DEPI - NTI

5/10/2024

Final Project
Cyber Security Consultation

For MediTech Hospital

رواد مصر الرقمية

NTI
National Telecommunication Institute

وزارة الاتصالات وتكنولوجيا المعلومات

Our Group Roles

Samar : Team Leader

Responsibility:
& Suggest project scenario.
& Present risk assessment.
& Present Project goals
& Coordinate and guide team.
& Work on Ransomeware Attack Scenario.

Sara : Member

Responsibility:
& Present policy development .
& collect Data.
& prepare pdf.
& prepare PowerPoint presentation.

Miar : Member

Responsibility:
& Work on Technological recommendations.
& collect Data.
& present Technological recommendations part.

Alaa^ : Member

Responsibility:
& Present Continuous monitoring.
& Collect Data.
& Prepare PDF for continuous monitoring.

Jihad : Member

Responsibility:
& Present Continuous monitoring.
& Collect Data.
& Prepare PDF for continuous monitoring.

Menna : Member

Responsibility:
& Present employee training.
& Collect Data.
& prepare PDF for employee training part.

Our Company Name:
CyberGuardians

Organization: Medi-Tech Hospital

Cyber Attack: Ransomware Attack

What is a Ransomware Attack ?

Ransomware is a type of malicious software that encrypts or locks your files, making them inaccessible until you pay a ransom. It's a form of cyber extortion, where attackers demand payment in exchange for restoring your data.

Scenario

A sophisticated ransomware group targets MediTech Hospital, compromising their Electronic Health Records (EHR) system. The attackers encrypt patient data, demanding a hefty ransom for decryption.

Scenario

The hospital is forced to shut down its EHR system, leading to significant disruptions in patient care, including delays in diagnosis, treatments, and access to medical records.

The attack also exposes sensitive patient information, potentially leading to identity theft and financial fraud.

1
Risk Assessment

2
Policy development

3
Security awareness training

4
Technology recommenda tion

5
Continuous monitoring and improvement

Project goals

The primary purpose

Project Goals

Presented by
Samar Mohamed Saker

Project Goals

Cybersecurity Audit is essential to identify, diagnose, and resolve security vulnerabilities or breaches within computer systems, networks, and digital infrastructure.

Its primary purpose is to:

Project Goals

The primary purpose

1. Protect sensitive data
2. Maintain system integrity
3. Minimize downtime and financial losses
4. Enhance overall security posture
5. Minimize Data Loss
6. Restore System Functionality
7. Prevent Future Attacks

Project Goals

1.Protect sensitive data

By identifying and rectifying vulnerabilities, cybersecurity troubleshooting helps safeguard critical information from unauthorized access, theft, or destruction.

2. Maintain system integrity

It ensures that systems are functioning as intended and are not compromised by malicious activities.

Project Goals

3.Minimize downtime and financial losses

Promptly addressing security issues can prevent disruptions to operations and reduce the costs associated with data breaches or system failures.

4.Enhance overall security posture

Through troubleshooting, organizations can identify weaknesses in their security measures and implement necessary improvements to strengthen their defenses.

Project Goals

5.Minimize Data Loss

Recover as much data as possible, even if it requires manual restoration from backups.

6.Restore System Functionality

Ensure that the affected system is operational and can be used again.

Project Goals

7.Prevent Future Attacks

Learn from the incident and implement measures to enhance security.

In essence, cybersecurity Audits acts as a proactive measure to maintain a secure and resilient digital environment

1 - Risk Assessment

Assessing Healthcare Vulnerability to Ransomware Attacks

Presented by
Samar Mohamed Saker

Assessing Healthcare Vulnerability to Ransomware Attacks

Healthcare organizations are prime targets for ransomware attacks due to their reliance on critical infrastructure, sensitive patient data, and often outdated IT systems. Let's explore some key vulnerabilities that make these institutions susceptible:

Assessing Vulnerabilities

1. Outdated IT Infrastructure:

Legacy System :

we find that healthcare facilities still rely on older systems that lack the security features and updates necessary to protect against modern threats.

Unpatched Software:

There was Outdated software with known vulnerabilities which was exploited by attackers to gain unauthorized access.

