TRAVELERS

Test Your Knowledge of Cyber Risk Terms

How's your cyber knowledge? Take our 3-minute cyber IQ quiz to ensure you can talk the talk, and help protect your organization against cybersecurity risks.

Table of Contents

THREATS

Question: A scheme to acquire private personal or financial information using a fraudulent email message is called:

1. Spamming
2. Hacktivism
3. Phishing
4. Cracking

The answer is phishing.

Phishing is a scheme to acquire private, personal or financial information using fraudulent email messages. These types of attacks are declining, though more targeted attacks against one or a small number of individuals, known as "spear phishing," have become more common.

Question: "Our company is starting to store backups off-site to better protect against (fill-in the blank) attacks."

1. Man-in-the-Middle
2. Spyware
3. CRACK Wi-Fi
4. Ransomware

The answer is ransomware.

Ransomware is a type of malicious software that prevents users from accessing their data or systems until a ransom is paid. Cyber criminals are known to have deleted backup files, so maintaining off-site backups is a sound practice.

Question: A (fill-in the blank) is when cyber criminals flood a network with fake traffic to prevent legitimate users from accessing the network.

1. Domain Hijacking Attack
2. Denial-of-Service (DoS) Attack
3. Data Breach
4. Zero-day Attack

The answer is Denial-of-Service (DoS) attack.

In a DoS attack, a network is flooded with spurious traffic to prevent legitimate users from accessing the network. Many experts believe that DoS attacks are likely to worsen as criminals begin to exploit vulnerabilities in the

"Internet of Things," such as networked appliances or smartphones, to carry out the attacks.

Question: A collection of compromised computers under the control of a single entity is commonly referred to as a:

1. Multiplex
2. Rootkit
3. Botnet
4. Virtual Protected Network (VPN)

The answer is botnet.

A botnet is a collection of compromised computers, sometimes numbering in the thousands or even millions, that are under the control of a single entity. Botnets are typically used to steal data, such as online banking credentials, or to facilitate other types of cyber crime, like spamming or DDoS attacks.

Question: The (fill-in the blank) is an anonymous part of the Internet where criminals can buy and sell information stolen from businesses or other entities.

1. World Wide Web
2. Black Market
3. Intranet
4. Dark Web

The answer is Dark web.

The Dark web is a marketplace where private, protected, and proprietary information, as well as the tools that cyber criminals use to hack into computers — such as viruses, exploit kits and other malware — are readily available for purchase and use.

Return to Start

PROTECTION

Question: "By using a (fill-in the blank) our employees can securely access our company's network remotely."

1. Wi-Fi Hotspot
2. Virtual Protection Network (VPN)
3. Virtual Machine
4. Network Segment

The answer is Virtual Private Network (VPN).

A VPN is a secured communication channel that typically uses encryption and is built atop another network, such as the Internet. Businesses that use a VPN to secure remote access to a corporate network are less vulnerable to certain threats, including those associated with using public Wi-Fi hotspots.

Question: A (fill-in the blank) system helps to ensure that known vulnerabilities throughout a network are identified and addressed.

1. Vendor Management
2. Patch Management
3. Mobile Device Management
4. Privileged Access Management

The answer is Patch Management.

Patch management systems are used by companies to obtain, prioritize, validate, and install the various "patches"

or code changes that are made available from the vendors of various applications and systems. Exploiting an unpatched vulnerability is one of the easiest and most common methods criminals use to compromise a computer system or network.

Question: While passwords provide a basic level of protection, a much stronger control for securing access to your organization's network is:

1. Multi-Factor Authentication (MFA)
2. Decryption
3. Remote Access
4. Data Aggregation

The answer is Multi-Factor Authentication (MFA).

MFA is an authentication tool that combines "something you know" (such as a password), "something you have" (such as a text message), and "something you are" (such as a fingerprint scan) to create a stronger access control than only requiring a password. MFA can prevent intruders from spreading across a network from a single compromised computer.

Question: Many experts believe that one of the best ways to protect sensitive data during transmission is to use (fill-in the blank):

1. Network and Application Logging
2. Encryption
3. Content Filtering
4. Firewalls

The answer is Encryption.

Encryption is a method of encoding data so that only authorized parties who possess a decryption key can access the data. Encryption should be considered to protect any sensitive data that is being stored ("data at rest") as well as data that is in transit ("data in motion").

Question: Which of the following services is not used to help a company identify gaps in its security controls?

1. Risk Assessment
2. Cloud Based Authentication
3. Pen Testing
4. None of the Above

The answer is Cloud-based authentication.

Cloud-based authentication can allow a company to consolidate and simplify its sign-on procedures, but is not generally used to identify gaps in a company's security. Risk assessments, however, are widely recommended by cybersecurity professionals because risk assessments can provide a company with an overall evaluation of its security strategy and potential gaps. Penetration testing ("pen testing") is also important in helping a company evaluate its cybersecurity by testing the company's security against a hypothetical attacker.

Return to Start

RESPONSE/RECOVERY

Question: A (fill-in the blank) is a professional who helps organizations navigate response and recovery efforts after a cyber breach.

1. Risk Manager
2. Data Breach Coach

3. Chief Technology Officer (CTO)
4. Contingency Planner

The answer is data breach coach.

A data breach coach is an outside legal counsel experienced in providing guidance throughout the incident response effort, particularly on issues relating to privacy, notification requirements, regulatory compliance, retaining forensic professionals, and managing crisis communications.

Question: Which of the following can help make it easier for your organization to launch a rapid and coordinated response after a cyber attack?

1. Crisis Management Policy
2. Business Continuity Plan
3. Incident Response Plan
4. Data Security Policy

The answer is incident response plan.

Many plans, policies, and strategies contribute to your organization's overall preparedness, but an incident response plan is specifically designed to minimize or contain damage associated with a data breach or network intrusion.

Question: Cybersecurity experts recommend that companies regularly conduct a (fill-in the blank) to test and improve their incident response plans.

1. Risk Analysis
2. Tabletop Exercise
3. Phishing Test
4. Vulnerability Scan

The answer is tabletop exercise.

A tabletop exercise is a discussion-based simulation involving the full incident response team. Conducted annually, it is designed to expose, report and fix any vulnerabilities in your incident response plan before an attack occurs, and it can help ensure post-incident recovery efforts run smoothly.

Question: "To help ensure business continuity in the event of a major cyber incident, we have established a (fill-in the blank) in a different location."

1. IT Help Desk
2. Security Operations Center
3. Hot Site
4. Red Team

The answer is hot site.

A "hot site" is a redundant data center that would be immediately available to support a company's operations if a primary data center were to fail. In contrast, a "cold site" is a backup data center that could be brought online in the event of an emergency, although with some time and effort.

Quesion: What does a cyber insurance policy typically cover?

1. Regulatory Fines and Penalties
2. Consultation with a ″Breach Coach″
3. Data Forensics Services
4. All of the Above

The answer is all of the above.

Cyber insurance is crucial to helping your company address business disruption, revenue loss, legal fees, public relations expenses, forensic analysis, and legally mandated notifications associated with a cyber breach.

Return to Start

Learn More: Cyber Terms
Learn More: 5 Types of Cyber Criminals

TRAVELERS

travelers.com