דוח מבקר המדינה - סייבר ומערכות מידע
אייר התשפ"ג | מאי 2023

משרד הבריאות

ביקורת סייבר במרכז הרפואי א' - מבדק חדירה לתשתית ולרשת התקשורת

ביקורת סייבר במרכז הרפואי א' - מבדק חדירה לתשתית ולרשת התקשורת

רקע

בעשור האחרון גברו תקיפות הסייבר על ארגונים ועל אנשים פרטיים ברחבי העולם. בשנת 2020 זוהו ברחבי העולם כ-9.5 מיליון ניסיונות למתקפות סייבר שמטרתן הייתה להשבית מערכות מחשוב ולמנוע את היכולת להשתמש בהן[1], זוהו ניסיונות למתקפה 18 פעמים בדקה בממוצע; במחצית הראשונה של שנת 2020 נגנבו או זלגו לאינטרנט לפחות 36 מיליארד נתונים אישיים בעקבות מתקפות סייבר. בהתאם, בשנים האחרונות גברו גם איומי הסייבר על מערכת הבריאות, ובכלל זה על מרכזים רפואיים. כן דווח כי מגזר הבריאות היה אחד מעשרת המגזרים המותקפים ביותר בישראל בשנת 2021[2].

לצורך הפעילות הרפואית משתמשים המוסדות הרפואיים בעשרות אלפי מכשירים רפואיים למגוון רחב של פעולות רפואיות. בין המכשירים הללו גם מכשירי דימות כמו - מכשירי דימות בתהודה מגנטית (MRI)[3], מכשירי טומוגרפיה ממוחשבת (CT)[4], מכשירי רנטגן ומכשירי אולטרה-סאונד. על המכשירים הרפואיים להיות זמינים באופן מלא ובקביעות, לנוכח מגוון הפעולות הרפואיות שיש לבצע באמצעותם, ובייחוד לנוכח נחיצותם לתהליכים מצילי חיים.

הגנת סייבר (אבטחת מידע) במכשור רפואי, לרבות מכשירי דימות, היא תהליך שמטרתו למנוע מגורם בלתי מורשה לבצע שינוי במידע שנאגר במכשירים הרפואיים; להשתמש ללא רשות או להשתמש לרעה במידע הרפואי שנאגר במכשיר הרפואי, שמעובד בו או שמועבר ממנו ליעד חיצוני; וכן לפגוע בפעילות המכשיר הרפואי. אחת הדרכים של ארגון להיערכות לאיומי סייבר היא ביצוע "מבדקי חוסן". מבדקים אלו נועדו לבחון את רמת ההגנה של הארגון, לאתר פרצות אבטחה וסיכונים אפשריים בו ולטפל בהם בהתאם. אחד מסוגי מבדקי החוסן הוא "מבדק חדירה" (PT - Penetration Test) - הליך שבו מתבצעת תקיפה מבוקרת ומתוכננת של המערכות הממוחשבות של הארגון, כדי לאתר בהן חולשות.

משרד מבקר המדינה ביצע במאי 2022 מבדק חדירה במרכז רפואי מסוים (להלן - מרכז רפואי א' או המרכז הרפואי). ההמלצות לתיקון הליקויים בדוח זה מופנות להנהלת המרכז הרפואי ולמשרד הבריאות הפועל כמאסדר של המוסדות הרפואיים, ובכלל זה בתחום אבטחת המידע, כדי שיבחן את תוצאות מבדק החדירה, ויפעל להטמיע את ההמלצות שניתנו בעקבותיו בכל המוסדות הרפואיים.

1 מתקפות מסוג DDOS - Distributed Denial Of Service Attack, התקפת מניעת שירות. המתקפות וזליגות הנתונים היו בתחומים נרחבים.

2 מערך הסייבר הלאומי, **סיכום שנה 2021**.

