



Glossary of Cyber Related Terms

Advanced Persistent Threat (APT): An attack in which an unauthorized actor, often a nation-state, employs highly sophisticated technology and/or tactics to gain and maintain surreptitious access to a network. The intention of an APT may be to steal data, or to cause damage to the network or organization, or to plant attack capabilities for future activation. Stuxnet is an example of an ATP.

Authentication: Procedures to verify that a network user is who he or she claims to be. A simple and common authentication procedure is a password. “Two-factor” authentication is the use of two independent forms of authentication, such as a password, a fingerprint, or a series of digits generated by a secure identification token, a small handheld device.

Botnet: A network of computers that have been penetrated, compromised, and programmed to operate on the commands of an unauthorized remote user, usually without the knowledge of their owners or operators. The network of “robot” computers can then be manipulated by the remote actor to commit attacks on other systems. The computers on botnets are frequently referred to as “zombies” and are often employed in digital denial of service attacks.

Continuous Monitoring: A continuous monitoring program is a process designed to regularly assess information systems to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time, as changes in the system occur. Continuous monitoring transforms the traditional model of static, sporadic security compliance assessments to dynamic, near-real-time situational awareness.

Covered Critical Infrastructure: Refers to critical infrastructure that would be subject to protections and conditions outlined under the Cybersecurity Act of 2012.

Critical Infrastructure: The PATRIOT Act defines critical infrastructure as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The Department of Homeland Security currently identifies 18 critical infrastructure sectors, including transportation, electricity, financial services, and nuclear power. Most critical infrastructure entities are dependent upon computer networks and therefore vulnerable to cyberattacks.

Cybercrime: Cybercrime is criminal activity conducted using computers and the Internet, often financially motivated. Cybercrime includes identity theft, fraud, and internet scams, among other activities. Cybercrime is distinguished from other forms of malicious cyber activity, which have political, military, or espionage motivations.

Digital Denial of Service (DDOS): A cyber war technique in which an Internet site, a server, or a router is flooded with more requests for data than the site or device can respond to or process. Consequently, legitimate traffic cannot access the site and the site is in effect shut down. Botnets are used to conduct such attacks, thus distributing the attack over thousands of originating computers acting in unison.

EINSTEIN: A program administered by the Department of Homeland Security's US-CERT that provides an automated intrusion detection system designed to block unauthorized network traffic from entering government websites. The program provides a process for collecting, correlating, analyzing, and sharing computer security information across the federal government to improve the nation's situational awareness. US-CERT has deployed two generations of EINSTEIN programs and is currently developing EINSTEIN 3.

Encryption: The scrambling of information so that it is unreadable to those who do not have the code to unscramble it.

FISMA: FISMA stands for the Federal Information Security Management Act. Passed in 2002, FISMA is intended to implement and inventory federal information technology systems to enhance government agencies' cybersecurity. FISMA requires annual reports from agencies to the Office of Management and Budget (OMB) on each agency's information security efforts and compliance with government issued standards. OMB then compiles all the reports and submits to Congress an annual compliance report.

Hack: A verb meaning to gain unauthorized access into a computer system.

Hacker: Someone who uses skills to gain access to a computer or network without authorization.

Hactivism: The exploitation of computers and computer networks as a means of protest to promote political ends. The anti-secrecy group Anonymous is an example of a hacktivist organization.

Hardware: Refers to the machines, wiring, and other physical components of a computer, network, or other information technology system.

Intellectual Property Theft: Intellectual property is any innovation, commercial or artistic; any new method or formula with economic value; or any unique name, symbol, or logo that is used commercially. State sponsored entities and cybercriminals are using cyber tools to secretly steal intellectual property, such as companies' trade secrets and proprietary information.

Internet Service Provider (ISP): A corporation (or government agency) that provides the wired or wireless connectivity from a user's home, office, or mobile computer to the Internet.

Keystroke Logger: A program or device that captures every key depression on the computer. Cybercriminals install them on computers to clandestinely record the computer user's passwords and other confidential information.

Logic Bomb: A software application or series of instructions that cause a system or network to shut down and/or to erase all data or software on the network. A logic bomb is a type of malware.

Malware: Malicious software that compromises or reprograms computers or networks with the intention of disrupting their intended functions or operations. Examples of malware include logic bombs, worms, viruses, Trojan Horses, and keystroke loggers.

Pharming: A technique used by hackers to redirect users to false websites without their knowledge.

Phishing: A socially-engineered attempt by malicious actors to deceive internet users into providing personal information such as usernames, passwords, social security numbers and credit card details. Common phishing tactics include posing as a known contact, a legitimate company, or an otherwise trusted entity in an electronic communication.

Router: Routers are computer hardware that direct the movement of internet data, ensuring that the data, such as emails or website requests, reaches its intended destination. Routers are a type of server.

SCADA: SCADA stands for supervisory control and data acquisition. It generally refers to an industrial control system, which is an automated system used to control industrial processes, such as regulation of electrical power transmission, wastewater treatment, or chemical mixing.

Server: A computer that is programmed to provide services – such as hosting software platforms, databases, or websites – to other computers and computer users. Typically, servers are designed to be automated, operating without constant human monitoring.

Software: Refers to the programs and other operating information used by a computer. Software programs provide the instructions that direct computers what to do and how to do it.

Trapdoor /Trojan/Trojan Horse: A type of malware added to a program to facilitate future unauthorized entry into a network or into the software program. Often after an initial entry, the perpetrators will leave behind a trapdoor that will permit future access to be faster and easier.

US-CERT: Stands for the United States Computer Emergency Readiness Team. It is an arm of the Department of Homeland Security's National Cyber Security Division (NCSA). US-CERT leads efforts to improve the nation's cybersecurity posture and coordinate cyber information sharing. US-CERT partners with private sector critical infrastructure owners and operators, academia, federal agencies, and state and local partners to enhance cybersecurity nationwide.

U.S. Cyber Command (CyberCom): Created in June 2009, CyberCom is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the DoD's information networks. CyberCom is the center of DoD's cyberspace operations and it works closely with interagency and international partners to execute cyber missions. CyberCom is a subunified command under U.S. Strategic Command (StratCom).

Zero-day Attack: A cyberattack that uses previously unknown coding (malware, etc.) or exploits a previously unknown security vulnerability. This type of attack is particularly dangerous because existing patches, anti-virus software, and other defenses are not programmed to defend against it. It is called a zero-day attack, because it occurs on "day zero" of learning of the vulnerability.