MUCO

Moravian Business College Olomouc

Introduction to the Issue of Security

Lukáš Pavlík, Ph.D.
Department of Informatics and Applied Mathematics
E-mail: lukas.pavlik@mvso.cz

The Goal of Course and Conditions of Exam

- The subject ICT Security and Data Protection ends with an exam.
- There is no credit before the exam.
- To pass the exam, it is necessary to pass at least 65 % of the test.

Definitions of 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.

The Concept of Information Security

- As computers and other digital devices have become essential to business and commerce, they have also increasingly become a target for attacks.

- In order for a company or an individual to use a computing device with confidence, they must first be assured that the device is not compromised in any way and that all communications will be secure.

The Base of Information Security - Confidentiality, Integrity, Availability

The Base of Information Security - Confidentiality

- When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone else should be disallowed from learning anything about its contents.
- This is the essence of confidentiality.
- For example, federal law requires that universities restrict access to private student information.
- The university must be sure that only those who are authorized have access to view the grade records.

The Base of Information Security - Integrity

- Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended.

- Just as a person with integrity means what he or she says and can be trusted to consistently represent the truth, information integrity means information truly represents its intended meaning.

- Information can lose its integrity through malicious intent, such as when someone who is not authorized makes a change to intentionally misrepresent something.

The Base of Information Security - Integrity

- An example of this would be when a hacker is hired to go into the university's system and change a grade.
- Integrity can also be lost unintentionally, such as when a computer power surge corrupts a file or someone authorized to make a change accidentally deletes a file or enters incorrect information.

The Base of Information Security - Availability

- Availability means that information can be accessed and modified by anyone authorized to do so in an appropriate timeframe.
- Depending on the type of information, *appropriate timeframe* can mean different things.
- For example, a stock trader needs information to be available immediately, while a sales person may be happy to get sales numbers for the day in a report the next morning.
- Companies such as Amazon.com will require their servers to be available twenty-four hours a day, seven days a week.
- Other companies may not suffer if their web servers are down for a few minutes once in a while.

Tools for Information Security

- In order to ensure the confidentiality, integrity, and availability of information, organizations can choose from a variety of tools.

- Each of these tools can be utilized as part of an overall information-security policy, which will be discussed in the next section.

Password Security

- So why is using just a simple user ID/password not considered a secure method of authentication?
- It turns out that this single-factor authentication is extremely easy to compromise.
- Good password policies must be put in place in order to ensure that passwords cannot be compromised.
- Below are some of the more common policies that organizations should put in place.

Password Security

- Require complex passwords.
- One reason passwords are compromised is that they can be easily guessed.
- A recent study found that the top three passwords people used in 2012 were *password*, *123456* and *12345678*.
- A password should not be simple, or a word that can be found in a dictionary.
- One of the first things a hacker will do is try to crack a password by testing every term in the dictionary!

Password Security

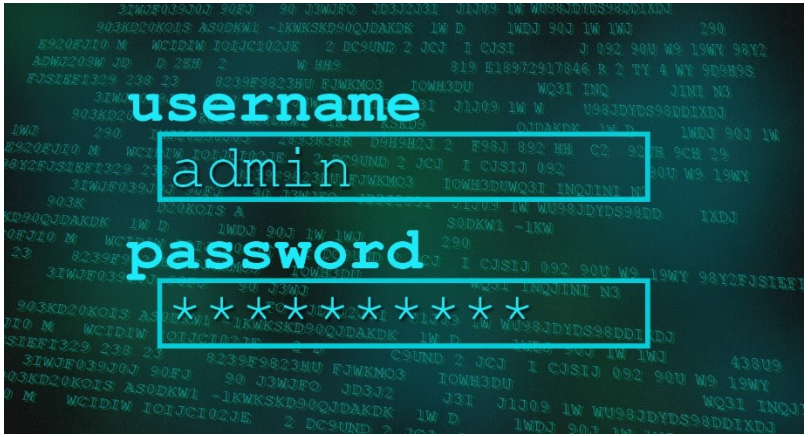
- Instead, a good password policy is one that requires the use of a minimum of eight characters, and at least one upper-case letter, one special character, and one number.
- Change passwords regularly.
- It is essential that users change their passwords on a regular basis.
- Users should change their passwords every sixty to ninety days, ensuring that any passwords that might have been stolen or guessed will not be able to be used against the company.

