means to carry out the attack in depth, but they behave differently. Ransomware acts immediately, renders part or all of the compromised area unusable and ends with a monetary demand. Eavesdropping is installed secretly, accumulates information for as long as possible and does not manifest either the activity or the purpose.

In the data protection system, it is necessary to force the hacker to continually readjust and refocus its attack techniques.

Ransomware does evident damage, while eavesdropping causes persistent but hidden damage and, as a last step, can open the door to ransomware. Collaboration between the two types of malware is the worst-case scenario because data confidentiality may have already been lost, and the organization then pays to restore the availability of data that have been deprived of their intrinsic value. The existence of these two malware types is the primary reason for evaluating all the risk factors associated with the loss of confidentiality and the availability of information assets.

The DiD method is effective in ensuring a low probability of success for the mentioned malwares. If malware has the ability to access the system, the presence of watertight compartments between parts of the system can intercept it before it accesses vital functions. Once eavesdropping malware has been detected in the system, identification of the information heard illegally is required to understand the severity of the breach. For ransomware, the loss must be accepted and justified by the fact that the environment is designed with low impact. In both cases, it is a good idea to trace the attacker and the techniques used, preferably with the support of the government bodies in charge of countering cybercrime, and holistically analyze the entire protection system and the reasons for its failure. The action of public authorities takes place during restoration efforts, allowing more effective tracking of criminal activity.

A final issue that deserves consideration is whether it is necessary to protect an environment connected to the Internet but without relevant or sensitive data. To maintain a dialogue with its malware, the attacker needs a data return buffer, which allows the malware to store data without being hindered by firewalls and allows the hacker to recover the data without risk. A weakly protected but legitimate site is an excellent candidate for exchanging data with malware. The hacker accesses the site, collects all the data with impunity, pours the data into the deep web, and leaves the unprotected site with the burden of justifying its participation. Therefore, the rule is to always protect. Regardless of the value attributed to the individual asset, a holistic risk analysis must be performed to define the right measures and avoid creating added value for bad actors due to a lack of attention.

Conclusion

In the fight against intentional attacks (e.g., ransomware and eavesdropping), a holistic risk assessment approach that balances the interests of the enterprise with the identified protection methods should be completed. The outermost layer of the defense system is the organizational front and it ensures the alignment of protection methods with business objectives. Then, penetrating the internal layers, are network mechanisms aimed at decreasing the probability of an attack's success. In the deeper layers—those related to the operating and application system—the priority is reducing the impact.

In addition to internal defense methods, there are also possible external aids from two directions: laws on a security baseline required of organizations and insignificant legal consequences for the hacker.

They are very useful levels of defense, but they are insufficient because an organization must operate on the basis of its risk assessment and not of satisfaction with minimum requirements imposed independently of the business objectives.

Hackers adopt technology as a means of forcing systems to compromise. Countering with technology alone is reactionary. The hacker moves to exploit a vulnerability that it knows but its target is unaware of; only after the hacker makes a move does the target detect the problem and respond. In the game of chess, making a reactionary move is a disadvantage. Thus, in the data protection system, it is necessary to force the hacker to continually readjust and refocus its attack techniques. In place of a single complex system, it is preferable to have multiple specialized subsystems with the right redundancy to ensure resilience and maintain constant alignment with the risk response. It is also important to avoid paying ransoms as it is a detriment to everyone to give attackers the expectation of receiving compensation for having performed illegal actions.

Endnotes

1 Sbriz, L.; "Capability Maturity Model and Risk Register Integration: The Right Approach to Enterprise Governance," *ISACA® Journal,* vol. 1, 2022, *https://www.isaca.org/archives*

2 US National Institute of Standards and Technology (NIST), "Vulnerability Assessment," Computer Security Resource Center, USA, *https://csrc.nist.gov/glossary/term/vulnerability_assessment*

3 US National Institute of Standards and Technology (NIST), "Penetration Testing," Computer Security Resource Center, USA, *https://csrc.nist.gov/glossary/term/penetration_testing*

4 Golomb, S.; L. D. Baumert; "Backtrack Programming," *Journal of ACM*, vol. 12, iss. 4, 1 October 1965, p. 516–524, *https://doi.org/10.1145/321296.321300*

5 Knuth, D. E.; T*he Art of Computer Programming: Volume 3, Sorting and Searching, 2nd Edition,* Addison-Wesley, USA, 1998