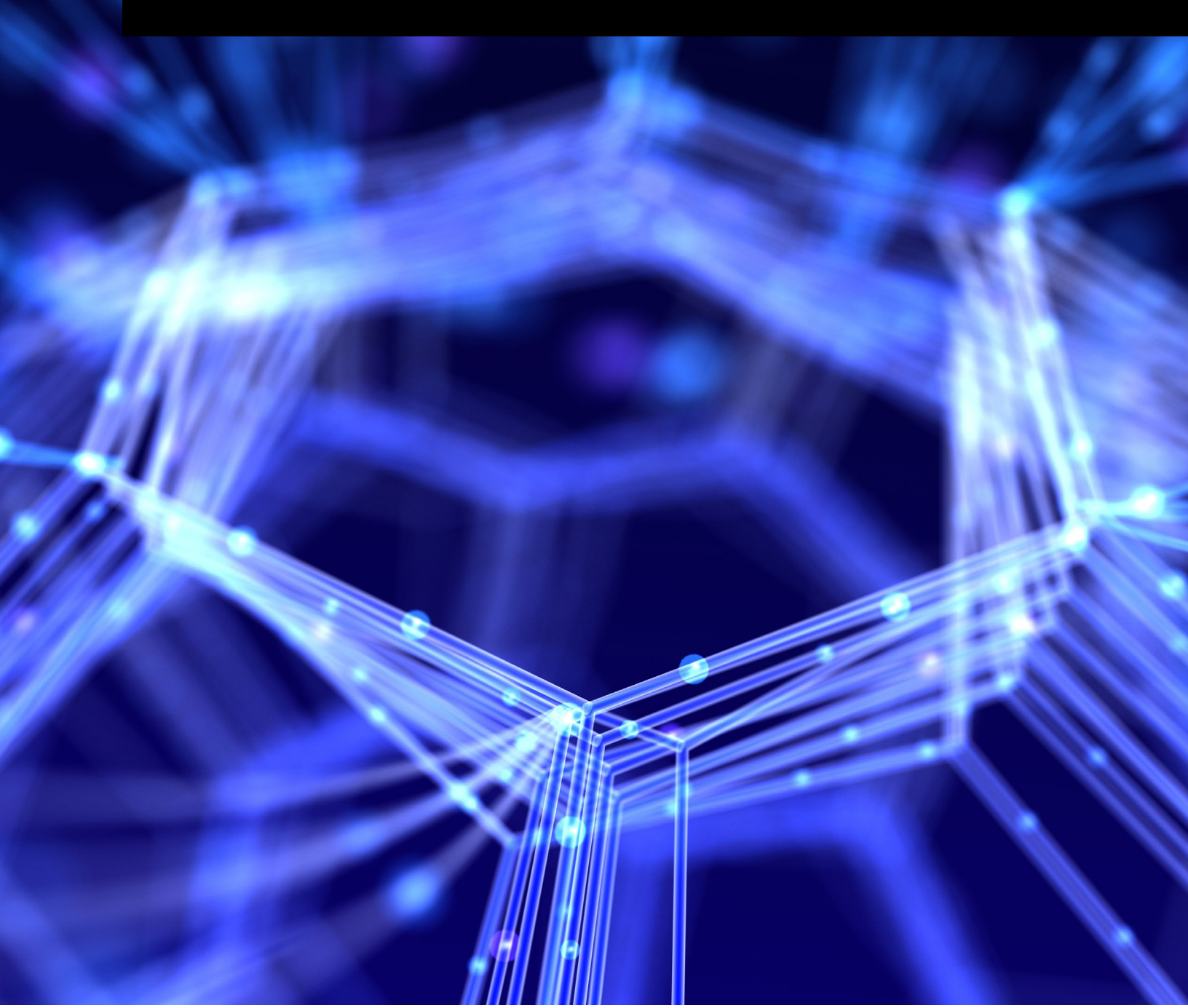
Glossary of Key Cybersecurity Terms

September 2022

LOCKTON®



Cyber exposures are an ever-present threat to businesses and other organizations, one that is constantly evolving as attackers grow more sophisticated and employ new strategies to disrupt operations and steal valuable data. As the methods of defending against such attacks similarly evolve, so does the language used by stakeholders.

This glossary is intended to help with key cybersecurity concepts. While not exhaustive, we hope it will serve as a useful reference document as organizations prepare for, mitigate and respond to cybersecurity threats.

Table of contents

A

Acceptable use policy (AUP)

A written plan outlining constraints and practices to which a user must agree for access to an organization's network or the internet. Organizations often require employees and independent contractors to sign an AUP before being granted a network ID, and in case of educational institutions, students may also be required to sign an AUP.

Active directory (AD)

Microsoft's proprietary directory service. A directory service maps the names of network devices to their unique network addresses. It runs on Windows Server and allows administrators to manage permissions and access rights. AD stores data as objects, each of which is a single element — a user, group, application or device, such as a printer. Objects can be resources, such as printers or computers, or security principals, such as users or groups.