Password Security

- Train employees not to give away passwords.
- One of the primary methods that is used to steal passwords is to simply figure them out by asking the users or administrators.
- Pretexting occurs when an attacker calls a helpdesk or security administrator and pretends to be a particular authorized user having trouble logging in.
- Then, by providing some personal information about the authorized user, the attacker convinces the security person to reset the password and tell him what it is.
- Another way that employees may be tricked into giving away passwords is through e-mail phishing.

Password Security

- Phishing occurs when a user receives an e-mail that looks as if it is from a trusted source, such as their bank, or their employer.
- In the e-mail, the user is asked to click a link and log in to a website that mimics the genuine website and enter their ID and password, which are then captured by the attacker.



Backups

- Another essential tool for information security is a comprehensive backup plan for the entire organization.
- Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up.
- A good backup plan should consist of several components.

Backups

- A full understanding of the organizational information resources.
- What information does the organization actually have?
- Where is it stored?
- Some data may be stored on the organization's servers, other data on users' hard drives, some in the cloud, and some on third-party sites.
- An organization should make a full inventory of all of the information that needs to be backed up and determine the best way back it up.

Backups

- Regular backups of all data.
- The frequency of backups should be based on how important the data is to the company, combined with the ability of the company to replace any data that is lost.
- Critical data should be backed up daily, while less critical data could be backed up weekly.
- Offsite storage of backup data sets.

Backups

- Test of data restoration.
- On a regular basis, the backups should be put to the test by having some of the data restored.
- This will ensure that the process is working and will give the organization confidence in the backup plan.
- Besides these considerations, organizations should also examine their operations to determine what effect downtime would have on their business.
- If their information technology were to be unavailable for any sustained period of time, how would it impact the business?

Backups

- Additional concepts related to backup include the following:
- Universal Power Supply (UPS).
- A UPS is a device that provides battery backup to critical components of the system, allowing them to stay online longer and/or allowing the IT staff to shut them down using proper procedures in order to prevent the data loss that might occur from a power failure

Backups

- Alternate, or “hot” sites.
- Some organizations choose to have an alternate site where an exact replica of their critical data is always kept up to date.
- When the primary site goes down, the alternate site is immediately brought online so that little or no downtime is experienced.
- As information has become a strategic asset, a whole industry has sprung up around the technologies necessary for implementing a proper backup strategy.
- A company can contract with a service provider to back up all of their data or they can purchase large amounts of online storage space and do it themselves.
- Technologies such as storage area networks and archival systems are now used by most large businesses.

