Protection of Confidential Data

Target Group
Civil Society Organisations

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Protection of Confidential Data

Target Group: Civil Society Organisations

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

January 2025
Doha, Qatar

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Contact the National Cyber Excellence Department

▯ **00974 404 663 79**   ☎ **00974 404 663 62**

🌐 www.ncsa.gov.qa/   ✉ academy@ncsa.gov.qa

Dear Participant,

In light of the rapid technological advancements and the pervasive presence of the internet in various aspects of life, cyber threats have become a challenge all segments of society encounter. This necessitates efforts to raise awareness about digital safety concepts, which serve as the shield protecting society from these threats.

As part of the "National Initiative for Digital Safety" efforts to enhance digital safety standards within the community, the National Cyber Security Agency presents this booklet with a collection of general tips and guidelines related to digital safety.

Introduction

Data protection is essential in our current era, particularly with the rapid technological advancements and the increasing volume of data collected and processed. This has necessitated the establishment of regulatory frameworks to safeguard the privacy and security of data, whether for individuals or organisations. These regulations provide strict guidelines for data handling and processing and have evolved over the years to cope with changes in the digital field.

The importance of data protection is highlighted by several key factors, foremost of which is the need to comply with data regulations in countries worldwide. These regulations impose several requirements on organisations, and failure to comply can result in hefty fines, strict legal actions and damage of the organisation's reputation.

Additionally, data protection is crucial in defending against increasingly varied and dangerous cyberattacks, resulting in significant financial losses for organisations that lack adequate security measures to counter these threats and protect their data.

Another critical aspect of data protection is safeguarding customer information. Organisations store large amounts of customer data, such as names, addresses and payment details. Protecting this information is critical to prevent data breaches or leaks and misuse, which could lead to financial losses and damage to the organisation's and the customers' reputations.

The above points emphasise that protecting data within organisations from leakage and breaches is crucial to ensuring business continuity. Any disruption in workflow can lead to a complete operational halt, resulting in decreased productivity and interruptions to operational and administrative processes.

It should be noted that data leakage occurs when sensitive information is unintentionally exposed to the public during transmission or use. This can happen during data transfers via emails, API calls, chat rooms and other communication channels. Data may also be exposed during periods of inactivity, such as when cloud storage is misconfigured, databases are unsecured, or devices are lost. Moreover, data in use is also vulnerable to leakage, such as information on printers, screenshots and USB drives.

01

Chapter 1

Data Leakage

- First: **Data Leakage Concept**
- Second: **Difference between Data Leakage and Data Breach**

Data Leakage

Data leakage is one of the most dangerous threats facing individuals and institutions in the digital age. This type of incident occurs when sensitive or confidential information is disclosed to unauthorised parties, whether due to cyberattacks, human errors or vulnerabilities in security systems.

Data leakage can lead to huge financial losses, reputation damage and illegal exploitation of personal or commercial information. With the continuous increase in digital activities, data protection has become a top priority for maintaining digital security and privacy across various sectors, including companies and government institutions.

First: Data Leakage Concept

Data leakage occurs when critical information is exposed to unauthorised individuals due to internal errors within the organisation. This often results from weak data security, outdated systems or insufficient employee training. Data leakage can lead to identity theft for employees and customers, data breaches, or the installation of malicious software such as ransomware.

Although data leakage is typically accidental and lacks malicious intent, it can still cause significant harm to organisations and their operations. For example, mistakenly sending a critical file to unauthorised parties results in its circulation, allowing cybercriminals to obtain it and exploit it later to execute attacks such as ransomware attacks.

⚠ **Warning!**

Data leakage leads to identity theft of either employees or customers or installation of malicious software such as ransomware.

Examples include:

1. When an employee within the organisation accidentally sends a critical document to external parties by email.
2. When important data is published due to incorrect settings in an application or because of human error, making it accessible to everyone.
3. Critical data may inadvertently appear in the backgrounds of pictures taken by personal cameras and shared publicly.

