Introduction: Description of the web appointment application

The purpose of this report is to examine the proposed web-based appointment and scheduling management information system (ASMIS), as well as to recognize both advantages and disadvantages of the ASMIS implementation, mainly from the cyber security point of view. Financial evaluation for the proposed product and alternatives' comparison is beyond this report's scope, and therefore, no further scrutiny will be made here on these topics.

ASMIS's primary target is to change the current way we book our patients' appointments and introduce a web-based application instead. Prospective patients will apply online for an appointment, choosing among the system's proposed dates and per the appropriate medical speciality. Further details regarding ASMIS implementation are discussed in a later part of this report.

Advantages

- The most apparent advantage expected from the web application is the minimization of the reception's workload, which nowadays seems to be quite increased, saving time for other significant tasks.
- Decrease the bottleneck of phone booking, allowing time for help desk tasks in case of patients who are not familiarized with technology (i.e., the elderly) or in case of error during the booking process.
- The administration workload will be reduced due to the decreased number of emails. The system will automate confirmation emails and communication between the medical centre and the patients. Internal communication and special cases are expected to be handled by the administration team.
- Remote access is an additional advantage for the reception team and the doctors alike. Authorized personnel could have access to the appointments' application regardless of working hours and physical presence.
- In the same fashion, 24/7 availability could be an added value for the patients. The appointment booking process will be available for patients not only during office hours, providing them with the convenience to arrange their appointment at any given moment.
- Traffic data reports would also help managers normalize the departments' workload and assess their efficiency.

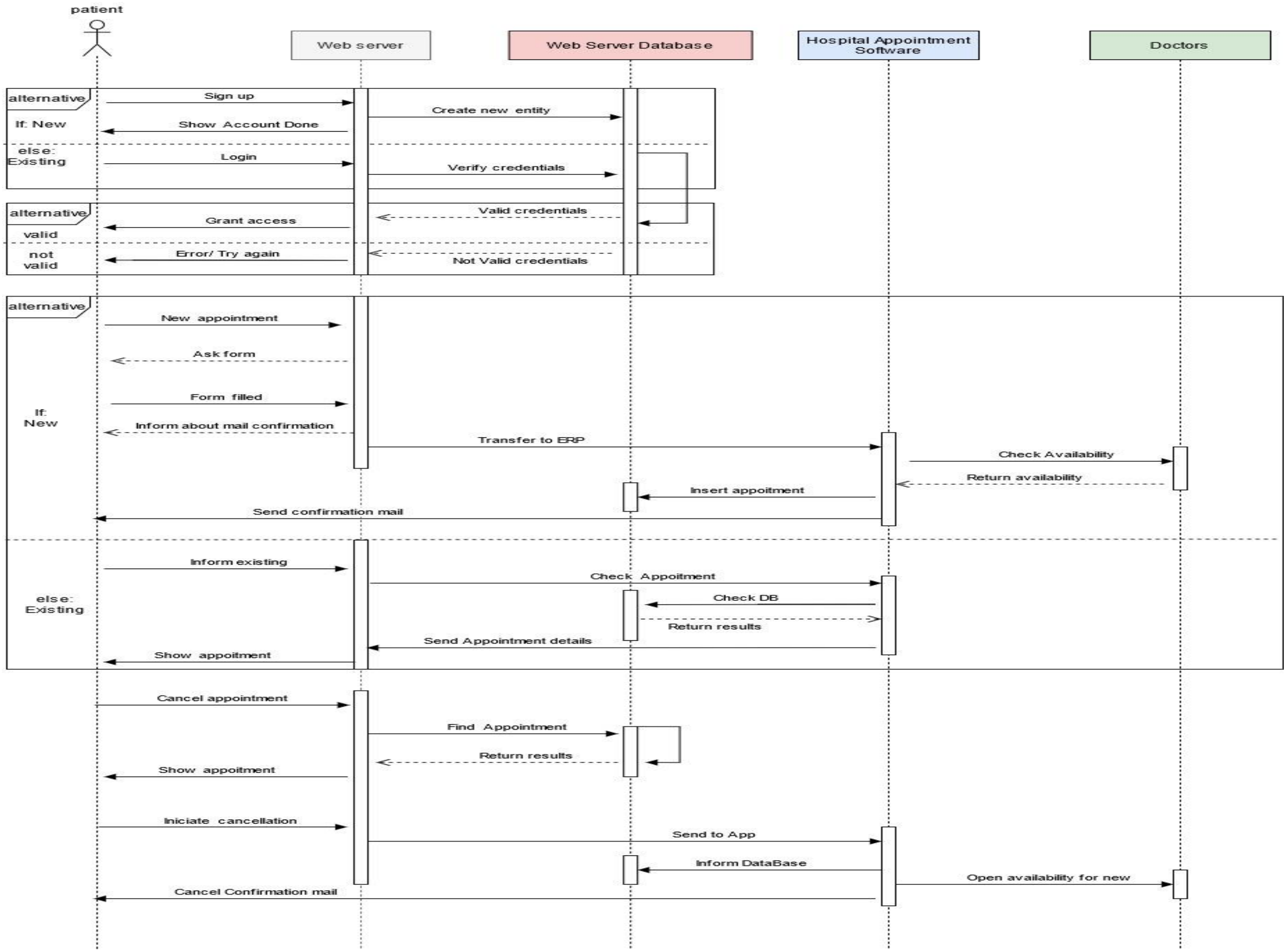
- Finally, a digital transformation and web presence are expected to upgrade the services' level and positively impact the clinic's image.

