Cybersecurity Terms

To help make security made simple.



Advanced Next Gen Firewall (NGFW): A deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.

Antivirus: Antivirus software (antivirus program) is a security program designed to prevent, detect, search and remove viruses and other types of malware from computers, networks and other devices.

Cybersecurity: Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.

Cloud Access Security Broker (CASB): A security checkpoint between users of cloud networks and cloud-based applications (SaaS), giving complete visibility into company assets within 3rd party environments. In short, a CASB helps ensure the security of an organization's data in the cloud.

Domain Name System (DNS): The DNS is a naming database in which Internet domain names are located and translated into Internet Protocol (IP) addresses.

Firewall: A firewall is 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.

Network Security: The strategic combination of hardware and software designed to protect the sensitive data housed within the corporate data center.

Secure Access Service Edge (SASE): A cloud architecture model that bundles together network and cloud-native security technologies and delivers them as a single cloud service.

Secure Web Gateway (SWG): Protects your network against unwanted software or malware that users may encounter on the web and blocks risky or unauthorized user behavior. SWGs operate in between company employees and the Internet. Like a water filter, which removes dangerous impurities from water so that it is safe to drink, SWGs filter unsafe content from web traffic to stop cyber threats and data breaches.

Shadow IT: IT applications and services that are acquired by end users without explicit organizational approval and without organizational IT knowledge and support.

Unified Threat Management (UTM): An information security (infosec) system that provides a single point of protection against threats, including viruses, worms, spyware and other malware, and network attacks.

Virtual Private Network (VPN): An encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

Zero Trust: A security framework that requires all users, whether inside or outside an organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or maintaining access to the network.

Zero Trust Network Access (ZTNA): Based on the fundamental principle: trust no one – verify everything. This model enhances network security by expanding access to the actual user endpoint by enforcing strict identity and integrity verification for everyone who accesses the environment.

Types of Threats

Botnet

A collection of Internet-connected devices, which may include personal computers (PCs), servers, mobile devices and Internet of Things (IoT) devices, that are infected and controlled by a common type of malware.

DDoS Attack

Where multiple compromised computer systems attack a target such as a server, website or other network resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down.

Insider Threat

A category of risk posed by those who have access to an organization's physical or digital assets.

Malware

Any program or file that is intentionally harmful to a computer, network or server.

Phishing

A fraudulent practice in which an attacker masquerades as a reputable entity or person in an email or other form of communication.

Ransomware

A subset of malware in which the data on a victim's computer is locked — typically by encryption — and payment is demanded before the ransomed data is decrypted and access is returned to the victim.

COMCAST BUSINESS

Solutions Advisor Program

FOR INTERNAL USE ONLY

©2023 Comcast. All rights reserved. CB-SAP-Cybersecurity-Terms-One-Sheet-D_10.23