Second: Difference between Data Leakage and Data Breach

The two terms are often used interchangeably to express the same idea; however, there are distinctions between them. While data leakage and data breach refer to unauthorised access to important data, the underlying cause determines the nature of the violation, whether it is a leakage or a breach.

Data leakage occurs when a source within the organisation exposes data. A data breach occurs when an external source breaches the system through a cyberattack. Therefore, data leakage is viewed as an accidental incident due to internal error or negligence, while a data breach is an intentional attack. Sometimes it can be challenging to distinguish between leakage and breach because cybercriminals use leaked data to execute a large-scale data breach. For example, by breaching one email account, they can execute business email fraud such as ransomware attacks.

Warning!

Mistakenly sending a critical file to unauthorised parties results in its circulation, allowing cybercriminals to obtain and exploit it later to execute attacks such as ransomware and fraud.

Consequently, cybercriminals only need a single instance of data leakage to escalate it into a significant data breach, which poses a serious threat to organisations[1]. Data breaches are categorised according to the type of attack vector utilised and the attacker's identity. **There are two main types of data breaches:**

1. Data breaches originating from external threat actors.
2. Data breaches originating from internal threats related to the organisation. These are divided into malicious attacks by a disgruntled employee, negligence attacks due to weak passwords and recruitment cases involving cybercriminals luring employees within the organisation to help them attack the network and steal data.

Based on the above, it becomes clear that data breaches are not accidental but harmful attacks targeting organisations.

Warning!

Cybercriminals need only one instance of data leakage to transform it into a significant data breach, posing a serious threat to organisations.

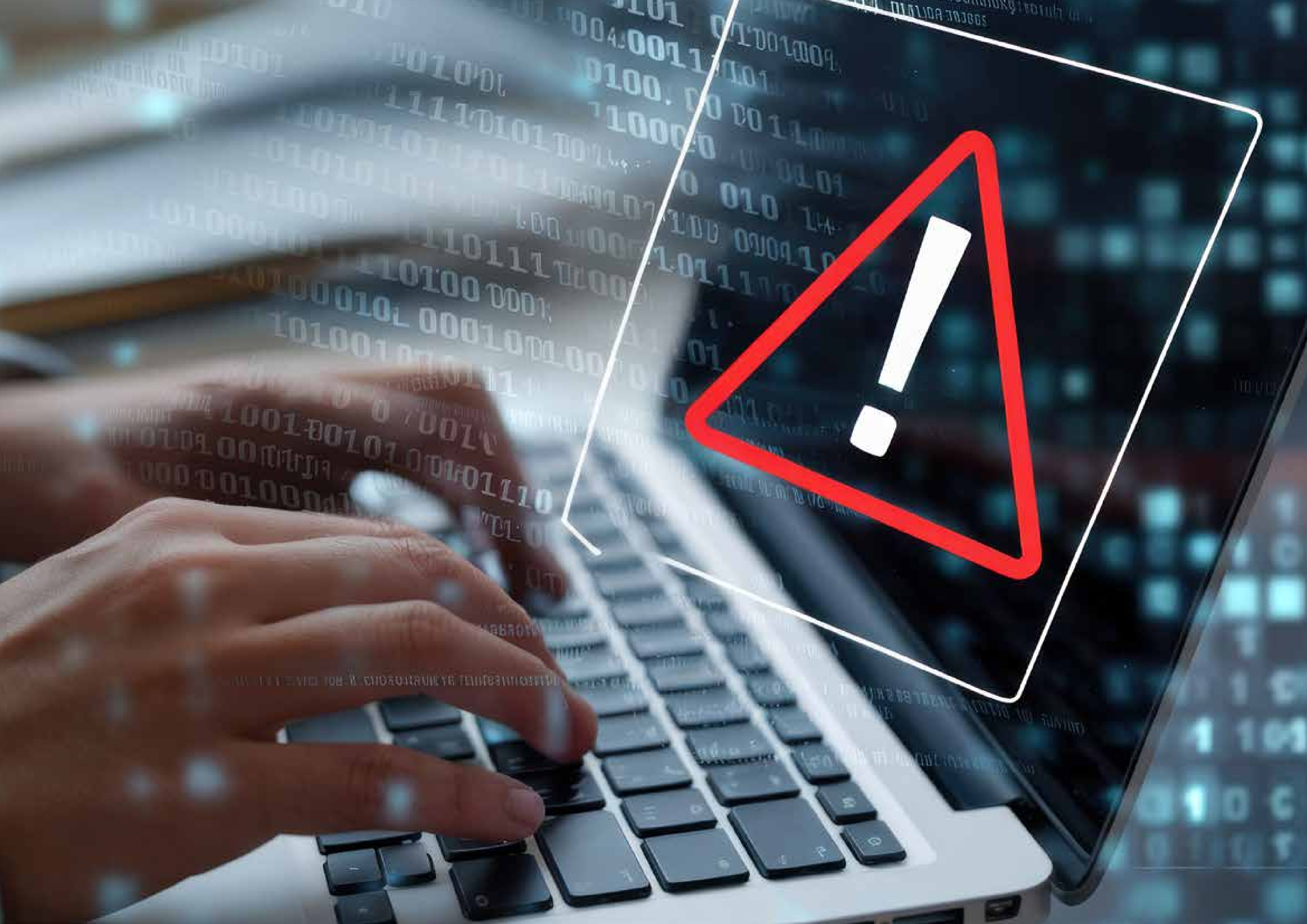
[1] Data Breach Versus Data Leak: What's The Difference?, 2024. Follow link: https://www.teramind.co/blog/data-breach-vs-data-leak/.

