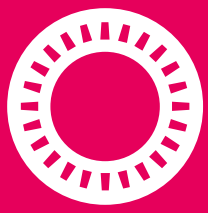


MATESO
PASSWORD SAFE

The Human Security Gap

Inhaltsverzeichnis

Introduction

The fight for more cyber security is an ongoing process without a pause. From Deepfakes to fake websites: In the course of digitalization, hackers are also upgrading and seem to be one step ahead in the development of new attack scenarios. With the growing external threat, one important factor is often overlooked - the danger in front of the PC: Your own employees represent an enormous security risk for companies – whether it happens consciously or unconsciously. According to current studies, 76% of those surveyed see poorly trained employees as the greatest security risk for companies. It`s an actual fact that some people would give away their password for a bar of chocolate.

This whitepaper is therefore intended to serve as an information basis for companies to learn to better assess their own employees as a risk factor when it comes to passwords and to develop protective measures accordingly.

> **There is no certainty, only varying degrees of uncertainty.**
>
> **Anton Neuhäusler,** professor of philosophy

Risk Scenarios

If one considers people as a security gap in cyber security, two dimensions emerge – the conscious and the unconscious damage of internal security mechanisms. Conscious data misuse is usually due to criminal intent, resentment or greed. The unconscious misuse of data, on the other hand, is caused by carelessness or lack of know-how and resources.

The resulting consequences can be enormous on both sides – financially as well as by suffering a loss of reputation. Although each case of data misuse is different, general scenarios can be outlined to derive patterns and develop solution scenarios.

Conscious Data Misuse

Espionage and theft of internal information and secrets

Not every departure of an existing employee is as harmonious as desired: If both parties do not part in peace, the internal data can be put at risk. This is because employees can copy data to make it available to their new employer or competing companies or use it to start their own business.

Arbitrariness in handling sensitive data

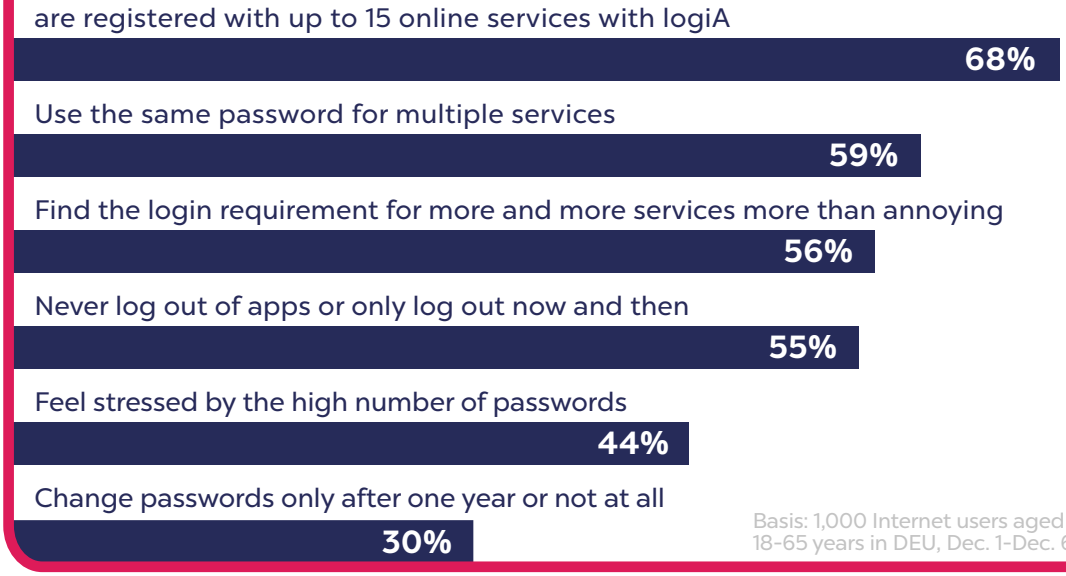
Also, employees who are not committed to the company could be negligent with internal data and secrets. This can manifest itself, for example, in careless handling of passwords, visiting insecure websites or potentially downloading malware. They could also delete data and accounts.

Data embezzlement and sabotage

In extreme cases, bad players may decide to deliberately attack and paralyze the internal IT infrastructure in order to provoke financial damage or black-mail the company. Since these bad players have access from within, it is also easy for them to collaborate with hackers and grant them access to all data. According to Bitkom, every second company has already fallen victim to data abuse such as sabotage

Password Facts[1]

Internet users surveyed on their handling of passwords



Basis: 1,000 Internet users aged 18-65 years in DEU, Dec. 1-Dec. 6, 2016.

