ECONOMY AND FINANCE • VOL. 12. ISS. 3 • SEPT 2025 • DOI: 10.33908/EF.2025.3.5

CYBER DEFENCE CONCEPTS AND THEIR INTERPRETATION

Levente Kovács - Elemér Terták[1]

ABSTRACT

For effective cyber defence, up-to-date and high-quality knowledge is essential. This must permeate law enforcement, the legislative framework, service platforms and defence systems, as well as educational and communication materials. In order to achieve this successfully, we have compiled what we consider to be the most comprehensive definitions and explanations of cyber defence concepts as of the summer of 2025. Given that cybercrime increasingly operates across borders, cyber security and cyber defence can only be truly effective if they are capable of efficient international cooperation, for which the precise definition of relevant concepts is one of the necessary preconditions.

JEL codes: K24, K42, M15

Keywords: cyber defence, cyber security, cyberspace concepts

Cyber security and cyber defence represent one of the most pressing challenges of our time from the perspective of individuals, society, public institutions, public services and businesses alike. As cyberspace is changing on an almost daily basis, the legal system is only able to follow these transformations with delay. The expansion of individual knowledge likewise cannot keep pace with the dynamics of development and change. Consequently, effective national and international law enforcement in the global cyberspace is significantly lagging behind, while cybercrime, by constantly adapting to technological advances and deploying new methods, seeks to enrich itself at the expense of others.

For individual preparedness, the formulation of legislation, and effective national and international cooperation, it is essential to standardise and refine the concepts and interpretations used in cyber defence and cybercrime. For this reason, based on publicly available internet sources, we have compiled this glossary in a way that includes the internationally used English equivalents of all relevant

[1] *Levente Kovács* Secretary General, Hungarian Banking Association; Head of Department, University of Miskolc. E-mail: kovacs.levente@bankszovetseg.hu.
Elemér Terták Member of the Board, Hungarian Economic Society. E-mail: elemertertak@gmail.com.

terms, thereby facilitating unambiguous communication in international crime prevention and law enforcement relations.

THE MOST IMPORTANT CONCEPTS OF CYBER DEFENCE AND CYBER SECURITY

1. **0-day/Zero-Day Attack**: A zero-day attack is a security vulnerability in software that is not publicly known and of which the vendor is also unaware. It is called a zero-day attack because it occurs before the target becomes aware of the existence of the vulnerability. The "zero-day" occurs on the very first or "day zero" when the developer has already learned of the flaw but has not yet had the opportunity to deliver a security patch to users of the software. In such cases, the attacker releases malicious code before the developer or vendor has been able to produce a patch to remedy the vulnerability. A zero-day attack begins when a software developer publishes vulnerable code that a malicious actor identifies and exploits. The attack is then either successful – likely resulting in identity theft or information theft – or the developer creates a patch to limit further exploitation. Once the patch has been written and applied, the exploitation is no longer referred to as a "zero-day" exploit.

   https://www.fortinet.com/resources/cyberglossary/zero-day-attack

   https://hu.wikipedia.org/wiki/Nulladik_napi_t%C3%A1mad%C3%A1s

2. **APT (Advanced Persistent Threat):** Advanced Persistent Threat (APT) groups are cybercriminal organisations that conduct long-term, targeted attacks against their victims, who are typically larger economic entities and, in rarer cases, states. The primary objective of APT groups is usually to obtain data that is encrypted, sensitive, personal in nature, or part of intellectual property. Furthermore, any data that can be used for extortion or to harm the targeted individual, and which may yield significant financial or political gain, can become a target. The motivations of the actors involved may vary, and considerable differences can be observed in their capabilities, sophistication, level of training, and the degree of support they receive. Among these, nation-state actors are considered the most sophisticated malicious actors: they are highly committed and possess advanced resources and tools. They generally carry out their operations with the utmost care to avoid detection. To this end, they conduct thorough reconnaissance to gather information about the target's organisational and IT infrastructure, corporate culture, employees, and security policies and procedures. They are capable of adapting to changes in the security controls introduced at the target. In addition

to these distinctive features, APT groups typically invest time in discovering zero-day vulnerabilities and in developing exploits or malware that remain undetected by their targets for extended periods. The motivations driving such actors are usually political or economic in nature.

https://nki.gov.hu/wp-content/uploads/2023/07/APT-csoportok.pdf

https://en.wikipedia.org/wiki/Advanced_persistent_threat

3. **Adware:** Adware is a specialised executable application that displays advertisements, with its primary purpose being the delivery of advertising material to the user unexpectedly and without request. Many adware applications also perform tracking functions, which is why they are classified among spyware technologies. Numerous users wish to remove such unwanted advertising software from their devices if it monitors their behaviour, if they do not want to see the advertisements displayed by the adware, or if they are disturbed by the software's negative impact on system performance. On the other hand, there are users who wish to retain certain adware applications, as their presence can reduce the cost of using a particular programm or service, thereby making them intentional and even beneficial. A good example of this is a type of advertisement that directly assists or complements what the user is using or searching for.

   https://www.eset.com/hu/termektamogatas/veszelyek/

   https://hu.wikipedia.org/wiki/Rekl%C3%A1mprogram

4. **Angler phishing (fake service provider assistance on social media):** Angler phishing is a specific type of phishing attack that has become widespread on social media. Cybercriminals are aware that service providers increasingly use social media to interact with their customers – not only for marketing and promotional purposes, but also for complaint handling and problem-solving. Offenders monitor the customer complaints submitted to the service providers' social media channels, and then, posing as representatives of the provider – by copying their social media profile or creating a fraudulent account that closely resembles it – they contact the complainant. Seemingly in the course of handling the complaint or addressing the reported issue, they request sensitive information (such as personal details, banking information, or login credentials and passwords for various accounts). With these, they can subsequently gain access to the victim's bank accounts and other online accounts.

   https://kiberpajzs.hu/csalastipusok/szamitogepes/angler-phishing/

   https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/angler-phishing-hamis-szolgaltatoi-ugy-intezes-a-kozossegi-mediaban

5. **Anti-Phishing:** Anti-phishing refers to defensive practices aimed at preventing or mitigating phishing attacks, in which attackers attempt to obtain sensitive information by impersonating seemingly trustworthy sources. Anti-phishing techniques combine human vigilance with advanced software solutions, such as email filters, link analysis, and integrated anti-malware systems for detecting malicious content. The objective is to establish a multilayered security approach that is both preventive and restorative.

   https://perception-point.io/guides/phishing/how-to-prevent-phishing-attacks/

6. **Antivirus:** An "antivirus" is software designed to protect against computer viruses and other malicious programs. The purpose of antivirus programs is to identify, filter, and eliminate harmful software from a computer, thereby safeguarding user data and maintaining system stability. In the context of online stores, antivirus protection is particularly important, as it helps secure the data of both customers and merchants, enabling safe online transactions. Antivirus programs continuously monitor regular software, file, and website activities to detect potential threats. To provide protection against the latest virus signatures and attack methods, antivirus software receives regular updates. Detected malware is immediately removed or quarantined to prevent further damage.

   https://webshopautomatizalas.hu/e-comm-lexikon/antivirus

7. **Attack Vector:** A cybersecurity attack vector is a pathway through which a hacker or malicious actor gains unauthorized access to a network, server, application, database, or device by exploiting system vulnerabilities. Through these vectors, various attacks can be launched, including data theft, the distribution of malicious software, or ransomware attacks. Common forms of attack vectors include malicious email attachments, infected links, pop-up windows, and social engineering techniques. Such attacks are often motivated by financial gain, data theft, or political objectives.

   https://www.fortinet.com/resources/cyberglossary/attack-vector

8. **Authentication:** Authentication is the process by which organisations ensure that only individuals, services and applications with the appropriate authorisations can access organisational resources. It is a crucial aspect of cybersecurity, as the primary objective of malicious actors is to gain unauthorised access to systems, typically by stealing the usernames and passwords of legitimate users. The authentication process consists of three main steps: iden-

tification (declaring the user's identity, e.g. with a username), authentication (verifying the declared identity, e.g. with a password, device, or biometric data), and authorisation (checking whether the given user is permitted to access the requested resource).

https://www.microsoft.com/hu-hu/security/business/security-101/what-is-authentication

9. **Backdoor:** A backdoor is a hidden, typically malicious program or code segment that allows attackers to bypass the authentication and encryption mechanisms of a computer, network device (e.g., a router), or other embedded system. Its purpose is to provide unauthorized access to the compromised device, often granting the attacker full control. Backdoors generally operate stealthily in the background, making them difficult to detect. While their operation resembles that of other types of malware, backdoors are considered among the most dangerous because they enable surveillance of the user, modification of files, installation of new (often malicious) programs, and even attacks on additional devices. These programs often include additional capabilities, such as keystroke logging, screenshot capture, file encryption, and other activities that compromise data security. Backdoors represent a serious security risk, particularly because they do not require continuous external control to function. It is important to note, however, that such malware typically cannot infiltrate a system independently without the user's knowledge; they are usually installed alongside other software, either intentionally or through deception.