Methods of data breach include:

1. Ransomware attacks are most common for obtaining money in exchange for stolen data, especially if organisations don’t have data backups.
2. Social engineering attacks targeting employees within organisations to deceive them and gain access to sensitive data by infiltrating the network. If these attempts are unsuccessful, the attacker may resort to credential stuffing attacks, where brute force methods are employed to guess employees’ passwords and gain access to the network. Additionally, malicious software such as Trojans may be used to compromise the system or breach servers through complex cyberattacks.

⚠ **Warning!**

The use of the same password by employees for multiple accounts increases the risk of falling victim to credential stuffing attacks, thereby facilitating the infiltration of organisations and the theft of their data.



02

Chapter 2

Data Leakage in Organisations

- First: **Causes of Data Leakage in Organisations**
- Second: **Types of Leaked Data in Organisations**

Data Leakage in Organisations

Data leakage in organisations represents an increasing threat that significantly impacts information security and operational integrity. Data leakage occurs when sensitive information, such as customer data, strategic plans or financial details, is exposed or leaked to unauthorised parties. This may result from cyberattacks, human errors or vulnerabilities in the security infrastructure. Organisations encountering such incidents suffer severe financial losses, reputational damage and loss of customer trust. Therefore, data protection has become one of the top priorities for companies to ensure business continuity and reduce risks in a digital environment full of challenges.

First: Causes of Data Leakage in Organisations

1. Weak Infrastructure

The lack of reliance on modern information security standards in Cybersecurity architectures can lead to incorrect configurations or permissions, resulting in data leakage[1].

2. Social Engineering Attacks

Although data breaches result from cyberattacks, cybercriminals employ similar methods to leak organisational data to launch other attacks, such as phishing emails that lead to the acquisition of login credentials for certain employees, ultimately resulting in a data breach for the organisation.

Warning!

Cybercriminals employ various methods to leak organisational data to launch other attacks, such as phishing emails that lead to the acquisition of login credentials for certain employees, subsequently resulting in a data breach for the organisation.

[1] . What Is a Data Leak? How They Happen and How To Prevent Them. Follow link: https://abnormalsecurity.com/glossary/data-leak

The parties executing cyberattacks often use social engineering techniques to deceive employees into providing sensitive information by impersonating a colleague or IT specialist.