Disadvantages

- The application's digital nature could exclude people who do not have the necessary digital skills or perceive the traditional call process as more convenient.
- Extra costs in terms of extra equipment, services, and training should also be taken into consideration.
- This application's operation and maintenance require reliable internet access, a prerequisite for both the clinic and the patients.
- The vendor's level of services and efficiency impacts our productivity; therefore, a thorough evaluation and product analysis should be considered mandatory.
- Delays and difficulties could also be encountered during the first stages of the implementation, either due to the personnel's unwillingness to adapt to new conditions or some initial misconfigurations.
- Additional cyber security threats may arise. (The following part of this report will identify and propose measures to mitigate them.)

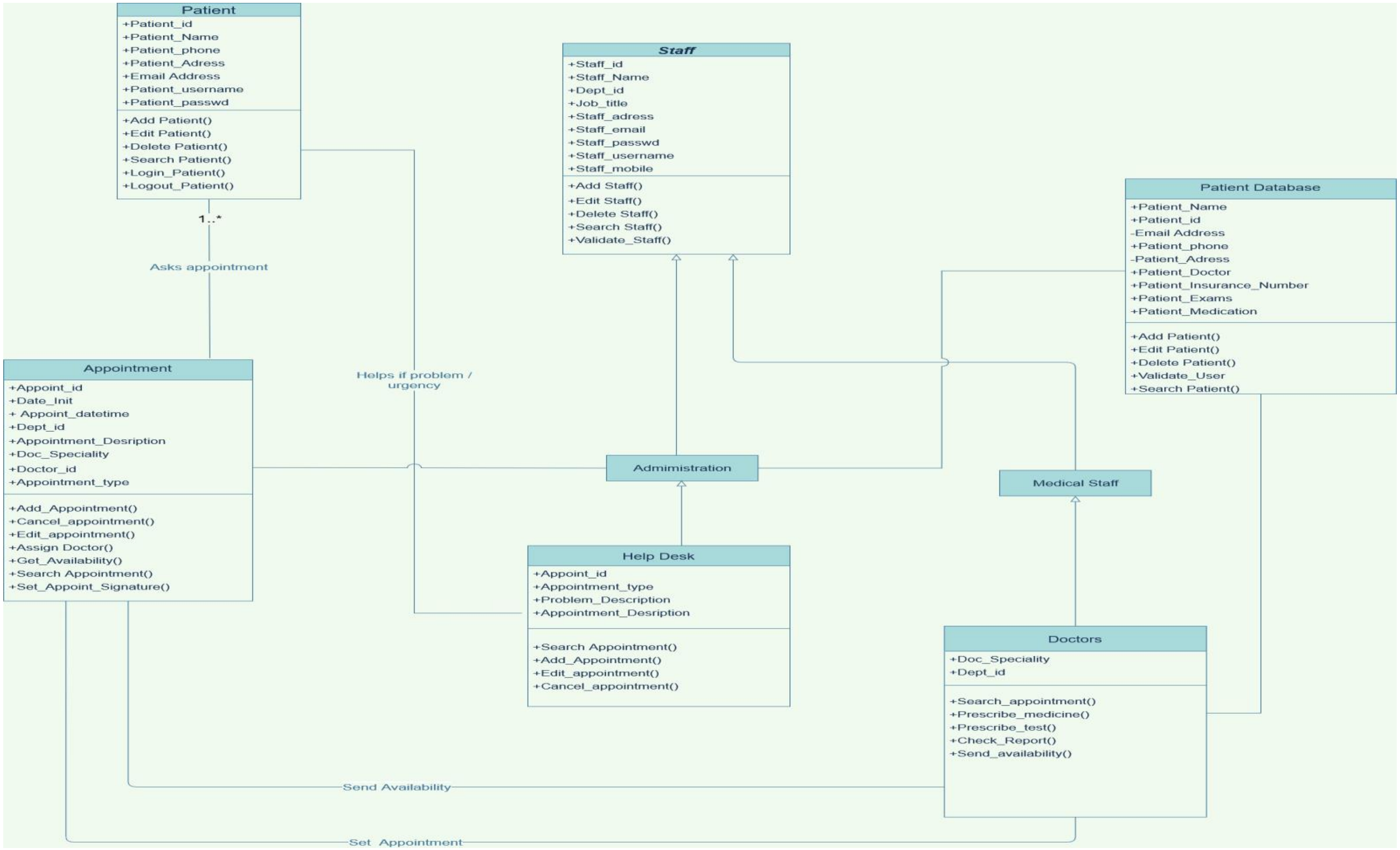
At this part of the report, some diagrams are presented in order to show the critical points of the ASMIS application and the interactions amongst the organization's parts.

Diagram 1 is a Sequence Diagram according to UML modelling (Booch et al., 2005), depicting the ASMIS procedure for three possible uses. In case of a new appointment, the prospect user logs in (or signs up) and requests a new appointment. The system replies, providing the user with a form to fill in the details of her/his case and the required medical speciality. When the form is submitted, the system informs the user that when the appointment is scheduled, he/she will be informed via email. In the meantime, the system is processing the submitted data, trying to match the appointment with the appropriate doctor based on availability. The application sets a new appointment, saves it, and forwards the appointment details via email to the patient. In case of cancellation or reminder, the user logs in and looks for his/her appointment details. The results return to the user, who can see the details or cancel. In the latter case, the request is transferred to the app, which updates and releases the slot while informing the doctors about the change.


patient
Web server
Web Server Database
Hospital Appointment Software
Doctors
alternative
If: New
Sign up
Create new entity
Show Account Done
else: Existing
Login
Verify credentials
alternative
Valid credentials
Grant access
valid
not valid
Error/ Try again
Not Valid credentials
alternative
New appointment
Ask form
Form filled
If: New
Inform about mail confirmation
Transfer to ERP
Check Availability
Return availability
Insert appoitment
Send confirmation mail
Inform existing
Check Appoitment
else: Existing
Check DB
Return results
Send Appointment details
Show appoitment
Cancel appointment
Find Appointment
Return results
Show appoitment
Iniciate cancellation
Send to App
Inform DataBase
Open availability for new
Cancel Confirmation mail

