Database Security

Dias Ilyas

Tenelbek Sabyrov

Timur Zhangazinov

SE-2222

Contents

1. Main Concepts

Types of Security

Threats to Databases

Database Security - Part of a Common System

1. Types of Security

Database Security Issues

Legal and ethical issues on the right to access information - for example, some information may be considered **confidential** and may not be legally accessible to outside organizations or persons.

Policy issues at the governmental, institutional or corporate level regarding which types of information should not be publicly available, such as **credit ratings** and **personal medical** records.

Systemic problems, such as system **levels**, at which various security functions should be performed, for example, whether the security function should be handled at the physical hardware level, at the operating system level, or at the DBMS level.

The need for some organizations **to identify multiple levels of security** and classify data and users based on these classifications - for example, **top secret, secret, confidential and unclassified**. An organization's security policy that allows access to various data classifications should be mandatory.

Kaspi.kz

Company that we have analyzed

Kaspi+Egov

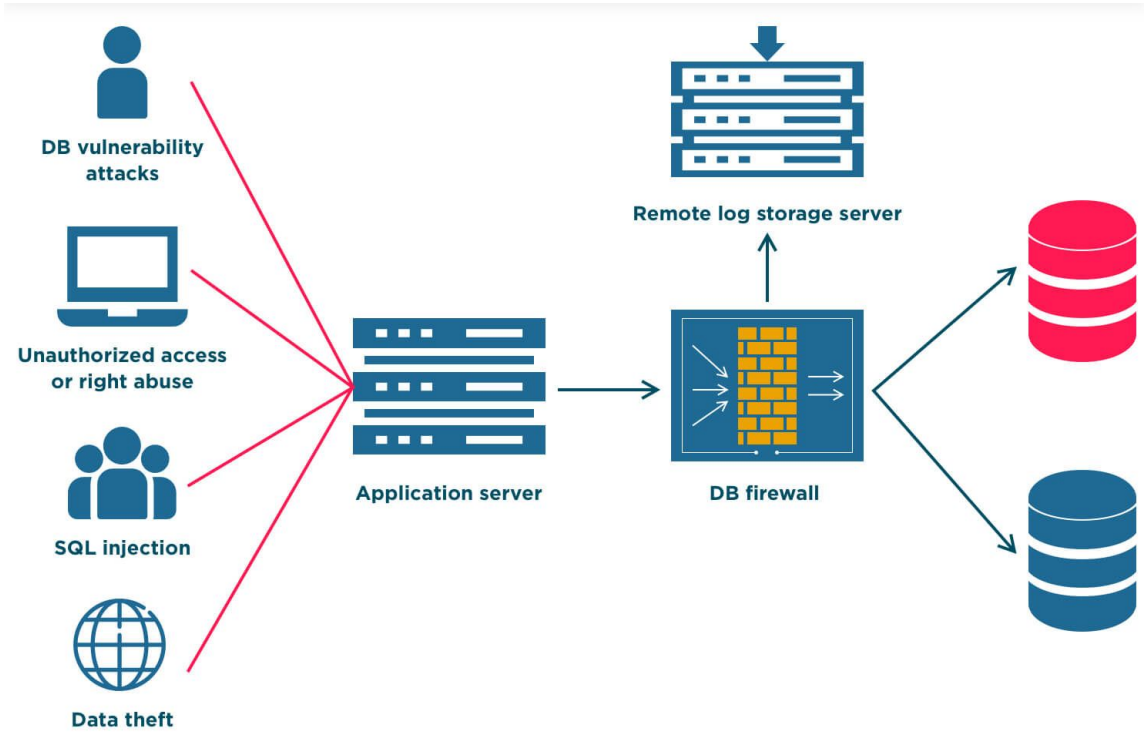

15:20
Госуслуги, штрафы, налоги
Поиск по Госуслугам
Цифровые документы
Оформить пособие
Получать все свои пособия на Социальный Счет в Kaspi.kz
Социальный Счет
ASHYQ. Сатус по коронавирусу
Штрафы
Налоги
Платежи для ИП

Threats to Databases

Loss of integrity. Database integrity refers to the requirement to **protect** information from **incorrect changes**.