Social engineering attacks aim to steal login credentials, phone numbers or names of employees with data access privileges[1].

Facts and Figures

500,000 Zoom credentials were sold on the dark web, with passwords reaching low prices due to abundance through credential stuffing attacks. Cybercriminals logged into Zoom using accounts leaked in old data breaches, then compiled successful logins into lists sold to other hackers[2].

3. Weak Passwords

Some users tend to use the same password across multiple accounts for ease of recall. Consequently, when a credential stuffing attack occurs, it can expose several accounts, leading to organisational breaches and data theft.

[1] Data Leakage: Common Causes, Examples & Tips for Prevention. Follow link: https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention.

[2] Over 500,000 Zoom accounts sold on hacker forums, the dark web. Follow link: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/.

4. Lost Devices

If an employee loses a device containing sensitive organisational information, this is considered a potential data breach as it facilitates the attacker's access to and breach of organisational data.

5. Security Vulnerabilities in Software and Applications

Security vulnerabilities create significant weaknesses within organisations, including undiscovered vulnerabilities. Cybercriminals may exploit these weaknesses to carry out multiple attacks targeting organisational data.

Warning!

The use of personal tools and devices by employees, such as home printers to print sensitive organisational data, exposes the organisation to the risk of data leakage, ransomware attacks and more.

6. Old Devices

These devices often run on outdated operating systems, making them easier to be breached. Additionally, their security standards tend to be low, creating a vulnerability that may lead to data leakage.

Warning!

The loss of a device that contains sensitive organisational information represents a potential data breach, as it enables an attacker to access and compromise the organisation's data.

Second: Types of Leaked Data in Organisations

1. Personally Identifiable Information (PII)

Information or records that identify employees and customers, such as names, phone numbers, addresses and email addresses. The goal is identity theft and fraud execution, as PII frequently appears in data leakage cases.

2. Financial Data

All data related to organisations' financial or banking affairs, such as tax information and invoices.

3. Account or Login Credentials

User account login details, including names, passwords and email addresses, are among the most in-demand as they enable cybercriminals to execute account takeovers and data breaches.

4. Organisation Information

This includes internal information generated and stored by the organisation, featuring important business data such as internal communications, confidential records, performance metrics, meeting notes, human resources records and all matters related to the organisation's operations.

5. Trade Secrets and Intellectual Property (IP)

This is highly confidential and protected information, and its disclosure can pose significant risks to organisations. This information includes confidential research, patents, plans, test materials, future project designs, software source code, proprietary technology and all strategic information associated with the organization[1].

[1] . What Is a Data Breach?. Follow link: https://www.akamai.com/glossary/what-is-a-data-breach.

Did You Know?

In 2021, research revealed that 74% of large companies and 61% of small companies experienced data breaches, and global data breach rates recorded an increase of over 70% in the third quarter of 2022.

03

Chapter Three

Strategies for Protecting Confidential Data from Leakage

- First: **Detecting Data leakage in the Organisation**
- Second: **General Procedures for Data Protection from Leakage**

◆ Strategies for Protecting Confidential Data from Leakage

Protecting confidential data from leaks is a critical aspect of modern cybersecurity strategies. With increasing reliance on technology in managing sensitive information such as financial data, strategic plans and customer data, it has become essential to implement strict measures to prevent unauthorised access to this information.

The leakage of such data can lead to severe financial losses and damage to the organisation's reputation. Therefore, protecting confidential data includes using encryption techniques, enhancing access policies, training employees on safe practices and continuously updating security systems. These efforts contribute to maintaining information confidentiality and protecting the organisation from external threats.

Warning!

Upon detecting an increase in failed login attempts or unauthorised access attempts to data, employees must promptly notify the cybersecurity department within the organisation.

Warning!

Sudden loss of files and inability to access certain information are indicators of data breach operations within organisations.