   https://avirus.hu/backdoors/

   https://en.wikipedia.org/wiki/Backdoor_(computing)

10. **Baiting:** Baiting is a form of social engineering that entices victims to accept free products, information, discounts, or rewards in exchange for providing confidential information or taking actions that pose a security risk. For example, an advertisement might invite website visitors to click on an offer to download a free movie, but to respond to the offer, the victim must provide their email address, thereby setting the stage for further identity theft attacks. Baiting attacks typically aim to trick victims into disclosing sensitive information, installing malicious software, or making payments. Criminals can target both consumers and businesses using bait. Malicious actors may use digital offers or physical items to initiate baiting attacks. In some respects, baiting is similar to phishing, but the two tactics differ in a key aspect: both rely on social engineering and deception, yet baiting offers apparent value to entice the victim into responding, whereas phishing usually offers nothing of value but masquerades as a legitimate source, exploiting trust, urgency, or

fear to provoke a response. While phishing relies on the misuse of personal data, baiting is based on fraudulent tactics.

https://www.cobalt.io/blog/cybersecurity-baiting-definition-introuduction

11. **Beaconing:** In the realm of malware, beaconing refers to the practice in which an infected computer sends short, periodic messages to a server controlled by an attacker to indicate that the malware running on the compromised machine is active, operational, and ready to receive instructions. These beacons often originate from internal, infected machines within a corporate network (such as bots or "zombies") and are directed toward external command-and-control servers. This communication strategy, also known as "calling home," enables botnet operators to automatically monitor, manage, and control hundreds or even hundreds of thousands of infected machines (VanBuskirk, 2014).

    https://en.wikipedia.org/wiki/Web_beacon

12. **Binder**: The term "binder" is frequently used in cybersecurity and antivirus software development to refer to tools that can combine two separate files into a single executable file. While similar technology is also employed for legitimate purposes in software development and system administration, the defining characteristic of binders in a cybersecurity context is that they are typically used for malicious purposes. Hackers often employ binders to conceal or mask a harmful code segment within an otherwise seemingly harmless file, thereby deceiving the average user into inadvertently executing malware or viruses on their device. In cybersecurity, a binder typically takes a legitimate file – such as an image, document, or executable program – and embeds additional malicious software or code within it. The result is a new file that appears and behaves like the original file to an unsuspecting user. When this file is opened, it performs the expected function while discreetly executing the embedded malicious code. This technique is particularly favoured by cybercriminals because it hides the true intent of the file, making detection more difficult. Binders play a key role in the distribution of many types of malware, including Trojans, worms, and other viruses. Their danger primarily arises from their everyday nature: by combining a legitimate file with hidden malicious code, most antivirus software may overlook the threat based on the file's apparent legitimacy. Such threats are harder for antivirus programs to detect because normal behaviour – such as opening a photo or document – typically does not trigger security protocols. Cybercriminals employ sophisticated techniques to make these bound files highly stealthy, including advanced encryption to

render the malicious portion unreadable or introducing decoy code segments that confuse antivirus programs without affecting the binder's operation.

https://cyberpedia.reasonlabs.com/EN/binder.html

13. **Biometric identification:** Biometric identification is based on recognising certain characteristics of the human body. These include facial, voice, iris, retina, vein, DNA, palm, and fingerprint recognition, but distinctive features can also be found in the way a person walks, signs their name, or even in their typing style. The purpose of biometric identification is to create systems that identify individuals not through codes, passwords, or documents – which may fall into anyone's possession – but on the basis of their unique personal attributes. Identification procedures may be either active or passive. Active procedures require the individual's active participation, while in passive procedures the individual's involvement is limited to sample provision (for example, using a fingerprint scanner or providing a DNA sample).

    https://www.ludovika.hu/blogok/cyberblog/2023/03/07/biometrikus-alapu-szemelyazonositas/

14. **Black Hat Hacker:** The term "black hat" refers to hackers who infiltrate computer systems and networks with malicious intent. These individuals or groups deliberately violate cybersecurity rules and laws to gain personal or financial advantage, cause harm, steal data, disable systems, or deploy ransomware. Black hat hackers typically exploit security vulnerabilities, crack passwords, use malicious software, or launch phishing attacks. Their activities are often criminal and pose a significant threat to the data security of companies, government agencies, and private individuals. They are the driving force behind most cyberattacks, standing in contrast to "white hat" hackers, who help strengthen defences by identifying security weaknesses. The term "black hat" originates from 1950s and 1960s Western films, in which villains typically wore black hats, a symbol that has since carried over into modern cybersecurity terminology with a distinctly negative connotation.

    https://www.fortinet.com/resources/cyberglossary/black-hat-security

    https://en.wikipedia.org/wiki/Black_hat_(computer_security)

15. **Bloatware:** Bloatware are typically unsolicited applications that are pre-installed by manufacturers on the devices they produce/distribute (computers, tablets and smartphones). While they are not considered malicious code in the first place, as they only provide convenience services, there have been more than one case where some pre-installed applications have been found

to hide malware or intercept users' activities, with or without the knowledge of the manufacturers.

https://makay.net/kiberbiztonsagi-fogalomtar

16. **Blocklist/Blacklist:** A blocklist, also known as a blacklist, is an access control system that prevents users, programs or networks on it from accessing certain systems or services. The purpose of the blocklist is to filter out unwanted or harmful traffic, such as spam, unauthorised access or malicious activity. Users or entities can be added to the list automatically or manually and blocked on this basis.

    https://www.infobip.com/glossary/blocklist

17. **BOT:** Short for robot, a bot is a program that performs tasks automatically. Initially, bots were used in the UNIX environment by system administrators to handle routine, repetitive tasks. Some bots automatically chat with the user or answer questions, mimicking a real, live human being. The bot can also be used for malicious purposes: a remote attacker can take control of the victim's infected computer by using a bot. The aim is exactly that: to make hundreds of thousands of infected computers remotely controllable from a single machine. Bot herders (also known as botnet operators) exploit the resources of hijacked computers to send unsolicited spam, as well as to download and store illegal software. Not infrequently, they are also used to store pornographic material or to participate in various computer attacks (DoS, DDoS), and this capacity may even be rented out for a set fee. In addition, a bot can scan the victim's hard drive and transmit confidential data to a remote website, enabling further crimes through the use of stolen personal, banking, residential, or social security information (identity theft). Such infected machines are often referred to as zombie computers.

    https://www.eset.com/hu/termektamogatas/veszelyek/

18. **Botnet:** A botnet, also known as a zombie network, consists of user devices that, as a result of a viral infection, run malware enabling them to be remotely controlled. Zombie network "commanders" are able to control the devices of their victims en masse (sometimes in the hundreds of thousands) to launch an overload attack against a specified target. This way, the attackers do not come into direct contact with the main target, but the infected devices of the victims do the work for them.

    https://makay.net/kiberbiztonsagi-fogalomtar

19. **Bug bounty:** A bug bounty, also known as a vulnerability reward programme, is an initiative in which organisations offer rewards – typically monetary – to ethical hackers or security researchers who identify security flaws or vulnerabilities in the company's systems, software, or services. The aim is to report and correct errors responsibly, before they fall into the wrong hands.

    https://www.techtarget.com/whatis/definition/bug-bounty-program

20. **Business Email Compromise:** In a business email compromise (BEC), attackers gain access to the correspondence of individual companies, monitor any requests for financial transactions (invoices, fee requests, advance requests, etc.) and send documents with fake, transcribed bank account numbers to the affected partners on behalf of the organisation, who then transfer the funds to the bank accounts managed by the attackers.

    https://makay.net/kiberbiztonsagi-fogalomtar

21. **CIRT (Computer Incident Response Team):** The CIRT, or Computer Incident Response Team, is a specialised team of highly trained information security professionals whose main task is to quickly and efficiently handle cyber security incidents and events in organisations. The primary role of CIRT is to protect IT systems and networks from potential cyber attacks and to minimise the consequences of attacks. The CIRT's activities include detecting and analysing incidents, identifying the source of attacks, implementing recovery processes, and developing defence strategies and recommendations to prevent recurrence. CIRT also works with other security units, such as CERTs (Computer Emergency Response Teams), and is actively involved in raising awareness of information security. The team's work is key to ensuring that organisations respond quickly to cyber attacks, minimise damage, maintain data security and preserve business continuity.

    https://www.group-ib.com/resources/knowledge-hub/cirt/

22. **Cookie**: A cookie is a small data packet that a browser stores at the request of a website and returns to the same website with each subsequent page load. A cookie can contain any information defined by the website. Importantly, a website can only set its own cookies and cannot access cookies from other sites. Websites frequently use cookies, for example, to manage user logins. After successful authentication, the website sends a unique identifier to the browser, which the browser stores. The browser then returns this identifier with each subsequent request, allowing the system to determine which content a particular user is permitted to access. Without this mechanism, a user,

for instance, would not be able to access their personal emails. Under European regulations, websites are required to inform users about the use of cookies. For certain types of cookies – such as those used for marketing or statistical purposes – users must provide prior, explicit consent.

