Queens Medical Centre

2022

Cyber Security

Report

Cyber Security Report for ASMIS

Contents

1 Introduction

Queens Medical Centre is a community clinic that acts as the first point of contact for any unwell residents in the catchment region. The clinic has professionals in a variety of medical fields. A consultation meeting with a specialist, on the other hand, requires an appointment, which can be made by calling the receptionist. However, the clinic has been experiencing a high number of calls, making it difficult for residents to get timely care. In addition, the management of Queens Medical Centre must plan forward to be ready to adapt to the community's increasing population. The clinic's management has opted to purchase a web-based Appointment and Schedule Management Information System (ASMIS) to address this issue. Prospective patients will be able to make appointments online due to this. The system will gather essential information from the patient to determine which specialist is most suited to handle a given situation, considering the specialist's availability and workload.

The clinic's administration was concerned about the recent spike in cybercrime and the government's patient data protection policy. The clinic's IT department has been charged with setting up a secure ASMIS system. This report covers the potential cyber threats and how to mitigate them.

2 Benefits of ASMIS

- Always available: Patients can make appointments 24/7
- Quick and easy: Patients can easily select the date, department and speciality they want, and only specialists with available appointments will be shown.
- Appointments are directly booked: Tedious tasks of syncing appointments to the specialist's diary can be reduced.
- Improve customer journey: Scheduling online appointments reduces patients' waiting time. Also, we can reduce the inconvenience for patients to step out of work or sit on hold for scheduling an appointment.
- Timely care: Residents and patients can receive the necessary care they require as they no longer need to wait to make appointments.
- Reduces admin time: There is no need to manually enter appointments, which gives more time for the receptionist to focus on other tasks.

3 ASMIS UML Diagram

Figure 1 shows the use case diagram of the ASMIS. This is used to model the behaviour of ASMIS and help capture the requirements of the system. We can see that there would be different types of users of the ASMIS and how they would interact with it.

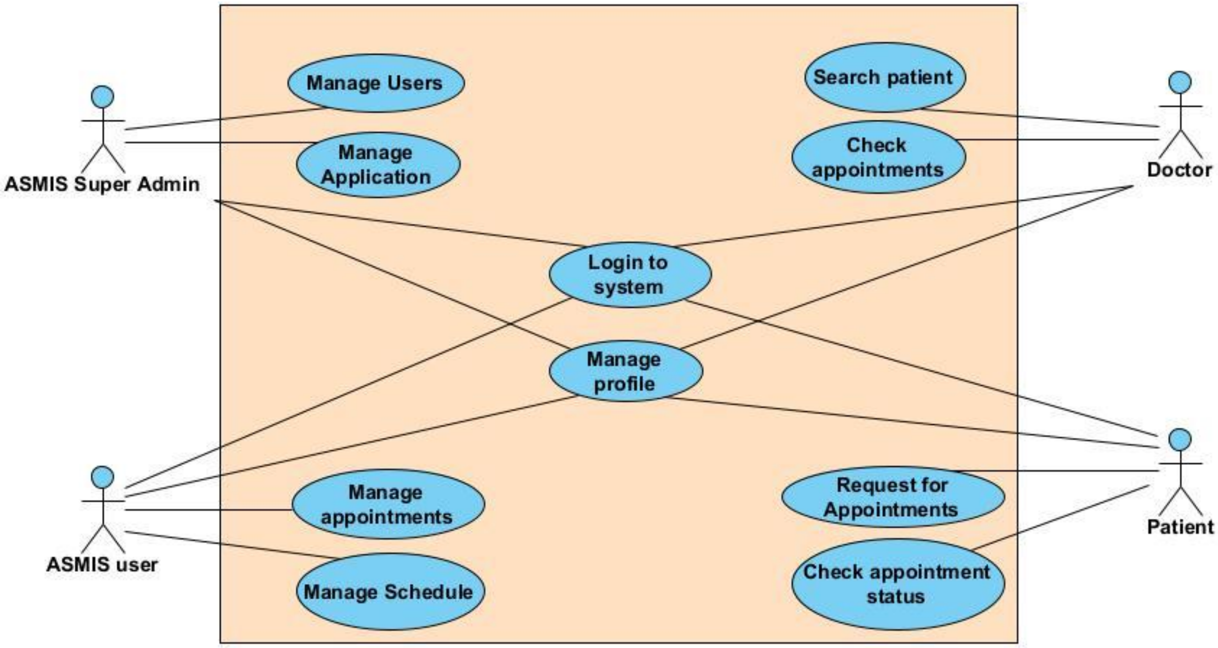

Figure 1: ASMIS Use case diagram

Figure 2 shows the sequence UML diagram, which captures the patient's journey while booking an appointment using the ASMIS.

