דוח מבקר המדינה | אייר התשפ"ב | מאי 2022

משרד הבריאות

הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם

הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם

רקע

בעשור האחרון גברו תקיפות הסייבר על ארגונים ועל אנשים פרטיים ברחבי העולם, ובשנים האחרונות גברו גם איומי הסייבר על מוסדות רפואיים. במרכזים רפואיים קיימות מערכות שהשבתתן עלולה להוביל לפגיעה בפעילות המרכז הרפואי ואף לסיכון חיי המטופלים. 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 בעקבות שינוי מידע בתיקים אישיים קליניים אשר יכול לגרום לקבלת החלטות רפואיות שגויות; פגיעה והרס של מכשור רפואי יקר.

לצורך הפעילות הרפואית משתמשים המוסדות הרפואיים בעשרות אלפי מכשירים רפואיים למגוון רחב של פעולות רפואיות; בין המכשירים הללו מכשירי הדימות[1] MRI (דימות בתהודה מגנטית), CT (טומוגרפיה ממוחשבת), רנטגן ואולטרסאונד נשים. על מכשירים רפואיים להיות זמינים באופן מלא ובקביעות לנוכח מגוון הפעולות שיש לבצע באמצעותם ובייחוד לנוכח נחיצותם לתהליכים מצילי חיים.

הגנת סייבר (אבטחת מידע) במכשור רפואי לרבות על מכשירי דימות, היא תהליך שמטרתו למנוע מגורם בלתי מורשה לבצע שינוי במידע שנאגר במכשירים הרפואיים; שימוש בלתי מורשה או שימוש לרעה במידע הרפואי שנאגר במכשיר הרפואי, שמעובד בו או מועבר מהמכשיר הרפואי ליעד חיצוני; וכן פגיעה בפעילות המכשיר הרפואי.

הדוח מתבסס על תשובות 25 המוסדות הרפואיים שהתבקשו להשיב על שאלון בנושא "הגנה ואבטחה של מידע במכשירים רפואיים" שהפנה אליהם משרד מבקר המדינה: 11 המרכזים הרפואיים הכלליים-ממשלתיים, שני המרכזים הרפואיים הציבוריים, שמונת המרכזים הרפואיים הכלליים של הכללית וארבע קופות החולים; הכללית השיבה בנוגע לחלק מהפרקים שבשאלון בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה, ולכן מספר המוסדות שבהם עוסקים פרקים אלה הוא 17.

באמצע אוקטובר 2021, במהלך תקופת הביקורת, פרצו פצחנים למחשבים ושרתים במרכז הרפואי הלל יפה שבחדרה. התקיפה הובילה לשיבוש פעילות המרכז הרפואי, וגרמה להסטת חולים מהמרכז הרפואי למרכזים אחרים, למעבר לעבודה ידנית ולא ממוחשבת, למניעת גישה

1 דימות רפואי הוא טכנולוגיה מתקדמת שבה מדגימים באמצעות תצלומים חלקים פנימיים בגוף נבדק. זהו שם כולל למגוון בדיקות בסיסיות הנעשות לפני חלק ניכר מאבחונים ופעולות רפואיים, לצורך אבחון קליני, תכנון של הטיפול, מעקב אחר החולים וסיוע בביצוע פעילות פולשנית (ניתוחים).

למידע הרפואי של המטופלים ועוד. תקיפה זו מחדדת את החשיבות להיערכות מיטבית לאיום הסייבר ולאבטחת המידע.

נתוני מפתח

כ-9.5 מיליון

ניסיונות למתקפות סייבר ברחבי העולם בשנת 2020, שמטרתן להשבית מערכות מחשוב[2]

כ-2,700

מספרם המשוער של מכשירי הדימות מסוג MRI, CT, רנטגן ואולטרסאונד נשים במוסדות הרפואיים שנבדקו

8%

שיעור התקציב המזערי שיש להקצות, על פי החלטת הממשלה, להגנת סייבר, מתוך תקציב מערכות המידע של המרכזים הרפואיים הממשלתיים

13 מתוך 17

מוסדות רפואיים[3] לא ביצעו סקר סיכונים[4] בנושא מכשור רפואי

13 מתוך 17

מוסדות רפואיים לא שילבו בתוכניותיהם את אופן הטיפול וההתאוששות של מערך המכשור הרפואי במקרה של אסון

5 מתוך 17

מוסדות רפואיים לא התנו רכישת מכשור רפואי בכך שממונה אבטחת המידע יבחן את היבטי אבטחת המידע הנוגעים למכשור הרפואי

13 מתוך 17

מוסדות רפואיים שאין בהם בקרת הרשאה לוגית (שם משתמש וסיסמה) לגישה למכשיר אולטרסאונד נשים

14 מתוך 17

מוסדות רפואיים לא ביצעו מבדקי חדירה[5] למכשור רפואי בשנים 2018 - 2021

2 מתקפות מסוג DDOS - Distributed Denial Of Service Attack, התקפת מניעת שירות.

3 הכללית נספרה כמוסד רפואי אחד אך ההתייחסות בהגדרה זו היא לכל שמונת המרכזים הרפואיים הכלליים שלה ולמרפאות בקהילה.

4 סקר סיכונים בוחן ומאתר איומים וחשיפות של אבטחת מידע במערכות של המוסדות הרפואיים ומעריך את רמת הסיכון הנשקפת לפעילותם בגין איומים אלה.

5 מבדק חדירה הוא הליך שבמהלכו מתבצעת תקיפה מבוקרת ומתוכננת של המערכת הממוחשבת של הארגון על מנת לאתר בה חולשות.

פעולות הביקורת

בחודשים ינואר-נובמבר 2021 בדק משרד מבקר המדינה את הגנת הסייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם, תוך התמקדות במכשירי דימות (CT, MRI, רנטגן ואולטרסאונד נשים). הנושאים שנבדקו: הפעילות המינהלית בתחום אבטחת המידע במוסדות הרפואיים; ההגנה על המכשירים בכל מעגל החיים שלהם: רכישתם, השימוש בהם וסיום השימוש בהם. בכלל זה נבדקו ההגנה על המכשירים ברשת המוסד הרפואי, הרשאות הגישה למכשירים, ניהול המשתמשים, אבטחת מידע בעת פענוח ממצאי הסריקות, ההגנה על המידע הרפואי שנאגר במכשירים ודרכי התחזוקה של המכשירים. הביקורת בוצעה במשרד הבריאות, ב-25 מוסדות רפואיים: בקופות החולים, בכל המרכזים הרפואיים הכלליים-ממשלתיים והממשלתיים-עירוניים במרכזים רפואיים כלליים של הכללית, ובשני מרכזים רפואיים ציבוריים[6]. בדיקות השלמה בוצעו במערך הסייבר הלאומי, ברשות להגנת הפרטיות במשרד המשפטים ובי"ענבל חברה לביטוח בע"מ", שהיא חברה ממשלתית לביטוח.

דוח זה הומצא לראש הממשלה ביום 15.2.22 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה. מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו על שולחן הכנסת ולא יפורסמו. ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאת הדוח כאמור לעיל.

תמונת המצב העולה מן הביקורת

האחריות לתחום הגנת הסייבר - כשש שנים לאחר קבלת החלטות הממשלה 2443 ו-2444 בנושא היערכות לאומית וקידום אסדרה לאומית בהגנת הסייבר (בשנת 2015)[7], ועל אף החשיבות הלאומית שבהסדרת הגנת הסייבר, לא הוסדרו סמכויות מערך הסייבר הלאומי כלפי היחידות להכוונה מקצועיות במשרדי הממשלה (יחידות מגזריות) לרבות במגזר הבריאות.

פעילות משרד הבריאות בתחום הגנת הסייבר - משרד הבריאות לא השלים את גיבוש הנחיותיו בתחום הגנת הסייבר הכוללות עקרונות יסוד לניהול הגנת סייבר וכלים להתמודד עם אירוע סייבר, והן לא הופצו; במסגרת בקרות הרישוי שביצע המשרד במרכזים

6 ברוב פרקי הדוח הכללית נספרה כגוף אחד, הכולל הן את מרפאות הקהילה והן את בתי החולים שלה, ועל כן מספר המוסדות בפרקים אלה הוא 17.

7 החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15); והחלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15). תאריך עדכון ההחלטה - 28.7.15.

הרפואיים בשנים 2019 ו-2020 הוא לא ביצע בקרה בנושא ההגנה על מכשור רפואי; וכן לא מבצע מעקב סדור אחר תיקון ליקויים שעלו בדוחות הבקרה שביצע בנושא אבטחת מידע, ובכך לא מוודא את אי-הישנותם; ה-SOC (מרכז לניטור, לשליטה ולבקרה על אירועי סייבר) של משרד הבריאות מאוייש חלקית - בשעות מסוימות בימי חול ועלו פערים מסוימים בפעילותו; הנחיות אגף ציוד רפואי (אמ"ר) במשרד הבריאות שעוסק ברישום מכשירים רפואיים ובמתן היתרי יבוא ושיווק שלהם לארץ אינן נוגעות לצורך בעמידתם בתקני אבטחת מידע.

- **אחריות חטיבת המרכזים הרפואיים הממשלתיים לתחום אבטחת מידע וסייבר** - לחטיבת המרכזים הרפואיים במשרד הבריאות אין תמונת מצב מיטבית בדבר איכות אבטחת המידע בכל אחד מהמרכזים הרפואיים שבאחריותה. אף שהחלטת הממשלה קובעת שהחטיבה תשמש גוף מטה בתחום מערכות מידע, ואף שמחוזר מנכ"ל משרד הבריאות עולה כי אחריות החטיבה כלפי אופן תפקודם של המרכזים הרפואיים כוללת, ומתייחסת גם להיבטים של מערכות מידע, בפועל - בחטיבה פועל אגף מערכות מידע, אולם העיסוק בתחום אבטחת המידע הוא בידי יחידת הסייבר המגזרית במשרד הבריאות, והחטיבה אינה מעורבת בכך.

- **מדיניות אבטחת מידע במוסדות הרפואיים - ועדת היגוי ובעלי תפקידים** - ב-19 מוסדות רפואיים מ-25 המוסדות הרפואיים שענו על שאלון אבטחת המידע מנכ"ל המוסד לא עמד בראש ועדת ההיגוי לתחום הגנת המידע; שמונה מ-25 המוסדות הרפואיים לא מינו ממונה הגנה על הפרטיות.

הממצאים שלהלן עלו משאלון אבטחת מידע שנשלח לכל המוסדות הרפואיים ובמסגרתו הכללית ענתה בשם כל שמונת המרכזים הרפואיים שלה ומרפאות הקהילה ולכן נספרה כמוסד רפואי אחד. הממצאים נוגעים אפוא ל-17 מוסדות רפואיים:

- **מדיניות אבטחת מידע במוסדות הרפואיים ועמידתם בנוהלי אבטחת המידע** - המוסדות הרפואיים נבדלים ביניהם במידה רבה מבחינת היחס בין מספר עובדי המוסד העוסקים בתחום אבטחת המידע או הגנת סייבר ובין מספר העובדים במוסד: בחמישה מוסדות יש איש צוות אבטחת מידע ל-1,000 עובדים ומטה ובשלושה יש איש צוות אחד ל-3,000 עובדים; שישה מ-11 מרכזים רפואיים כלליים-ממשלתיים הקצו להגנת סייבר בממוצע בשנים 2015 - 2020 שיעור קטן מזה שקבעה החלטת הממשלה - 8% מההקצאה התקציבית לאבטחת מידע[8]; במועד ביצוע הביקורת לכל המרכזים הרפואיים הממשלתיים לא היה ביטוח סייבר. בנוגע לשאר המוסדות הרפואיים, לחלקם היה ביטוח סייבר ולחלקם לא. חמישה מוסדות רפואיים לא כללו בתוכנית העבודה שלהם לשנים 2020 ו-2021 התייחסות לשיפור ההגנה על מכשור רפואי ואבטחת המידע הנאגר בו; שמונה מ-17 מהמוסדות הרפואיים לא ביצעו ביקורת פנים בתחום אבטחת מידע; 13 מ-17 מוסדות רפואיים לא ביצעו סקר סיכונים בנושא מכשור רפואי; 11 מ-17 המוסדות רפואיים לא הגדירו קבוצות סיכון למכשור הרפואי לפי סיווגי סיכון.

8 החלטת הממשלה בנושא לא עסקה במרכזים רפואיים ציבוריים או בקופות החולים, ולכן המוסדות הרפואיים שנבדקו בפרק זה היו 11 מרכזים רפואיים כלליים-ממשלתיים.

התאוששות מאסון והמשכיות עסקית של מכשור רפואי - מתוך 17 המוסדות, לשניים אין תוכנית להתאוששות מאסון (למשל מתקפת סייבר על תשתיות מערכות המידע של המוסד הרפואי) או תוכניות להמשכיות עסקית (יכולתו של ארגון להמשיך בפעילותו הרגילה); לשישה אין אתר חלופי (DR) זמין לטובת המשך פעילות מערכות המידע במקרה של אסון; 13 לא שילבו בתוכניות שלהם להתאוששות מאסון או בתוכנית להמשכיות עסקיות את אופן הטיפול וההתאוששות של מערך המכשור הרפואי.

מדיניות אבטחת מידע

	מוסד א'	מוסד ט"ז	מוסד ג'	מוסד ד'	מוסד י"ד	מוסד ו'	מוסד ז'	מוסד י"ז	מוסד ט'	מוסד י'	מוסד י"א	מוסד י"ב	מוסד י"ג	מוסד ח'	מוסד ה'	מוסד ט"ו	מוסד ב'
מנהל המוסד בראש ועדת ההיגוי	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🟢	🔴	🟢	🟢	🔴	🔴
ממונה אבטחת מידע	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
ממונה הגנת הפרטיות	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟢	🔴	🔴	🔴	🟢	🟢	🟢	🟢	🟢	🟢
תוכנית עבודה בתחום אבטחת המידע	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
תוכנית העבודה מתייחסת להגנה על מכשור רפואי	🟢	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
סקר סיכונים בתחום אבטחת המידע	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
עדכנו את סקר הסיכונים	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢
סקר סיכונים בנושא מכשור רפואי	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🟢	🔴	🔴
הגדירו קבוצות סיכון למכשירים רפואיים	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🟢	🟢	🔴
תוכנית להמשכיות עסקית או להתאוששות מאסון	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
אתר חלופי זמין (DR)	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟡
התוכנית להתאוששות מאסון עוסקת במכשירים רפואיים	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🟡	🔴
נוהל להתמודדות עם אירוע אבטחת המידע	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢
ביקורת פנים בתחום אבטחת מידע	🔴	🔴	🟢	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🟢	🟢	🟢	🟢	🟢	🟢

🟢 כן 🔴 לא 🟡 חלקי/בתהליך/בבחינה

אבטחת מידע בעת רכישת מכשיר רפואי חדש - מתוך 17 המוסדות שנבדקו, חמישה לא כללו בנוהלי הרכש שלהם התייחסות להיבטי אבטחת מידע במכשור הרפואי, ולאחד אין נוהל רכש; חמישה לא התנו את רכישת המכשור הרפואי בכך שממונה אבטחת המידע יאשר את ביצוע הרכש, ולעיתים מוסדות רפואיים שדרשו בנוהליהם אישור של ממונה אבטחת המידע לצורך הרכש רכשו בפועל את המכשירים בלי שהתקבל אישור לכך; כמו כן ניכרים פערים בין סוגי בדיקות אבטחת המידע שביצעו המוסדות הרפואיים בעת רכישת מכשור רפואי ולפני התחלת השימוש בו ומספרן, ובכלל זה הסרת יישומים שאינם נדרשים מהמכשיר וסריקת המכשיר באמצעות כלי לזיהוי נוזקות, פוגענים ופעילויות חריגות.

הגנה על המכשירים הרפואיים בזמן השימוש בהם במוסד הרפואי - מבין 17 המוסדות הרפואיים שנבדקו שישה לא מיפו את כל המכשירים הרפואיים שברשותם; לא כל המוסדות כללו במיפויים שעשו את מאפייני אבטחת המידע העיקריים של המכשירים; קיימים חוסרים מהותיים במערך ההגנה שהמוסדות הרפואיים הטמיעו ברשת לצורך הגנה על מכשור רפואי ובכלל זה מכשירי דימות מסוג MRI ו-CT, ובחלק מהמוסדות יש שילוב של חוסרים המגבירים את חשיפתם של המכשירים לסיכוני אבטחת מידע; 11 מ-17 המוסדות לא גיבשו נוהל להסדרת עדכוני תוכנה, הנדרש על מנת להבטיח פעולה רציפה ובטוחה של המכשור הרפואי, ועשרה מוסדות לא תיעדו את עדכוני גרסאות התוכנה שביצעו במכשירים רפואיים; 14 מוסדות לא ביצעו מבדקי חדירה שכללו תקיפה של מכשור רפואי בשנים 2018 - 2021, כפי שקבע נוהל משרד הבריאות.

בקרות הרשאה פיזיות ולוגיות למכשירי דימות - הרשאות גישה, ניהול רשימת משתמשים ומדיניות סיסמאות הם כלי מרכזי ביישום מדיניות אבטחת מידע בכל ארגון. שבעה מוסדות לא ביצעו לפחות פעם אחת עדכון של רשימת המשתמשים בעלי הרשאות לוגיות (שם משתמש וסיסמה) למערך המכשור הרפואי בשנים 2019 - 2020; בשני מוסדות יש מכשירי רנטגן ללא בקרת הרשאה פיזית (חדר נעול) וללא בקרה הרשאה לוגית. בשני מוסדות רפואיים אין בקרות

הרשאה פיזיות ולוגיות על חלק ממכשירי אולטרסאונד הנשים. בארבעה מוסדות רפואיים לא קיימת בקרת הרשאה לוגית בשום סוג של מכשירי הדימות שנבדקו.

הגנה על המכשירים ועל המידע שבהם בעת תחזוקתם ובעת פיענוח תוצאות - במוסד אחד טכנאים חיצוניים מבצעים פעילות תחזוקה ללא ליווי של המוסד הרפואי ושני מוסדות רפואיים לא החתימו את החברות הנותנות שירותי תחזוקה למכשירים הרפואיים, או את טכנאי חברות אלו, על הסכם סודיות; מתוך 14 מוסדות המאפשרים ליצרני המכשירים להתחבר למכשירי ה-MRI וה-CT מרחוק, מוסד אחד לא הסדיר את אופן ההתחברות מרחוק באמצעות נוהל, ושניים לא ביצעו ניטור של ההתחברות מרחוק, למשל באמצעות רישום הפעולות או הקלטת ההתחברות; לשבעה מ-12 מהמוסדות שהוציאו מכשור רפואי לתחזוקה מחוץ למוסד הרפואי לא היה מידע מדויק בנוגע למספר המכשירים שהוצאו לתחזוקה בשנת 2020 ולזהותם.

