II

OBJECTIVE #1:
DATA SECURITY

PROBLEM

THE MAIN REASON WHY SECURITY MEASURES CAN FAIL TO PROTECT COMPUTER SYSTEMS IS that most specialists and users don't understand what computer system security is:

Unaware of what they're facing, they can't tackle problems competently

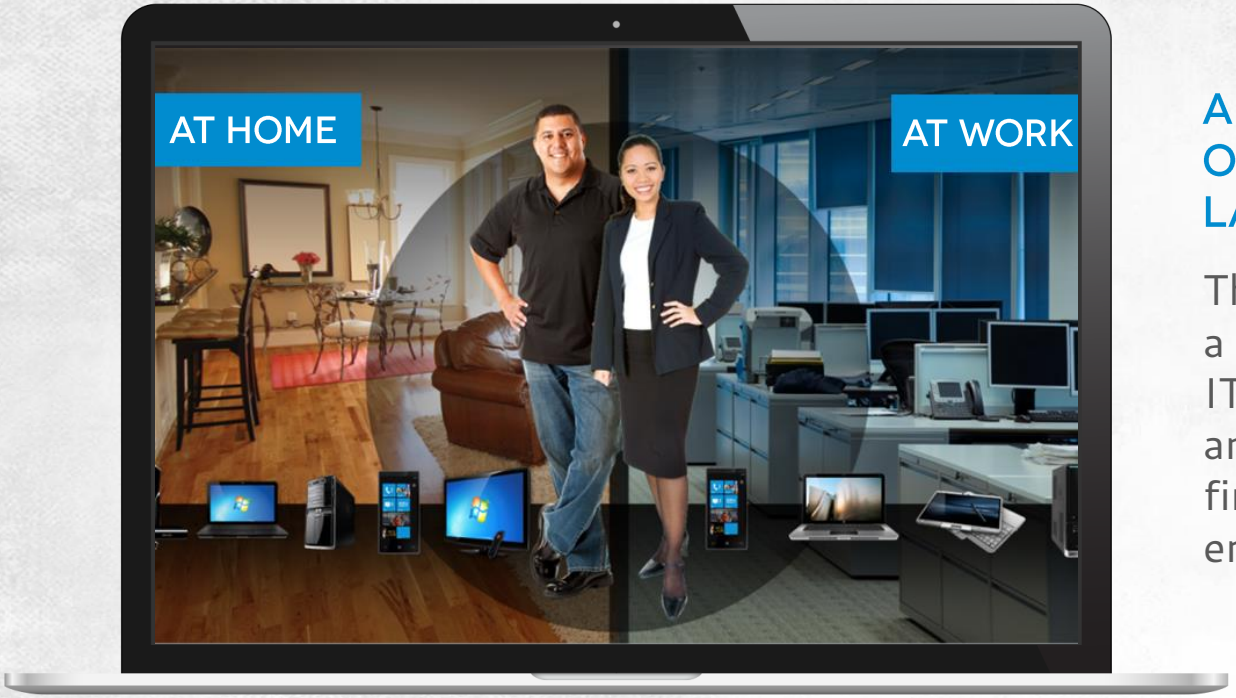
Not knowing what resources need safeguarding, they can't protect them competently

PROBLEM

NOT KNOWING HOW SECURITY MEASURES work and how they are interdependent, they don't understand their limitations

Unaware of new trends, they can't protect the ever-evolving computer systems or prevent them from new cyber threats