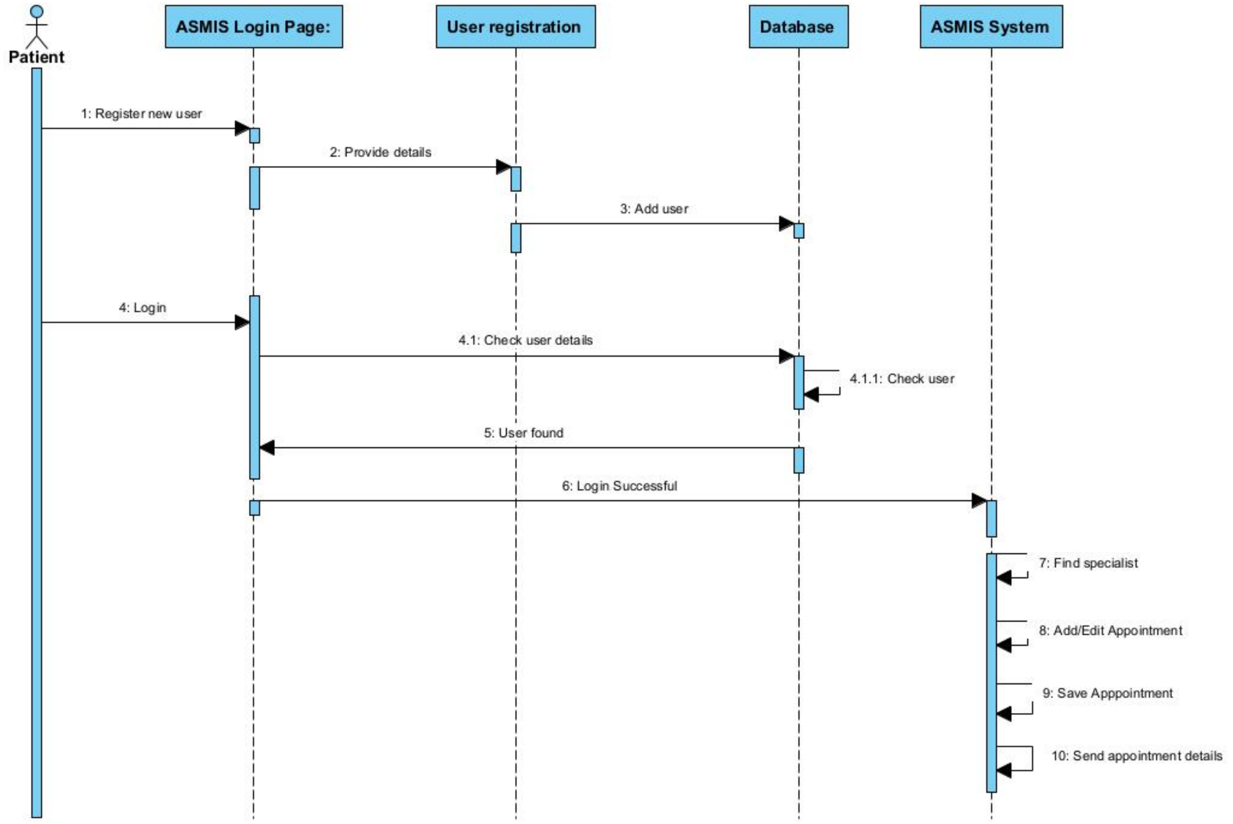

Figure 2: ASMIS Sequence diagram

4 Threat Modelling

Threat modelling aids security analysts in identifying, classifying and prioritising threats, which is the overall goal of a cyber security program. An efficient threat intelligence assists the security defence and security operations teams in safeguarding IT assets against threats and vulnerabilities.

STRIDE

For this report, the STRIDE threat modelling approach was adopted. Loren Kohnfelder and Praerit Garg developed this in the late 1990s. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. It is as described below:

	Threat	Violation	Methodology
S	Spoofing	Authentication	Impersonating something or someone known and trusted
T	Tampering	Integrity	Modifying data at rest or in motion
R	Repudiation	Non-Repudiation	Claiming not being responsible for an action
I	Information Disclosure	Confidentiality	Disclosure of information to someone not authorised
D	Denial of Service	Availability	Denying access to resources required to provide service
E	Elevation of Privilege	Authorisation	Allowing access to someone without proper authorisation