https://lexiq.hu/cookie

https://en.wikipedia.org/wiki/HTTP_cookie

23. **Cross-site scripting:** This is an attack in which the attacker adds a malicious script to the content of a legitimate website. Cross-site scripting (XSS) attacks allow the attacker to execute scripts (e.g. JavaScript) written in different languages in the browsers of unsuspecting website users. Attackers can exploit XSS for session cookie theft, enabling them to impersonate the compromised users. But they can also distribute malicious software, tag websites, look for user credentials, and perform other malicious activities using XSS. In many cases it is combined with social engineering techniques such as phishing. XSS remains a consistently prevalent attack vector and ranked second on the 2023 CWE Top 25 Most Dangerous Software Weaknesses list.

    https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

    https://en.wikipedia.org/wiki/Cross-site_scripting

24. **Cryptojacking:** Cryptojacking is a method of attack in which attackers inject some form of cryptocurrency mining code into the victim's device – that is, the victim's device generates digital money for the attackers, usually in Bitcoin, Ethereum or Monero.

    https://makay.net/kiberbiztonsagi-fogalomtar

    https://en.wikipedia.org/wiki/Cryptojacking

25. **Cryptotrojan:** A cryptotrojan is a type of digital malware embedded in user software that, when the software is in use, covertly mines digital currency (cryptocurrencies) using the resources of the user's device without their knowledge, benefiting the malware's creator.

    https://makay.net/kiberbiztonsagi-fogalomtar

26. **Cyber**: The word "cyber" is an English term whose Hungarian meaning relates to computers, computing, or the virtual realm. It is typically used in combination with other words. In Hungarian, it has spread in the form "kiber". The expression originated in science fiction and later entered everyday usage. It is used in combination with another word to indicate that the referenced thing exists in a computer-based or digital form. For example, the English

term “cyberbullying” refers to online harassment, while “kiberbűnözés” denotes computer-based crime.

https://lexiq.hu/cyber

https://en.wikipedia.org/wiki/Cyber

27. **Cyber Attribution:** The purpose of cyber attribution is to determine who carried out a cyber attack, that is, to identify the identity or location of the attacker or any intermediary involved. The identification may reveal a person’s name, user account, pseudonym, or other information that can be linked to a specific individual. Geolocation can refer to a physical (geographical) location or a virtual location, such as an IP address or Ethernet address (Wheeler–Gregory, 2007).

    https://en.wikipedia.org/wiki/Cyber_attribution

28. **Cyber Threat Intelligence:** The term currently has no common Hungarian equivalent, but it is best described as an intelligence operation in which a specialised team identifies potential cyber threats that could compromise the security of data and systems in a vast amount of information gathered from a variety of sources (Open Source Intelligence, Social Media Intelligence, Deep Web, etc.).

    https://makay.net/kiberbiztonsagi-fogalomtar

29. **Cyberbullying:** Cyberbullying means online harassment using digital technologies. It can happen on social media, messaging platforms, gaming platforms and mobile phones. This is a repetitive behaviour aimed at intimidating, angering, or shaming the targets. Examples include, but are not limited to: spreading lies or posting embarrassing photos or videos of someone on social media; sending hurtful, abusive or threatening messages, pictures or videos through messaging platforms; misusing someone’s name or fake accounts to send malicious messages to others; committing sexual harassment or bullying using generative artificial intelligence tools. Harassment in person and online can often occur in parallel. However, cyberbullying leaves a digital footprint – a record that can be useful and provide evidence to stop the abuse.

    https://www.unicef.org/stories/how-to-stop-cyberbullying

    https://hu.wikipedia.org/wiki/Cyberbullying

30. **Cybercrime:** Cybercrime is a crime that targets or exploits a computer, computer network or network device. Most cybercrimes are committed by cy-

bercriminals or hackers seeking to make money. However, sometimes cybercrime is aimed at damaging computers or networks for political or personal reasons, rather than for financial gain. Cybercrime can be committed by individuals or organisations. Some offenders are organised, use advanced techniques and are highly skilled technicians. Cybercriminals targeting computers can infect devices with malware to delete or steal data. Attackers may prevent users from accessing a website or network, or prevent a business's software service from working – this is known as a denial of service (DoS) attack. By using computers for other criminal activities, cybercriminals can distribute malicious software, illegal information or illicit content. It is common for attackers to combine several methods, such as first infecting computers with a virus and then using these machines to spread further malware to other devices or networks. Some jurisdictions also recognise a third type of cybercrime, where the computer is used as an accessory to crime – for example to store stolen data.

https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

31. **Cybersecurity:** Cybersecurity is the set of processes, recommended practices and technologies that help users protect their critical systems, data and networks from digital attacks. As data is used almost everywhere and an increasing number of people work and connect from any location, perpetrators have developed extensive expertise and skills. The number of cyberattacks rises year by year as attackers continuously refine their tactics, techniques, and procedures while scaling their operations. This ever-evolving threat landscape requires organisations to establish dynamic, ongoing cybersecurity programmes to remain resilient and adapt to emerging risks. An effective cybersecurity programme combines personnel, processes, and technological solutions to mitigate the risks of operational disruption, data theft, financial loss, and reputational damage resulting from attacks. Cybersecurity is essential for protecting against unauthorized access, data breaches, and other cyber threats.

    https://www.microsoft.com/hu-hu/security/business/security-101/what-is-cybersecurity

32. **Cyberspace:** Cyberspace is an artificially created, dynamically changing domain in which interconnected information and communication devices and systems – also utilising the electromagnetic spectrum – operate to collect, store, process, transmit, and use information, thereby enabling continuous and global connectivity between people and various devices.

    https://makay.net/kiberbiztonsagi-fogalomtar

33. **Cyber warfare:** The term cyber warfare is often used to describe any kind of online threat, regardless of who the attacker or target is. However, there is a narrower definition among security professionals: an attack by one country against the infrastructure of another. The legal definition of cyber warfare includes acts that result in declaration of war, acts of war, death or destruction. However, the definition and classification of such events is often a contentious and complex issue.

    https://nki.gov.hu/figyelmeztetesek/archivum/tisztazni-kell-a-kiberfegyver-es-kiberhaboru-fogalmat/?utm_source https://nki.gov.hu/figyelmeztetesek/archivum/kiberhaboru/?utm_source

    https://en.wikipedia.org/wiki/Cyberwarfare

34. **Cyber weapon:** A cyber weapon is a digital device, malicious program or code specifically designed to steal sensitive information, cripple systems or cause significant damage. It can be aimed at disrupting critical infrastructure, such as energy networks, communications systems or health services, or at achieving military or political objectives. It can be used for offensive, defensive or dual purposes, and may involve data destruction, espionage or physical sabotage. Cyber weapons often appear in the hands of state actors, as they offer the possibility of plausible deniability, i.e. the country concerned can deny direct responsibility for the attack.

    https://www.ebsco.com/research-starters/science/cyberweapon

    https://en.wikipedia.org/wiki/Cyberweapon

35. **Dark web:** The dark web is that part of the deep web (i.e. sites not seen by traditional search engines) that can only be viewed using special software, settings or access rights. Some dark web services allow the user to bypass state censorship, browse anonymously or communicate securely with journalists, for example. In addition, the dark web is often used for illegal activities such as the sale of weapons, drugs and counterfeit goods.

    https://lexiq.hu/dark-web

36. **DDoS attack:** A DDoS (Distributed Denial-of-Service) attack is the intentional overloading of an IT service with the aim of partially or completely paralysing the service or disrupting its proper functioning. During an attack, several – often thousands – of infected devices (members of a so-called zombie network) simultaneously send too many requests to the target system, which cannot handle them and become inaccessible to users. Attackers con-

trol these devices centrally and use the mass traffic to force the target to deny service.

https://makay.net/kiberbiztonsagi-fogalomtar

37. **Deepfake:** Deepfake is a collective term for images, videos or audio material that have been modified or created using artificial intelligence-based tools or editing software. They can depict real or fictional individuals and are considered a form of synthetic media – media typically created by artificial intelligence systems by combining various media elements into a new media product. While the creation of false content is not new, deepfakes uniquely exploit machine learning and artificial intelligence techniques, including facial recognition algorithms and artificial neural networks such as variational autoencoders and generative adversarial networks. The field of image forensics, in contrast, develops techniques to detect manipulated images. Deepfakes have received widespread attention due to their potential use in producing material related to child sexual abuse, celebrity pornography, revenge porn, disinformation, scams, harassment, and financial fraud.

    https://en.wikipedia.org/wiki/Deepfake

38. **Deep web:** The deep web is the part of the web that is not visible to traditional search engines such as Google. Parts of the deep web include password-protected sections of webmail or banking sites, paid content, pages accessible only after registration, restricted medical databases, or sites that can only be accessed through specific software (e.g., the Tor browser). These pages exist in formats not indexed by search engines or are not linked anywhere, which is why search engines cannot locate them. The term is often mistakenly used as a synonym for the dark web, but the latter is actually only a small part of the deep web.