First: Detecting Data Breaches in the Organisation

Some indicators proactively reveal data breach operations, representing any unusual activity suggesting a problem, such as[1]:

- ✓ Unusually high traffic on the website.
- ✓ Unexpected password reset requests.
- ✓ An increase in failed login attempts.
- ✓ A decrease in the number of email messages.
- ✓ Unauthorised access attempts to data.
- ✓ Attempts to access company systems outside of regular working hours.

[1] How to Detect a Data Breach (5 Critical Steps). Follow link: https://www.breachsense.com/blog/data-breach-detection/.

- System performance issues, as many cyber threats, such as DDoS attacks, impact network performance and speed. Therefore, a slow performance without justification may indicate that the system is under attack.
- Overall increase in login attempts.
- Presence of encrypted files due to ransomware attacks.
- Sudden changes in the database.
- Sudden loss of files.
- Inability to access specific information.
- Increase in phishing emails targeting organisation employees.

Did you know?

In 2020, Twitter (now X) employees fell victim to a phishing attack that allowed cybercriminals to access 130 private and institutional accounts on the platform, including those of Elon Musk and Bill Gates[1].

The attack was initiated with an email claiming to be from Twitter's IT team. As a result of the internal employee's failure to verify the email, the cyberattack was successful.

[1] Hackers targeted Twitter employees to hijack accounts of Elon Musk, Joe Biden and others in digital currency scam. Follow link: https://www.cnbc.com/2020/07/15/hackers-appear-to-target-twitter-accounts-of-elon-musk-bill-gates-others-in-digital-currency-scam.html

Second: General Procedures for Data Protection from Leakage

Organisations require a set of regulatory procedures to protect their diverse data, which is considered one of their essential assets. This is crucial to prevent loss, leakage and the risk of exposure to cybercriminals who may exploit such data to conduct further cyberattacks for financial gain, including ransomware attacks.

Key protection procedures include:

1. Data Encryption

Encryption refers to converting important data into codes to prevent unauthorised access. The process includes all sensitive data such as customer information, financial data and intellectual property. Data encryption converts readable data into an unreadable format using specific algorithms. Decrypting this data requires obtaining the key that decodes the used algorithm[1].

[1] Who should encrypt the data in my company?. Follow link: https://www.sealpath.com/blog/data-encryption-for-enterprises/.

2. Data Backup

Regular data backup processes enhance organisations' ability to recover from data breaches and leaks more swiftly and at a lower cost. Therefore, it is recommended to perform regular backups of data, ensuring they are stored in secure locations[1].

3. Employee Awareness

Key cyber protection practices include: awareness and education of organisation's employees of the best practices of data protection, such as creating strong passwords and distinguishing between secure and phishing emails.

4. Data Access Controls

One matter that should be considered is restricting access to sensitive data within the organization. Organizations must ensure employees only access data necessary for their work tasks and not grant them broad authorization to access all data.

[1] . Paul Kirvan, How can your ransomware backup strategy improve?, Feb 2020. Follow link: https://www.techtarget.com/searchdatabackup/answer/How-can-your-ransomware-backup-strategy-improve?utm_source=google&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lp01252024GOOGOTHR_GsidsDataBackup_ExaGrid_Essential_II0244839_LI2764124&utm_campaign=ExaGrid_EG_sDB_WW&Offer=sy_lp01252024GOOGOTHR_GsidsDataBackup_ExaGrid_Essential_I0244839_LI2764124&gad_source=1&gclid=EAIaIQobChMI5sep5O_IhgMVKwMGAB0gTQXxEAAYAiAAEgLR2PD_BwE

5. Regular Security Auditing

Regular security audits help identify data protection vulnerabilities and subsequently determine the procedures that must be followed to address these points in organisations[1].

Regular verification and adoption of a zero-trust approach contribute to preventing unauthorised access to sensitive data in organisations.

6. Multi-Factor Authentication

A strong password policy is beneficial but should not be relied upon alone. Implementing multi-factor authentication ensures that a password breach alone is insufficient to result in a data breach[2].

