THE (ISC)² CYBERSECURITY LEXICON

An introduction to basic cybersecurity terminology and concepts

INTRODUCTION

(ISC)² – the world's largest nonprofit membership association of certified cybersecurity professionals – is pleased to provide you with the (ISC)² Cybersecurity Lexicon. Developed with industry leaders, technology experts and academics comprising the (ISC)² North American Advisory Council, this easy reference tool will quickly introduce non-technical personnel to key cybersecurity concepts they need to know.

The Cybersecurity Lexicon provides legislators, legal professionals, journalists, boards of directors and others with a quick reference guide of common cybersecurity terms. Our goal is to encourage the creation of more effective legislation, standards and policies by encouraging broader understanding of how the accurate use of these terms ensures more effective cybersecurity programs.

We welcome your comments and experiences on using the Lexicon. Feel free to contact the (ISC)² Cybersecurity Advocate team at www.isc2.org/cybersecurity-advocates.

A

Antivirus
software designed to detect and prevent computer viruses and other malware from entering and harming a system.

Application Security
the use of software, hardware and procedural methods to protect applications from external and internal threats.

Artificial Intelligence
the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making and translation between languages.

Asset
any item perceived as having value; includes both tangible items such as information systems and physical property, as well as intangibles such as intellectual property and data.

Attack Surface
the sum of the security risk exposure; it is the aggregate of all known, unknown and potential vulnerabilities and controls across all software, hardware, firmware and networks. A smaller attack surface can help make your organization less exploitable, reducing risk.

A typical attack surface has complex interrelationships among three main areas of exposure: software attack surface, network attack surface and the often-overlooked human attack surface.

Software Attack Surface
comprised of the software environment and its interfaces. These are the applications and tools available to authorized (and unauthorized) users.

Network Attack Surface
presents exposure related to ports, protocols, channels, devices (from routers and firewalls to laptops and smart phones), services, network applications (SaaS) and even firmware interfaces.

Human Attack Surface
humans have a range of complex vulnerabilities that are frequently exploited. One of the great strengths of highly secure organizations is their emphasis on communicating security awareness and safety principles to their employees, partners, supply chain and even their customers.

Authentication
the process or action of verifying the identity of a user or process.

Authorization
the function of specifying access rights/privileges to resources related to information security and computer security in general and to access control in particular.

B

Business Impact Assessment (BIA)
a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of exploitation, disaster, accident or emergency.

C

Cloud Computing
a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Three main cloud computing service models are:

Software as a Service (SaaS)
is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the internet.

Platform as a Service (PaaS)
is where a third-party provider delivers hardware and software tools — usually those needed for application development — to users over the internet. A PaaS provider hosts the hardware and software on its own or another third-party's infrastructure.

Infrastructure as a Service (IaaS)
a cloud computing service model that provides a comprehensive suite of services and technology to operate an end-to-end IT system.

Other cloud computing models used are:

Identity as a Service (IDaaS)
is an authentication infrastructure that is built, hosted and managed by a third-party service provider. IDaaS can be thought of as single sign-on (SSO) for the cloud.

Communications as a Service (CaaS)
is an outsourced enterprise communications solution that can be leased from a single vendor. Such communications can include voice over IP (VoIP or internet telephony), instant messaging (IM), collaboration and videoconference applications using fixed and mobile devices.

Desktop as a Service (DaaS)
is a cloud computing solution in which virtual desktop infrastructure is outsourced to a third-party provider.

Security as a Service (SecaaS)
web-based security solutions that are delivered over the cloud. However, Security as a Service is better defined as a general business model for outsourcing cybersecurity capabilities.

D

Discretionary Access Control (DAC)
an access policy determined by the owner of a file or other resource.

E

Encryption
the conversion of electronic data into ciphertext that theoretically can only be decoded by authorized parties.

Endpoint
a general term referring to a desktop computer, laptop or notebook computer or mobile device.

Exploit
software, a subset of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack — an event where a human threat successfully takes advantage of a vulnerability for denial or delay of service, exfiltration or unauthorized modification of data.

F

Firewall
a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Usually the first line of defense in a network.

Five Pillars of Information Security

Confidentiality
the attribute of data that ensures information is only being exposed to appropriately authorized parties and other systems.

Integrity
the attribute of data that ensures the information accurately reflects reality. Data and systems/processes cannot be modified without authorization.

Availability
the attribute of data that ensures it is always available to appropriate parties when required for use.

Non-repudiation
a method of guaranteeing message transmission between parties via digital signature and/or encryption.

Authentication
the process or action of verifying the identity of a user or process.

G

Governance, Risk and Compliance (GRC)
the process of how an organization manages its information resources. This process usually includes all aspects of how decisions are made for that organization, such as policies, roles and procedures the organization uses to make those decisions. It is designed to ensure the business focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes, and addresses how expected performance will be evaluated.

H

Hacker
a slang term that can mean a hostile human threat to IT systems, an IT security professional, a vulnerability researcher or an amateur security person.

Honeypot
decoy servers or systems set up to gather information regarding human threats.

I

Identity and Access Management (IAM)
the framework for business processes that facilitates the management of electronic or digital identities. The framework includes the organizational policies for managing digital identity as well as the technologies needed to support identity management.

