State Comptroller's Report – Cyber and Information Systems | May 2023

Ministry of Health

Cyber Audit at Medical Center A – Penetration Test on the Infrastructure and the Communication Network

Cyber Audit at Medical Center A – Penetration Test on the Infrastructure and the Communication Network

Background

Over the past decade, cyber-attacks on organizations and individuals worldwide have increased. In 2020, about 9.5 million attempted cyber-attacks were detected worldwide, the purpose of which was to disable computer systems and prevent the ability to use them[1]; 18 attempted attacks per minute were detected, on average; In the first half of 2020, at least 36 billion personal data items were stolen or leaked to the internet following cyber-attacks. Accordingly, cyber threats to the health system, including medical centers, have increased in recent years. Furthermore, the health sector was one of Israel's ten most attacked sectors in 2021[2].

Medical institutions use tens of thousands of medical devices for various medical operations. Among these devices are imaging devices such as magnetic resonance imaging devices (MRI), computed tomography (CT), X-ray, and ultrasound devices. The medical devices must be thoroughly and regularly available given the variety of medical operations performed, and especially given their necessity for life-saving procedures.

Cyber security (information security) in medical devices, including imaging devices, prevents an unauthorized party from making changes to the information stored in the medical devices; Unauthorized use or misuse of the medical information stored in the medical device, processed in it, or transferred from it to an external destination; As well as harm the operation of the medical device. One of the ways for an organization to prepare for cyber threats is to perform "resilience tests." These tests are designed to examine the organization's level of protection, locate security breaches and possible risks, and handle them accordingly. One of the resilient tests is a "penetration test" (PT) – a process in which a controlled and planned attack is carried out on the organization's computerized systems to find vulnerabilities.

In May 2022, the State Comptroller's Office performed a penetration test at a specific medical center (Medical Center A or the Medical Center). The recommendations for rectifying the deficiencies in this report are addressed to the Medical Center's management and the Ministry of Health, the regulator of the medical institutions, including in their information security, so that it examines the results of the penetration test, and implement the recommendations made as a result of it in all medical institutions.

1 DDOS – Denial of Service Attack Distributed attacks. The attacks and leaking of data were in various extensive fields.

2 The National Cyber Directorate, Year 2021 Summary.

Key Figures

9.5 million
cyber-attacks attempts worldwide to disable computer systems were detected in 2020

18 times a minute
cyber-attack attempts were detected, on average, in 2020 worldwide

36 billion
personal data items were stolen or leaked online following cyber-attacks in the first half of 2020 worldwide

1 of 10
the health sector was one of the ten most attacked sectors in Israel in 2021

over 100
the State Comptroller's Office scanned in the infrastructural penetration test over 100 servers and endpoints of the medical equipment of Medical Center A

10
out of 13 findings in the State Comptroller's Office penetration test were of a "high" severity level. Three were of "moderate" severity

NIS 10 million
the annual estimated cost to rectify the deficiencies raised in the penetration test

about NIS 36 million
the Hillel Yaffe Medical Center restoration cost after the cyber-attack perpetrated in October 2021

Audit Actions

In May 2022, the State Comptroller's Office published an audit report on "Cyber Security of Medical Devices and the Security of the Information Stored Therein"[3]. Following the above audit report, in May 2022, the State Comptroller's Office performed a penetration test on the infrastructure and the communication network that manages the medical equipment at Medical Center A. The penetration test was conducted with the assistance and accompaniment of an external consulting company. It was carried out in the production environment[4] of the network that manages the medical devices. The penetration test was performed in the format of a resilience test that included a risk survey and a scan of vulnerabilities and weaknesses in the system.

3 State Comptroller, **State Comptroller's Report, May 2022**, "Cyber Protection of Medical Devices and the Security of the Information Stored Therein", pp. 1133–1238.

4 The production environment – the work environment that serves the end users and includes software systems and other technological products.

The Knesset State Audit Committee sub-committee decided not to bring this report in its entirety before the Knesset but to publish only parts thereof to protect the state's security under Section 17 of the State Comptroller's Law, 1958 [Consolidated Version].

Key Findings

In the penetration test, 13 significant findings were found in five areas: segmentation and flow control, network access control, protection of workstations and servers, out-of-date software, and insecure access. Ten of the findings were of high severity, and three were of moderate severity.

The Cooperation of Medical Center A's Management and the Deficiencies Rectifying – the cooperation of the Medical Center's management in performing the test and rectifying the deficiencies is commended.

Key Recommendations

It is recommended that the Medical Center's management examine all the medical devices and their supporting systems where deficiencies were found and regularly and habitually manage the risk involved in vulnerable equipment systems to minimize the risks. It is recommended that the management consider the restoration costs due to damage that may occur if these systems are not replaced and examine which systems to upgrade according to their priority. Regarding systems that cannot be upgraded or that will be prioritized as low priority, it is appropriate that the management consider implementing additional compensatory controls. All this is to mitigate the possible harm to the patient's lives and privacy.

It is also recommended that the management formulate an organization-wide work plan to eradicate the risks or minimize them when it is impossible to rectify the deficiencies that have arisen. It is also recommended to carry out penetration tests following a regular plan.

It is recommended that the Ministry of Health, which acts as the regulator in the health sector including information security, complete the penetration tests that it has begun in all medical institutions in Israel and establish a format for periodically performing penetration tests in all institutions. It is further recommended that the Ministry of Health

examine the penetration test findings carried out at Medical Center A and implement the recommendations based on the test findings in all medical institutions. It is also recommended that the Ministry of Health ensure that all medical institutions perform periodic penetration tests, examine the findings of the tests, follow up on rectifying the deficiencies found, and, accordingly, publish recommendations to all medical institutions. In addition, it is recommended that the Ministry of Health continue, as a rule, to help all medical institutions at the national level to cope with the challenges of information security regarding medical equipment.

The Areas in which Deficiencies were Found in the Penetration Test (some were rectified by the audit completion)

Summary

One of the ways to prepare for cyber threats is to perform penetration tests on the organization, to identify vulnerabilities in its defense and to minimize them, and when it is not possible to address the vulnerabilities that were found – to bring the potential risks to the attention of the organization's management and manage them on an ongoing basis. Following the penetration test, the management of Medical Center A rectified several deficiencies and, in particular, updated the security level of specific systems. According to the Medical Center's management, the total cost of rectifying the deficiencies may be over NIS 10 million annually on an ongoing basis. It is recommended that the management formulate an organization-wide work plan to eradicate the risks or minimize them when it is impossible to rectify the deficiencies found. It is also recommended to perform penetration tests following a regular plan.

The Ministry of Health is the regulator of medical institutions, including information security. It is recommended that the Ministry of Health, as the health regulator, complete the penetration tests it has begun to perform in all medical institutions in Israel and establish a format to perform penetration tests in all institutions periodically. It is further recommended that the Ministry of Health examine the penetration test findings carried out at Medical Center A and implement the recommendations based on the test findings in all medical institutions. It is further recommended that the Ministry of Health ensure that all medical institutions perform periodic penetration tests, examine the findings of the tests, follow up on rectifying the deficiencies found, and, accordingly, publish recommendations to all medical institutions. In addition, it is recommended that the Ministry of Health continue to help all medical institutions at the national level to cope with the challenges of information security regarding medical equipment.