Hardening Cybersecurity Presentation - March 14, 2025

Benjamin Taylor

Slide 1: Title - "Hardening Cybersecurity"

What is Cybersecurity?

- Practice of protecting computer systems, networks, and data from cyberattacks
- Attacks can come from hackers, viruses, ransomware, and other malicious people

“Hardening Cybersecurity” Meaning

- Making a system more secure by reducing vulnerabilities
- Hardened cybersecurity makes it harder for hackers to break in, like a castle with thick walls and a moat

Slide 2: "How to Hack a Hospital" - The Reality of Cyber Attacks on Healthcare

Why are Hospitals a Target?

- Hospitals rely on tech heavily for patient records, medical devices, and communication
- If a hospital is hacked, lives are at risk - they are more likely to pay the ransom to restore records
- Many hospitals use outdated software that is easy for hackers to break into

Slideshow Purpose

- Not to teach people how to hack but instead to help them understand how cybercriminals exploit hospitals so we can learn to stop them

Slide 3: Disclaimer

Why is this Important?

- Cybersecurity is very important, but it must be ethical
- Learning about attacks helps defend against them, but using the knowledge to hack would be illegal

Slide 4: Bruce Schneier Quote

> **"The internet is about to start killing people, and the government regulates things that kill people."** – Bruce Schneier, 2019

What Does This Mean?

- Bruce Schneier is a cybersecurity expert who warns that as we connect more life-critical systems (hospitals, power grids, transportation, etc) to the internet, hackers could cause real-world harm, even deaths

How Could Cyber Attacks Harm Lives?

1. Hospital Systems: If ransomware locks medical records, doctors can't treat patients
2. Traffic Lights & Power Grids: Cause accidents or blackouts
3. Hacked Medical Devices: pacemakers, insulin pumps, ventilators, etc., can be remotely controlled and compromised

Slide 5: Purpose of Presentation

Aims to Explore Cybersecurity in Healthcare from:

1. Historical Perspective: Past cyberattacks on hospitals
2. Scientific Perspective: How attacks technically work
3. Ethical Perspective: What security measures are needed to protect people

Slide 6: WannaCry Ransomware Attack (May 12, 2017)

One of the most **devastating cyberattacks** in history

What is Ransomware?

- Ransomware is a type of malware (malicious software) that:
  1. Encrypts (locks) files on a computer
  2. Demands a ransom (money) in Bitcoin to unlock them

What Happened in the WannaCry Attack?

- 200,000+ computers in 150+ countries were infected
- Hospitals, businesses, and governments were affected
- Notable victims: UK's National Health Service (NHS), FedEx, Honda, and more

Slide 7: WannaCry Ransomware Attack (May 12, 2017)

The **UK's National Health Service** (NHS) was one of the **hardest-hit victims**

How WannaCry Affected NHS Hospitals

- **80+ hospitals affected** - computers stopped working
- **595 General Practitioner (GP) offices affected** - doctors couldn't access patient files
- **Surgeries cancelled, ambulances diverted** - patients in need couldn't get immediate treatment
- **Medical devices infected** - MRI scanners and blood storage refrigerators stopped working
- **Ransom demand: $300 per system in Bitcoin** - hackers demanded digital payments to unlock the files

Why is This So Serious?

- When hospitals go offline, lives are at risk
- Even non-hacked hospitals suffer since they must take in diverted patients
- Medical records and diagnostic tools are very important - without them, doctors cannot properly treat people

Slide 8: Why are Hospitals Vulnerable / How WannaCry Spread

Hospitals were hit hard by WannaCry because of four major weaknesses:

1. **Outdated Systems:** Many hospitals used Windows XP (released in 2001), which Microsoft no longer updated
2. **Interconnected IoT Devices:** Medical devices like MRI scanners were connected to the internet but had weak security
3. **Lack of Cybersecurity Funding:** Hospitals focused on patient care, not IT security
4. **Improper Data Backups:** Without backups, hospitals had no way to restore files after the attack took place

---

What Made WannaCry So Dangerous?

- **EternalBlue Exploit (NSA leak)** - allowed hackers to break into computers
- **Self-spreading worm** - once inside a network, it automatically spreads
- **Data Encryption & Ransom** - files were locked, and a ransom demand appeared

EXPLANATION – EternalBlue Exploit (NSA Leak)

What is EternalBlue?

- A software vulnerability in Microsoft Windows (found in Windows XP, Windows 7, etc)
- Discovered by the National Security Agency (NSA) in the U.S.
- Instead of reporting to Microsoft, the NSA kept it secret to use for spying purposes
- Uses scanning with Nmap and Metasploit

What is an Exploit?