הקמת מרכז לניטור, שליטה ובקרה (SOC - Security Operating Center) של מגזר הבריאות - בשנת 2016, עוד לפני שניתנה הנחיית מערך הסייבר הלאומי, החליט משרד הבריאות להקים SOC מגזרי שייתן שירות למוסדות רפואיים - יפעל כמרכז המשמש לניטור אירועי סייבר וכן לשליטה ולבקרה עליהם. ה-SOC החל לפעול בסוף אותה שנה.

עמידה בתקן ISO וקיומה של תוכנית עבודה - במועד סיום הביקורת (נובמבר 2021) כל המוסדות הרפואיים שבהם עסק דוח זה עמדו בתקן הבין-לאומי ISO 27799 לאבטחת מערכות מידע בתחום הבריאות. כמו כן לכל 17 המוסדות הרפואיים שענו על שאלון אבטחת המידע הייתה תוכנית עבודה שנתית או רב-שנתית בתחום אבטחת המידע.

עיקרי המלצות הביקורת

מבקר המדינה חוזר על המלצתו מדוח קודם לקדם את תהליך האסדרה של סמכויות מערך הסייבר הלאומי כלפי היחידות המגזריות במשרדי הממשלה ובכללן כלפי מגזר הבריאות, ושל הפער בין סמכויות המאסדרים.

מומלץ שמשרד הבריאות:

- ישלים את גיבוש הנהלים הכוללים עקרונות יסוד לניהול הגנת סייבר ויפרסמם, שישלב באופן סדור בבקרות שהוא מבצע במרכזים הרפואיים ובקופות החולים בדיקה הן של נושא אבטחת מידע והן של מכשור רפואי ושיעקוב אחר תיקון הליקויים שעלו בבקרות. כמו כן מומלץ שהמשרד יגבש תוכנית רב-שנתית להגנת סייבר במוסדות הרפואיים הכוללת הגדרת יעדים, סדרי עדיפויות, מדדים וכן הערכה תקציבית נדרשת ואת מקורות המימון האפשריים. מומלץ גם שהמשרד ישקול לקבוע חובת מינוי ממונה על הגנת הפרטיות בדומה למחויב במדינות מערביות רבות.

- יבחן את הממשקים שבין חטיבת המרכזים הרפואיים הממשלתיים לבין יחידת הסייבר המגזרית ויבחן בידי מי נכון להפקיד את האחריות לטיפול בנושא אבטחת המידע בכלל המרכזים הרפואיים הממשלתיים (הכלליים, הגריאטריים ולבריאות הנפש), גם נוכח החלטת הממשלה בנושא.

- יפעל לכך שה-SOC של היחידה המגזרית יפעל באופן שוטף, ייתן מענה לפערים שעלו וישלים את חיבור כלל המוסדות הרפואיים ל-SOC. עוד מומלץ שהמשרד ישקול לשלב תקני אבטחת מידע בהליך האישור של אגף ציוד רפואי (אמ"ר) לייבוא ולשיווק של מכשור רפואי לישראל. צעד זה יאפשר לנהל בדיקה מרוכזת בדבר קיומם של מדדי אבטחת המידע הנדרשים במכשור רפואי חדש וישפר את רמת האבטחה של מכשירים רפואיים המשמשים את בתי החולים, קופות החולים ומוסדות רפואיים נוספים. כמו כן מומלץ שהמשרד יבחן אם יש צורך להגדיר במישור הלאומי אילו מכשירים רפואיים יש לכלול ברמת הסיכון הגבוהה ביותר, שבהתאם לכך יש לתת להם את המענה ההגנתי המרבי.

מומלץ שהמוסדות הרפואיים:

- יבטיחו כי המנכ"ל יעמוד בראש ועדת ההיגוי לתחום הגנת המידע כנדרש בחוזר מנכ"ל משרד הבריאות משנת 2015; שיפעלו בהתאם להוראות החלטת הממשלה ויקצו תקציב ייעודי להגנת סייבר בשיעור שקבעה החלטת הממשלה; שיבצעו סקר בנושא הסיכונים הנשקפים למכשירים הרפואיים שהם משתמשים בהם ויגדירו קבוצות סיכון למכשור רפואי. על המבקרים הפנימיים במוסדות הרפואיים להכין תוכנית ביקורת פנים שתשלב בחינה של נושאים בתחום אבטחת המידע.

- על מנת להבטיח את היכולת של המוסדות הרפואיים לחזור, בהקדם האפשרי, לפעילות תקינה וסבירה במקרה של אירוע אסון, נדרש שהם יקדמו הקמה של אתר חלופי (DR)[9]. כמו כן מומלץ שהם ישלבו בתוכניות שלהם להמשכיות עסקית והתאוששות מאסון התייחסות לאופן הטיפול והשחזור של מערך המכשור הרפואי, בהתאם לתיעדוף של המכשירים על פי מידת חשיבותם במסגרת פעילות המוסד הרפואי.

- מומלץ שהמוסדות יוודאו שנוהל הרכש יתייחס להיבטי אבטחת מידע של מכשור רפואי, ובכלל זה - למעורבות בעלי תפקידים בתחום אבטחת מידע, עמידת המכשירים הרפואיים בתנאי סף שקבע המוסד הרפואי והבדיקות שיש לבצע מול הספק; על המוסדות הרפואיים שטרם עשו זאת לשלב את ממונה אבטחת המידע בשרשרת האישורים של מכשור רפואי חדש, ולהטמיע הליך זה בפעילות הרכש השוטפת שלהם; מומלץ גם שישלבו בדיקות מקיפות של המכשירים הרפואיים שהם רוכשים לפני השימוש בהם ושיקבעו גורם אחראי במוסד שיהיה אמון על ביצוע הבדיקות ועל תיעוד הביצוע.

- מומלץ שהמוסדות ישלימו את החוסרים שנמצאו אצלם במרכיבי ההגנה על מכשור

9 DR - Disaster Recovery - אתר חלופי זמין לטובת המשך פעילות מערכות המידע במקרה של אסון - נזק או השבתה של האתר המרכזי. אתר כזה יאפשר במקרה של אסון להעלות לשימוש באופן מהיר את מערכות המידע של המוסד הרפואי, לשחזר מידע על המטופלים ולהמשיך במתן השירותים הרפואיים.

רפואי; ישלימו גיבוש של נוהל המסדיר את תהליך עדכוני התוכנה במוסד הרפואי, שיתעדו את עדכוני הגרסאות שביצעו במערכות המחשוב לרבות במערך המכשור הרפואי; על המוסדות הרפואיים לשלב בתוכניות העבודה שלהם מבדקי חדירה עיתיים למכשור רפואי הן ברמת התשתית והן ברמת היישום, מומלץ שהמבדקים יבוצעו על בסיס סקר סיכונים שיאפשר לזהות את המכשירים הרפואיים החשופים לסיכון האבטחתי הגבוה ביותר; מומלץ גם שכל המוסדות הרפואיים ישפרו את מערך הבקרה הלוגית במערך מכשירי הדימות שלהם, ואם קיימת מגבלה להגדרת בקרה כזאת, מומלץ שיטמיעו בקרות מפצות בסביבת עבודה זו, על מנת לצמצם את הסיכונים הנלווים לשימוש במכשירים אלה.

- מומלץ כי המוסדות יוודאו כי טכנאים חיצוניים המבצעים עבודות תחזוקה במוסד הרפואי יגיעו רק לאחר תיאום עם הגורמים הרלוונטיים, וילוו כל העת בעובד המוסד; שיסדירו בנוהל את אופן ההתחברות מרחוק של הספקים ויטמיעו תהליכי בקרה על פעילות התחזוקה מרחוק; על המוסדות הרפואיים לנהל רישום מלא של כל המידע הנחוץ קודם להוצאת המכשירים הרפואיים לתחזוקה מחוץ למוסד, ובכלל זה עליהם לציין במסגרת הרישום אם המידע הרפואי השמור במכשירים נמחק לפני הוצאתם לתחזוקה ועם סיום השימוש בהם.

- למשרד הבריאות ולמערך הסייבר הלאומי מומלץ לשקול את הצורך לקבוע תקן מזערי ודרישות לגבי גודל צוות אבטחת המידע הרצוי במוסד רפואי בהתאם למאפייניו.

תהליך ההגנה על המכשירים הרפואיים "במעגל החיים" שלהם

סיכום

איומי הסייבר על מערכת הבריאות הולכים ומתרבים, הם ממשיים ואינם רק בגדר איום, ניסיונות תקיפה של פצחנים מתבצעים כל העת. תקיפות כאלה עלולות להוביל לשיבוש בפעילות השוטפת של המוסדות הרפואיים, לזליגה של מידע רפואי של מטופלים ולגרימת נזק למכשירים רפואיים חיוניים. ואולם לא מדובר רק בניסיונות תקיפה של פצחנים אלא גם בניסיונות מצד גורמים בעלי עניין שיש להם גישה למערכות ולמכשור ומעוניינים לפגוע בהם או לשבש את פעילותם. נוסף על כך, אף פעילות שגרתית ותמימה עלולה להביא לפגיעה במערכות המידע, במאגרי המידע ובמכשור רפואי. איומים אלה מחייבים את משרד הבריאות ואת הנהלות המוסדות הרפואיים לשים את הדגש הראוי על סיכוני אבטחת המידע הכרוכים בשימוש במכשירים רפואיים ועל הדרך הראויה להתמודדות עימם.

הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם

מבוא

בעשור האחרון גברו תקיפות הסייבר על ארגונים ועל אנשים פרטיים ברחבי העולם. על פי הערכות של חברות אבטחת מידע[10], מספר מתקפות הסייבר גדל ב-67% משנת 2014 עד 2019. בשנת 2020 זוהו ברחבי העולם כ-9.5 מיליון ניסיונות למתקפות סייבר שמטרתן הייתה להשבית מערכות מחשוב ולמנוע את היכולת להשתמש בהן[11], זוהתה מתקפה כל 18 דקות בממוצע; במחצית הראשונה של שנת 2020 נגנבו או זלגו לאינטרנט לפחות 36 מיליארד נתונים אישיים בעקבות מתקפות סייבר.

במרכזים רפואיים קיימות מערכות שהשבתתן עלולה להוביל לפגיעה בפעילות המרכז הרפואי ואף לסיכון חיי המטופלים. מערכות אלה כוללות את תשתיות המרכז הרפואי כגון תשתיות מים, חשמל וגז, תשתיות מערכות מידע ובפרט רשתות תקשורת, רשומות רפואיות וכן מכשור רפואי.

הגנת סייבר (להלן גם - אבטחת מידע) במכשור רפואי היא תהליך שמטרתו למנוע מגורם בלתי מורשה לבצע שינוי במידע שנאגר במכשירים הרפואיים; שימוש בלתי מורשה או שימוש לרעה במידע הרפואי שנאגר במכשיר הרפואי, מעובד בו או מועבר מהמכשיר הרפואי ליעד חיצוני[12]; ופגיעה בפעילות המכשיר הרפואי[13]. הגנת סייבר מתמקדת בשלושה מרכיבים שיש לשאוף אליהם (המכונים מרכיבי ה-"CIA"[14]):

- סודיות - הנתונים, המידע או מבנה המכשיר צריכים להיות נגישים רק לעובדים ולגורמים מורשים.
- שלמות ואמינות - הנתונים והמידע מדויקים ושלמים ולא בוצעו בהם שינויים.
- זמינות - הנתונים, המידע ומערכות המידע נגישים וזמינים בזמן ובמקום הנדרש.

איומי הסייבר הנשקפים למערכות המידע המודרניות גוברים והולכים. 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 בעקבות שינוי מידע

10 Varonis, "Cybersecurity Statistics and Trends for 2021", (16.3.21)

11 מתקפות מסוג Distributed Denial Of Service Attack - DDOS, התקפת מניעת שירות.

12 משרד הבריאות, נוהל מס' א-14.2 בנושא "מדיניות לאבטחת מידע והגנת סייבר במכשור רפואי" (6.5.18).

13 שם.

14 שילוב של שלושה מרכיבים יכול לסייע לגבש את מטרות אבטחת המידע של ארגון: Confidentiality, integrity and availability

בתיקים אישיים קליניים אשר יכול לגרום לקבלת החלטות רפואיות שגויות[15]; פגיעה והרס של מכשור רפואי יקר.

אבטחת המידע הרפואי היא בעלת חשיבות גבוהה, ועם התגברות האיומים על מערכות מבוססות מחשוב, נדרשים מוסדות במערכת הבריאות להגן על מערכות המחשוב הקריטיות שלהם על מנת להבטיח רצף טיפולי וניהולי כנדרש[16].

למרכזים הרפואיים ולקופות החולים (להלן בדוח זה - המוסדות הרפואיים או המוסדות) מאפיינים ייחודיים: מבנה הרשתות שלהם מורכב מאלפי מכשירים רפואיים שונים, חלקם ישנים מאוד או בעלי מערכות הפעלה מיושנות או לא מעודכנות[17] ולכן הם פגיעים לתקיפות סייבר; הם פועלים במתכונת חירום, בנסיבות שבהן הצלת חיי אדם חשובה יותר מכול וכללי אבטחת מידע הופכים לעיתים למשניים; המוסדות הרפואיים הללו נגישים לציבור, ובחלקם מבקרים בכל יום אלפי אנשים העוברים ליד מכשירים רפואיים ותשתיות מחשוב; הם אוגרים מידע רב, בכלל זה מידע רפואי אישי של מטופלים ומידע על מחקר רפואי המתבצע במוסד הרפואי. מידע זה הוא בעל ערך רב לפצחנים[18], לחברות מסחריות ולמדינות עוינות (למשל, מחיר רשומה רפואית בשנת 2021 מוערך ב-250 דולר - כ-800 ש"ח[19]); ולעיתים צוותים רפואיים אינם ערים לכללי השמירה על אבטחת המידע. כל אלה הופכים את המוסדות הרפואיים לפגיעים במיוחד בפני תקיפות סייבר לצורך גניבת מידע, שינוי מידע, סחיטה או פגיעה פיזית.

תקיפות סייבר במערכת הבריאות במדינות העולם[20]: בשנים האחרונות גברו האיומים על מוסדות רפואיים ברחבי העולם והתקיפות בהם (בייחוד תקיפות סחיטה), וחלקן אף הובילו לשיבוש בפעילותם של המוסדות, למשל, בשנת 2017 התרחשה תקיפה נרחבת בשם "WannaCry", והיא שיבשה את הפעילות בבתי חולים ומרפאות במערכת הבריאות בבריטניה; בשנת 2019 תקיפת סייבר שיתקה 6,000 מחשבים בבית חולים בצפון צרפת והצוות הרפואי נאלץ לעבור לעבוד ידנית; בשנת 2020 אירעה תקיפה בבית חולים בדיסלדורף בגרמניה ובה נפגעו מערכות המחשוב שלו, עקב כך מטופלת הועברה לבית חולים מרוחק יותר ונפטרה בשל העיכוב בטיפול; בצ'כיה דווח כי בשנת 2020 בית חולים שבו מעבדה גדולה לבדיקות קורונה הושבת בעקבות מתקפת סייבר בשיא המשבר[21]; בשנת 2021 פצחנים תקפו תשתיות מחשוב ברשת המחשבים של מערכת הבריאות באירלנד ושיבשו, בין היתר, את מערכות קביעת התורים, את פעילות המעבדות ואת מערכות המידע שבהן נשמרו ממצאי בדיקות רפואיות.

15 משרד הבריאות, חוזר מנכ"ל מס' 3/15 בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות" (15.2.15).

16 שם.

17 למשל, במחקר שפרסמה חברת האבטחה Forescout בשנת 2019 הובאו ממצאי מדגם של 75 מוסדות בריאות המשתמשים ביותר מ-1.5 מיליון מכשירים מחוברים - נמצא כי 59% ממכשירים אלה פועלים באמצעות תוכנת Windows, ומתוך אלה 71% פועלים באמצעות גרסאות תוכנה ישנות שכבר לא מתבצעים בהן עדכוני תוכנה ותחזוקה. Forescout Device Cloud Report, (15.5.19).

18 פצחן הוא אדם בעל ידע רב במחשבים ובמערכות ההפעלה שלהם, המסוגל לפצח קודים (מכונה באנגלית "האקר").

19 ראו אתר FIERCE Healthcare [קישור].

20 אירלנד: 'Cyber-attack on Irish health service 'catastrophic, BBC News (20.5.21), [קישור]; גרמניה: A Patient Dies After a Ransomware Attack Hits a Hospital, Wired (9.19.20), [קישור]; צרפת: Ransomware Attack: French Hospital Reverts to Pen and Paper, CISO MAG (25.11.19), [קישור].

21 מערך הסייבר הלאומי, **סיכום שנה 2020**.

בשל המתקפות הגוברות על מוסדות רפואיים בעולם כמה סוכנויות ממשל בארה"ב, ובהן ה-FBI (Federal Bureau of Investigation - לשכת החקירות הפדרלית בארה"ב), פרסמו באוקטובר 2020 הודעה[22] המתריעה על הרצון ההולך וגובר של פצחנים לתקוף את מגזר הבריאות ולפגוע בו.

גם בסיכום שנת 2020 של מערך הסייבר הלאומי במשרד ראש הממשלה[23] (להלן - מערך הסייבר הלאומי) צוין כי בשנה זו חל גידול ניכר בהיקף תקיפות הסייבר כנגד מוסדות רפואיים, מכוני מחקר ובתי חולים ברחבי העולם, וכי חלק מתקיפות אלה הובילו לשיבוש הפעילות הרציפה וכן לשיבוש בתפקודם של בתי החולים. עוד צוין בסיכום זה כי נדרש סיוע בהגנה מוגברת על מערכת הבריאות הישראלית בתקופת הקורונה, וכי חל בה גידול ניכר בניסיונות למתקפות עליה.

דוגמאות לתקיפות סייבר במערכת הבריאות בישראל: ביולי 2021 פצחנים שיתקו ושיבשו את פעילות אתרי האינטרנט (מרשתת) של המרכז הרפואי רמב"ם בחיפה ושל המרכז הרפואי הדסה בירושלים (וכן של גופים נוספים) במסגרת מתקפת סייבר; באמצע אוקטובר 2021 פרצו פצחנים למחשבים ושרתים במרכז הרפואי הלל יפה שבחדרה, נעלו את הגישה למחשבים שהכילו מידע ניהולי של המרכז הרפואי ומידע רפואי אישי של מטופלים. התקיפה הובילה לשיבוש פעילות המרכז הרפואי, וגרמה להסטת חולים מהמרכז הרפואי למרכזים אחרים, למעבר לעבודה ידנית ולא ממוחשבת, למניעת גישה למידע הרפואי של המטופלים ועוד. מערכות הדימות הממוחשבות, ובהן מכשירי רנטגן, MRI ו-CT המשיכו לפעול כרגיל, אך שגרת העבודה השתבשה מאוד, והפצחנים דרשו תשלום כופר כדי להפסיק את התקיפה. מערכות המרכז הרפואי חזרו לפעול בסוף נובמבר, יותר מחודש לאחר המתקפה.