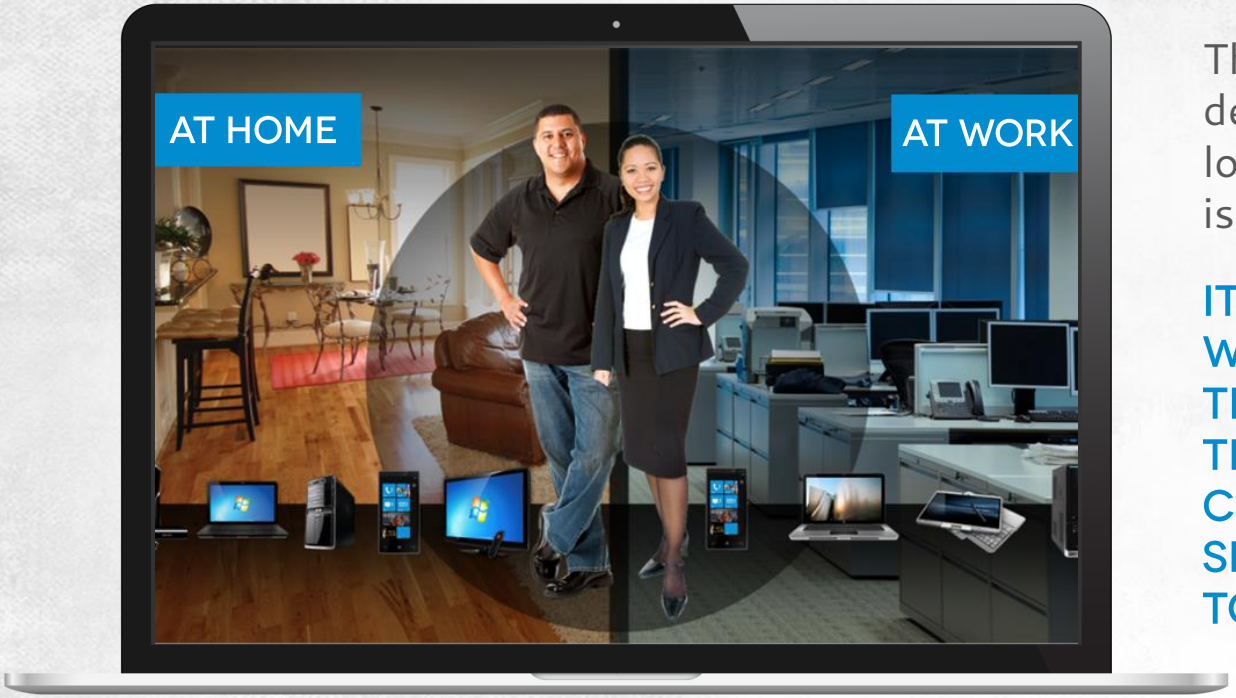
CONSUMERISATION OF IT



A TREND THAT'S BEEN OBSERVED OVER THE LAST COUPLE YEARS.

The consumerisation of IT is a recent change where new IT technologies are sold to and aimed at consumers first, and only later employed in business

CONSUMERISATION OF IT



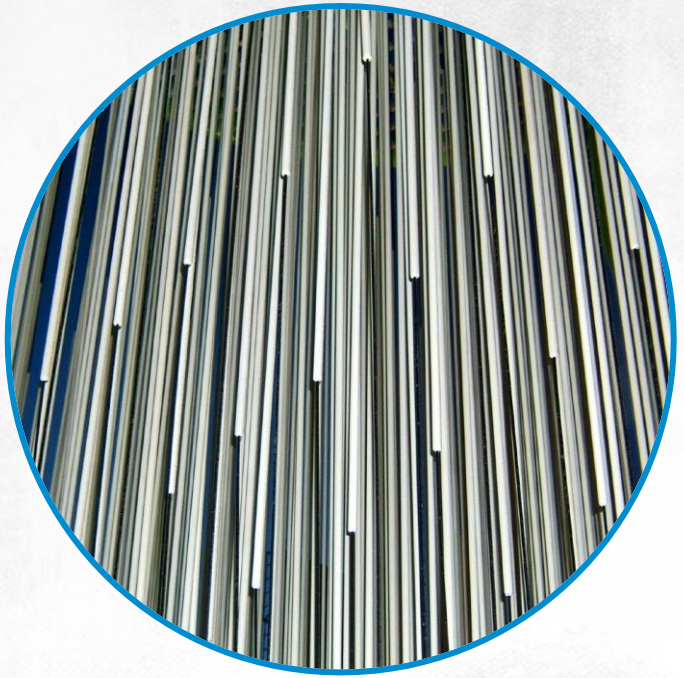
The paradigm of software development has shifted: no longer device-orientated, it is now user-focused

IT WAS CYBERCRIMINALS WHO FIRST UNDERSTOOD THE IMPLICATIONS OF THIS REVERSAL FOR COMPUTER SYSTEM SECURITY AND STARTED TO EXPLOIT IT

APT: ADVANCED PERSISTENT THREAT

The term APT was coined and defined in 2006 by the American military, originating as a response delivered for the Department of Defense upon the realization that the then-existing computer security models were ineffective when faced with the new cyber threats

INITIALLY, THE TERM WAS USED FOR COMPLEX, COORDINATED AND SYSTEMATIC EFFORTS THAT BYPASSED EXISTING SECURITY MEASURES AND WERE LAUNCHED AGAINST THE US GOVERNMENT AND AMERICAN CORPORATION COMPUTERS



