DAYANG NUR NAZIHAH BINTI M ROSLAN
A22DW0255 SECTION 38

CYBERSECURITY IN HEALTHCARE

A MATTER OF LIFE AND DEATH

Start Now →

TYPES OF CYBER THREATS

Malware

- program/code
- infect, damage, or gain access to computer systems
- infiltrates without signals

1. malware triggered to download

2. starts task
   - install more malware
   - steal data

3. stays in the system until detected

COMMON EXAMPLE

Ransomware

Blackmails you

Botnet

Turns your PC into a zombie

Trojans

Sneaks malware onto your PC

TYPES OF CYBER THREATS

Distributed Denial of Service (DDoS)

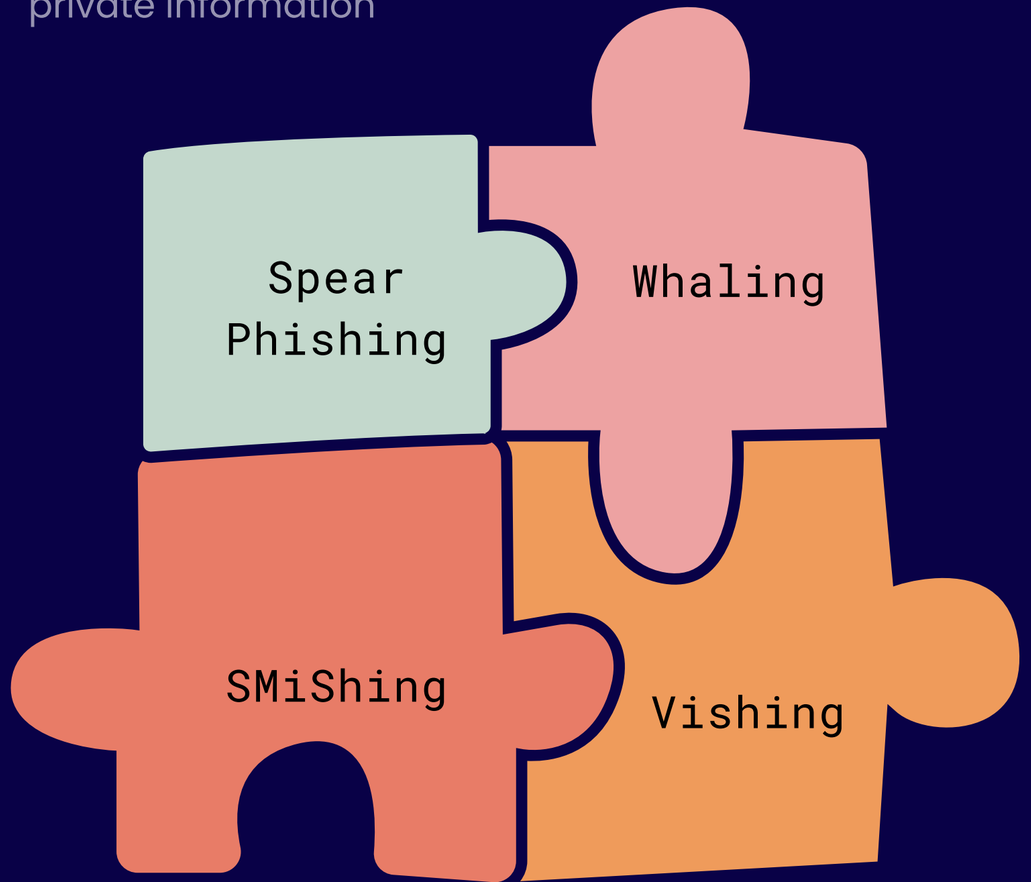
- targeted attack that bombards a network with false request
- disrupts business operations

1. Malware -> network of infected devices
2. “Botnet” floods server’s traffic with false request
3. Normal traffic is denied of service

TYPES OF CYBER THREATS

Phishing

- Utilizes emails, SMS, phone calls to lure victims into sharing their private information