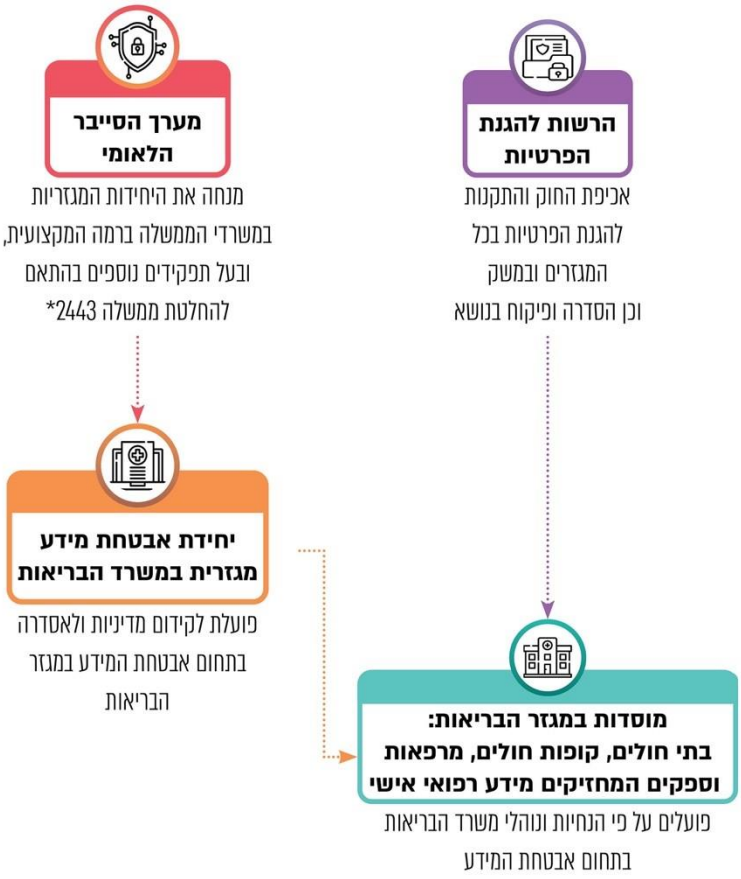
הגורמים האמונים על היבטי אבטחת מידע במערכת הבריאות: כמה גורמים אמונים על היבטי אבטחת המידע והסייבר במערכת הבריאות[24], והם יוצגו בתרשים שלהלן. אחריותו של כל גורם שהביקורת עסקה בו תובא בהמשך הדוח.

22 Joint Cybersecurity Advisory - Ransomware Activity Targeting the Healthcare and Public Health Sector, (28.10.20).

23 מערך הסייבר הלאומי, **סיכום שנה 2020**.

24 גורמים נוספים המעורבים בתחום אבטחת המידע במערכת הבריאות הם: היחידה להגנת הסייבר בממשלה (יה"ב) ברשות התקשוב הממשלתי במשרד הדיגיטל הנותנת הכוונה והנחיה מקצועית למשרדי הממשלה, ובהם משרד הבריאות, על מנת שמשרדים אלה יתגוננו בפני איומי סייבר, וכן שירות הביטחון הכללי (שב"כ) הנותן הכוונה בתחום הגנת הסייבר לגופים המוגדרים כתשתיות מדינה קריטיות (תמ"ק) - במגזר הבריאות למגן דוד אדום (מד"א).

תרשים 1: **הגורמים האמונים על היבטי אבטחת המידע והסייבר במערכת הבריאות**



* פירוט תפקידי מערך הסייבר מובאים להלן בתת-הפרק בנושא "מערך הסייבר הלאומי במשרד ראש הממשלה".

אבטחת מכשירים רפואיים והגנה עליהם: לצורך הפעילות הרפואית משתמשים המוסדות הרפואיים בעשרות אלפי מכשירים רפואיים למגוון רחב של פעולות רפואיות. בין המכשירים הללו: מכשירי דימות (מכשירי הדמיה לצרכים אבחנתיים ברפואה, ראו להלן), אק"ג (רישום הפעילות החשמלית של הלב), מכשירי הרדמה, ציוד מעבדה, מכונות הנשמה ולב-ריאה, מכשירי טיפול נמרץ לבוגרים ופגים, מכשירי רובוטיקה לניתוחים, משאבות עירוי ומכשירי דיאליזה. על מכשירים אלה להיות זמינים באופן מלא ובקביעות לנוכח מגוון הפעולות שיש לבצע באמצעותם ובייחוד לנוכח נחיצותם לתהליכים מצילי חיים; לצורך כך נדרשות אבטחה של המכשירים והגנה עליהם - הן הגנה פיזית והן הגנה לוגית (הגנה על מערכת המחשוב והמידע).

אחד האיומים על המכשירים הרפואיים הוא תקיפות של פצחנים. תקיפות כאלו עלולות להוביל לזליגה של מידע, לפגיעה במידע שנאגר במכשיר, לסילוף המידע במכשיר, ובמקרי קיצון - לפגיעה במכשיר שתוביל לשיתוקו ולהרס שלו. במהלך השנים אירעו בישראל לפחות שני אירועי תקיפה שפגעו במישרין או בעקיפין במכשור רפואי ובתפקודו.

נוכח אתגרי האבטחה של מכשירים רפואיים, בשנת 2021 מינה ה-FDA[25] לראשונה בעל תפקיד (מומחה בתחום הסייבר) לגורם האמון על אבטחת מידע בתחום המכשור הרפואי. באחריות אותו גורם לשפר את המודעות לסכנות הכרוכות במכשור רפואי ולקדם אסדרה (רגולציה) שתשפר את רמת האבטחה שלו, ובכלל זה - להתמודד עם חולשות כגון הגנה על מכשור ישן, צורך בעדכוני תוכנה ואבטחת המכשירים, הגנה מפני פרצות החשופות לאיומי סייבר שהיצרנים יצטרכו לספק ועוד[26].

דוח ביקורת זה בוחן את אבטחת המידע של מכשירים רפואיים תוך התמקדות במכשירי דימות כמקרה בוחן.

דימות רפואי הוא טכנולוגיה מתקדמת שבה מדגימים באמצעות תצלומים חלקים פנימיים בגוף הנבדק. זהו שם כולל למגוון בדיקות בסיסיות הנעשות לפני חלק ניכר מאבחונים ופעולות רפואיים, לצורך אבחון קליני, תכנון של הטיפול, מעקב אחר החולים וסיוע בביצוע פעילות פולשנית (ניתוחים)[27]. במכשירי הדימות נאגר מידע אישי על המטופלים הכולל את פרטיהם האישיים ואת תצלומי הדימות שבוצעו למטופלים שיכולים להעיד על ממצאים רפואיים. בביקורת נבדקה אבטחת המידע במכשירי הדימות האלה: רנטגן (X-RAY), טומוגרפיה ממוחשבת (CT[28]), דימות בתהודה מגנטית (MRI), ואולטרסאונד נשים.

חלק ממכשירי הדימות (בייחוד MRI ו-CT) הם מכשירים יקרים, בעלי משמעות אסטרטגית לבתי החולים, ופגיעה בהם עלולה לגרום נזק קשה בפעילות המוסד הרפואי. למשל, מחלקה לרפואה דחופה (מלר"ד) שאין ברשותה CT כשיר פעיל תתקשה לאבחן פגיעות מוח באופן מדויק (אחרי תאונות דרכים, בעת חשש לשבץ מוחי וכד').

פגיעה במכשירי דימות יכולה להוביל לפגיעה בתפקוד המכשיר ולזליגה של מידע רפואי ממנו, היא גם יכולה לשמש למתקפת סייבר נרחבת יותר. במסגרת פגיעה במכשירי הדימות עלול להתבצע, בין היתר, שינוי בממצאי הבדיקות של המטופלים. למשל, חוקרים ישראלים פרסמו בשנת 2019 מחקר[29] ובו הוכיחו כי בהינתן גישה לגורם בלתי מורשה למכשיר CT - אותו גורם יכול להסיר ממצאים מתצלום שהפיק המכשיר, או להוסיף ממצאים לתצלום זה; לדוגמה ניתן להוסיף גרורות סרטניות לתצלום של מטופל שאין לו גרורות כאלה, ולהפך.

להתקפות מסוג זה השלכות אפשריות רבות, ובהן פגיעה במטופלים בכלל ובמטופלים ספציפיים שהם בעמדות רגישות בפרט, פגיעה בפרטיות המטופלים, חשיפת מידע רפואי שלהם, מתן

25 Food and Drug Administration - מינהל המזון והתרופות של ארה"ב, הגוף הממשלתי האמון על הרגולציה והפיקוח של מוצרי מזון, ציוד רפואי, מוצרי קוסמטיקה ותרופות בארה"ב.

26 FDA wants to require timely updates, patches for legacy devices: cyber chief, MedtechDive, (30.6.21), [קישור].

27 ראו גם מבקר המדינה, **דוח שנתי 65ג** (2015), בפרק "בדיקות דימות מתקדמות", עמ' 609.

28 בכלל זה מכשירים מסוג PET-CT ו-SPETCT.

29 Mirsky, Mahler et al. ,CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning, 28th USENIX Security Symposium (11.1.19).

אבחנה רפואית שגויה, סחיטה כלכלית של המוסד הרפואי או של המטופלים, איומים עליהם, ביצוע מעילות והונאה מול חברות ביטוח, פעילות עבריינית ושיבוש בפעילות המכשיר הרפואי[30].

הביקורת נעשתה ב-25 מוסדות רפואיים: 11 מרכזים רפואיים כלליים-ממשלתיים; שמונת המרכזים הרפואיים הכלליים של שירותי בריאות כללית (להלן - הכללית); שני מרכזים רפואיים ציבוריים; וארבע קופות החולים. בסה"כ במוסדות שנבדקו יש כ-2,700 מכשירי דימות, כמוצג בתרשים שלהלן:

תרשים 2: **מספרם המשוער של מכשירי הדימות במוסדות הרפואיים שנבדקו, 2021**

על פי מענה של המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מדיניות ונהלים

תקן בין-לאומי ISO 27799: תקן International Standards Organization - ISO 27799 (להלן - תקן ISO) הוא תקן בין-לאומי לאבטחת מערכות מידע בתחום הבריאות, שפרסם ארגון התקינה הבינלאומי - ISO בסוף שנת 2010. התקן עוסק במגוון פעולות בתחום אבטחת המידע שיש לקבוע להן מדיניות לאבטחת מידע, לסיווג המידע על פי רמת רגישותו ולבקרות גישה למערכות המידע. מטרת תקן ISO היא לתת בידי מוסדות רפואיים כלים לצורך הגנה על המידע הרפואי שברשותם ולצורך התמודדות עם האתגרים הייחודיים של מערכת הבריאות כמו מספר המבקרים הגדול במוסדות, התקצוב החסר וניהול מאגרי מידע מרובים. משרד הבריאות אימץ תקן זה וחייב את המוסדות הרפואיים לעמוד בו החל מינואר 2014[31]. מהתשובות של המוסדות הרפואיים על שאלון אבטחת המידע, עלה כי בנובמבר 2021 (להלן - מועד סיום הביקורת) כל המוסדות הרפואיים שבהם עסק דוח זה עמדו בתקן.

30 המגמה העולמית הגוברת של פיתוח אמצעי רפואה אישיים שניתן לעשות בהם שימוש ביתי כוללת גם פיתוח של מכשירים רפואיים, לרבות מכשירי דימות. למשל, הכללית החלה להציע למבוטחיה בשנת 2021 את האפשרות לרכוש מכשיר אולטרסאונד ביתי עבור נשים בהריון, לבצע סקירה, ובאמצעות חיבורו לטלפון נייד חכם - להעביר את ממצאי הסקירה לפענוח לצורך קבלת אבחנה של רופא. מתוך אתר הכללית. [קישור], נדרש להגן גם על המידע המועבר באמצעות מכשירים אלה.

31 משרד הבריאות, חוזר מנכ"ל 18/12 בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות" (13.9.12). לחוזר זה פורסם נוסח מעודכן בשנת 2015. ראו להלן - חוזר מנכ"ל משרד הבריאות משנת 2015. הנוהל משנת 2012 הגדיר מוסד רפואי כבית חולים, קופת חולים ומרפאה.

חוק הגנת הפרטיות והתקנות: חוק הגנת הפרטיות, התשמ"א-1981, מסדיר כללים מרכזיים בתחום הפרטיות, ובין היתר, בנושאי פגיעה בפרטיות, הגנה על הפרטיות במאגרי מידע, ומסירת מידע או ידיעות מאת גופים ציבוריים. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות הגנת הפרטיות), קובעות כללים מנחים בתחום אבטחת המידע של מאגרי מידע ובפרט בנוגע למינוי ממונה על אבטחת מידע, קביעת נוהל אבטחה, מיפוי מערכות המאגר וביצוע סקר סיכונים, אבטחה פיזית וסביבתית וניהול הרשאות גישה. התקנות מסווגות מאגרי מידע לפי רמת האבטחה שלהם (בסיסית, בינונית או גבוהה) - מידע רפואי מסווג כמידע שחלה עליו רמת אבטחה בינונית, לכל הפחות[32]. הרשות להגנת הפרטיות במשרד המשפטים הוא הגוף המסדיר את תחום הגנת הפרטיות בישראל, המפקח עליו והמבצע אכיפה בנושא[33].

מערך הסייבר הלאומי במשרד ראש הממשלה: מערך הסייבר הלאומי שבמשרד ראש הממשלה הוא גוף האמון על הגנת מרחב הסייבר הלאומי ועל קידום ישראל בתחום. המערך פועל ברמת המדינה לשיפור רמת ההגנה על הארגונים והאזרחים, לטיפול בתקיפות סייבר ולסילוקן ולהיערכות לחירום, הוא משמש כגורם מנחה לארגונים בנושאים אלה. המערך פועל מתוקף החלטות הממשלה[34], וכן מתוקף החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998. למערך כמה תפקידים, ובהם[35]:

- להוביל את מאמצי ההגנה על מרחב הסייבר הלאומי.
- לקדם את יכולת הציבור והמשק הישראלי להיערך לקראת איומי סייבר ולהתגונן מפניהם באמצעות הטמעת טכנולוגיות מתקדמות, הכוונה, פיתוח כוח אדם מיומן והגברת המודעות לנושא.
- לבסס ולחזק את בניין הכוח המדעי-טכנולוגי בתחום הסייבר, בין היתר באמצעות עידוד מחקר אקדמי מתקדם וקידום מחקר ופיתוח טכנולוגי חדשני.
- לקדם את מדינת ישראל למעמד של מובילה עולמית בתחום הסייבר באמצעות שיתופי פעולה בין-לאומיים, סיוע למדינות והובלת תהליכים גלובליים.
- לקדם אסטרטגיה ומדיניות בתחום הסייבר בזירות הלאומית והבין-לאומית ולשמש מוקד ידע, סמכות מקצועית מרכזית בתחום וגוף מייעץ לראש הממשלה ולממשלה כולה.

מערך הסייבר הלאומי מנחה מהבחינה המקצועית את היחידות המגזריות במשרדי ממשלה (כגון משרד הבריאות ומשרד התחבורה) שאחראיות במישור האסדרתי בתחום הסייבר מתוקף

32 בהתאם לתנאים שנקבעו בתוספת הראשונה והשנייה לתקנות.

33 אתר המרשתת של הרשות להגנת הפרטיות במשרד המשפטים [קישור]. החלטת הממשלה 4660 "הקמת רשות משפטית לטכנולוגיות מידע והגנה על הפרטיות במשרד המשפטים" (19.1.2006); החלטת הממשלה 3019, "שינוי שם הרשות למשפט טכנולוגיה ומידע במשרד המשפטים" (7.9.2017).

34 החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15); החלטת הממשלה 3270, "1. איחוד יחידות מערך הסייבר הלאומי 2. מתן פטור ממכרז למשרת ראש מערך הסייבר הלאומי 3. הוספת משרת ראש מערך הסייבר הלאומי לתוספת לפי סעיף 23 לחוק שירות המדינה (מינויים) 4. קביעת שכר ותנאי שירות של ראש מערך הסייבר הלאומי" (17.12.17); והחלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15). תאריך עדכון ההחלטה - 28.7.15.

35 תפקידי מערך הסייבר הובאו מאתר המרשתת של מערך הסייבר, [קישור].

תפקידם כרגולטורים, מכוח החלטת ממשלה 2443 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (להלן- החלטת הממשלה 2443 בנושא הגנת הסייבר), על יחידות משנה אחרות ומנחה גופים המוגדרים בעלי תשתית מדינה קריטית (תמ"ק)[36], כגון חברת החשמל, מד"א, בנק ישראל ורשות שדות התעופה.

באפריל 2018 פרסם מערך הסייבר הלאומי את "תורת ההגנה בסייבר לארגון גרסה 1.0" (להלן - תורת ההגנה בסייבר או תורת ההגנה). מטרת תורת ההגנה היא למזער את סיכוני הסייבר במשק הישראלי באמצעות מתודה סדורה של פעולות המשפרות את ההגנה על הארגון. התורה כוללת המלצות כגון נוהגים מקובלים ("Best Practice") בעולם אבטחת המידע, המוצעים לארגונים במשק הישראלי, שיישומם ישפר את רמת האבטחה של הארגון בפני תקיפות. ביוני 2021 עדכן מערך הסייבר הלאומי את תורת ההגנה[37] (להלן - תורת ההגנה המעודכנת). בגרסה המעודכנת הטמיע מערך הסייבר הלאומי תובנות שעלו במסגרת תהליכי ביקורות קודמים שעשה, והוטמעו בגרסה זו כלים שעל בסיסם יכול הארגון לגבש תפיסה פרטנית המותאמת במיוחד לו, הושם דגש רב יותר על הבנת ה"יריב" שבגינו נשקף סיכון לארגון, וכן עודכנה התורה בהתאם לעדכון מונחים וטכנולוגיות אשר נמצאים בחזית המחקרים בנושא. דוח ביקורת זה עוסק בעיקר בגרסה הראשונה של תורת ההגנה, זו שעמדה לרשות המוסדות הרפואיים במהלך הביקורת, ובמידת הצורך מובאת גם התייחסות לגרסה המעודכנת. מלבד תורת ההגנה, פרסם מערך הסייבר בשנת 2020 גם המלצות להגנה על מכשור רפואי[38] (להלן - המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי).

משרד הבריאות: החל בשנת 2016 פועלת במשרד הבריאות יחידת סייבר מגזרית (להלן - יחידת הסייבר במשרד הבריאות או היחידה), שבכל הנוגע לתחום הגנת מרחב הסייבר, הגוף המנחה אותה הוא מערך הסייבר הלאומי. במשך השנים פרסם משרד הבריאות (להלן גם - המשרד) חוזרים ונהלים בתחום אבטחת המידע. שני מסמכים עיקריים הם חוזר מנכ"ל משנת 2015 בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות"[39] (להלן - חוזר מנכ"ל משרד הבריאות משנת 2015) ונוהל "מדיניות לאבטחת מידע והגנת סייבר במכשור רפואי" שאישר אגף מערכות מידע ומחשוב במשרד הבריאות בשנת 2018[40].

