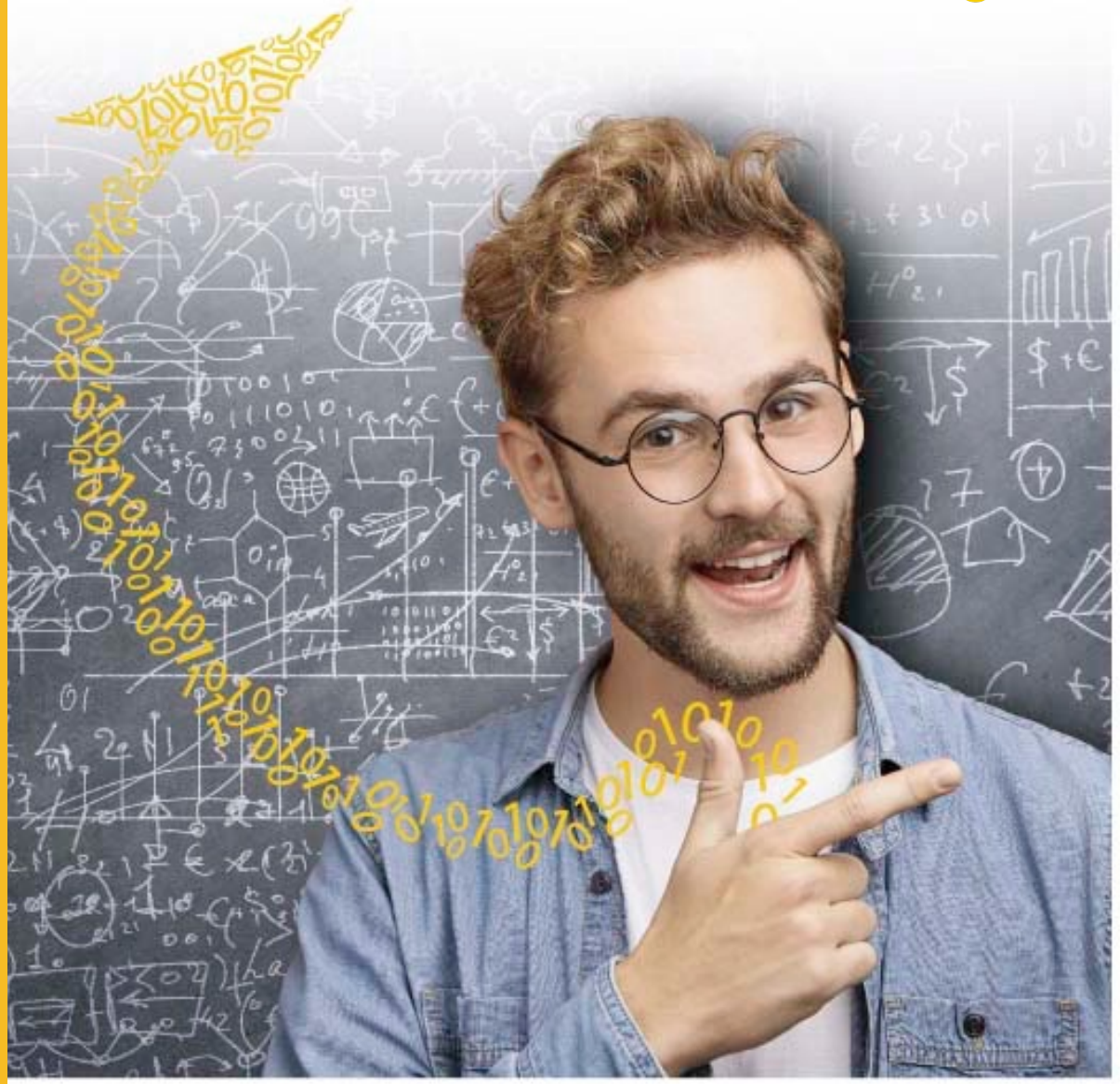
Information Security Management (ISM)



KNOWDigital

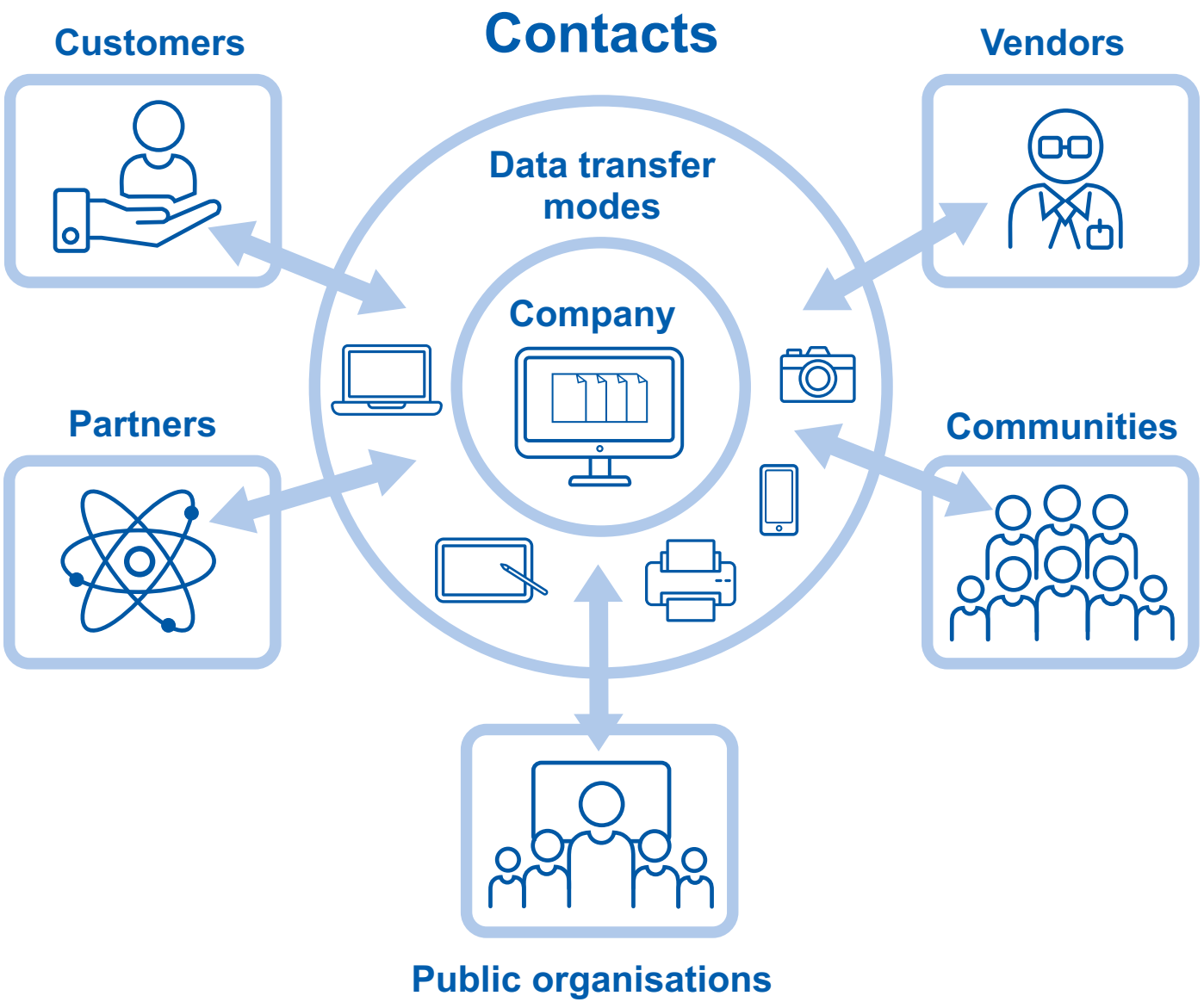
April 13, 2022

Lionel Pilorget

Agenda

- Rationale for Information Security
- The psychology of hacking
- Attack techniques
- Main protections
- Norms and Standards
- Preparing the organization

Various interactions with external agents



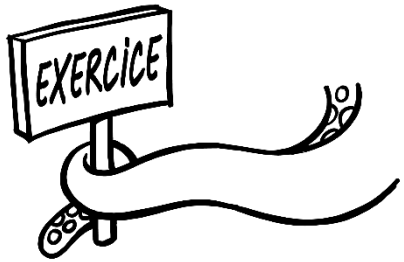
Requirements for information and communication

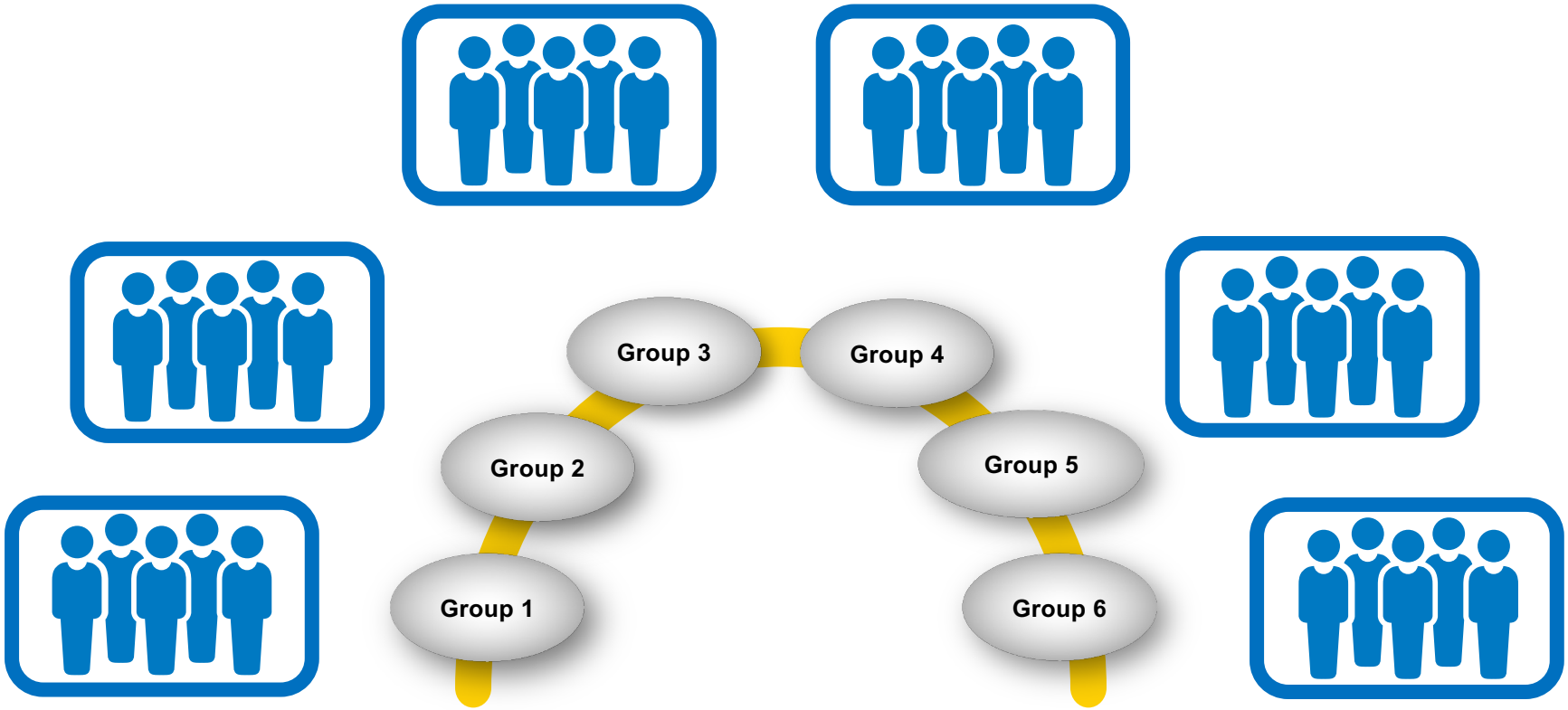
- Accessibility
- Completeness
- Availability
- Response Time
- Easiness
- Privacy
- Compatibility

Exercise

Define key elements to be protected for the following organizations

1. University
2. Bank
3. Hospital
4. Consultancy Company
5. Movie Producer
6. Pharma Company





Why is Cybersecurity a major issue?