The significance of multi-factor authentication arises from the various methods cybercriminals use to obtain login credentials. This authentication method requires employees in organizations or external parties to provide two or more verification factors to confirm their identity before accessing sensitive data or the accounts and applications of the organisation. Instead of merely requiring a username and password to verify the employee's identity, additional information such as a one-time passcode, encryption key or fingerprint is verified.

[1] Kevin Mitch Group, Importance of Data Protection within the Organization, March 2023. Follow link: https://www.linkedin.com/pulse/importance-data-protection-within-organization-kevin-mitch-group/.

[2] How Security Leaders Can Use Multi-Factor Authentication to Protect Sensitive Data. Follow link: https://www.terranovasecurity.com/blog/multi-factor-authentication-protect-sensitive-data.

There are three main types of authentication factors:

- Information known by the employee or external contractor, such as passwords or PIN.
- Things the employee or external contractor knows like encryption codes.
- Something personal such as fingerprint, voice or facial recognition.

7. Adaptive Multi-Factor Authentication

It is also known as risk-based authentication. It is an advanced security technique requiring the employee within the organisation or any external contractors to provide two or more verification factors to access their accounts. It's called "adaptive" because it adjusts authentication factors according to various risks such as device type, access time, network security, employee behaviour patterns, geographic location, operating system and others. This differs from regular multi-factor authentication[1].

For example, some employees work remotely or from home using a laptop and public Wi-Fi network. By implementing multi-factor authentication, the organisation can establish one set of authentication procedures for employees in the event of working from home and a different set in the event of working while traveling.

[1] What is Adaptive Multi-Factor Authentication (MFA)?. FOLLOW LINK: https://www.cyberark.com/what-is/adaptive-mfa/.

8. Third-Party Risk Monitoring

Organisations must consider monitoring third-party risks. Supply chain attacks can occur when a third-party vendor experiences a data breach, leading to widespread data leaks.

Facts and Figures

In 2020, the average cost of a data breach was $3.9 million.

Currently, organisations, especially with the advent of cloud computing, remote work and global supply chain ecosystems, have increased their reliance on third-party services to enhance efficiency, increase productivity and deliver goods and/or services. However, this growing dependence is accompanied by a corresponding rise in cyber threat opportunities related to third parties handling the organisation’s sensitive data.

9. Identifying and Classifying Sensitive Data

Organisations must identify the types of data they manage, such as personal information, financial records, intellectual property and trade secrets. They should classify data according to its importance, sensitivity level and potential impact in case of leakage. Clear guidelines must be established for handling each data classification, ensuring employees understand these protocols.

10. Installing Antivirus and Anti-malware Software

Among the necessary data protection measures, the organisation should install antivirus and anti-malware software and ensure its effectiveness across all endpoints, including servers, desktop computers and laptops. Additionally, this software should be updated regularly to ensure its capability to detect and promptly address vulnerabilities and threats.

11. Incident Response and Data Leakage Detection

This is accomplished by establishing a rapid incident response plan to reduce impact on the organisation. This requires building an effective and cross-functional incident response team, including members from IT, legal affairs, public relations and other relevant departments. The team should develop a clear plan defining roles, responsibilities and procedures to be followed in case of data leakage[1].

[1] Preventing and Detecting Data Leaks: The Complete Guide. Follow link: https://flare.io/learn/resources/blog/data-leakage-prevention/.

Exercises

The exercises are based on the material presented in this booklet and are provided here without answers. The answers are included at the end of the booklet.

Exercise 1

• Choose the correct answer

1. “Shadow IT” means ...

1 Using information technology systems, devices, software, applications, and services without direct authorisation from the organisation’s IT department.

2 An attacker resorting to credential stuffing attacks to guess employee passwords and access the network.

3 An employee intervening directly without the involvement of authorised specialists to address and resolve the issue or tampering with security settings.

4 (1) and (3).