3 Magnetic Resonance Imaging

4 Computed Tomography

נתוני מפתח

9.5 מיליון
ניסיונות למתקפות סייבר שמטרתן הייתה להשבית מערכות מחשוב זוהו ב-2020 ברחבי העולם

18 פעמים בדקה
בממוצע זוהו ניסיונות למתקפת סייבר ב-2020 ברחבי העולם

36 מיליארד
נתונים אישיים לפחות נגנבו או זלגו לאינטרנט בעקבות מתקפות סייבר במחצית הראשונה של 2020 ברחבי העולם

1 מתוך 10
מגזר הבריאות היה אחד מעשרת המגזרים המותקפים ביותר בישראל ב-2021

יותר מ-100
שרתים ועמדות קצה במערכות הקשורות למכשור הרפואי נסרקו במבדק החדירה התשתיתי במרכז הרפואי א' שנערך ע"י משרד מבקר המדינה

10
מתוך 13 ממצאים שעלו במבדק החדירה, שביצע משרד מבקר המדינה, היו בדרגת חומרה "גבוהה". עוד שלושה היו בדרגת חומרה "בינונית"

10 מיליון ש"ח
הערכה לעלות השנתית לתיקון הליקויים שעלו במבדק החדירה

כ-36 מיליון ש"ח
עלות שיקום המרכז הרפואי הלל יפה אחרי מתקפת הסייבר שאירעה באוקטובר 2021

פעולות הביקורת

במאי 2022 פרסם משרד מבקר המדינה דוח ביקורת בנושא "הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם"[5]. בהמשך לדוח ביקורת זה ביצע משרד מבקר המדינה במאי 2022 מבדק חדירה לתשתית ולרשת התקשורת שמנהלת את המכשור הרפואי במרכז הרפואי א'. מבדק החדירה נערך בסיוע ובליווי של חברת ייעוץ חיצונית

5 מבקר המדינה, **דוח מבקר המדינה, מאי 2022**, "הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם", עמ' 1133 - 1238.

והתבצע בסביבת הייצור[6] של הרשת שמנהלת את המכשור הרפואי. מבדק החדירה בוצע במתכונת של מבדק חוסן שכלל סקר סיכונים וסריקת פגיעויות וחולשות במערכת.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

תמונת המצב העולה מן הביקורת

במבדק החדירה זוהו 13 ממצאים משמעותיים בחמישה תחומים: "סגמנטציה ובקרת זרימה"; "בקרת גישה לרשת"; "הגנת עמדות ושרתים"; "תוכנה לא עדכנית"; ו"גישה לא מאובטחת". עשרה מהממצאים בדרגת חומרה גבוהה ושלושה בדרגת חומרה בינונית.

שיתוף הפעולה של הנהלת המרכז הרפואי א' והתחלת הטיפול בתיקון הליקויים - יצוין לטובה שיתוף הפעולה של הנהלת המרכז הרפואי בביצוע המבדק וכן בהתחלת הטיפול בתיקון הליקויים שעלו בו.

עיקרי הממצאים הביקורת

מומלץ כי הנהלת המרכז הרפואי תבחן את כלל המכשירים הרפואיים והמערכות התומכות שלהם שבהם עלו ליקויים, ותנהל באופן עיתי ושוטף את הסיכון הכרוך בקיום ציוד עם מערכות שיש בהן חולשות, כדי שהסיכונים ימוזערו. מומלץ כי ההנהלה תשקול את העלויות שעשויות להיגרם כתוצאה מנזק שעלול להתרחש אם לא יוחלפו מערכות אלה ותבחן אילו מערכות לשדרג ובהתאם לאיזה סדר עדיפויות. בנוגע למערכות שלא ניתן לשדרג או שיתועדפו בעדיפות נמוכה מוצע שההנהלה תבחן הטמעה של בקרות מפצות נוספות. כל זאת כדי לצמצם את הפגיעה האפשרית בחיי המטופלים ובפרטיותם.

עוד מומלץ כי ההנהלה תגבש תוכנית עבודה רוחבית למיגור הסיכונים או למזעורם במקרים שבהם לא ניתן לתקן את הליקויים שעלו. כמו כן מומלץ לבצע מבדקי חדירה בהתאם לתוכנית סדורה.

מומלץ כי משרד הבריאות, הפועל כמאסדר בתחום הבריאות, ובכלל זה בתחום אבטחת המידע, ישלים את ביצוע מבדקי החדירה שהחל לבצע בכלל המוסדות הרפואיים בארץ, ויקבע מתכונת עיתית להמשך ביצוע מבדקי חדירה בכלל המוסדות. עוד מומלץ כי משרד הבריאות יבחן את ממצאי מבדק החדירה שבוצע במרכז הרפואי א', ויפעל להטמיע בכלל

6 סביבת הייצור - סביבת העבודה המשרתת את משתמשי הקצה וכוללת מערכות תוכנה ומוצרים טכנולוגיים אחרים.

