SECURITY GUIDEBOOK

RIHAM AHAMED ABDUL RAHEEM
HND COMPUTING IDM

Contents

Introduction to Security

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats.

This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Security is critical for enterprises and organizations of all sizes and in all industries.

Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat.

When you create systems that store and retrieve data, it is important to protect the data from unauthorized use, disclosure, modification or destruction.

Ensuring that users have the proper authority to see the data, load new data, or update existing data is an important aspect of application development. Do all users need the same level of access to the data and to the functions provided by your applications?

Are there subsets of users that need access to privileged functions?

Are some documents restricted to certain classes of users? The answers to questions like these help provide the basis for the security requirements for your application.

Assets, Risks & Threats

An asset is any object or piece of information that has a monetary value, and is something that we're always trying to protect.

A risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting vulnerability.

Any form or way that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset is called a threat.

Risk Analysis

Risk analysis is the review of the risks associated with a particular event or action. It is applied to projects, information technology, security issues and any action where risks may be analyzed on a quantitative and qualitative basis. Risk analysis is a component of risk management.

The risk management process involves a few key steps. First, potential threats are identified. For example, risks are associated with individuals using a computer either incorrectly or inappropriately, which creates security risks.

Risks are also related to projects that are not completed in a timely manner, resulting in significant costs.

Next, quantitative and/or qualitative risk analysis is applied to study identified risks.

Quantitative risk analysis measures expected risk probability to forecast estimated financial losses from potential risks. Qualitative risk analysis does not use numbers but reviews threats, and determines and establishes risk mitigation methods and solutions.

A contingency plan may be used during risk analysis. If a risk is presented, contingency plans help minimize damage.

	A	B	C	D
1	**Area**	**Goal**	**Risk Level**	**Situation**
2	Possible Areas of Risk		Very low to very high.	Where your startup stands today.
3	*Product/Market Fit (B2B)*	You're building something people want.		
4	Product/Market Fit (B2C)		Medium	You have some early unaffiliated users, but user acquisition economics aren't great.
5	Product/Market Fit (Churn)		Very High	Engagement is very low, churn is very high.
6	Product Quality	You can build a great, high-quality product.	Very High	You have a prototype, and it's very mediocre.
7	Team	You have a great team in relevant areas.	Low	...your full-time team covers most of those areas.
8	Recruiting	You can grow your team.	Medium	You have prior recruiting and management experience.
9	Sales	Your team can sell the product.	High	You've done sales, but not much or not recently or not of the same flavor that you'll need for your company.
10	Market	You can make enough money to become a huge company.	Medium	You found a Gartner report that gives an estimate of market size.
11	Funding	You have enough capital to reach your milestones.	Medium	You are self-funded with a decent likelihood of future funds or more than 35% of your time generating funds.
12	Short-Term Competition	You're differentiated from existing players.	Low	There are very few competitors, and strong differentiation between you and them.
13	Long-Term Competition	You have defensibility.	Very High	You're not the first mover and you don't have a real competitive advantage.

Figure 1:Startup Risks

Physical Security

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution.

This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

Physical security is often overlooked -- and its importance underestimated in favor of more technical threats such as hacking and malware.

However, breaches of physical security can be carried out with brute force and little or no technical knowledge on the part of an attacker.

Physical security has three important components: access control, surveillance and testing.

Obstacles should be placed in the way of potential attackers and physical sites should be hardened against accidents, attacks or environmental disasters. Such hardening measures include fencing, locks, access control cards, biometric access control systems and fire suppression systems.

Second, physical locations should be monitored using surveillance cameras and notification systems, such as intrusion detection sensors, heat sensors and smoke detectors.

Third, disaster recovery policies and procedures should be tested on a regular basis to ensure safety and to reduce the time it takes to recover from disruptive man-made or natural disasters.

The below figure illustrates effectively what physical security is based on.

Figure 2: Physical Security

Virtual Security

Any compromise to integrity, authentication and availability makes a software unsecure. Software systems can be attacked to steal information, monitor content, introduce vulnerabilities and damage the behavior of software. Malware can cause DoS (denial of service) or crash the system itself.

Buffer overflow, stack overflow, command injection and SQL injections are the most common attacks on software.

Buffer and stack overflow attacks overwrite the contents of the heap or stack respectively by writing extra bytes.

Command injection can be achieved on the software code when system commands are used predominantly.

New system commands are appended to existing commands by the malicious attack. Sometimes system command may stop services and cause DoS.

SQL injections use malicious SQL code to retrieve or modify important information from database servers. SQL injections can be used to bypass login credentials.

Sometimes SQL injections fetch important information from a database or delete all important data from a database.

The only way to avoid such attacks is to practice good programming techniques. System-level security can be provided using better firewalls. Using intrusion detection and prevention can also aid in stopping attackers from easy access to the system.