Assessing Vulnerabilities

2. Lack of Cybersecurity Awareness:

Phishing Attacks:

One of Healthcare staff Used more susceptible phishing email, especially those that impersonate patients or colleagues.

Clicking on Malicious Links:

Some Employees clicked on malicious links or attachments, leading to malware infections.

Assessing Vulnerabilities

3. Interconnected Systems:

Lateral Movement:

Some attackers gain a foothold in a network, they could exploit interconnected systems to spread laterally and access sensitive data.

Supply Chain Attacks:

Compromised third-party vendors or suppliers can serve as entry points

Assessing Vulnerabilities

4. Data Sensitivity

Patient Records:
Healthcare organization hold highly sensitive patient data, including personally identifiable information (PII), medical records, and financial details.

Financial Data:
Ransomware attackers often target healthcare organizations for financial gain, demanding ransoms in exchange for decrypting encrypted data.

Assessing Vulnerabilities

5. Operational Criticality:

Disruption of Care:
Ransomware attackers could disrupt essential healthcare services, leading to delays in patient care, compromised safety, and increased costs.

Financial Loss:
Downtime due to ransomware attacks could result in significant financial losses, including lost revenue, increased operational costs, and potential legal liabilities.

Assessing Vulnerabilities

6. Regulatory Compliance:

HIPAA and ISO27001:

Healthcare organization was subject to strict data privacy regulations like HIPAA and ISO27001, which impose penalties for data breaches.

Reputation Damage:

A ransomware attack could damage a healthcare organization's reputation, leading to loss of trust from patients, insurers, and other stakeholders.

RISK CONTROL

RISK TREATMEN

1.Risk Control

Isolate Infected Systems:	Implement Incident Response Plan	Implement log management System	Implement framework Security Standard
Quickly isolate the compromised EHR system from the hospital network to prevent further lateral movement of the ransomware.	Activate the hospital's incident response plan, ensuring that all relevant stakeholders are informed and coordinated.	Collect as much evidence as possible about the attack, including logs, network traffic, and any indicators of compromise (IOCs).	relevant regulatory bodies, such as the Health Insurance Portability and Accountability Act (HIPAA) and ISO27001 enforcement agency.

2.Incident Analysis and Remediation

1 Determine Root Cause

Conduct a thorough investigation to understand how the ransomware gained access to the hospital's network and identify any vulnerabilities that allowed the attack to occur.

2 Remediate Vulnerabilities

Patch all known vulnerabilities in the hospital's systems and implement security controls to prevent similar attacks in the future.

2.Incident Analysis and Remediation

3 Restore System

Develop a plan to restore the EHR system from backups, ensuring that patient data is recovered accurately and without corruption.

4 Strengthen Security Measures

Implement stronger security measures, such as multi-factor authentication, intrusion detection systems, and regular security awareness training for staff.

2.Incident Analysis and Remediation

5 Notify Patients

Communicate with patients about the data breach and the potential risks, including identity theft and financial fraud.

6 Offer Support

Provide patients with resources and guidance on how to protect themselves, such as monitoring their credit reports and changing passwords.
Comply with Regulations: Ensure that the hospital complies with all relevant data privacy regulations, including HIPAA and ISO27001

3.Long-Term Recovery and Resilience

DEVELOP A ROBUST BUSINESS CONTINUITY PLAN

Create a comprehensive business continuity plan that outlines how the hospital can continue to provide essential services in the event of a future cyberattack.
systems are functioning as intended and are not compromised by malicious activities

CONDUCT POST-INCIDENT REVIEW:

Conduct a detailed review of the incident to identify lessons learned and areas for improvement.

BUILD PARTNERSHIPS

Collaborate with other healthcare organizations and industry experts to share best practices and learn from collective experiences.
Specific Recommendations for MediTech Hospital

INVEST IN CYBER SECURITY

Allocate sufficient resources to invest in ongoing cyber security measures, including staff training, technology upgrades, and incident response capabilities.

3.Long-Term Recovery and Resilience

ENCRYPT DATA AT REST AND IN TRANSIT

Ensure that patient data is encrypted both when stored on disk and when transmitted over the network.

IMPLEMENT A ZERO-TRUST ARCHITECTURE

Adopt a zero-trust security model that assumes all network traffic is untrusted, requiring strict verification and authorization before access is granted.