    https://lexiq.hu/deep-web

39. **Demilitarised zone (DMZ):** A demilitarised zone, also known as a demarcation zone or border network, is a physical or logical subnetwork that contains and exposes an organization's internal services to a larger, untrusted network, usually the Internet. The purpose of a DMZ is to provide an extra layer of security for an organisation's local area network (LAN). This way, an external attacker can only access the devices in the DMZ, not the entire network.

    https://hu.wikipedia.org/wiki/Demilitariz%C3%A1lt_z%C3%B3na_(informatika)

40. **Digital footprint:** A digital footprint is any information left behind by someone's online presence on the Internet or, more broadly, any data captured by some digital technology that can be linked to that person. For example, an intentional digital footprint can be a photo or post on a social networking site, a registration on a website, or a like on a post. There are also unintended footprints that some companies or states collect about us, such as the pages we visit, how much we scroll down a page and where we click. In a broader sense, a digital footprint includes, for example, call data from mobile phone use, SMS messages or CCTV footage. The resulting data is typically used to serve ads to users that interest them, but there are also dangers to digital footprints, such as their use in phishing or social engineering attacks, or for manipulative purposes. However, it can be problematic if, for example, a prospective employer makes a hiring or rejection decision based on an applicant's previous online activity. The extensive collection of data means that in most cases it is not possible to eliminate digital footprints, but it is possible to reduce them, for example by deleting previous registrations, by asking individual companies to delete stored data under the GDPR, and by checking the settings of the services used to disable the collection of certain data.

    https://lexiq.hu/digitalis-labnyom

41. **DKOM (Direct Kernel Object Manipulation):** DKOM is a technique that directly modifies data structures and objects in the operating system kernel. The main purpose is usually to hide malicious activities and circumvent security measures. In cybersecurity, DKOM is often used to hide processes, files or system keys from traditional security tools, thus allowing malicious or unauthorised operations to be carried out undetected. Detection of such attacks is extremely difficult, as the changes are made deep in the kernel and may remain invisible to standard protection solutions. Therefore, their detection requires the use of special analytical tools and advanced techniques.

    https://dotcommagazine.com/2023/09/dkom-a-fascinating-comprehensive-guide/

42. **DNS spoofing:** The domain name server (DNS) allows users to access websites by mapping domain names and URLs to IP addresses that computers use to find websites. Hackers can exploit DNS records to redirect victims to a website controlled by the attacker instead of the one they were expecting. These fake websites look exactly like the websites that users expect. As a result, victims of DNS spoofing attacks are not suspicious when they are asked to enter their account login credentials on a website they think is real.

https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

43. **DNS tunnelling:** refers to the manipulation of the DNS protocol with the aim of redirecting malicious traffic through the organisation's defence system. By using malicious domains and DNS servers, the attacker can exploit DNS to bypass network security and obtain data.

    https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

44. **DoS attack:** In a Denial-of-Service (DoS) attack, a single attacker attempts to overload and force a target into denial of service from a single source. Exploiting various vulnerabilities on the target side may at times prove effective, and such an attack can even be carried out using a single smartphone.

    https://makay.net/kiberbiztonsagi-fogalomtar

45. **Doxing:** The disclosure of an individual's or an organisation's private or personally identifiable data (in particular, information suitable for personal identification). Methods used to obtain such information include searches in publicly accessible databases and on social networking sites (such as Facebook), hacking, and psychological manipulation. Doxing is closely linked to online revenge and hacktivism. It may be carried out for a variety of reasons, including (socially positive) support for law enforcement, business analysis, but also for malicious (and potentially unlawful) purposes, such as extortion, coercion, harassment, online shaming, and revenge.

    https://sealog.hu/tudastar/fogalomtar/doxing-v-doxxing

46. **Easter Egg:** An "Easter egg" is a hidden code in computer software that performs a function outside its normal operation, sometimes installed by the manufacturer or illegally placed by the manufacturer to provide a back door. These hidden features or messages can be found in various digital platforms such as video games, websites and software applications and are popular among users, aiming to improve the user experience and showcase the creativity of developers.

    https://www.twingate.com/blog/glossary/easter-egg

47. **Encryption:** Encryption refers to technical methods that secure data and systems, making it difficult to access information or disrupt networks and transactions. In modern cryptography, encryption requires the use of an encryption algorithm or cipher to convert readable plaintext into ciphertext

(unreadable encrypted data). Encrypted text can only be decrypted into plain text by those who have been granted access to the data.

https://bitmarkets.academy/hu/crypto-for-advanced/what-are-encryption-and-decryption

48. **Ethical hacking:** Ethical hacking involves finding vulnerabilities in computer systems or networks – but instead of being used for illegal activities, ethical hackers help to develop security countermeasures. They hack into computer systems or networks with the owner's permission and in compliance with the law. They report any security risks they identify to the owner and, if necessary, inform hardware and software vendors about the vulnerabilities they find. Experts in ethical hacking are called ethical hackers, who carry out security assessments to improve an organisation's security measures.

    https://www.unite.ai/hu/what-is-ethical-hacking-how-does-it-work/

49. **Evil twin phishing:** In this method of attack, the perpetrators create a fake wireless (Wi-Fi) access point with the same name as a known, legitimate one. They then trick victims into connecting their devices to it, and subsequently monitor and intercept the online traffic of users who unsuspectingly join the network. In this way, they can gain access to sensitive data such as usernames and passwords. Users often do not even realise that they have fallen victim to an attack.

    https://kiberpajzs.hu/csalastipusok/szamitogepes/evil-twin-phishing/

50. **Exploit:** An exploit is a program or piece of code designed to detect and take advantage of a security flaw or vulnerability in an application or computer system, usually for malicious purposes such as installing malware. An exploit means the method used by cybercriminals to deliver malicious software, and not the malware itself. Exploits contain data or executable code capable of exploiting one or more software flaws on a local or remote computer. For example, a browser vulnerability may allow "arbitrary code" execution, meaning the installation and execution of a malicious application on the system, or the triggering of unexpected system behaviour without the user's knowledge. Attackers usually begin with privilege escalation, which enables them to do virtually anything on the compromised system. Browsers, Flash, Java and Microsoft Office belong to the most frequently targeted categories of software. Because of their widespread use, they are actively investigated by both security experts and hackers, while browser developers are forced to release regular patches to eliminate vulnerabilities. It is advisable to install such patches as soon as possible, but this is not always feasible. Naturally, the

exploitation of vulnerabilities discovered by criminals but as yet unknown to developers – so-called zero-day vulnerabilities – poses a unique challenge. It may take a long time before manufacturers detect and correct the problem.

https://mpost.io/hu/glossary/exploit/

51. **Firewall:** Firewalls are software programs or hardware devices that filter and examine information coming over the Internet. They represent the first line of defence, as they can prevent malware or attackers from gaining access to the network and information before any potential damage can be done. Hardware firewalls are included in some routers and require little or no configuration because they are built into the hardware itself. These firewalls monitor the traffic of computers and devices connected to the router's network, i.e. they can filter access to all devices with a single device. Hardware firewalls provide essential security for IoT devices such as smart thermostats and smart bulbs. These new devices often have weak security features that leave the network vulnerable, but a hardware firewall helps prevent such security problems.

    https://www.mcafee.com/hu-hu/antivirus/firewall.html

52. **Gray Hat Hacker:** A gray hat hacker is a person who accesses computer systems without permission to find vulnerabilities, but who does not act with the intention of causing harm or making financial gain. Their activities fall somewhere between white hat (ethical) and black hat (malicious) hackers. Although they may use illegal methods – for example, disclosing a system vulnerability without informing the administrator – their intention is often to increase security. However, because these actions are not always carried out with the knowledge or consent of the party concerned, the activities of grey hat hackers are legally and ethically divisive. Some see them as useful, others as risky from a cybersecurity perspective.

    https://www.twingate.com/blog/glossary/gray-hat-hacker

53. **Hacker:** A hacker is a person skilled in computer science, programming, who aims to find weaknesses in a computer system. A hacker (also known as cracker) most often refers to a cybercriminal who "hacks" into IT devices in order to steal the information and data they contain. In common parlance, cybercriminals are also called hackers, most of the time wrongly. Not all hackers are cybercriminals and not all cybercriminals are hackers.

    https://makay.net/kiberbiztonsagi-fogalomtar

54. **Hacktivist:** hacktivists are criminal groups that band together to carry out cyber attacks in support of political causes. Hacktivists typically target entire industries, but sometimes they also attack organisations that they believe do not share their political views or practices. In some cases, hacktivists target organisations based on their customers and business partners rather than the beliefs of the victim organisation (Wheeler–Gregory, 2007).