המוסדות הרפואיים את ההמלצות המתבססות על ממצאי המבדק. כמו כן מומלץ שמשרד הבריאות יוודא כי כלל המוסדות הרפואיים מבצעים מבדקי חדירה תקופתיים, יבחן את הממצאים שיעלו במבדקים, יעקוב אחר תיקון הליקויים שעלו בהם ובהתאם לכך יפרסם המלצות לכלל המוסדות הרפואיים. נוסף על כך מומלץ שמשרד הבריאות ימשיך לפעול ככלל כדי לסייע במישור הלאומי לכל המוסדות הרפואיים להתמודד עם אתגרי אבטחת המידע לגבי המכשור הרפואי.

התחומים שבהם נמצאו ליקויים במבדק החדירה (חלקם תוקנו עד מועד סיום הביקורת)

סיכום

אחת הדרכים להיערכות לאיומי סייבר היא לבצע מבדקי חדירה לארגון, כדי לזהות חולשות במעטפת ההגנה שלו ולפעול למזער אותן, ובמקרים שבהם לא ניתן לטפל בחולשות שעלו - להביא לידיעת הנהלת הארגון את הסיכונים האפשריים ולנהל אותם באופן שוטף. בעקבות מבדק החדירה תיקנה הנהלת המרכז הרפואי א' כמה ליקויים, ובפרט עדכנה את רמת האבטחה של מערכות מסוימות. להערכת הנהלת המרכז הרפואי העלות הכוללת לתיקון הליקויים יכולה להסתכם ביותר מעשרה מיליון ש"ח לשנה באופן שוטף. מומלץ כי ההנהלה תגבש תוכנית עבודה רוחבית למיגור הסיכונים או למזעורם במקרים שבהם לא ניתן לתקן את הליקויים שעלו. כמו כן מומלץ לבצע מבדקי חדירה בהתאם לתוכנית סדורה. משרד הבריאות פועל כמאסדר של המוסדות הרפואיים, ובכלל זה בתחום אבטחת המידע. מומלץ כי משרד הבריאות, כמאסדר בתחום הבריאות, ישלים את ביצוע מבדקי החדירה שהחל לבצע בכלל המוסדות הרפואיים בארץ, ויקבע מתכונת עיתית להמשך ביצוע מבדקי חדירה בכלל המוסדות. עוד מומלץ כי משרד הבריאות יבחן את ממצאי מבדק החדירה שבוצע במרכז הרפואי א', ויפעל להטמיע בכלל המוסדות הרפואיים את ההמלצות המתבססות על ממצאי המבדק. כמו כן מומלץ שמשרד הבריאות יוודא כי כלל המוסדות הרפואיים מבצעים בעצמם מבדקי חדירה תקופתיים, יבחן את ממצאי המבדקים האלה, יעקוב אחר תיקון הליקויים שיעלו בהם ובהתאם לכך יפרסם המלצות לכלל המוסדות הרפואיים. נוסף על כך מומלץ שמשרד הבריאות ימשיך לפעול ככלל כדי לסייע במישור הלאומי לכל המוסדות הרפואיים להתמודד עם אתגרי אבטחת המידע לגבי המכשור הרפואי.

ביקורת סייבר במרכז הרפואי א' - מבדק חדירה לתשתית ולרשת התקשורת

מבוא

בעשור האחרון גברו תקיפות הסייבר על ארגונים ועל אנשים פרטיים ברחבי העולם. בשנת 2020 זוהו ברחבי העולם כ-9.5 מיליון ניסיונות למתקפות סייבר שמטרתן הייתה להשבית מערכות מחשוב ולמנוע את היכולת להשתמש בהן[7]. זוהו ניסיונות למתקפה 18 פעמים בדקה בממוצע; במחצית הראשונה של שנת 2020 נגנבו או זלגו לאינטרנט לפחות 36 מיליארד נתונים אישיים בעקבות מתקפות סייבר. בהתאם, בשנים האחרונות גברו גם איומי הסייבר על מערכת הבריאות, ובכלל זה על מרכזים רפואיים. כן דווח כי מגזר הבריאות היה אחד מעשרת המגזרים המותקפים ביותר בישראל בשנת 2021[8].