2. Causes of data leakage in organisations include...

1 Incorrect settings or permissions.

2 Keeping an old version of a software.

3 Phishing emails.

4 All the above.

3. Intellectual property includes the following...

1 Confidential research.

2 Test materials.

3 Software source code.

4 Strategic organisational information.

5 All the above.

4. The benefits of data loss prevention tools focus on...

1 Manual data classification, which helps prevent sharing sensitive data with unauthorised persons.

2 Scanning the dark web, regular web and illegal Telegram channels to find data leaks before any cyberattack occurs through them.

3 Enabling organisations to circumvent data protection standards, laws and regulations, with the ability to prepare the falsified reports necessary for the organisation to complete compliance audits.

4 All the above.

Exercise 2

Write “True” for correct statements and “False” for incorrect statements, and correct the false statements

1. Data leakage occurs when critical data is revealed to authorised persons due to errors within the organisation. (......................................)

2. Data breach occurs when an external source breaches the system through a cyberattack. (......................................)

3. Cybercriminals need several data leaks to carry out a massive data breach, posing a serious threat to organisations. (......................................)

4. Ransomware attacks are the most common for obtaining money in exchange for stolen data, especially if organisations don’t have data backups. (......................................)

5 The loss of electronic devices by an employee does not threaten the organisation they work for, as it is difficult for an attacker to access and breach its data. (..............................)

6 It is challenging for cybercriminals to breach organisation data in case of lost electronic devices. (..............................)

7 Employees using personal tools and devices, such as home printers, helps safeguard the organisation against data leaks. (..............................)

8 Password recovery attempts not initiated by the employee are one of the indicators of data leakage. (..............................)

9 Data can be encrypted during transfer between networks, from workplace to cloud, or from device to device within the organisation. (..............................)

Exercise 3

Complete the following statements

1. Data leakage leads to ...., or ...., or ....

2. Types of leaked data in organisations include ...., ...

   , ...

3. Data breaches may result from internal threats related to the organisation, divided into .... carried out by a disgruntled employee, and .... due to weak passwords, and .... which ensures cybercriminals deceive employees within the organisation to help them attack the network and steal data.

4. Organisation data can be protected from leakage through the following steps: ....,

   ...., ...

5. One key factor organisation must consider is .... due to the potential for supply chain attacks, which can result in widespread data leakage.

6. Organisations can benefit from .... that help evaluate and monitor third-party risks.

7. For rapid incident response to reduce impact on the organisation, this requires building .... to develop a clear plan defining roles, responsibilities and procedures to be followed when data leakage occurs.

8. .... is a security solution that works to identify and help prevent unsafe or inappropriate sharing, transferor use of sensitive data.

9. Maintaining .... helps organisations comply with data protection standards, laws and regulations, with the ability to prepare reports needed by the organisation to complete audit processes.

Exercises Answers

Question

Exercise One: Choose the correct answer

Answer

1. Both (1) and (3).
2. All the above.
3. All the above.
4. Scanning the dark web, regular web and illegal Telegram channels to find data leaks before they are used in any cyberattack.

Question

Exercise Two: Write "True" for the true statement and "False" for the incorrect statement, and correct the false statements

Answer

1. **False.** Data leakage occurs when critical data is revealed to unauthorised individuals due to internal errors within the organisation.

2. **True.**

3. **False.** A single instance of data leakage is sufficient to cause a massive data breach, threatening organisations.

4. **True.**

5. **False.** The loss of devices can threaten the organisation, facilitating the attacker's access and breach of its data.

- **6. False.** Losing devices poses a potential data breach.

- **7. False.** Employees using personal tools and devices, such as home printers, to print sensitive organisational data pose a risk. An employee may mistakenly use a USB drive or external storage device containing sensitive information, leading to the device being stolen by unauthorised individuals, thereby exposing the organisation to the risk of data leakage, ransomware attacks and other threats.

- **8. True.**

- **9. True.**

Question

Exercise Three: Complete the following sentences

Answer

1 Data leakage leads to **Identity theft of employees or customers**, **data breaches**, or **installation of malicious software such as ransomware.**

2 Types of leaked date within organisations include **Personally identifiable information**, **financial data**, and **account or login credentials**.