55. **Hoax:** Hoaxes are usually silly pranks that take the form of chain letters or so-called urban legends. Hoaxes about computer viruses attempt to instil fear, uncertainty and doubt in recipients, leading them to believe they are facing an undetectable virus. Some of these emails indeed contained malicious code that could delete files from users' computers. Ignore such messages and simply delete them. Our good fortune in life is in no way dependent on sending a warning letter to twenty of our best friends, and this method is not in any way conducive to the security of our computers, and it also causes unnecessary mail traffic.

    https://www.eset.com/hu/termektamogatas/veszelyek/

56. **Indicator of Compromise:** An IOC, or Indicator of Compromise, is a digital trace suggesting that an endpoint or network may have been compromised. Just as physical evidence can aid an investigation, these digital traces enable information security professionals to identify malicious activities or security threats, such as data theft, insider misuse, or malware attacks. Investigators may collect these indicators manually when suspicious activity is detected, but they can also be gathered automatically as part of an organisation's cybersecurity monitoring systems. Such data can be used to mitigate an ongoing attack, to remediate a security incident that has already occurred, and to develop more advanced tools capable of identifying and quarantining suspicious files in the future. Unfortunately, IOC monitoring is reactive in nature, meaning that once such an indicator is found, it is almost certain that unauthorised access or a security incident has already taken place. However, if the event is still in progress, the rapid detection of an IOC may help contain the attack in its early stages, thereby reducing its business impact. As cybercriminals continue to adopt increasingly sophisticated methods, the detection of IOCs is becoming ever more challenging.

    https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/indicators-of-compromise-ioc/

57. **Internet of Things (IoT):** The IoT, or Internet of Things, is a network of connected objects and devices that are equipped with sensors, software and other

technologies to send and receive data from other systems or devices. In the most general sense, any "thing" that can connect wirelessly to the internet can be part of the IoT. Nowadays, IoT refers in particular to devices that are designed to collect and transmit data in order to inform users or automate various operations. Whereas in the past connectivity was primarily established via Wi-Fi, today 5G and other advanced network technologies enable the fast and reliable handling of large volumes of data almost anywhere in the world.

https://www.sap.com/hungary/products/technology-platform/what-is-iot.html

58. **Intrusion Prevention System (IPS):** IPS, or intrusion prevention system, is a network security technology that monitors network traffic, identifies malicious activity and automatically prevents it from being carried out. IPS systems are capable of detecting and blocking various threats, such as malware, the exploitation of vulnerabilities, and command-and-control communications, before they reach the target system. IPS systems play a key role in modern network security, as they can detect and prevent various threats in real time, contributing to the protection of organisations' IT infrastructure.

    https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

59. **Kernel mode:** Kernel mode is the privileged mode of operation of the central processing unit (CPU) of a computer system. As a critical element of the operating system architecture, it enables the execution of all machine instructions and provides unlimited access to hardware and system resources. In this mode, the CPU has the highest level of control, so it can manage memory, hardware devices and processes.

    https://www.ituonline.com/tech-definitions/what-is-kernel-mode/

60. **Keylogger:** A keylogger is a program or hardware device that tracks and records the user's keystrokes while typing. The information collected is sent to a hacker via a so-called command-and-control server (C&C - Command and Control). The hacker then analyses the keystrokes to find usernames and passwords that can be used to gain access to otherwise protected systems. There are two types of keyloggers: a software keylogger is a malicious program that installs itself on the user's computer and can spread to other devices, while a hardware keylogger is a physical device that does not spread but can also leak sensitive information. Both types pose a serious threat to digital security, as they can give attackers access to various accounts and systems.

    https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers

61. **Killware:** Killware is a generic term for digital malware that is designed to cause physical damage or threat to critical infrastructure such as oil pipelines, water supply systems or hospitals. Examples include ransomware that specifically attack hospitals and life support systems.

    https://makay.net/kiberbiztonsagi-fogalomtar

62. **Live Response:** Live Response (or Live Triage) in cybersecurity is a real-time incident management method by which security professionals collect data from active, operational systems during a cyber attack or suspicious activity. The aim is to quickly identify threats and take the necessary steps to minimise damage. For example, running processes, network connections, log files and memory data are scanned, often with remote command line access.

    https://www.upguard.com/blog/cybersecurity-triage

63. **Logic Bomb:** A logic bomb is malicious code embedded in software that remains dormant until specific conditions are met. Once triggered, the logic bomb executes a destructive operation, such as deleting files or disrupting critical systems. Unlike traditional malware, a logic bomb does not spread actively but waits for the predefined activation event.

    https://www.beyondtrust.com/resources/glossary/logic-bomb

64. **Malvertising:** Malvertising uses online advertising networks to infect victims' computers or mobile devices with malware. Attackers place fake advertisements or malicious code on legitimate advertising networks, some of which may be displayed on websites, and these can infect victims' computers if they click on the advertisement. There have been cases where attackers placed malicious advertisements on eBay's online auction website.

    https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

65. **Malware:** The term malware covers all kinds of malicious software or code, including the most well-known types such as Trojans, ransomware, viruses, worms and banking malware. What they have in common is the malicious intent of their authors and creators. It is difficult for a general user to determine which files are malware and which are not. This is why security solutions exist that maintain huge databases of previously detected malicious patterns and apply multiple protection technologies against new ones, thus helping effective detection. Malware writers have unfortunately been very creative lately. Their "products" spread through vulnerabilities in outdated systems, by circumventing previous security rules, hiding in memory or going undetected by mimick-

ing known applications. But even today, the weakest link to the most effective infections is the user. Well-crafted emails with malicious attachments are a proven yet inexpensive way to compromise a system.

https://www.eset.com/hu/malware/

66. **Malware-based phishing:** A common phishing method. Such attacks include, for example, malware disguised as a legitimate email attachment (such as a CV or bank statement). In some cases, opening attachments containing malware can even cripple an entire IT system.

    https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing

67. **Man in the middle attack:** In a MitM attack, the communication between two parties is intercepted and manipulated by an attacker, who gains unauthorised access and presents themselves to each party as the other. As a result, both parties believe they are communicating directly with each other, while in reality, they are both interacting solely with the attacker. This allows the attacker to circumvent unprepared challenge/response protocols by simply forwarding the challenge to the other party and then relaying the response back. A successful MitM attack enables attackers to capture or manipulate sensitive personal information, such as login credentials, transaction details, account data, and credit card numbers. These attacks often target users of online banking applications and e-commerce websites, frequently employing phishing emails to infect users with malware that facilitates the attack.

    https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

68. **Man in the Disk:** A MitD vulnerability allows a third party – whether an individual or malicious code – besides the vulnerable software and its user, to gain access to and/or modify the locally stored data and components of the software.

    https://makay.net/kiberbiztonsagi-fogalomtar

69. **Multifactor Authentication (MFA):** Multifactor authentication is a security procedure that requires the user to provide not one, but at least two different authentication factors to log in. These factors are categorised into three types: something the user knows (e.g., a password or PIN), something the user possesses (e.g., a mobile phone or security key), and something the user is (e.g., a fingerprint or facial recognition). Multifactor authentication aims to signifi-

cantly reduce the chances of unauthorised access and increase the security of online accounts and data.

https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

70. **Nigerian-type scams:** The "Nigerian-type" scam is one of the oldest forms of deception, which became widespread at the end of the 19th century and is also referred to as Nigerian letters or 419 fraud. Initially, it spread through traditional postal services or fax, but with the development of telecommunications and the rise of the internet and email, this type of scam has largely moved online. In Nigerian scams, perpetrators use deceptive communication – typically via email – to persuade victims to transfer money, meaning the clients themselves make the payment. The fraudulent messages usually request assistance from the recipient, such as recovering the assets of refugees, reclaiming an unlawfully seized inheritance, or accessing temporarily unavailable funds. A variation of the Nigerian scam also circulates on social media and online dating platforms, in which the perpetrator establishes a romantic relationship with a prospective victim before requesting money under the guise of a touching story. The deceptive narrative is supported by seemingly genuine but fake social media profiles and documents that appear authentic but are also fictitious. To make the story more convincing, scammers may initiate an international transfer, only to reverse it, demonstrating that the funds are supposedly available but obstructed by an administrative issue cited in the message. The assistance requested in the email generally involves transferring a specific sum of money. In return, the victim is promised a substantial reward, which they never receive, while the transferred funds are lost. Another common tactic involves requesting the recipient's bank account details to "facilitate the transfer of assets", which, instead of depositing funds, gives the perpetrators access to the account and may result in it being emptied.

    https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/nigeriai-csalas

71. **Online Fraud:** Online fraud – also known as cyber fraud or internet fraud – encompasses unlawful activities aimed at deceiving individuals or organisations to obtain financial or other advantages. These scams rely on various methods and exploit the anonymity and wide accessibility of the internet. Their consequences can include data loss, financial damage, or reputational harm.

    https://www.fraudsmart.ie/personal/fraud-scams/online-fraud/

72. **OSINT:** OSINT (Open Source Intelligence) is an intelligence method that collects and analyses publicly available information to obtain intelligence, for example on the Internet. The purpose of OSINT is to collect, select, analyse, assess and use information relevant for intelligence purposes, such as security, but it can also be used by other organisations and individuals.