תקיפות סייבר במערכת הבריאות עשויות לגרום לנזקים נרחבים, ובכלל זה פגיעה במתן שירות רפואי חיוני בעיתות שגרה וחירום; גניבת מידע רפואי אישי וניצולו לרעה, דבר שיש לו השפעות חמורות ברמה האישית וברמת האמון במוסדות הרפואיים במדינה; שיבוש מכוון של מידע בתיקים אישיים קליניים אשר יכול לגרום לקבלת החלטות רפואיות שגויות; פגיעה והרס של מכשור רפואי יקר. לגבי מרכזים רפואיים, קיימות בהם מערכות שהשבתתן עלולה לגרום לפגיעה בפעילות המרכז הרפואי ואף לסיכון חיי המטופלים.

לצורך הפעילות הרפואית משתמשים המוסדות הרפואיים בעשרות אלפי מכשירים רפואיים למגוון רחב של פעולות רפואיות. בין המכשירים הללו גם מכשירי דימות כמו - מכשירי דימות בתהודה מגנטית (MRI)[9], מכשירי טומוגרפיה ממוחשבת (CT)[10], מכשירי רנטגן ומכשירי אולטרה-סאונד. על המכשירים הרפואיים להיות זמינים באופן מלא ובקביעות, לנוכח מגוון הפעולות הרפואיות שיש לבצע באמצעותם, ובייחוד לנוכח נחיצותם לתהליכים מצילי חיים.

הגנת סייבר (אבטחת מידע) במכשור רפואי, לרבות מכשירי דימות, היא תהליך שמטרתו למנוע מגורם בלתי מורשה לבצע שינוי במידע שנאגר במכשירים הרפואיים; להשתמש ללא רשות או להשתמש לרעה במידע הרפואי שנאגר במכשיר הרפואי, שמעובד בו או שמועבר ממנו ליעד חיצוני; וכן לפגוע בפעילות המכשיר הרפואי.

כמו כן, כדי לשמור על הזמינות, השלמות והמהימנות של המידע הנאגר במוסד רפואי, נדרש מערך גיבוי אפקטיבי, יעיל ונרחב. מערך כזה יאפשר לאחזר נתונים שעלולים להינזק או להימחק בעקבות פריצה למערכות המידע של המוסד, וזאת בפרק זמן סביר ותוך מזעור הנזק ככל הניתן.

7 מתקפות מסוג DDOS - Distributed Denial Of Service Attack, התקפת מניעת שירות. המתקפות וזליגות הנתונים היו בתחומים נרחבים.

8 מערך הסייבר הלאומי, **סיכום שנה 2021**.

9 Magnetic Resonance Imaging

10 Computed Tomography

במאי 2022 פרסם משרד מבקר המדינה דוח ביקורת בנושא "הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם"[11] (להלן - דוח הביקורת על הגנת סייבר על מכשירים רפואיים). הביקורת בנושא בוצעה במשרד הבריאות, וב-25 מוסדות רפואיים: בארבע קופות החולים, בכל המרכזים הרפואיים הכלליים-ממשלתיים והממשלתיים-עירוניים, במרכזים רפואיים כלליים של שירותי בריאות כללית ובשני מרכזים רפואיים ציבוריים.

באמצע אוקטובר 2021 פרצו פצחנים (האקרים) למחשבים ולשרתים במרכז הרפואי הממשלתי הלל יפה שבחדרה. התקיפה גרמה לשיבוש רציפות הפעילות במרכז הרפואי במשך כשלושה חודשים, להסטת חולים מהמרכז הרפואי למרכזים אחרים, למעבר לעבודה ידנית ולא ממוחשבת, למניעת גישה למידע הרפואי של המטופלים ועוד. עלות שיקום המרכז הרפואי הלל יפה אחרי מתקפת הסייבר הוערכה בכ-36 מיליון ש"ח. תקיפה זו מחדדת את החשיבות להיערכות מיטבית לאיום הסייבר ולאבטחת המידע.

אחת הדרכים של ארגון להיערכות לאיומי סייבר היא ביצוע מבדקי חוסן. מבדקים אלו נועדו לבחון את רמת ההגנה של הארגון, לאתר פרצות אבטחה וסיכונים אפשריים בו ולטפל בהם בהתאם. בתרשים שלהלן מפורטים סוגי מבדקי החוסן שניתן לבצע בארגון.

תרשים 1: **סוגי מבדקי החוסן שניתן לבצע בארגון**

11 מבקר המדינה, **דוח מבקר המדינה, מאי 2022,** "הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם", עמ' 1133 - 1238.