Table 1: STRIDE threat modelling methodology

The STRIDE threat model can detect threats and vulnerabilities during the development of an application or system. The first phase takes a proactive approach to identifying possible threats. To model the application, a Data Flow Diagram (DFD) should be utilized, and each item should be evaluated. Modeling can be done for the entire system or just specific features. The cornerstone for detecting threats is the system's design. The subsequent steps involve identifying and addressing gaps in the system's implementation. One of the significant benefits of STRIDE is that it can be performed by Security experts or application designers, developers, and testers. Other benefits include:

- **Threat modelling reduces attack surface**: The capability to identify, analyze, and retain a list of vulnerabilities enables security professionals in adopting the appropriate actions to mitigate them or getting the resources needed to remediate them. Risks can be recorded and monitored over time to assess progress against them.
- **Prioritization of mitigation efforts**: Enterprises must prioritise their limited resources when addressing cyber risks. Threat modelling assists organisations in quantifying risks and vulnerabilities, ensuring that those that require the most attention and help do so in a deliberate manner to reduce their attack surface.
- **Improvement of security posture**: Threat modelling is a method for systematically capturing every aspect of a system or software. In the end, we are documenting the critical features of every technical asset that our organisation cares about, how we will protect it, the countermeasures that are available, and what the cyber security team is trying to protect it from. As the business evolves and becomes more connected, the number of potential threats uncovered might

trend downward as threat modelling becomes a more regular part of the development and governance processes.

5 ASMIS Threat Model

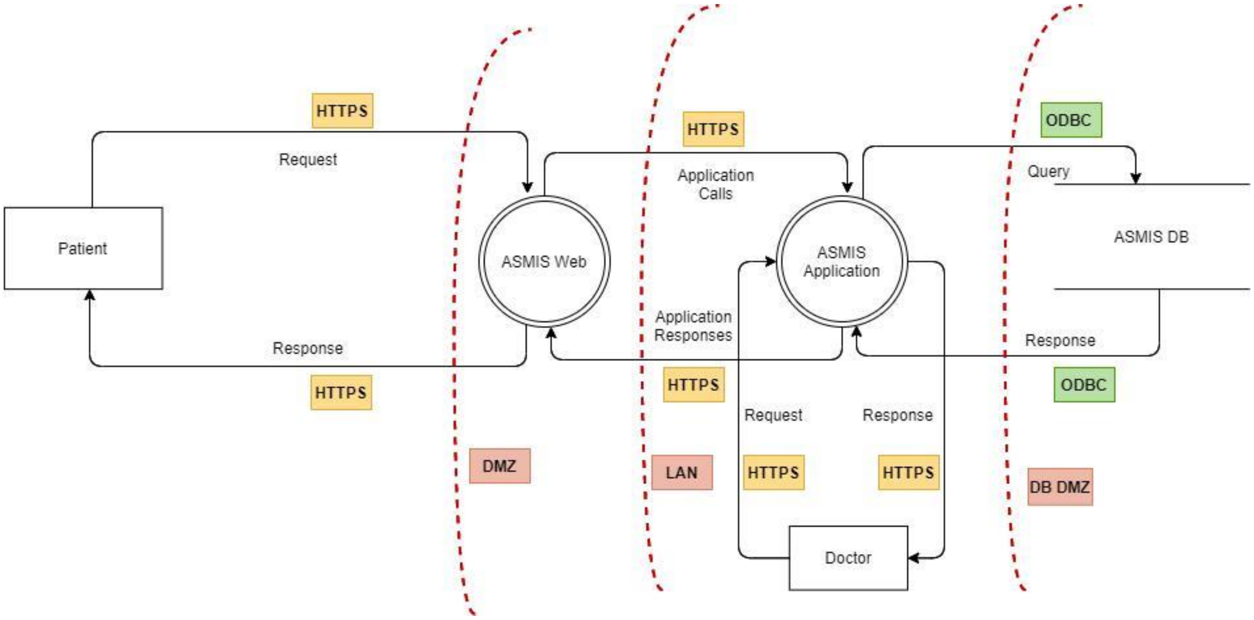

Figure 3: STRIDE Threat Model for ASMIS

Figure 3 shows the Data Flow diagram of ASMIS. As we can see from the chart, there are three trust boundaries: DMZ, LAN, and DB DMZ. Trust boundaries show where the components of the system change trust levels and offer different levels of privilege. The diagram also shows the various parts of the ASMIS and their interactions.