Authentication

Proof or assurance that an individual attempting to log in to a service or perform a transaction online possesses and actively controls a token or authenticator that verifies their identity.

Authenticator assurance level (AAL)

The confidence or the degree of assurance that an individual possesses an authenticator. There are three AALs:

- AAL1 requires either single-factor or multifactor authentication using a wide range of available authentication technologies. Successful authentication requires that the user prove possession and control of the authenticator through a secure authentication protocol.
- AAL2 provides high confidence that the user controls one or more authenticators bound to the subscriber's account. Proof of possession and control of two different authentication factors is required through secure authentication protocols.
- AAL3 provides very high confidence that the claimant controls one or more authenticators bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication requires a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfill both of these requirements.

B

Breach & attack simulation (BAS)

An advanced computer security testing method. A BAS identifies vulnerabilities in security environments by imitating the likely attack vectors used by threat actors. BAS solutions provide automatic vulnerability detection and prioritize mitigation activities to minimize exposure.

Business continuity (BC)

Actions, policies, procedures, processes and tools to ensure an organization can continue critical operations in the event of a cyber incident.

Business impact analysis (BIA)

A process whereby an organization's assets are catalogued and annotated to reflect how critical each asset is to the organization.

Capability maturity model (CMM)

A capability maturity model is focused on quality management processes. A maturity model is a tool businesses use to evaluate their operations.

Five levels are included in a CMM, each containing several key practices.

- CMMC level 1: Safeguard federal contract information.
- CMMC level 2: Serve as a transition step in cybersecurity maturity progression to protection controlled unclassified information.
- CMMC level 3: Protect controlled unclassified information (CUI).
- CMMC levels 4-5: Protect CUI and reduce the risk of advanced persistent threats.

Common vulnerability & exposures (CVE)

A list of publicly disclosed and catalogued computer security flaws, each of which is assigned a CVE ID number.

CVE identifiers are assigned by a CVE numbering authority (CNA). There are about 100 CNAs, representing major IT vendors — such as Red Hat, IBM, Cisco, Oracle and Microsoft — as well as security companies and research organizations. MITRE, a nonprofit organization that manages federally funded research and development centers, can also issue CVEs directly.

Security advisories issued by vendors and researchers almost always mention at least one CVE ID. CVEs help IT professionals coordinate their efforts to prioritize and address vulnerabilities to make computer systems more secure.

Common vulnerability scoring system (CVSS) score

A numerical (0-10) representation of the severity of an information security vulnerability. CVSS scores are commonly used by information security professionals in vulnerability management programs to provide a point of comparison between vulnerabilities and to prioritize remediation of vulnerabilities.

Cross-site scripting (XSS or CSS)

A web application attack used to gain access to private information by delivering malicious code to end-users via trusted websites. Typically, this type of attack is successful due to an application's lack of user input validation — for example, allowing users to supply application code in HTML forms instead of normal text strings.

Cybersecurity & Infrastructure Security Agency (CISA)

A federal agency within the Department of Homeland Security (DHS), tasked with protecting the United States' critical infrastructure. CISA was created through the Cybersecurity and Infrastructure Security Agency Act of 2018, which "rebranded" DHS' National Protection and Programs Directorate as CISA and transferred NPPD's resources and responsibilities to the newly created agency. NPPD previously managed nearly all cybersecurity-related matters for DHS.

CISA's mission is to "build the national capacity to defend against cyber-attacks" and to work "with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the .gov networks that support the essential operations of partner departments and agencies."

D

Data loss prevention (DLP)

Tools, processes and procedures ensuring that sensitive data is not lost, misused or accessed by unauthorized users. DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance.

Demilitarized zone (DMZ)

A perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic.

The objective of a DMZ is to find the balance between allowing access to untrusted networks, such as the internet, while ensuring that the private network or LAN remains secure.

Disaster recovery (DR)

Processes, tasks and activities required to bring an organization back to normal operations and reinstate regular operations after a disruptive incident.

Domain name system (DNS)

Essentially, the phone book of the internet. Humans access information online through domain names — for example, lockton.com, nytimes.com or espn.com. Web browsers interact through IP addresses. DNS translates domain names to IP addresses so browsers can load internet resources.

E

Endpoint

An endpoint is any device connected to a computer network. Examples include servers, desktop computers, laptops, mobile phones, tablets, point-of-sale systems and Internet of Things devices.

Endpoint detection & response (EDR)

An integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. Also known as endpoint threat detection and response (ETDR).

H

Hypertext markup language (HTML)

A computer programming language used to create pages that a web browser can display. Most web pages on the internet are stored as HTML files. A website represents a collection of related HTML pages stored on a shared server.

I

Identity & access management (IAM)

A system for ensuring specified individuals and job roles in an organization (identities) can access the tools they need for their particular tasks and positions. An IAM system enables an organization to manage applications without logging in to each application as an administrator and to manage a range of identities, including people, software and hardware, like robotics and IoT devices.

