Cyber Security Glossary

by Breakwater IT

Use our Cyber Security Glossary to help you understand some of the common terminology used when discussing security measures.

A

Antivirus
Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Attacker
Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

B

Blacklist
A list of entities (users, devices) that are either blocked, denied privileges or access.

Botnet
A network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge.

Breach
An incident in which data, computer systems or networks are accessed or affected in a non-authorised way.

Brute force attack
Using a computational power to automatically enter a huge number of combination of values, usually in order to discover passwords and gain access.

C

Cloud
Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services. Resources can include infrastructure, platform or software services.

Credentials
A user's authentication information used to verify identity - typically one, or more, of password, token, certificate.

Cyber Attack
Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber Incident
A breach of the security rules for a system or service - most commonly;

- Attempts to gain unauthorised access to a system and/or to data.
- Unauthorised use of systems for the processing or storing of data.
- Changes to a systems firmware, software or hardware without the system owners consent.
- Malicious disruption and/or denial of service.

Cyber Security
The protection of devices, services and networks — and the information on them — from theft or damage.

D

Data at Rest
Describes data in persistent storage such as hard disks, removable media or backups.

Data breach
The unauthorised movement or disclosure of information, usually to a party outside the organisation.

Decryption
The process of deciphering coded text into its original plain form.

Dictionary Attack
A type of brute force attack in which the attacker uses known dictionary words, phrases or common passwords as their guesses.

Digital Footprint
A 'footprint' of digital information that a user's online activity leaves behind.

Denial of Service (DoS)
When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Download Attack
The unintentional installation of malicious software or virus onto a device without the users knowledge or consent. May also be known as a drive-by download.

E

Encryption
A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End User Device (EUD)
Collective term to describe modern smart phones, laptops and tablets that connect to an organisation's network.

Endpoint
A collective term for internet-capable computer devices connected to a network – for example, modern smart phones, laptops and tablets are all endpoints.

Ethical hacking
The use of hacking techniques for legitimate purposes – i.e. to identify and test cyber security vulnerabilities. The actors in this instance are sometimes referred to as 'white hat hackers'.

F

Firewall
Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to or from a network.

H

Hacker
In mainstream use as being someone with some computer skills who uses them to break into computers, systems and networks.

I

Incident
A breach of the security rules for a system or service, such as:

- attempts to gain unauthorised access to a system and/or data
- unauthorised use of systems for the processing or storing of data
- changes to a systems firmware, software or hardware without the system owners consent
- malicious disruption and/or denial of service

Insider Risks
The potential for damage to be done maliciously or inadvertently by a legitimate user with privileged access to systems, networks or data.

ISO 27001
The gold standard in information security management systems (ISMS), demonstrating the highest level of accreditation.

M

Macro
A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Malvertising
Using online advertising as a delivery method for malware.

Malware
Malicious software - a term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals.

Mitigation
Steps that organisations and individuals can take to minimise and address risks.

Mobile Device Management (MDM)
A type of security software, specifically for monitoring, managing and securing mobile, tablet and other devices, allowing remote administration and management of the device.

N

Network
Two or more computers linked in order to share resources.

P

Patching
Applying updates to firmware or software to improve security and/or enhance functionality.

Pentest
Short for penetration test. An authorised test of a computer network or system designed to look for security weaknesses so that they can be fixed.

Pharming
An attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address.

Phishing
Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Proxy server
A go-between a computer and the internet, used to enhance cyber security by preventing attackers from accessing a computer or private network directly.

R

Ransomware
Malicious software that makes data or systems unusable until the victim makes a payment.

Router
A network device which sends data packets from one network to another based on the destination address. May also be called a gateway.

S

Security perimeter
A well-defined boundary within which security controls are enforced.

Smishing
Phishing via SMS: mass text messages sent to users asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website.

Social engineering
Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Spam
The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spear-Phishing
A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Spoofing
Faking the sending address of a transmission to gain unauthorised entry into a secure system.

T

Token
In security, a token is a physical electronic device used to validate a user's identity. Tokens are usually part of the two-factor or multi-factor authentication mechanisms. Tokens can also replace passwords in some cases and can be found in the form of a key fob, a USB, an ID card or a smart card.

Trojan
A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

Two-Factor Authentication (2FA)
The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

V

Virus
Programs which can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.

Virtual Private Network (VPN)
An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

Vulnerability
A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.

W

Whaling
Highly targeted phishing attacks (masquerading as a legitimate emails) that are aimed at senior executives.

Whitelist
A list of entities that are considered trustworthy and are granted access or privileges.