SECURITY AUDITS AND PENETRATION TESTING

Conduct regular security audits and penetration tests to identify vulnerabilities and assess the effectiveness of security controls.

PROVIDE COMPREHENSIVE STAFF TRAINING:

Train staff on security best practices, including password management, phishing awareness, and recognizing signs of a cyberattack.

3.Long-Term Recovery and Resilience

CONSIDER A MANAGED SECURITY SERVICE PROVIDER (MSSP)

Partner with a reputable MSSP to provide ongoing monitoring, threat detection, and incident response capabilities.thorization before access is granted.

Thank You!

2- Policy development

CRAFTING POLICY TO SECURE MEDI-TECH HOSPITAL INFORMATION

Presented by
Sara Mohamed Radwan

POLICY DEVELOPMENT

Is created in order to protect the Confidentiality, Integrity and Availability of information created, collected, and maintained.

1.Acceptable Use

2. Access Management

2.1 Authentications

3. Data Security

4. Hardware and Software

5. Internet

6. Enforcement

1 Acceptable Use

1. Personnel are responsible for complying with the hospital's policies when using the hospital information resources.

2. Personnel must promptly report misuse or any action that goes against the policy to their manager or a member of the Incident Handling Team; involving:
   - Hospital assets
   - Hospital information

3.Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system.

For example:
hospital personnel should not run

- password cracking programs
- any other non-approved programs

on any hospital Information Resource.

4. Hospital Information Resources are provided to facilitate hospital business and should not be used for personal financial gain.

5. Personnel are expected to cooperate with incident investigation.

2 Access Management

1. Access to information is based on a "need to know".

- Personnel are permitted to use only the network issued to them by hospital IT and should not attempt to access any data or programs contained on hospital systems for which they do not have authorization.

2. All remote access connections made to internal hospital networks must be made through approved, and hospital-provided, virtual private networks (VPNs).

3.Personnel must <u>not share</u> their (personal authentication information, including:

1. Account passwords,
2. Personal Identification Numbers (PINs),
3. Security Tokens (i.e. Smartcard),
4. Multi-factor authentication information
5. Access cards and/or keys

2.1 Authentications

1.All personnel are required to maintain the confidentiality of personal authentication information.

2.Any group/shared authentication information must be maintained solely among the authorized members of the group.

3. If the security of a password is in doubt, the password should be changed immediately.

4. Personnel should not give permission to any application or website to remember their password.

3 Data Security

1.Personnel should use approved encrypted communication methods whenever sending confidential information over Internet.

2. Confidential information transmitted via USB or other mail service must be secured

3. Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.

1.Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.

2. Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.

3. Confidential information must be transported by IT Management.

4 Hardware and software

1.All hardware must be formally approved by IT Management before being connected to hospital networks.

2.Software installed on hospital equipment must be approved by IT Management and installed by IT personnel.

3.All hospital assets taken off-site should be physically secured at all times.

4.Employees should not allow family members or other non-employees to access hospital Information Resources.

5 Internet

1.Internet is Managed by Firewall (Technological Recommendations)

2.The Internet must not be used to communicate hospital confidential or internal information, unless the confidentiality and integrity of the information is ensured and the identity of the recipients is established.

3. Use of the Internet with hospital networking or computing resources must only be used for business-related activities.

- Unapproved activities include, but are not limited to:

1. Recreational games,
2. Streaming media,
3. Personal social media,
4. attempting or making unauthorized entry to any network or computer accessible from the Internet.

6 Enforcement

1. Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

2.Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract, and related civil or criminal penalties.

Thank You!

3- Security Awareness Training

TRAINING EMPLOYEES AND RAISING AWARENESS

Presented by
Menna Kamal

CYBER SECURITY AWARENESS TRAINING

Presented by Menna Kamal
Junior cybersecurity analyst at CyberGuardians Solutions

ABOUT US

Cyberguardians is a well known cybersecurity corporate that had been in the market for 10 years. We provide top tier security services to different customers from different sectors. We had the honor of working with several hospitals, hotels and even banks like the WQB bank and the Cure hospital. We provide professional awareness training for your employees, implement various cybersecurity solutions such as advanced firewall implementation, data backup, network monitoring and regular risk and vulnerability assessments. We aspire to provide you with the stability and confidence that enables you to deliver the best experience to your customers.