APT: ADVANCED PERSISTENT THREAT

ADVANCED PERSISTENT THREATS ARE:

Internal attacks, launched from within the organization, for example by dishonest employees or rogue counterparties. They include social engineering attacks and may occur when an attacker takes a position in the company

Launching malicious software downloaded from the Internet on targeted machines

Remote attacks, mass attacks exploiting known security holes, attacks making use of a target service being run on a server with other services provided, public cloud attacks, wireless network hacking, mobile devices hacking

APT: ADVANCED PERSISTENT THREAT

ADVANCED PERSISTENT THREATS ARE:

Local attacks launching malware

Trusted path attacks. This type of attacks uses stolen, intercepted credentials that allow an attacker to make a VPN connection and gain control over an authenticated host that can establish a remote connection to intercept and eavesdrop on transmissions between companies or company departments and to break into partner companies.

CONFIDENTIALITY

Ensuring the confidentiality of data means precluding unauthorized persons from obtaining information which they are not supposed to have
Based on their level of sensitivity, information may be:

PUBLIC:

accessible to everyone

INTERNAL:

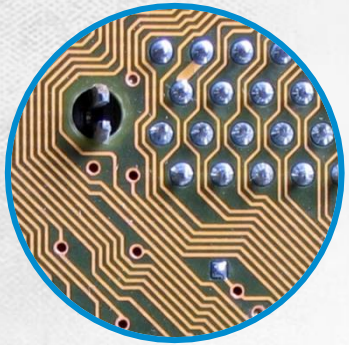
accessible to all employees in a company, selected counterparties and clients

Disclosure of internal information does not compromise the security of the entire system directly

PERSONAL:

personally identifiable information that identifies a person uniquely

CONFIDENTIALITY



SENSITIVE:

data that, if disclosed, could bring direct losses to the company or person it relates to

Includes personal info like health details and preferences, financial data like contract clauses

CLASSIFIED:

if disclosed, this category of data would spell a disaster for a company or its computer system

This category includes user passwords and documentation relating to products to be launched on the market

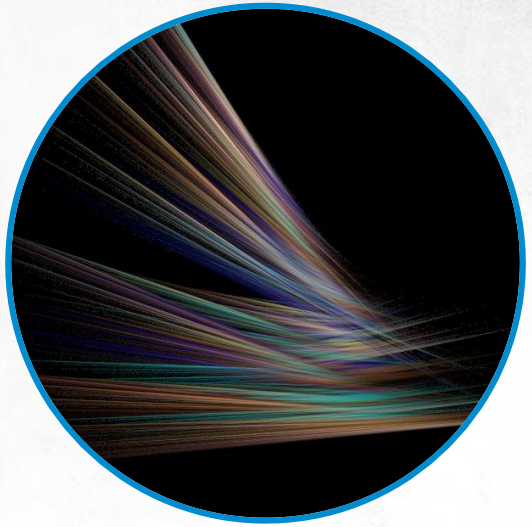
NEGLIGING DATA CONFIDENTIALITY CLASSES LEADS TO THE INTERNET BEING FULL OF NOT ONLY OF PUBLIC INFO, BUT ALSO PRIVATE, SENSITIVE AND EVEN CLASSIFIED DATA

CONFIDENTIALY

EXERCISE

How much classified and security-critical information may be found on the Internet?

IF YOU PUT SOMETHING ON THE INTERNET,
it stays there forever www.archive.org
Google Hacking:

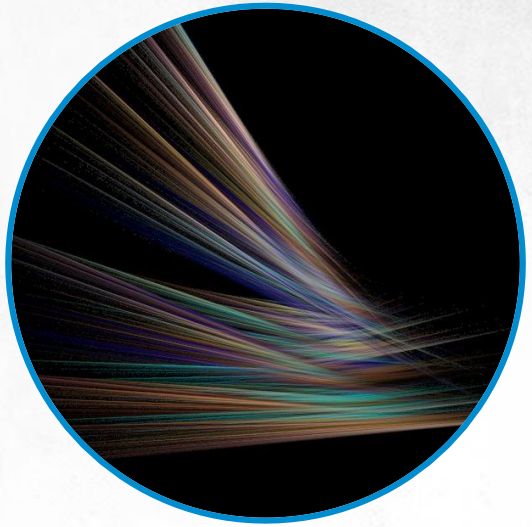


- Site:com filetype:xls "Accounts„
- Site:gov.pl filetype:xls users
- Site:gov.pl filetype:doc employees
- filetype:ini WS_FTP PWD
- site:pl "index of /" password.txt
- filetype:txt inurl:"account|users|admin| administrators|passwd|password"

EXERCISE

How much classified and security-critical information may be found on the Internet?