פעולות הביקורת

בחודשים ינואר-נובמבר 2021 בדק משרד מבקר המדינה את הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם, תוך התמקדות במכשירי דימות (MRI, CT, רנטגן ואולטרסאונד נשים). הנושאים שנבדקו: הפעילות המינהלית בתחום אבטחת המידע במוסדות הרפואיים; ההגנה על המכשירים בכל מעגל החיים שלהם: בתהליך רכישתם, במהלך השימוש בהם (בכלל זה מיפוי מערך המכשור הרפואי, הגנה על המכשירים ברשת המוסד הרפואי, הרשאות הגישה למכשירים, ניהול המשתמשים, אבטחת מידע בעת פענוח ממצאי הסריקות), ובעת סיום השימוש

36 גופי תמ"ק הם גופים בעלי מערכות ממוחשבות חיוניות למדינה.

37 מערך הסייבר הלאומי, **תורת ההגנה 2.0**: "לנהל את הסיכון - המדריך היישומי (השלם) להגנת הסייבר של הארגון" (יוני 2021).

38 מערך הסייבר הלאומי, "המלצות הגנה רכיבי מכשור רפואי מבוססי IoMT" (אוקטובר 2020).

39 משרד הבריאות, חוזר מנכ"ל מספר 3/15 בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות" (15.2.15).

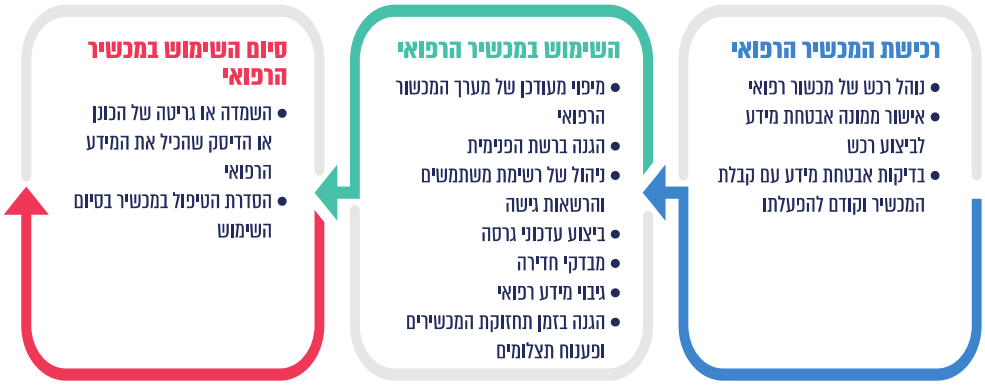
40 משרד הבריאות, נוהל מס' א-14.2 בנושא "מדיניות לאבטחת מידע והגנת סייבר במכשור רפואי" (6.5.18).

בהם; ההגנה על המידע הרפואי עצמו שנאגר במכשירים; ודרכי התחזוקה של המכשירים. הביקורת בוצעה במשרד הבריאות, ב-25 מוסדות רפואיים: בארבע קופות החולים, בכל המרכזים הרפואיים הכלליים-ממשלתיים והממשלתיים-עירוניים - 11 מרכזים רפואיים, בשמונת המרכזים הרפואיים הכלליים של הכללית, ובשני מרכזים רפואיים ציבוריים - המרכז הרפואי הדסה והמרכז הרפואי אסותא אשדוד. בדיקות השלמה בוצעו במערך הסייבר הלאומי, ברשות להגנת הפרטיות במשרד המשפטים וב"ענבל חברה לביטוח בע"מ", שהיא חברה ממשלתית לביטוח.

הביקורת כללה ביצוע סקרי אבטחה במוסדות הרפואיים ובהם בחנה באמצעות תשאול את מדיניות האבטחה במוסדות הרפואיים ואת אופן ההגנה על התהליכים העסקיים ועל נכסי המידע בהם, זאת בהתאם לתקני אבטחת מידע, לנהלים בתחום ולנוהגים מקובלים ("Best Practice"). הביקורת כללה גם ביצוע מבדק תאימות במוסדות הרפואיים ובו בחנה באמצעות תשאול האם המוסדות עומדים בעקרונות העיקריים של הגנת סייבר והעלתה את הפערים שנמצאו. במסגרת הביקורת נשלח שאלון ל-25 המוסדות הרפואיים; הכללית השיבה בנוגע לרוב הפרקים שבשאלון בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה, ולכן מספר המוסדות שבהם עוסקים פרקים אלה הוא 17.

ראו בתרשים שלהלן את תהליך ההגנה על המכשירים הרפואיים בכל מעגל החיים שלהם כפי שנבדק בביקורת:

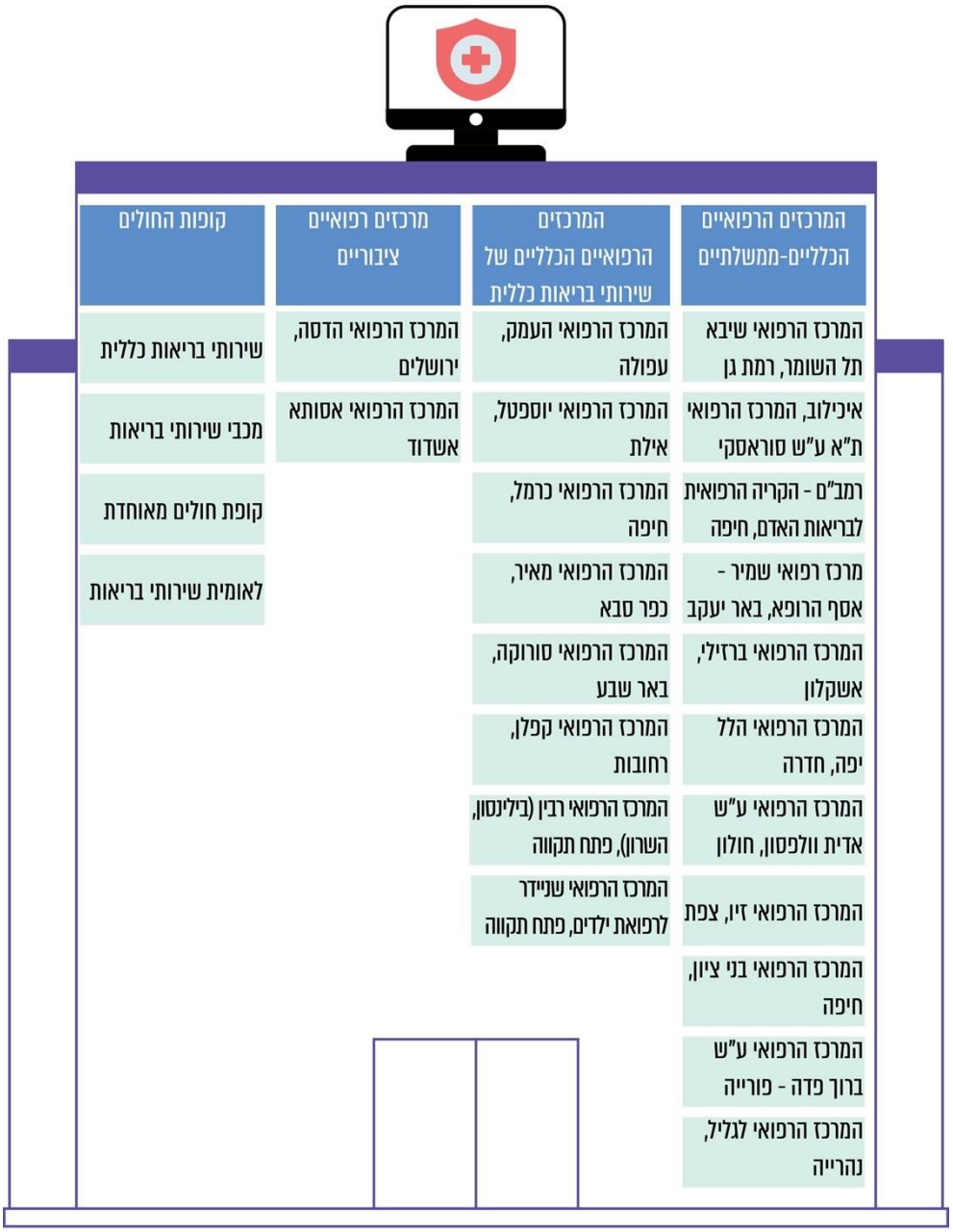
תרשים 3: **תהליך ההגנה על המכשירים הרפואיים בכל מעגל החיים שלהם כפי שנבדק בביקורת**



כמו כן, במסגרת הבדיקה הפנה משרד מבקר המדינה שאלון בנושא "הגנה ואבטחה של מידע במכשירים רפואיים" (להלן - שאלון אבטחת המידע) לכל 25 המוסדות הרפואיים שנכללו בביקורת. כל המוסדות הרפואיים השיבו על השאלון[41]. להלן הפירוט:

41 יש לציין כי במחוזות של הכללית, במכבי שירותי בריאות ובקופת חולים לאומית אין משתמשים במכשירי MRI ו-CT אלא רק במכשירי אולטרסאונד ורנטגן, וכך ציינו הקופות בתשובותיהן על השאלון. המענה של המוסדות הרפואיים מתייחס גם להשלמות שביקש צוות הביקורת על מידע שלא נכלל בשאלונים.

תרשים 4: **המוסדות הרפואיים שנבדקו בביקורת**



דוח זה הומצא לראש הממשלה ביום 15.2.22 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה. מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היוועצות עם

הגופים האמונים על אבטחת המידע הביטחוני ובתאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו על שולחן הכנסת ולא יפורסמו. ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאת הדוח כאמור לעיל.

האחריות לתחום הגנת הסייבר

אחריות מערך הסייבר הלאומי

בשנת 2015 החליטה הממשלה לקדם אסדרה לאומית בהגנת הסייבר[42] (להלן - החלטת ממשלה בנושא הגנת הסייבר). מטרת ההחלטה הייתה להעלות באופן שיטתי ורציף את רמת הגנת הסייבר במדינת ישראל באמצעות מימוש סטנדרטים מקצועיים בארגונים, וכן באמצעות הסדרה של שוק שירותי הגנת הסייבר (אנשי מקצוע, שירותים ומוצרים) במגוון כלים. בהחלטת הממשלה נקבע כי על משרדי הממשלה לקדם את הטיפול בהיערכות לאיומי סייבר במגזר שבו הם פועלים על ידי קידום הגדרת מדיניות ודרישות האסדרה ליישום החלטת הממשלה במגזר שהם אחראים לו, ובאמצעות הקמת יחידה מגזרית להכוונה מקצועית בתחום הגנת הסייבר בכל משרד, שתפקידיה יהיו, בין היתר, להגדיר מדיניות ונהלים בתחום, להכווין, להנחות, ללוות במישור המקצועי ולתת מענה על פניות מקצועיות של המוסדות הכפופים ליחידה (להלן - יחידה מגזרית); לבצע בקרות על מידת עמידתם של המוסדות בדרישות המקצועיות של היחידה ולבחון את הפערים הקיימים במוסדות; לבנות ולהפעיל תהליכי שיתוף מידע פנימיים וחיצוניים בתוך המגזר, וכן להגדיר את נוהלי הדיווח ואת שיטות הדיווח בין הגופים במגזר; ליזום ולממש פעילות נרחבת שתכליתה לשפר את הגנת הסייבר במגזר.

החלטת הממשלה בנושא הגנת הסייבר הובילה להקמה של יחידות מגזריות במשרדי ממשלה בתחום הסייבר, ואלה פועלות בהכוונת מערך הסייבר הלאומי ומוסרות דיווח על תכנון פעולותיהן לעומת ביצוען.

סמכויות מערך הסייבר הלאומי: בדוח קודם של מבקר המדינה בנושא "היערכות גופים חיוניים להגנת הסייבר"[43] צוין כי לא הוסדרו בחקיקה סמכויות עובדי מערך הסייבר הלאומי הפועל מתוקף החלטות הממשלה (ראו לעיל) כלפי היחידות המגזריות במשרדי הממשלה והארגונים הכפופים לאחריות המערך, וכן היבטים תפעוליים בעבודתם מול גופים אלו. עוד צוין כי היעדר מקור נורמטיבי לסמכות עובדי המערך עלול להקשות את שיתוף הפעולה עם הגופים ולגרום להימנעותם של עובדי המערך מביצוע פעולות מסוימות עקב חוסר בהירות בעניין תחומי הסמכות.

עוד צוין בדוח כי בשנת 2018 הכין מערך הסייבר הלאומי תזכיר של חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018. כשלוש שנים לאחר מכן, בשנת 2021, הוגש תזכיר הצעת חוק: הגנת הסייבר ומערך הסייבר הלאומי (סמכויות לצורך חיזוק הגנת הסייבר) (הוראת שעה), התשפ"א-2021[44]. נכון למועד סיום הביקורת תזכיר החוק נמצא בשלב טיוטת הצעת חוק.

---

42 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15). תאריך עדכון ההחלטה - 28.7.15.

43 מבקר המדינה, **דוח שנתי 69ב** (2019), "היערכות גופים חיוניים להגנת הסייבר", עמ' 2067.

44 הפורטל המשפטי לאינטרנט, סייבר וטכנולוגיית מידע [קישור].

עלה כי במועד סיום הביקורת, כשש שנים לאחר קבלתן של החלטת הממשלה 2443 בנושא הגנת הסייבר והחלטת הממשלה 2444 בנושא "קידום ההיערכות הלאומית להגנת הסייבר" (בשנת 2015), ועל אף החשיבות הלאומית שבהסדרת הגנת הסייבר, לא הוסדרו סמכויות מערך הסייבר הלאומי כלפי היחידות המגזריות במשרדי הממשלה, ובכללן במגזר הבריאות.

אחריות היחידה המגזרית לאבטחת מידע: החלטת הממשלה 2443 בנושא הגנת הסייבר הגדירה את אחריות היחידות המגזריות במשרדים הממשלתיים.

מבקר המדינה כבר העיר בדוח הקודם בנושא "היערכות גופים חיוניים להגנת הסייבר", שפעילות ההנחיה על ידי היחידות מבוססת על סמכויות האסדרה הקיימות בכל משרד ומשרד, אשר מטבען שונות בכל אחד מהמשרדים ומשפיעות גם על אפשרויות הבקרה, הפיקוח והאכיפה של יחידות ההכוונה המגזרית. מבקר המדינה הוסיף כי בהיעדר תשתית משפטית מספקת לביסוס הנחיה מגזרית על ידי משרדי הממשלה מתעורר קושי למלא את החלטות הממשלה[45].

מבקר המדינה המליץ בדוח הקודם משנת 2019 כי על מערך הסייבר הלאומי בשיתוף משרד המשפטים ומשרד ראש הממשלה לקדם תהליך חקיקה שיאפשר לטפל בבעיות האסדרה הקיימות בנושא סמכויות עובדי מערך הסייבר הלאומי והפער בין סמכויות המאסדרים[46].

מערך הסייבר הלאומי מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תשובת מערך הסייבר), כי אף שטרם הוסדרה סמכותו בחקיקה ראשית, המערך פועל במגוון דרכים כדי לקדם את רמת הגנת הסייבר במשק הישראלי, ועובד בשיתוף היחידה המגזרית במשרד הממשלתי הרלוונטי בתחום הגנת הסייבר, באופן שהמערך הוא המנחה המקצועי והמשרד הממשלתי הוא בעל הסמכות. המערך הוסיף כי באוקטובר 2021 הוא עשה עבודת מטה מול כל משרדי הממשלה והמאסדרים הרלוונטיים בנוגע לסמכויות האסדרה שלהם בתחום הגנת הסייבר.

מבקר המדינה ממליץ למערך הסייבר לקדם את תהליך האסדרה של סמכויות מערך הסייבר הלאומי כלפי היחידות המגזריות במשרדי הממשלה, ובכללן כלפי מגזר הבריאות, ושל הפער בין סמכויות המאסדרים.

45 מבקר המדינה, **דוח שנתי 69ב** (2019), "היערכות גופים חיוניים להגנת הסייבר", עמ' 2067.

46 שם.

אחריות משרד הבריאות בתחום אבטחת המידע והגנת סייבר

משרד הבריאות נושא בריבוי כובעים - מחד גיסא הוא המאסדר של תחום שירותי הבריאות בישראל, ומאידך גיסא הוא גם הבעלים, המבטח והמפעיל של מרבית שירותי הבריאות בישראל[47]: הוא המאסדר של כלל מערכת הבריאות, ובה בעת הוא הגורם המבטח בתחומים שונים המפורטים במסגרת התוספת השלישית לחוק ביטוח בריאות ממלכתי, התשנ"ד-1994[48]. כמו כן, הוא אחראי לאספקת שירותי בריאות באמצעות הפעלת 24 המרכזים הרפואיים הממשלתיים שהוא בעליהם, באמצעות מאות תחנות לבריאות המשפחה (טיפות חלב) ועוד.

בהיותו המאסדר של מערכת הבריאות הוא המנחה את המוסדות הרפואיים בכל הנוגע לתחום אבטחת המידע והגנת סייבר. לצורך כך גיבש המשרד חוזרים ונהלים ובהם הנחיות לאופן שבו על המוסדות הרפואיים לפעול כדי להבטיח את הגנת מערכות המידע שלהם והמידע השמור בהם. עליו גם להנחותם בכל הנוגע להגנת סייבר בהתאם להמלצות מערך הסייבר הלאומי. המשרד גם מקיים בקרה ומעקב בעניין יישום הנחיותיו בכלל[49], ובעניין ההנחיות המסדירות את תחום אבטחת המידע והגנת סייבר בפרט, בכל המוסדות הרפואיים במערכת הבריאות[50].

חוזרים ונהלים במשרד הבריאות: לצד הקמת יחידת הסייבר במשרד הבריאות, קידם משרד הבריאות את תחום אבטחת המידע באמצעות חוזרים ונהלים החלים על כלל המוסדות הרפואיים במגזר הרפואי: נוהלי המשרד וחוזרי המנכ"ל הם בגדר הנחיות מחייבות כלפי המוסדות הרפואיים, ועל המשרד לפקח על יישומם.

- בשנת 2012 פרסם משרד הבריאות חוזר מנכ"ל בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות"[51]. החוזר הנחה את המוסדות הרפואיים בישראל לפעול לאבטח את המידע שברשותם, ובכלל זה באמצעות הקמת ועדת היגוי בתחום אבטחת המידע, פעילות להסמכה לתקן אבטחת מידע למוסדות רפואיים, רישום מאגרי מידע, שיפור הכלים הטכנולוגיים למימוש הגנה על המידע, הגדרות משתמשים במערכות, הזמינות הנדרשת של המערכות ואופן הטיפול במשברים.
- בשנת 2015 פרסם משרד הבריאות נוסח מעודכן לחוזר באותו נושא (חוזר מנכ"ל משרד הבריאות משנת 2015). החוזרים נבדלים ביניהם מבחינת מידת עמידתם של ספקים חיצוניים של מוסד רפואי בתקני ISO לאבטחת מידע: החוזר משנת 2012 המליץ לתת עדיפות לספקים העומדים בתקן, ואילו חוזר מנכ"ל משרד הבריאות משנת 2015 מחייב את

47 מבקר המדינה, **דוח שנתי 70ב** (2020), "מעמדו המעורב של משרד הבריאות כמאסדר וכבעלים של בתי חולים ממשלתיים", עמ' 899.

