ENPM686 Project Report

By :

Akshay Manoj (UID: 116921169)

Contents

Scenario Introduction

In light of the new COVID-19 crisis many hospitals are tirelessly working to help stabilize the state of the world right now. Amidst this global pandemic , many healthcare facilities have been targeted by cyber criminals, specifically ransomware based attacks and DDoS attacks are used to bring down the IT infrastructure behind these facilities. One such important hospital has employed us to secure its IT infrastructure from these threats and any other security flaws that may exist in their system.

Infrastructure Assumptions:

- All internal tablets and smart healthcare devices run a simple Linux GUI that directly opens the Hospital's interface on start up.
- Nurse stations, front desk and inhouse pharmacy has machines that run on Windows.
- The Hospital IT Admin uses Active directory for Identity management.
- Smart medical equipment runs on a different network from the Nurse station machines and the front desk.
- The hospital also provides an internet connected WIFI network that can be used by the patients and their visitors when admitted to the hospital.
- This WIFI network should be isolated from all the other intranet networks used by the medical staff.
- The virology research labs store their data in an on premise datastore that is backed up to an air gapped server to ensure that the data is not tampered.
- Two buildings with security cam covering the entrance, exit and the lobby
- Openly accessible patient waiting area
- Pharmacy storeroom and Research labs with key card secured doors
- Nurse station, Front desk, Doctor's Tab all are password protected. No password reset policy
- All endpoint systems are running the latest version of a premium antivirus software.

Previous compromise:

The hospital has suffered from a cyberattack 2 months ago that has caused a lot of damage to the IT infrastructure of the facility as well as lost a lot of money and data. The attack was a DDoS attack targeting the intranet devices of the hospital, which was followed by a malware that leaked employee information[6].

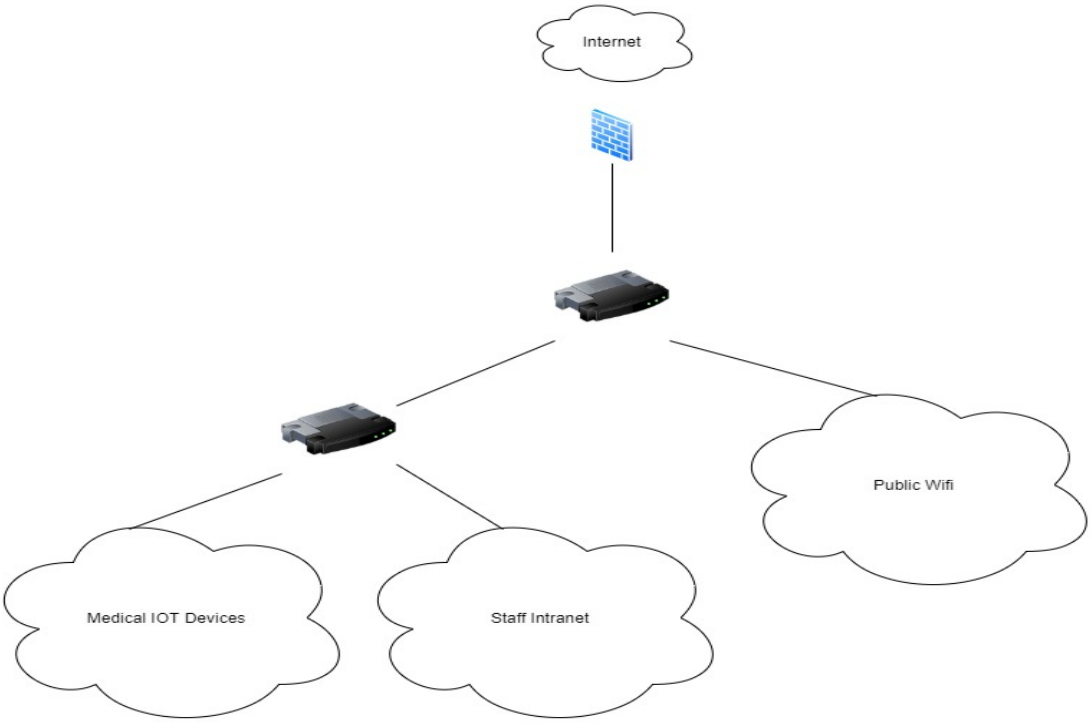
The attack on the network caused some medical support machines to lose function for a few hours. The malware managed to leak 3500 employee records, including their credentials, phone numbers and personal data. The failure of the medical devices has also affected the reputation of the hospital in the patient's eyes.