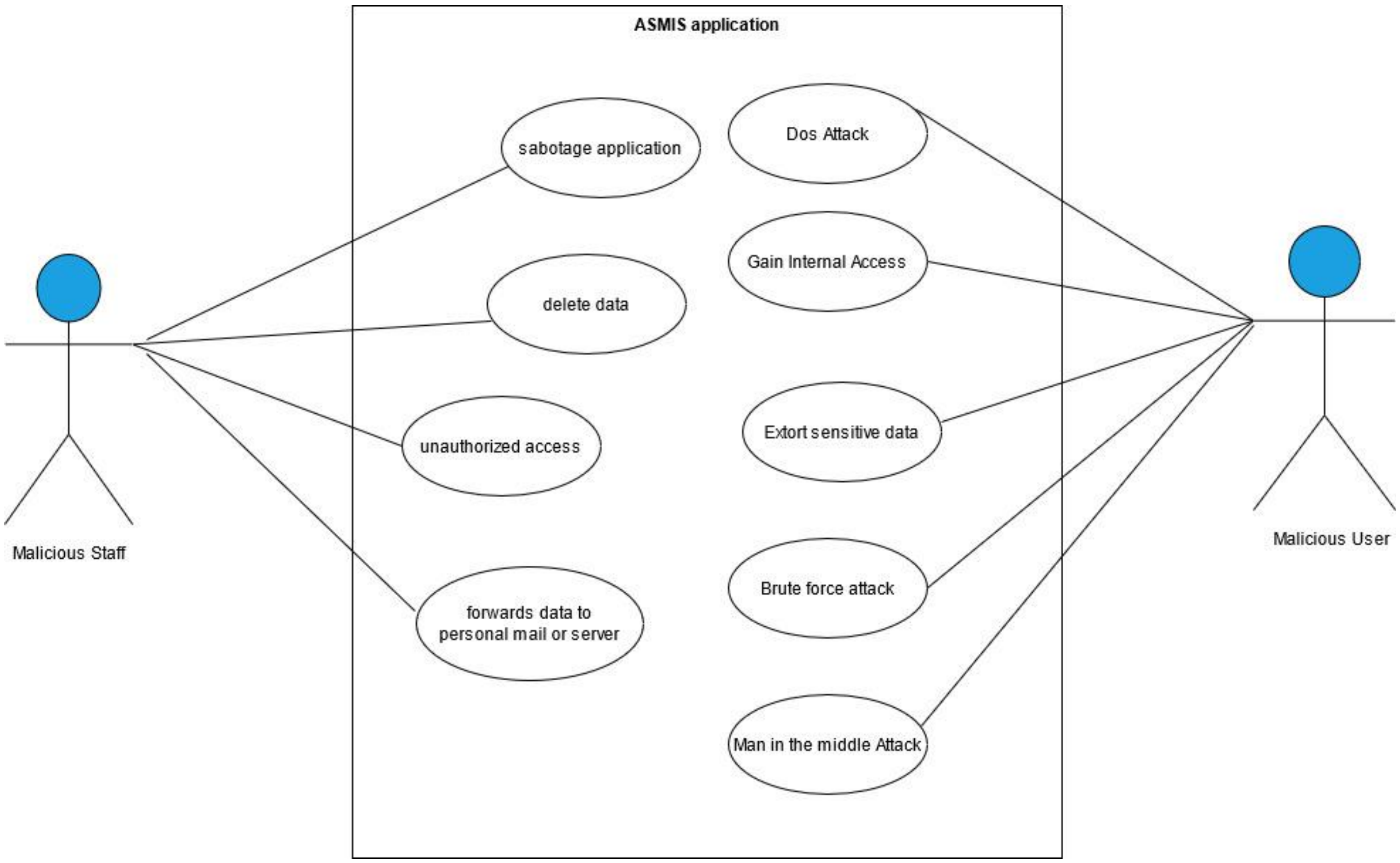
(Diagram 1)