48 ובהם אשפוז סיעודי, שירותי רפואה מונעת, סל שירותים בתחום בריאות הנפש והשתתפות במימון רכישת מכשירי שיקום.

49 למשל, במסגרת בקרות הרישוי של המשרד הוא עושה בקרות, בין היתר, בנושאים האלה: תהליכים בניהול הרפואי, היבטים באיכות הטיפול, זכויות החולה, רשומות, בטיחות העובד והמטופל, עמידה בנהלים, תשתיות הנדסיות, תנאי מבנים, תברואה ואבטחת מידע.

50 מרכזים רפואיים: ממשלתיים, ציבוריים, של קופות החולים, פרטיים; קופות החולים; מרפאות וכו'.

51 משרד הבריאות, חוזר מנכ"ל מס' 18/12 בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות" (13.9.12).

המוסדות הרפואיים להתקשר רק עם ספקים העומדים בתקן החל מינואר 2016 (ראו בהרחבה להלן בפרק "אבטחת מידע אצל ספקים חיצוניים המבצעים בדיקות דימות"). בחוזר הנחה המשרד את מנהלי המוסדות הרפואיים להטמיע בנהלים פנימיים את עקרונות החוזר.

- בשנת 2018 פרסם המשרד נוהל "מדיניות לאבטחת מידע והגנת סייבר במכשור רפואי" (להלן - נוהל מכשור רפואי של משרד הבריאות משנת 2018). הנוהל כולל הנחיות מקיפות בדבר הגדרות אבטחת המידע של המכשור הרפואי במוסדות הרפואיים. הוא קובע כי האחריות ליישום דרישות האבטחה המצוינות בו חלה על המוסדות הרפואיים המפעילים מכשור רפואי ועל משתמשים פרטיים של מכשור רפואי. הנוהל אף מגדיר דרישות אבטחת מידע שיצרני המכשור הרפואי צריכים לבחון אם קיימים במכשיריהם.
- כמו כן, משרד הבריאות הכין בסוף שנת 2016 שתי טבלאות אקסל[52] המשמשות לניהול מכשור רפואי, והעביר טבלאות אלה בשנת 2017 למוסדות רפואיים, ככלי עבודה אפשרי.

לנוכח קצב התפתחות הטכנולוגיה והחמרת איומי הסייבר, גיבש משרד הבריאות בשנים 2017 - 2020 מסמכי הנחיות מקיפים יותר, ולהלן יפורטו העיקריים שבהם:

- "פק"ל אבטחת מידע וסייבר - היערכות וניהול משבר סייבר" (2019), ובהם הנחיות המתארות כיצד על ארגון בריאות[53] להתמודד עם אירוע סייבר שהתממש ובתוצאותיו, בכלל זה פגיעה במכשור רפואי.
- טיוטת "תורת הגנה ארגונית - אבטחת מידע וסייבר במגזר הבריאות" (2018), הכוללת כללים למימוש תורת הגנה במגזר הבריאות, בקרות שיש להטמיע, דרכים שבהן ארגון צריך להתכונן לאירוע סייבר, הגברת מודעות העובדים לסיכוני אבטחת מידע וסייבר, מדריך לתרגול סייבר עצמי, ועוד. הטיוטה כוללת גם פרק בנושא אבטחה של מכשור רפואי.
- טיוטת חוזר מנכ"ל מורחב בשם "רגולציית יסוד להגנת סייבר במערכת הבריאות בישראל" (2020) (להלן - טיוטת חוזר מנכ"ל בנושא רגולציית יסוד), הכוללת הנחיות למוסדות הרפואיים, ובכלל זה עקרונות יסוד לניהול הגנת סייבר, ממשל תאגידי ובעלי תפקידים נדרשים, מסגרת לניהול סיכוני סייבר, יעדי בקרה ובקרות הגנת סייבר וכללים להגנה על הפרטיות.

נכון למועד סיום הביקורת משרד הבריאות לא השלים את גיבוש מסמכי ההנחיות, והם לא הופצו, אף שמדובר בהנחיות יסוד החיוניות לשם הגנה על תשתיות, מכשור ומידע במערכת הבריאות, ואף שההנחיות כוללות כלים להתמודדות עם אירועי סייבר שהמציאות מוכיחה את היתכנותם.

52 טבלה אחת היא רשימה המשמשת למיפוי המכשור הרפואי במוסד הרפואי, והטבלה השנייה מציגה תמונת מצב של חולשות וחוזקות של המכשור הרפואי על פי מדדים בחמש קטגוריות שונות: ניהול, הגנה, זיהוי, תגובה והתאוששות.

53 ארגון בריאות הוא מוסד רפואי הנותן שירותי בריאות, והוא אחד מאלה: משרד הבריאות ויחידות הסמך שלו, קופת חולים ומוסדותיה, בית חולים (ציבורי או פרטי), בית מרקחת, ארגוני פינוי והצלה ומרפאות או ארגונים אחרים החייבים ברישוי של משרד הבריאות.

נוכח האיומים הגוברים על מגזר הבריאות בתחום אבטחת המידע ובכלל בנושא הגנה מפני תקיפות סייבר והתמודדות איתן, מומלץ שמשרד הבריאות ישלים את גיבוש הנהלים ויפרסם אותם למוסדות הרפואיים.

משרד הבריאות מסר בתגובתו למשרד מבקר המדינה מינואר 2022 (להלן - תגובת משרד הבריאות) כי הנהלת המשרד אישרה לפרסם את טיוטת חוזר המנכ"ל בנושא רגולציית יסוד והיא כוללת, בין היתר, את התכנים המופיעים בטיוטות הנהלים האחרות שגיבש המשרד. המשרד הוסיף כי פרסום הנוהל הסופי מתוכנן בטווח הזמן המיידי.

מומלץ שהמשרד יוודא כי המוסדות הרפואיים מטמיעים את הנהלים באופן שהם יתווספו לארגז הכלים העומד לרשותם לצורך התמודדות עם אתגרי הסייבר.

בקרות של משרד הבריאות בנושא אבטחת מידע בכלל ואבטחת מידע במכשור רפואי בפרט

בקרות רישוי

בהתאם לפקודת בריאות העם 1940, ולתקנות בריאות העם (רישום בתי חולים), התשכ"ו-1966, מוסדות רפואיים חייבים באישור מראש ממשרד הבריאות קודם להקמתם, וכן חייבים באישור לפתיחתם, ניהולם והפעלתם (אישור רישום או אישור רישוי)[54]. משרד הבריאות מבצע אחת לשלוש שנים לערך בקרות בבתי החולים בנושאים שונים על מנת להמליץ על המשך פעילות וחידוש רישוי של בתי החולים (להלן - בקרות הרישוי)[55]. בקרות דומות מבצע משרד הבריאות במחוזות של קופות החולים. המשרד מפרסם את דוחות הבקרה הסופיים באתר המרשתת שלו. בדוח קודם של מבקר המדינה על "היבטים בהגנה על הפרטיות במאגרי מידע" הוא עמד על הצורך שמשרד הבריאות יגבש תוכנית לפיקוח ובקרה גם על אבטחת המידע בכל המוסדות הרפואיים[56].

במסגרת בקרות הרישוי התקופתיות שמבצע המשרד בבתי החולים[57], הוא גיבש בשנת 2018 שני מסמכי בקרות העוסקים בתחום אבטחת המידע בבתי החולים ובתחום המכשור הרפואי לצורך שילובם ברשימת הנושאים שייבדקו בעת ביצוע בקרות הרישוי.

מסמך הבקרה בנושא אבטחת מידע בבתי החולים בוחן, בין היתר, את מעורבות ההנהלה בתחום זה, את המודעות לצורך באבטחת מידע, בקרות על האבטחה הפיזית, בקרות על הגישה, הפרדת רשתות, ניהול סיכונים, זיהוי פעילויות ואירועים חריגים ברשת (אנומליות), זיהוי גורמים חיצוניים

54 אתר משרד הבריאות, "רישוי בתי חולים כלליים". [קישור].

55 אתר משרד הבריאות, "חידוש רישוי של בית חולים כללי פעיל". [קישור].

56 מבקר המדינה, **דוח שנתי 69ב** (2019), "היבטים בהגנה על הפרטיות במאגרי מידע", עמ' 5.

57 יש לציין שבמסגרת תקן האקרדיטציה (JCI) - תקן בין-לאומי לאיכות ובטיחות לארגוני בריאות - שניתן לבתי החולים, נבחנים מדדים של ניהול מידע כללי והשמירה עליו. בקרות הרישוי של משרד הבריאות מתבצעות נוסף על הליך האקרדיטציה, ובודקות באופן מעמיק תהליכי אבטחת מידע והיבטים במכשור רפואי.

המתחברים מרחוק, מערך של הגיבויים והשחזורים, ניהול אירועי סייבר וטיפול בהם ותוכנית התאוששות מאסון.

מסמך הבקרה בנושא מכשור רפואי בבתי החולים בוחן, בין היתר, נושאים אלה: ניהול בדיקות הציוד והטיפולים בו, השירות והתחזוקה של הציוד במוסד הרפואי, השירות והתחזוקה שמספקים הספקים, הרשאות הגישה לתוכנת התחזוקה, תיעוד החזרות של הציוד ואירועים חריגים בציוד רפואי.

צוות הביקורת בדק 14 בקרות שביצע משרד הבריאות בשנים 2019 ו-2020 בבתי חולים (כלליים-ממשלתיים, ציבוריים, פרטיים, וכלליים של הכללית), וכן 15 בקרות שביצע המשרד במחוזות של קופות החולים[58].

בביקורת עלה כי בבקרות שביצע המשרד בבתי החולים ובקופות החולים בשנים 2019 ו-2020 שאותן בדק צוות הביקורת, המשרד ביצע בקרה בנושא אבטחת מידע[59], אולם במסגרת הבקרות האמורות הוא לא ביצע בקרה בנושא מכשור רפואי, בהתאם למסמך הבקרה שגיבש בשנת 2018.

מנהלת המחלקה לבקרה רפואית במשרד הבריאות מסרה לצוות הביקורת כי החל משנת 2021 המשרד משלב בקרות בתחום אבטחת המידע ובתחום המכשור הרפואי כחלק בלתי נפרד מהבקרות שהוא מבצע בבתי החולים.

אשר לתיקון הליקויים שהועלו בבקרות הרישוי ציינה מנהלת המחלקה לבקרה רפואית כי במשך השנים לא ביצע המשרד מעקב מסודר אחר תיקון הליקויים בבתי החולים, וכי הרישיון לבתי החולים ניתן גם בלא שהדבר נבדק. מנהלת המחלקה הוסיפה כי החל במאי 2021 המחלקה מגבירה את מאמציה לבצע מעקב אחר תיקון הליקויים כתנאי לקבלת רישיון, במסגרת מדיניות חדשה שהמחלקה מטמיעה באופן הדרגתי.

מנהלת המחלקה לבקרות על קופות החולים במשרד הבריאות מסרה לצוות הביקורת כי לפי עמדת המשרד, האחריות לתיקון הליקויים מוטלת על הקופה, וגם במקרים של ליקויים לתיקון מיידי הקופה היא שנדרשת להתייחס לליקוי ולוודא שהוא תוקן.

עולה מכך שהמשרד כמאסדר אינו מבצע מעקב סדור אחר תיקון ליקויים שהועלו בדוחות הבקרה, ובכך לא מוודא את אי-הישנותם, לשם צמצום סיכוני הסייבר שאליהם חשופים המוסדות.

58 את הבקרות בקופות החולים ביצע האגף לרפואה קהילתית במשרד הבריאות. האגף הוקם בשנת 2008 ומופקד, בין היתר, על בקרה על הפעילות ועל קביעת הסטנדרטים של השירותים הרפואיים שנותנות קופות החולים בקהילה.

59 הבקרות העלו ליקויים בתחום אבטחת המידע ובהם חוסר הפרדה בין מכשירים רפואיים לבין יתר הרשת, בעיות הרשאות של משתמשים, היעדר סקירת סיכונים וליקויים ביכולת להתאושש מאסון.

מומלץ כי משרד הבריאות ישלב באופן סדור בבקרות שהוא מבצע במרכזים הרפואיים ובקופות החולים בדיקה הן של נושא אבטחת מידע והן של מכשור רפואי. הטמעת נושאים אלה בבקרות תניע את המוסדות הרפואיים לתקן ליקויים שעלו ותשפר את עמידתם בנוהלי אבטחת המידע של משרד הבריאות, וכן תאפשר למשרד הבריאות כמאסדר לגבש תמונת מצב מקיפה בעניין אתגרי אבטחת המידע (ובכלל זה של מכשור רפואי) בשטח ובעניין הדרכים הראויות להתמודד עימם בהתאם לכך. עוד מומלץ כי המשרד יבצע הליך סדור של מעקב אחר תיקון הליקויים שעלו בבקרות.

פרסום מידע רגיש במסגרת דוחות הבקרה באתר המרשתת של משרד הבריאות

עקרון השקיפות נועד להבטיח את תקינות פעילותו של המינהל הציבורי. שקיפות הממשל מגבירה את אחריות הממשל לפעולותיו, מאפשרת לאזרחים לפקח על מעשי הממשל, מפחיתה אי-תקינות שלטונית ומאפשרת הפצת מידע לציבור. לצד זאת היקף השקיפות היא סוגיה הנדרשת לאיזון בין הצורך בה לבין הסיכון בחשיפת מידע. כך למשל בנוגע לחשיפה של מידע אישי - סעיף 9(א)(3) לחוק חופש המידע, התשנ"ח-1998, קובע כי רשות ציבורית (ובכלל זה משרד ממשלתי) לא תמסור מידע אשר גילויו מהווה פגיעה בפרטיות[60].

גם פרסום ליקויים (ובפרט החולשות) שהועלו בבקרות בתחום אבטחת מידע נדרש לאיזון בין הצורך בשקיפות לבין מזעור הסיכון שבחשיפה, שכן הדבר עלול לחשוף נקודות חולשה באבטחה של מערכות הארגון וכך לעודד תקיפת סייבר בנקודות אלו.

באתר המרשתת של המשרד מפורסמים בין השאר דוחות שהוכנו בשנים 2019 ו-2020, בבתי חולים כלליים-ממשלתיים, בבתי חולים של הכללית, בבתי חולים ציבוריים, בבתי חולים פרטיים ובקופות החולים.

עלה כי כ-20 דוחות כללו, בין היתר, ממצאים בתחום אבטחת המידע, ובכלל זה חולשות שהתגלו במוסדות הרפואיים ובקופות החולים בתחום זה.

בעקבות פניית צוות הביקורת למשרד הבריאות ציינו נציגיו כי בבדיקה שביצע המשרד אכן נמצאו כמה דוחות שפורסמו ובהם פרק אבטחת מידע מלא ללא הסרת מידע רגיש כנדרש. עוד ציינו כי הפרסום בוצע בעקבות טעות אנוש ובשל כך שהדוחות לא עברו כנדרש לאישור ממונה אבטחת המידע של המשרד לפני פרסומם. בעקבות פניית צוות הביקורת הוסרו הדוחות מהאתר. אשר לדוחות הבקרה על קופות החולים, נציגי המשרד ציינו כי פרסומם התבצע לאחר בקרה על המידע ובחינה שלו באופן שלא יגרום נזק, וכי הפרסום לא הזיק לארגונים.

משרד מבקר המדינה מציין את תיקון הליקוי תוך כדי ביצוע הביקורת.

60 החוק מאזן את חשיפת המידע גם עם שיקולים נוספים וקובע כי רשות ציבורית לא תמסור מידע שיש חשש שגילויו יביא לפגיעה בביטחון המדינה, ביחסי החוץ שלה, בביטחון הציבור או בביטחונו או בשלומו של אדם.

על משרד הבריאות להעביר מידע שיש בכוונתו לפרסם לציבור לאישור ממונה אבטחת המידע של המשרד לפני פרסומו, ובפרט בנוגע למידע רגיש המכיל ליקויים בתחום אבטחת המידע. כמו כן מומלץ שלפני שהמשרד מפרסם לציבור דוחות בקרה הכוללים ליקויים בתחום אבטחת המידע הוא יביא לידיעת ממוני אבטחת המידע של המוסדות הרפואיים, את הכוונה לפרסם מידע זה.

אחריות חטיבת המרכזים הרפואיים הממשלתיים לתחום אבטחת מידע וסייבר

החלטת הממשלה משנת 2014 בנושא הקמת רשות מרכזים רפואיים ממשלתיים[61] קבעה כי הרשות תשמש גוף מטה העוסק בסוגיות ניהול רוחביות הנוגעות לבתי החולים הממשלתיים הכלליים, ובין היתר לנושא מערכות מידע. כשנה לאחר מכן ביטלה הממשלה את החלטתה משנת 2014, וקבעה כי במקום הרשות תוקם חטיבה במשרד הבריאות אשר תהיה אחראית על המרכזים הרפואיים הממשלתיים[62]. בהתאם לכך, משנת 2016 פועלת במשרד חטיבת מרכזים רפואיים ממשלתיים (להלן - החטיבה).

על פי חוזר מנכ"ל בנושא "חטיבת המרכזים הרפואיים הממשלתיים במשרד הבריאות" אחריות החטיבה היא לשאת באחריות כוללת לניהול המרכזים הרפואיים (הכלליים, הגריאטריים ולבריאות הנפש)[63] במכלול ההיבטים הקשורים לפעילות המרכז הרפואי ובכללם היבטים הנוגעים למערכות המידע[64]. יצוין שכאשר המשרד מפרסם בשגרה חוזרים ונהלים החטיבה אחראית ליישומם במרכזים הרפואיים הממשלתיים.

עלה כי אף שבהחלטות הממשלה האמורות נקבע כי החטיבה תשמש גוף מטה בתחום מערכות מידע, ואף שמחוזר מנכ"ל עולה כי אחריות החטיבה כלפי אופן תפקודם של המרכזים הרפואיים כוללת ומתייחסת גם להיבטים של מערכות מידע, בפועל - בחטיבה פועל אגף מערכות מידע, המעסיק כ-200 עובדי מחשוב, אולם העיסוק בתחום אבטחת המידע הוא בידי יחידת הסייבר המגזרית במשרד, והחטיבה אינה מעורבת בכך. במצב דברים זה לחטיבה אין תמונת מצב מיטבית בדבר איכות אבטחת המידע בכל אחד מהמרכזים הרפואיים שבאחריותה.

יצוין שבדצמבר 2019 כתבה מנהלת חטיבת המרכזים הרפואיים הממשלתיים דאז למנכ"ל משרד הבריאות כי מתן אחריות ליישום הגנת סייבר לגורם שאינו הגוף האחראי לפיתוח המערכות, לתחזוקתן ולתפעולן (החטיבה) עלול לגרום לסיכון ממשי של תקינות המערכות ושל אפקטיביות

61 החלטת הממשלה 1622, "הקמת רשות מרכזים רפואיים ממשלתיים" (25.5.14), בה נקבע כי תוקם רשות מרכזים רפואיים ממשלתית אשר תפעל כיחידת סמך מקצועית ותרכז את תפקידי הניהול והפיקוח על התנהלות בתי חולים ממשלתיים כיחידות סמך ממשלתיות.

