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 Distributed Denial Of Service Attack - DDOS, 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 המלצות 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.