מבדק חדירה (Penetration Test - PT): מבדק חדירה הוא הליך שבו מתבצעת תקיפה מבוקרת ומתוכננת של המערכות הממוחשבות של הארגון, כדי לאתר בהן חולשות. המבדק יכול להתבצע בכמה סביבות עבודה של המערכות הממוחשבות, ובהן "סביבה נקייה" שבה אפשר לבצע בדיקות עם סיכון נמוך לגרימת נזק למערכות המידע (סביבת בדיקה[12] - Testing); או לחלופין במערכות הממוחשבות עצמן (סביבת ייצור[13] - Production) באופן שמאפשר לבחון באופן מדויק יותר את החולשות, אך תוך סיכון גדול יותר לפגיעה במערכות אלה. ניתן לבצע סוגים שונים של מבדקי חדירה, ובהם מבדק חדירה אפליקטיבי ומבדק חדירה תשתיתי.

מבדק חדירה אפליקטיבי: המבדק האפליקטיבי מאתר את החולשות ביישומים (אפליקציות) מבוססי דפדפן, למשל אתר מרשתת (אינטרנט). המבדק מזהה פרצות במערך האבטחה שיכולות לאפשר גישה לבסיסי נתונים, למשל למידע אישי של לקוחות, לגרום לדליפתו כמו גם לשיבושו, לביצוע מתקפות למניעת שירות ולשיבוש מהלך העבודה התקין.

מבדק חדירה תשתיתי: המבדק התשתיתי מזהה את הנקודות החשופות ביותר לפגיעה באבטחת תשתיות הרשת הפנימית של הארגון ובכלל זה במערכות ההפעלה שלו בשרתים ובציוד תקשורת, ומאפשר לארגון לתקן את החולשות שעלו במבדק לטובת התגוננות מרבית מפני התקפות גורמים זדוניים על הרשת הארגונית.

פעולות הביקורת

בהמשך לדוח הביקורת על הגנת סייבר על מכשירים רפואיים, ביצע משרד מבקר המדינה במאי 2022 מבדק חדירה לתשתית ולרשת התקשורת שמנהלת את המכשור הרפואי במרכז רפואי מסוים (להלן - מרכז רפואי א' או המרכז הרפואי). מבדק החדירה נערך בסיוע ובליווי של חברת ייעוץ חיצונית והתבצע בסביבת הייצור של הרשת שמנהלת את המכשור הרפואי. מבדק החדירה בוצע במתכונת של מבדק חוסן שכלל סקר סיכונים וסריקת פגיעויות[14] וחולשות במערכת.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

הנהלת המרכז הרפואי א' אחראית על יישום ההנחיות בנושא אבטחת המידע והסייבר והטמעתן ועל ניהול מערכות המידע במוסד. ההמלצות מופנות להנהלת המרכז הרפואי ולמשרד הבריאות הפועל כמאסדר של המוסדות הרפואיים, ובכלל זה בתחום אבטחת המידע, כדי שיבחן את תוצאות מבדק החדירה, ויפעל להטמיע את ההמלצות שניתנו בעקבותיו בכלל המוסדות הרפואיים.

12 סביבת בדיקה היא פלטפורמה, תוכנה או מערכת המאפשרת ליצור ולנהל בדיקות תוכנה, בסביבה המדמה את הסביבה האמיתית.

13 סביבת הייצור - סביבת העבודה המשרתת את משתמשי הקצה וכוללת מערכות תוכנה ומוצרים טכנולוגיים אחרים.

14 פגיעות היא נקודת חולשה באבטחה.

ממצאי מבדק החדירה התשתיתי

התכנון והביצוע של מבדק החדירה התשתיתי (להלן - מבדק החדירה או המבדק) בוצע בשיתוף הנהלת המרכז הרפואי א'.

יצוין לטובה שיתוף הפעולה של הנהלת המרכז הרפואי א' בביצוע המבדק וכן בהתחלת הטיפול בתיקון הליקויים שעלו בו.