- site:dk +hotel filetype:xls
- Site:mil filetype:pdf "Top Secret„
- site:com +password filetype:xls
- Inurl:admin users passwords
- inurl:admin intitle:index.of
- camera linksys inurl:main.cgi
- "Toshiba Network Camera - User Login„

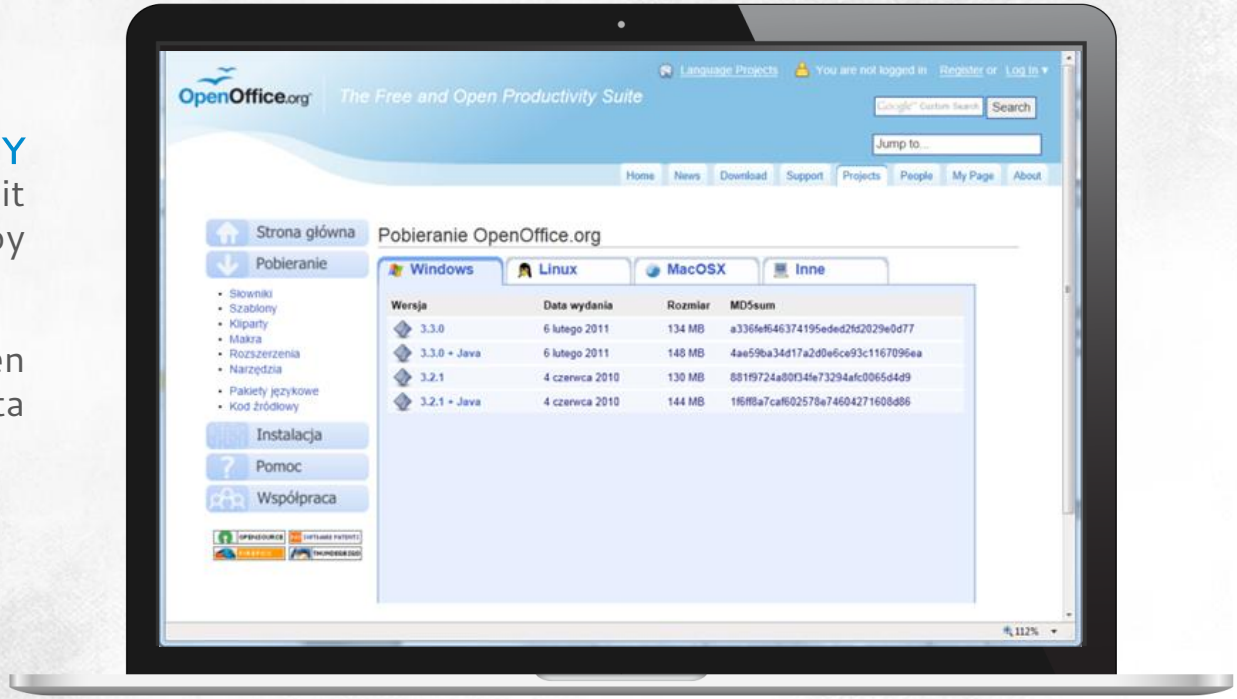


SPECIALIZED TOOLS (GOOLAG SCANER, BIDIBLAH, FOCA)

INTEGRITY

ENSURING THE INTEGRITY OF DATA means protecting it against being modified by unauthorized persons