Diagram 2 is a Class diagram (Ambler, 2003) that describes the relationships between different objects of the application and some basic operations that are performed. Essential information about staff, patients and appointments is exchanged between these parts during the system operations (i.e., passwords, patient's address)



(Diagram 2)

Diagram 3 is an abuse case diagram. It is an adaptation of the use case diagram (Booch et al., 2005) depicting some security threats presented by different actors.



(Diagram 3)

In order to identify some critical threats, STRIDE modelling is proposed. STRIDE was invented in 1999 by Loren Kohnfelder and Praerit Garg and adopted by Microsoft in 2002, and it is considered the most mature method to this day (Shevchenko et al., 2018). The acronym STRIDE stands for six threat types that violate one of the CIA triad (Confidentiality, Integrity, Availability) and some expansions (Non-repudiation, Authenticity, and Authorization). A brief category description follows:

Spoofing: an action of pretending to be someone who is not.

Tampering: a modification or sabotage which mainly aims to serve the attacker's purpose.

Repudiation: a claim that someone did not commit the act or was not responsible for it.

Information Disclosure: information exposed to someone who did not have authorized access.

Denial of Service: An action that targets system resources to disrupt them or stop the function completely.

Elevation of Privilege: upgrading user's access to resources without the appropriate authorization.

The following part of this report focuses on some critical threats identified by the previous UML diagrams and listed according to STRIDE categories. Security measures to mitigate them, along with some general security practices, will be proposed. The threats mentioned below are indicative, therefore the list should not be considered exhaustive.

Number	Threat	STRIDE Category	Potential Effect
1	SQL injection from malicious users	T, R, I, D, E	The attacker could extort sensitive data from the database or change/destroy the database
2	Attacker floods services with a significant number of HTTP requests	D	The system could be overloaded and become inoperable
3	Attacker gains access from web application error messages	I	Error information could help intruder gain access
4	Cross-Site Scripting (XSS) – Site manipulation leads the unsuspected user to a different site (the attacker’s one)	T	Attackers could tamper the site, lead patients to a similar web page, and ask patients for sensitive data (i.e., card number, bank account)
5	Attacker intercepts and replay authentication session	S, R	Unauthorized access
6	Brute Force / Dictionary attack to exploit admin credentials	E	Administration credentials could be revealed, providing access with admin privileges

General Security measures:

a) Network Segmentation:

Different clinic departments will have separate networks based on roles and functions, following different employee privilege policies. In this way, we minimize the attacker's surface by limiting the incident's effect on a specific network, avoiding the infection of the rest of the departments. The segmentation will also benefit the network monitoring process as well as the network's performance.

Although these may be true, efficient network segmentation could be a challenging assignment for the network engineers. Sometimes the wrong setup could result in a vulnerability or hamper the organization's tasks (Wagner et al., 2017).

b) Backups – Disaster plan:

Every-day backups are proposed regarding the clinic's Databases. Moreover, considering the increasing ransomware incidents and cyber-attacks, the organization should be prepared for these events. Keeping backups could help minimize the recovery time and the potential data loss due to such incidents. This strategy would also prove valuable in case of physical disasters. Choosing between a colocation Backup server or cloud service calls for further analysis. Synchronization speeds, availability, different cost ranges, and additional vulnerabilities are some factors that should be scrutinized (Hawkins et al., 2000).

c) Security mentality and frequent personnel training:

The human factor has to be taken into account, as it is considered the weakest link in cyber security. Even the best technologies and measures fail when the human factor is involved. Phishing emails and social engineering are known factors that cyber crooks use for their nefarious purposes. In many cases, the decoy is very sophisticated and could deceive even advanced users (Dhamija et al., 2006)

Consequently, frequent personnel training is a measure that has to be taken into consideration. A survey conducted at Columbia University (Bowen et al., 2011), regarding phishing emails that were sent to assess students' awareness and capacity to identify phishing emails, showed that the number of individuals who had failed in the first round decreased significantly in the following rounds. Specifically, a repetition of three rounds proved to be sufficient for almost all the students to succeed in the test.