Industrial Control Systems (ICS)
IT systems used to control industrial processes such as manufacturing, product handling, production and distribution.

Information States
information has three primary, non-overlapping states: transmission, storage and processing. Data is in one of these three states at any given point.

Infrastructure as a Service (IaaS)
a cloud computing service model that provides a comprehensive suite of services and technology to operate an end-to-end IT system.

Internet of Things (IoT)
the network of physical or wireless IP-connected objects that are embedded with electronics, software, sensors and network connectivity.

Internet Protocol (IP)
the Open Systems Interconnection (OSI) Layer 3 protocol that's the basis of modern internet communications.

Intrusion Detection System (IDS)
a technology that alerts organizations to adverse or unwanted activity; a real-time monitoring of events as they happen in a computer system or network, using audit trail records and network traffic and analyzing events to detect potential intrusion attempts.

Intrusion Prevention System (IPS)
a technology that monitors activity like an IDS, but will automatically take proactive, preventive action if it detects unacceptable activity; any hardware or software mechanism that can detect and stop attacks in progress.

K

Key Management System (KMS)
a framework for the generation, storage, distribution deletion, archiving, and application of encryption and decryption keys in accordance with a security policy.

M

Machine Learning
application of artificial intelligence (AI) that provides systems with the ability to learn and improve from experience automatically without being explicitly programmed or upgraded.

Managed Security Services Provider (MSSP)
a vendor providing security services to many clients that would otherwise be unaffordable to medium and small companies due to cost or be unattainable due to resource limitations such as qualified security personnel.

Managed Service Provider (MSP)
a company that remotely manages a client's information technology infrastructure.

Mandatory Access Controls (MAC)
access control that requires the system itself to manage access controls in accordance with the organization's security policies.

Multi-Factor Authentication
an authentication method that requires two or more ways of establishing identity.

N

Network
system of computers, and/or connected devices that are joined together so that they can communicate by exchanging information and sharing resources.

Network Access Control (NAC)
network computer technology that uses a set of protocols for authenticating to a network control device such as a switch, router or wireless access point, usually based on a unique address or a certificate.

P

Penetration Test
an assessment of the effectiveness of established security defenses through mimicking the actions of a hostile human threat for finding exploitable vulnerabilities or other weaknesses and to attempt to exploit those vulnerabilities or weaknesses.

Perimeter-Based Security Model
technique of securing a network by controlling access to all entry and exit points of a defined networked environment.

Personal Health Information
any patient-related health information as defined by the Health Insurance Portability and Accountability Act of 1996.

Personally Identifiable Information (PII)
information that can be traced back to an individual user through their name, postal address or email address. Personal user preferences tracked by a website can also be considered personally identifiable when linked to other personally identifiable information.

Privacy Policy
the right of a human individual to control the distribution of information about themselves; it documents the rights and obligations of individuals and organizations with respect to the collection, use, retention and disclosure of personal information.

Privacy Impact Assessment (PIA)
decision tool used to identify and mitigate privacy risks. Notifies the public of 1) what PII is being collected, 2) why the PII is being collected, 3) how the PII will be retrieved, shared, accessed and stored.

R

Red Team Testing
penetration testing done by security personnel to mimic an attack of an external, hostile, experienced human threat on an organization's infrastructure for locating and reporting on vulnerabilities.

Risk
the possibility of damage or harm, and the likelihood that damage or harm will be realized; a function of the likelihood of a given threat source exploiting a potential vulnerability, and the resulting impact of that adverse event on the organization.

Risk Assessment
assessing the threats, vulnerabilities and assets of information systems to determine the likelihood threats will exploit these vulnerabilities and weaknesses to cause adverse effects.

Risk Management
The process of designing, developing, sustaining and modifying operational processes and systems in consideration of applicable risks to asset confidentiality, integrity and availability. Applicable risks are those reasonably expected to be realized and to cause an unacceptable impact.

Role-Based Access Control (**RBAC**)
an access control model that bases the access control authorizations on the roles (or functions) that the user is assigned to within an organization.

S

Safeguard
a process, procedure, technique or feature that mitigates the effects of a risk. Safeguards can be classified as technology, procedures/policies or human factors.

Secrecy
attempting to hide information or data.

Secure Coding
the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities.

Software as a Service (**SaaS**)
a cloud computing service model that provides software applications.

T

Threat
a person, event or circumstance with the potential to cause harm to an asset. Threats are either environmentally or human-based.

Threat Actor
human-based agent that can negatively impact a system's IT assets. The threat agent is evaluated on the agent, intent, target and mechanism used.

V

Virtual Desktop Infrastructure (VDI)
a desktop operating system running within a virtual machine (VM) on a physical host server.

Virtual Machine
an IT endpoint or server designed to perform in a software environment in exactly the same way as the dedicated hardware.

Vulnerability
a weakness or exposure in a technology, protocol or design of an information technology system such as hardware, firmware and software.

Vulnerability-Based Security Model
risk assessment methodology centered on the presence or absence of vulnerabilities irrespective of the threat or asset value. For example, banning specific items considered dangerous from commercial aircraft passengers because they could be used as weapons.

ABOUT (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, over 130,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™. For more information on (ISC)², visit www.isc2.org.

NOTES

NOTES

INSPIRING A SAFE AND SECURE CYBER WORLD.