WHAT IS CYBERSECURITY

Cybersecurity is the means of securing data, networks and devices to ensure data *availability*, *integrity* and *confidentiality*, and protect from unauthorized access or malicious exploitation of these systems and data.

THE IMPORTANCE OF CYBERSECURITY

Protecting online presence:

You may not realise it but as you browse the internet you leave digital footprints everywhere, and cookies collect data about you: data which the attacker can exploit to initiate a cyberattack.

THE IMPORTANCE OF CYBERSECURITY

Avoiding theft:

Most likely the **motives of the attackers** centre around **financial gain** ,so what happens if your **credit card's information** is not well guarded?

Also consider that some attacker may steal parts of your processor power for **crypto mining**.(however this attack is usually hard to notice)

THE IMPORTANCE OF CYBERSECURITY

Personal data:

- SSID No., medical profile, address
- Credit card and bank account information

Corporates and companies:

- Secret company strategies, secret policies
- Company's IT infrastructure
- Data of employees and customers

THE IMPACT OF CYBER THREATS ON BUSINESS PERFORMANCE

Ransomware

- Leads to data encryption and loss.
- Financial loss to get the cipher key: warning! Never pay the ransom.

Distributed denial of services (DDOS)

- Halting of business services
- Ruining business reputation

Spyware

- Leakage of sensitive data
- Attacker will likely know enough about you to impersonate you.
- Which might lead to identity theft, and legal problems.

THE IMPACT OF CYBER THREATS ON BUSINESS PERFORMANCE

Worms

- Self replicating malware
- Can spread on its own over the network
- May be hard to detect

Rootkits

- Malware that hides in the OS kernel
- Extremely hard to detect and remove
- Can allow attacker to have complete control over the system

Zero-day exploits

- Attackers who exploit known software vulnerabilities to gain unauthorized access
- Can be difficult to protect against due to little given time for preparation

THE IMPACT OF CYBER THREATS ON BUSINESS PERFORMANCE

THE IMPACT OF CYBER THREATS ON BUSINESS PERFORMANCE

A real life example: Wanna cry ransomware

The WannaCry ransomware attack was a global cyberattack that took place in May 2017. It exploited a vulnerability in windows 7 OS. It hit around 230,000 computers globally (in about 150 countries), and led to financial losses of an estimated 4 billion dollars.

THE IMPACT OF CYBER THREATS ON BUSINESS PERFORMANCE

A real life example: Wanna cry ransomware

Could have been avoided with a simple software update.

But instead we lost 4 billion $ in one year !

THE IMPACT OF CYBER THREATS ON BUSINESS PERFORMANCE

A real life example: Wanna cry ransomware

Is WannaCry Still a Threat?

- Yes, WannaCry is still a threat: due to evolving attack surfaces and vectors.
- WannaCry exploits outdated systems: many organizations fail to update operating systems despite available patches from Microsoft.
- Ransomware activity is increasing: In 2021, there was a 53% rise in successful WannaCry attacks.

THE IMPACT OF CYBER THREATS ON BUSINESS PERFORMANCE

A real life example: Wanna cry ransomware

Is WannaCry Still a Threat?

- Variants are emerging: New cryptoworm and ransomworm variants are spreading globally.
- Rapid spread: WannaCry can propagate through networks quickly, needing only a single entry point to infect entire systems.
- Insufficient protection: Many networks remain vulnerable due to poor cybersecurity measures and lack of regular updates.

SOCIAL ENGINEERING: EXPLOITING THE HUMAN ERROR

Be careful who you trust:

Hackers don’t only tend to exploit software vulnerabilities, but they also leverage human empathy, DO NOT ever dispose of sensitive information without consulting IT and company policy.