The lost assets has cost a lot of money to the hospital , $12000 for hiring a disaster recovery team to restore lost data, $50000 for restoring functionality of the medical support systems back to normal, $20000 for rebranding the hospital image to regain the patient's trust.

Current state of security:

In response to the attack that occurred previously, the hospital IT staff made some changes and put in place the following measures to ensure better security:-

- Password protected access to Doctor Tablet
- VPN Required to access internal hospital records
- Network level Firewall preventing incoming connections which are not through the VPN
- Public WIFI is separated from the Hospital Intranet



Assets Identified for protection

An analysis of the hospital's IT framework revealed some important assets that would need to be considered for an effective security plan. The assets are identified by their accessibility, the value of data they hold or the criticality of their function for the hospital to remain operational. The assets and a brief description about them are given below:

- Public WIFI:
  An easily accessible point of entry for an attacker in the hospital. This network is separated from the internal network used by the hospital equipment and staff but can be used to target patients and their personal devices. Priority for protection: Medium

- Private Intranet for devices:
  Internal network used by the hospital equipment and staff to communicate and work with each other. If attackers gain access to this they can sabotage the medical equipment, steal medical data and employee data. Priority for protection: High

- Research lab servers (Highly Critical):
  Servers that store important information about the COVID-19 Cure research program. The data in these servers are highly critical and need to be protected from any breach. Priority of Protection: High

- Patient file servers (Highly Critical):
  Servers that store medical history and patient treatment records that need to be kept private between the doctor and patient. Attackers and cyber criminals can use medical records to blackmail and extort money out of patients. Priority of Protection: High

- Employee record servers:
  Servers that store employee information including their personal details and financial information. Priority of Protection : Medium

- Doctor/Nurse handheld devices:
  Tablets and PDAs used by doctors and nurses to fetch patient medical history, write prescription and view and create treatment plans.

- Telemedicine sessions:
  New service provided during the pandemic where a patient doesn't have to be in the same room as the doctor, OPD setups allow for patients to come into a room and talk to the doctor through a video call.

- Pharmacy inventory tracking software:
  Software used to keep track of inventory information, allows the doctors to know if a particular drug is low in count and thus facilitates the doctor to write prescription with alternative medicines. Also tells the pharmaceutical department to order more of which drug.

- Internal application used for accessing medical records:
  Application running on the medical staff's end devices and tablets.

Objectives of Proposal:

After analysis of the assets mentioned previously and the requirements stated by the hospital executives. Here we have a list of objectives that the security proposal will need to achieve in order to be deemed complete

- Secure the Highly critical assets as identified earlier
- Ensure privacy of patients and doctors from unwanted observers
- Protect critical systems from attacks
- Prevent tampering of records and prescriptions
- Prevent leak of research data or patient data.
- Security measures should not obstruct the workflow
- Security changes should not inconvenience the user unless necessary

Flaws in current security:

Since the last cyber attack the hospital executives made some changes to their security and added a few more things to their security infrastructure. Analysis of the current state of security at the hospital reveals the following flaws that can be found. Below is a list that identifies and explains these flaws and their impacts

- Lack of a hierarchical structure for regulating access privileges:
  There is no hierarchical structure in the access levels. A user with a doctor or nurse key card could enter any of the key card rooms. A user with internal credentials can access any internal document. This means that if a user is able to get even one credential from a medical personnel , they can access all the internal resources of the hospital

- Snooping attacks on the intranet:
  If an attacker manages to inject himself into the network the communication between the medical IOT devices are not encrypted and anybody can sniff and snoop the messages from the network. This means that attacker might be able to send fake notifications to doctors and send fake messages to the medical devices.

