CYBERSECURITY:

Key Terms
A – Z

A Authentication

The process of proving an individual is a claimed identity. Authentication is the first element of the AAA services concept, which includes Authentication, Authorization, and Accounting. Authentication occurs after the initial step of identification (i.e. claiming an identity). Authentication is accomplished by providing one or more authentication factors—

- Type 1: something you know (e.g. password, PIN, or combination)
- Type 2: something you have (e.g. smart card, RSA SecureID FOB, or USB drive), and
- Type 3: something you are (e.g. biometrics—fingerprint, iris scan, retina scan, hand geometry, signature verification, voice recognition, and keystroke dynamics).

B Backing Up

Creating a duplicate copy of data onto a separate physical storage device or online/cloud storage solution. A backup is the only insurance against data loss. With a backup, damaged or lost data files can be restored. Backups should be created on a regular, periodic basis such as daily. A common strategy is based on the 3-2-1 rule: you should have three copies of your data - the original and 2 backups; you should use 2 different types of media (such as a physical media (such as a hard drive or tape) and a cloud storage solution); and do not store the three copies of data in 1 plane (i.e. backups should be stored offsite). It is important to store backups for disaster recovery at an offsite location in order to insure they are not damaged by the same event that would damage the primary production location. However, additional onsite backups can be retained for resolving minor issues such as accidental file deletion or hard drive failure.

C Cloud Computing

A means to offer computing services to the public or for internal use through remote services. Most cloud computing systems are based on remote virtualization where the application or operating environment offered to customers is hosted on the cloud provider's computer hardware. There are a wide range of cloud solutions including software applications (examples include e-mail and document editing), custom code hosting (namely execution platforms and web services) as well as full system replacements (such as remote virtual services to host databases or file storage). (See SaaS, PaaS, and IaaS.) Most forms of cloud computing are considered public cloud as they are provided by a third party. However, private cloud (internally hosted), community cloud (a group of companies' privately hosted cloud), a hosted private cloud (the cloud servers are owned and managed by a third party but hosted in the facility of the customer) and hybrid cloud (a mixture of public and private) are also options.

Cybersecurity Resources

virginiasbdc.org/programs/cybersecurity/

D Digital Certificate

A means by which to prove identity or provide authentication commonly by means of a trusted third-party entity known as a certificate authority. A digital certificate is based on the x.509 v3 standard. It is the public key of a subject signed by the private key of a certificate authority with clarifying text information such as issuer, subject identity, date of creation, date of expiration, algorithms, serial number and thumbprint (i.e. hash value).

E Encryption Key

The secret number value used by a symmetric encryption algorithm to control the encryption and decryption process. A key is a number defined by its length in binary digits. Generally, the longer the key length, the more security (i.e. defense against confidentiality breaches) it provides. The length of the key also determines the key space, which is the range of values between the binary digits being all zeros and all ones from which the key can be selected.

F Firewall

A security tool, which may be a hardware or software solution that is used to filter network traffic. A firewall is based on an implicit deny stance where all traffic is blocked by default. Rules, filters or ACLs can be defined to indicate which traffic is allowed to cross the firewall. Advanced firewalls can make allow/deny decisions based on user authentication, protocol, header values and even payload contents.

H Hacker

A person who has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations and altering its abilities and capabilities. A hacker may be ethical and authorized (the original definition) or may be malicious and unauthorized (the altered but current use of the term). Hackers can range from professionals who are skilled programmers to those who have little to no knowledge of the specifics of a system or exploit but who can follow directions; in this instance, they are called script kiddies.

I ISP (Internet Service Provider)

The organization that provides connectivity to the Internet for individuals or companies. Some ISPs offer additional services above that of just connectivity such as e-mail, web hosting and domain registration.

J JBOH (JavaScript-Binding-Over-HTTP)

A form of Android-focused mobile device attack that enables an attacker to be able to initiate the execution of arbitrary code on a compromised device. A JBOH attack often takes place or is facilitated through compromised or malicious apps.

Cybersecurity Resources

virginiasbdc.org/programs/cybersecurity/

K Keylogger

Any means by which the keystrokes of a victim are recorded as they are typed into the physical keyboard. A keylogger can be a software solution or a hardware device used to capture anything that a user might type in including passwords, answers to secret questions or details and information form e-mails, chats and documents.

L LAN (Local Area Network)

An interconnection of devices (i.e. a network) that is contained within a limited geographic area (typically a single building). For a typical LAN, all of the network cables or interconnection media is owned and controlled by the organization unlike a WAN (Wide Area Network) where the interconnection media is owned by a third party.

M Malware (Malicious Software)

Any code written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system. Malware includes a wide range of types of malicious programs including: virus, worm, Trojan horse, logic bomb, backdoor, Remote Access Trojan (RAT), rootkit, ransomware and spyware/adware.

O Outsider Threat

The likelihood or potential that an outside entity, such as an ex-employee, competitor or even an unhappy customer, may pose a risk to the stability or security of an organization. An outsider must often gain logical or physical access to the target before launching malicious attacks.

P Phishing

A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over e-mail, text messages, through social networks or via smart phone apps. The goal of a phishing attack may be to learn logon credentials, credit card information, system configuration details or other company, network, computer or personal identity information. Phishing attacks are often successful because they mimic legitimate communications from trusted entities or groups such as false emails from a bank or a retail website.

R Risk Assessment

The process of performing a risk assessment and evaluating the responses to risk in order to mitigate or otherwise handle the identified risks. Countermeasures, safeguards or security controls are to be selected that may eliminate or reduce risk, assign or transfer risk to others (i.e. outsourcing or buying insurance) or avoid and deter risk. The goal is to reduce risk down to an acceptable or tolerable level.

S SaaS (Software-as-a-Service)

A type of cloud computing service where the provider offers the customer the ability to use a provided application. Examples of a SaaS include online e-mail services or online document editing systems. A user of a SaaS solution is only able to use the offered application and make minor configuration tweaks. The SaaS provider is responsible for maintaining the application.

T Two-Factor Authentication

The means of proving identity using two authentication factors usually considered stronger than any single factor authentication. A form of multi-factor authentication. Valid factors for authentication include

- Type 1: Something you know such as passwords and PINs;
- Type 2: Something you have such as smart cards or OTP (One Time Password) devices; and
- Type 3: Someone you are such as fingerprints or retina scans (aka biometrics).

U Unauthorized Access

Any access or use of a computer system, network or resource which is in violation of the company security policy or when the person or user was not explicitly granted authorization to access or use the resource or system

V Vulnerability

Any weakness in an asset or security protection which would allow for a threat to cause harm. It may be a flaw in coding, a mistake in configuration, a limitation of scope or capability, an error in architecture, design, or logic or a clever abuse of valid systems and their functions.

W Wi-Fi

A means to support network communication using radio waves rather than cables. The current Wi-Fi or wireless networking technologies are based on the IEE 802.11 standard and its numerous amendments, which address speed, frequency, authentication and encryption.

Z Zombie

A term related to the malicious concept of a botnet. The term zombie can be used to refer to the system that is host to the malware agent of the botnet or to the malware agent itself. If the former, the zombie is the system that is blinding performing tasks based on instructions from an external and remote hacker. If the latter, the zombie is the tool that is performing malicious actions such as DoS flooding, SPAM transmission, eavesdropping on VoIP calls or falsifying DNS resolutions as one member of a botnet.