Cyberattacks are now the greatest operational risk to the financial system

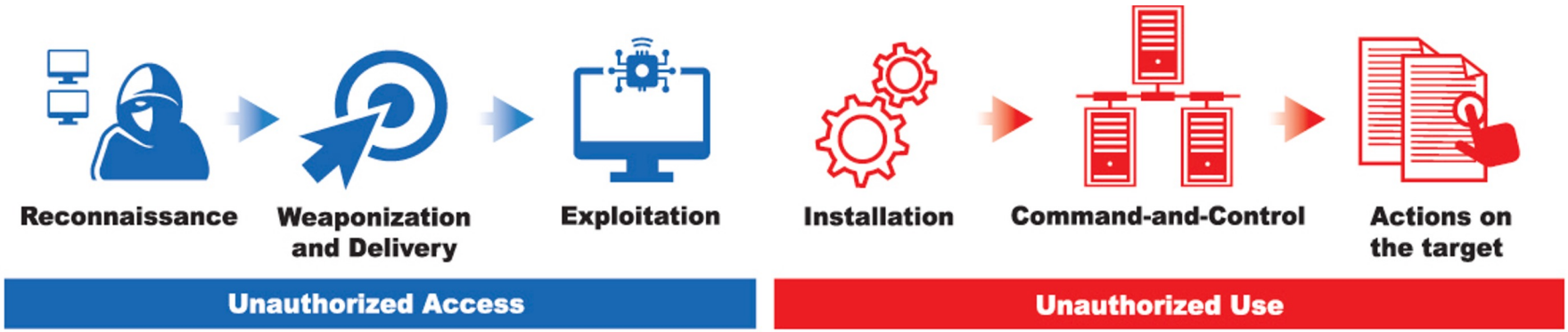
«Cyberangriffe sind inzwischen das grösste operationelle Risiko für das Finanzsystem», Mark Branson

Source: www.finma.ch/de/dokumentation/dossier/dossier-cyberrisiken/

Cyber attack maps

Source: threatmap.bitdefender.com

The Cyber Kill Chain



Exploit a vulnerability

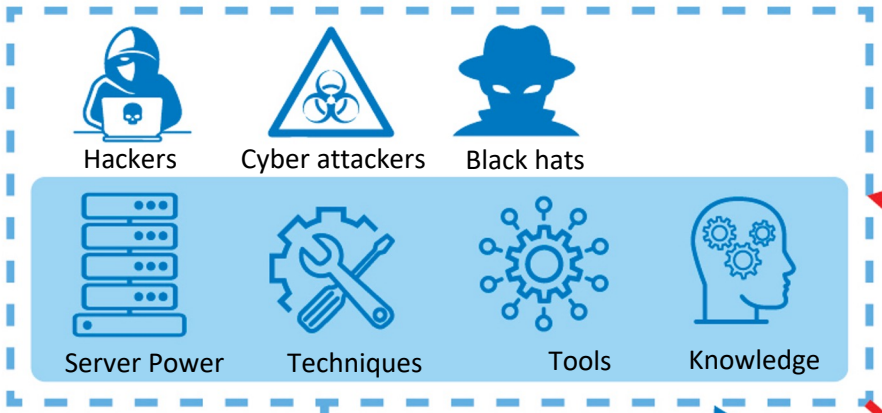
- Malicious data file that is processed by a legitimate application (for insfance Acrobat leader, Chrome…)
- Takes advantage of a vulnerability in the legitimate app which allows the attacker to run code
- 'Tricks' the legitimate application into running the attacker's code
- Small payload

Execute Malicious Activities

- Malicious code in an executable file
- Does not rely on any application vulnerability
- Already executes code and aims to control the machine
- Large payload

Identify the weaknesses

Exploit, Identify the Weaknesses and Damage



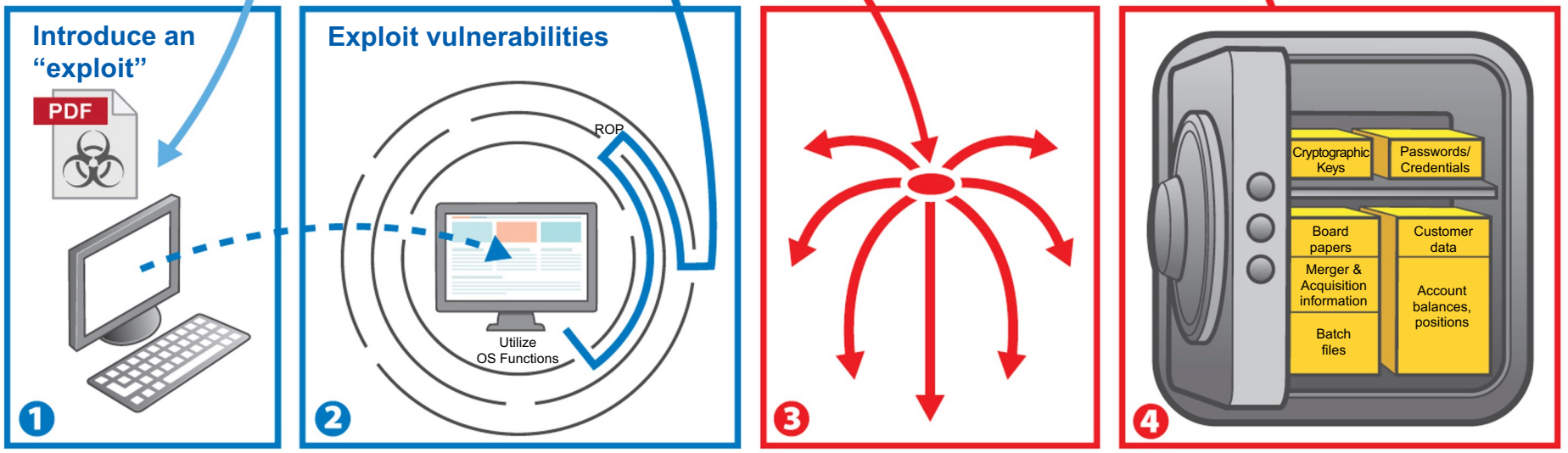
1/ Introduce a virus
2/ Exploit vulnerabilities
3/ Introduce a virus and deploy the attack
4/ Execute the virus and get critical assets

identify the target and pairing a malicious code with an exploit to create a weapon

get authorized accesses to applications

deploy the attack to command and control

achieve the objectives of the intrusion (data copy, data destruction, ransom…)



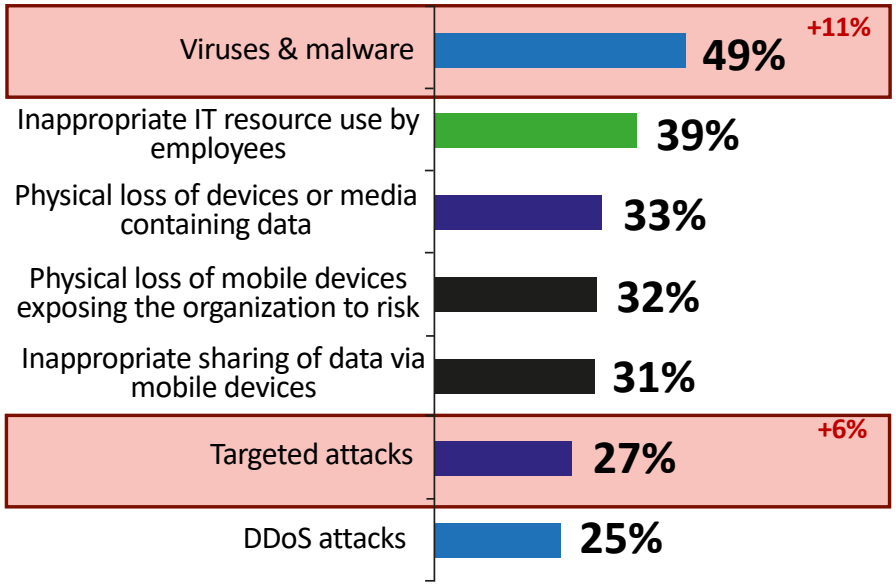
OS: Operating System
ROP: Return Oriented Programming

Which attack techniques have you experienced?

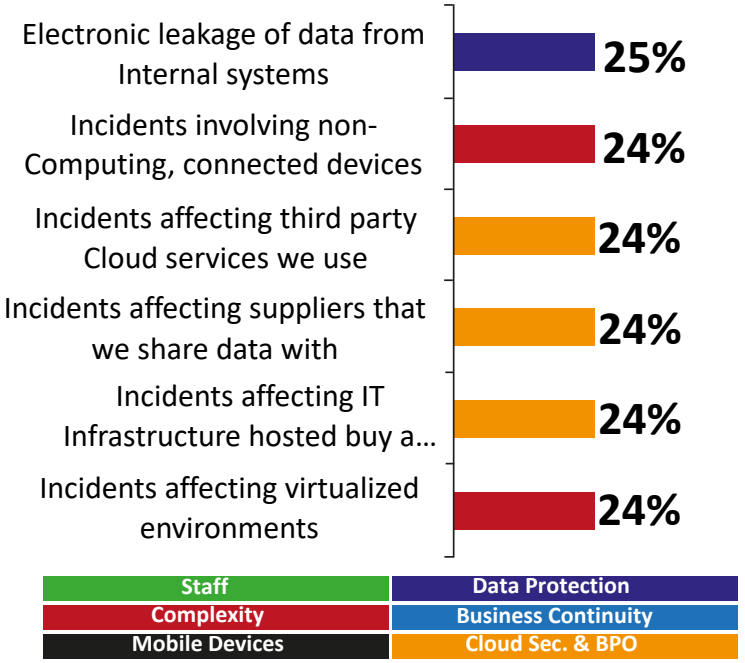
TYPES OF SECURITY EVENT EXPERIENCED

The proportion of businesses reporting experiencing an attack rose significantly to 77% this year.
In fact, **all types of attack showed a significant increase**

% of all businesses experiencing each type of security event



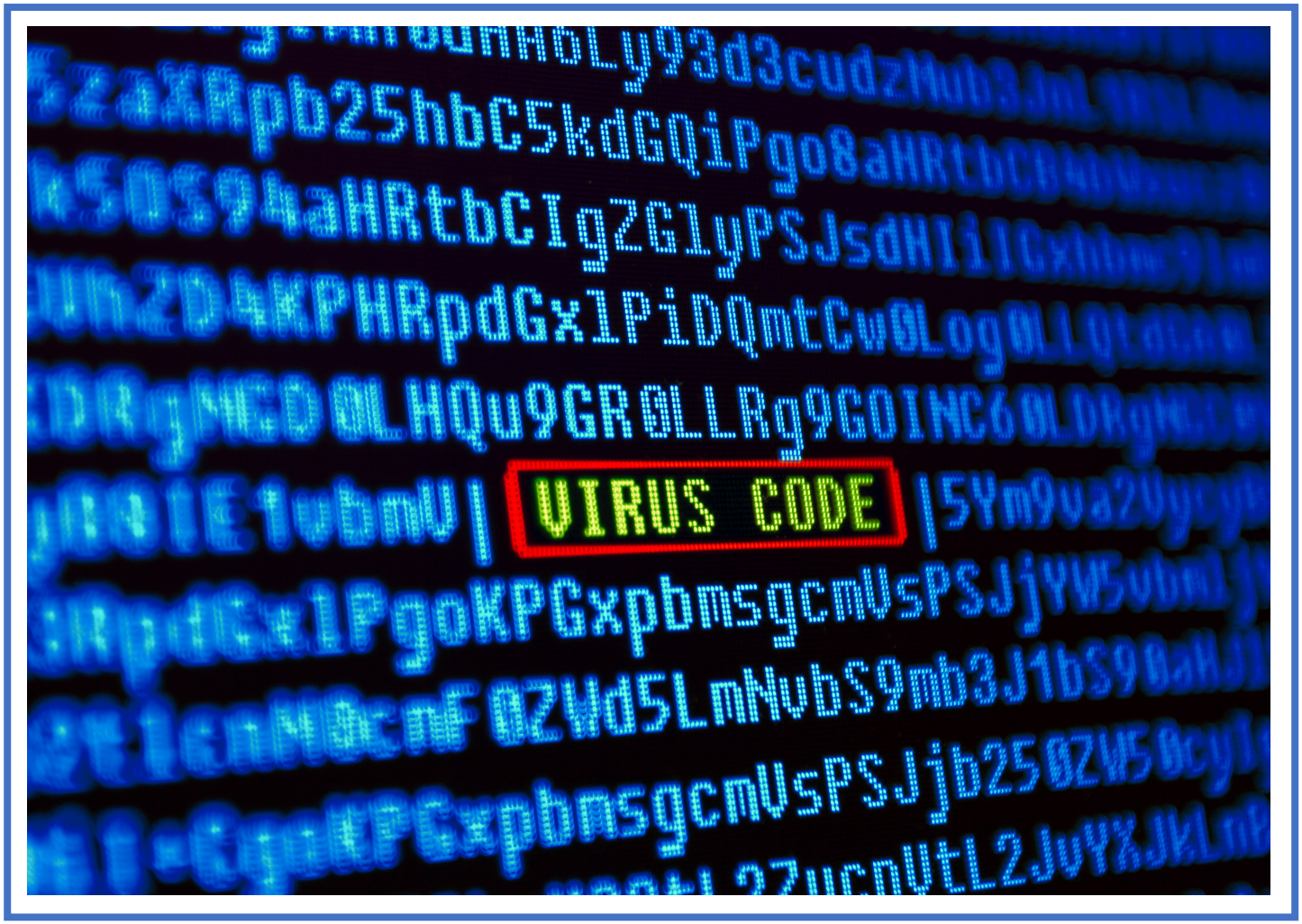
These incidents in particular saw a Large increase



Base : 5,274 *All Respondents*

Source: media.kasperskycontenthub.com

And the winner is



What is a computer virus?

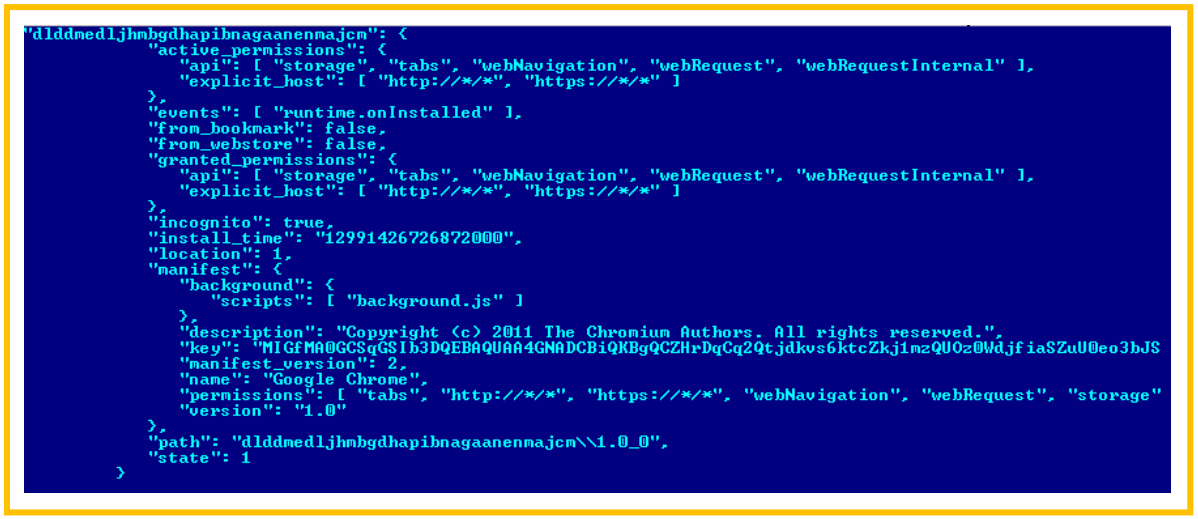
A "**virus**" is the generic term for an unwanted program that spreads itself and causes damage on the infected computer. Computer viruses generally require a host program, where its own code is written and executed first.