danaconnect.com

VULNERABILITIES IN THE HEALTHCARE SYSTEM

1. LEGACY SYSTEM

old technology used in systems

- ✗ security
- ✗ updates
- ✓ costly to replace

VULNERABILITIES IN THE HEALTHCARE SYSTEM

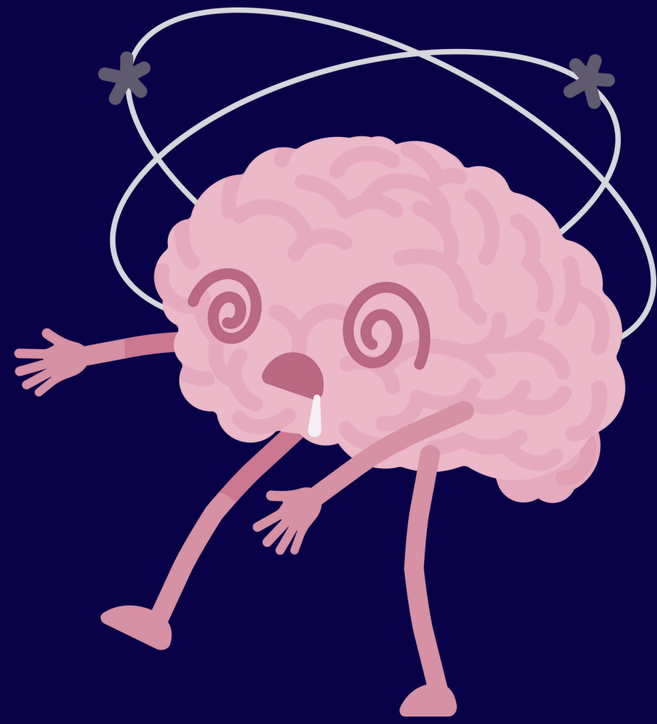
2. INTERNET OF MEDICAL THINGS (IOMT)

interconnected medical devices analysis of medical data for better patient outcome

- seamless communication and compatibility are key factors in a smooth operation
- when not executed, security gaps that are invisible until revealed are created

IMPACT OF CYBERSECURITY BREACHES

1. PATIENT SAFETY AND CARE DISRUPTION



1. compromised patient data
   - hackers can alter patient data that can lead to medical errors
   - identify theft, fraud
2. delayed or inadequate care
   - disrupted access during ransomeware or other incidents, EHRs cannot be accessed for procedures

2. FINANCIAL COST

1. recovery costs
   - investment in remedition
2. direct financial lost
   - hackers steal money from ransomware

CASE STUDIES

CASE STUDIES

RANSOMWARE ATTACK ON HSE IRELAND 2021

- Date: May 2021
- Target: Health Service Executive (HSE) of Ireland

Attack Vector:

- Sophisticated ransomware attack
- Exploited vulnerabilities in IT systems
- Used Conti ransomware, known for rapid spread across networks
- Ransom Demand: 20 million in Bitcoin

Response:

- HSE refused to pay the ransom
- Relied on backups and IT recovery efforts
- Engaged international cybersecurity experts for assistance

CASE STUDIES

DATA BREACH AT UNITYPOINT HEALTH 2024

- Date: March 2024
- Target: UnityPoint Health, a major nonprofit health system in the Midwest, US

Attack Vector:

- Phishing campaign targeted employees with emails that mimicked trusted sources.
- Attackers gained access to email systems and patient databases after several employees provided their login credentials.

Data Compromise:

- The breach exposed sensitive personal and medical data of over 1.5 million patients.

Response:

- UnityPoint Health quickly secured compromised accounts and systems.
- Cybersecurity experts were engaged to investigate and assess the breach.
- Patients were notified promptly, with offers of free credit monitoring and identity theft protection.

CASE STUDIES

DATA BREACH AT MEDSTAR HEALTH 2024

- Date: April 2024
- Target: MedStar Health, a major healthcare provider in the U.S.

Attack Vector:

- Third-Party Vendor Compromise:
- MedStar Health's patient data was exposed due to a security breach at a third-party vendor handling billing and insurance processing.
- Attackers exploited vulnerabilities in the vendor’s system to gain unauthorized access to MedStar Health's patient records.

Data Compromise:

- The breach involved the exposure of personal, medical, and financial information for over 500,000 patients.

CYBERSECURITY STRATEGIES AND BEST PRACTICE FOR HEALTHCARE

HOW?

DATA ENCRYPTION

SECURE CONNECTION

Utilise apps with end-to-end encryption for internal communications.

Secure email

- use encrypted email services

VPN (VIRTUAL PRIVATE NETWORK)

- Encrypts internet traffic and hides IP addresses, securing data during transmission.

REGULAR SECURITY TRAINING

Importance of Employee Training

Educates staff about the latest cybersecurity threats and best practices.

Reduces the risk of human errors that can lead to data breaches.

Ensures employees are aware of and adhere to data protection regulations.

Prepares employees to recognize and report potential security incidents promptly, minimizing potential damage.

INCIDENT RESPONSE AND DISASTER RECOVERY PLANNING

WHAT TO DO?

1. Define roles and responsibilities for the response team.
2. Establish procedures for identifying and analyzing potential security incidents.
3. Outline steps to contain breach, remove threats, restore systems to normal operations.
4. Include protocols for internal and external communication during an incident.

CONCLUSION

Cybersecurity is crucial for safeguarding patient data and maintaining trust in healthcare systems.

Key Strategies:

- Data Encryption: Keeps sensitive information secure and compliant with regulations.
- Secure Communication: Ensures confidentiality during data transmission.
- Employee Training: Reduces risk through awareness and preparedness.
- Incident Response: Prepares for and mitigates impacts of security breaches.

Outcome: Adopting these practices enhances data security, complies with regulations, and supports operational resilience.

QNA

Cybersecurity Presentation

THANK YOU FOR ATTENTION

See You Next →