Identity provider (IdP)

A service that stores and manages digital identities. These services allow an organization's employees or users to connect with the resources they need, providing a way to manage access — adding or removing privileges — while keeping security tight.

If you've ever used your Google or Facebook login to access an application, you've used an IdP. Your username and password open doors to another resource, and you don't have to do anything special to make it happen.

Incident response plan (IRP)

A document that outlines an organization's procedures, steps and responsibilities of its incident response program.

Internet of Things (IoT)

The network of physical objects — "things" — that are embedded with sensors, software and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. Examples of IoT-enabled office products include intelligent lighting, smart thermostats, smart locks, GPS trackers and air quality monitoring apps.

Internet protocol (IP)

The set of rules governing the format of data sent via the internet or local network.

IP address

A unique address that identifies a device on the internet or a local network.

IP address management (IPAM)

An integrated suite of hardware and/or software tools enabling end-to-end planning, deploying, managing and monitoring of IP address infrastructure. IPAM automatically discovers IP address infrastructure servers and DNS servers on a network and enables administrators to manage them from a central interface.

M

Managed detection & response (MDR)

A combination of technology and human expertise to perform threat hunting, monitoring and response. Using MDR can help with rapidly identifying and limiting the impact of threats without additional staff.

Managed service provider (MSP)

An outsourced third party that manages and assumes the responsibility of a defined set of daily management services to its customers. Those can include network, application, database and other general IT support and services. It is common for organizations of all sizes to use MSPs.

Managed security service provider (MSSP)

A provider of outsourced monitoring and management of security devices and systems. MSSP services can include managing firewalls, intrusion detection, VPNs, vulnerability scanning and antiviral services. An MSSP can provide incident response planning and services.

Multifactor authentication (MFA)

An authentication method that requires a user to provide two or more verification factors to gain access to a resource, including applications, platforms, accounts, and processes. Theses verification factors are often a combination of something the user knows (e.g., password), something the user has (e.g., a token), and/or something the user is (e.g., fingerprint). MFA is an essential component of a robust IAM policy and can help reduce the likelihood of a successful cyberattack.

P

Protected health information (PHI)

Any information that was created, used or disclosed while receiving healthcare services that can be used to identify an individual. Examples can include dates, such as birth, discharge, admittance and death dates; biometric identifiers, such as fingerprints and voice prints; and full-face photographic images and any comparable images, along with video of one's movement.

Personally identifiable information (PII)

Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

R

Recovery time objective (RTO)

The target time set for recovering from any interruption.

Remote desktop protocol (RDP)

A secure network communications protocol developed by Microsoft. RDP enables network administrators to remotely diagnose problems that individual users encounter and gives administrators access to the user's computer.

RDP can be useful to a variety of users — for example, admins responsible for system maintenance and employees who need access to their in-office computers while working from home or traveling, but it must be managed appropriately.

S

Security information & event management (SIEM)

Software that provides real-time analysis of security alerts generated by applications and network hardware. SIEM software matches events against rules and analytics engines and indexes them to detect and analyze advanced threats using globally gathered intelligence. This gives the organization's security professionals visibility into and a record of activities within their IT environments by providing data analysis, event correlation, aggregation, reporting and log management.

Security operation center (SOC)

A centralized group of people using hardware and software tools that monitors, prevents, detects, investigates and responds to cyber threats around the clock.

Software-as-a-service (SaaS)

A method of delivering an application over the internet as a service. Also known as web-based software, on-demand software or hosted software.

Instead of installing and maintaining software, users access SaaS via the internet. The provider manages access to the application, including security, availability and performance, relieving the purchaser of the responsibilities of having to maintain and manage the software.

Structured query language (SQL)

A standard computer programming language used to store, manipulate and retrieve data in a relational database. Threat actors use SQL injection as way to attack a computer system.

SQL injection

A security exploit in which an attacker supplies SQL in the form of a request for action via a web form, directly to a web application to gain access to back-end database and/or application data. This can cause unintended and malicious behavior by the targeted application. Typically, this type of attack is successful due to a web application's lack of user input validation — for example, allowing users to supply SQL application code in HTML forms instead of normal text strings.

System & organization controls (SOC II)

A voluntary compliance standard for organizations specifying how organizations should manage customer data. The standard is based on several trust services criteria, including security, availability, processing integrity, confidentiality and privacy.

V

Virtual private network (VPN)

A protected network connection when using public networks. VPNs encrypt internet traffic and disguise a user's online identity, making it more difficult for third parties to track their activities online and steal data. Encryption takes place in real time.

W

Web application firewall (WAF)

A system that protects web applications from a variety of application layer attacks, such as XSS, SQL injection and cookie poisoning, among others.

Attacks on applications are a significant cause of breaches — they are the gateway to any organization's valuable data. An organization can block the array of attacks that aim to exfiltrate data by compromising systems through web applications by using WAF.

UNCOMMONLY INDEPENDENT

KC: 1848442