Many viruses are programmed in such a way that after installation on a computer they automatically spread to all addresses stored in the e-mail address book and according to this snowball system they spread at lightning speed.

Often, the entire software of the infected computer has to be reinstalled to get rid of the virus. If entire companies are affected by such an incident, the damage can be extensive.

Different types of virus:

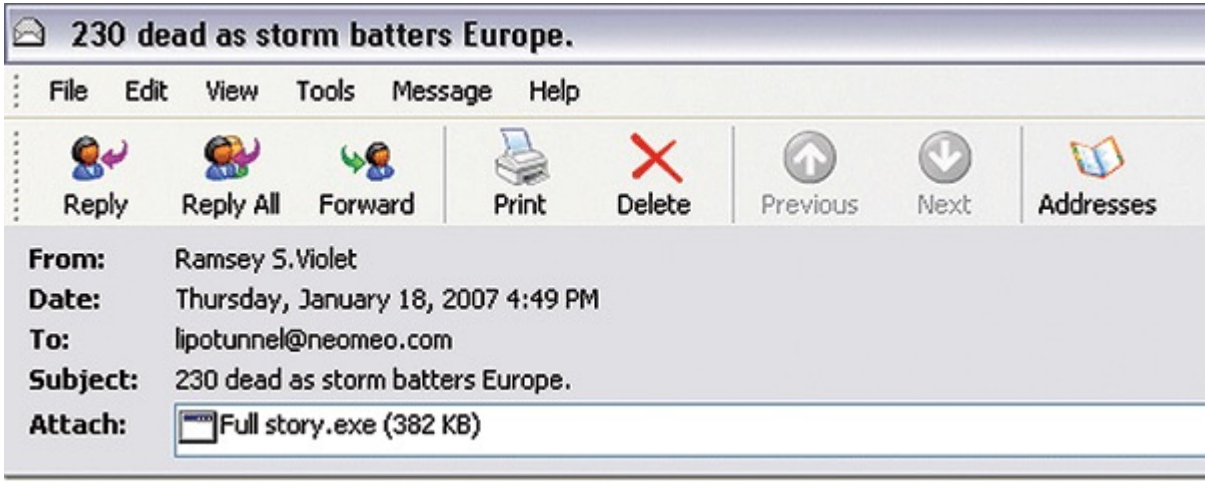
File-infecting Virus
Ransomware
Macro Virus
Browser Hijacker
Web Scripting Virus
Boot Sector Virus
Polymorphic Virus
Resident Virus
Multipartite Virus



Computer worm

A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers. Worms do not passively wait to be spread by a user on a new system, but actively try to penetrate new systems. They do it by exploiting security problems on the target system, especially network services.

A **helpful worm** or **anti-worm** is a worm designed to do something that its author feels is helpful, though not necessarily with the permission of the executing computer's owner.



Source: en.wikipedia.org/wiki/Computer_worm

A Trojan horse

A **Trojan horse** is a destructive program that looks as a genuine application. One function could be to execute a virus. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

Trojans are often infiltrated as an authentic-looking email attachment of a phishing email or as freeware and shareware downloaded from the Internet. The Trojan is introduced with a fake file name and often with a double extension. For example, it would look like this: "suesse-katze.mp4.exe“

A Trojan only starts working once the user launches the program. Thus, once the program starts, the Trojan can install other software on the computer.

Famous computer virus

Onel de Guzman

Reonel Ramones

- **Mydoom:** spread by mass emailing. At one point, the Mydoom virus was responsible for 25% of all emails sent
- **Sobig**
- **Klez** infected about 7.2% of all computers in 2001 (7 million PCs)
- **ILOVEYOU** sent copies of itself to every email address in the infected machine's contact list
- **WannaCry** takes over your computer and holds it hostage
- **Zeus** an online theft tool

Source: www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history

Phishing

Phishing is a variant of e-mail abuse. Phishing e-mails feign a reputable origin, e.g. from banks, the post office, DHL, etc., and ask the recipient to enter personal data, passwords, credit card numbers and PIN codes.
To do this, the recipient is either directed to a prepared website or a corresponding form in the mail takes the data.

This is to notify all Students, Staffs of University that we are validating active accounts.

Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

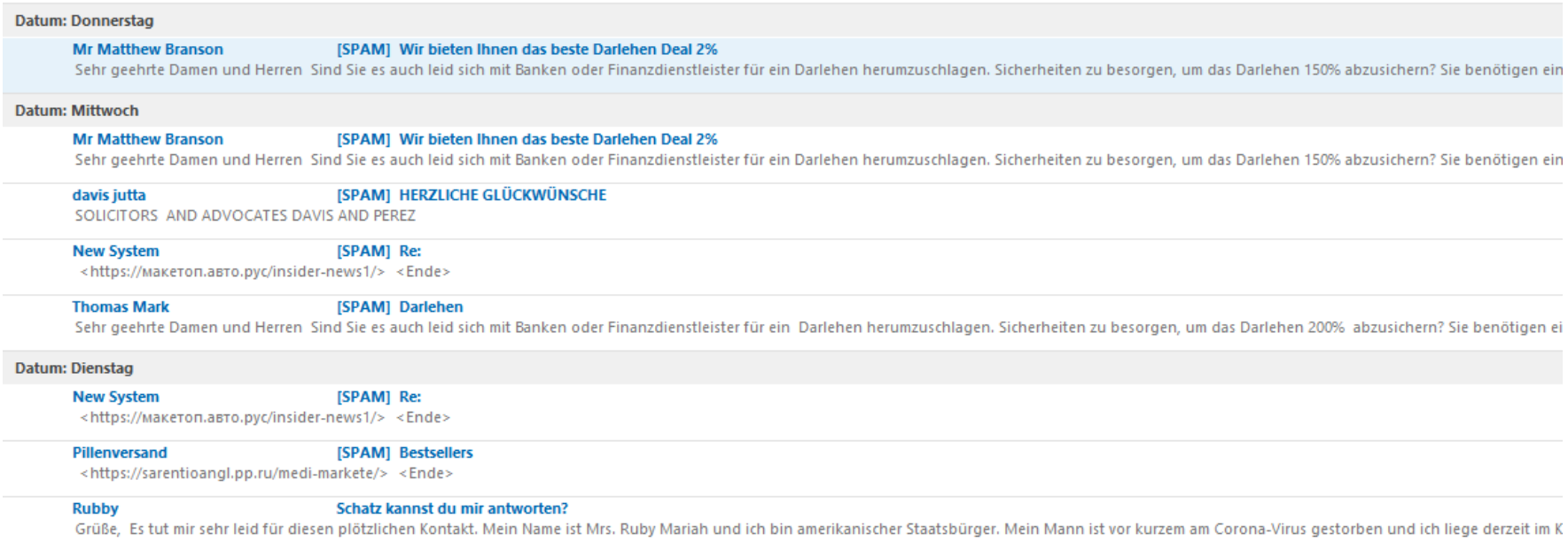
Sincerely

IT Help Desk

Office of Information Technology

Spam

Spam is a collective term for unsolicited advertising e-mails that are usually sent in bulk. Virus e-mails are also often disguised as spam. Careful handling of unknown e-mails is therefore extremely important. According to various studies, each person with an e-mail connection needs around 5 minutes per working day to delete unwanted e-mails. The productivity losses are in billions worldwide.



E-Mail ducks or hoaxes

Email ducks or hoaxes are messages that warn of imaginary viruses or dangers or contain fake requests for help or similar. Most often, recipients of such emails are asked to forward the message to as many addressees as possible. This leads not only to the spread of misleading messages, but also to unnecessary load on the email system.

Information Posted on Clinic's Letterhead is Internet Hoax

December 14, 2012

A sign in one of Memorial Physician Services' Jacksonville offices contained false information from a common internet Hoax circulating on Facebook. The sign has been removed.

A photo taken of the sign, which was on MPS letterhead, has been widely circulated. The hoax claimed that a popular drug, referred to as "Strawberry Quick" was being targeted toward children. The hoax claimed the drug looked like "Pop Rocks" candy, was dark pink in color and has a strawberry scent.

Memorial Health System issued the following statement on its Facebook page: "To anyone who's seen a photo of a sign in one of our Memorial physican Services' Clinics circulating on Facebook about 'strawberry quick' drugs being given to children – the message on the sign is an internet hoax and is not true. We are sorry for the inconvenience."

The website Snopes.com, which examines the validity of popular rumors and urban legends, confirms that the information is false. The website quoted an official with the U.S. Drug Enforcement Administration who said that "we checked with all of our labs, and there's nothing to it." The e-mail scare has been in circulation since around 2007.

E-mails getting into the wrong hands

Another problem is that e-mails may accidentally or intentionally reach the wrong recipient. Confidential data and information in the hands of unintended addressees can cause serious problems.

An email is sent quickly: which situations could be risky?

Social Engineering

Social engineering is defined as "the deliberate manipulation of people rather than machines to circumvent a company's or consumer's security systems”.
Social engineering can be done by phone, fax, email, or even face-to-face.

This results in the following points of attack:

Types of information

Companies process a wide variety of types of information, depending on the industry and their classification (e.g. "Confidential"), which represents a high value for the company.
Typical examples of such information include:

- Financial data
- Personal data
- Research and Development data
- Contracts

Potential for danger

The potential for danger is that a social engineer is always interested in a company's information, which also represents value to third parties.

Social engineering methods

There are three different methods of social engineering with which attackers try to obtain information. Attackers always assume foreign roles and never reveal their actual identity.

Computer-Based/Online Social Engineering

Attackers use technical tools such as:

- Phishing: the sender of an email pretends to be someone else in order to trick the recipient into performing an unintended action (e.g. entering passwords).
- SMiShing: same principle as above, but by means of SMS
- Abusive / manipulated websites: Websites that trick the victim into revealing confidential information, making pseudo purchases.

Human-Based Social Engineering

Attackers obtain information by non-technical means by approaching people directly, such as:

- Intimidation or making people feel guilty
- Influencing or persuading
- Exploitation of any need for help
- Searching through waste paper and garbage ("Dumpster Diving")
- Obtaining unauthorized access ("Piggy-Backing")
- Surreptitious glances over another person's shoulders ("shoulder surfing")

Reverse social engineering

The attacker does not obtain the desired information directly from the victim, but tries to get a user to voluntarily and actively provide the information to the attacker. Example: The attacker introduces himself to the victim by phone as a new support employee and leaves his phone number for assistance. He then creates a problem and gets the victim to contact him instead of asking for help from the relevant service desk.

Points of attack

Information carriers / technologies

Information carriers are generally considered to be anything that can be used to store and transmit information, e.g.:

- CD
- USB stick
- External hard disk
- Notebooks
- Smartphones

Places

- Any place where people are present or where information data carriers are stored represents a potential point of attack, depending on the situation.

Possible sources of danger

- Building entrance
- Reception
- Workplace
- Storage of waste
- Locations of printers, scanners, copiers
- Public transportation, restaurants, etc.

Fraud Purpose of Social Engineering

Social engineering has **various purposes**, like fraud, industrial espionage, identity theft.
Obtaining authorization information, for example, to take over a system or compromise the availability of individual or multiple processes.

Danger potential
The information data carriers themselves are of less interest to the social engineer, but rather those persons who have access to information carriers, i.e., who represent an interface to the information.

Another source of danger is the technology with the corresponding vulnerabilities, which in turn can be exploited by hackers for a possible attack.

Who is Robin Sage?