SOCIAL ENGINEERING: EXPLOITING THE HUMAN ERROR

Watch what happens during social engineering :

https://youtu.be/lc7scxvKQOo?si=DI-ybDgfUj7Vy4LD

TYPES OF CYBER THREATS

TYPES OF THREAT ACTORS AND THEIR MOTIVES

Cybercriminals

- Motives are variable and mainly financial

Hacktivists

- Usually they have some political agenda to promote

State sponsored

- Directed cyber warfare against enemy countries

Insider threat

- Could be intentional (disgruntled employee)
- Or could be unintentional (an employee with little cyber awareness)

COMMON VULNERABILITIES

Social engineering

- Hackers may leave behind infected USB drives for curious employees
- Attackers may use emotional manipulation to steal personal data or credentials

Outdated software

- Software without recent security patches can have known vulnerabilities.
- Cybercriminals exploit unpatched software to infiltrate systems.
- Regular updates and patch management are critical to defence.

COMMON VULNERABILITIES

Weak or compromised credentials

- Simple or reused passwords are easy for attackers to guess or crack.
- Stolen credentials from breaches can give attackers direct access.
- Strong passwords and multi-factor authentication reduce the risk.

Phishing

- Attackers use fraudulent emails or websites to trick users into revealing sensitive information.
- Often used to steal login credentials, financial data, or install malware.
- Employee training and email filtering are key defences against phishing.

How to Spot a Phishing Email

Cyber Security Top Tips

mtechsystems

Proven Innovation

PHISHING

A cybercrime whereby individuals are targeted via email by someone fraudulently posing as a legitimate business to encourage them to reveal personally identifiable information, including passwords and bank details.

Be alert, stay vigilant, don't give out important information.

It's always better to question a request than action it.

To: mr.teacher@yourschool.co.uk

From: Mrs Headteacher <joe.bloggs@yoursch00l.co.uk>

Subject: You've won!

Dear Sir,

You've won the teecher of the term competition - 4 tickets to the theatre for you and 3 colleagues!

To get your tickets, please send the name, address and date of birth for each of your guests to this secure link.

Leave your details by midday today or the prize will roll over to next term.

Well done!

Mrs Headteacher

Would the sender normally address you in this way?

Are there unusual spelling and grammar errors?

Hover over the link, where does it go? Would you expect the need for a link?

Is there a signature, would you expect to see one?

Does the 'From' name match the email address?

Does the email address match the organisation name?

Is there really a competition and did you enter?

Why are you being asked to provide the personal information of colleagues?

Is there a sense of urgency - does there need to be?

CYBERGUARDIANS

TECHNOLOGY & CYBERSCUITY

INCIDENT RESPONSE: FIRST AID THREAT REMEDIATION

What to do when an attacker strikes

- Identify the Threat
- Contain the Breach
- Deal With Contingencies
- Notify Law Enforcement
- Investigate the Breach

INCIDENT RESPONSE: FIRST AID THREAT REMEDIATION

CYBERGUARDIANS
TECHNOLOGY & CYBERSCUITY

What to do when an attacker strikes

- Restore the System
- Talk to Your Legal Team
- Contact Those Affected
- Follow Up on the Attack
- Evaluate and Update Your Cybersecurity plan

PREVENTATIVE MEASURES

Do NOT open fishy links WRITE TO US Check their URL first

Never give your password or credentials to a friend or colleague (or anyone in general)

Do NOT download any software from unofficial websites

Consult IT and security team for a regular malware scan

CYBERGUARDIANS
TECHNOLOGY & CYBERSCUITY

PREVENTATIVE MEASURES

If you have a device from the company, keep it in a safe and secure location.

Avoid connecting the company's mobile device(s) to free wifi (it can easily be a hacking bait)

Ensure the use of strong passwords

Limit the use of external devices such as flash drives without the IT's consent

MORE ON RANSOMWARE

https://youtu.be/lIsWpCMBxHQ?si=CrNGOAYPR3dOeHu5

Q & AS

THANK YOU !

4- Technology recommendation

RECOMMENDING THE BEST TECHNOLOGY

Presented by
Maiar Wael Elshamy

1- Firewall Configuration

- A robust firewall is essential for controlling network traffic.
- **Acts as the first line** of defense against unauthorized access.
- **Next-Generation Firewall (NGFW) provides:**
  - Advanced threat detection.
  - Deep Packet Inspection (DPI).
  - Monitoring of encrypted traffic.

Proper firewall policies should block suspicious IP addresses and restrict unnecessary communication between internal systems.