Although staff training is expected to be a time demanding process and it will possibly encounter some unwillingness, nevertheless it could yield substantial benefits in terms of security and readiness.

Additional measures:

- Cryptography

Due to data sensitivity, no plain text should be stored, at rest or in transfer. All data stored in Databases should be encrypted following contemporary security standards. Cryptographic techniques and practices are essential for security, and due to the complexity of this field, solid mathematical understanding and experience are required (Pham, n.d.). Hence, well-known and approved solutions should be preferred, to refrain from mistakes and experiments. Similarly, the website should also use a secure connection protocol TLS (Transport Layer Security).

Despite the undeniable merit encryption provides, it should not be considered a panacea. Over time, many vulnerabilities can be exploited, either due to inefficient implementation or inherent characteristics (Satapathy et al., 2016).

- Two-factor authentication

A strong password policy combined with two-factor authentication should be mandatory for accessing the ASMIS platform both locally and remotely. This technology seems to increase for Health Industry(Gabriel et al., 2015). Two-factor authentication enhances the password security level and tends to become standard practice nowadays. Emails or text messages could be used as the second verification step. Face recognition or fingerprints are more privacy-invasive methods that sometimes proved less safe and prone to a fault, while they are more complex to apply. Additionally, although biometrics are unique and therefore upgrade the identification process, they sometimes give the impression of infallibility, which is far from reality (Pomputius, 2018).

- Next-Generation Firewall

Firewalls are the first line of network defence, and their technology has been around for many years, serving both end-users and businesses. They come in different forms (i.e., hardware, software) and types (i.e., packet-filtering, stateful packet inspection). The most current and updated form is the Next-Generation Firewalls that are nowadays considered a more sophisticated solution due to the additional functions embodied(Neupane et al., 2018). Unlike its predecessors, it is capable of deep packet inspection up to the application level. Intrusion and malware detection features are integrated, constructing a more efficient and holistic tool. More advanced rules and parameters can be set, even to the single-user level. Despite the advanced security level and the advantages of the NGFW, some shortcomings should also be considered. Performance issues due to the demanding resources, frequent false-positives and incompatibility issues are the most significant ones (Abdel-Aziz, 2021)

- Penetration testing from an external party

Penetration testing is a fundamental security practice for security assessment and reinforcement. A well designed and executed penetration test could provide essential feedback about potential vulnerabilities, preventing possible incidents. Unlike the vulnerability scans, which often form as an automated process using different fixed tools, penetration testing from an experienced professional is a more comprehensive approach. Infrastructure, processes, applications, and people are tested for weaknesses, using the same methods and techniques a cyber perpetrator could use. An additional advantage of external penetration testing is the unbiased and objective view of the outsider. Some already known or overlooked problems could be revealed that under different circumstances would not be mentioned (Conrad, 2012).

Even though external penetration testing is a valuable tool, there are some weaknesses. The quality of the service depends on the expert’s skills and the given duration of the test. Moreover, frequent tests are needed in order to remain up to date and, hence, it could be proved a pricey strategy.

Conclusion:

The proposed ASMIS application is expected to upgrade the service level and the efficiency of the organization. Daily routine and tasks will develop and therefore a significant commitment to change and training will be the keys to success. The transition to a digital environment raises additional risks, therefore we have to be prepared. The security measures noticed in this report are a valuable guide, serving as well some GDPR compliance purposes for the time being. In the long run, additional actions and methods may be applied. Cyber security is a fast-changing field and requires continuous research and update.