    https://makay.net/kiberbiztonsagi-fogalomtar

73. **Payload:** A malicious routine, often referred to as a payload, is the function that a piece of malware – such as a virus, worm, or Trojan – actually executes once it has infiltrated a system. This supplementary function serves the attacker's original purpose. Malicious routines can take many forms, including: data theft (stealing sensitive information such as passwords, credit card details, or personal files); file modification or deletion (destroying or overwriting important documents or system components); system crashes (rendering the computer inoperable); disk overwriting (irreparably damaging the data on a hard drive); and BIOS overwriting (corrupting the computer's fundamental boot program, preventing startup). It is important to note that not all malware causes immediately noticeable damage. Some older viruses, for instance, produced only minor, disruptive effects – such as generating sounds when keys were pressed – without harming the system, though they still inconvenienced the user. In the case of Trojan programs, the malicious activity is a hidden function intentionally concealed by the creator. This function represents the program's true purpose and may appear, for example, as a data-stealing module hidden behind an application that appears legitimate.

    https://www.eset.com/hu/termektamogatas/veszelyek/

74. **PDoS attack:** A Permanent Denial-of-Service (PDoS) attack involves an attacker attempting to render a specific service or system application permanently unavailable through physical or hardware damage. This is in contrast to traditional DoS (Denial of Service) attacks, which make the service unavailable through overloading. PDoS attacks can be dangerous, as they can make the service unavailable for extended periods of time and even cause physical damage.

    https://makay.net/kiberbiztonsagi-fogalomtar

75. **Penetration test:** A penetration test is an assessment of an IT system (server, website, etc.) for security (software, configuration) vulnerabilities. In contrast to vulnerability testing, penetration testing not only assumes the exist-

ence of a vulnerability from the responses and behavioural patterns sent by the subject, but also tests their exploitability using offensive methods.

https://makay.net/kiberbiztonsagi-fogalomtar

76. **Phishing:** a form of fraud targeting clients through deceptive emails intended to persuade the recipient to disclose personal, financial, or security-related information. These emails can appear identical to messages sent by legitimate banks: the scammers replicate the logos, appearance, and style of genuine emails and may even include details from previous (real or fake) correspondence. They are generally urgent in tone, for example threatening penalties if the recipient does not respond, or instructing them to download an attachment or click on a link. Cybercriminals exploit the fact that people are often busy: on a cursory glance, the fake emails appear authentic. As a result, recipients are more likely to take them seriously and act as instructed.

    https://kiberpajzs.hu/csalastipusok/emailes/phishing/

77. **Phreaking:** Phreaking refers to activities that study, experiment with, or explore telecommunications systems, such as equipment and networks connected to public telephone systems. In phreaking, unauthorized individuals manipulate or bypass the operation of telephone systems using technical tools to make free calls or gain access to confidential parts of the network. Originally, it pertained to fraud involving analogue telephone networks, but with the advancement of digital technology, the practice has expanded to include the hacking of modern communication systems.

    https://www.ninjaone.com/it-hub/endpoint-security/what-is-phreaking/

78. **Polymorphic virus:** Polymorphic viruses are complex codes that are able to generate modified versions of themselves with each infection, while retaining basic functional routines. To avoid source code disclosure, the virus code is encrypted and different encryption keys are used each time. Their operation is based on a mutation engine, which alters the decryption routine with each new infection. As a result, a polymorphic virus does not use static code, making it more difficult for traditional antivirus software to detect. Advanced mutation engines can generate billions of different decoding routines, further enhancing the virus's ability to evade detection.

    https://www.trendmicro.com/vinfo/us/security/definition/polymorphic-virus

79. **Pretty Good Privacy (PGP):** PGP is encryption software designed to provide privacy, security and authentication for online communication systems. Although initially only used to protect email messages and attachments, PGP is

now widely used for a wide range of applications, including digital signatures, full disk encryption and network protection. One of the most common uses of PGP is to protect emails. An email protected with PGP is transformed into an unreadable character string (encrypted text) that can only be deciphered using the appropriate decryption key. Its operational mechanisms are essentially the same as those used for securing text messages, and there are software applications that allow PGP to be integrated with other applications, effectively providing an encryption system for otherwise unsecured messaging services. While PGP is primarily used to secure internet communications, it can also be applied to encrypt certain devices. In this context, PGP can be used to encrypt partitions on a computer or mobile device. With hard drive encryption, the user must enter a password at every system startup.

https://academy.binance.com/en/articles/what-is-pgp

80. **Psychological manipulation (social engineering):** Psychological manipulation is a strategy employed by individuals or groups to manipulate people, through deception, into disclosing sensitive information or performing actions that compromise their security. The method is based on psychology and human behaviour rather than technical expertise. Psychological manipulation attacks often involve the attacker posing as a trusted person or source to gain the victim's trust. The tactics used by attackers include impersonation, persuasion and deception to obtain valuable information such as passwords, financial data, systems and network access details. Psychological manipulation attacks can take several forms. This strategy is all about exploiting human vulnerabilities to achieve their goals, whether it's unauthorised access, data theft or theft of money.

    https://www.consilium.europa.eu/hu/policies/cybersecurity-social-engineering/

81. **Punitive routine:** see Payload

82. **QR code scams:** In this type of fraud, perpetrators exploit the fact that users cannot know in advance what will happen when a QR code is scanned, forcing them to trust its creator. The aim of the scam is phishing: attackers attempt to gain access to personal or bank account information. QR codes are placed on fake websites or stickers, and various tricks are used to encourage people to scan them. QR codes contain data and function as links or references, which may lead to a fraudulent website, a malicious application download link, or even an automatic payment operation. It is common for attackers to exploit the branding of legitimate organisations, replacing

original QR codes on official posters, advertisements, or leaflets with their own.

https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/qr-kodos-csalas

83. **Ransomware:** Ransomware is a type of malicious software or malware that cybercriminals use to prevent access to, destroy or disclose a victim's critical data unless a significant ransom is paid.Traditional ransomware threatens both individuals and organisations, but two recent developments – human-operated ransomware and ransomware-as-a-service – pose an increasing threat to businesses and other large organisations. In human-operated ransomware, a group of attackers use collective intelligence to gain access to corporate networks. Before installing the ransomware, they will research the company to identify vulnerabilities and, in some cases, uncover financial documents that can be used to determine the ransom amount. The ransomware-as-a-service model involves a team of organised criminal developers creating the ransomware and then hiring other cybercriminal affiliates to infiltrate the target organisation's network and deploy the ransomware. The two groups share the profits in agreed shares. All ransomware causes significant losses to the individuals and organisations under attack. It can take days, weeks or even months to bring the affected systems back online, resulting in a loss of productivity and sales. The reputation of organisations can also be damaged among customers and the community.

    https://www.microsoft.com/hu-hu/security/business/security-101/what-is-ransomware

84. **Romance Scam:** Romance scams are a form of fraud in which scammers pretend to have romantic intentions in order to gain the sympathy of their victims and then use their goodwill to trick them into sending them money under various false pretexts. The selection of the target group has psychological motivations, as it has been observed that an older, single woman is most likely to experience loneliness, which carries the risk of her being more careless than average in the hope of forming a romantic relationship. In such cases, scammers also exploit the human tendency for rationality and sound decision-making to be sidelined in situations where emotions take precedence. Unfortunately, the justification for fraud and its growing trend is that people are not sufficiently aware of it. If they were able to recognise the scammers and their tricks, they would soon disappear from public life, because it would not be worth the energy invested. The techniques, stories

and minor details used vary from one case to another, but generally speaking, the main points mentioned are common to all these types of scams.

https://nki.gov.hu/wp-content/uploads/2024/02/A-romantikus-csalas.pdf

85. **Rootkit:** A rootkit is a malicious program that allows cybercriminals to gain undetected access to computing devices and take control of a computer. Initially, rootkits were released for the UNIX operating system (including Linux platforms), and were a collection of tools that could be used by an attacker to gain administrative privileges within a system (called "root" privileges under UNIX). The term rootkit is commonly used on Windows-based systems to describe programs that hide running processes, files or registry keys from the operating system or the user. Such a rootkit installed on Windows uses features that not only allow it to hide itself, but also to make other malicious code – such as a keylogger – undetectable. Rootkits are not necessarily used solely for creating malicious code, but in recent times this stealth technique has been increasingly employed by malware developers.

    https://www.eset.com/hu/termektamogatas/veszelyek/

86. **Sandbox:** Sandboxing is a cybersecurity practice that employs an isolated execution environment, or "sandbox," where security teams within a Security Operations Center (SOC) can detonate, monitor, analyse, detect, and block suspicious findings as part of the incident response cycle. This method provides an additional layer of defence against unknown attack vectors. By using a sandbox, security teams can conduct advanced malware analysis by executing suspicious files in a controlled environment that emulates the end-user's operating system. The primary advantage of sandboxing is that it allows the observation of the behaviour of executable files, scripts, or malicious documents, enabling the detection of entirely new and previously unknown malware, as well as malware specifically designed to run in a particular environment. This represents the next evolutionary step following signature-based detection implemented by traditional antivirus (AV) engines.