1- Firewall Configuration

2- Intrusion Detection/ Intrusion Prevention Systems (IDS/IPS)

- **IDS/IPS** are critical for identifying and blocking malicious activity on the hospital network.
- **Implementing network-based IDS/IPS solutions allows for:**

- Monitoring traffic for abnormal behavior.
- Detecting ransomware signatures and preventing exploit attempts.

2- Intrusion Detection/ Intrusion Prevention Systems (IDS/IPS)

The system should:

- Alert security personnel immediately upon detecting an attack pattern.
- Block malicious traffic in real time -in the case of IPS

2- Intrusion Detection/ Intrusion Prevention Systems (IDS/IPS)

- **IPS threat prevention methods:**

Blocking malicious traffic

An IPS may end a user's session, block a specific IP address or even block all traffic to a target. Some IPSs can redirect traffic to a honeypot, a decoy asset that makes the hackers think they've succeeded when, really, the SOC is watching them.

Removing malicious content

An IPS may allow traffic to continue but scrub the dangerous parts, such as by dropping malicious packets from a stream or removing a malicious attachment from an email.

2- Intrusion Detection/ Intrusion Prevention Systems (IDS/IPS)

- **IPS threat prevention methods:**

Triggering other security devices

An IPS may prompt other security devices to act, such as by updating firewall rules to block a threat or changing router settings to prevent hackers from reaching their targets.

Enforcing security policies

Some IPSs can prevent attackers and unauthorized users from doing anything that violates company security policies. For example, if a user tries to transfer sensitive information out of a database it's not supposed to leave, the IPS would block them.

What Does an Intrusion Detection System Do?

3- Anti-virus and Anti-malware Solutions

- **Installing** a reliable and up-to-date anti-virus and anti-malware solution is crucial for preventing ransomware spread.
- **The solution should provide:**
  - Real-time scanning capabilities.
  - Quarantine for suspicious files.
  - Regular updates to protect against emerging ransomware variants.

3- Anti-virus and Anti-malware Solutions

Centralized management allows IT administrators to:

- Monitor the health of all devices.
- Respond quickly to detected threats

4- Physical Access Controls

Physical security is crucial for safeguarding sensitive systems.

MediTech Hospital should:

- Restrict access to sensitive areas (e.g., server rooms) using biometric authentication or keycard systems.
- Ensure only authorized personnel have physical access to critical hardware to reduce tampering risks.

5- Closed-Circuit Television (CCTV)

areas (e.g., data centers, server rooms) adds an extra layer of protection.

·**CCTV monitoring should be:**

- Integrated with access control systems to log and review entries into secure areas.
- Continuously monitored for real-time surveillance and historical records for investigations.

6- Switch Upgrades for Port Security

MediTech Hospital should upgrade networking switches to support port security features.

6- Switch Upgrades for Port Security

This upgrade ensures:

- Only authorized devices can connect to the network, reducing malware risks.
- IT teams can limit connections to switch ports and apply MAC address filtering.
- Switches are configured to shut down a port automatically if a violation is detected.

7- Network Segmentation

- **Definition**: Divides the hospital's network into smaller, isolated segments.
- **Benefits**:
  - Limits the spread of ransomware.
  - Reduces lateral movement by attackers.

8- Data Backup and Recovery Systems

Importance: Minimizes the impact of ransomware.

Strategy:

- Maintain encrypted, offline backups of patient data and critical systems.
- Enables quick restoration of operations without paying ransom.

8- Data Backup and Recovery Systems

Best Practices:

- Automate the backup process.
- Conduct frequent backups stored in multiple locations.
- Perform periodic testing for recovery readiness.

9- Encryption of Sensitive Data

Purpose: Protects sensitive data, such as patient records.

Mechanism:

- Ensures attackers cannot read files without encryption keys.
- Implement end-to-end encryption for all sensitive data.

Outcome: Makes it harder for ransomware actors to profit from stolen data.

10- Multi-Factor Authentication (MFA)

- **Functionality**: Adds an extra layer of security for critical system access.
- **Requirements**:
  - Users must verify identity using two or more factors (e.g., password and biometric scan).
- **Advantage**: Prevents unauthorized access even if login credentials are stolen

11- Patch Management and System Updates

Necessity: Protects against ransomware exploits.

Implementation:

- Keep systems updated with the latest security patches.
- Use an automated patch management system for timely updates.