Unconscious Data Misuse

Improper use of passwords

If employees have little sensitivity in dealing with security-relevant data and accesses, careless handling of passwords is usually the result. Passwords are shared in plain text, written on slips of paper and passed on and stored in insecure places like Excel lists. This procedure can already be a violation of data protection, which employees are usually not aware of. In addition, employees register for new applications and websites on their own initiative and use insecure or already used passwords for the respective accesses.

Furthermore, if employees do not have a sense for more security awareness, security policies can also be implemented incorrectly, so that they can actually do more harm than good to the company. If employees who remember passwords in their heads are advised to change them regularly, for example, they will be happy to use only slightly modified versions of existing passwords by changing them slightly or adding special characters and numbers.

These patterns are well known to hackers, which is why such passwords are particularly easy to decipher and can be cracked quickly.

The following methods of attack are particularly favored by hackers:

Password Spraying

This attack attempts to access a large number of accounts/ user names with a few, frequently used passwords. If the employee uses a common password and/or a password for several accounts, the risk to get hacked by password spraying increases.

Dictionary Attacks

Even logical combinations or words that can be found in dictionaries are no challenge for hackers. So-called dictionary attacks use a password list to determine an unknown password. So, if the employee uses a password that can also be found (partially) in the dictionary, the risk of being hacked increases considerably.

Download / Installation of Malware

If an employee is unaware of risks, malware programs can easily gain access to companies - for example, by clicking on the wrong link. A conscious installation of the program is no longer even necessary, as viruses and the like settle in the system automatically and the damage takes its course.

Special monitoring programs can document and also block unwanted downloads and/or installations. This always includes prevention measures in the sense of awareness training, so that the click on a dangerous link can be excluded as a risk in advance.

Incorrect handling of data security incidents

In order to be able to act correctly in the event of a breach of internal security guidelines, the relevant security officers must first and foremost become aware of it. If the employee covers up an incident out of fear or is not even aware of the violation, the parties cannot take preventive or reactive measures.

Even if no internal catalog of measures has been implemented at all, employees are sometimes uncertain as to whom they can turn to and when. For two-way healthy communication, a positive working atmosphere is also essential to lower the inhibition threshold for employees to admit security incidents.

Social Engineering

Social engineering, also known as social hacking, describes the procedure of exploiting human characteristics such as good faith, helpfulness and insecurity by deception and manipulation in order to obtain security-relevant data or install malware.

Phishing

Phishing is an attempt to obtain personal data via fake websites, e-mails and/or short messages. Phishing can easily lead to account looting by users entering their account information on a fake website, to which they are redirected by clicking on the link in a deceptively genuine e-mail from their bank provider such as Postbank.

Further attack scenarios can be derived from phishing:

Spoofing

Spoofing is the pretending of another identity in order to penetrate the PC or networks. In most cases IP and/or address are faked in such a way that the recipient considers them trustworthy and then clicks on the link contained or opens the attachment. As a result, malware or keyloggers can be installed on the system unnoticed.

To prevent spoofing, employees should always be encouraged to report suspicious e-mails and should rather seek expert advice if there is any uncertainty about their trustworthiness. If the login information is stored in a Password Manager, this problem is not even necessary: Because the login data contained in the e-mail, such as the IP address, is stored there for automatic login, the Password Manager recognizes fake addresses and successfully prevents the login. This way the employee notices in time that he is dealing with a wrong link, even though he clicked on the link.

Pharming

Pharming is an advanced method of phishing by manipulating domain name system (DNS) requests to the web browser. DNS is used to convert web addresses into IP addresses. If, for example, a number of the IP address in the host file is changed, the user is forwarded to the fake site without noticing, even though the web address was entered correctly. In pharming, therefore, not even clicking on a false link is necessary to deceive. If the user now enters his confidential data on the fake site, the pharming is successfully completed.

To prevent pharming, the address should always begin with „https://“ when entering the address. It is also possible to request an authentication of the server by automatically exchanging a certificate. An up-to-date virus program and a good firewall are also essential to prevent pharming.

Deepfakes

Artificial intelligence also takes phishing attacks to a new level. Because AI enables attackers to deceive their victims even better. Deepfakes are particularly worthy of mention here - derived from the terms deep learning and fake. Deepfakes enable attackers to manipulate media content such as images, videos or audio files using AI and machine learning in order to trick their victims.