6 Cyber threats to the ASMIS

Now that we have charted the various components and their interactions, we can now enumerate the different threats using the STRIDE methodology as discussed above. The below table shows the threats identified as a quick reference guide:

DFD Elements	S	T	R	I	D	E
Patient to ASMIS web	✓		✓	✓	✓	
ASMIS web to application		✓		✓	✓	
Doctor to ASMIS application	✓	✓	✓	✓		✓
ASMIS application to ASMIS DB		✓		✓	✓	✓

Table 2: ASMIS threats

From table 2, we can enumerate the following threats:

6.1 Privacy exposure due to data loss

The threat modeling exercise has identified information disclosure as a significant threat. A data leak that results in the disclosure of confidential personal data might have catastrophic consequences. Any information that can be used to directly or indirectly identify an individual is considered to be confidential or sensitive in nature and needs to be protected. This includes name, email address, IP addresses, images, and biometric or genetic data. A data breach would result in legal action as well as damage to one's reputation. Organizations are legally bound under GDPR to provide due care and due diligence to secure personal data in accordance with data protection regulations. If their data is compromised, whether purposefully or unintentionally, individuals may file a lawsuit to seek compensation. This would also result in a reputational damage. According to surveys, a third of customers in the healthcare industries will cease doing business organisations that has suffered a data breach. Furthermore, 85% will inform others about their ordeal, and 33.5 percent will vent their frustrations on social media.

6.2 Ransomware

In 2021, ransomware was a hot topic in cybersecurity. A ransomware attack occurs when a threat actor acquires access to an organisation’s information systems (perhaps via a phishing email or infected USB) and then demands payment ("ransom") to re-enable vital systems or keep sensitive material from being released. Healthcare organisations are especially vulnerable to ransomware attacks because of the essential nature of their services—lives could be at risk if critical systems are unavailable during an attack.

6.3 Phishing

An email phishing attack is perhaps the most popular and well-known cyber threat. The prominence of this form of assault stems from its relative ease of deployment, ability to target multiple victims at once, and risk-to-reward ratio. In a phishing attack, a threat actor poses as someone they are not, such as a trusted individual or an employee of a well-known company. They want the recipient to click on a bad link, email them sensitive information, or even transfer money.

6.4 Web application attacks

The Healthcare industry is again the target for web application attacks because of COVID-19 related activity. Imperva Research Labs observed a 51 per cent surge in web application attacks against healthcare targets after the first vials of COVID-19 vaccines were distributed in December. This data represents a 10% year-over-year increase, highlighting the increased vulnerability of web apps for healthcare institutions, many of which are still unable to keep up with the demands of the ongoing global pandemic.

6.5 Denial of Service Attack

During a denial-of-service (DoS) attack a malicious actor disrupts the normal operation of a computer or other device to make it unavailable to its intended users. There are two kinds of DoS attacks. A flood attack work by flooding the network with an incredible number of packets and a buffer overflow attack overloads a targeted machine with requests until normal requests cannot be handled.

7 Mitigations

7.1 Multifactor Authentication (MFA)

MFA keeps us secure by adding a layer of security to stop bad actors when a password or authentication method is compromised. This can be established by having the patient enter a unique One Time Password (OTP) sent to their mobiles or downloading an app (like Google or Microsoft authenticator) to generate the OTP for them while logging in. We could also geofence the login to certain country blocks to reduce the attack surface.

7.2 Network segregation

Application-aware Next-Generation Firewalls (NGFW) can be used to segregate the network into different zones, as shown in figure 3. One significant advantage of NGFWs is that it provides visibility. When a user visits a malicious website, it gives us insights into potential outbreaks. This also helps to reduce the attack surface when dealing with phishing.

7.3 Web Application firewalls (WAF)

WAF protects online apps by screening, monitoring, and blocking potentially harmful web traffic, as well as prevent unauthorised data from leaving the app. WAF is governed by policies, which are a set of rules. These policies attempt to protect against application vulnerabilities by blocking out dangerous communications. A WAF's usefulness comes from the speed and ease with which policy changes can be implemented, allowing for faster responses to various attack vectors. WAF acts as an intermediary between the patient and ASMIS, analysing all communication before reaching the system or user. It can protect against the OWASP top 10 vulnerabilities which include:

- Injection attacks
- Broken Authentication
- Sensitive data exposure
- XML External Entities (XXE)
- Broken Access control
- Security misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization

7.4 Endpoint Detection and Response

Endpoints will be constantly monitored by EDR to detect and respond to threats such as malware and ransomware. EDR can record activities and events on endpoints and across all workloads, giving security staff the visibility, they need to discover vulnerabilities. EDR provides visibility into what is happening on endpoints in real-time and in the past. EDR will also interact with threat intelligence to quickly detect harmful threats, techniques, and procedures (TTPs).