    https://hungarian.opswat.com/blog/what-is-sandboxing

87. **Security through obscurity:** The principle of "security through obscurity" advocates the removal of any technical information (e.g. software types and version numbers, internal network IP addresses, etc.) from interfaces accessible to potential attackers (e.g. HTTP headers, server software banners, etc.) that could facilitate the success of an attack.

    https://makay.net/kiberbiztonsagi-fogalomtar

    https://en.wikipedia.org/wiki/Security_through_obscurity

88. **Scams:** Scams are very similar to phishing, but the aim is not to steal personal data, but to manipulate human emotions (social engineering): to create pity or to rely on human greed. For example, almost every natural disaster – such as earthquakes, storms, floods, wars, or famines – is quickly followed by fraudulent schemes in the form of purported charitable appeals. Another category of scams relates to fees, often referred to as Nigerian-type or 419 scams, in which perpetrators entice the target with the promise of accessing a large sum of money if they assist in transferring assets from an African country. These schemes invariably rely on requesting the victim to send an advance payment for administrative purposes, which can amount to several thousand dollars. In some cases, a deceived victim travelling to the country in question may even be kidnapped or killed. In less extreme instances, many people have lost thousands of dollars through such scams. Here are some practical tips for avoiding these fraudulent schemes: legitimate charitable organisations only contact individuals who have explicitly requested or consented to receive such emails – a practice known as "opted in". Unsolicited, spam-like messages are almost always scams, and they tend to appear very quickly following disasters or other extraordinary events. A healthy degree of scepticism is therefore essential. Fraudulent emails often imitate the formatting and graphical elements of genuine organisations' communications, making them appear almost entirely authentic. Many of these messages include tragic stories about disaster victims to elicit emotional responses.

    https://www.eset.com/hu/termektamogatas/veszelyek/

89. **Script Kiddie:** The term "script kiddie" is a derogatory term coined by computer hackers to describe immature but often equally dangerous individuals who exploit Internet vulnerabilities. Script kiddies use existing, well-known techniques, programs and scripts to find and exploit weaknesses in computers connected to the Internet. Their attacks are random and they have little knowledge of the tools they use, how they work and the damage they cause. Script kiddies are typically motivated by simple, personal reasons – entertainment, causing chaos, seeking attention, or revenge.

    https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie

90. **Smishing:** Smishing (a combination of the words SMS and phishing) is a scam in which attackers use SMS to try to obtain personal, financial or security information. They disguise themselves as a trusted source, pretending to be a bank, card issuer, courier, utility or some other service provider. The message asks the recipient – usually in an urgent manner – to open a link to a website, install an

application or call a phone number to check, update or reactivate their account, for example. The link is to a fake website and the phone number is to a scammer pretending to be from the company. The purpose of the fraud is to obtain information that can then be used to steal the unwary customer's money.

https://kiberpajzs.hu/csalastipusok/sms/smishing/

91. **Social engineering:** Social engineering is a security attack technique in which the attacker employs psychological manipulation to deceive or persuade individuals into disclosing confidential information, granting access, or performing actions that would normally be disallowed or unsafe. This method does not rely on technical tools, such as software or hardware exploits, but instead exploits human trust, inattentiveness, or goodwill. Social engineering can take various forms, including phone scams, email phishing, or in-person persuasion, with the objective of causing the victim to unwittingly assist the attacker in obtaining sensitive data or system access.

    https://en.wikipedia.org/wiki/Social_engineering_(security)

92. **Spam:** Spam is any unsolicited digital communication sent in bulk. Spam often comes in the form of email, but it can also spread via text messages, phone calls or social media. Spammers use many forms of communication to send unsolicited messages in bulk. Some of these are marketing messages offering unsolicited goods. Other types of spam messages can distribute malware, trick the recipient into giving out personal information, or scare them into thinking they have to pay to avoid trouble. Many of these types of messages are filtered by email spam filters, and telephone operators often warn about the "spam threat" from unknown callers. Whether it comes via email, SMS, phone or social media, some spam messages will get through; it's worth recognising them and avoiding these threats.

    https://www.malwarebytes.com/spam

93. **Spear phishing:** The method of spear phishing is employed when an attacker specifically targets an individual or their company in an attempt to gain access to confidential information, such as trade secrets, sensitive technological designs, or classified governmental communications. In some cases, the individual may serve merely as an entry point to reach another person or organisation. Since the potential gains are considerable, attackers are willing to invest significant time and resources in mapping out their targets. For instance, a foreign government may consider a particular company to be developing a product or technology crucial to its economy and therefore decide to attack it. They examine the company's website, identify several key figures,

and compile complete dossiers on them. After analysing these individuals, the attackers craft a spear phishing email, for example in the name of one of the company's suppliers. The email contains an attachment that appears to be an invoice but is in fact a file embedding malicious code. Approximately 50–60% of recipients are deceived into opening the attachment, thereby granting the attacker access to their computer. Spear phishing poses a far more serious threat than generic phishing attacks, as the attackers design personalised operations against a select group of individuals. This not only increases their chances of success but also renders detection significantly more difficult.

https://www.biztonsagosinternet.hu/tippek/szemelyes-biztonsag-az-interneten/celzott-adathalaszat

94. **Spoofing:** Spoofing generally refers to the process of altering or falsifying the identity of the information sender, thereby concealing it. Caller ID spoofing is a specific technique used in vishing (fraudulent banking calls) and other phishing activities. In this method, attackers modify the number displayed on the recipient's phone, hiding the true identity of the caller. Consequently, the recipient sees a different number – often one that appears familiar, such as a bank's number – making the call seem more legitimate. The primary goal of such calls is to build trust and bypass the first line of defence against phishing attacks: vigilance. Displaying a familiar number increases the likelihood that the victim will cooperate, disclose sensitive information, install applications, or carry out financial transactions as instructed by the attacker.

    https://kiberpajzs.hu/csalastipusok/telefonos/spoofing/

95. **Spyware:** Spyware is tracking software that is installed on a computer without the user's knowledge or consent. It aims to monitor user habits, sensitive data such as browsing history, passwords, bank identifiers, and transfer them to unauthorised third parties. Some spyware enters a system as components of other programs, similarly to Trojan applications, or as part of computer worms. Sometimes they are installed on the device through vulnerable websites in a hidden way. There are also fake anti-spyware programs that are in fact spyware themselves. In a broader sense, according to the Anti-Spyware Coalition, spyware includes unsolicited monitoring and data collection software such as some cookies, commercial keyloggers and other tracking technologies.

    https://www.eset.com/hu/termektamogatas/veszelyek/

96. **SQL Injection:** In an SQL Injection attack, the attacker – or an authorized ethical hacker – enters code or character strings into an online input interface

(such as a search field, registration form, or login form) that, during server-side processing, allows manipulation of the database, potentially including modifications, to which they would not normally have access.

https://makay.net/kiberbiztonsagi-fogalomtar

97. **Synthetic identity theft:** This method involves not only the theft of personal data but also the creation of a fictitious digital persona. Data is collected from various sources, such as national identifiers, birth dates, email addresses, phone numbers, and residential addresses. The resulting synthetic identity can appear legitimate at first glance, as it is constructed from real information. The fraudsters then bring this persona to life in the digital space, exhibiting behaviour similar to that of real individuals and maintaining activity on social media, e-commerce platforms, forums, and online communities. In doing so, they create the appearance of a credible, seemingly real person.

    https://www.fintechradar.hu/fintech/0603/novekvo-fenyegetest-jelent-a-szintetikus-szemelyiseglopas/

98. **Time Bomb:** A time bomb is a malicious piece of code that is embedded in software and is only activated at a predefined time. In contrast, the activation of other types of malware often requires some user action or the fulfilment of a specific condition. A time bomb, however, relies on the passage of time: it remains hidden and undetected until its predetermined activation moment. This characteristic makes it particularly insidious. It is often deliberately timed to coincide with significant events or dates to cause maximum disruption or damage, such as data loss, system shutdowns, or other unauthorized activities.

    https://www.twingate.com/blog/glossary/time-bomb

99. **Trojan Horse:** The "Trojan" – whose story originates from Greek mythology – is a program that performs functions other than those it claims to carry out. These functions are not necessarily destructive or harmful in every case, but often they are: they may delete files, overwrite the hard drive, or provide the attacker with remote access to the system. A classic Trojan usually includes a keylogger, disguised by its creators as a game or some useful utility. Such Trojans may be deployed for a variety of purposes: to enable hidden remote access (backdoor) to a given computer, to monitor keystrokes, or to specialise in stealing passwords (most spyware falls into the latter category).

    https://www.eset.com/hu/termektamogatas/veszelyek/

100. **Virus:** A virus is a malicious program that can reproduce itself – either in identical or modified form – into another executable code. Viruses may ex-

ploit different types of host programs, the most common being: executable files (computer programs), boot sectors (which indicate to the computer where to find the data required for the start-up process), script codes (in scripting languages such as Windows Scripting or Visual Basic), and macro instructions embedded in documents (these have lost significance since Microsoft Windows no longer executes them by default). When a virus embeds its own copy into another executable code, this ensures that the virus code is executed whenever the original program runs, spreading further by continuously seeking new, clean, and vulnerable programmes during execution. Some viruses overwrite the original program code – thereby destroying the original program – but in most cases they attach themselves in such a way that both the host program and the virus code remain operational. Depending on the coding, viruses can spread through many different file types, via network shares, within document files, and even in the boot sectors of disks. While some viruses also spread through email messages, the majority of malicious software appearing in electronic mail is classified as worms. A virus merely needs to ensure the replication of itself; it does not necessarily have to contain a destructive routine or become widely disseminated.