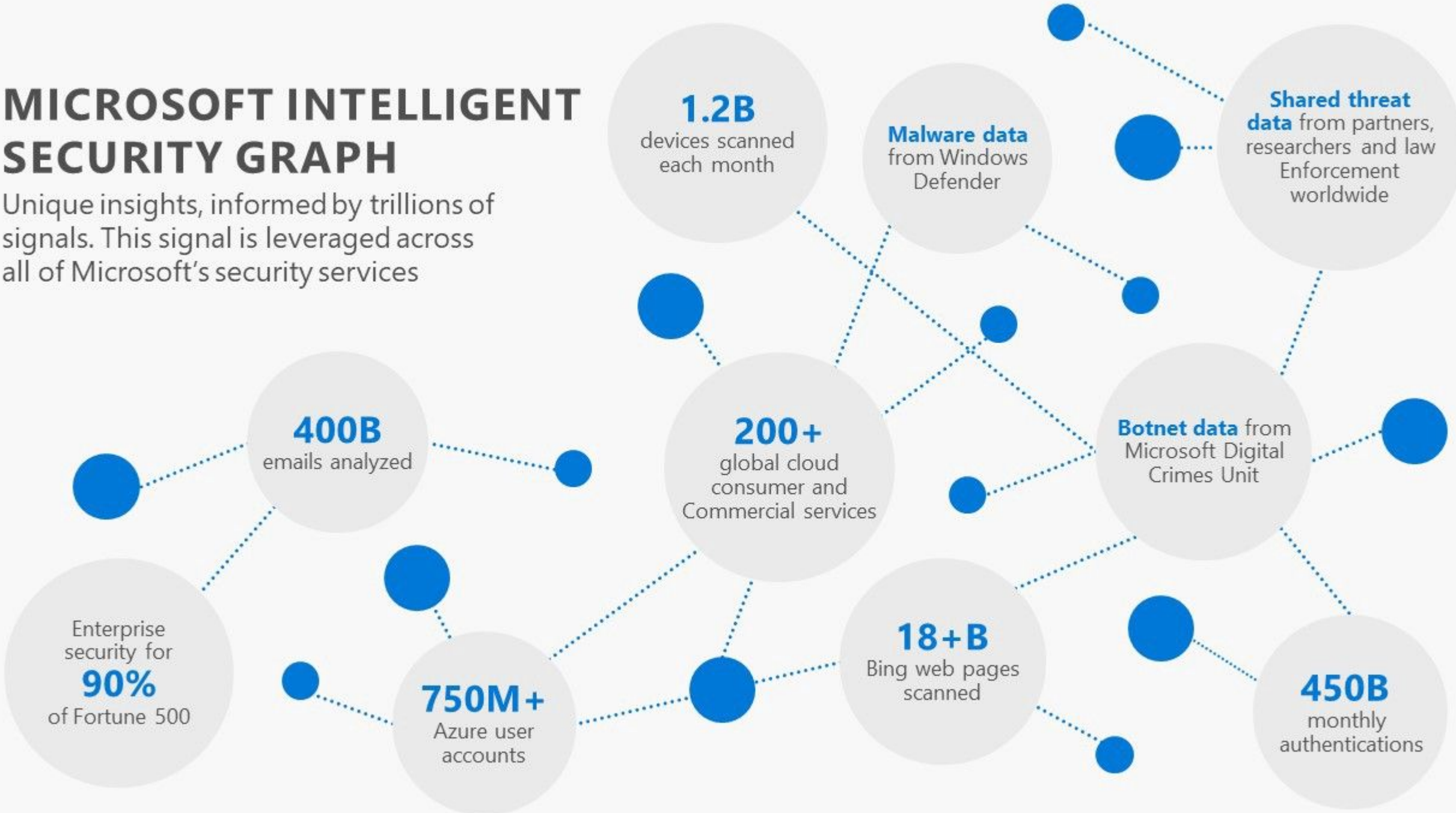
Loss of availability. Database availability means the accessibility of objects to a user or program that has a **legal right** to these data objects.