Conventions that must be followed within Ascom

Establishing strong passwords

Implementing strong passwords is the easiest thing you can do to strengthen your security. Definitely avoid using any personal data (such as your birthdate), common words spelled backwards and sequences of characters or numbers, or those that are close together on the keyboard.

The industry standard for changing passwords is "every 90 days," but if the data is highly sensitive then much more frequent password changing is acceptable.

Use a strong firewall

In order to have a properly protected network, firewalls are compulsory A firewall protects a network by controlling internet traffic coming into and flowing out of your business. Both software and hardware firewalls can be used. Using a hardware firewall is a significant necessity in the industry.

Install antivirus protection

Antivirus and anti-malware software are essentials in your arsenal of online security weapons, as well.

These software help combat the viruses, spyware or malware that may make it through the previous stages of security defense.

Automatically updating virus definitions and the anti-virus database is highly recommended.

At industrial level Malware Bytes, Kaspersky and AVG will keep the systems safe and sound.

Update your programs regularly

Making sure your computer is "properly patched and updated" is a necessary step towards being fully protected; there's little point in installing all this great software if you're not going to maintain it right.

Secure laptops & mobile phones

Because of their portable nature, laptops are at a higher risk of being lost or stolen than average company desktops. It's important to take some extra steps to make certain your sensitive data is protected. So do mobile phones, as they are widely used and hold so much data in them.

One big solution is encrypting the device.

Encryption software changes the way information looks on the hard drive so that, without the correct password, it can't be read.

For mobile phones, encryption and password protection must be employed. Since the frequency and the likelihood for a mobile phone to get lost is high, remote swiping must also be implemented. This will allow a consumer of the mobile phone after undergoing authentication to completely wipe the data in the phone.

Backup regularly

Scheduling regular backups to an external hard drive, or in the cloud, is a painless way to ensure that all your data is stored safely.

The general rule of thumb for backups: servers should have a complete backup weekly, and incremental backups every night; personal computers should also be backed up completely every week, but you can do incremental backups every few days per your liking.

Train your staff

Regularly training your staff and giving them the necessary knowledge they need to know about security is one of the best ways to mitigate potential risks, as your staff are the biggest vulnerability to your company. They have permission and access rights, so if they do something wrong unintentionally and create an exploit, this will be a big loophole in UniCare's security.

Using demilitarized zone

The general idea is that you put your public faced servers in the "DMZ network" so that you can separate them from your private, trusted network.

The use case is that because your server has a public face, it can be remotely rooted. If that happens, and a malicious party gains access to your server, he should be isolated in the DMZ network and not have direct access to the private hosts (or to a database server for example that would be inside the private network and not on the DMZ).

So how do you do it? There are several ways, but the common way is by utilizing two firewalls (you can achieve the same result with one firewall and smart configuration, although hardware isolation is nicer).

Your main firewall is between internet and the server and the second firewall between the server and the private network. On this second firewall, all access from the server to the private network ideally would be forbidden. Iwould be a state full firewall so if you initiate a connection from the private network to the server it would work.

Implementing static IPs

A static IP address an Internet Protocol (IP) address number assigned to a network device by an administrator. A static IP is an alternative to dynamic IP assignment on Internet Protocol networks.

Most IP networks use dynamic addressing via Dynamic Host Configuration Protocol rather than static IP assignment because dynamic IP addresses are the most efficient for the service provider. Dynamic addressing is convenient because it's easy for administrators to set up.

- A static IP addresses best supports name resolution across wide area networks (WANs), enabling devices to be reliably reached by their assigned host names.
- Using static IP addresses on networks provides slightly better protection against network security problems than does DHCP address assignment.
- Some network devices do not support DHCP. Using static IP assignment for all devices on the network avoids potential IP address conflicts where DHCP might supply an address already assigned statically elsewhere.
- A static IP address provides geo-location that is more accurate than a dynamic IP address.
- Download and upload speeds are often faster with static IPs than with dynamic IPs.

References

Anon., 2016. *Techo Pedia.* [Online]
Available at: https://www.techopedia.com/definition/16522/risk-analysis
[Accessed 19 February 2021].

Anon., 2021. *Instiute of Forensics and ICT Security.* [Online]
Available at: https://www.forensicsinstitute.org/what-does-software-security-mean/
[Accessed 19 February 2021].

Anon., 2021. *Threat Analysis Group.* [Online]
Available at: https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/
[Accessed 19 February 2021].

Contributor, T., January 2017. *TechTarget.* [Online]
Available at: https://searchsecurity.techtarget.com/definition/security#:~:text=Security%2C%20in%20information%20technology%20(IT,software%20tools%20and%20IT%20services.
[Accessed 19 February 2021].