מטרת המבדק הייתה למדוד את רמת ההגנה על רשת המכשור הרפואי במרכז הרפואי המכילה מכשירים שונים, ובהם מכשירי CT, ממוגרפיה, PACS[15], אולטרה-סאונד, רדיוגרפיה (CR) ותחנות פענוח[16]. במסגרת המבדק סרק כלי הבדיקה יותר מ-100 שרתים ועמדות קצה במערכות הקשורות למכשור הרפואי, כדי לבחון את הפגיעויות התשתיתיות הקיימות בהן ובסביבתן. במכשירים רפואיים מסוימים, כמה רכיבים שמצויים בסיכון הורצו באופן פרטני ומבוקר ובאישור המרכז הרפואי, כאשר לא התבצעה במכשירים אלה בדיקה רפואית באותה העת. במבדק הושם דגש על הנושאים האלה: חוסן המכשור אל מול מתקפות ואיומים ידועים, איתור הפערים בין המצב המאובטח הנוכחי למצב המאובטח הרצוי ואיתור כל החולשות והמפגעים התשתיתיים הקיימים. בעקבות המבדק ניתנו המלצות לצורך תיקון מיידי של הליקויים.

חומרת הממצאים דורגה על פי חומרת הנזק הגלומה בהם - נמוכה, בינונית או גבוהה. חומרת הנזק נקבעה בהתאם לרמת ההשפעה על יכולת הגוף המבוקר לקיים את התהליכים התפעוליים במקרה של התממשות הסיכון. הגדרת חומרת הממצאים לא התייחסה לבקרות המפצות (פעולות להפחתת סיכון) הקיימות במרכז הרפואי.

במבדק החדירה זוהו 13 ממצאים משמעותיים, עשרה בדרגת חומרה גבוהה ושלושה בדרגת חומרה בינונית. להלן בתרשים פירוט התחומים בהם נמצאו הליקויים:

תרשים 2: **התחומים שבהם נמצאו ליקויים במבדק החדירה (חלקם תוקנו עד מועד סיום הביקורת)**

15 מערכת PACS (Picture Archiving and Communication System) היא ארכיב דיגיטלי של צילומי דימות ממכשירי דימות.

16 רדיוגרפיה היא שיטת צילום באמצעות קרינה מיוננת; תחנת פענוח היא המחשב שעל גביו מפענחים את צילומי הדימות.

בקרות מפצות שהטמיעה הנהלת המרכז הרפואי א' עוד לפני ביצוע המבדק כדי להתמודד עם פגיעויות

הנהלת המרכז הרפואי מסרה בתגובתה לממצאי הביקורת שעוד לפני ביצוע המבדק היא התמודדה עם פגיעויות שעלו, בין השאר, גם במבדק החדירה, והטמיעה בקרות מפצות (פעולות להפחתת סיכון) שבכוחן להקטין נזקים שעלולים להיגרם בשל פגיעויות המערכת.

בתגובת הנהלת המרכז הרפואי לממצאי מבדק החדירה מאוקטובר 2022 היא ציינה כי להערכתה, העלות הכוללת של תיקון הליקויים יכולה להסתכם ביותר מ-10 מיליון ש"ח לשנה באופן שוטף. ההנהלה הוסיפה בתגובתה לממצאי הביקורת בינואר 2023 כי כבר קבעה כמטרה לטפל בסיכוני האבטחה במכשור הרפואי, גיבשה מדיניות בהתאם ונקטה צעדים בנושא. עוד הוסיפה כי היא דנה באופן שוטף בניהול סיכוני סייבר והיא מביאה בחשבון את הפערים שעולים.

משרד הבריאות מסר בתגובתו למשרד מבקר המדינה בדצמבר 2022 כי כחלק מהיערכותו להתמודדות עם איומי הסייבר על מערכת הבריאות בישראל, הוא פועל בכמה מישורים כדי להגביר את רמת המוכנות של המוסדות הרפואיים לאירועים כאלה. משרד הבריאות ציין כי במסגרת פעילותו זו הוא בין היתר פרסם חוזר בנושא רגולציית יסוד להגנת סייבר במערכת הבריאות, הקובע למוסדות הרפואיים עקרונות להתמודדות עם איומי הסייבר; הוא החל בשנת 2022 בקידום פרויקט לאומי להגנה על מכשור רפואי במוסדות הרפואיים, שהטמעתו תחל בשנת 2023; הוא ביצע בשנת 2022 סקרי סיכונים בבתי החולים, במטרה לאמוד את מוכנותם להתמודדות עם האיומים ולשפר את מערך ההגנה של המוסדות הרפואיים ואת חוסנם. יצוין כי משרד הבריאות ביצע בשנת 2022 מבדקי חדירה ב-19 בתי חולים ובשתי קופות חולים, ועתיד להשלים ביצוע מבדקי חדירה נוספים בשלושה בתי חולים ובשתי הקופות הנותרות בשנת 2023. המשרד גם ביצע בשנת 2022 תרגיל סייבר לבחינת המוכנות להתאוששות מאסון בעשרה בתי חולים, ומגבש תוכנית עבודה לביצוע תרגילים נוספים כאלה.