Loss of confidentiality. Database confidentiality refers to the protection of data from unauthorized disclosure.



MICROSOFT INTELLIGENT SECURITY GRAPH

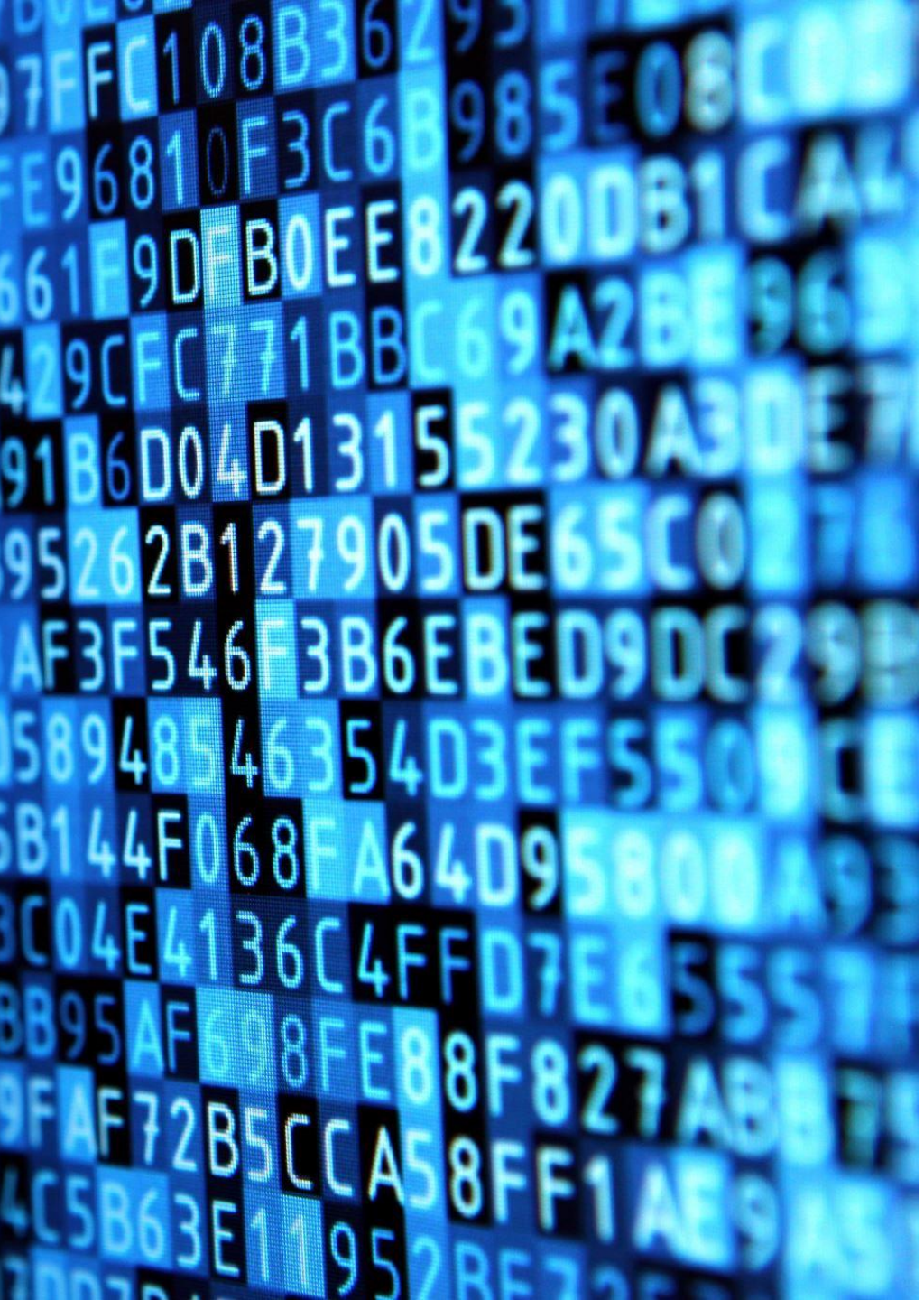
Unique insights, informed by trillions of signals. This signal is leveraged across all of Microsoft's security services