62 החלטת הממשלה 337, "חיזוק הרפואה הציבורית ואסדרת תחום ביטוחי הבריאות והתכניות לשירותי בריאות נוספים - אישור החלטת ועדת השרים לענייני חברה וכלכלה" (5.8.15).

63 11 כלליים, 5 גריאטריים, 8 בריאות הנפש.

64 חוזר מנכ"ל 4/2017 בנושא "חטיבת המרכזים הרפואיים הממשלתיים במשרד הבריאות" (19.4.17).

ההגנה עליהן. עוד היא ציינה את חוסר היכולת של החטיבה לפקח על הנעשה בתחום הגנת הסייבר במרכזים הרפואיים, בשל חוסר בכוח אדם המוכשר לכך. היא התריעה כי במצב הקיים קשה לוודא שדרישות אסדרתיות חדשות מיושמות באופן שוטף, קשה להבטיח תקינות סבירה של פעילויות בקרת סייבר, וקשה לבצע תחקור אירועי סייבר כנדרש. מנהלת החטיבה ציינה שכל אלה מהווים גורמי סיכון ממשיים, וחשוב לטפל בהם בהקדם. היא המליצה להטיל על האגף למערכות מידע בחטיבה את האחריות ליישום, לתפעול ולבקרה של הנוגע לפעילויות הדרושות להגנה מאיומי סייבר, ובכלל זה – ההנחיה של המרכזים הרפואיים הממשלתיים וכן הפיקוח עליהם והמעקב אחריהם.

מומלץ שהמשרד יבחן את הממשקים שבין חטיבת המרכזים הרפואיים הממשלתיים לבין יחידת הסייבר המגזרית ויבחן בידי מי נכון להפקיד את האחריות לטיפול בנושא אבטחת המידע בכלל המרכזים הרפואיים הממשלתיים, גם נוכח החלטת הממשלה 337.

כן מומלץ שהמשרד יעמוד על המשמעות של הפרדת תחומי האחריות בין שני הגופים ויבחן אם יש צורך לעדכן ולשפר ממשקים אלו או לשנות את מבנה האחריות לתחום אבטחת המידע והגנת סייבר במרכזים הרפואיים הממשלתיים.

פעילות היחידה המגזרית במשרד הבריאות בתחום הגנת סייבר

פעולות היחידה המגזרית במשרד הבריאות: מאז הקמת היחידה המגזרית במשרד הבריאות בשנת 2016 היא ביצעה מגוון פעולות, ובהן הקמה וניהול של חדר מלחמה (חמ"ל) לאומי-מרכזי במשרד: SOC[65] (ראו להלן), הכוונת גופי הבריאות[66], ארגון ימי עיון והדרכות, חקר וליווי של אירועי סייבר, ביצוע תרגילי סימולציה לתקיפות סייבר במוסדות הרפואיים[67], הקמת צוות תגובה לאירוע סייבר, בקרות בשטח, סקירת מערכות אבטחה, קידום שיתוף ידע בין ארגונים במגזר ועוד.

בשנת 2021 פעלה יחידת הסייבר לאגד ולהסדיר את פעילותה תחת קורת גג של מיזם (פרויקט) רחב בשם "כיפת מגן", שמטרתו להבטיח אבטחה של מגזר הבריאות ועמידה שלו בפני איומי סייבר, וזאת באמצעות ארבעה מרכיבים מרכזיים:

1. כוח אדם: ביצוע הכשרות, ימי עיון, אימוני צוות תגובה ועוד.
2. טכנולוגיות הגנה: אספקת טכנולוגיות אבטחה בצורה מרוכזת למגזר הבריאות.
3. תהליכים: איסוף מידע, טיוב מערכות הגנה ועוד.

65 Security Operating Center; "חמ"ל" לניטור, של אירועי אבטחת מידע במגזר הבריאות, ולשליטה ולבקרה עליהם.

66 לכל מוסד רפואי עם רישיון הפעלה שמשרד הבריאות הנפיק: מרפאות קטנות, קופות חולים, מעבדות, מרכזים רפואיים ועוד.

67 בשנים 2017 - 2020 למשל ביצע משרד הבריאות 29 תרגילי סייבר לפחות במוסדות רפואיים שונים.

4. תקנים ואסדרה (רגולציה): ביצוע בקרות והמשך ניסוח הנחיות ונהלים.

כוח האדם ביחידה המגזרית: היחידה פועלת במסגרת אגף מערכות מידע ומחשוב שבחטיבת רגולציה, מחשוב ובריאות דיגיטלית במשרד הבריאות. את העיסוק בתחום אבטחת המידע מרכז "מנהל הטכנולוגיות הראשי וממונה אבטחת מידע וסייבר"[68] (להלן - ממונה אבטחת מידע במשרד הבריאות). מערך הסייבר הלאומי הגדיר ב-2015 את היקף היחידה המגזרית במשרד הבריאות כהיקף פעילות בינוני, הדורש איוש של שלושה אנשי צוות: מנהל היחידה המגזרית, עובד שיהיה אחראי לתחום ההכוונה המקצועית ועובד שיהיה אחראי לתחום הבקרות.

עלה כי המשרה של אחראי תחום הבקרות אינה מאוישת, והבקרה מבוצעת באופן חלקי בידי בעל תפקיד אחר.

משרד הבריאות מסר בתגובתו כי הוא בוחן מקורות תקציביים לאיוש המשרה בהקדם.

מערך הסייבר מסר בתגובתו כי יש להגדיר את משרד הבריאות מחדש כמשרד עם היקף פעילות גדול בתחום הסייבר, הדורש איוש של חמישה אנשי צוות.

לנוכח איומי הסייבר על מערכת הבריאות ובהיותן של מערכות המידע משאב חיוני הנדרש, בין השאר, לצורך הצלת חיים, מומלץ שמשרד הבריאות ישלים את איוש המשרות שבתקן היחידה המגזרית.

מרכז שליטה ובקרה (Security Operating Center - SOC) של מגזר הבריאות

בהחלטת הממשלה בנושא הגנת הסייבר[69] נקבע כי על המטה הקיברנטי הלאומי (כיום חלק ממערך הסייבר הלאומי) והיחידה להגנת הסייבר בממשלה (יה"ב) להקים ביחד מרכז שליטה ובקרה ממשלתי בנושא איומי סייבר - SOC ממשלתי (SOC - Security Operating Center), אשר יעסוק בגיבוש תמונת מצב ממשלתית שוטפת בהיבטי הגנת סייבר ומתן מענה לטיפול באירועי סייבר. יצוין כי החלטת הממשלה לא הטילה על היחידות המגזריות (היחידות להכוונה מקצועית בתחום הגנת הסייבר במשרדים הממשלתיים) חובה להקים SOC ייעודי לכל מגזר, ועם זאת בשנת 2019 מערך הסייבר הלאומי הנחה את היחידות המגזריות לפעול להקמת SOC מגזרי.

בשנת 2016, עוד לפני שניתנה הנחיית מערך הסייבר הלאומי, החליט משרד הבריאות להקים SOC מגזרי שייתן שירות למוסדות רפואיים - יפעל כמרכז המשמש לניטור אירועי סייבר וכן לשליטה ולבקרה עליהם. ה-SOC החל לפעול בסוף אותה שנה. מטרת ה-SOC היא לספק באופן שוטף תמונת מצב של האירועים במגזר הבריאות ולהתערב באירועים עם התרחשותם. צוות ה-SOC כולל אנליסטים בתחום הסייבר (אנשים המנתחים מידע באופן מקצועי) האוספים ומנטרים מידע באמצעות מערכות הגנה, ועל בסיס זאת מזהים ניסיונות תקיפה ופעילות חריגה ברשת של

68 CTO - Chief Technology Officer

69 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15). תאריך עדכון ההחלטה - 28.7.15.

הארגון. לעיתים קרובות ה-SOC הוא המוקד הראשוני לטיפול באירוע סייבר ולניהולו. יצוין כי ל-SOC של משרד הבריאות קיים ממשק להעברת ידע עם המרכז הארצי לניהול אירועי סייבר של מערך הסייבר הלאומי.

במאי 2020 היו מחוברים ל-SOC כ-35 מוסדות רפואיים ובהם בתי חולים ממשלתיים, בתי חולים ציבוריים, בתי חולים פרטיים, בתי חולים גריאטריים, בתי חולים פסיכיאטריים ולשכות בריאות[70]. משרד הבריאות המשיך לפעול לכך שיחוברו ל-SOC המוסדות הרפואיים שטרם חוברו אליו, ובהם מוסד ח, מוסד ה, מוסד ט"ו, מוסד ב וכן מוסד י"ז.

יש לציין לחיוב את יוזמת משרד הבריאות להקמת ה-SOC המגזרי הנותן שירות לכלל המוסדות הרפואיים.

מומלץ כי משרד הבריאות יפעל להשלמת החיבור של כלל המוסדות הרפואיים ל-SOC.

מוסד י"ז מסר בתגובתו למשרד מבקר המדינה מינואר 2022 (להלן - תגובת מוסד י"ז), כי הוא מצוי בשלב השלמת חיבורו ל-SOC המגזרי.

משרד הבריאות מסר בתגובתו כי הוא פועל להשלים את חיבור כלל המוסדות הרפואיים ל-SOC.

פעילות רציפה של ה-SOC: על מנת שה-SOC יוכל לטפל באופן מלא ויעיל באירועי סייבר שעלולים להתרחש במוסדות המחוברים ל-SOC, חשוב לאיישו ללא הפסקה - 24 שעות ביממה ושבעה ימים בשבוע, זאת על מנת להגיב לאירועים כאלה בזמן אמת. טיפול מהיר באירוע סייבר יתרום למזעור הנזקים ובכלל זה לצמצום אובדן מידע ולעצירה מהירה של התפשטות המתקפה, למשל באמצעות שליחה מהירה של צוות תגובה של אנשי מקצוע לשטח או ניתוק מיידי של המערכות הממוחשבות המותקפות.

בביקורת עלה כי ה-SOC של משרד הבריאות מאויש חלקית בימי חול, בשעות היום מ-07:30 עד 18:00. בשאר הזמן ה-SOC מקבל שירות של ספק חיצוני הבוחן את המידע שאוסף ה-SOC אחת לכמה שעות בלבד ולא באופן שוטף.

בפברואר 2020 פנתה מנהלת אגף בריאות דיגיטלית ומחשוב למנכ"ל משרד הבריאות דאז והעלתה את הצורך בהפעלת ה-SOC 24 שעות ביממה, שבעה ימים בשבוע. במכתבה ציינה כי בהיעדר איוש מלא אין בידי המשרד היכולת למנוע את איומי הסייבר הקיימים.

מומלץ כי משרד הבריאות יפעל לכך שה-SOC יפעל באופן שוטף, באופן שיאפשר התמודדות מקיפה ובזמן אמת עם איומי הסייבר הקיימים.

משרד הבריאות מסר בתגובתו כי הוא פועל לגייס ולהכשיר כוח אדם להפעלת ה-SOC 24 שעות ביממה ושבעה ימים בשבוע. המשרד הוסיף כי הצפי להפעלת המרכז במתכונת זו הוא הרבעון הראשון של שנת 2022.

70 יצוין כי קופות החולים מפעילות כל אחת SOC עצמאי של הקופה.

היבטים בפעילות ה-SOC: עלו פערים מסוימים בנושא זה.

משרד מבקר המדינה ממליץ למשרד הבריאות לתת מענה לפערים אלו.

משרד הבריאות מסר בתגובתו כי הוא נערך לממש מיזם לאומי להגנה על מכשור רפואי במוסדות הרפואיים, שישפר את ההגנה של כל המוסדות הרפואיים. מיזם זה ממתין לאישור תקציבי לשנת 2022.

הקמת מעבדת סייבר בתחום המכשור הרפואי

בשנת 2020 יזמו נציגים ממשרד הבריאות, מאיכילוב וממערך הסייבר הלאומי הקמה של מרכז סייבר באיכילוב, ובו מעבדה טכנולוגית, שבה אמורים היו להתבצע במרוכז בדיקות אבטחה ומחקרים על מערכות ומכשירים רפואיים, וזאת בשיתוף של חברות אבטחת מידע ושל יצרני מכשור רפואי. על פי מסמך ההקמה של המיזם, מטרותיו הן: איתור וחקירות של סיכונים הכרוכים בשימוש במכשור רפואי; להוות גורם ממליץ עבור אמ"ר (אגף אביזרים ומכשירים רפואיים במשרד הבריאות, ראו להלן) בנושא עמידה של מכשור רפואי בדרישות אבטחה שהאגף קבע; וקידום טכנולוגיות הגנה חדשניות. תוכנן שבמרץ 2020 יוקצה למעבדה אזור מסוים באיכילוב.

עד שנת 2022 צפויות לקום בישראל שתי מעבדות במגזרים אחרים - מעבדה במשרד התחבורה ומעבדה במשרד האנרגייה, שבהן יתבצעו מחקרי אבטחת מידע על מכשירים עיקריים: מקור התקציב של מעבדות אלה הוא מערך הסייבר הלאומי, המשרד הממשלתי הרלוונטי, ובמקרה של המעבדה במשרד התחבורה - גם מימון של שותפים פרטיים.

עלה כי יוזמת הקמת מעבדת הסייבר בתחום המכשור הרפואי לא התממשה.

מנהל אגף מחשוב מידע ותקשורת באיכילוב מסר לצוות הביקורת כי בשל היעדר תקציב, היוזמה לא תתממש והמעבדה לא צפויה להיבנות.

הפעלת מעבדה לצורך מחקר וביצוע בדיקות אבטחה של מכשור רפואי הם צעדים חשובים בצבירת ידע בדרג הלאומי ובשיפור ההגנה עליהם. יש לכך חשיבות יתרה בשל העובדה שמעורבים בתהליך שותפים שונים שהם בעלי עניין - המוסדות הרפואיים, הגורמים המקצועיים והמאסדרים ממגזר זה וגורמים מקצועיים פרטיים. פעילותם המשותפת יכולה לייצר ערך מוסף ייחודי שיתרום לקידום תחום אבטחת המידע, תביא לשיפור היכולת לאתר חולשות ותשפר את האבטחה הקיימת על המכשירים; ביצוע הבדיקות במרוכז עשוי גם לייעל תהליכים - הן בשל שיתוף ידע ולמידת עמיתים והן בשל האפשרות לבצע ולממן במשותף את אותם מבדקים עבור אותם המכשירים.

מומלץ למשרד הבריאות ולמערך הסייבר הלאומי לשקול את יישום ההקמה של מעבדת סייבר למכשור רפואי ולבחון לשם כך מודלים אפשריים של תקצוב.

משרד הבריאות מסר בתגובתו כי יבחן את הקמת מעבדת הסייבר בתחום המכשור הרפואי בהתאם לאילוצי תקציב.

אישור השיווק של מכשור רפואי חדש בישראל

אגף ציוד רפואי: אמ"ר (אביזרים ומכשירים רפואיים) הוא אגף במשרד הבריאות העוסק ברישום מכשירים רפואיים ובכלל זה במתן היתרי יבוא ושיווק לארץ של מכשירים רפואיים. חוק ציוד רפואי, התשע"ב-2012, ותקנות ציוד רפואי (רישום ציוד רפואי בפנקס וחידושו), התשע"ג-2013, מסדירים את הפעילות לאישור אמ"ר.

הנחיות בחו"ל: אגף אמ"ר מאשר את השימוש במכשיר רפואי בישראל ושיווקו, בהסתמך על אישוריהן של רשויות בריאות שונות כפי שהוגדרו בתוספת הראשונה לחוק ציוד רפואי, התשע"ב-2012, ובהן ארה"ב, אוסטרליה, קנדה, בריטניה, שווייץ וגרמניה (המכונות "מדינות מוכרות"), כגון אישור ה-FDA בארה"ב או ה-CE[71] במדינות אירופה.

יצוין כי בפועל ההנחיות הרגולטוריות של ה-FDA[72] כוללות המלצות בעניין אבטחת מידע של מכשירים רפואיים ואינן מחייבות את הספקים במלואן. במסמך של ה-FDA המפרט את הצעת התקציב של הסוכנות לשנת 2021 מצוין כי נכון לשנה זו אין שום חיוב סטטוטורי לכך שיצרני מכשור רפואי יתייחסו להיבטי אבטחת מידע וסייבר[73]. גם מסמך ההנחיות של האיחוד האירופאי בנושא מכשור רפואי[74] עוסק בין היתר באבטחת מידע אך זאת באופן כללי, והוא אינו נותן בהכרח מענה על צרכים של מוסדות רפואיים במגזר הבריאות בישראל[75].

אישור יבוא של מכשיר רפואי: לצורך קבלת אישור מאגף אמ"ר לייבא מכשיר רפואי לישראל מגיש הבקשה ממלא טפסים עם פרטים אסדרתיים (רגולטוריים) וטכניים שונים הנוגעים למכשיר, ובכלל זה מסמכים המעידים על בטיחות המכשיר למטופלים, בטיחות חשמל, סטריליזציה וניהול איכות, אולם הנחיות אמ"ר אינן נוגעות לצורך בעמידתו של המכשיר בתקני אבטחת מידע. כמו כן הספקים חייבים לדווח לאמ"ר בתוך 48 שעות על תקלות חמורות עד כדי סיכון חיים, אולם חובת דיווח כזאת אינה חלה על תקלות אבטחת מידע חמורות שהתגלו במכשיר.

---

71 Conformité Européenne (בצרפתית) - תו תקן שניתן למכשור רפואי העומד בדירקטיבת המכשירים הרפואיים של האיחוד האירופי.

72 למשל, Postmarket Management of Cybersecurity in Medical Devices משנת 2016.

73 - Justification of Estimates for Appropriations Committees ,Department of Health and Human Services ,2021

74 - Regulation (EU) 2017/745 of the European Parliament and of The Council of on medical devices; האיחוד האירופאי גם פרסם המלצות מפורטות לשיפור האבטחה של מכשור רפואי (MDCG 2019-16 Guidance on Cybersecurity for medical devices) אך אלה ברובן המלצות לא מחייבות.

75 דוגמה לאסדרה בין-לאומית בתחום הסייבר, שתכליתה לתת מענה על אתגרי אבטחת המידע, היא החלטה WP29 של האו"ם בתחום הרכב, שבעקבותיה יחולו בהדרגה בשנים 2022 - 2024 תקנות סייבר מחייבות על יצרני רכבים באיחוד האירופי שמטרתן לשפר את ההגנה על רכבים בפני מתקפות סייבר (למשל החובה לספק עדכוני תוכנה בתחום אבטחת המידע); UNECE, UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles , (24.6.20), [קישור].

נוהל מכשור רפואי של משרד הבריאות משנת 2018 שגיבש המשרד בעקבות קבלת המלצות ועדה שעסקה באבטחת מידע במכשור רפואי שהוקמה בשנת 2012 אינו נותן מענה לצורך בקביעת מדדים מחייבים בתחום אבטחת מידע בהליך אישור מכשור רפואי על ידי אמ"ר.

