Draft 1

Security analysis of large scale computer systems

Introduction

For the last decade, attacks targeting hospitals has increased steadily. This is why, I decided to chose, as subject of this case-study, a state-run hospital network computer infrastructure to study. This case-study is not based on an existing infrastructure and come from the imagination of the author.

1 Phase 0

First of all, it is necessary to define the purpose of the system, the main technical components and what is considered inside and outside of the scope of this study.

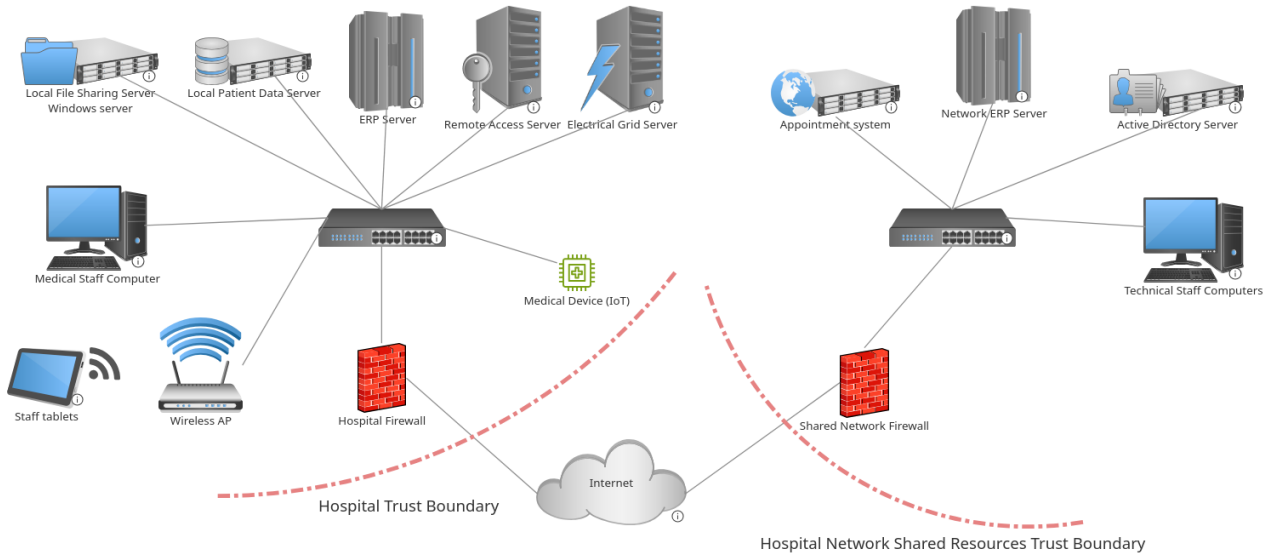

Figure 1: Diagram of the hospital network infrastructure

The Figure 1 represents the studied infrastructure of the hospital network. The resources shared among all hospitals and one hospital network is depicted on the figure. The latter is the same exact copy for every hospitals of the studied network.

1.1 Component description

For the hospital internal infrastructure, there are the following components:

- Hospital Firewall: bridges between the hospital local area network and internet;
- Local file sharing system: enables medical staff to store and exchange files;
- Local patient data server: stores internal medical data of the patients (medical background, stays at the hospital, prescriptions, ...);
- ERP Server: manages the hospital resources (supplies management, in which room is which patient, available beds, ...);
- Remote access server: enables technical staff to access remotely the local area network of the hospital;

- Electrical grid server: manages and optimises the allocation of electricity accross hospital as well as backup generator;
- Medical staff computer: enables medical staff to access local area network of the hospital;
- Staff tablets: enables medical staff to access local area network of the hospital through WiFi;
- Wireless AP: enables staff tablets to connect to the hospital local area network;
- Medical devices (IoT): optionnally connected medical devices (MRI, scanners, patients monitoring, ...);

And the shared resources infrastructure is made of the following components:

- Shared network firewall: bridges between the shared resources internal network and internet;
- Appointment system: more widely public website of the hospital network that enables the patient to book appointment with doctors and access their prescriptions;
- Network ERP system: manages the network resources between hospital (distributing supplies, managing staff allotment and salaries, ...);
- Active directory server: LDAP server using microsoft active directory to manage accounts and permissions for staff;
- Technical staff computer: enables technical staff to access shared resources infrastructure and vpn servers of different hospitals;

2 Phase 1

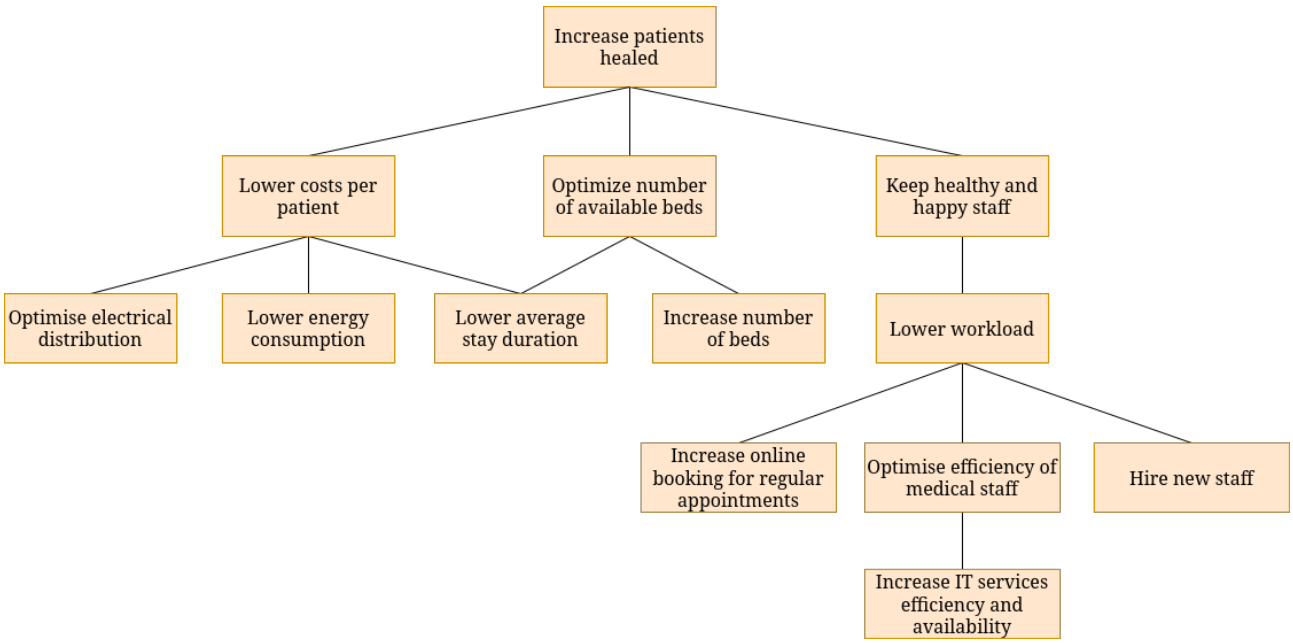

Figure 2: Diagram depicting the business goal of the hospital network

Goals are ordered by importance from top to bottom. A link between two goals indicates that the lower goal serves as a means of achieving the higher goal.

3 Phase 2

4 Phase 3