In the world today, if we look at technology and how it has evolved, pressure is mounting on businesses to move away from the old way of doing things like manual filing systems and working on outdated computer systems to keeping data stored in the building in a basement where the company is located.

Companies that are considering adopting this new technology which can be referred to as the digital age (David Thomas, 2019) must plan for new challenges that will be presented to them. Challenges can include security of data when transitioning to a cloud solution like Microsoft Azure (Lars Klint, 2021) or to a datacenter and the costs involved. One of the biggest challenges they will have to look at is Cybersecurity and how to identify and mitigate threats.

Existing staff will need to be trained and new staff members will need to be employed so that they can assist in ensuring systems are secure from cyber threats. Let’s look at example of a company needing to move to an online system in the health sector.

If you need a doctor, dentist or specialist, you will need to phone your local clinic or medical practice to make a booking. The problem with this method is that if the phone lines are down to one of these facilities or the phone is constantly busy, it will take time to get through to them and as a result, the facility can start losing business because they cannot keep up with the number of patients calling in and patients will move on and call another practice.

A solution that can be adopted by the clinics is to implement an online booking system, also known as “web-based appointment and scheduling management information system (ASMIS)” (Anon, 2021) that can assist with patients booking a doctor as an example online without the need to call the practice. While this solution does offer relief to receptionists attending to calls at the practices, it does have some disadvantages.

One of the major advantages of the online booking system is that a patient can access the system using any device that has an internet connection such as a phone, tablet, computer etc. without the need to call the clinic or practice. If a patient does prefer to call in, the receptionist can look at the calendar to provide a quicker booking to patient as all the doctors bookings will be available immediately.

Some of the disadvantages of an online booking system is if the clinic or practice provider hosting the solution is experiencing internet issues, the booking system will be unavailable, and this will result in high calls to the practice. Another potential problem is if the booking system does not update the calendar feature and patients think they can book a doctor or specialist because of the availability show, will result in multiple bookings for a doctor and cause disruption at the clinic.

The main disadvantage related to an online booking system is the cybercrime and the theft of patient and doctor information. In countries such as the United States, there is a federal law called “Health Insurance Portability and Accountability Act of 1996 (HIPAA)” (Anon, 2018) and in the UK it is called the “Data protection act” (Anon, 2018) and these are in place to ensure that data cannot be disclosed without the patient’s approval.

To add to the disadvantages listed above, if the system chosen uses a software database known to attack, the security team will need to ensure that the software the clinic will make use of, is an easy-to-use system but secure enough when storing patient data. The security team will provide a modelling technique listing the potential cyber threats for that system and how these can be mitigated and used to identify any potential threat in the foreseeable future.

The threat modelling technique we will be discussing is called STRIDE (Fred Donovan, 2021). This is broken down into the following items, each letter deals with a category as shown in the table below:

|  |  |
| --- | --- |
| Modelling Technique definition | Category |
| S | Spoofing |
| T | Tampering |
| R | Repudiation |
| I | Information Disclosure |
| D | Denial of Service |
| E | Elevation of Privilege |

Let’s briefly expand on each of the categories listed above. The modelling technique table below explains each category and how to mitigate a potential threat.

|  |  |  |
| --- | --- | --- |
| Category | Explanation | Mitigation |
| Spoofing | This is a common technique where an attacker impersonates someone, for example, posing as a doctor sending an email to a patient requesting sensitive information about the patient. | Users should make use strong passwords and have multi-factor enabled on all accounts. Password policies enforced by the security team will ensure this is achieved.  Tools such as SPF, DMARC and DKIM need to be implemented to detect spoofed accounts. These are DNS records created against the domain.  Protocols such as SSL or TLS should be implemented to ensure encrypted communication between systems. |
| Tampering | This technique is used tamper with data and affects the integrity of the data. Tampering can include modifying the data while in transit between systems. Integrity is part of the CIA triad. | Permissions need to be assigned to users. For example, a receptionist does not need access to secure patient data compared to a doctor. If an attacker gains access to the receptionist account, the damage can be limited to what the person has access to. |
| Repudiation | An example of this technique is if a doctor sends information about a patient to someone else like a 3rd party and then denies that anything was ever sent. | Auditing needs to be implemented on the email system as well as any system handling patient data so that it can show who accessed the data and when it was accessed. Email auditing will show when it was sent and to whom it was sent |
| Information Disclosure | This technique refers to data that has been leaked by means of providing information to an attacker or person that should not have access to the data.  Confidentiality is part of the CIA triad. | This is like tampering where you need to control who has access to what data. An example might be that doctor does not have access to the IT systems like the backend database but only to systems like the portal where they can see who the next patient is. |
| Denial of Service | This technique is used to disrupt service by an attacker flooding the system with information and causing it to stop responding. | Newer devices like routers, switches and firewalls have built in mechanisms to detect these kinds of attacks but they need to be enabled and configured correctly. |
| Elevation of Privilege | An example of this may be that an attacker pretends to be an IT admin and requests the details to the backend database server so they can perform maintenance on the server. | Role based access control is controlling who has access to what system and the level of access. The IT or Security director may be the only ones accessing the backend database to provide information to senior management and no IT admin should just have access to the system nor should medical staff. |

In the sections below, we provide UML diagrams for each section listed in the modelling technique STRIDE above.