Firewalls

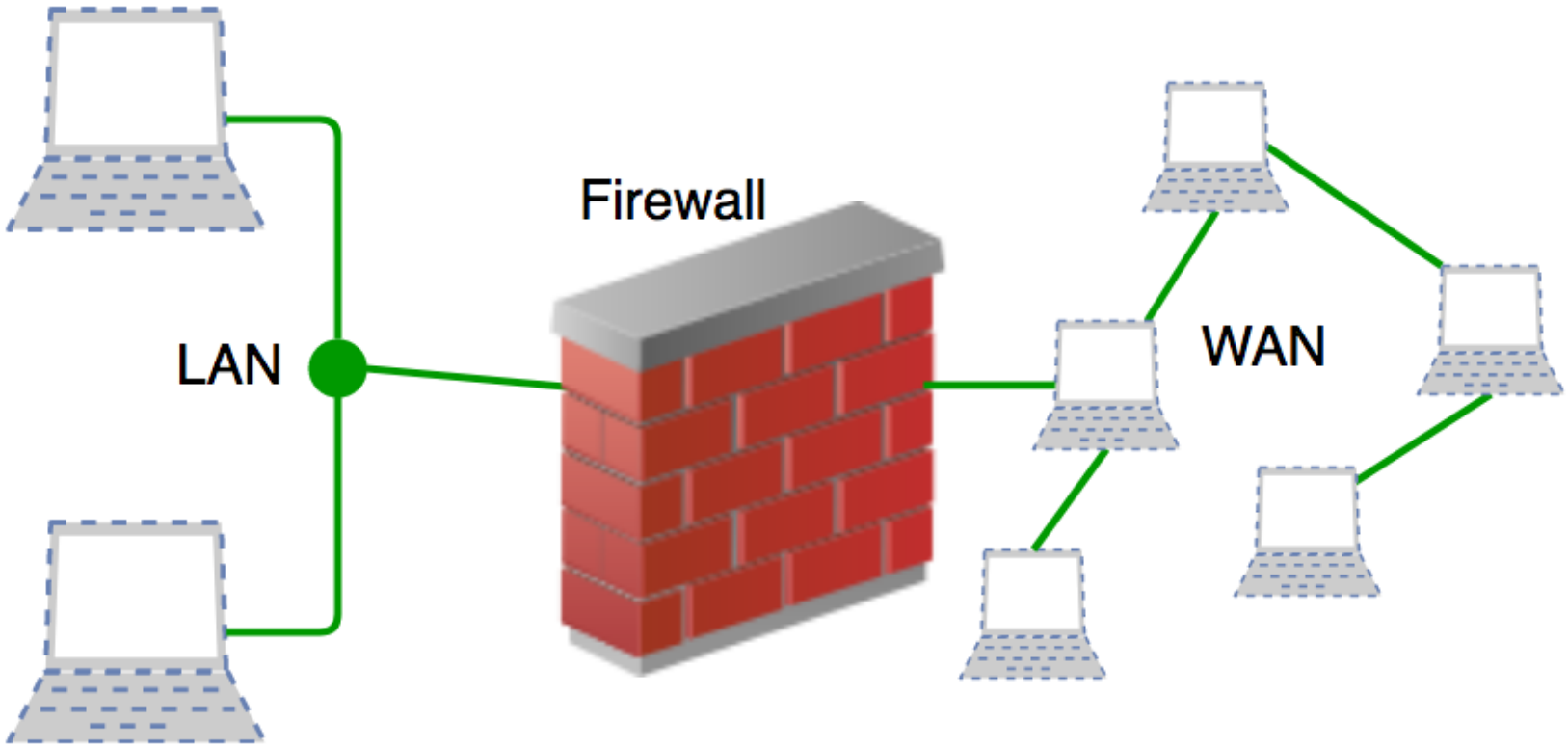
- Another method that an organization should use to increase security on its network is a firewall.
- A firewall can exist as hardware or software (or both).
- A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules.
- A software firewall runs on the operating system and intercepts packets as they arrive to a computer.
- A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria.
- A firewall may also be configured to restrict the flow of packets leaving the organization.
- This may be done to eliminate the possibility of employees watching YouTube videos or using Facebook from a company computer.

Firewalls

- Some organizations may choose to implement multiple firewalls as part of their network security configuration, creating one or more sections of their network that are partially secured.

- This segment of the network is referred to as a DMZ, borrowing the term *demilitarized zone* from the military, and it is where an organization may place resources that need broader access but still need to be secured.

Firewalls



Physical Security

- An organization can implement the best authentication scheme in the world, develop the best access control, and install firewalls and intrusion prevention, but its security cannot be complete without implementation of physical security.

- Physical security is the protection of the actual hardware and networking components that store and transmit information resources.

- To implement physical security, an organization must identify all of the vulnerable resources and take measures to ensure that these resources cannot be physically tampered with or stolen.

Physical Security

- **Locked doors:** It may seem obvious, but all the security in the world is useless if an intruder can simply walk in and physically remove a computing device.
- High-value information assets should be secured in a location with limited access.
- **Physical intrusion detection:** High-value information assets should be monitored through the use of security cameras and other means to detect unauthorized access to the physical locations where they exist.
- **Secured equipment:** Devices should be locked down to prevent them from being stolen.
- One employee's hard drive could contain all of your customer information, so it is essential that it be secured.

