ELTE - Faculty of Informatics

Subject: Information Security Management

Lecturer: Péter Burcsi

Group project: Assignment 1

Date of submission: 18th of May 2022

Group members:

Ali Aqeel Zafar (AAFZDE)

Cristian Luca Angheluta (NZTBIF)

Friedrich Ostertag (D7KQBF)

Massimo Morello (XO5DWV)

Olimpia Demetraki-Paleolog (CAS7KZ)

Company overview

We are working for **CyShop**, a software development company which was founded at the start of the pandemic and helped us get in contact with many businesses that needed the web shop apps our company developed.
We continued to grow and now we stand at 700 employees that work together in order to provide the best possible service to our clients.
The headquarters of our business is located in Florida, USA since they have a big market centered on web shops and we focus on making business with small to medium sized companies, which deal with a large amount of customer data.

Conclusions from survey

17% of employees share credentials and 23% of developers leave desks unobserved and computers unlocked. For both vulnerabilities the resulting risks are mostly similar.
It might be easier to get credentials as this is possible through remote communication (phishing mails / calls). But on the other hand, a remote attack might be restricted by firewalls and similar security mechanisms which could in the best case prevent the attacker from causing any harm even when possessing the credentials.
Making use of an unlocked computer at an unobserved workplace requires an attacker inside the company which is not as easy and likely to happen as a remote attack. Nevertheless, such an incident has the potential to cause much more harm, as the attacker would have direct access to not only company software, but also hardware. For example, malicious hardware could be placed inside the company network.
While the accessible resources differ depending on who's workplace is accessed, even access on the lowest level can cause serious security problems and has to be avoided. That is especially true for employees who work in development. And as we know from the survey, many of them leave their workstation unlocked from time to time.
The **worst-case scenario** would be an attacker exploiting both vulnerabilities combined, which could lead to an attacker having almost unrestricted access from inside the internal network.
To conclude we would say that sharing credentials is a vulnerability that is more likely to be exploited but also with probably a lower impact, while leaving the workstation unlocked is less likely to be exploited but more likely to have a high impact when being exploited. Still, both will lead to the risk of attackers accessing and modifying resources that they should not be able to see or change. These risks will be introduced and explained in the following chapter.

Risks

1. **Risks related to account credentials information**

Let us begin with the risks that arise because of employees leaking credential information:

1.1. Changing credentials

The acquired credentials can be used by an attacker to change the login for the affected user and block the user's access (at least temporarily). This can be used combined with an attack to prevent/disrupt/delay appropriate attack retaliation.

1.2. Remote access to sensitive resources

The credentials might be used by the attacker to login to various applications remotely, without requiring physical access to the company.

2. **Risks related to leaving the workstations unlocked**

2.1. Malicious hardware

Accessing an unobserved workplace enables an attacker to place malicious hardware connected to the workstation / internal network.

2.2. Malicious software

Accessing an unlocked computer at an unobserved workplace allows the installation/setup of malicious software that can track/interfere/alter internal activities and communication.

3. **Risks relate to both**

3.1. Stolen data

In both cases of vulnerabilities data can be stolen by the attacker. That could include sensitive personal data, financial information about our company, as well as source code and documentation about the past and ongoing web shop projects.

3.2. Changed data

Furthermore, it might be possible for an attacker to alter or delete some of the data mentioned in 3.1.. Especially if the source code of the projects is manipulated, that can cause a lot of harm to us and our customers, as the sold web shop software might behave maliciously. This can mean not functioning, leaking sensitive customer information (personal & financial), or infecting customer's systems with viruses.

3.3. System corruption

The last identified risk is the corruption of our own system. That can concern clients, servers and/or firewalls. Their functionality can be reduced or even disabled. This can cause system failure which would stop the entire workflow until being fixed and many more problems. Also it could open the door for further exploitation.

How we mitigate risks

1. **Risks related to account credentials information**

1.1. Changing credentials

By using a password manager with 2-factor-authentication only one password has to be remembered by each employee. And even if that password is leaked, the attacker cannot access the password manager and change credentials, as he/she doesn't control the 2nd authentication factor.