- 25-year-old "cyber threat analyst" at the Naval Network Warfare Command (Virginia)
- MIT Graduation
- 10 years of work experience

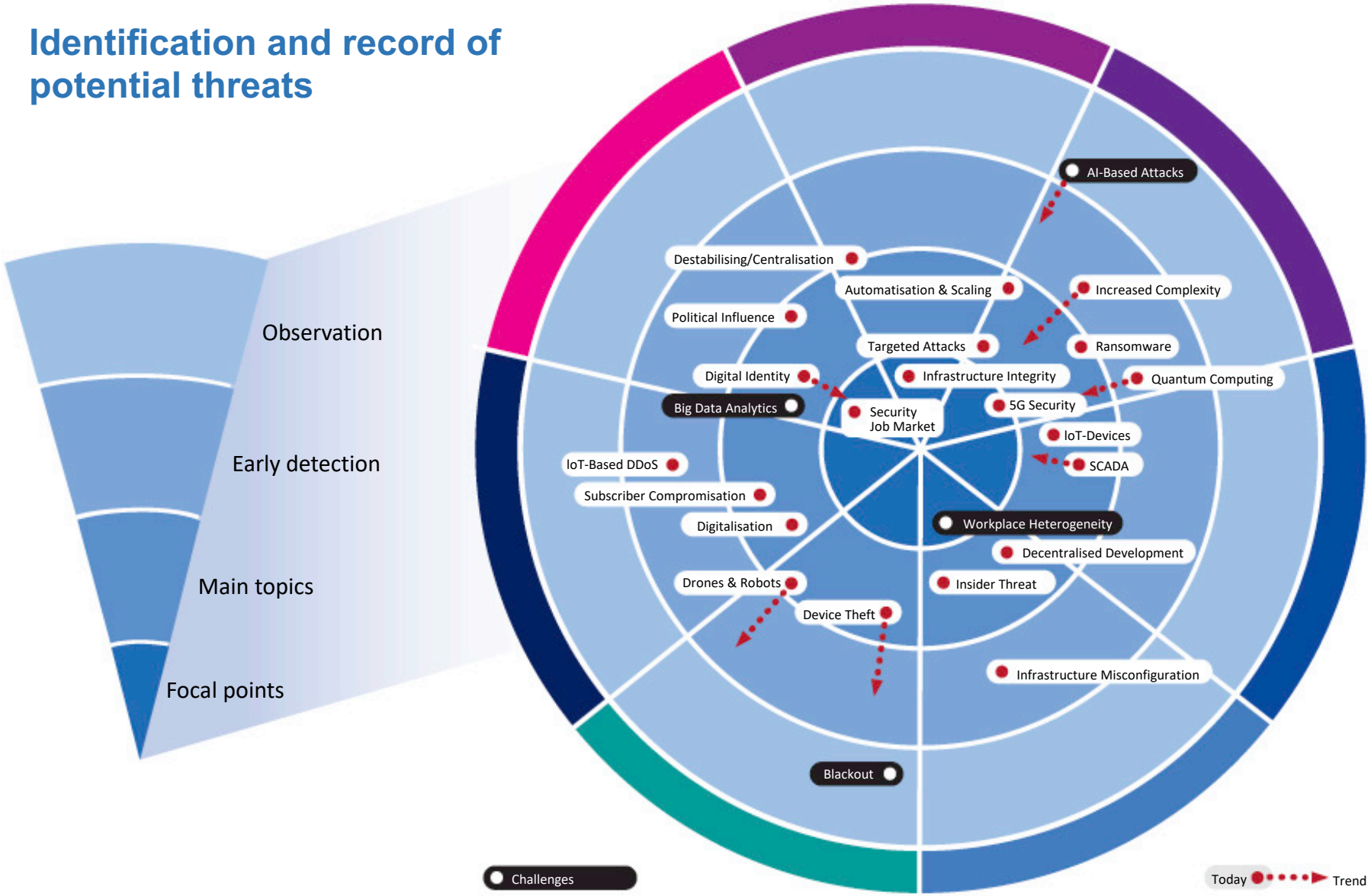
- access to email addresses and bank accounts
- learning the location of secret military units
- private documents for review
- offered to speak at several conferences

Robin Sage is a *fictional* American cyber threat analyst.

Source: en.wikipedia.org/wiki/Robin_Sage

Threat radar from Swisscom

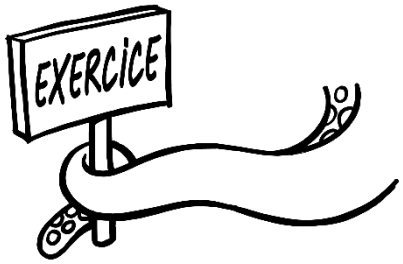
Identification and record of potential threats



Source: [Cyber crime: where the threat comes from | Swisscom]

Define the Do´s and Don´ts

1. At the office
2. During a business trip
3. Visiting a provider
4. During an internal web call
5. During a public web conference
6. By teleconsultation with a customer



How to protect?

Scope of IT Security

Passwords

- Always use different passwords for private and business use!
- Always use a different password for each service
- Good passwords are easy to remember but difficult to guess
- Passwords should be strong enough for the risk they pose
- Choose 2-factor authentication for Internet services if possible

TOP 20 MOST COMMON PASSWORDS

(as a percentage of all passwords)

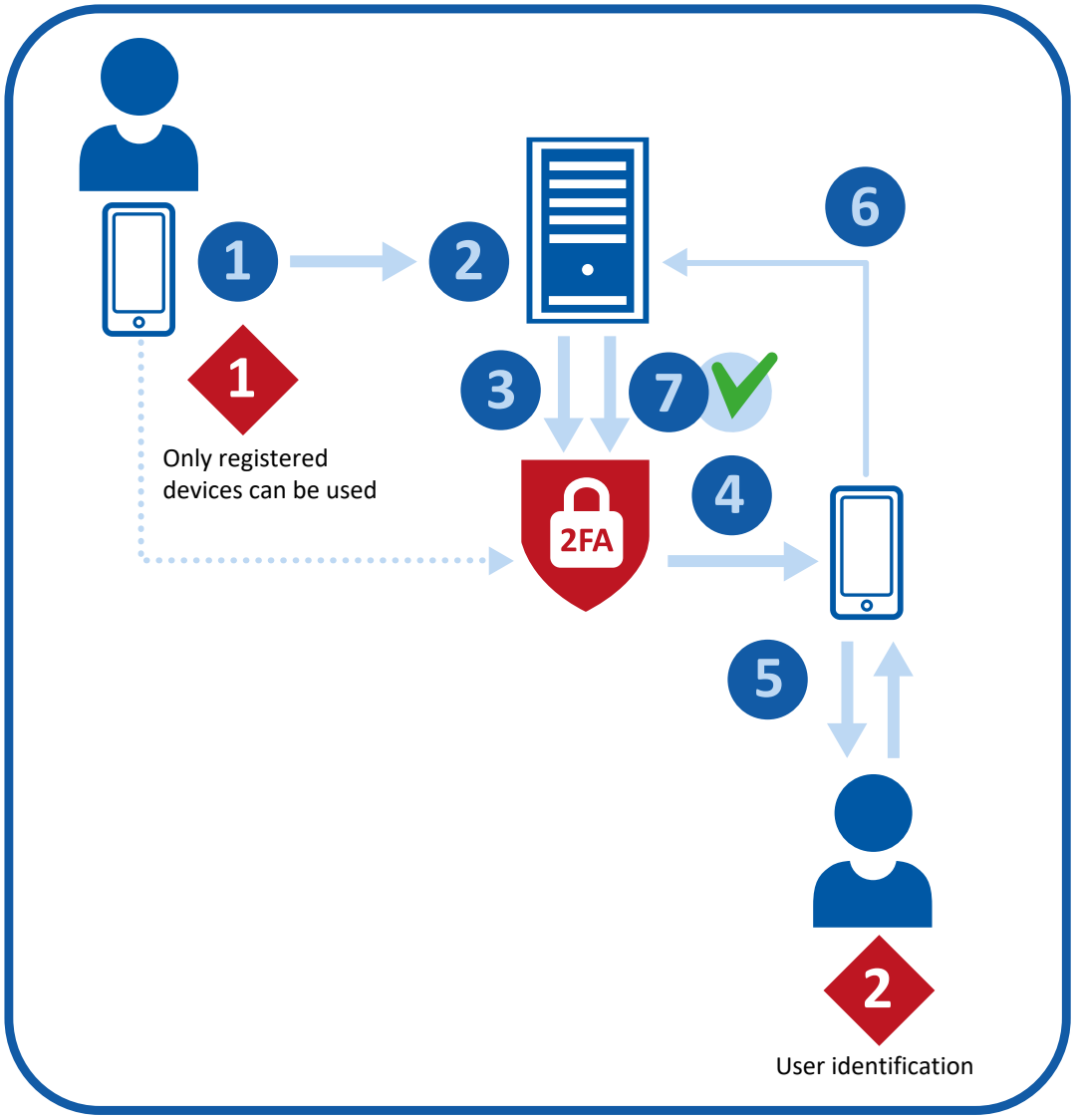
1.	123456	4,1%	11.	login	0,2%
2.	password	1,3%	12.	welcome	0,2%
3.	12345	0,8%	13.	loveme	0,2%
4.	1234	0,6%	14.	hottie	0,2%
5.	football	0,3%	15.	abc123	0,2%
6.	qwerty	0,3%	16.	121212	0,2%
7.	1234567890	0,3%	17.	123456789	0,2%
8.	1234567	0,3%	18.	flower	0,2%
9.	princess	0,3%	19.	password	0,2%
10.	solo	0,2%	20.	dragon	0,1%

Source: www.mcafee.com/blogs/enterprise/cloud-security/how-to-create-a-strong-password-you-actually-remember/

2 Factor Authentication (2FA)

2 FA is a method in which a user is granted access to a website or application only after successfully presenting two pieces of evidence (or factors) to an authentication mechanism

2FA Example for Mobile Banking



1. User uses the mobile app to login
2. Mobile app sends data to the server
3. Server requests the 2FA backend to send a confirmation message to the user
4. 2FA backend sends a message (e.g. push) back to the mobile app
5. Face recognition to identify the user
6. Mobile app signs the response and sends it to the backend
7. Backend verifies via 2FA the signed response from the mobile app

Antivirus

Viruses are usually spread unintentionally and unnoticed.
How should you protect yourself?

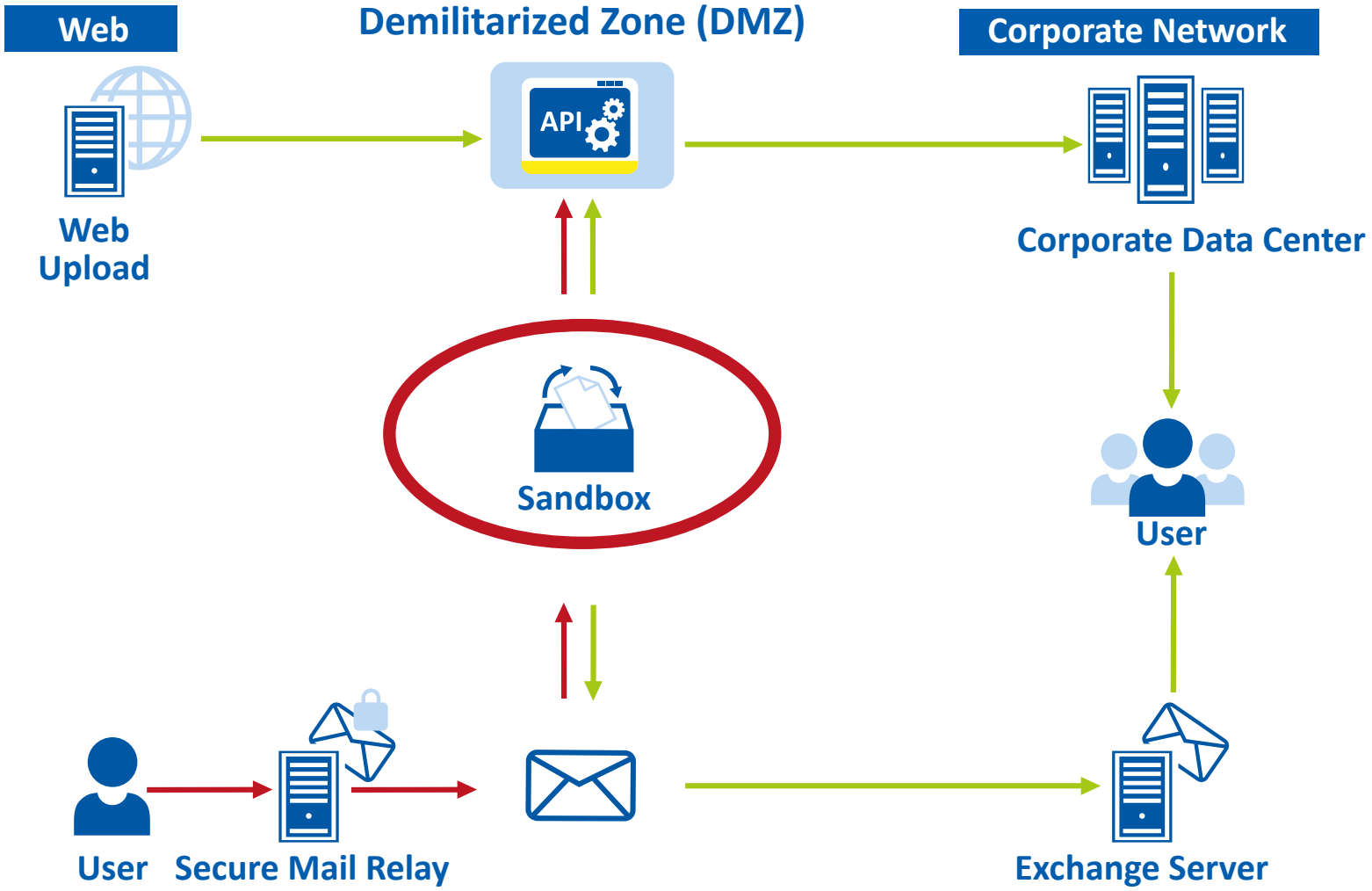
- Open attachments only if there are no doubts about the business use and the sender.
- Do not open any foreign or unsolicited files or programs.
  Also be suspicious if the e-mail content from known senders is atypical, e.g. in a language that is unusual for the sender.
- Never reply to suspicious e-mails.
  Also, never click on suspicious links that are built into e-mails.

An antivirus software works **by scanning incoming files or code being passed through your network traffic**. When files, programs, and applications are flowing in and out of your computer, the antivirus compares them to its database to find matches.

