July Health Care Provider Cybersecurity Call

John Petrozzelli
Director MassCyberCenter
Agenda

• Ransomware Attack Blamed for Hospital Failure in Illinois
• EU USB attack from China
• HCA Data Breach
• Ransomware Defense
• Post Attack
Ransomware Attack in Illinois

• “You’re dead in the water,” Linda Burt, vice president of quality and community service at St. Margaret’s Health, told NBC. “We were down a minimum of 14 weeks. And then you’re trying to recover. Nothing went out. No claims. Nothing got entered. So it took months and months and months.”

https://www.fiercehealthcare.com/health-tech/rural-illinois-hospital-says-shutdown-partially-caused-2021-ransomware-attack
Around the world with Malware

Hackers are mailing out USB drives infected with ransomware

News  By Sead Fadilpašić published 10 January 2022

USB drives often come with a fake thank you note
HCA Healthcare says data breach may affect 11 million patients in 20 states

Medical giant HCA Healthcare, which operates 180 hospitals in the U.S. and Britain, says the personal data of about 11 million patients in 20 states may have been stolen in a data breach

By FRANK BAJAK AP Technology Writer
July 11, 2023, 12:39 PM
Ransomware Defense

People

• Cybersecurity training and SLAM phishing (Sender, Links, Attachments, Message)
• Implement Least Privilege, Role Based Access Control, and Limit Admin accounts to those who really need them
• Utilize password managers and complex passwords or passphrases. Don’t re-use or share passwords. Don’t share accounts
• Create, maintain, and regularly exercise a basic cyber incident response plan (IRP) and associated communications plan that includes response and notification procedures
Ransomware Defense (Con’t)

Process

• Regularly patch and update software and operating systems

• Maintain offline, encrypted backups of critical data

• Employ logical or physical means of network segmentation

• Retain and adequately secure logs from network devices, local hosts, and cloud services

• Conduct regular vulnerability scanning to identify and address vulnerabilities

• Implement monitoring and enable security settings in association with cloud environments

• Implement third party vendor risk management policies
Ransomware Defense (Con’t)

Technology

- Disable ports and protocols that are not being used for business purposes. Limit remote desktop where possible
- Secure domain controllers (DCs) and ensure that all virtual machines and associated IT infrastructure, including network and storage components, are updated and hardened
- Restrict usage of PowerShell to specific users on a case-by-case basis by using Group Policy or software
- Establish a security baseline of normal network traffic and tune network appliances to detect anomalous behavior.
Post Attack Steps

• IT Depends - be flexible and build your incident response plan to adapt to different problems

• Determine and immediately isolate impacted systems

• Consider powering down devices and/or firewalls (be careful: do this only if your responders are not remote)

• Triage impacted systems for restoration and recovery

• Examine existing organizational detection or prevention systems
  • (e.g., antivirus, Intrusion Prevention System) and logs

• Contact your cyber insurance company when appropriate

Source: CISA Stop Ransomware
START HERE: Watch Introduction Video to Learn More About the “Basics” of Cybersecurity

Click on the following hexagon graphics to advance to each individual goal for achieving a minimum baseline of cybersecurity.

- Trained and Cyber-Secure Employees
- Improved Threat Sharing
- Cyber Incident Response Planning
- Secure Technology Environment and Best Practices

https://masscybercenter.org/cyber-resilient-massachusetts/minimum-baseline-cybersecurity-municipalities

Questions?