HISCOX

CYBERCLEAR®

Hiscox CyberClear glossary

Unscrambling cyber security terms

Hiscox CyberClear glossary

HISCOX
CYBERCLEAR®

Access control
The process of granting or denying specific requests or attempts to:
- obtain and use information and related information processing services; and
- enter specific physical facilities.

Advanced persistent threat (APT)
A type of high-level targeted attack carried out by an attacker who has time and resources to plan an infiltration into a network. These are usually seeking to obtain information, proprietary or economic, rather than simple financial data. APTs are persistent in that the attackers may remain on a network for some time and usually bypass regular security controls.

Air gap
The physical separation or isolation of a system from other systems or networks.

Anti-malware/anti-virus (AV)
Software which uses a scanner to identify programs that are, or may be, malicious.

Attack surface
All of an organisations internet-facing assets including both hardware and software. A larger number of such assets yields more potential vulnerabilities that an adversary can exploit to attack an organisation.

Authentication
The process of verifying the identity or other attributes of an entity. May also be used in multi-factor (or two-factor) authentication, which refers to the process in which multiple methods are used to identify and authenticate an individual.

Backdoor (Trojan)
A piece of malicious software which allows someone to take control of a user's computer without their permission.

Blacklist
A list of entities, IP addresses etc. that are blocked or denied privileges or access.

Botnet
A collection of infected computers or internet connected devices that are remotely controlled by a hacker and report to a command-and-control server.

Brute force attack
A type of attack in which hackers use software to try a large number of possible password combinations to gain unauthorised access to a system or file.

Bug
An unexpected and relatively small defect, fault, flaw or imperfection in an information system, software code or device.

Command-and-control server
A computer that issues instructions to members of a botnet.

Cookie
Files placed on your computer that allow websites to remember details.

Cyber essentials
A government-backed cyber security certification scheme that sets out a good baseline of cyber security. The base level requires completion of a self-assessment questionnaire, which is reviewed by an external certifying body. Cyber essentials plus adds an extra level by requiring tests of systems to be made by the external body.

Data loss prevention (DLP)
A set of procedures and software tools to stop sensitive data from leaving a network.

Distributed denial-of-service attack (DDoS)
An attack which prevents users from accessing a computer or website by overwhelming it with requests /instructions, often carried out using a botnet.

Domain name system (DNS)
The phone book of the internet. It allows computers to translate website names, like www.hiscox.com, into IP addresses so that they can communicate with each other.

DNS hijacking
An attack which changes a computer's settings to either ignore DNS or use a DNS server that is controlled by malicious hackers. The attackers can then redirect communication to fraudulent sites.

Drive-by download
The infection of a computer with malware when a user visits a malicious website, without the user specifically initiating the download.

Encryption
The process of converting information or data into a code, so that it is unreadable by anyone or any machine that doesn't know the code.

Endpoint
An internet-capable hardware device. The term can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers, etc.

Exploit
An attack which takes advantage of a vulnerability (typically a flaw in software code) in order to access or infect a computer.

Firewall
A barrier between networks or parts of a network, blocking malicious traffic or preventing hacking attempts. The firewall inspects all traffic, both inbound and outbound, to see if it meets certain criteria. If it does, it is allowed; if not, the firewall blocks it.

Hacktivism
Used to describe hacking activity carried out for a political, ethical or societal ends.

Hashing
A process that uses an irreversible encryption algorithm to turn a data entry into a random alphanumeric value. Typically used to protect passwords from compromise in the event that a malicious actor gains access to the database where they are kept. Often combined with 'salting' (see below).

Incident response plan (IRP)
A set of predetermined and documented procedures to detect and respond to a cyber incident.

Intrusion detection system (IDS)
A device or software application that monitors a network or systems for malicious activity or policy violations, with any unusual activity being flagged.

Intrusion prevention system (IPS)
A proactive version of IDS that can automatically take actions to block suspicious behaviour.

Insider threat
A person or group of persons within a company who pose a potential risk through violating security policies, either maliciously or negligently.

ISO27001
An international standard that describes best practice when it comes to information security risk management.

Keylogger
A type of malware that can secretly record a user's keystrokes and send them to an unauthorised third party.

Malware
A general term for malicious software. Malware includes viruses, worms, Trojans and spyware. Many people use the terms malware and virus interchangeably.

NIST cybersecurity framework
A set of standards, best practices, and recommendations for improving cyber security. It is industry, geography and standards agnostic, and is outcome rather than input-focused.