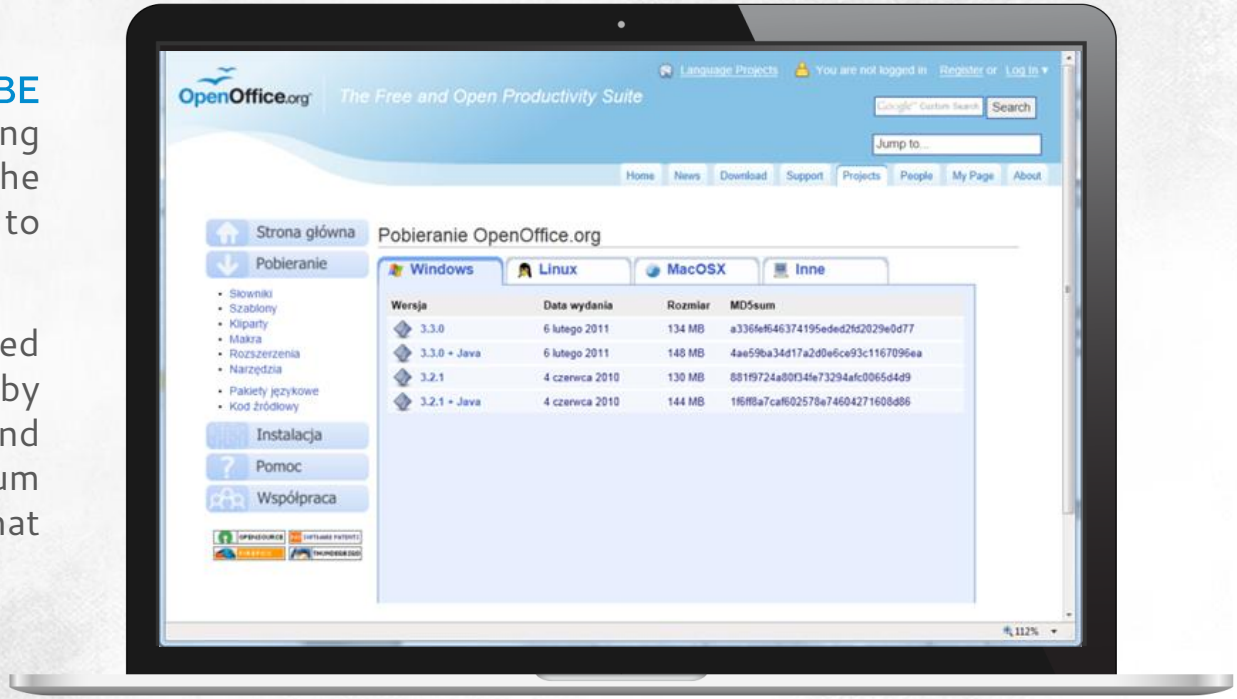
Integrity may be often seen as more important than data confidentiality



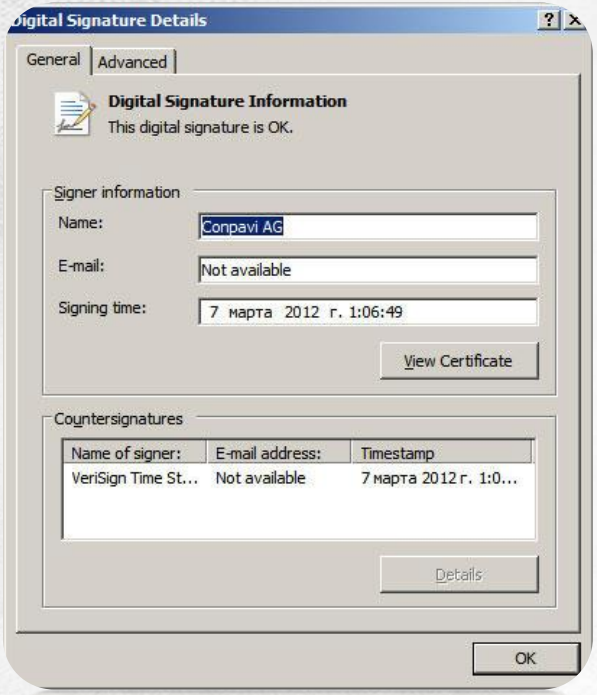
INTEGRITY

DATA INTEGRITY CAN BE MAINTAINED by adding checksums to the data: the easiest way to do that is to share them along with files

Before you open a downloaded file, check its integrity by calculating the checksum and comparing it with the checksum provided by the company that sent or shared the file