- Critical servers are always connected to the intranet:
  Servers containing highly critical data like the Covid 19 research servers and the patient records system need to be made more secure , as mentioned previously anyone with internal credentials can access them easily and there is no logging of who accessed what record

- Physical access to nurse workstations needs to be restricted:
  Nurse workstations are connected to the same intranet as the patient file servers and thus if an outsider is able to access these they might be able to gain unauthorized access to medical records and confidential data.

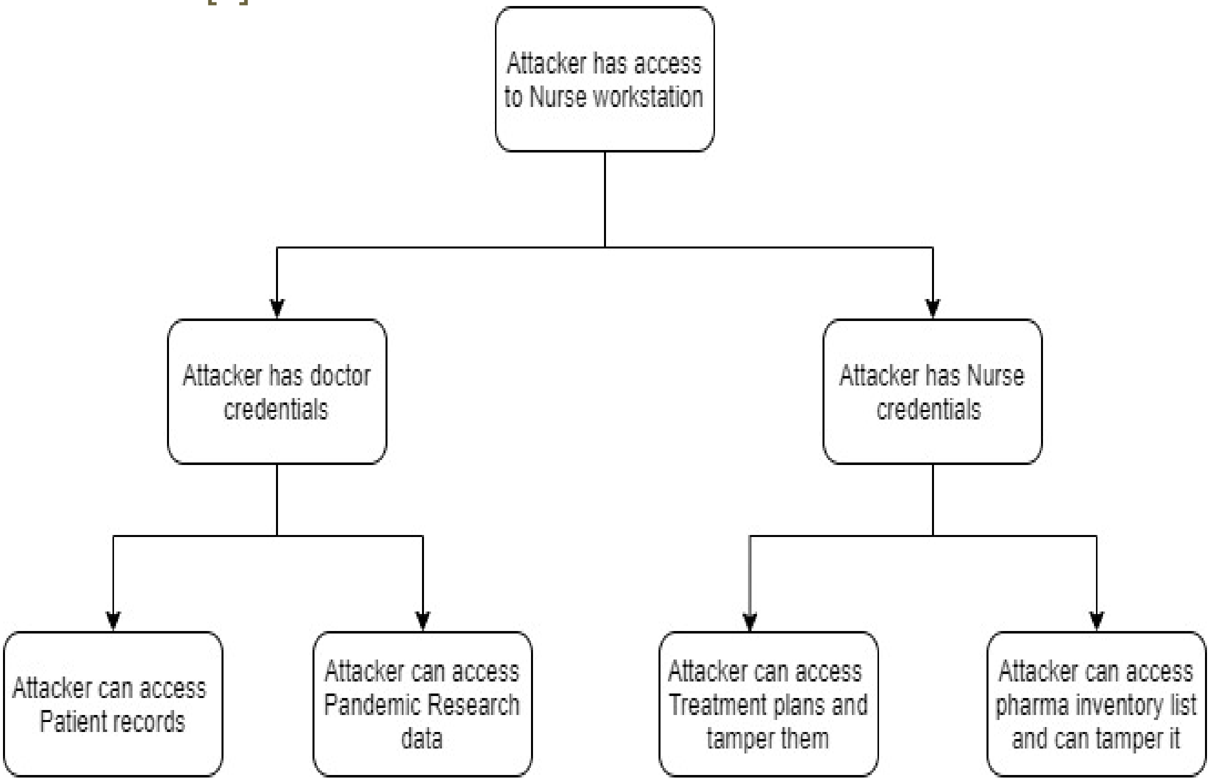
- No backup systems for critical file servers:
  Critical data storage systems seem to be running without any disaster recovery plan. There are no backups for the servers and no cloud stores.