ביוני 2017 ציין ממונה אבטחת מידע במשרד בכנס מקצועי כי בכוונת המשרד להרחיב את התקנות שמפרסם אמ"ר ולהוסיף להן נדבך של אבטחת מידע; המשנה למנכ"ל דאז ציין בכינוס בנושא בית חולים חכם ומוגן סייבר בשנת 2019 כי "היעדר תקני אמ"ר לסייבר בכל הנוגע לציוד רפואי" הוא אחד הנושאים ש"משרד הבריאות נדרש לעשות 'שיעורי בית' בהם"; לפי תוכנית העבודה של היחידה המגזרית במשרד הבריאות לשנת 2021 בתחום אבטחת המידע במשרד, ברבעון האחרון בשנת 2021 תכנן המשרד עבודה על "תקנות לחוק אמ"ר" והכנת טיוטה ראשונה עד סוף שנת 2021.

עולה כי במועד סיום הביקורת המשרד לא נתן מענה לאומי לצורך בקביעת מדדים מחייבים בתחום אבטחת מידע בעת אישור לייבוא ולשיווק של מכשור רפואי בישראל.

מומלץ שמשרד הבריאות ישקול לשלב תקני אבטחת מידע בהליך האישור של אמ"ר לייבוא ולשיווק של מכשור רפואי לישראל. צעד זה יאפשר לנהל בדיקה מרוכזת בדבר קיומם של מדדי אבטחת המידע הנדרשים במכשור רפואי חדש וישפר את רמת האבטחה של מכשירים רפואיים המשמשים את בתי החולים, קופות החולים ומוסדות רפואיים נוספים.

☆

תחום הגנת הסייבר במערכת הבריאות הוא בעל חשיבות רבה, שכן זמינותם המלאה והקבועה של מערכות המידע והמכשור הרפואי נחוצה לתהליכים מצילי חיים. היעדר אסדרה של סמכויות מערך הסייבר הלאומי כלפי היחידות המגזרית במשרדי הממשלה עלול להקשות את שיתוף הפעולה עם הגופים. לצד ההנחיה של מערך הסייבר הלאומי, משרד הבריאות פועל כמאסדר של המוסדות הרפואיים, בכלל זה בתחום אבטחת המידע. על משרד הבריאות כמאסדר של המוסדות הרפואיים להשלים את גיבוש הנהלים בתחום אבטחת המידע. על המשרד מוטלת האחריות גם לוודא כי המוסדות פועלים לשפר את ההגנה שלהם על מערכות המידע והמכשור הרפואי, וכן כי הם עומדים בנוהלי המשרד בתחום אבטחת המידע. כפי שעלה בדוח זה, בקרות הרישוי של משרד הבריאות בבתי החולים ובקופות החולים בשנים 2019 - 2020 לא כללו בקרה בנושא מכשור רפואי, וכן המשרד לא בדק אם תוקנו ליקויים שהועלו בתחום אבטחת המידע.

מומלץ שמשרד הבריאות יגבש תוכנית רב-שנתית להגנת סייבר במוסדות הרפואיים הכוללת הגדרת יעדים, סדרי עדיפויות, מדדים וכן הערכה תקציבית נדרשת ואת מקורות המימון האפשריים.

משרד הבריאות מסר בתגובתו כי בתחילת שנת 2022 הוא החל לגבש המלצות לתוכנית מסגרת לצורך היערכות להתמודדות עם איומי הסייבר במערכת הבריאות בישראל, שתעסוק, בין היתר, בהתייחסות לתהליכי העבודה בין היחידות השונות במשרד, בניהול הסיכונים בנוגע לפגיעה האפשרית ברציפות התפקודית במערכת הבריאות, במשאבים הנדרשים ובמקורות התקצוב, ביעדי בקרה בעבודה מול רשויות נוספות במדינה, ובשינוי תפיסה ותרבות ארגונית בתחום אבטחת המידע.

מדיניות אבטחת מידע במוסדות הרפואיים

אחד העקרונות המרכזיים בתחום אבטחת המידע הוא מדיניות וממשל בתחום מערכות המידע בכלל (IT Governance) ובתחום אבטחת מידע בפרט. מונח זה נוגע לתהליך התאגידי שבאמצעותו ההנהלה מוודאת כי מערכות המידע תומכות ביעדים המקצועיים והעסקיים של הארגון, ובה בעת שהסיכונים הרבים הכרוכים בשימוש במערכות מנוהלים כראוי. פרק זה בוחן סוגיות מרכזיות במדיניות של המוסדות הרפואיים בתחום אבטחת המידע.

ועדת היגוי ובעלי תפקידים

פרק זה מתבסס על תשובות 25 המוסדות הרפואיים על השאלון שנשלח אליהם במסגרת הביקורת (להלן - שאלון אבטחת המידע): 11 המרכזים הרפואיים הכלליים-ממשלתיים, שני המרכזים הרפואיים הציבוריים, שמונת המרכזים הרפואיים הכלליים של הכללית וארבע קופות החולים. (כפי שיפורט בהמשך, ביתר פרקי השאלון, פרט לפרק זה, הכללית השיבה בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה).

בעל התפקיד העומד בראש ועדת ההיגוי לתחום הגנת המידע: על פי תורת ההגנה בסייבר, האחריות להגנה על המידע מוטלת בראש ובראשונה על הנהלת הארגון. חוזר מנכ"ל משרד הבריאות משנת 2015 קובע כי כל מנהל מוסד רפואי ימנה ועדת היגוי לתחום הגנת המידע שהוא יעמוד בראשה. הוועדה תתווה את מדיניות אבטחת המידע במוסד[76].

בכל 25 המוסדות הרפואיים שענו על שאלון אבטחת המידע פעלה ועדת היגוי, ובשישה מהם - מוסד י"ז, מוסד ט"ז, מוסד י"א, מוסד י"ב, מוסד ח ומוסד ה - עמד בראשה מנהל בית החולים או מנהל הקופה כנדרש בחוזר מנכ"ל משרד הבריאות משנת 2015. בראשן של הוועדות במוסדות האחרים עמדו סגן מנהל בית חולים, סמנכ"ל, חבר הנהלה אחר או המנהל האדמיניסטרטיבי.

מוסד ב מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד ב), כי המנכ"ל מקיים ישיבות בתחום אבטחת מידע וסייבר פעם בחודש וחצי.

הדרישה כי מנהל המוסד הרפואי יעמוד בראש ועדת ההיגוי לתחום הגנת המידע מכוונת לכך שמדובר בצורך ארגוני, אסטרטגי בעל חשיבות מהמעלה הראשונה. על המוסדות הרפואיים להבטיח כי מנהל המוסד יעמוד בראש הוועדה כנדרש בחוזר מנכ"ל משרד הבריאות משנת 2015.

מוסד ו מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד ו), כי יעדכן את כתב המינוי של הוועדה באופן שבראש הוועדה יעמוד מנהל המרכז הרפואי.

76 יצוין כי בטיוטת חוזר מנכ"ל בנושא רגולציית יסוד מ-2020 נכתב כי בראש ועדת ההיגוי יעמוד המנהל הכללי של הארגון או מי מטעמו שהוא חבר הנהלה בכירה. כאמור, במועד הביקורת טרם פורסם החוזר.

מוסד ז מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד ז), כי מנהל המרכז הרפואי יעמוד בראש ועדת ההיגוי.

ממונה אבטחת מידע: תקנות הגנת הפרטיות קובעות כי חלה חובה למנות ממונה על אבטחת מידע במוסדות המחזיקים מעל חמישה מאגרי מידע החייבים ברישום או בגופים ציבוריים כהגדרתם בחוק הגנת הפרטיות. חוזר מנכ"ל משרד הבריאות משנת 2015 קובע כי בכל מוסד רפואי ימנה מנהל המוסד ממונה אבטחת מידע.

ב-24 מ-25 המוסדות הרפואיים שהשיבו על שאלון אבטחת המידע ציינו שפועל אצלם ממונה אבטחת מידע; מוסד י ציין כי ממונה אבטחת המידע נמצא בתהליכי גיוס.

ממונה הגנת הפרטיות: הימצאות מידע אישי ורגיש בארגונים המחזיקים מאגרי מידע, ובפרט מידע רפואי אישי הנשמר במערכות של המוסדות הרפואיים, מחייבת אסדרה תוך שימת דגש על אבטחת המידע. בהתאם לכך, מינוי ממונה הגנה על הפרטיות בארגונים הפך לתקנה מחייבת במדינות מערביות רבות. למשל, האסדרה הכללית להגנה על מידע של האיחוד האירופי משנת 2016 (ה-GDPR - General Data Protection Regulation), מחייבת למנות ממונה הגנה על הפרטיות בארגונים שמחזיקים מאגרי מידע רפואי ולהבטיח את עצמאותו של בעל תפקיד זה. הצורך בהפרדת תפקיד ממונה הגנת הפרטיות מתפקידים אחרים, ובהם מנהל הסיכונים וממונה אבטחת המידע, והצורך בעצמאותו של ממונה הגנת הפרטיות נדונה גם בפורומים מקצועיים ברחבי העולם. למשל, בשנת 2020 הרשות הבלגית להגנה על הפרטיות הטילה קנס על חברה שמינתה ממונה הגנה על הפרטיות שכיהן גם כמבקר הארגון וכמנהל הסיכונים[77].

במשך השנים הועלו בישראל הצעות למנות ממונה הגנה על הפרטיות בכל ארגון המחזיק מידע כזה, על מנת שזה יבטיח עמידה בדיני הגנה על מידע אישי ויוביל להטמעה של עקרונות ושיקולי פרטיות בתהליכי העבודה של הארגון[78]. למשל:

- באוקטובר 2020 פרסמה הרשות להגנת הפרטיות טיוטה להערות הציבור בנושא "מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו"[79], ובו המליצה למנות ממונה הגנה על הפרטיות בכל ארגון. בינואר 2022, לאחר מועד סיום הביקורת, פרסמה הרשות את מסמך ההמלצות בנושא[80].
- ועדה שהקים משרד הבריאות בשנת 2017 בנושא "התמודדות עם איום הפגיעה בפרטיות המטופל ובסודיות המידע הרפואי וגיבוש תוכנית פעולה לצמצום התופעה ומיגורה" המליצה למנות ממונה ארגוני להגנה על הפרטיות.
- בינואר 2020 משרד הבריאות גיבש טיוטת חוזר מנכ"ל בנושא רגולציית יסוד. על פי טיוטת הנוהל, על מנהל הארגון למנות ממונה על הגנת הפרטיות מקרב עובדי הלשכה המשפטית בארגון, שישמש מנחה מקצועי בתחום לכל הארגון ויהיה אחראי לפיתוח שיטות הטמעה להגנת פרטיות המידע ולהדרכה בנושא, להתוויית הוראות עבודה להגנת פרטיות המידע,

77 Privacyproficient, בלגיה, "Can a CISO be a DPO?"

78 ראו גם מבקר המדינה, **דוח שנתי 69ב** (2019), "היבטים בהגנה על הפרטיות במאגרי מידע", עמ' 3.

79 הרשות להגנת הפרטיות, "מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו" (29.10.20).

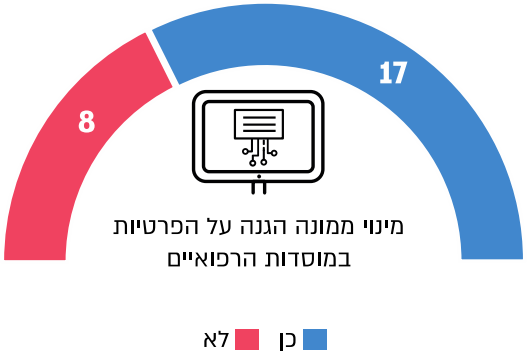
80 הרשות להגנת הפרטיות, "מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו" (25.01.22), [קישור].

לבקרה וביקורת על יישום הגנת הפרטיות.

משרד הבריאות מסר לצוות הביקורת כי מנכ"ל המשרד אישר את הטיוטה, וכי המשרד הפיץ אותה למוסדות הרפואיים לצורך קבלת הערותיהם וצפוי לפרסם את הנוהל הסופי בסוף שנת 2021.

ראו בתרשים ובלוח שלהלן מידע על המוסדות שמינו ממונה הגנה על הפרטיות, ופרטים על המוסדות:

תרשים 5: **מינוי ממונה הגנה על הפרטיות במוסדות הרפואיים**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 1: **מינוי ממונה הגנה על הפרטיות במוסדות הרפואיים**

מינו ממונה הגנה על הפרטיות	לא מינו
מוסד י"ג	מוסד ד
מוסד ז	מוסד ט"ז
מוסד י"ז	מוסד ט
מוסד ח	מוסד ו
מוסד י"ב	מוסד י"א
מוסד ט"ו	מוסד י
מוסד ב	מוסד ג
מוסד ה	מוסד א
מוסד י"ד	
שמונת המרכזים הרפואיים של הכללית	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי שמונה מ-25 המוסדות הרפואיים לא מינו ממונה הגנה על הפרטיות.

מוסד ו מסר בתגובתו כי ימנה ממונה הגנה על הפרטיות לאחר שהמאסדרים יפרסמו הנחיות ברורות ומחייבות בנושא.

מוסד א מסר בתגובתו כי ימנה ממונה הגנה על הפרטיות לאחר שהמאסדרים יפרסמו הנחיות ברורות ומחייבות בנושא.

נוכח המידע האישי הנאגר במערכות המידע ובמכשור הרפואי במוסדות רפואיים ונוכח הסיכון שבחשיפתם הלא מבוקרת, מומלץ למשרד הבריאות לשקול לקבוע חובת מינוי ממונה על הגנת הפרטיות בדומה למחויב במדינות מערביות רבות ולמגמות שעולות מהטיוטות של הרשות להגנת הפרטיות ושל משרד הבריאות. כמו כן מומלץ לבחון לבצע הפרדה בין ממונה הגנת הפרטיות לממונה אבטחת מידע, כדי להבטיח בקרה מספקת מצד ממונה הגנת הפרטיות על עבודת צוות אבטחת המידע במוסד הרפואי, כן מומלץ לבחון הגדרה של הממשקים בין בעלי תפקידים אלה.

משרד הבריאות מסר בתגובתו כי הנהלת המשרד אישרה לפרסום את טיוטת חוזר מנכ"ל בנושא רגולציית יסוד כאמור, והחוזר מגדיר את בעלי התפקידים שיש למנות במסגרת מדיניות אבטחת המידע במוסדות הרפואיים, שבהם ממונה הגנה על הפרטיות.

מוסד י"ז מסר בתגובתו כי ימנה בשנת 2022 ממונה על הגנת הפרטיות במרכז הרפואי.

צוות אבטחת מידע והגנת סייבר במוסד הרפואי

צוות אבטחת המידע והגנת סייבר במוסדות הרפואיים הוא לרוב חלק מאגף מערכות המידע. צוות זה מרכז, בין היתר, את גיבוש מדיניות אבטחת המידע של המוסד ואת הנהלים בנושא, ביצוע סקרי סיכונים, ניהול אבטחתי שוטף של רשת בית החולים, ביצוע עדכוני תוכנה, מתן מענה על התרעות אבטחת מידע ותקיפות, ניהול הרשאות ומשתמשים ברשת. תקן הצוות, מבחינת תפקידיו ומספר המשרות שלו, נתון לשיקול דעתה של הנהלת המוסד הרפואי. יצוין כי נוהלי משרד הבריאות אינם מגדירים את מספר התקנים של צוות אבטחת המידע והדבר נתון לשיקול דעתה של הנהלת המוסד הרפואי.

צוות הביקורת בדק את גודל צוותי אבטחת המידע במוסדות הרפואיים[81] יחסית למספר העובדים ולמספר המחשבים שבהם נעשה שימוש בכל מוסד[82]. להלן הפירוט:

81 ללא יועצים חיצוניים.

82 יצוין כי מחקר בנושא ניהול אבטחת מידע הגדיר את התקינה הנדרשת של צוות אבטחת המידע בארגון כדי שיוכל לתת מענה על איומי סייבר כנדרש: עובד אחד עבור כל 1,000 עובדים או משתמשים, או עובד אחד עבור כל 5,000 מחשבים ומכשירים המחוברים לרשת. Carnevalli & Nassif, Calculation Model of the Status and Staffing for Security Management – A Case Study, 2015.

לוח 2: **היחס בין מספר עובדי אבטחת מידע למספר העובדים ולמספר המחשבים במוסדות הרפואיים, אוקטובר 2021**

המוסד הרפואי	היחס בין מספר עובדי אבטחת מידע למספר העובדים	היחס בין מספר עובדי אבטחת המידע למספר המחשבים
מוסד י"ג	1:800	1:725
מוסד ה	1:800	1:640
מוסד י	1:850	1:435
מוסד ט"ו	1:900	1:950
מוסד י"ז	1:1,000	1:900
מוסד ב	1:1,170	1:1,670
מוסד ח	1:1,200	1:1,375
מוסד א	1:1,510	1:1,260
מוסד ט"ז	1:1,520	1:1,100
מוסד ד	1:2,075	1:1,600
מוסד י"ב	1:2,500	1:2,160
מוסד ו	1:2,500	1:2,500
מוסד ט	1:2,500	1:1,500
מוסד ג	1:2,850	1:2,250
מוסד י"א	1:3,000	1:2,000
מוסד י"ד	1:3,000	1:2,500
מוסד ז	1:3,000	1:2,000

מהלוח עולה כי המוסדות הרפואיים נבדלים ביניהם במידה רבה מבחינת היחס בין מספר עובדי המוסד העוסקים בתחום אבטחת המידע או הגנת סייבר ובין מספר העובדים במוסד: בחמישה מוסדות יש איש צוות אבטחת מידע ל-1,000 עובדים ומטה ובשלושה יש איש צוות אחד ל-3,000 עובדים.

מומלץ כי משרד הבריאות ומערך הסייבר הלאומי ישקלו את הצורך לקבוע תקן מזערי ודרישות לגבי גודל צוות אבטחת המידע הרצוי במוסד רפואי בהתאם למאפייניו.

משרד הבריאות מסר בתגובתו כי הוא יבחן הקמת צוות להגדרת תקינה של גודל צוות אבטחת המידע הרצוי במוסדות הרפואיים.