Network access control (NAC)
A method to bolster security by restricting network access to those devices that comply with a defined security policy.

Patches
Software and firmware add-ons designed to fix bugs and security vulnerabilities.

Payment card industry data security standard (PCI-DSS)
An information security standard created by PCI-SSC (see below) that governs how companies accepting payments by credit/debit card have to handle and protect that information. There are four tiers of governance, based on the volumes of transactions that a company is handling, from level 4 at the bottom end to level 1 at the top. The exact boundaries of these tiers are set by the individual card brands.

Payment card industry security standards council (PCI-SSC)
The body responsible for developing and promoting the PCI-DSS and relevant tools to aid compliance. Founded by the five main card bards (Visa, Mastercard, American Express, JCB and Diners) and supported by an 'advisory board' made up of representatives from major partners (retails, processors, banks, etc.).

Penetration testing
A process whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing
The fraudulent practice of sending emails purporting to be from reputable sources in order to induce individuals to perform particular actions, such as revealing information, transferring funds, or opening attachments/links.

Phreaking
Using a computer or other device to trick a phone system. Typically, phreaking is used to make free phone calls or to have calls charged to a different account.

Qualified security assessor (QSA)
A person who has been certified by the PCI-SSC to audit merchants for PCI-DSS compliance.

Ransomware
A piece of malicious software that encrypts or blocks access to data/systems, with a decryption key only being provided upon payment of a fee.

Red team exercise
An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by a hacker to attack or exploit vulnerabilities in a company's network.

Redundancy
Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

Report on compliance (RoC)
Issued by a QSA if the audit of a merchant's systems have been found to be in compliance with PCI-DSS.

Resiliency
The ability of a network to:
- provide continuous operation (i.e. highly resistant to disruption and able to operate at a lower level damaged);
- recover effectively if failure does occur; and
- scale to meet rapid or unpredictable demands (such as DDoS attacks).

Rootkit
A piece of software that hides programmes or processes running on a computer.

Salting
The addition of a unique, random string of characters to a password before it is hashed to make deciphering the password more difficult.

Secure file transfer protocol (SFTP)
A methodology for exchanging/transmitting files over the internet in an encrypted format.

Secure sockets layer (SSL)
An outdated protocol (replaced by TLS – see below) for transmitting private data via the internet by utilising cryptographic systems that use two keys to encrypt data.

Security information and event management (SIEM)
A security solution that provides visibility of a company's cyber security by aggregating alerts and logs generated by multiple sources and security assets (IPS, IDS, AV, etc.)

Self assessment questionnaire (SAQ)
A self-assessment form used by smaller merchants to verify their compliance with PCI DSS.

Social engineering
The methods attackers use to deceive victims into performing an action, often including phishing, but also phone calls, fake LinkedIn accounts, etc. Typically, these actions are opening a malicious webpage or running an unwanted file attachment.

Spearphishing
A targeted phishing attack against a certain individual.

Spoofing
When the sender address of an email is forged for the purposes of social engineering/phishing.

Spyware
Software that permits advertisers or hackers to gather sensitive information without your permission.

SQL injection
SQL is a computer programming language to tell a database what to do. An SQL injection is where that language is manipulated to instruct the database to perform a different task to what was intended.

Threat actor
An individual, group, organisation, or government that conducts or has the intent to conduct detrimental activities. A hacker, essentially.

Threat vector
The method that a threat actor uses to gain access to a network.

Transport layer security (TLS)
The successor to SSL (see above), and also a protocol for transmitting private data via the internet by utilising cryptographic systems that use two keys to encrypt data. Many internet browsers indicate a connection protected by TLS by displaying a padlock or security certificate near the website address field. Often still referred to as SSL.

Trojan
Malicious programs that pretend to be legitimate software, but actually carry out hidden, harmful functions.

Virtual private network (VPN)
A method of connecting remote computers to a central network, allowing users to communicate or access the organisation's servers securely over the internet.

Virus
Malicious computer programs that can spread to other files.

Vulnerability
Bugs in software programs that hackers exploit to compromise computers.

Whitelist
A list of entities, IP addresses, applications etc. that are considered trustworthy and are granted access or privileges.

Worm
A form of malware that can replicate and spread without the need for human or system interaction. Think of it as malware on autopilot.

Zero-day vulnerability
A software bug, unknown to the developers, that hackers have detected and can exploit to adversely affect computer programs, data, additional computers or a network.

Zombie (aka bot)
An infected computer that is remotely controlled by a hacker. It is part of a botnet.