Cybersecurity Tech Accord: Definitions of the terms used

Active defense

Cyber defensive measures designed to inflict damage on an attacker, by exploiting vulnerabilities in attack toolkits, distributing disinformation, inflicting malicious code, etc.[1]

Adversary

An individual, group, organization, or government that conducts (or intends to conduct) detrimental activities. This could be done by discovering secret data, corrupting some of the data, spoofing the identity of a message sender, or forcing system downtime.[2]

Advanced Persistent Threat

Elaborate, multi-step targeted attacks aimed at infiltrating a specific network, such as governmental institutions or companies. [3]

Attack

An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.[4]

Attacker

A party who acts with malicious intent to compromise an information system.[5]

Attribution

Attribution is the process of establishing who is behind a hack.[6]

Backdoor

An unauthorized way of accessing a computer, service, system, or data. Backdoors are designed to remain undetected by users and administrators or systems.[7] A backdoor can be intentional. It could be the result of a well-meaning customer support engineer, a third-party software library, or the actions of a bad actor.[8]

Breach

The moment an attacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.[9]

Bug

A bug is a flaw or error in a software program or service.[10] A product bug is clearly unintentional, as it can negatively affect the customer experience.[11]

[1] https://www.thecyberwire.com/glossary.html

[2] https://cyberpolicy.com/glossary

[3] https://www.avira.com/en/security-term/t/advanced-persistent-threat/id/2

[4] https://niccs.us-cert.gov/glossary

[5] https://csrc.nist.gov/Glossary/?term=3019#AlphaIndexDiv

[6] https://motherboard.vice.com/en_us/article/mg79v4/hacking-glossary

[7] https://motherboard.vice.com/en_us/article/mg79v4/hacking-glossary

[8] https://blogs.cisco.com/security/features-bugs-and-backdoors-the-differences-how-language-can-be-misused-and-a-word-of-caution

[9] https://www.cybintsolutions.com/16-cyber-security-terms-that-you-should-know/

[10] https://motherboard.vice.com/en_us/article/mg79v4/hacking-glossary

[11] https://blogs.cisco.com/security/features-bugs-and-backdoors-the-differences-how-language-can-be-misused-and-a-word-of-caution

Civilian

Noncombatant, nonmilitary person, ordinary citizen, private citizen not affiliated with or benefiting a nation-state entity.

Cyber defense

Synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. [12] It involves no intrusion into hostile or non-cooperating networks or systems, but focuses entirely on the defended networks.

Cyber exposure

Cyber exposure includes broad visibility into the security of any asset across any computing environment, spanning traditional IT, cloud environments and Internet of Things, to accurately determine where and to what extent an asset is secure or exposed. Cyber exposure also translates technical data into business insights to measure cyber risk in a way that enables better strategic decisions based on business risk.[13]

Cyber espionage

Cyber espionage is the use of computer networks to gain illicit access to confidential information.[14]

Cyber offense

Unprovoked and deliberate malicious exploitation of computer systems, technology-dependent enterprises and networks.

Cyber space

The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.[15]

Cyber warfare

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.[16]

Cyber weapon

A tool, device, or software that is the direct and proximate cause of or is used with intent to cause significant physical damage, including injury or death to persons or damage or destruction of physical objects, that constitutes a use of force under international law and the U.N. Charter.

DDoS

Distributed denial of service [DDoS] is a type of cyber-attack that entails having attackers utilize a large network of remote PCs, called botnets, to overwhelm another system’s connection or processor, causing it to deny service to the legitimate traffic it’s receiving. A DDoS attack is designed to interrupt or shut down a network, service, or website and make it unavailable for legitimate traffic requests.[17]

[12] https://csrc.nist.gov/Glossary/?term=2820#AlphaIndexDiv

[13] https://www.tenable.com/cyber-exposure

[14] https://cyberpolicy.com/glossary

[15] https://csrc.nist.gov/Glossary/?term=3818#AlphaIndexDiv

[16] https://www.rand.org/topics/cyber-warfare.html

[17] https://www.trendmicro.com/vinfo/us/security/definition/distributed-denial-of-service-temp

Exploit

A malicious application or script that can be used to take advantage of a computer's vulnerability.[18]

Hack back

The use of active defenses to counterattack in response to a cyber-attack.

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.[19]

Intrusion detection

The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack.[20]

Nation-state attack

A cyber-attack conducted by nation states or state-backed cybercriminals.

Penetration testing

An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.[21]

Phishing

Phishing is a form of identity theft in which a scammer uses an authentic-looking email from a legitimate business to trick recipients into giving out sensitive personal information, such as a credit card, bank account, or other sensitive personal information.[22]

Risk

A function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization[23].

Root Cause Analysis

A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks[24].

Rootkit

A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence[25].

[18] https://www.cybintsolutions.com/16-cyber-security-terms-that-you-should-know/

[19] https://csrc.nist.gov/Glossary/?term=4730#AlphaIndexDiv

[20] https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

[21] https://niccs.us-cert.gov/glossary

[22] https://www.trendmicro.com/vinfo/us/security/definition/phishing

[23] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

[24] https://csrc.nist.gov/publications/detail/sp/800-39/final

[25] https://www.veracode.com/security/rootkit

Spear Phishing

Spear phishing is a phishing method that targets specific individuals or groups within an organization. It is a potent variant of phishing, a malicious tactic which uses emails, social media, instant messaging, and other platforms to get users to divulge personal information or perform actions that cause network compromise, data loss, or financial loss.[26]

Spoofing

A spoofing attack happens when a malicious party successfully impersonates another user or device.[27]

Tampering

An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.[28]

Threat

A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage[29].

Vulnerability

A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.[30]

Vulnerability scanning

An automated process to proactively identify security weaknesses in a network or individual system.[31]

Weakness

A shortcoming or imperfection in software code, design, architecture, or deployment that, under proper conditions, could become a vulnerability or contribute to the introduction of vulnerabilities.[32]

[26] https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing

[27] https://www.veracode.com/security/spoofing-definition

[28] https://csrc.nist.gov/Glossary/?term=2082#AlphaIndexDiv

[29] https://www.techopedia.com/definition/25263/threat

[30] https://identity.utexas.edu/everyone/glossary-of-identity-and-cybersecurity-terms

[31] https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

[32] https://identity.utexas.edu/everyone/glossary-of-identity-and-cybersecurity-terms