סיכום

אחת הדרכים להיערכות לאיומי סייבר היא לבצע מבדקי חדירה לארגון, כדי לזהות חולשות במעטפת ההגנה שלו ולפעול למזער אותן, ובמקרים שבהם לא ניתן לטפל בחולשות שעלו - להביא לידיעת הנהלת הארגון את הסיכונים האפשריים ולנהל אותם באופן שוטף. מבדק החדירה התשתיתי, נשוא דוח זה, בוצע במרכז הרפואי א' וזוהו בו 13 ממצאים הנוגעים לפגיעויות באבטחה של תשתיות הרשת הפנימית של המכשור הרפואי, שעשרה מהם היו בדרגת חומרה גבוהה.

בעקבות מבדק החדירה תיקנה הנהלת המרכז הרפואי כמה ליקויים, ובפרט עדכנה את רמת האבטחה של מערכות מסוימות. להערכת ההנהלה, העלות הכוללת של תיקון הליקויים יכולה להסתכם ביותר מ-10 מיליון ש"ח לשנה באופן שוטף. מומלץ כי ההנהלה תבחן את כלל המכשירים הרפואיים והמערכות התומכות שלהם שבהם עלו ליקויים, ותנהל באופן עיתי ושוטף את הסיכון הכרוך בקיום ציוד עם מערכות שיש בהן חולשות כדי שהסיכונים ימוזערו. מומלץ כי ההנהלה תשקול את העלויות שעשויות להיגרם כתוצאה מנזק שעלול להתרחש אם לא יוחלפו מערכות אלה, ותבחן אילו מערכות לשדרג ובהתאם לאיזה סדר עדיפויות. בנוגע למערכות שלא ניתן לשדרג או שיתועדפו בעדיפות נמוכה מוצע שההנהלה תבחן הטמעה של בקרות מפצות נוספות. כל זאת כדי לצמצם את הפגיעה האפשרית בחיי המטופלים ובפרטיותם. עוד מומלץ כי ההנהלה תגבש תוכנית עבודה רוחבית למיגור הסיכונים או למזעורם במקרים שבהם לא ניתן לתקן את הליקויים שעלו. כמו כן מומלץ לבצע מבדקי חדירה בהתאם לתוכנית סדורה.

משרד הבריאות פועל כמאסדר של המוסדות הרפואיים, ובכלל זה בתחום אבטחת המידע. בדוח בנושא "הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם" המליץ מבקר המדינה שמשרד הבריאות יגבש תוכנית רב-שנתית להגנת הסייבר במוסדות הרפואיים, הכוללת הגדרת יעדים, סדרי עדיפויות ומדדים וכן הערכה לגבי התקציב הנדרש ומקורות המימון האפשריים. בהמשך להמלצות שצוינו בדוח הקודם ונוכח ממצאי הדוח הנוכחי, מומלץ כי משרד הבריאות, כמאסדר בתחום הבריאות, ישלים את ביצוע מבדקי החדירה שהחל לבצע בכלל המוסדות הרפואיים בארץ, ובמסגרת התוכנית שיגבש הוא יקבע מתכונת עיתית להמשך ביצוע מבדקי חדירה בכלל המוסדות. עוד מומלץ כי משרד הבריאות יבחן את ממצאי מבדק החדירה שבוצע במרכז הרפואי א' ויפעל להטמיע בכלל המוסדות הרפואיים את ההמלצות המתבססות על ממצאי המבדק. כמו כן מומלץ שמשרד הבריאות יוודא כי כלל המוסדות הרפואיים מבצעים בעצמם מבדקי חדירה תקופתיים, יבחן את ממצאי המבדקים האלה, יעקוב אחר תיקון הליקויים שיעלו בהם ובהתאם לכך יפרסם המלצות לכלל המוסדות הרפואיים. נוסף על כך מומלץ שמשרד הבריאות ימשיך לפעול ככלל כדי לסייע במישור הלאומי לכל המוסדות הרפואיים להתמודד עם אתגרי אבטחת המידע בתחום המכשור הרפואי.