Source: www.soscanhelp.com/blog/how-does-antivirus-work

Sandboxes

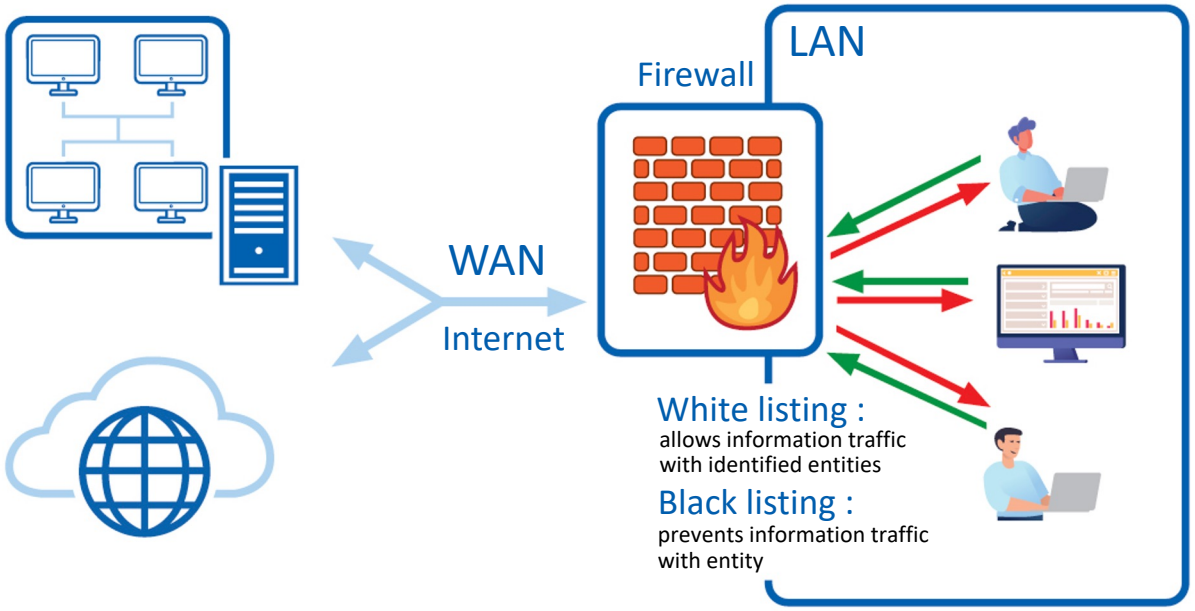
Sandboxing security techniques and tools enable to check suspicious software and files into an isolated environment, a so-called sandbox.



Firewalls

A firewall is a kind of filter, between the computer and the Internet or any other form of network to secure an environment against unauthorized access.

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

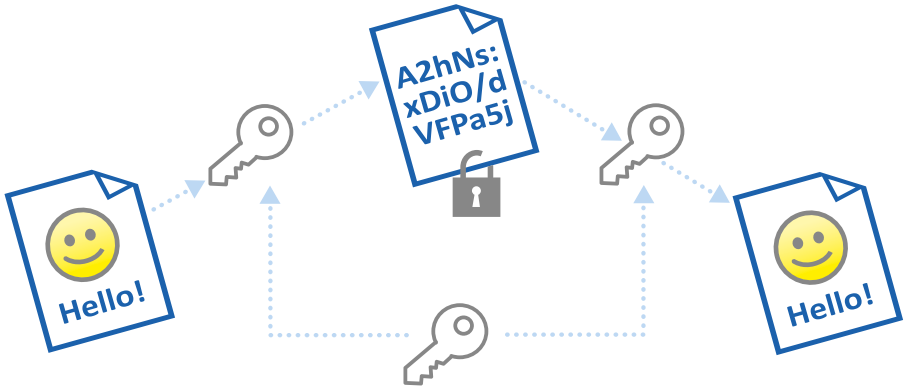


WAN: Wide Area Network
LAN: Local Area Network

Source: www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html

Encryption

Confidential data sent to external parties must be protected.
Encryption is the method that encodes data that can be read only by the receiver and not by the third party as an algorithm is used to scramble or encrypt data and then uses again in reverse order to unscramble and decrypt the information or data.



Various types of cryptographic systems exist that have different strengths and weaknesses. Typically, they are divided into two classes: those that are strong, but slow to run and those that are quick, but less secure. Most often a combination of the two approaches is used.

Symmetric Cryptography

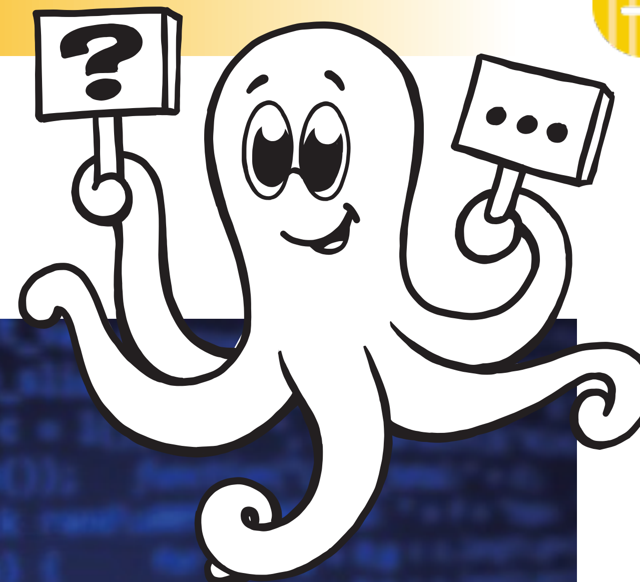
Symmetric Cryptography is the most traditional form of cryptography. In a symmetric cryptosystem, the involved parties share a common secret (password, pass phrase, or key). Data is encrypted and decrypted using the same key. These algorithms tend to be comparatively fast, but they cannot be used unless the involved parties have already exchanged keys.

Asymmetric Cryptography (also called Public/Private Key Cryptography)

Asymmetric algorithms use two keys, one to encrypt the data, and either key to decrypt. These inter-dependent keys are generated together. One is labeled the Public key and is distributed freely. The other is labeled the Private Key and must be kept hidden.

Source: wiki.owasp.org/index.php/Guide_to_Cryptography#Cryptographic_Algorithms

Is it enough?



What is Cybersecurity?

Cybersecurity refers to the practice of safeguarding systems, computers and data from digital attacks. These attacks often involve attempts to breach, modify, or damage the target's computer system, resulting in interruption or downtime for services, theft of confidential or proprietary data and exposure of personal information.

Source: techbootcamps.utexas.edu/blog/the-beginners-guide-to-cybersecurity/

Cyber attacks are unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems.
Criminal organizations, state actors and private persons can launch cyber attacks against enterprises. One way to classify cyber attack risks is by outsider versus insider threats.

Source: www.ibm.com/topics/cyber-attack

Cybersecurity Threats

Source: techbootcamps.utexas.edu/blog/the-beginners-guide-to-cybersecurity/

Build cyber resilience

“Cyber-Attacken sind wie Radioaktivität”
"Cyber attacks are like radioactivity"

Source: Münchner Cyber Dialog 2016

Source: www.wired-gov.net/wg/news.nsf/articles/Cyber+resilience+How+important+is+your+reputation+How+effective+are+your+people+03082016161500?open

Detect and Prevent

Detect

- Definition of use cases to detect anomalies
- Applying detection rules to detect anomalies in systems or running processes
- Management of alerts

Prevent

- Apply Vulnerability Management
- Server Patching
- Use collective experience (for instance verification of new SW package before 1st execution in a sandbox)
- Whitelisting and Blacklisting

Security information and event management

Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).

Source: www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

A SIEM comes in three basic types:

- **In-house SIEM**
- **Cloud-based SIEM**
- **Managed SIEM**

SIEM Functionalities

Successful Host Login after Brute Force Attempts from a Single Source

If after at least 10 failed login attempts, there is a successful one, this rule gets triggered.

AND Time Window : 20 minutes	**Login - Brute Force Login Attempts on an Internal from a Single Source** Normalization Rule (In) [Host Login] Event Subtype (In) [success] Destination IP (Not In) [0.0.0.0] Source User (Not In)

Signature IDs used in the rule

Description in the SIEM

This rule detects a successful login after brute force login attempts on a local host from a single source IP address.

Brute Force is a common attack method to "guess" login credentials. The attacker automates a process to send login requests using a long list of common and inferred usernames and passwords. The attacker enumerates each possibility, running the process until they find a match and are granted access. It's a rapidfire process, sometimes sending hundreds or thousands of requests per second. In this case, a brute force login attempt on a host was detected, followed by a successful login from the same source IP address.
Possible Action:
Immediately block access to the account and system, notifying the authorized user who to contact to restore their credentials and reset their password. Review your security policy's number of maximum failed login attempts before a user is locked out for the system accessed, revising if necessary. Investigate the characteristics of the attack and be able to prevent similar ones in the future.

Vulnerability

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their "attack surface.“

Scanners rely on declared and constantly updated lists of recognized **vulnerabilities**.

Source: www.rapid7.com/fundamentals/vulnerability-management-and-scanning/

Types of Vulnerability Scanners

Network-Based Scans

Identifies possible network security attacks and vulnerable systems on networks

Host-Based Scans

Finds vulnerabilities in workstations, servers, or other networks hosts, and provides visibility into configuration settings and patch history

Wireless Scans

Identifies rogue access points and validate that a company's network is securely configured

Application Scans

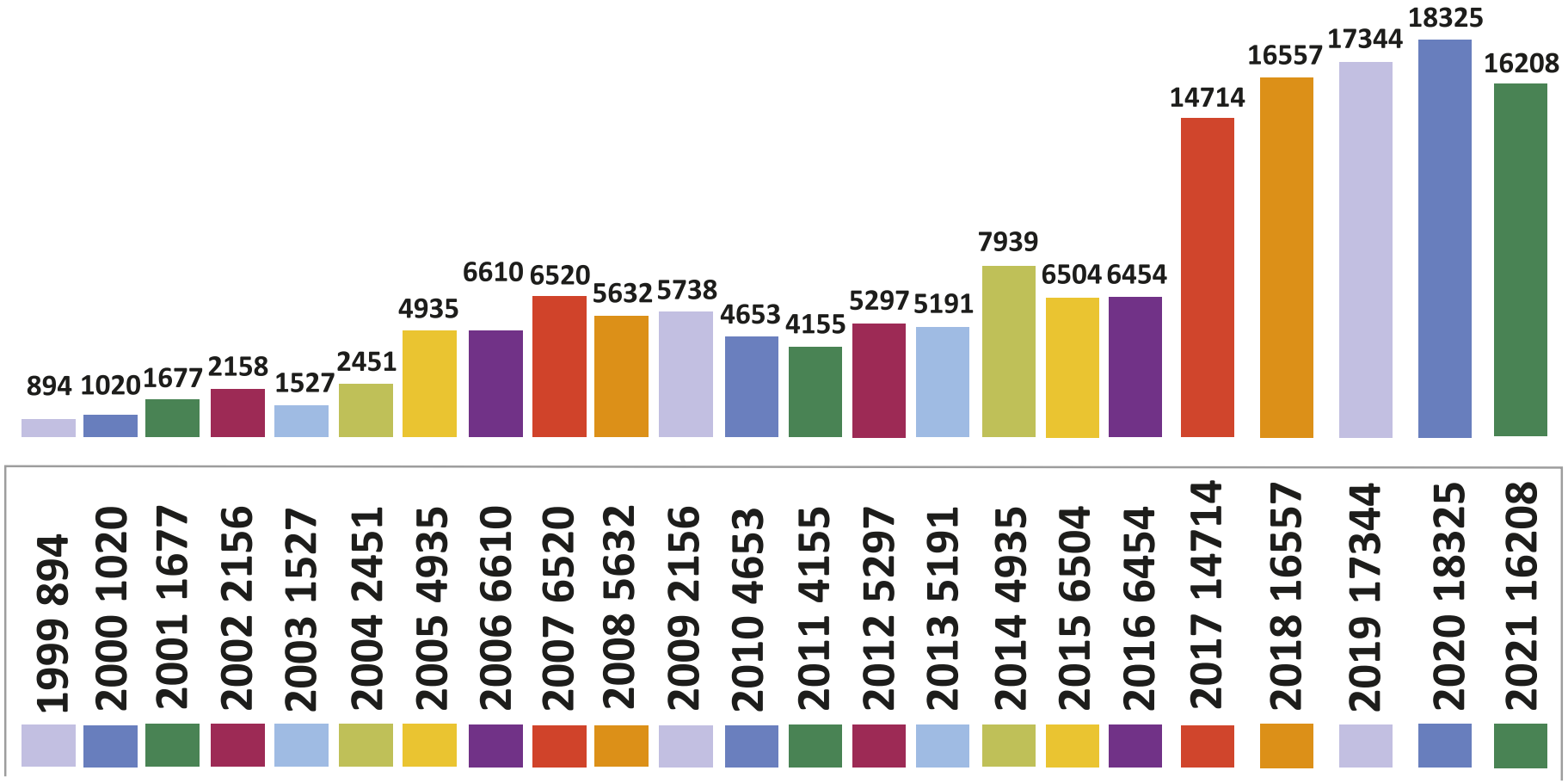
Detects known software vulnerabilities and mis-configurations in network or web apps