3 Data breaches may result from internal threats related to the organisation, divided into **Malicious attacks** carried out by a disgruntled employee, and, **negligence attacks** due to weak passwords, and **recruitment cases.**which ensures cybercriminals deceive employees within the organisation to help them attack the network and steal data.

4 Organisation data can be protected from leakage through the following steps: **Data encryption**, **data backup**, **defining access controls to data**.

5 One key factor organisation must consider is **Monitoring third-party risks** potential for supply chain attacks, which can result in widespread data leakage.

6 Organisations can benefit from **Risk assessment tools** that help evaluate and monitor third-party risks.

7 For rapid incident response to reduce impact on the organisation, this requires building **An effective cross-functional team including members from IT, legal, public relations, and other relevant departments** to develop a clear plan defining roles, responsibilities and procedures to be followed when data leakage occurs.

8 **Data Loss Prevention (DLP)** is a security solution that works to identify and help prevent unsafe or inappropriate sharing, transfer or use of sensitive data.

9 Maintaining **Regulatory compliance** helps organisations comply with data protection standards, laws and regulations, with the ability to prepare reports needed by the organisation to complete audit processes.

References

1. Data Breach Versus Data Leak: What's The Difference?, 2024. Follow link: https://www.teramind.co/blog/data-breach-vs-data-leak/.

2. What Is a Data Leak? How They Happen and How To Prevent Them. Follow link: https://abnormalsecurity.com/glossary/data-leak.

3. Data Leakage: Common Causes, Examples & Tips for Prevention. Follow link: https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention.

4. Over 500,000 Zoom accounts sold on hacker forums, the dark web. Follow link: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/

5. What Is a Data Breach?. Follow link: https://www.akamai.com/glossary/what-is-a-data-breach.

6. How to Detect a Data Breach (5 Critical Steps). Follow link: https://www.breachsense.com/blog/data-breach-detection/

7. Hackers targeted Twitter employees to hijack accounts of Elon Musk, Joe Biden and others in digital currency scam. Follow link: https://www.cnbc.com/2020/07/15/hackers-appear-to-target-twitter-accounts-of-elon-musk-bill-gates-others-in-digital-currency-scam.html

8. Who should encrypt the data in my company?. Follow link: https://www.sealpath.com/blog/data-encryption-for-enterprises/

9. Paul Kirvan, How can your ransomware backup strategy improve?, Feb 2020. Follow link: https://www.techtarget.com/searchdatabackup/answer/How-can-your-ransomware-backup-strategy-improve?utm_source=google&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lp01252024GOOGOTHR_GsidsDataBackup_ExaGrid_Essential_IIO244839_LI2764124&utm_campaign=ExaGrid_EG_sDB_WW&Offer=sy_lp01252024GOOGOTHR_GsidsDataBackup_ExaGrid_Essential_IO244839_LI2764124&gad_source=1&gclid=EAIaIQobChMI5sep5O_lhgMVKwMGAB0gTQXxEAAYAiAAEgLR2PD_BwE.

10. Kevin Mitch Group, Importance of Data Protection within the Organization, March 2023. Follow link: https://www.linkedin.com/pulse/importance-data-protection-within-organization-kevin-mitch-group/

11. How Security Leaders Can Use Multi-Factor Authentication to Protect Sensitive Data. Follow link: https://www.terranovasecurity.com/blog/multi-factor-authentication-protect-sensitive-dataDavid Shepardson, VW says data breach at vendor impacted 3.3 million people in North America, June 2021. Follow link: https://www.reuters.com/business/autos-transportation/vw-says-data-breach-vendor-impacted-33-million-people-north-america-2021-06-11/.

12. What is Adaptive Multi-Factor Authentication (MFA)?. FOLLOW LINK: https://www.cyberark.com/what-is/adaptive-mfa/

13. Preventing and Detecting Data Leaks: The Complete Guide. Follow link: https://flare.io/learn/resources/blog/data-leakage-prevention/