AUTHENTICITY



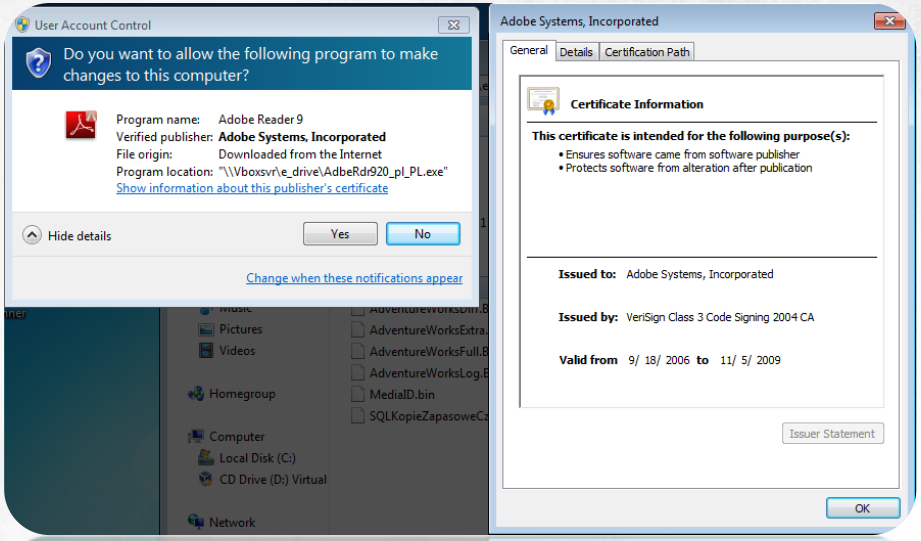
ENSURING DATA AUTHENTICITY MAY BE HARDER TO DO.

Apart from ensuring data accuracy and integrity, you make sure the source of the information is really what it claims to be

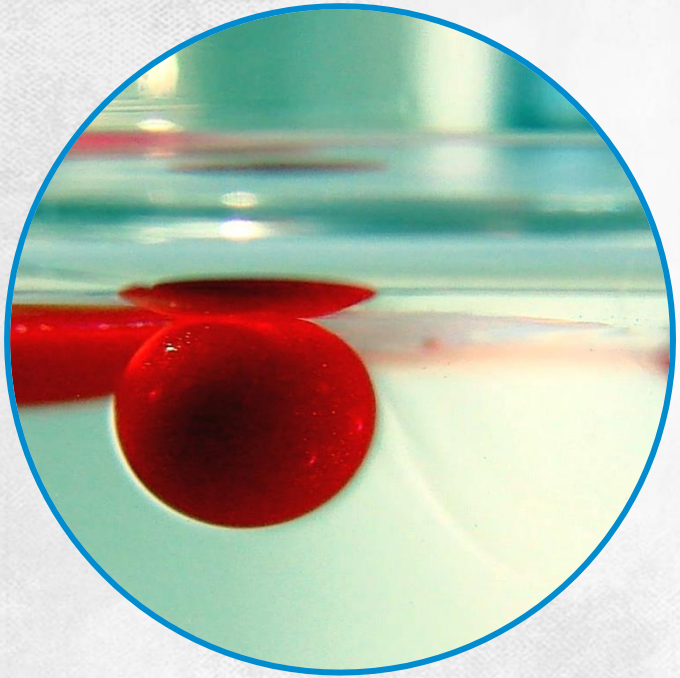
AUTHENCITY

TO ENSURE THE AUTHENTICITY OF A DATA STREAM, YOU SHOULD ADD A CHECKSUM TO IT THAT IS ENCRYPTED USING A SENDER'S PRIVATE KEY

This method is used to sign programs and email messages using certificates of their senders



AVAILABILITY



AVAILABILITY MEANS A SERVICE CAN BE ACCESSED AND USED BY ITS INTENDED AUDIENCE WITHOUT TROUBLE

A constantly available service is a service safeguarded by appropriate solutions: making a service highly available is a process that should be consulted with their users

A SLA (Service Level Agreement) is a contract ensuring the high availability of a service

AVAILABILITY

The two most important elements of an SLA

Observing the RTO (Recovery Time Objective), or the duration of time when a service may be unavailable. It is usually expressed in a number of nines:

Five nines means you guarantee that the service will be available 99,999% of the time (can only be down for five minutes in a year)

Four nines is 52.5 minutes of downtime in a year

Three nines is 8 hours and 45 minutes of downtime in a year

AVAILABILITY

The two most important elements of an SLA

Observing the RPO (Recovery Point Objective), or the maximum tolerable period in which data may be lost in the case of a disaster

This is expressed in the number of transactions lost or the period in which data may be lost

Many SLAs guarantee a RPO that equals zero

AVAILABILITY

The two most important elements of an SLA

The following high availability solutions are often deployed:

Cluster services

Hardware solutions protecting data through backups

Replicating servers that provide a service

THANKS