References

Abdel-Aziz, A. (2021) *SANS Institute Information Security Reading Room Intrusion Detection & Response-Leveraging Next Generation Firewall Technology*.

Ambler, S.W. (2003) *The Elements of UML™ Style*. Cambridge, UK: Cambridge University Press. Available from: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=125014&site=ehost-live. [Accessed 5 March 2021].

Anderson, R.J. (2008) *Security Engineering : A Guide to Building Dependable Distributed Systems*. Indianapolis, Wiley. Available from: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=343359&site=ehost-live. [Accessed 10 February 2021].

Booch, G., Rumbaugh, J. & Jacobson, I. (2005) *Unified Modeling Language User Guide, The (2nd Edition) (Addison-Wesley Object Technology Series)*. Addison-Wesley Professional.

Bowen, B.M., Devarajan, R. & Stolfo, S. (2011) Measuring the human factor of cyber security. *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, pp.230–235. Available from: https://doi.org/10.1109/THS.2011.6107876.

Conrad, J. (2012) Seeking help: The important role of ethical hackers. *Network Security*, 2012(8), pp.5–8. Available from: https://doi.org/10.1016/S1353-4858(12)70071-5.

Dhamija, R., Tygar, J.D. & Hearst, M. (2006) Why phishing works. *Conference on Human Factors in Computing Systems - Proceedings*, 1(November 2005), pp.581–590. Available from: https://doi.org/10.1145/1124772.1124861.

Gabriel, M., Charles, D., Henry, J. & Wilkins, T.L. (2015) State and National Trends of Two-Factor Authentication for Non-Federal Acute Care Hospitals, (32), pp.1–7. Available from: https://dashboard.healthit.gov/evaluations/data-briefs/hospital-two-factor-authentication.php.

Hawkins, S.M., Yen, D.C. & Chou, D.C. (2000) Disaster recovery planning: A strategy for data security. *Information Management and Computer Security*, 8(5), pp.222–229. Available from: https://doi.org/10.1108/09685220010353150.

Mansfield-Devine, S. (2018) Friendly fire: how penetration testing can reduce your risk. *Network Security*, 2018(6), pp.16–19. Available from: https://doi.org/10.1016/S1353-4858(18)30058-8.

Neupane, K., Haddad, R. & Chen, L. (2018) Next Generation Firewall for Network Security: A Survey. *SoutheastCon 2018*. pp.1–6. Available from: https://doi.org/10.1109/SECON.2018.8478973.

The OWASP Foundation (2020) OWASP Top Ten. Available from: https://owasp.org/www-project-top-ten/ [Accessed 20 March 2021].

Pham, V. (N.D) Implementing Cryptography: good theory vs. bad practice. Available from: https://owasp.org/www-pdf-archive/OwaspTalkMarch.pdf.

Pomputius, A.F. (2018) A Review of Two-Factor Authentication: Suggested Security Effort Moves to Mandatory. *Medical Reference Services Quarterly*, 37(4), pp.397–402. Available from: https://doi.org/10.1080/02763869.2018.1514912.

Satapathy, A.& Livingston, J. (2016) A Comprehensive Survey on SSL/ TLS and their Vulnerabilities. *International Journal of Computer Applications*, 153(5), pp.31–38. Available from: https://doi.org/10.5120/ijca2016912063.

Shevchenko, N., Chick, T.A., Riordan, P.O., Scanlon, T.P. & Woody, C. (2018) Threat Modeling : a Summary of Available Methods. *Research Report*, (July), p.26. Available from: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf.

Wagner, N., Sahin, C.S., Winterrose, M., Riordan, J., Pena, J., Hanson, D. & Streilein, W.W. (2017) Towards automated cyber decision support: A case study on network segmentation for security. *2016 IEEE Symposium Series on Computational Intelligence, SSCI 2016*, pp.1–10. Available from: https://doi.org/10.1109/SSCI.2016.7849908.