INFORMATION

NCSC glossary

The NCSC glossary - a set of straightforward definitions for common cyber security terms

A

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

allowed list
Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications. Can also be known as 'whitelisting' across the industry.

app
Short for *Application*, typically refers to a software program for a smartphone or tablet.

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

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.

browser
A software application which presents information and services from the web.

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.

bring your own device (BYOD)
An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

C

certificate
A form of digital identity for a computer, user or organisation to allow the authentication and secure exchange of information.

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.

deny list
An access control mechanism that blocks named entities from communicating with a computer, site or network. Can also be known as 'blacklisting' across the industry.

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 smartphones, laptops and tablets that connect to an organisation's network.

exploit
May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.

F

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

G

H

hacker

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

honeypot (honeynet)
Decoy system or network to attract potential attackers that helps limit access to actual systems by detecting and deflecting or learning from an attack. Multiple honeypots form a honeynet.

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 privilleged access to systems, networks or data.

Internet of things (IoT)
Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

J

K

L

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.

N

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

O

P

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

pentest

Short for *pen*etration *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.

platform
The basic hardware (device) and software (operating system) on which applications can be run.

Q

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

software as a service (SaaS)
Describes a business model where consumers access centrally-hosted software applications over the Internet.

sanitisation

Using electronic or physical destruction methods to securely erase or remove data from memory.

smishing

Phishing via SMS: mass text messages sent to users asking for sensitive information (eg 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.

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.

T

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.

U

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

water-holing (watering hole attack)

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

whaling

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

X

Y

Z

zero-day

Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

PUBLISHED

23 November 2016

REVIEWED

5 January 2018

Was this article helpful?

Yes No