2. Control Measures

Access control

- It includes two main components: authentication and authorization.
- **Authentication** is a method of verifying the identity of a person who is accessing your database.
- **Authorization** determines whether a user should be allowed to access the data or make the transaction he’s attempting.



5. Data encryption

- **Database encryption** is the process of converting **data**, within a **database**, in plain text format into a meaningless cipher text by means of a suitable algorithm.
- **Database decryption** is converting the meaningless cipher text into the original information using keys generated by the **encryption** algorithms.

Common threats and challenges

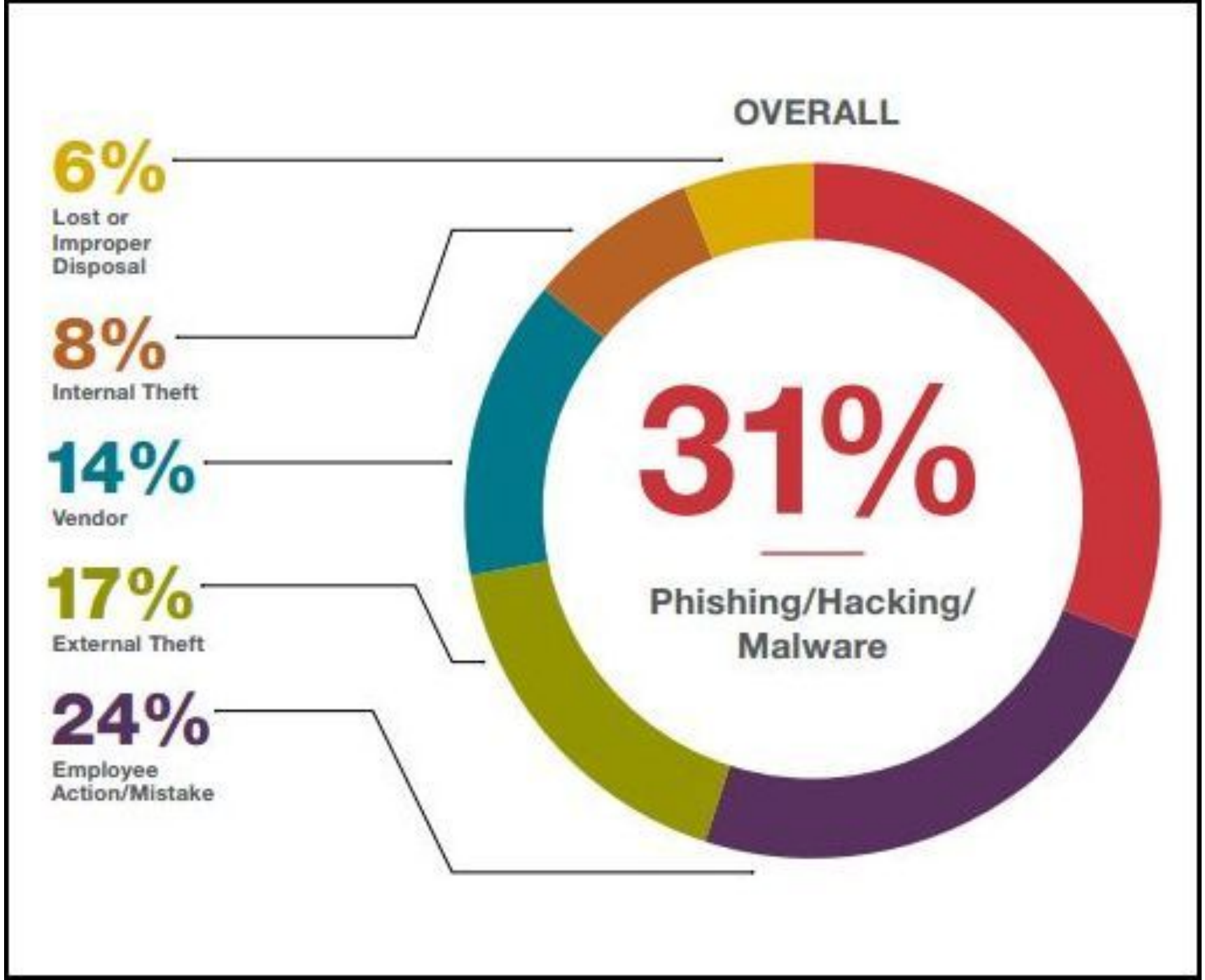
1. Human error
2. Exploitation of database software vulnerabilities
3. Denial of service (DoS/DDoS) attacks
4. Malware
5. Attacks on backups