Database Scans

Identifies weak points in a database

Source: www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/

Number of Vulnerabilities and Exposures over time



Source: www.cvedetails.com

Main Vulnerabilities known

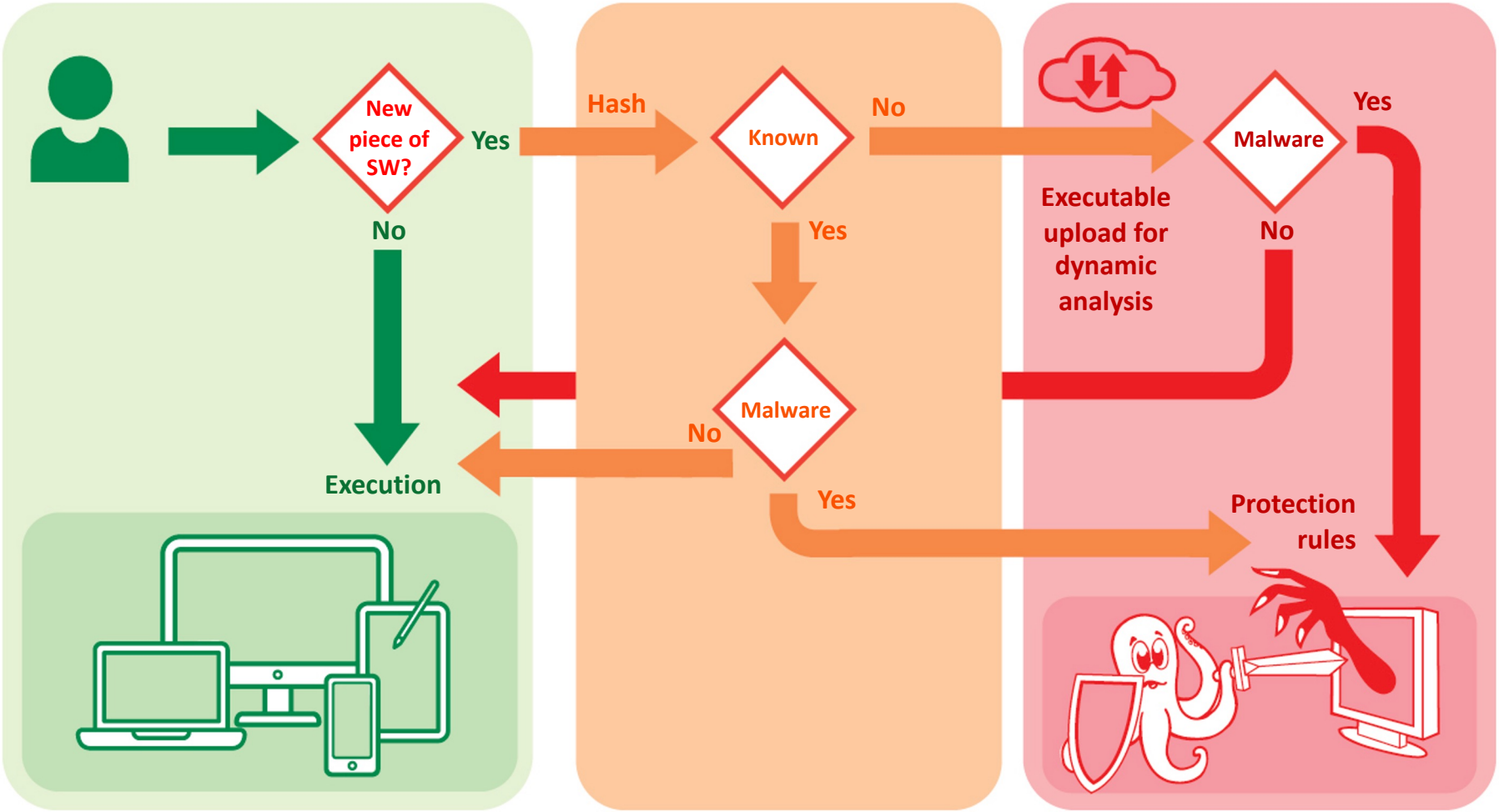
CVSS Score Distribution For Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities										Weighted Average	% Of Total									
			0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+
1	Microsoft	5830	2	97	296	59	806	740	333	1423	26	2048	7.60	0	2	5	1	14	13	6	24	0	35
2	Oracle	5291	2	102	228	418	1516	1383	606	447	23	566	6.10	0	2	4	8	29	26	11	8	0	11
3	Apple	4272	1	53	263	43	722	523	1060	675	15	917	7.00	0	1	6	1	17	12	25	16	0	21
4	IBM	3977	2	61	230	586	1099	680	410	508	28	373	5.90	0	2	6	15	28	17	10	13	1	9
5	Google	3553		9	55	14	653	432	433	932	25	1000	7.50	0	0	2	0	18	12	12	26	1	28
6	Cisco	3531	1	4	51	76	695	814	495	999	42	354	6.90	0	0	1	2	20	23	14	28	1	10
7	Adobe	2571			18	3	230	168	92	131	1	1928	9.00	0	0	1	0	9	7	4	5	0	75
8	Linux	2125	1	91	315	47	645	139	170	584	5	128	5.90	0	4	15	2	30	7	8	27	0	6
9	Mozilla	2047		9	78	11	390	420	237	346	1	555	7.20	0	0	4	1	19	21	12	17	0	27
10	Redhat	1903		46	168	87	289	374	239	425	6	169	6.30	0	2	9	5	20	20	13	22	0	9
11	Debian	1772		20	85	51	385	374	313	436	5	103	6.40	0	1	5	3	22	21	18	25	0	6
12	SUN	1630	3	26	105	45	312	283	119	422	4	311	6.80	0	2	6	3	19	17	7	26	0	19
13	HP	1615	1	10	58	35	281	235	137	383	24	451	7.40	0	1	4	2	17	15	8	24	1	28
14	Novell	1540	1	24	63	57	338	346	203	289	2	217	6.60	0	2	4	4	22	22	13	19	0	14
15	Canonical	1122		25	56	29	286	250	179	220	3	74	6.30	0	2	5	3	25	22	16	20	0	7
16	Apache	1041		6	39	28	265	341	119	186	2	55	6.20	0	1	4	3	25	33	11	18	0	5
17	GNU	649	1	10	42	27	142	157	116	121		33	6.20	0	2	6	4	22	24	18	19	0	5
18	PHP	593		1	21	6	67	174	79	203	1	41	6.90	0	0	4	1	11	29	13	34	0	7
19	Wireshark	531			24	32	174	230	7	42	3	19	5.70	0	0	5	6	33	43	1	8	1	4

CVSS: Common Vulnerability Scoring System
See: www.first.org/cvss/calculator/3.1

Source: www.cvedetails.com

Use of Vulnerabilities Management Services



Methods to exploit vulnerabilities

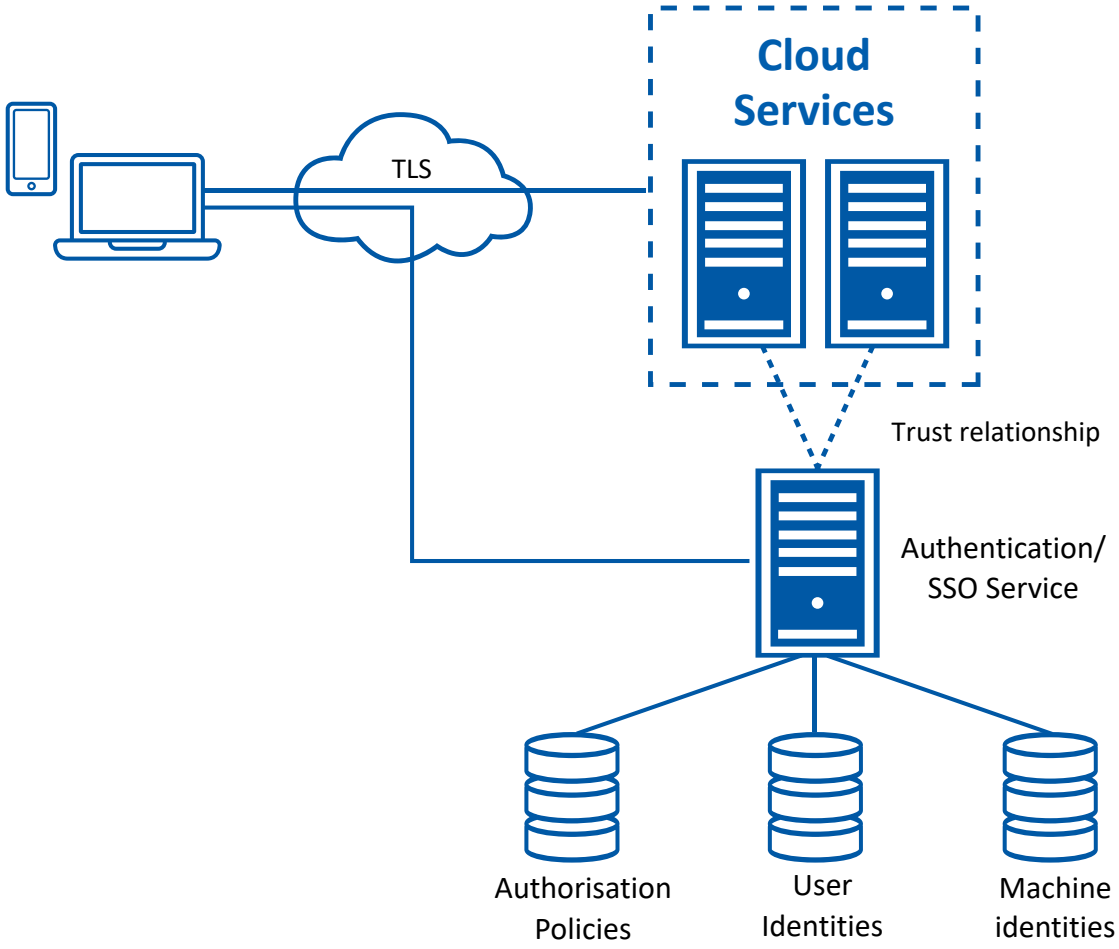
Adversarial Tactics, Techniques, and Common Knowledge (ATT &CK)

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Sotware	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Excecution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scriptsc	Graphical User Interface	Data Staged	Data Encrypted	Custom Command and Control Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfert Size Limits	Custom Cryptographic Protocol
Changez Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Mediac	Exfiltration Over Command and Control Channel	Fallback Channels
DLL Search Order Hijacking	Legitimate Credentials	DLL Slide-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Neytwork Medium	Multi-Stage Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Rundil32	Screen Capture	Scheduled Transfer	Multilayer Encryption
Local Port Monitor	Path Interception	File Deletion		Query Registry	Shared Webroot	Scheduled Taskc			Peer Connections
Logon Scripts	Scheduled Task	File System Logicial Offsets		Remote System Discovery	Taint Shared Content	Scripting			Remote File Copy
Modify Existing Service	Service File Permissions Weakness	Indicator Blocking		Security Software Discovery	Windows Admin Shares	Service Execution			Standard Application Layer Protocolc
New Service	Service Registry Permissions Weakness	Indicator Removal from Tools		System Information Discovery	Windows Remote Management	Third-party Software			Standard Cryptographic Protocol
Path Interception	Web Shell	Indicator Removal on Host		System Owner/User Discovery		Windows Management Instrumentation			Standard Non-Application Layer Protocol
Redundant Access		InstallUtil		System Service Discovery		Windows Remote Management			Uncommonly Used Port
Registry Run Keys/ Start Folder		Legitimate Credentials							Web Service

Source: *attack.mitre.org/matrices/enterprise/*

Zero Trust Access (ZTA)

never trust, always verify



SSO : Single Sign-On
TLS : Transport Layer Security

Source: Network architectures - NCSC.GOV.UK

SASE = Secure Access Service Edge

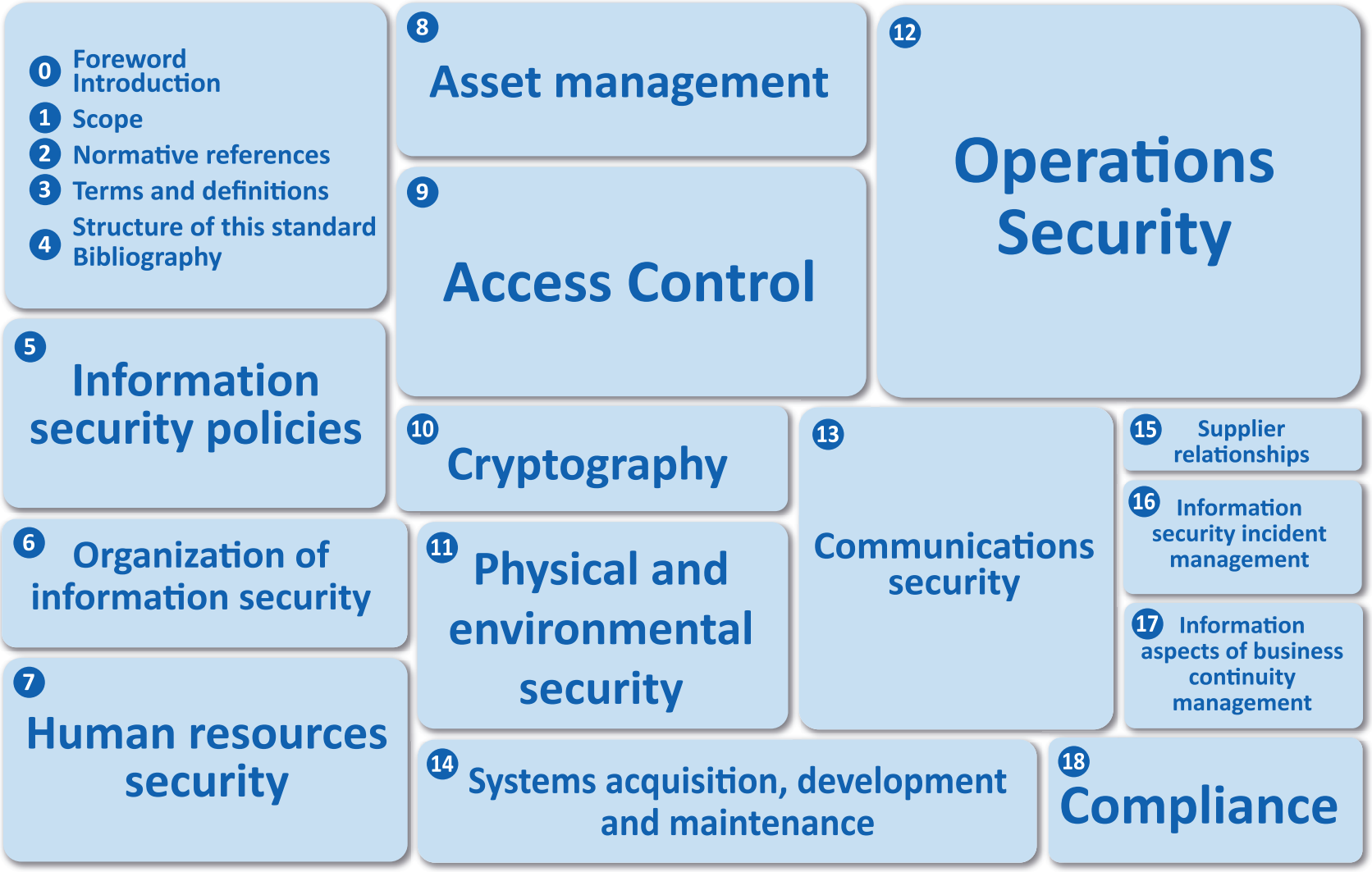
A **secure access service edge** (**SASE**) is a term coined by analyst firm Gartner. SASE was promoted for computer security in wide area networks (WANs) by delivering both as a cloud computing service directly to the source of connection (user, device, branch office, Internet of things (IoT) device, or edge computing location) rather than a data center.