In the meantime, deepfakes have even become so sophisticated that the copy can hardly be distinguished from the original. So it could easily imitate the voice of the CEO on the phone, offering the employee to transfer a certain amount of money to that account immediately.

Since deepfakes are still a relatively new method, protection mechanisms are still difficult to define. The fact is that they bring the need for awareness training even more to the fore, so that employees learn to question actions and are better prepared for more unknown tactics

Shoulder Surfing

Not to be taken on the light shoulder is the so-called Shoulder Surfing. Here, the perpetrator literally looks over the victim‘s shoulder while the victim enters his password, for example. Especially in public, it can happen that secret information is read on the train and then stolen. This seemingly simple method is equally efficient for the perpetrator, since he does not need any technical know-how to obtain passwords or PIN codes.

Employees should therefore always be reminded to enter sensitive data undercover - especially when on the move. Privacy filters and foils also make it difficult for third parties to view the screen. If a password manager is in use, it can be specified that passwords can only be entered covertly via single sign-on.

Security Awareness as a Solution

The first priority is to generate security awareness in each individual employee. Security Awareness means that the employee actively contributes to the protection of the company, as his attitude towards it, his associated knowledge as well as his associated actions are compliant with the internal data security guidelines.

This awareness can be achieved through education and training as well as through specific campaigns implemented by each employee, taking into account their individual level of technical knowledge

Standardized Processes and Documents

Every employee must be aware of the contact person in the company to whom he can turn if he has questions about IT security or a security incident has occurred and how to proceed. Corresponding documents must be easily accessible to every employee, so that they can keep themselves up to date and be informed about the latest changes.

Content-related points to create security awareness:

- Cyber threats are ubiquitous and can affect any business or individual.
- The complexity as well as strength of cyber attacks is increasing exponentially.
- Cyber security affects every employee - regardless of position or department - not just the IT security officer or system administrator.
- The damage caused can be not only financial, but also damage to the company‘s image and reputation.
- Not only sensitive company data, but also personal information of the individual employee can be disclosed.
- Security incidents must be reported immediately to limit the damage.
- In the event of negligent action or verifiably intentional misuse of data, the company can also hold the employee responsible.

Security Awareness as continuous Development

Companies must be aware that security awareness cannot be introduced overnight or through one-time training. The support and reassurance of individual employees are essential for the long-term implementation of security structures. Both parties learn from each other through mutual exchange.

Internal audits provide support here in order to gain an overview of what works well and where adjustments are necessary. Through regular anonymous surveys and/or feedback meetings, for example, it is possible to find out which points are still open or incomplete and which processes employees might still be unsure about during implementation. In this way, structures can always be adjusted to the needs of the employees to ensure that they are realistic in terms of time and effort.

Information Security Awareness

Employees must also be constantly encouraged and reaffirmed as a key role in security compliance. Through internal circulars, security newsletters, a guideline or visually prepared measures such as posters, employees do not feel left alone in the implementation process by repeatedly bringing the topic to the fore.

Conclusion

In conclusion, it can be said that the human vulnerability can best be eliminated by understanding the possible risks and by healthy internal communication. The path to more security awareness cannot be defined for companies in a general way, but must be decided individually for their own employees depending on their level of knowledge, motivation and implementation possibilities.

The respective requirements differ depending on legal regulations, the size and the industry of the company. However, taking into account all the factors mentioned in this white paper, any company can contribute to a more stable internal security infrastructure by giving people the attention they need.

Author:
Kristina Kaya
Product Marketing Manager

Source directory:

1 Statista 2020: Web.de, the big password hassle

2 Statista 2019: Online survey by VDE Bayern

3 Bitkom Study Report 2018: Espionage, Sabotage and data theft - economic protection in industry

MATESO

MATESO is a leading German IT company that has successfully established itself in the DACH region since its foundation in 2006. The developed password security solution Password Safe is distributed internationally through its worldwide partner network. Well-known references testify to the technological and know-how advantage of the IT software.

Today, the steadily growing company has more than 10,000 corporate customers with several million users worldwide - among them 20 of the Dax TOP 30 companies.

PASSWORD SAFE

Pioneer in Enterprise Password Management

Password Safe serves as a central digital vault for enterprises to secure, manage and monitor sensitive data such as passwords, documents and secrets.

In dealing with passwords the human being is still indispensable.

One thing is certain: All mistakes, he can make will be made.

Thomas Malchar
CEO of MATESO

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.com
Email: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE