LaSalle Street Podcast:
Cybersecurity Glossary for Episode 7

By Jahru McCulley, Financial Markets Analyst, Financial Markets Group

Advanced persistent threats (APT) – "a covert cyber-attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period."[1]

Authentication as a service (authentication service providers) – provides "authentication and user management services for applications." It also provides "configurable user login pages (or widgets), logout functionality, federated identities with social media accounts, user databases, and some degree of user management."[2]

Attack vector – "a way or method used by an attacker to obtain illegal access to a local or remote network or computer."[3]

Automated vulnerability scanning – when a tool is "configured to carry out scans at set intervals automatically." The tool can be configured to run periodically, e.g., hourly, daily, weekly, or monthly.[4]

Business as usual (BAU) – an "unchanging state of affairs despite difficulties or disturbances."[5]

Business continuity planning (BCP) – "a document that outlines how a business will continue operating during an unplanned disruption in service."[6]

Network behavior anomaly detection (NBAD) – "the real-time monitoring of a network for any unusual activity, trends, or events."[7]

Configuration management database (CMDB) – "a centralized repository that stores information on all the significant entities" within an applicable IT environment.[8]

Cyberattack – "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm."[9]

Cyber-defense – "a computer network defense mechanism, which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities, and other possible networks."[10]

Distributed denial of service attacks (DDoS) – when "hackers have attempted to make a website or computer unavailable by flooding or crashing the website with too much traffic."[11]

Endpoint detection and response (EDR) – "an integrated endpoint security solution that combines real-time endpoint monitoring and collection of endpoint data with rules-based automated response and analysis capabilities."[12]

Endpoint security – **"**the practice of securing endpoints or entry points of end-user devices, such as desktops, laptops, and mobile devices, from being exploited by malicious actors and campaigns."[13]

Hacktivism – "computer hacking (as by infiltration and disruption of a network or website) done to further the goals of political or social activism."[14]

Intelligent bot – "a robot that functions as an intelligent machine, that is, it can be programmed to take actions or make choices based on input from sensors."[15]

Malicious code – "unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses."[16]

Malware – "software designed to interfere with a computer's normal functioning."[17]

Penetration test – "test to check the security of a computer system through an externally connected network, such as the Internet, and to detect vulnerabilities in the system and network while attempting actual attack methods by hackers."[18]

Phishing – a fraudulent communication aimed at soliciting sensitive information from an individual on the internet.[19]

Ransomware – malware that demands payment from an individual for access to encrypted files.[20]

Regression test – a practice that tests the functionality of an application following any code changes, upgrades, or enhancements.[21]

Sandbox – "an isolated environment on a network that mimics end-user operating environments. Sandboxes are used to safely execute suspicious code without risking harm to the host device or network."[22]

Security operation center (SOC) – "a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents."[23]

Security posture assessment – an evaluation of the security status of a system or network.[24]

Significantly important financial institution (SIFI) – an financial institution that poses significant risk to other entities or systems, if it were to fail, as determined and designated by regulators.[25]

Social engineering – (in an information security context) refers to deceitful tactics used to solicit sensitive information from an individual for unauthorized purposes.[26]

Spear-phishing – A scheme using electronic communications to improperly target or solicit individuals, organizations, or business.[27]

Static analysis security testing tool (SAST) – "a technique and class of solutions that performs automated testing and analysis of program source code to identify security flaws in applications."[28]

Threat hunting – a real-time IT security drill aimed at identifying undetected cyber-attacks.[29]

Virtual desktop network – "preconfigured images of operating systems and applications in which the desktop environment is separated from the physical device used to access it."[30]

Vendor risk management – "the process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance."[31]

Virtual private network (VPN) – "a method employing encryption to provide secure access to a remote computer over the internet."[32]

Vulnerability management – procedures that assess and analyze weaknesses in a software system.[33]

---

[1] Cisco. (n.d.). What is an Advanced Persistent Threat (APT)? Cisco. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html.

[2] Okawa, J. (2018, February 4). How to choose the best Authentication as a Service Provider for your company. Medium. https://medium.com/free-code-camp/evaluating-authentication-as-a-service-providers-6903895a8450.

[3] Borges, E. (2020, April 9). What is an Attack Vector? SecurityTrails Index Page. SecurityTrails https://securitytrails.com/blog/attack-vector#:~:text=%20Types%20of%20attack%20vectors%20%201%20Compromised,criminals%20to%20break%20into%20systems%20and...%20More%20.

[4] Krishnan, P. (2021, January 12). Automate Vulnerability Scanning and Transform your Endpoint Security Game. SecPod Blog. https://www.secpod.com/blog/automated-vulnerability-scanning/#:~:text=What%20is%20automated%20vulnerability%20scanning%3F%20An%20automated%20vulnerability,be%20configured%20to%20run%20daily%2C%20weekly%2C%20or%20monthly.

[5] Lexico Dictionaries. (n.d.). BUSINESS as usual: Definition of business as usual by Oxford dictionary on LEXICO.COM also meaning of business as usual. Lexico Dictionaries | English. https://www.lexico.com/definition/business_as_usual.

[6] IBM Services. (2020, November 25). What is a business continuity plan (BCP)? IBM. https://www.ibm.com/services/business-continuity/plan.

[7] Techopedia. (2017, January 18). What is Network Behavior Anomaly Detection (NDAD)? - definition from Techopedia. Technopedia. https://www.techopedia.com/definition/16119/network-behavior-anomaly-detection-nbad.

[8] ManageEngine. (n.d.). Configuration Management Database. ManageEngine AssetExplorer. https://www.manageengine.com/products/asset-explorer/cmdb-configuration-management-database.html. https://www.manageengine.com/products/asset-explorer/cmdb-configuration-management-database.html.

[9] Merriam-Webster. (n.d.). Cyberattack. Merriam-Webster. https://www.merriam-webster.com/dictionary/Cyberattack

[10] Techopedia. (2019, February 5). What is Cyber Defense? - definition from Techopedia. Techopedia. https://www.techopedia.com/definition/6705/cyber-defense.

[11] Coggeshall, S. (2020, July 23). What is a DDoS Attack? Norton. https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html.

[12] McAfee. (n.d.). What is Endpoint Detection and response? (EDR). McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html.

[13] McAfee. (n.d.). What Is Endpoint Security? McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint.html.

[14] Merriam-Webster. (n.d.). Hactivism. Merriam-Webster. https://www.merriam-webster.com/dictionary/hacktivism.

[15] *McGraw-Hill Dictionary of Scientific & Technical Terms*, 6E, Copyright © 2003 by The McGraw-Hill Companies, Inc.

[16] Cybersecurity and Infrastructure Security Agency (CISA). (2018, September 28). Protecting Against Malicious Code. Cybersecurity and Infrastructure Security Agency (CISA). https://us-cert.cisa.gov/ncas/tips/ST18-271.

[17] Merriam-Webster. (n.d.). Malware. Merriam-Webster. https://www.merriam-webster.com/dictionary/malware.

[18] Sharief, K. (n.d.). What is a Penetration Test (Pen Test)? - Definition, Methods and More. Computer Tech Reviews. https://www.computertechreviews.com/definition/penetration-test/#:~:text=A%20penetration%20test%20%28pen%20test%29%20is%20a%20test,methods%20by%20hackers.%20It%20will%20be%20a%20check.

[19] Merriam-Webster. (n.d.). Phishing. Merriam-Webster. https://www.merriam-webster.com/dictionary/phishing.

[20] Merriam-Webster. (n.d.). Ransomware. Merriam-Webster. https://www.merriam-webster.com/dictionary/ransomware.

[21] Katalon. (2019, September 27). What is Regression Testing? Katalon. (2021, June 24). https://www.katalon.com/resources-center/blog/regression-testing/.

[22] Forcepoint. (n.d.). What is Sandbox Security? Forcepoint. https://www.forcepoint.com/cyber-edu/sandbox-security.

[23] McAfee. (n.d.). What Is a Security Operations Center (SOC)? McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html#:~:text=What%20Is%20a%20Security%20Operations%20Center%20%28SOC%29%3F%20A,preventing%2C%20detecting%2C%20analyzing%2C%20and%20responding%20to%20cybersecurity%20incidents.

[24] Testbytes. (2020, April 10). What is Security Posture Assessment? Testbytes. (2020, April 10). https://www.testbytes.net/blog/what-is-security-posture-assessment/.

[25] Liberto, D. (2021, May 31). Systemically Important Financial Institution (SIFI) Definition. Investopedia. https://www.investopedia.com/terms/s/systemically-important-financial-institution-sifi.asp#:~:text=Key%20Takeaways%201%20A%20systemically%20important%20financial%20institution,give%20them%20greater%20flexibility%20to%20expand%20their%20businesses.

[26] Lexico Dictionaries. (n.d.). Social engineering English definition and meaning. Lexico Dictionaries | English. https://www.lexico.com/en/definition/social_engineering.

[27] Kaspersky. (n.d.). What is Spear Phishing? - definition. Kaspersky. https://usa.kaspersky.com/resource-center/definitions/spear-phishing.

---

[28] Robinson, R. M. (2015, July 29). Static Analysis Security Testing: How to Get the Most From It. Security Intelligence. https://securityintelligence.com/static-analysis-security-testing-how-to-get-the-most-from-it/#:~:text=Static%20analysis%20security%20testing%20%28SAST%29%20is%20a%20technique,security%20tool%20that%20offers%20a%20variety%20of%20advantages.

[29] Cisco. (n.d.). What is Threat Hunting - Steps and Advice. Cisco. https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-threat-hunting.html.

[30] VMware. (n.d.). What are Virtual desktops. VMware. https://www.vmware.com/topics/glossary/content/virtual-desktops#:~:text=Virtual%20desktops%20are%20preconfigured%20images,desktops%20remotely%20over%20a%20network.&text=A%20virtual%20desktop%20looks%20and%20feels%20like%20a%20physical%20workstation

[31] Gartner Inc. (n.d.). Definition of Vendor Risk Management (VRM) - Gartner information technology glossary. Gartner. https://www.gartner.com/en/information-technology/glossary/vendor-risk-management.

[32] Lexico Dictionaries. (n.d.). Virtual Private Netowork English definition and meaning. Lexico Dictionaries | English. https://www.lexico.com/en/definition/virtual_private_network.

[33] Rapid7. (n.d.). What is Vulnerability Management and Scanning? Rapid7. https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/.