Source: en.wikipedia.org/wiki/Secure_access_service_edge#cite_note-:0-2

Recognized frameworks

Standard	Description	Applicability
ISO 27000 series (ISO)	Globally recognized standards for information security management, focus on governance, processes, controls	Guideline and basis for the ISMS (Information security management system) to ensure governance
NIST Cybersecurity Framework (CSF)	Framework for improving the cybersecurity infrastructure. Basis of FINMA requirements for cybersecurity.	Reference work for the definition of concrete security requirements for IT. Complementary to ISO 27000. Ensuring Secure IT Operations, Identification of Gaps
CIS Critical Security Controls (CSC)	Catalogue of specific measures and controls, similar to an implementation manual for NIST CSF	External reference for concrete improvement measures, improvement, closing gaps

Content of the ISO 27002 standard



Source: www.iso27001security.com/html/27002.html

Norms and Standards

ISMS Supporting Guidelines and Code of Practice

- ISO/IEC 27002: Code of practice for information security management
- ISO/IEC 27003: ISMS implementation guidelines
- ISO/IEC 27004: Information security management measurements
- ISO/IEC 27005: Information security risk management

ISMS Accredited Certification and Auditing Standards

- ISO/IEC 27006: International accreditation guidelines for the accreditation of bodies operating certification/registration of information security management systems
- ISO/IEC 27007: Guidelines for information security management systems auditing
- ISO/IEC 27008: Guidelines for auditors on ISMS controls
- ISO/IEC 27009: Sector-specific application of ISO/IEC 27001—requirements
- ISO/IEC 27021: Competence requirements information security management professionals

ISMS Sector Specific

- ISO/IEC 27010: Information security management for intersector and interorganisational communications
- ISO/IEC 27011: Information security management guidelines for telecommunications organisations based on ISO/IEC 27002
- ISO/IEC 27013: Guidelines on the integrated implementation of ISO/ IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27015: Information security management guidelines for financial services
- ISO/IEC 27017: Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002

Source: Edward Humphreys, Implementing the ISO/IEC 27001 ISMS Standard

Content of the NIST CSF

5 Functions with 23 Categories and 98 Controls

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

CIS Controls

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use Of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation, and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration For Network Devices, Such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring And Control

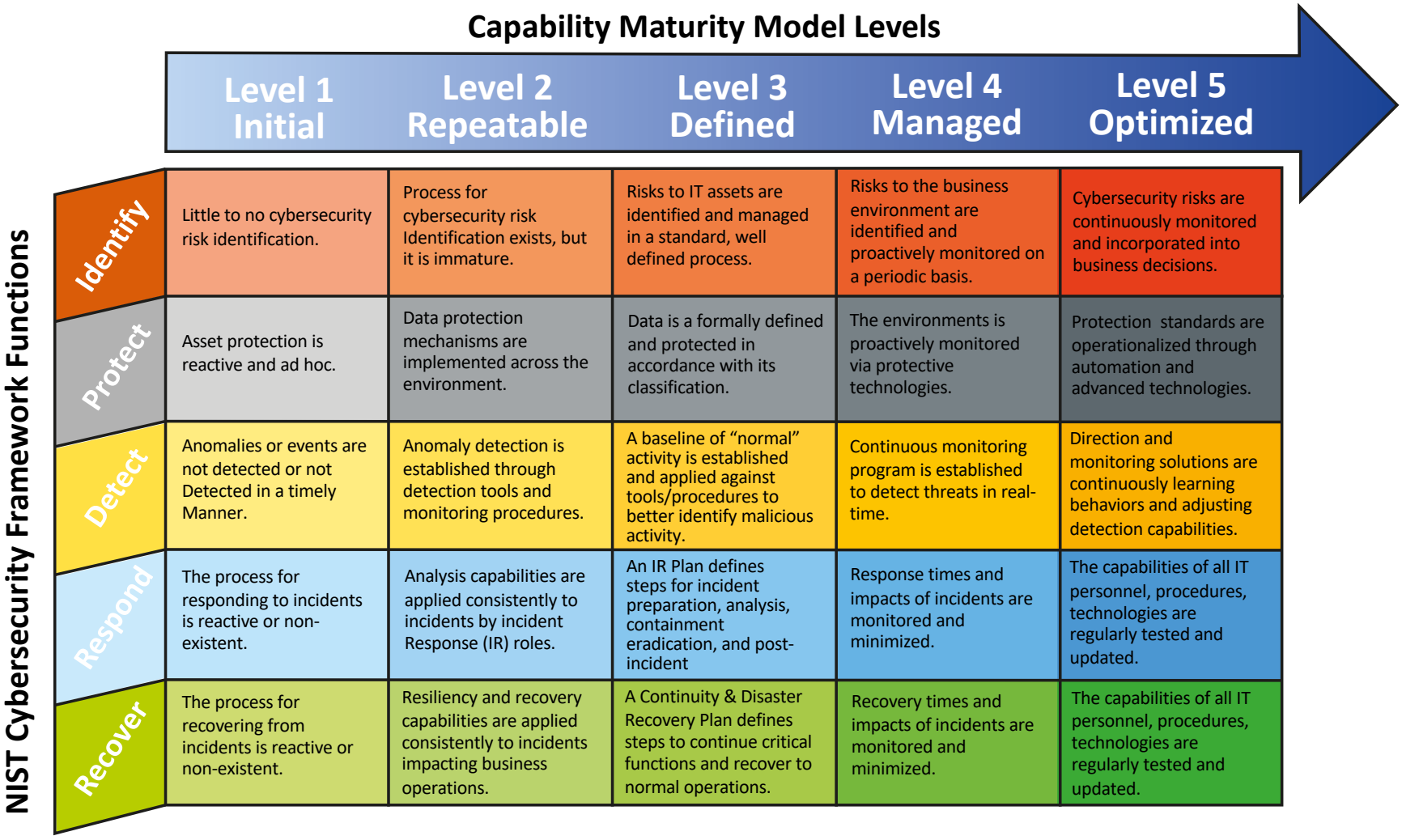
Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercices

Basic = Implementation required to achieve basic protection (47 measures).
Foundational = Recommended implementation (risk-based, 88 measures)
Organisational = Concerns people / processes, not technology (36 measures)

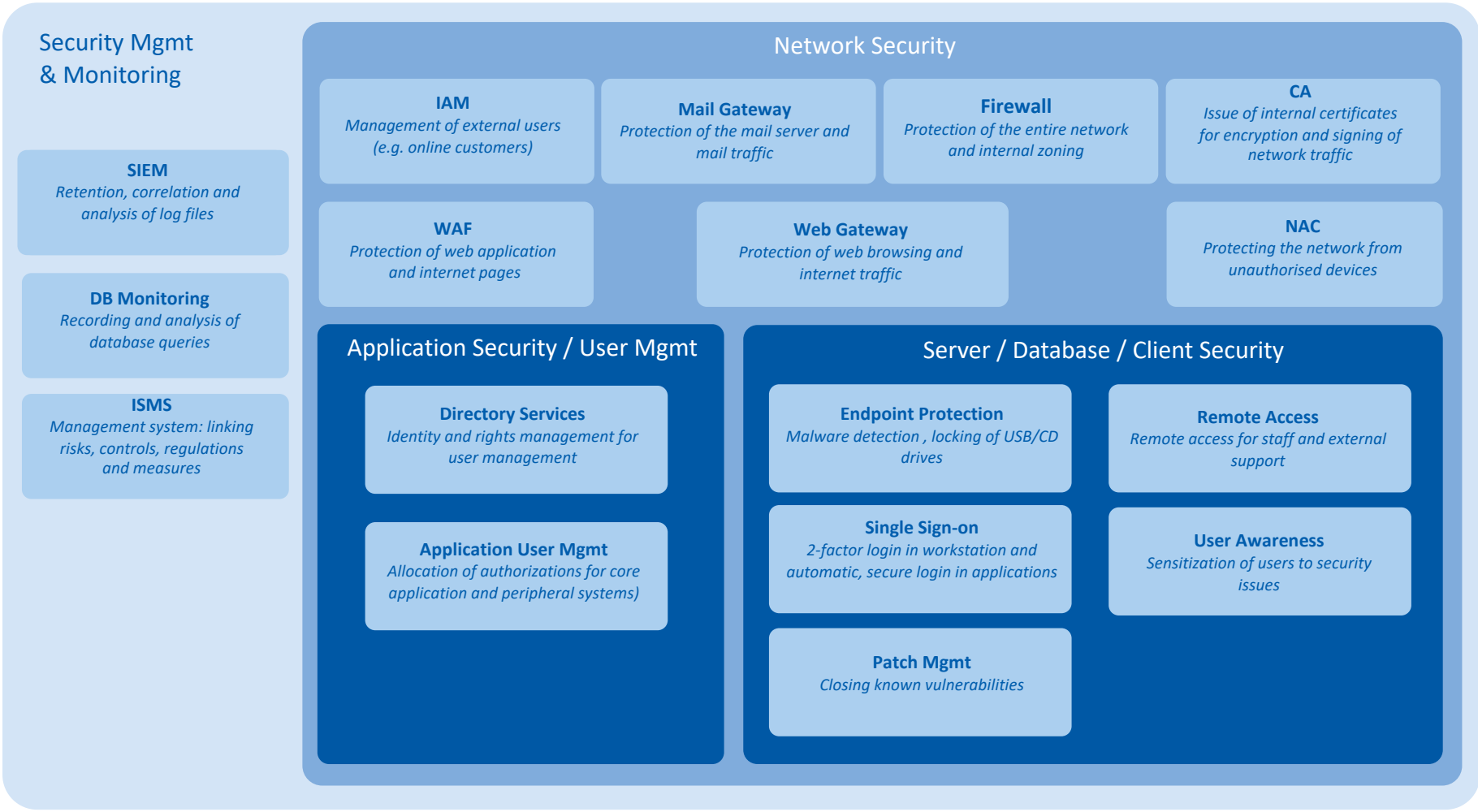
Source: www.cisecurity.org/spotlight/cybersecurity-spotlight-cis-controls

Assessing the Maturity Level



Source: www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-a-guide-to-assessing-security-maturity.pdf

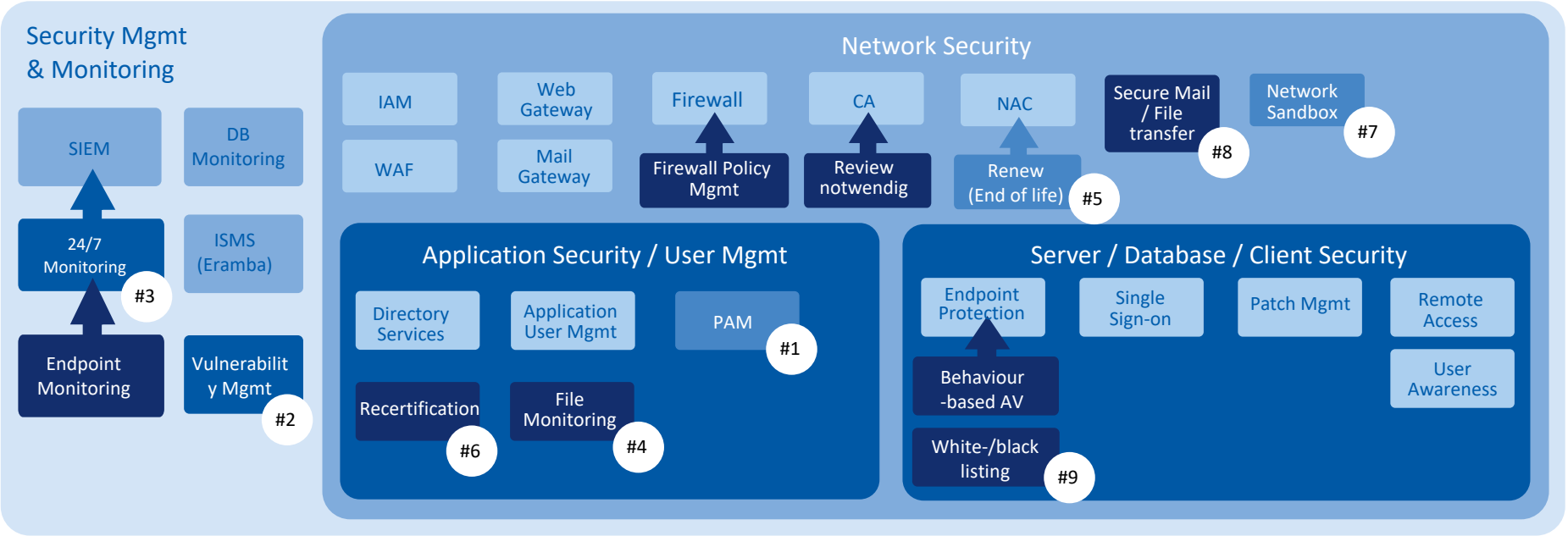
Security Architecture – As-Is



- CA: Certificate Authority
- SIEM: Security Information and Event Management
- ISMS: Information Security Management System
- DB: Database
- IAM: Identity and Access Management
- NAC: Network Admission Control
- WAF: Web Application Firewall
- USB: Universal Serial Bus
- CD: Compact Disk