UML Diagram 1

Treemap chart, square

Description automatically generated

UML Diagram 2

Diagram

Description automatically generated

Applications, databases, executive personnel, IT staff, IT equipment and end users need to be protected from external threats trying to access the local area network (LAN) and the wide area network (WAN). The WAN could link clinics together that are in different areas. An example of this is Houston Texas and Austin Texas.

The following Cyber Security technologies can be implemented to address the categories and problems listed in the table above.

|  |
| --- |
| Cyber Security Technology |
| Data Loss Prevention (DLP) |
| Antivirus |
| Intrusion Prevention System (IPS) |
| Firewalls |
| Security Incident and Event Management (SIEM) |
| Intrusion Detection System (IDS) |

We will discuss the pros and cons of each Cyber Security Technology below.

**Data Loss Prevention (DLP)**

In our example we are dealing with a clinic using an ASMIS system. Data loss can happen due to the clinics system or end user machines being infected with malware and data being stolen by attackers before they Ransomware the machines and the patient data being made available on the dark web. Sensitive data that resides on a database, should be isolated from the main network so if a breach happens it is isolated. The underlying systems should also be patched and be running supported operating systems. The downside of patching is that if it is not done consistently, then that system can be vulnerable to attacks (Debra Bruce, 2021)

**Antivirus (AV)**

Antivirus provides some basic protection to an end user. In an example of the receptionist at a clinic, if this person opens an email that has some malicious data in, the Antivirus should stop the attempt to infect the system and provide a warning. The weakness of just using AV is that is does not detect or block everything like some kinds of malware or ransomware used in Rootkits. Example by (Wen, H.J., Tarn, J.M, 1998)

**Intrusion Prevention System (IPS)**

An IPS can be implemented on the network as a network device (physical) or software device that monitors the network for malicious traffic and stops traffic. The main downside of an IPS solution is that a switch port can be overwhelmed and not handle all the traffic and result in packets being lost. Example by (Cesar Urrutia, Nick Ierace, Richard Basset, 2005)

**Firewalls**

A firewall protects the company from threats. Next generation firewalls (NGFW) can be implemented to ensure security on the LAN but also blocking malware. A web- application firewall (WAP) can be implemented so that the ASMIS is not exposed directly to the internet and work in conjunction with the NGFW. Example by (Zach Haenert, 2018)

**Security Incident and Event Management (SIEM)**

A SIEM solution provides collaboration with other systems and checks for malicious actors, traffic or anything in log files constantly and creates an alert for the security team if something is found. One drawback of a SIEM solution is the amount of data captured if the solution is not configured correctly and reading reports can be hard to understand. Example by (Dhanusha S, 2019)

**Intrusion Detection System (IDS)**

Intrusion detection system (IDS) is a tool that monitors an entire incoming network traffic and checks for anything malicious before raising an alarm. This is extremely useful because there is no human factor involved which could result in events not being detected. The weakness of an IDS solution that it does produce false positives however these alerts can be fine-tuned. Example by (Tom Dunigan, Greg Hinkel, 1999)

In conclusion, cyber threats cannot be handled by just one solution. A range of solutions is required to ensure that cyber threats can be detected, fixed if there was a breach and a solution put in place to mitigate the breach in future. Monitoring of systems is a key factor because if nothing is in place, it can take up to 228 days (reference) before a breach is detected. Healthcare providers that keep patient data must comply with government requirements in each country and to ensure that the CIA triad (Confidentiality, Integrity and availability) is met.

References

David Thomas. (2019) What is the digital age?. Available from: <https://www.ventivtech.com/blog/what-is-the-digital-age> [Accessed 23 September 2021].

Lars Klink. (2021) What is Azure? Microsoft’s cloud platform explained. Available from: <https://acloudguru.com/blog/engineering/what-is-microsoft-azure> [Accessed 23 September 2021].

Anon. (2021) Launching into Cyber Security August 2021. Available from: <https://www.my-course.co.uk/mod/assign/view.php?id=527421> [Accessed 23 September 2021].

Anon. (2018) Public Health Professionals Gateway. Available from: <https://www.cdc.gov/phlp/publications/topic/hipaa.html> [Accessed 23 September 2021].

Fred Donovan. (2021) What is STRIDE and How Does It Anticipate Cyberattacks?. Available from: <https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/> [Accessed 23 September 2021].

Debra Bruce. (2021) Use Cases of Data Loss Prevention. Available from: <https://www.knowledgenile.com/blogs/data-loss-prevention-use-cases/> [Accessed 23 September 2021].

Wen, H.J., Tarn, J.M. (1998) Internet security: a case study of firewall selection: *Information Management & Computer Security* 6(4): 178-184. DOI: <https://doi.org/10.1108/09685229810227658>

Cesar Urrutia., Nick Ierace., Richard Basset. (2005) Intrusion Prevention Systems. Available from: <https://ubiquity.acm.org/article.cfm?id=1071927> [Accessed 23 September 2021].

Zach Haenert. (2018) Raytheon Company (TechValidate). Available from: <https://www.forcepoint.com/resources/case-study/raytheon-company-techvalidate> [Accessed 23 September 2021].

Dhanusha, S. (2019) A Case Study on SIEM Implementation. Available from: <https://medium.com/vault-infosec/a-case-study-on-siem-implementation-58e39a1f56f4> [Accessed 23 September 2021].

Tom Dunigan., Greg Hinkel. (1999) *Intrusion Detection and Intrusion Prevention*

*on a Large Network: A Case Study*. Available from: <https://www.usenix.org/legacy/events/detection99/full_papers/dunigan/dunigan.pdf> [Accessed 23 September 2021].