Threat Modelling

STRIDE[2]:

- Spoofing Identity:
    - Unauthorized access to doctor-patient information using stolen credentials of doctor
    - Using an unattended doctor tablet to access medical records
- Tampering Data:
    - Modifying patient medical records or hospital inventory data.
    - Tampering with prescriptions and doses to cause harm to a patient
- Repudiation:
    - Prescriptions modified by a third party without any accountability
- Information Disclosure:
    - Stealing the patient's medical records and releasing theme to the public
- Denial of Service:
    - Disrupt the function or communication between the medical IOT devices
- Elevation of Privilege:
    - Accessing the doctor's patient list from a non-medical privilege account

Attack tree [3]:


Attacker has access to Nurse workstation
Attacker has doctor credentials
Attacker has Nurse credentials
Attacker can access Patient records
Attacker can access Pandemic Research data
Attacker can access Treatment plans and tamper them
Attacker can access pharma inventory list and can tamper it

Security Proposal Plan:

After reviewing the user requirements and identifying the assets and existing security flaw the following security plan has been proposed for maximizing the security of the hospital IT infrastructure. The security proposal plan components are as follows:

- Implement new Password Policy:
  New updated password policy to force the users of the system to change their credentials every few months. This would solve the existing threat of an attacker cracking a credential, because by the time the attacker cracks one credential every user would have updated their credentials to different ones.
  Password policy will also be updated to have a minimum of 10 characters with a mix of numbers and symbols along with alphabets

- Setup Access Hierarchy:
  New access levels need to be implemented within the medical staff. Splitting the workforce into doctors, nurses and research technicians each having different set of privileges.
  This would prevent someone with nurse privilege from accessing the resources of a lab technician. This would also reduce the priority of having to secure Nurse stations as the credentials logged in on these stations would not have unrestricted access to the hospital resources.
  Example of permissions per role:

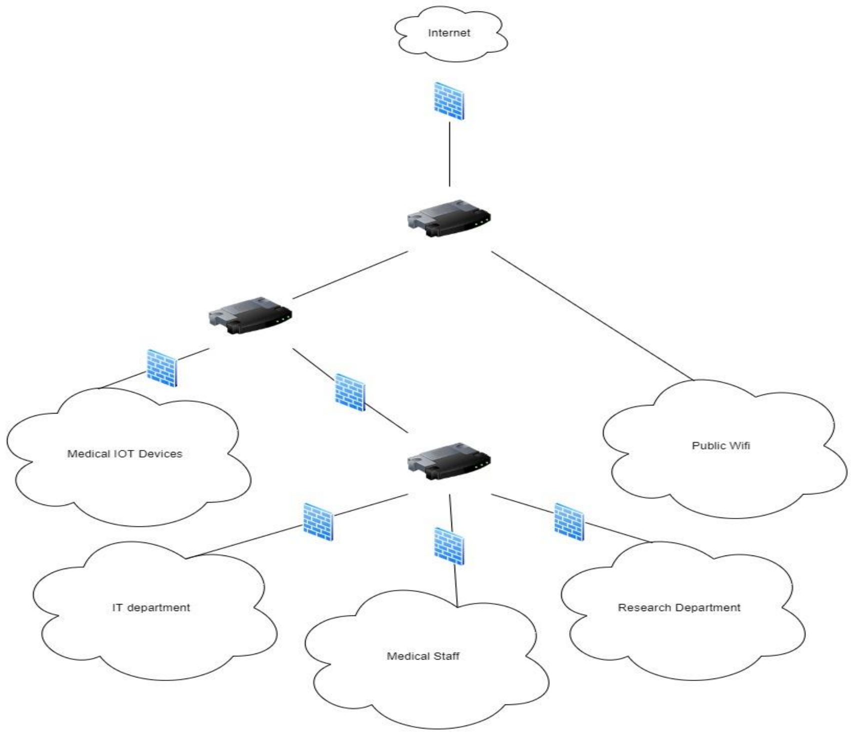
	Treatment plan	Drug inventory data	Covid-19 Research data	Patient medical record
Nurse	r	r	none	r
Doctor	r, w	r	r	r, w
Researcher	none	none	r, w	none

- Implement BLP:
  A new security access model like BLP can ensure that the data leak from the system is at a minimum. Workers at a lower level should not be able to access critical assets and the data from them cannot be written to a lower level.