7.5 Security Operations Center (SOC)

Reducing cybersecurity risk requires continuous monitoring of the infrastructure and data. SOC will aid businesses to detect, prevent, and respond to cyber threats and incidents. One major component of SOC is a robust Security Information and Event Management (SIEM) tool. It will collect logs and events from all systems, bring them into a single platform, and perform correlation. It will generate an alert and define a threat level based on rules. SOC analysts will go through these alerts and take appropriate action.

This could lead to alert fatigue as analysts deal with thousands of alerts per day. Alert handling should be powered through machine learning and AI to reduce the load on SOC analysts as it will improve the validation process and allow analysts to prioritise alerts.

Implementing SOAR (Security Orchestration Automation and Response) solution will significantly reduce the response time for analysts and reduce the attack damage.

8 Conclusion

Threat modelling is an important activity for finding and evaluating threats and vulnerabilities. There are many different methods of threat modelling but the aim of all is to find the most relevant threats facing an organisation and the mitigations for it. It is a continuous activity that is a major part of a successful security program.

References:

Commusoft. (n.d.). 7 Benefits of Using an Online Appointment System. [online] Available at: https://www.commusoft.co.uk/online-appointment-system-benefits/ [Accessed 16 Jan. 2022].

www.supersaas.com. (n.d.). Advantages of Online Scheduling. [online] Available at: https://www.supersaas.com/info/advantages [Accessed 16 Jan. 2022].

Strawbridge, G. (2020). 5 Damaging Consequences of a Data Breach. [online] MetaCompliance. Available at: https://www.metacompliance.com/blog/5-damaging-consequences-of-a-data-breach/ [Accessed 16 Jan. 2022].

Recorded Future. (2021). The Biggest Cybersecurity Threats Facing Healthcare Organizations—and How to Protect Yourself. [online] Available at: https://www.recordedfuture.com/biggest-cybersecurity-threats-facing-healthcare-organizations/ [Accessed 16 Jan. 2022].

Vijayan, J. (2021). 5 biggest healthcare security threats for 2021. [online] CSO Online. Available at: https://www.csoonline.com/article/3262187/biggest-healthcare-security-threats.html?upd=1642312982685 [Accessed 16 Jan. 2022].

Blog. (2021). Web Application Attacks on Healthcare Spike 51% As COVID-19 Vaccines are Introduced | Imperva. [online] Available at: https://www.imperva.com/blog/web-application-attacks-on-healthcare-spike-51-as-covid-19-vaccines-are-introduced/ [Accessed 16 Jan. 2022].

crowdstrike.com. (n.d.). What are Denial-of-Services (DoS) Attacks? | CrowdStrike. [online] Available at: https://www.crowdstrike.com/cybersecurity-101/denial-of-service-dos-attacks/ [Accessed 22 Jan. 2022].

EC-Council. (n.d.). Threat Modeling | Importance of Threat Modeling. [online] Available at: https://www.eccouncil.org/threat-modeling/ [Accessed 22 Jan. 2022].

Donovan, F. (2021). What is STRIDE and How Does It Anticipate Cyberattacks? [online] Security Intelligence. Available at: https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/ [Accessed 22 Jan. 2022].

Infosec Resources. (n.d.). 6 benefits of cyber threat modeling. [online] Available at: https://resources.infosecinstitute.com/topic/6-benefits-of-cyber-threat-modeling/ [Accessed 22 Jan. 2022].

www.pingidentity.com. (n.d.). 8 Benefits of Multi-Factor Authentication (MFA). [online] Available at: https://www.pingidentity.com/en/company/blog/posts/2021/eight-benefits-mfa.html#:~:text=Multi%2Dfactor%20authentication%20keeps%20data. [Accessed 28 Jan. 2022].

F5.com. (2019). What is a Web Application Firewall (WAF)? | Glossary | F5. [online] Available at: https://www.f5.com/services/resources/glossary/web-application-firewall. [Accessed 28 Jan. 2022].

crowdstrike.com. (n.d.). EDR Security | What is Endpoint Detection and Response? [online] Available at: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ [Accessed 28 Jan. 2022].

Busse, G. (2020). Next Gen SOC: what is the future for Security Operations Centres? [online] News from Westcon-Comstor. Available at: https://news.westconcomstor.com/next-gen-soc-what-is-the-future-for-security-operations-centres/ [Accessed 28 Jan. 2022].

What is a Denial-of-Service (DoS) Attack? | Cloudflare UK. (n.d.). Cloudflare. [online] Available at: https://www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/[Accessed 28 Jan. 2022].