ABCs of Cybersecurity

SECUR-SERV

32 Cybersecurity acronyms and terms you need to know

THREAT

Advanced Persistent Threat (APT)

A cyber attack in which an advanced (possibly state backed) hacker or bad actor targets a specific organization for a long period of time by staying hidden in a network.

Bring Your Own Device (BYOD)

A policy allowing employees to use personal devices to access company resources.

Data Incident (or data breach)

An event that occurs when information is accessed and/or exfiltrated by an unauthorized person or entity, like a hacker, without the knowledge of the organization from which it came.

Distributed Denial of Service (DDoS)

A type of attack in which a network is flooded with traffic from multiple sources to overload it and cause a service disruption.

Encryption

The process of converting plaintext into ciphertext using a secret key.

Hacker

Also known as a bad actor or threat actor. An individual who uses a computer system to gain unauthorized access to an account or system for data.

Living off the Land

A cybersecurity attack that involves hackers using the targets existing and known hardware and/or software resources to engage in malicious activity.

Malware

Also known as malicious software that is designed to cause harm to a computer system or network.

Phishing

The most common form of cybercrime in which a hacker or bad actor attempts to gain access to personal and/or company data. Phishing typically occurs via email with links containing malware.

Ransomware

A form of malware where bad actors encrypt information on a computer system so users are unable to access their own data and demand payment in exchange for giving back the information.

Risk Assessment

A big-picture snapshot of your current cyber risk exposure — revealing vulnerabilities and uncovering opportunities to improve defenses.

Zero-day attack

A cyber-attack that infiltrates information systems through unknown vulnerabilities in software and/or firmware. Any server, device, or system pose a risk in vulnerable areas within the update.

SOLUTIONS

Anti-virus (AV)

Software used to identify and isolate (quarantine) viruses, worms, and other malicious software from endpoints (laptop, servers, mobile devices, etc.)

Business Continuity and Disaster Recovery (BCDR)

A solution to reduce business downtime, mitigate legal ramifications, and save SMBs from losing money as the result of disasters, whether natural or human-made.

Cloud Computing

The delivery of computing services, including servers, storage, databases, and software, over the internet.

Cybersecurity Insurance

A form of insurance that protects businesses and individuals from financial loss from cyber attacks or incidents.

Disaster Recovery Plan

A documented procedure for an organization to follow to recover from a disaster that impacts normal operations.

Endpoint Detection and Response (EDR)

A tool that identifies and investigates threats to a business's endpoints. EDR solutions replace traditional Anti-virus software by offering more security.

eXtended Detection Response (XDR)

An advanced security technology that combines multiple security tools and data sources to provide a more thorough and comprehensive look inside your organization's security posture.

Firewall

A network security system that monitors and controls incoming and outgoing network traffic based on security rules.

Incident Response (IR)

A formal, documented, and organized approach to managing the effects of a security incident or cyberattack.

Managed Detection Response (MDR)

A cybersecurity solution that uses EDR monitored 24/7/365 using trained expert humans (SOC) to provide a more complete cybersecurity defense.

Multi-factor Authentication (MFA)

A security method used to add a second layer of authentication when accessing accounts and/or devices. In addition to a username and password - requiring codes, biometrics, or other information.

Secure Access Service Edge (SASE)

A cloud based zero-trust architecture which requires no on-premise hardware.

Security Information and Event Management (SIEM)

Log monitoring and archiving tool providing your business with the ability to identify threats in real time, or investigate historic network, system, and user activity.

Single Sign-On (SSO)

A technology giving users access to multiple accounts with one set of login credentials, reducing the risk of poor password hygiene like weak or reused passwords,

Virtual Private Network (VPN)

A remote connection method used to obfuscate network traffic using strong encryption. Often used to access a corporate network, or add security when using public networks. (airports or hotels.

Vulnerability Management

A service that routinely scans for and patches weak points in your system that could be exploited - providing real-time visibility into potential flaws so they can be addressed before they pose a serious risk.

PEOPLE

Chief Information Security Officer (CISO)

A senior-level executive who is responsible for managing the security of a company's information and technology.

Managed Security Services Provider (MSSP)

An MSP (Managed Services Provider) with a focus on security. MSSPs provide services like cybersecurity, BCDR, network monitoring, and more.

Network Operations Center (NOC)

A centralized location where a team of IT professionals monitor and manage the performance and security of remote monitoring and management software.

Security Operations Center (SOC)

A 24/7 operation staffed by expert humans who review incoming security alerts to take immediate action to isolate and remediate potential threats before they cause significant damage.

4211 South 143rd Circle
Omaha, NE 68137

800-228-3628
secur-serv.com