Americans Worried About Data Security on Social Media

% of U.S. internet users who are very worried about data security on following platforms

* Online services
On a scale of 1 to 10 (1=not at all, 10=very much):
How much do you worry about the security of your personal data with...?
Answer shown: very much (10–8)
Survey of 1,037 U.S. residents 16 years and older in May 2017

Source: Statista survey


OVERALL
6%
Lost or Improper Disposal
8%
Internal Theft
14%
Vendor
17%
External Theft
24%
Employee Action/Mistake
31%
Phishing/Hacking/ Malware

Human error

- Accidents,
- weak passwords,
- password sharing,

•and other unwise or uninformed user behaviours continue to be the cause of nearly half (49%) of all reported data breaches.

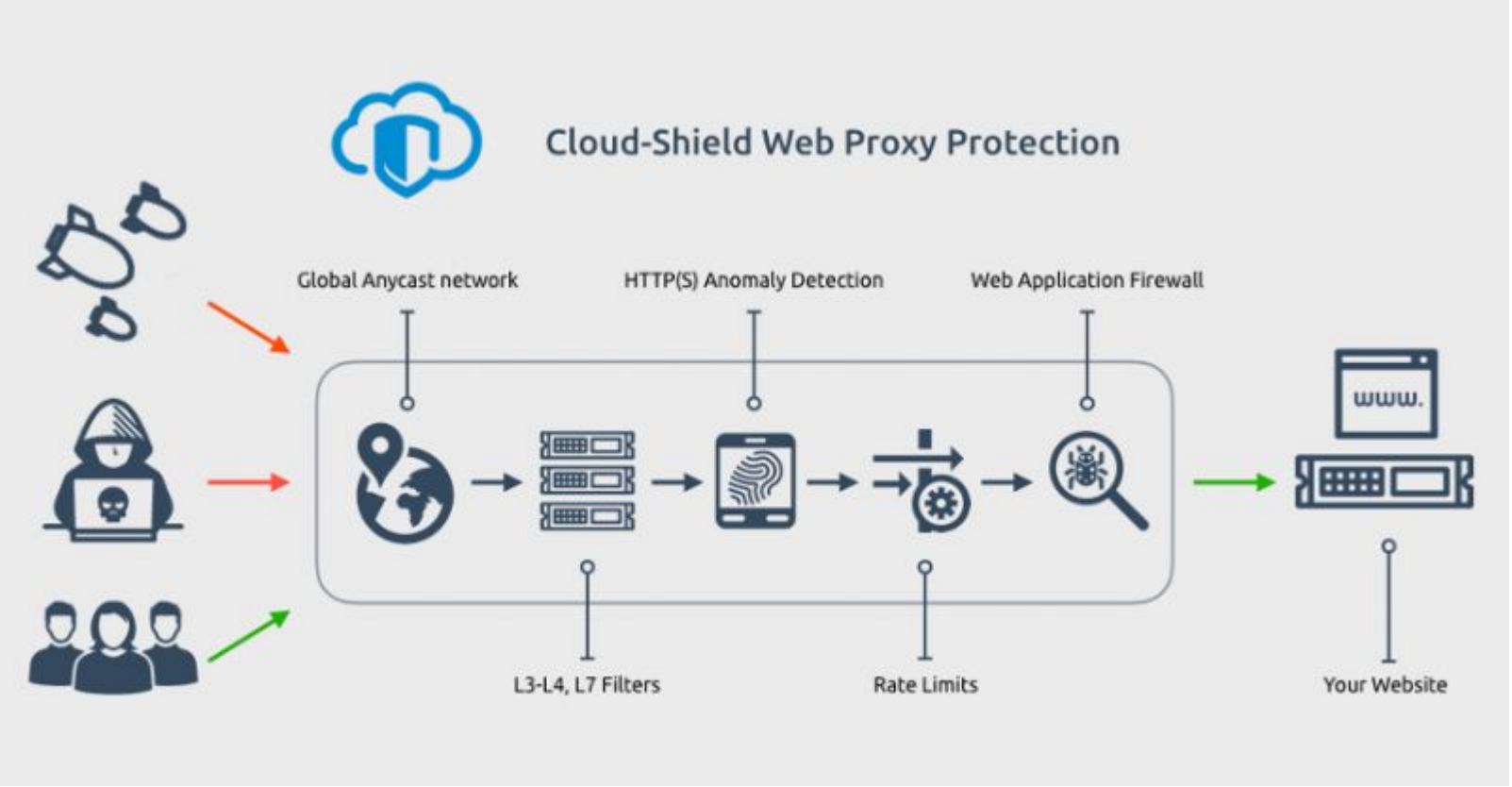
Denial of service (DoS/DDoS) attacks

In a **denial of service** (DoS) attack, the attacker floods the target server — in this case, the database server — with so many queries that the server can no longer perform legitimate queries from real users, and in many cases the server becomes unstable or crashesor making it extremely slow.

In a **distributed denial of service** (DDoS) attack, a stream arrives from multiple servers, making it difficult to stop the attack.

DoS/DDoS Attacks Solutions:

- security patches for operating systems,
- router configuration,
- firewalls
- intrusion detection systems.



Malware

•**Malware** is software written specifically to exploit vulnerabilities or otherwise cause damage to the database. Malware may arrive via any endpoint device connecting to the database's network.

•**Malware Solutions**:
•A range of antivirus software, firewalls and other strategies are used to help protect against the introduction of malware, to help detect it if it is already present, and to recover from malware-associated malicious activity and attacks.

