Cybersecurity Essentials

Cybersecurity protects systems, networks, and data from digital attacks.

CIA TRIAD:

1. Confidentiality
   - Information accessible only to authorized users
   - Encryption, access controls
   - Data classification
2. Integrity
   - Data accuracy and consistency
   - Hashing, digital signatures
   - Version control
3. Availability
   - Systems accessible when needed
   - Redundancy, backups
   - DDoS protection

TYPES OF CYBER ATTACKS:

1. Malware
   - Virus: Attaches to files, spreads
   - Worm: Self-replicating, spreads through network
   - Trojan: Disguised as legitimate software
   - Ransomware: Encrypts files, demands payment
   - Spyware: Secretly collects information
   - Adware: Unwanted advertisements
2. Phishing
   - Fraudulent emails/messages
   - Tricks users into revealing credentials
   - Spear phishing: Targeted attack
   - Prevention: Verify sender, don't click suspicious links
3. Man-in-the-Middle (MITM)
   - Intercepts communication between two parties
   - Eavesdropping, data modification
   - Prevention: HTTPS, VPN, encryption
4. SQL Injection
   - Injects malicious SQL code
   - Gains unauthorized database access
   - Prevention: Parameterized queries, input validation

   Example Attack:

   ```
   ' OR '1'='1
   ```
5. Cross-Site Scripting (XSS)
   - Injects malicious scripts into websites
   - Steals session cookies, credentials
   - Prevention: Sanitize inputs, Content Security Policy

6. DDoS (Distributed Denial of Service)
   - Overwhelms system with traffic
   - Makes service unavailable
   - Prevention: Rate limiting, CDN, firewalls
7. Zero-Day Exploit
   - Attacks unknown vulnerabilities
   - No patch available yet
   - Prevention: Intrusion detection, regular updates

CRYPTOGRAPHY:

1. Symmetric Encryption
   - Same key for encryption and decryption
   - Algorithms: AES, DES, 3DES
   - Fast, but key distribution challenge
2. Asymmetric Encryption
   - Public key for encryption, private key for decryption
   - Algorithms: RSA, ECC
   - Slower, but secure key exchange
   - Used in HTTPS, SSH
3. Hashing
   - One-way function, cannot decrypt
   - Algorithms: SHA-256, MD5, bcrypt
   - Used for password storage, data integrity
4. Digital Signatures
   - Verifies authenticity and integrity
   - Uses asymmetric encryption
   - Non-repudiation

NETWORK SECURITY:

1. Firewalls
   - Filters incoming/outgoing traffic
   - Types: Packet filtering, stateful, application-level
   - Rules based on IP, port, protocol
2. Intrusion Detection System (IDS)
   - Monitors network for suspicious activity
   - Alerts administrators
   - Signature-based, anomaly-based
3. Intrusion Prevention System (IPS)
   - IDS + blocks malicious traffic
   - Active defense
4. VPN (Virtual Private Network)
   - Encrypts internet traffic
   - Hides IP address
   - Protocols: OpenVPN, IPSec, WireGuard

AUTHENTICATION:

1. Something You Know

- Password, PIN
- Weak: Single factor

2. Something You Have
   - Security token, smartphone
   - OTP (One-Time Password)
3. Something You Are
   - Biometrics: Fingerprint, face, iris
   - Behavioral: Typing pattern

Multi-Factor Authentication (MFA):

- Combines two or more factors
- Significantly increases security
- Example: Password + SMS code

SECURITY BEST PRACTICES:

1. Strong Passwords
   - Minimum 12 characters
   - Mix of uppercase, lowercase, numbers, symbols
   - Use password managers (LastPass, 1Password)
   - Don't reuse passwords
2. Regular Updates
   - OS, software, firmware
   - Patches security vulnerabilities
   - Enable automatic updates
3. Backups
   - 3-2-1 Rule: 3 copies, 2 different media, 1 offsite
   - Regular schedule
   - Test restoration
4. Principle of Least Privilege
   - Users have minimum necessary permissions
   - Reduces attack surface
   - Regular access reviews
5. Security Awareness Training
   - Educate users about threats
   - Phishing simulations
   - Report suspicious activity

COMPLIANCE AND STANDARDS:

1. GDPR (General Data Protection Regulation)
   - EU data protection law
   - User consent, right to deletion
   - Heavy penalties for violations
2. PCI DSS
   - Payment Card Industry Data Security Standard
   - Protects credit card data
   - Required for payment processors
3. HIPAA

- Healthcare data protection (US)
  - Patient privacy
  - Encryption, access controls

4. ISO 27001
   - Information Security Management System
   - International standard
   - Risk assessment, controls

INCIDENT RESPONSE:

1. Preparation: Policies, tools, training
2. Identification: Detect and classify incident
3. Containment: Limit damage
4. Eradication: Remove threat
5. Recovery: Restore systems
6. Lessons Learned: Post-incident review

PENETRATION TESTING:

- Ethical hacking to find vulnerabilities
- Tools: Metasploit, Burp Suite, Nmap
- Types: Black box, white box, gray box
- Regular testing recommended