- Reconfigure the ID Cards:
  In accordance to the new access privileges mentioned above we will need to implement similar restrictions in the physical access of those resources

- Implement the access privilege rules into the internal application:
  Internal application used by doctors and nurses to access the patient records need to be updated with the same access privilege rules as mentioned in the previous step so that there is no backdoor method for any person without the correct access rights to access any resource.

- Redesign Network Infrastructure :
  A new network layout to separate unrelated departments from each other. This will further allow the critical servers to be isolated from other parts of the internal network. For e.g. separate the Research labs internal network from the other hospital intranet, therefore gives a layer of protection to the research lab resources.
  Each separate domain of the intranet needs to be secured with a network layer firewalls that will log communications between the domains and also blocks communication from certain domains who do not need to access the resource. For e.g. Front desk executive machine should not be requesting data from the research lab servers.



- Update the security policy for personal devices:
  A new rule needs to be appended to the security policy for people entering the high-tech area of the hospital. Bluetooth enabled devices need to be turned off to ensure that IOT devices within the hospital are not compromised or snooped on. Like most IOT devices the IOT medical devices use Bluetooth low energy (BLE) to communicate with each other to aid in medical diagnosis, certain tools like hcitool and gattool can snoop the Bluetooth network to scan for BLE devices.

- Setup and configure cloud storage facility:
  A newly setup cloud storage solution for the hospital. Using a cloud storage to backup important critical data would allow us to tackle the lack of disaster recovery in the current implementation of servers in the hospital. A proper setup and configuration should be done, preferably also train the IT team at the hospital in configuring and spinning up new instances of the cloud. Often times it happens that the configuration of cloud storage facilities leads to them being the most vulnerable part of the IT framework of a company.

- Schedule a regular upload data to secure cloud facilities:
  Cloud storage solutions setup in the previous step in the plan need to be followed up with a regular scheduled upload of data to them, similar to a backup. This needs to be done frequently enough so as to not suffer majorly if the critical data servers go down at any point but at the same time should not be a live copy as that may mean corrupted data might reach the cloud storage and corrupt the backup data too.

- Add authentication to the Doctor’s Tablet:
  By adding some form of authentication either biometric (Fingerprint) or voice matching, we can ensure that not just anyone can pick up a stray tablet in the hospital and start spoofing the doctor to whom the tablet belonged.
- Setup a blockchain-like system for medical document updating:
  In order to ensure that medical records , prescriptions , treatment plans of a patient are not tampered with, setup a block chain like system to ensure that the medical documents always have a log of who updated and what changes were made. This would add accountability to any modifications made to a document and would discourage care less updating of medical documents.

Alternative approaches

Some other steps that could be taken as an additional or alternate way of ensuring security of the system are mentioned below. These were not added to the proposed plan either due to conflicts with one or more of the objectives or due to budget restrictions.

- Turn off public WIFI within hospital. (can inconvenience the patient)
- Implement a separate network for non-medical and medical staff (Cost inefficient, goals can be achieved using role based or hierarchical access control structure)
- Secure the smart patient monitoring devices (Cost inefficient, IOT devices will require to be changed)
- Backup the critical data into air-gapped servers (Could be effective but need to invest into monitoring physical access to air-gapped systems)

Cost estimate

As per the budget stated by the client, the cost breakdown of implementing the proposed plan is given below:-

- Implementing new hierarchy structure, BLP model and retraining staff to understand what this entails: $30K
- Creating new password policy: $100
- Separating out network layout:
    - Invest in new Industrial routers: $20K
    - Setup new IDS/Firewall at each router: $24K
- Setup and maintain Cloud storage[5]:
    - Setup: $50K , Monthly charge: $40 (recurring)
- Setup blockchain system of maintaining accountability of medical records update: variable ($30k -$50k per month for a blockchain engineer)[1]

References

1. https://azati.ai/how-much-does-it-cost-to-blockchain/
2. https://en.wikipedia.org/wiki/STRIDE_(security)
3. https://en.wikipedia.org/wiki/Attack_tree
4. https://archer-soft.com/blog/what-smart-hospital-and-how-build-your-own-solution
5. https://wire19.com/best-cloud-storage-providers-comparison/
6. https://www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/