Risk: Unpatched vulnerabilities are common entry points for ransomware attacks.

12- Email Filtering and Security Awareness Training

Risk Mitigation: Reduces risk of ransomware entering through phishing emails.

Solutions:

- Deploy advanced email filtering solutions to scan for suspicious attachments, links, and sender patterns.

12- Email Filtering and Security Awareness Training

Training: Conduct regular security awareness training for staff on phishing threats and safe browsing habits.

13- Incident Response Plan (IRP)

- **Purpose**: Ensures quick and effective response during a ransomware attack.
- **Components**:
  - Steps for detecting an attack.
  - Procedures for isolating affected systems.
  - Plans for restoring operations from backups.
- **Readiness**: Conduct regular drills and simulations to ensure preparedness.

14- Zero Trust Architecture

"Never Trust, Always Verify"

- **Model:** Assumes no device, user, or system can be trusted until verified.
- **Access Control:**
  - Limits access based on identity.
  - Continuously monitors even trusted entities for suspicious behavior.
- **Outcome**: Reduces likelihood of unauthorized lateral movement within the network.

15- Endpoint Detection and Response (EDR)

- **Function**: Allows for continuous monitoring and threat detection across all endpoints.
- **Capabilities**:
  - Analyzes device behavior in real-time.
  - Detects anomalies and isolates infected devices.
- **Goal**: Prevents ransomware from spreading within the network.

Thank You!

5- Continuous monitoring and improvement

MONITORING EVERY THING

Presented by
Jihad Gomaa Aldaly
Alaa’ Shaaban

Implementing Continuous Monitoring and Improvement

Conduct a Thorough Incident Response and Forensic Investigation

Identify the attack vector and the scope of the breach.

Gather evidence to understand the attacker's methods and motives.

Document the incident response process for future reference and improvement.

Enhance Security Posture

Patch Management:

Implement a rigorous patching process to address known vulnerabilities in the EHR system and other critical infrastructure

Network Segmentation

Isolate sensitive systems from the public internet and implement strong network segmentation to limit the spread of malware

Enhance Security Posture

ACCESS CONTROLS

Implement robust access controls to restrict access to sensitive data and systems based on the principle of least privilege

Multi-Factor Authentication (MFA)

Require MFA for all user accounts, especially those with privileged access.

Enhance Security Posture

REGULAR SECURITY ASSESSMENTS

Conduct regular vulnerability assessments and penetration testing to identify and address potential weaknesses in the security infrastructure.

Implement Continuous Monitoring

1 Security Information and Event Management (SIEM):

Deploy a SIEM solution to collect, analyze, and correlate security events from various sources.
Network Traffic Monitoring: Monitor network traffic for suspicious activity, such as unusual data transfers or unauthorized access attempts.

2 Endpoint Detection and Response (EDR):

Use EDR solutions to detect and respond to threats at the endpoint level.

Implement Continuous Monitoring

3 Cloud Security Posture Management (CSPM)

If the EHR system is hosted in the cloud, implement CSPM tools to monitor and manage cloud security posture.

4 Data Backup and Recovery:

Implement a robust data backup and recovery plan to ensure that critical data can be restored in the event of a successful attack. Test the backup and recovery plan regularly to verify its effectiveness.

Implement Continuous Monitoring

5 Employee Training and Awareness:

Provide employees with regular security awareness training to help them recognize and avoid phishing attacks, social engineering, and other common threats.
Educate employees about the importance of following security best practices, such as using strong passwords and avoiding sharing sensitive information

Implement Continuous Monitoring

6 Incident Response Planning

Develop and maintain a comprehensive incident response plan that outlines the steps to be taken in the event of a security breach. Conduct regular tabletop exercises to test the incident response plan and identify areas for improvement.

Implement Continuous Monitoring

7 Regular Security Audits and Reviews

Conduct regular security audits and reviews to assess the effectiveness of security controls and identify areas for improvement.

Implement Continuous Monitoring

8 Engage external security experts

Engage external security experts for independent assessments to provide a fresh perspective.

1
Risk Assessment

2
Policy development

3
Security awareness training

4
Technology recommenda tion

5
Continuous monitoring and improvement

By implementing these measures, MediTech Hospital can significantly improve its security posture

Any Questions?

Thank You