https://www.eset.com/hu/termektamogatas/veszelyek/

101. **Vishing:** Vishing (a combination of the English words "voice" and "phishing") is a telephone scam in which the attacker tries to trick victims, usually bank customers, into sharing personal, financial or security information or transferring money. A typical form of vishing is when the phishing caller tries to make the user believe that they are actually talking to a bank employee and are calling about a financial transaction error or suspected fraud.

     https://kiberpajzs.hu/csalastipusok/telefonos/vishing/

102. **Vulnerability assessment:** A vulnerability assessment involves evaluating an IT system (such as a server or website) for security weaknesses, including software or configuration vulnerabilities. Unlike penetration testing, a vulnerability assessment infers the presence of vulnerabilities based on the responses and behavioural patterns exhibited by the system under examination, without actively testing their exploitability through offensive methods.

     https://makay.net/kiberbiztonsagi-fogalomtar

103. **Wallet recovery:** A wallet recovery phrase is a security mechanism created when a cryptocurrency wallet is used. This is a predefined sequence of usually 12-24 words that allows the user to recover the wallet in case they lose access or forget the password. With the wallet recovery phrase in hand, anyone can access the wallet again, so it is vital that the code is stored securely.

The loss or disclosure of the recovery phrase can result in a complete loss of access to cryptocurrencies.

https://nki.gov.hu/it-biztonsag/tudastar/mi-az-a-wallet-recovery-phrase/

104. **Wangiri:** Wangiri, originating in Japan, has become one of the most widespread types of fraud thanks to mobile phones. The essence of this scheme is that fraudsters, as part of mass-generated computerised calls, contact their victims from unfamiliar, usually foreign numbers – typically with African country codes beginning with 2, or Central American country codes beginning with 5. They end the call after just one or two rings in the hope of prompting a return call. However, returning the call is charged at a much higher rate than a domestic one, and the fraud succeeds even if the call appears unsuccessful: for instance, if it keeps ringing without answer, does not connect at all and cuts off, or continuously signals a busy line.

https://kiberpajzs.hu/csalastipusok/telefonos/wangiri/

105. **Wardriving:** Wardriving is the activity of searching for WiFi networks from a moving vehicle – such as a car, bike or even on foot – using smart devices and free software. Its primary purpose is typically the identification of vulnerable or open networks, which may later be exploited for unauthorised use, though ethical hackers also employ it to detect security flaws. The term originates from the film WarGames (1983), and in its current sense was introduced by security researcher Pete Shipley in 2000. Data collected during wardriving is often displayed on maps (so-called access point mapping). In recent years, its significance has declined due to the widespread adoption of modern encryption technologies.

https://www.kaspersky.com/resource-center/definitions/what-is-wardriving

106. **Watering hole attack:** In a watering hole attack, the attacker exploits a security vulnerability to insert malicious code into a legitimate website, so that when users visit the site, the code automatically infects their computer or mobile device. One form of watering hole attack involves identifying and exploiting security gaps left open on regularly visited websites. Attackers typically carry out such attacks on sites that attract a large number of visitors who have access to information the attackers seek to obtain. For instance, a security researcher discovered that attackers had used a Portuguese-language strategic consultancy website to infect European and South American visitors with spyware. Watering hole attacks are usually silent and invisible, and they are often detected only after damage has already been done.

https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

107. **Whaling:** Whaling refers to attacks in which perpetrators target high-profile individuals, such as business executives or celebrities. These attackers often conduct thorough research on their targets to identify an opportune moment to steal login credentials or other sensitive information. Given the high-value nature of such targets, attackers can achieve substantial gain from a successful whaling attempt.

https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing

108. **White Hat Hacker:** A white hat hacker, also known as an ethical hacker, is an IT professional who is licensed and legally allowed to investigate security flaws in systems, software or networks in order to prevent malicious attacks. They only conduct tests on systems for which they have received authorisation, often within the framework of bug bounty programmes that reward the responsible disclosure of vulnerabilities.

https://www.techtarget.com/searchsecurity/definition/white-hat

109. **Wildcard certificate:** A wildcard certificate is typically a server-side security certificate in which the "Subject Alternative Name" field includes not only the primary domain's www subdomain, but also multiple other domain variations using the * wildcard (e.g. *.makay.net). This issuance and request policy should be avoided due to the associated security risk, as a single security incident affecting one server using the certificate may result in unauthorised access to, and compromise of, the communication of the other servers as well.

https://makay.net/kiberbiztonsagi-fogalomtar

110. **Worm:** In computer terminology, worms are a subset of viruses, and although they have the ability to replicate themselves, they do not require a host file to infect. Just as viruses infect programs, worms infest systems. Such worms are able to spread extremely quickly over networks containing vulnerabilities, without even requiring user intervention. The worm is usually spread by infected email messages containing code that exploits a computer vulnerability and the email itself conveys an enticing and interesting message. Worms are usually much easier to remove than viruses because they do not infect files and can be easily deleted. The worm usually makes sure that it can run every time the system boots by manipulating the Startup Folder or Registry entries.

https://www.eset.com/hu/termektamogatas/veszelyek/

111. **Zero Trust:** The "Zero Trust principle" refers to a security approach based on the assumption that unauthorised access to, or a security incident within, our systems is inevitable – and has quite possibly already occurred – therefore no system component or access attempt can be considered trustworthy. The model focuses on protecting access to data, assets, applications and services (DAAS), which must be ensured through strict verification, regular reassessment, and continuous monitoring of network threats. It is important to recognise that its implementation is a highly time- and resource-intensive process, particularly when attempting to transform an existing IT infrastructure.

https://nki.gov.hu/it-biztonsag/hirek/nsa-utmutato-a-zero-bizalmi-biztonsagi-modell-megvalositasahoz/

SUMMARY

At the time of its compilation, this cyber security glossary contains 111 core cyber-related concepts and the English equivalents for 33 Hungarian terms, providing a necessary reference for those interested in, or working within, the field of cyber security to navigate this evolving domain.

The glossary will remain relevant over time if, alongside this first printed edition, an electronic version – anticipated to be available at www.kiberpajzs.hu – is continuously expanded and updated. In this endeavour, the support of professionals specialising in cyber issues is expected and welcomed.

REFERENCES

Binance Academy https://academy.binance.com/en/.

Avirus https://avirus.hu/.

BitMarkets Academy https://bitmarkets.academy/.

Cyberpedia – ReasonLabs https://cyberpedia.reasonlabs.com/.

DotCom Magazine https://dotcommagazine.com/.

Wikipédia https://www.wikipedia.org/.

OPSWAT Magyarország https://hungarian.opswat.com/.

KiberPajzs https://kiberpajzs.hu/.

Lexiq https://lexiq.hu/.

Makay.net https://makay.net/.

Mpost.io https://mpost.io/.

Nemzeti Kibervédelmi Intézet https://nki.gov.hu/.

Perception Point https://perception-point.io/.

Sealog https://sealog.hu/.

Webshop Automatizálás https://webshopautomatizalas.hu/.

BeyondTrust https://www.beyondtrust.com/.

Biztonságosinternet.hu https://www.biztonsagosinternet.hu/.

Cobalt.io https://www.cobalt.io/.

Európai Unió Tanácsa https://www.consilium.europa.eu/.

CrowdStrike https://www.crowdstrike.com/en-us/.

EBSCO https://www.ebsco.com/.

FintechRadar https://www.fintechradar.hu/.

Fortinet https://www.fortinet.com/.

FraudSmart https://www.fraudsmart.ie/.

Group-IB https://www.group-ib.com/.

Infobip https://www.infobip.com/.

ITU Online https://www.ituonline.com/.

Kaspersky Magyarország https://hu.kaspersky.com/.

Ludovika Egyetem https://www.ludovika.hu/.

Malwarebytes https://www.malwarebytes.com/.

Mcafee https://www.mcafee.com/.

Microsoft Magyarország https://www.microsoft.com/hu-hu/.

Magyar Nemzeti Bank https://www.mnb.hu/web/fooldal.

NinjaOne https://www.ninjaone.com/.

Palo Alto Networks https://www.paloaltonetworks.com/.

SAP Magyarország https://www.sap.com/hungary/index.html.

TechTarget https://www.techtarget.com/.

TrendMicro https://www.trendmicro.com/en_gb/business.html.

Twingate https://www.twingate.com/.

UNICEF https://www.unicef.org/.

Unite.AI https://www.unite.ai/.

UpGuard https://www.upguard.com/.

ZTS Hungary https://www.zts.hu/.