- An exploit is a method hackers use to take advantage of security weaknesses
- In this case, EternalBlue allowed hackers to break into computers remotely

How Was It Leaked?

- A hacking group called the Shadow Brokers stole EternalBlue from the NSA
- They released it online in April 2017, a month before the WannaCry attack

How WannaCry Used EternalBlue

1. A hacker sends malware to an unpatched computer
2. EternalBlue lets the hacker take full control of the computer
3. The ransomware installs itself and spreads to other computers automatically

Slide 9: NotPetya (June 27, 2017) - Even More Destructive

A different cyberattack **one month after WannaCry**, but even worse

How NotPetya Was Different

- Also used the EternalBlue exploit (like WannaCry)
- Not ransomware, but it did pretend to be. Instead, permanently deleted files
- **Major victims** - shipping companies, pharmaceuticals, FedEx, and even Chernobyl's radiation monitoring stations
- $**10 billion in damages** - one of costliest cyberattacks ever

Slide 10: Real-World Consequences

Cyberattacks aren't just about stolen passwords/leaked emails; they affect real people, disrupt life-saving treatments, and cost billions of dollars

1. **Immediate Impact on Hospitals**
   - Over 19,000 Appointments and Surgeries Canceled
     - If the scheduling system is hacked, doctors and nurses can't see when patients are coming in
     - Life-threatening delays: some people who need urgent surgery may not be treated in time to save them
     - Surgeries relying on digital medical imaging (X-rays, MRIs, CT scans) may be impossible without computer access
   - Ambulances Diverted
     - Hospitals rely on digital systems to track which ER rooms are available
     - If computers stop working, hospitals cannot handle new patients, forcing ambulances to drive further to uncompromised hospitals
     - This costs lives, especially when it comes to heart attacks, strokes, etc., where seconds matter
   - Locked Out of Patient Records
     - Medical records contain everything about a patient's history - allergies, medications, test results, etc.
     - When a hospital is hit with ransomware, these files are encrypted (locked), so doctors cannot access them
     - This means they don't know how to treat their patients safely
   - Inoperable Medical Devices
     - Many modern medical devices rely on computers, so they can be hacked: MRI machines, CT scanners, blood storage refrigerators, IV pumps, ventilators, heart monitors, pacemakers
     - If these devices stop working, it can lead to misdiagnosis or failure to treat critically ill patients

2. **Financial & Operational Costs**
   - Approx. $4 Billion Lost in Recovery and Services
     - Hospitals had to pay ransom demands, buy new equipment, and spend months restoring data
     - Lost revenue: while systems were down, hospitals couldn't bill patients or insurance companies
     - Hiring IT experts for recovery costs millions
   - Massive Delays in Patient Treatment
     - Even after a cyberattack is stopped, it can take weeks to restore all systems
     - Doctors are forced to use paper records, slowing down treatments
     - Hospital staff must manually check everything, increasing error risk
   - Data Restoration Took Weeks
     - If a hospital doesn't have backups, it may lose all patient records permanently
     - Even with backups, it takes time to restore every system

3. **Long-Term Consequences**
   - Increased Investment in Cybersecurity Awareness & IT Infrastructure
     - After WannaCry, hospitals had to spend millions updating security systems
     - Stronger firewalls, better backups, and cybersecurity training became priorities
       - Hospitals already have tight budgets
       - Investing in cybersecurity means less money for patient care
       - Many hospitals are still vulnerable to this day
   - New Government Regulations for Healthcare Cybersecurity Compliance
     - Governments have started passing laws to improve hospital cybersecurity
     - Example: U.S. CISA now requires hospitals to meet certain security standards
     - Hospitals that don't comply face penalties
   - More Ransomware Attacks on Hospitals
     - Hospitals continue to be attacked by newer ransomware:
       - Ryuk (2018) - targeted hospitals in the U.S., demanding millions in Bitcoin
       - Conti (2020-2022) - forced hospitals to shut down, delaying cancer treatments and surgeries
     - Attacks keep happening because hackers know hospitals will pay ransoms when lives are at risk
     - New malware is constantly evolving, and it's a never-ending arms race between hackers and cybersecurity teams

Slide 11: How to Prevent Another WannaCry

Keep Software Up to Date (Turn on Automatic Updates)

- Software updates fix security weaknesses that hackers can exploit
- Microsoft released a security patch for EternalBlue in March 2017, two months before the WannaCry attack
- Many hospitals never installed the update, leaving them vulnerable (sometimes in fear that updating could break their existing systems)