8. Attacks on backups

Threats are compounded by the following:

Growing data volumes: Data capture, storage, and processing continues to grow exponentially across nearly all organizations. Any data security tools or practices need to be highly scalable to meet near and distant future needs.

Cybersecurity skills shortage: Experts predict there may be as many as 8 million unfilled cybersecurity positions by 2022..

Encryption, software and applications

- **Encryption:** ALL data—including data in the database, and credential data—should be protected with best-in-class encryption while at rest and in transit.
- **Database software security:** Always use the latest version of your database management software, and apply all patches as soon as they are issued.
- **Application/web server security:** Any application or web server that interacts with the database can be a channel for attack and should be subject to ongoing security testing and best practice management.

Backup and Auditing

Backup security: All backups, copies, or images of the database must be subject to the same (or equally stringent) security controls as the database itself.

Auditing: Record all logins to the database server and operating system, and log all operations performed on sensitive data as well. Database security standard audits should be performed regularly.

https://www.ibm.com/cloud/learn/database-security

Literature

1. Ramez Elmasri, Shamkant B. Navathe. Fundamentals of database systems: Sevens edition. - Pearson Education, 2016. – 1273 p.

2. Database Security. https://www.ibm.com/cloud/learn/database-security

3. SQL Server Security. https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/sql/sql-server-security

4. Ethical Hacking. https://www.guru99.com/what-is-hacking-an-introduction.html