1.2. Remote access to sensitive resources

We use appropriate firewall topology and settings to restrict remote access to internal resources as much as possible. If remote access is required, we use VPN technology to allow external access for authenticated user devices only. Even if the credentials are known, the attacker would also have to control the physical device to be able to access internal resources remotely.

2. **Risks related to leaving the workstations unlocked**

2.1. Malicious hardware

By restricting usage of external unauthenticated hardware on a physical and software level, we prevent external (and potentially malicious) hardware from being used and causing harm.

2.2. Malicious software

Mitigating the installation of malicious software on an unlocked computer by an attacker is almost impossible (would require very restrictive internet access). Since it is only possible, if the computer is unlocked/credentials are known, we focus on this point in our awareness training to reduce this risk and use an automated locking function which will lock workstations after a short time of inactivity.

3. **Risks related to both**

The previously introduced security mechanisms (2FA-password manager, firewall, training) will mitigate the risk of unauthorized external and internal system access and modifications. That way the risk of data being stolen (3.1), data being changed (3.2) and system corruption (3.3) will be mitigated as well.

Our survey to assess state of security awareness

We use the survey to gain knowledge about our employees' security awareness in different topics. This knowledge will be used to specify the theoretical security briefings, as well as the practical training accordingly. The survey looks like the following:

1. Do you close your computer during breaks? If not, how long do you usually take a break for?

2. Do you know who to contact in case you are hacked or if your computer is infected? a. Yes, I know who to contact. If yes, who? b. No, I do not know who to contact.

3. How secure do you feel your computer is?
    a. Very secure b. Secure c. Not secure

4. What are the risks associated with a phishing attack?

5. How probable do you think it is?

6. Do you know what email fraud is and how to identify one? a. Yes, I do. b. No, I do not. → recognize a suspicious email (with screenshots)

7. If you delete a file from your computer or USB stick, that information can no longer be recovered.
    a. True b. False

8. What is the worst-case scenario of someone entering your work account/computer?
    a. Nothing bad can happen; b. the attacker will act as me; c. Data gets stolen; d. Whole company can be corrupted.

9. Click on this link for the next set of questions:
   www.totallynotsuspiciousatall.com

Security campaign

Our **security campaign** consists of **4 elements**:

- **Quarterly common ground rule briefing**

Every 3 months there will be a security briefing for every employee of the company. This will set common ground rules for everyone working in the company. The rules will be easily understandable and secure for everyone. While different positions might differ in access to sensitive resources and privileges, even taking over a lower-level account can enable an attacker to cause serious problems. That's why we want to establish policies that can provide security throughout all hierarchical levels of the company.

The briefing contains:

1) Explanation of the password manager, s.t. everybody feels comfortable using it.
2) How to deal with e-mails

We will implement a system that marks e-mails from authenticated internal sender addresses. Part of the training will be how internal and external mails can be differentiated reliably. Furthermore, there will be a set of rules defining what content to share and how to interact with content of mails, depending on if they are internal or external communication.

3) How to deal with phone calls

Same system as with e-mails. There will be a secure authentication mechanism to distinguish between internal and external calls. Rules regarding what information to share in each of these will be set and taught.

- **Ongoing phishing tests**

Since social engineering in the form of phishing is considered as the most common and serious risk, we want to keep the employees continuously aware and engaged. To achieve this there will be random phishing mail and calls from the security department to employees.

- **Ongoing awareness game**

To ensure ongoing security awareness at the workplace we make use of gamification. Employees will receive simulated sensitive tokens (can simulate e.g., sensitive documents, passwords, information). Throughout each year random employees will be assigned the task of acquiring specific tokens from their colleagues through a given method. This keeps awareness high on the side of the "attackers" as well as the "targets". The usage of tokens prevents actual sensitive information from being accessed by unauthorized persons (colleagues).

- **Rewards & Specific additional briefings**

There will be a ranking system for the practical security training (phishing tests & awareness game). There won't be any punishment for failing / making mistakes at those, but points can be gathered for correct responses to phishing and successfully acquiring colleagues' tokens. There will be a visible leaderboard of the "top 10 security aware employees". For employees achieving bad results in the practical training, we will provide additional specific security briefings about the problematic topics, if needed.