Use Strong and Unique Passwords

- Many cyberattacks start because people use easy-to-guess passwords
- Hackers use brute-force attacks, where they try millions of password combinations per second to break into accounts

Enable Two-Factor Authentication (2FA)

- Adds an extra layer of security beyond a password
- How does 2FA work?
  - You enter your password, and the system asks for a second factor
    - One-time code, fingerprint scan, security key, etc
- Even if hacker gets your password, they cannot log in without the second factor

Don't Click on Suspicious Links (Avoid Phishing Attacks)

- Phishing is a trick used by hackers to steal passwords and personal information by pretending to be someone trustworthy
- How Phishing Works:
  - You receive an email that looks real (Microsoft Support, Your Bank, etc)
  - The email asks you to click a link and log in
  - The link takes you to a fake website that looks real
  - When you enter your username and password, the hacker steals it

Slide 12: Video

Slide 13-14: Hardening Cybersecurity

Zero Trust Security Model

- Traditional cybersecurity assumes that if you're inside a network, you can be trusted. In the Zero Trust Model, no one is trusted by default
- How Does Zero Trust Work?
  - Every request is verified every time
  - Only necessary access is given to users
  - Constant monitoring makes sure there is no unauthorized access
- Multi-Factor Authentication (MFA), Least Privilege Access, Micro-Segmentation

- If a hacker breaks into one computer, cannot move across the network
- Essential for remote work and cloud security

Network Segmentation

- Separate Networks for Different Devices
  - Medical devices (MRI machines, ventilators) are on their own network
  - Office computers and email systems are separate
  - Guests and visitors use a separate Wi-Fi network
- Firewall Rules Between Segments
  - Even if two systems need to communicate, a firewall controls what data is allowed to pass
  - Example: A hospital billing system can talk to the appointment system but not to MRI machines.
- Monitoring Traffic Between Segments
  - If suspicious activity is detected in one segment, it can be locked down before spreading

Continuous Monitoring & Threat Detection

- Security software constantly scans for threats (unusual logins, malware activity)
- AI and machine learning detect suspicious behavior
- Alerts notify IT teams immediately when a cyberattack is detected
- Cyberattacks happen fast, and without monitoring, hackers can steal data or install ransomware before anyone notices

Regular Security Audits & Compliance

- Like a cybersecurity check-up, where it examines how well an organization is protected
- During an audit, experts search for weaknesses and suggest fixes before hackers find them
- Types of Security Audits:
  - Penetration Testing
  - Compliance Audits
  - Vulnerability Scans
- Audits are important because they catch security weaknesses early before hackers exploit them, ensure compliance with government regulations, and improve cyber resilience by regularly testing defenses

Slide 15: IoT Everywhere is at Risk

What is IoT?

- The Internet of Things (IoT) refers to smart devices that connect to the internet and can communicate with each other (Alexa, Tesla, pacemakers, traffic lights, etc)
- Vulnerable because most IoT devices do not have strong security

Smart Cities

- Use connected technology to improve the services they provide, such as transportation, electricity, and public safety
- Attackers could change traffic lights, shut down electricity, and disable police radios - all causing risk-situations

Smart Homes

- Many homes today use internet-connected devices that control lights, security systems, and even refrigerators
- Hackers can hijack smart locks, smart cameras, and thermostats to cause harm or damage property

Smart Vehicles

- Modern cars have Wi-Fi, Bluetooth, GPS, and even autopilot systems, and if they are hacked, the consequences can be deadly
- Hackers can remotely control brakes or accelerators, disable safety features, and even track the real-time location of car

Slide 16: Moving Forward

What Needs to Happen Next to Improve Cybersecurity

- Invest in Stronger Security Practices
  - Hospitals, businesses, and even individual users must proactively improve cybersecurity instead of waiting for an attack to happen.
  - Organizations must increase cybersecurity budgets instead of treating it as an afterthought.
  - Cybersecurity teams should have full-time staff monitoring threats 24/7.
- Raise Awareness & Educate People
  - Most cyberattacks start with human error - people clicking on phishing emails, using weak passwords, or ignoring security warnings
  - Make cybersecurity training mandatory for healthcare workers, employees, and the general public
  - Run awareness campaigns to educate older adults and non-tech users about online scams
- Advocate for Better Regulations & Policies
  - Many companies cut corners on security because cybersecurity improvements cost money. Governments must enforce regulations to ensure organizations follow security best practices
  - Governments must pass stricter cybersecurity laws for hospitals, banks, and IoT devices
  - Enforce compliance through fines and regular security audits