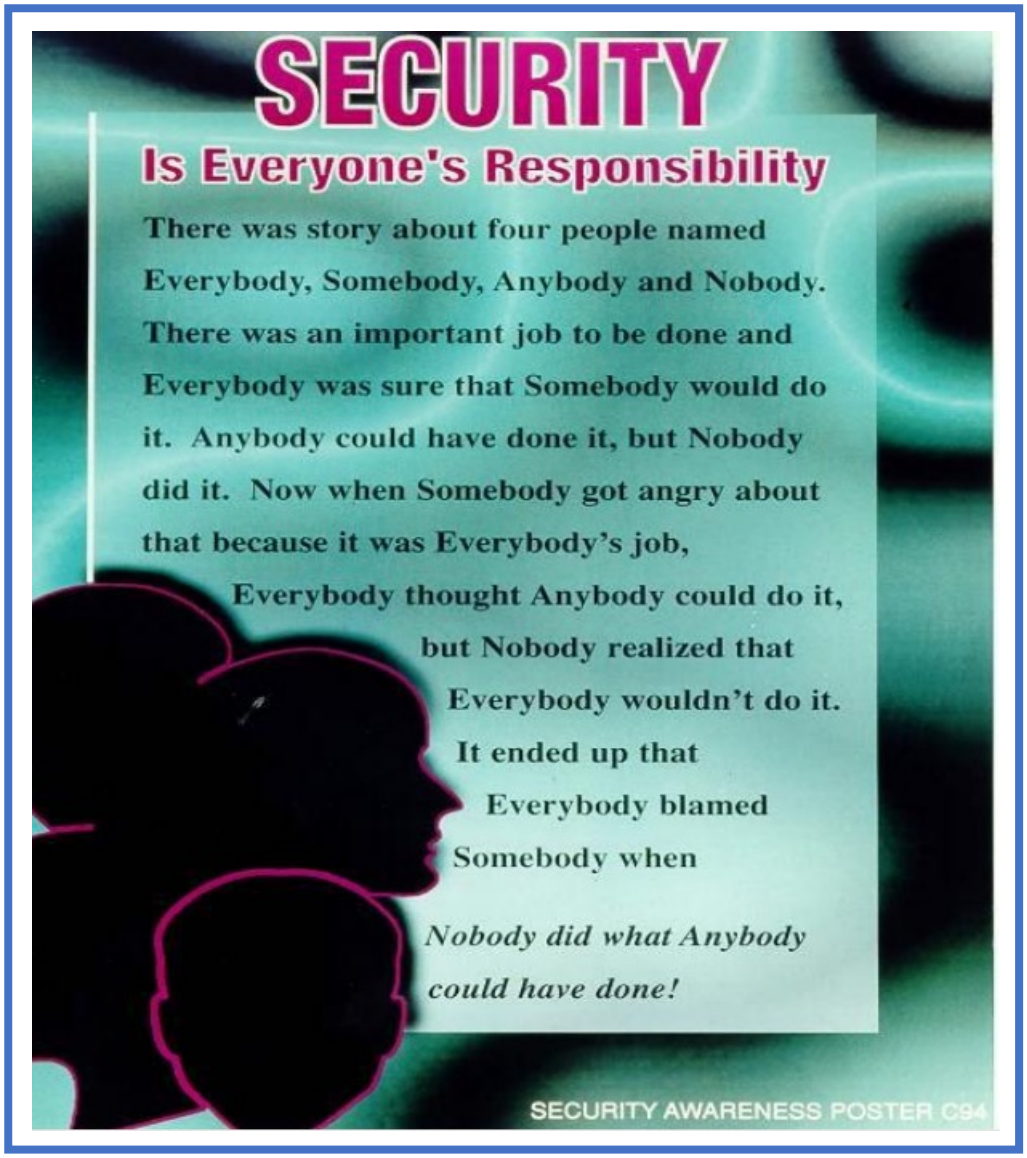
Example: Audit and Improve

Taking Measures to improve the security



- #1 Implement a Privileged Access Solution
- #2 Put a Vulnerability Management in place
- #3 Monitor SIEM 7/24
- #4 Check accesses on file directories
- #5 Define a cryptographic controls policy
- #6 Analyze a Software-supported solution to manage access rights
- #7 Introduce sandboxing, which can be used in the internal and external network boundaries
- #8 Evaluate a secure mail system and a secure file transfer system
- #9 Evaluate the possibilities for blacklisting / whitelisting of applications

Protection policy



Source: www.wrc.noaa.gov

Corporate Policies

Use of Emails

- Look for the following characteristics before you open an email: Do you know the sender? Does the subject make sense? Are there programs disguised as documents in the attachment, for example ending with .exe or .vbs?
- If one or more of these characteristics occur, report the e-mail in question to Security using the "Report Phishing Mail Lucy" button
- Phishing e-mails pretend to be from a legitimate source
- Never reply to spam e-mails

Access Management

- Grant Access to information, applications and systems appropriately to a user's responsibilities
- Access will be controlled at least once a year

Security Information and Training

- Web-based training on a regular basis
- „Phishing" internal security Mails to check the responsiveness of the users
- Information how to deal with and report lost or stolen devices
- Rules to use third party cloud or file sync services such as Gmail, Dropbox, et

Major functions of IT Security

- **Restrict data access**
  - Identification and Authentication
  - Access Management
  - Physical Accesses
- **Prevent and secure data transfer**
  - Email
  - Electronic Data Transfer
- **Control transport media**
  - Physical Electronic Data Transfer
  - Physical output distribution

IT Security covers different areas

Data security

Internet security, including virus protection, Trojan protection and firewalls, plays a key role. Companies can go even further by blocking Internet sites, prohibiting downloads and taking other measures.

Cloud security
Data Download
Network Domains

User and Access Management

User Identification, including user name
User Authentication, like a password or using multifactor authentication
Remote Access
Privileged Accesses, meaning special access or abilities above and beyond that of a standard user like system administrators

Physical Access Control

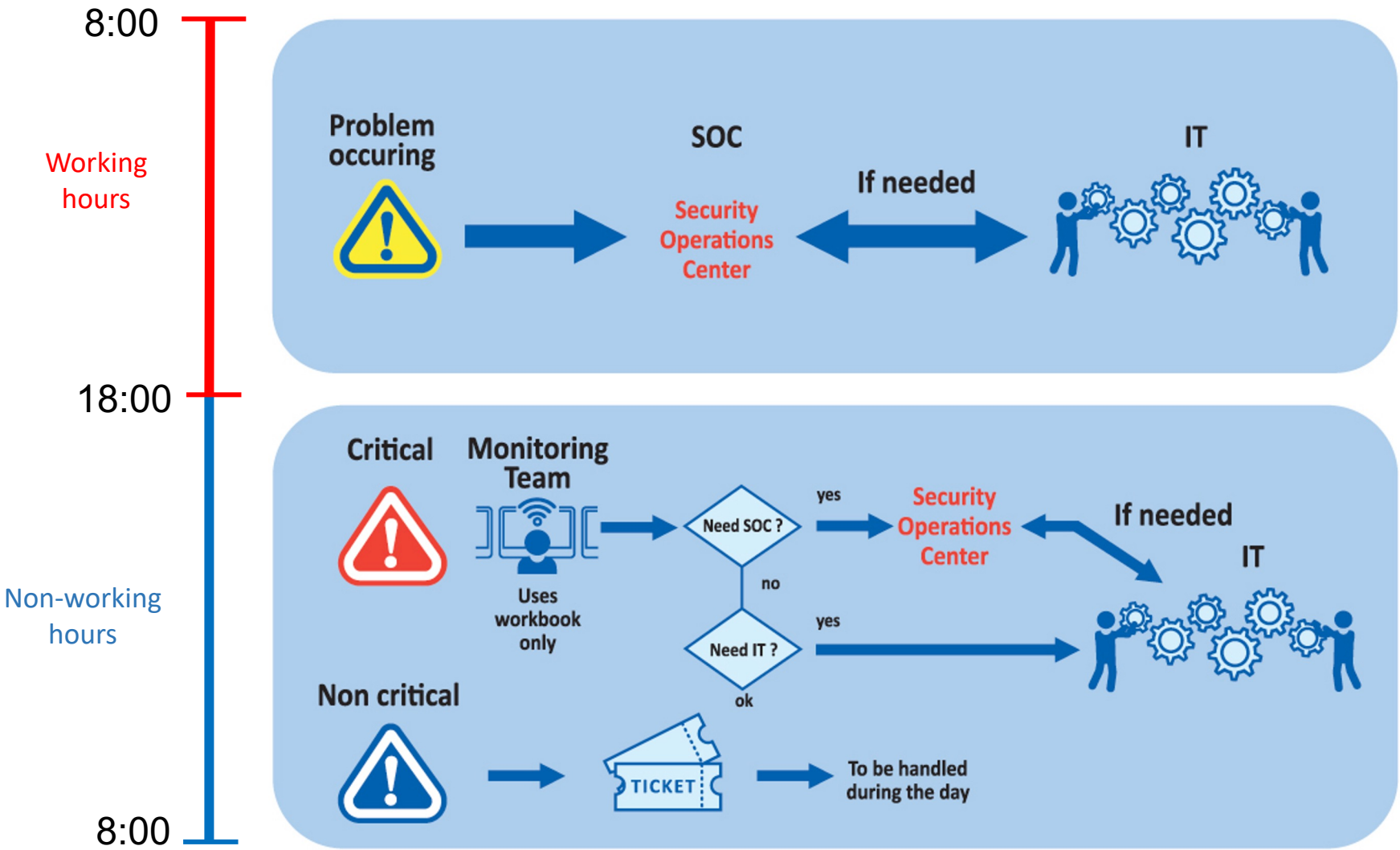
Access exclusively for employees with key cards or even NFC technologies.
Server Rooms with restricted access, alarms and no windows
Data Center Security, Securing the racks and network cables including a biometric security access and a mantrap entry room

Asset Management

Workstations, Laptops, Tablets
Mobile devices
Network Components
Wireless Network
USB Stick

NFC : Near Field Communication

Security Operations Center (SOC)



Threats and Answers from ISM

Threats

- Unauthorized access
- Unauthorized remote access
- System admin access
- Mobile device
- Login Attempts
- Logon Attempts
- Wireless access
- Wrong application accesses
- Unauthorized network access
- Data loss
- Unpermitted Data Download
- Malicious e-mails
- Wrong level of SW protection
- Sending confidential information
- User-Installed Software
- Virus, Worms, Bots
- Buffer overflow
- Head Spray

Answers from ISM

- Access Control for Mobile Devices
- Role-Based Security Training
- Penetration Testing
- Configuration Change Control
- Information System Backup
- Information System Recovery
- Identification and Authentication
- Privileged Access Management (PAM)
- Restricted Media Use
- Rules of Behavior
- System Maintenance Life Cycle
- Patching
- Public Key Infrastructure Certificates
- Client SW Engineering
- Anti-Spam Software
- Honeypots (trap for bots or hackers)
- Session Locking and Termination
- Sandboxes
- Whitelisting / Blacklisting

A battle lost in advance?

Zero-day Attack

"Zero-day" is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems. The term "zero-day" refers to the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it. A zero-day attack takes place when hackers exploit the flaw before developers have a chance to react.

Source: www.kaspersky.com/resource-center/definitions/zero-day-exploit

Dark web

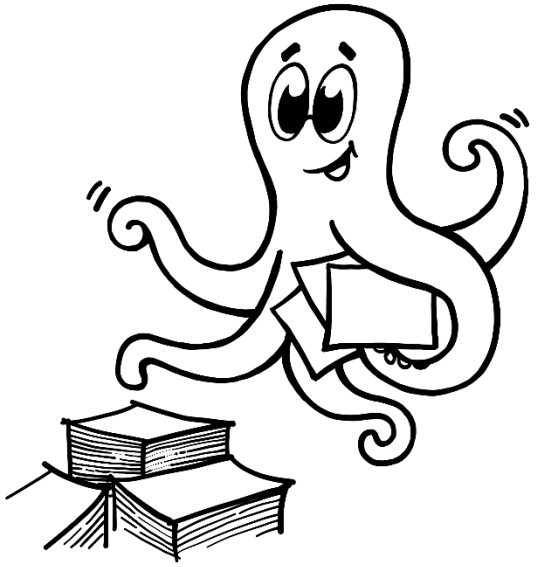
The widespread availability of dark web forums dedicated to freely sharing privacy-enabling technologies, intrusion software and exploitable code means global law enforcement agencies face an uphill struggle. There’s a growing number of technically-savvy ‘amateur hackers’ carrying out cyber-attacks, though as yet they’ve had little impact. But for businesses that means even the average customer could buy a cyber-attack service anonymously – or possibly learn to conduct their own cyber-attack – without being caught.

Source: www.paconsulting.com/insights/why-the-dark-web-is-becoming-a-cyber-security-nightmare-for-businesses

Be alert

Take away and must know!

- The logic of Cyberattack
- Main Security Threats
- Main Protection Techniques
- Major Roles of IT Security
- Best Practices for Protection (prevent and detect)



Literature

- Dotson C. (2019) Practical Cloud Security - A Guide for Secure Design and Deployment. O´REILLY, Sebastopol - CA
- Humphreys E (2016) Implementing the ISO/IEC 27001 ISMS Standard. ARTECH HOUSE, Boston-London
- Jarpey G, Scott McCoy R. (2017) Security Operations Center Guidebook. Elsevier
- National Institute of Standards and Technology (2013) Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Gaithersburg

---

- www.ncsc.admin.ch
- www.ebas.ch
- www.swisscom.ch/de/magazin/datensicherheit-infrastruktur/
- www.broadcom.com/support/security-center
- www.cisecurity.org
- www.itsecdb.com/oval/
- www.cvedetails.com
- attack.mitre.org/matrices/enterprise

KNOWLEDGE

www.know-ledge.ch