Physical Security

- **Environmental monitoring:** An organization's servers and other high-value equipment should always be kept in a room that is monitored for temperature, humidity, and airflow.
- The risk of a server failure rises when these factors go out of a specified range.
- **Employee training:** One of the most common ways thieves steal corporate information is to steal employee laptops while employees are traveling.
- Employees should be trained to secure their equipment whenever they are away from the office.

Security Polices

- Besides the technical controls listed above, organizations also need to implement security policies as a form of administrative control.
- In fact, these policies should really be a starting point in developing an overall security plan.
- A good information-security policy lays out the guidelines for employee use of the information resources of the company and provides the company recourse in the case that an employee violates a policy.

Security Polices

- According to the SANS Institute, a good policy is “a formal, brief, and high-level statement or plan that embraces an organization’s general beliefs, goals, objectives, and acceptable procedures for a specified subject area.”
- Policies require compliance; failure to comply with a policy will result in disciplinary action.
- A policy does not lay out the specific technical details, instead it focuses on the desired results.
- A security policy should be based on the guiding principles of confidentiality, integrity, and availability.

Security Polices

- A good example of a security policy that many will be familiar with is a web use policy.
- A web use policy lays out the responsibilities of company employees as they use company resources to access the Internet.
- A good example of a web use policy is included in Harvard University's " ilities".

Security Polices

- A security policy should also address any governmental or industry regulations that apply to the organization.
- For example, if the organization is a university, it must be aware of the Family Educational Rights and Privacy Act (FERPA), which restricts who has access to student information.
- Health care organizations are obligated to follow several regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).
- A good resource for learning more about security policies is the SANS Institute's Information Security Policy Page.

Usability

- When looking to secure information resources, organizations must balance the need for security with users' need to effectively access and use these resources.
- If a system's security measures make it difficult to use, then users will find ways around the security, which may make the system more vulnerable than it would have been without the security measures!
- Take, for example, password policies.
- If the organization requires an extremely long password with several special characters, an employee may resort to writing it down and putting it in a drawer since it will be impossible to memorize.

Personal Information Security

There is no way to have 100 % security, but there are several simple steps we, as individuals, can take to make ourselves more secure.

- Keep your software up to date.
- Whenever a software vendor determines that a security flaw has been found in their software, they will release an update to the software that you can download to fix the problem.
- Turn on automatic updating on your computer to automate this process.

Personal Information Security

- Install antivirus software and keep it up to date.
- There are many good antivirus software packages on the market today, including free ones.

Personal Information Security

- Be smart about your connections.
- You should be aware of your surroundings.
- When connecting to a Wi-Fi network in a public place, be aware that you could be at risk of being spied on by others sharing that network.
- It is advisable not to access your financial or personal data while attached to a Wi-Fi hotspot.
- You should also be aware that connecting USB flash drives to your device could also put you at risk.
- Do not attach an unfamiliar flash drive to your device unless you can scan it first with your security software.

Personal Information Security

- Back up your data.
- Just as organizations need to back up their data, individuals need to as well.
- And the same rules apply: do it regularly and keep a copy of it in another location.
- One simple solution for this is to set up an account with an online backup service, such as Mozy or Carbonite, to automate your backups.

Personal Information Security

- Secure your accounts with two-factor authentication.
- Most e-mail and social media providers now have a two-factor authentication option.
- The way this works is simple: when you log in to your account from an unfamiliar computer for the first time, it sends you a text message with a code that you must enter to confirm that you are really you.
- This means that no one else can log in to your accounts without knowing your password and having your mobile phone with them.

Personal Information Security

- Make your passwords long, strong, and unique.
- For your personal passwords, you should follow the same rules that are recommended for organizations.
- Your passwords should be long (eight or more characters) and contain at least two of the following: upper-case letters, numbers, and special characters.
- You also should use different passwords for different accounts, so that if someone steals your password for one account, they still are locked out of your other accounts.

Personal Information Security

- Be suspicious of strange links and attachments.
- When you receive an e-mail, tweet, or Facebook post, be suspicious of any links or attachments included there.
- Do not click on the link directly if you are at all suspicious.
- Instead, if you want to access the website, find it yourself and navigate to it directly.

Thank you for your attention