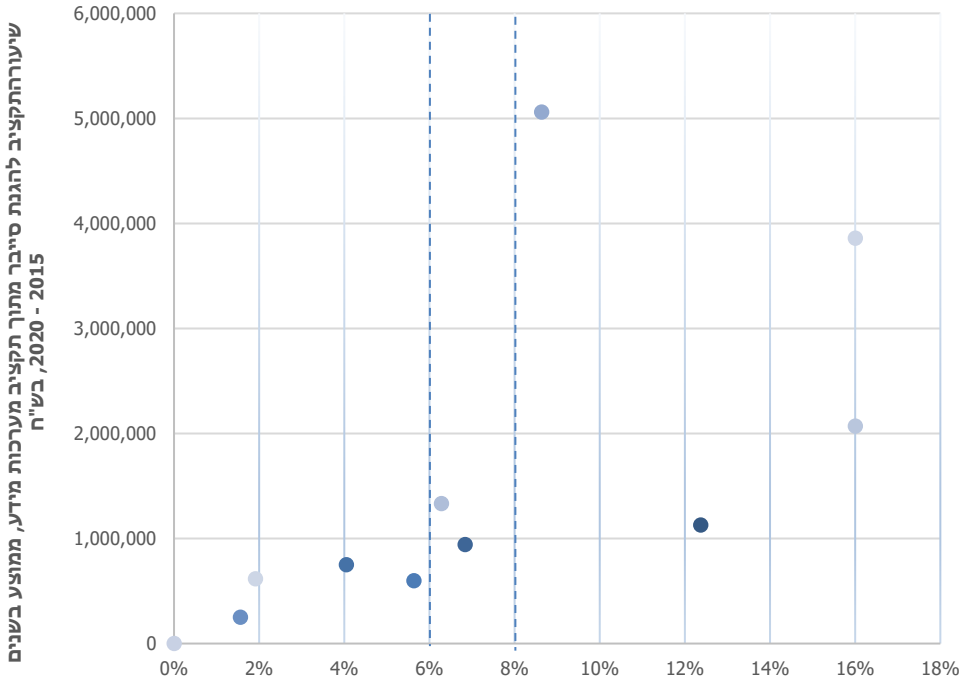
מוסד י"ד מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד י"ד) כי לנוכח ממצאי הביקורת הוא יצרף בעל תפקיד חדש (מיישם סייבר) נוסף על מנהל אבטחת המידע.

הקצאה תקציבית ייעודית להגנת סייבר

בהחלטת הממשלה 2443 בנושא הגנת הסייבר משנת 2015 נקבע כי המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך (בתי החולים הממשלתיים מוגדרים כיחידות סמך[83] של משרד הבריאות) יסדירו את מבנה התקציב השנתי של משרדם באופן שלכל הפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת סייבר. עוד נקבע בהחלטה כי מנכ"ל משרד ממשלתי או מנהל יחידת הסמך, לפי העניין, יוכלו בנסיבות מיוחדות לאשר הפחתה מה-8% בהחלטה מפורטת ומנומקת, שתדווח לוועדת ההיגוי הממשלתית בתחום הגנת הסייבר שתוקם, ובלבד שלפחות 6% מתקציב תחום טכנולוגיית המידע יופנה להגנת סייבר. להלן בתרשים יוצגו שיעור ההקצאה להגנת סייבר מתוך תקציב מערכות המידע במרכזים הרפואיים הכלליים-הממשלתיים:

83 יחידת סמך היא ישות הפועלת במסגרתו של משרד ממשלתי, אך נהנית מעצמאות מסוימת, יחסית ליחידות הפועלות כחלק מובנה מהמשרד. ראו גם מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2021** (2021), בפרק "התנהלות הרשויות המקומיות בעת משבר הקורונה". חוק שירות המדינה (משמעת), התשכ"ג-1963, מגדיר "יחידת סמך" – יחידה במשרד שוועדת השירות העניקה לה סמכויות מינהליות של משרד, בהתאם לכללים הנהוגים בשירות המדינה.

תרשים 6: **שיעור התקציב להגנת סייבר מתוך תקציב מערכות מידע במרכזים הרפואיים הכלליים-ממשלתיים, הממוצע בשנים 2015 - 2020**[84]



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי שישה מ-11 המרכזים הרפואיים הקצו להגנת סייבר שיעור קטן מזה שקבעה החלטת הממשלה - 8%. ארבעה מהמרכזים גם לא הקצו להגנת סייבר את השיעור המזערי שנקבע בהחלטת הממשלה - 6%. עוד עלה כי באחד המוסדות לא הייתה הקצאה תקציבית ייעודית לאבטחת מידע ובכלל זה להגנת סייבר. מוסד אחר מסר כי שיעור התקציב להגנת סייבר מתוך תקציב מערכות המידע היה כ-49%, ומוסד נוסף כ-20%.

84 תקציב כולל של בית החולים, תאגיד הבריאות, אגודת הידידים ועוד; הנתון בתרשים מתאר את סך התקציב שהוקצה להגנת סייבר מתוך סך תקציב שהוקצה למערכות מידע באותה שנה; התקציב הממוצע של מוסד י"ז לא כולל את שנת 2019, שההשקעה בה בתחום הגנת סייבר הייתה גדולה אף יותר וחריגה בשל תוכנית התאוששות מאסון; התקציב המוצג של מוסד ד, כפי שהועבר לצוות הביקורת, מתייחס לנתוני שנת 2020 בלבד.

יצוין כי במוסד מסוים שיעור התקציב גדל במהלך השנים והיה כ-11% בשנת 2020, במוסד אחר היה יותר מ-10% בשנים 2019 ו-2020, ובמוסד נוסף היה בשנים 2019 ו-2020 6% עד 8%. עוד מוסד מסר בתגובתו כי בשנת 2021 שיעור הקצאת התקציב להגנת סייבר עמד על 10.5%.

עלה גם כי המוסדות הרפואיים נבדלים ביניהם מבחינת הסעיפים התקציביים שהם מכלילים בחישוב ההקצאה התקציבית להגנת סייבר, ועל כן, בין היתר, קיימת שונות בין התקציבים עליהם דיווחו המוסדות בשאלון אבטחת המידע.

על הנהלות המוסדות הרפואיים לפעול בהתאם להוראות החלטת הממשלה ולהקצות תקציב ייעודי להגנת סייבר בשיעור שקבעה החלטת הממשלה. מומלץ שמשרד הבריאות יגבש קווים מנחים שיגדירו את ההוצאות אותן יש לכלול במסגרת הקצאת תקציב להגנת סייבר. עוד מומלץ שבמסגרת התוכנית הרב-שנתית להגנת סייבר יכלול המשרד גם את ההערכה התקציבית הנדרשת ואת מקורות המימון האפשריים.

תוכניות עבודה וסקרי סיכונים

שיפור האבטחה של מכשור רפואי במסגרת תוכנית העבודה: השלב הראשון בתהליך ההגנה, על-פי תורת ההגנה בסייבר, הוא תכנון והערכה שעיקריו הם מיפוי יעדי הגנה בסייבר בארגון, הערכת סיכונים, בחינת אמצעי ההגנה (הבקרות) הקיימים והקמת תוכנית עבודה לסגירת פערי הגנה. על בסיס תוכנית עבודה זו המוסדות הרפואיים מתכננים את פעילותם בתחום אבטחת המידע.

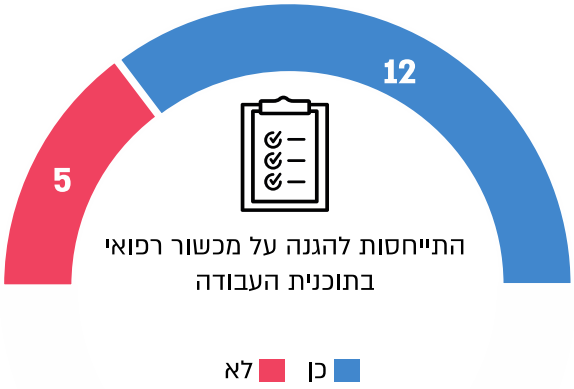
פרק זה מתבסס על תשובות המוסדות הרפואיים שהתבקשו להשיב על שאלון אבטחת המידע; הכללית השיבה בעניין זה בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה - כגוף אחד, שכן תוכנית העבודה וסקר הסיכונים של כל מוסדות הכללית מתבצעים באופן מרוכז ברמת מטה הכללית. לכן סה"כ מספרם הכולל של המוסדות בהם עסק פרק זה הוא 17[85].

לכל 17 המוסדות הרפואיים שענו על שאלון אבטחת המידע (ובהם המרכזים הרפואיים הכלליים-ממשלתיים, שני המרכזים הרפואיים הציבוריים, וארבע קופות החולים) הייתה תוכנית עבודה שנתית או רב-שנתית בתחום אבטחת המידע.

ראו בתרשים ובלוח שלהלן את המוסדות שתוכנית העבודה שלהם בנושא אבטחת מידע לשנים 2020 - 2021 עסקה, בין היתר, בהגנה על מכשור רפואי, והפרטים על המוסדות הללו:

85 11 המרכזים הרפואיים הכלליים-ממשלתיים, שני המרכזים הרפואיים הציבוריים וארבע קופות החולים.

תרשים 7: **תוכנית עבודה בנושא אבטחת מידע שכללה התייחסות להגנה על מכשור רפואי, 2020 - 2021**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 3: **תוכנית עבודה בנושא אבטחת מידע שכללה התייחסות להגנה על מכשור רפואי, 2020 - 2021**

תוכנית העבודה כללה התייחסות למכשור רפואי	לא כללה
מוסד י"ג	מוסד ז
מוסד ט	מוסד י"א
מוסד י"ד	מוסד ד
מוסד י"ב	מוסד ט"ז
מוסד ו	מוסד ג
מוסד י"א	
מוסד י	
מוסד א	
מוסד ח	
מוסד ט"ו	
מוסד ב	
מוסד ה	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי חמישה מוסדות רפואיים לא כללו בתוכנית העבודה שלהם לשנים 2020 ו-2021 התייחסות לשיפור ההגנה על מכשור רפואי ואבטחת המידע הנאגר בו.

מומלץ שהמוסדות הרפואיים יגבשו תוכנית עבודה בנושא אבטחת המידע, הכוללת התייחסות לשיפור ההגנה על מכשור רפואי ואבטחת המידע הנאגר בו, זאת בהמשך להמלצות שבתורת ההגנה בסייבר.

מוסד י"ז מסר בתגובתו כי החל בשנת 2022 הוא יעסוק בנושא המכשור הרפואי במסגרת תוכנית העבודה שלו.

מוסד ד מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד ד), כי בכוונתו להקים ועדת היגוי מוסדית בתחום המכשור הרפואי, שתפעל להגביר את מוכנות המרכז הרפואי לאיומים על מכשירים אלה, ותוכל לעמוד על פעולות שיש לבצע, על התועלת הגלומה בהן ועל המשאבים הנדרשים למטרה זו.

מוסד ז מסר בתגובתו כי גיבש תוכנית לשיפור ההגנה על מכשור רפואי במסגרת התוכנית לאבטחת מידע של המרכז הרפואי.

סקר סיכונים בתחום אבטחת מידע: כלי חשוב שיש להיעזר בו בעת גיבוש תוכנית עבודה הוא סקר סיכונים. סקר סיכונים בוחן ומאתר איומים וחשיפות של אבטחת מידע במערכות של המוסדות הרפואיים ומעריך את רמת הסיכון הנשקף לפעילותם בגין איומים אלה. תקן ISO מדגיש את החשיבות שבביצוע הערכת סיכונים לצורך בחינת הבקרות הקיימות. לפי תורת ההגנה בסייבר, הערכת סיכונים היא הבסיס להקמת תוכנית עבודה רב-שנתית למזעור הפערים במרחב הסייבר.

עלה כי בכל 17 המוסדות הרפואיים שנבדקו בוצע סקר סיכונים בתחום אבטחת המידע.

עדכון סקר הסיכונים: מוסדות רפואיים מאופיינים בסביבה טכנולוגית משתנה, ובה מערכות ומכשירים חדשים משולבים בפעילותם השוטפת. על פי תורת ההגנה בסייבר, יש להגדיר וליישם תהליך תקופתי של הערכת סיכוני סייבר בהתאם למתאר האיומים של הארגון, לרמת החשיפה של יעדי ההגנה לאיומים ולבקרות ההגנה המיושמות. יש לבצע את הסקר באופן תקופתי ולעדכנו בעת שינויים בתהליכים ובמערכות הארגון.

עלה כי מוסד י"א עדכן את הסקר לאחרונה כשמונה שנים לפני סיום הביקורת - בשנת 2013. יתר המוסדות הרפואיים עדכנו את סקר הסיכונים זה מכבר - בשנים 2019 - 2021.

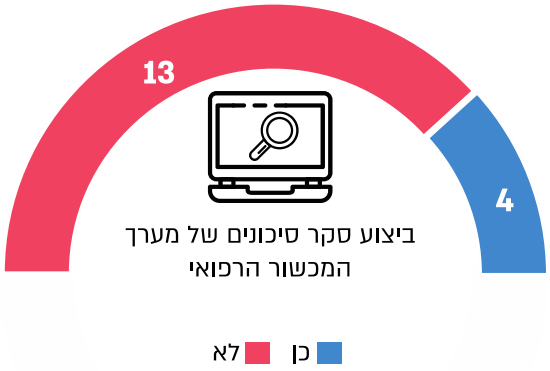
היכולת של סקר סיכונים משנת 2013 לעמוד על הסיכונים בתחום אבטחת המידע בשנת 2021 מוגבלת לנוכח השינויים הטכנולוגיים התדירים ואיומי הסייבר המתפתחים. מומלץ שמוסד י"א יעדכן את סקר הסיכונים באופן שימפה את הסיכונים בתחום אבטחת המידע. עוד מומלץ שכלל המוסדות הרפואיים יעדכנו את הסקרים באופן עיתי.

מוסד י"א מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד י"א) כי יעדכן את סקר הסיכונים במסגרת תוכנית העבודה שלו לשנת 2022.

סקר סיכונים בנושא מכשור רפואי: אשר לסקר סיכונים של מכשור רפואי, נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי מנהל אבטחת המידע ייזום סקרי אבטחת מידע של מערך המכשור הרפואי של המוסד.

ראו בתרשים ובלוח שלהלן את המוסדות שביצעו סקר סיכונים בנושא מערך המכשור רפואי ואת פרטי המוסדות:

תרשים 8: **ביצוע סקר סיכונים בנושא מכשור רפואי במוסדות הרפואיים, 2018 - 2020**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 4: **ביצוע סקר סיכונים בנושא מכשור רפואי, 2018 - 2020**

ביצעו סקר סיכונים	לא ביצעו
מוסד י"ג	מוסד ז
מוסד ו	מוסד י"ז
מוסד ה	מוסד ט"ז
מוסד ח	מוסד ט
	מוסד י"ד
	מוסד י"א
	מוסד י
	מוסד ג
	מוסד א
	מוסד ט"ו*
	מוסד ב
	מוסד י"ב
	מוסד ד

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

* מוסד ט"ו ביצע סקר סיכונים רק בנוגע למעבדה שבה יש מכשור רפואי רב.

מהתרשים ומהלוח עולה כי בשנים 2018 - 2020 13 מ-17 המוסדות הרפואיים לא ביצעו סקר סיכונים בנושא מכשור רפואי.

האיומים ההולכים וגוברים על מערכות המידע ומאגרי המידע בכלל ועל מערך המכשור הרפואי מחייבים נקיטת פעולות לצמצום הנזק האפשרי מפגיעה במערכות המידע התומכות במכשירים ובמאגרי המידע השמורים בהם. על המוסדות הרפואיים לבצע סקר בנושא הסיכונים הנשקפים למכשירים הרפואיים שהם משתמשים בהם, כנדרש בנוהל מכשור רפואי של משרד הבריאות משנת 2018. על משרד הבריאות לוודא שהמוסדות הרפואיים עומדים בנוהל שקבע.

מוסד י"ב מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד י"ב) כי יבצע סקר שיכלול הגדרת מדדים לבחינת רמת החשיבות של המכשירים הרפואיים לפעילות המוסד הרפואי ורמת הסיכון שלהם, ידרג את המכשירים לפי מדדים אלה ועל בסיס דירוג זה יגבש תוכנית כוללת להגנה על המכשירים לפי רמת חשיבותם.

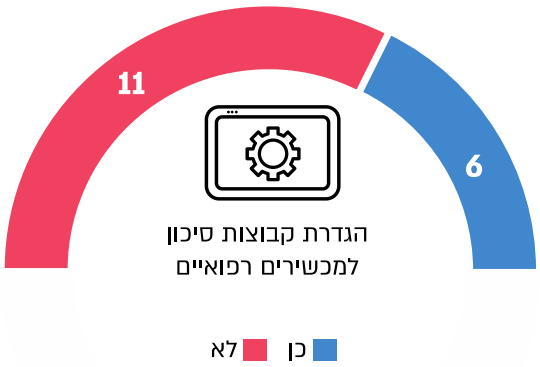
מוסד ז מסר בתגובתו כי הוא מקבל את המלצת משרד מבקר המדינה.

מוסד ב מסר בתגובתו כי הוא מקבל את המלצת משרד מבקר המדינה.

סיווג מכשירים רפואיים לפי רמת הסיכון הנשקף להם: נוהל מכשור רפואי של משרד הבריאות משנת 2018 מבצע חלוקה בין ארבע רמות סיכון של מכשירים שונים מרמת הסיכון הנמוכה ביותר עד רמת הסיכון הגבוהה ביותר: מכשיר שלא נאגר בו מידע ואינו מחובר לרשת; מכשיר שלא נאגר בו מידע אך מחובר לרשת; מכשיר שנאגר בו מידע ואינו מחובר לרשת; והמכשיר בעל רמת הסיכון הגבוהה ביותר הוא מכשיר שנאגר בו מידע והוא מחובר לרשת. הנוהל קובע גם כי יש לסקור מכשור רפואי בעל סיכון גבוה לפחות אחת ל-18 חודשים, וכי יש לסקור מכשיר רפואי אחר בתדירות שקובעת ההנהלה בהתאם לרגישות המערך. יצוין כי מלבד אופן אגירת המידע ומיקומו ברשת, מוסדות עשויים לסווג מכשירים רפואיים כבעלי סיכון גבוה בשל חשיבותו האסטרטגית של המכשיר הרפואי, מידת חשיפתו של המכשיר לפגיעה, רגישות המידע שנאגר במכשיר ועוד.

לצורך קביעת תדירות סקירת המכשירים הרפואיים על המוסדות הרפואיים להגדיר את הסיווג לפי קבוצות הסיכון למכשירים (האם המכשיר הרפואי הוא בעל סיכון גבוה או לא). בתרשים שלהלן מוצגים המוסדות שהגדירו קבוצות סיכון למכשירים רפואיים לפי סיווגי סיכון, והפרטים על המוסדות:

תרשים 9: **הגדרת קבוצות סיכון למכשירים רפואיים**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 5: **הגדרת קבוצות סיכון למכשור רפואי**

הגדירו קבוצת סיכון למכשירים הרפואיים	לא הגדירו
מוסד י"ג	מוסד ז
מוסד א	מוסד י"ז
מוסד ה	מוסד ד
מוסד ט"ו	מוסד ט"ז
מוסד ג	מוסד ט
מוסד ח	מוסד י"ד
	מוסד ו
	מוסד י"א
	מוסד י
	מוסד י"ב
	מוסד ב

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי 11 מ-17 המוסדות הרפואיים לא הגדירו קבוצות סיכון למכשור הרפואי לפי סיווגי סיכון.

במרכזים הרפואיים ובקופות חולים בישראל משתמשים באלפי מכשירים רפואיים מסוגים שונים, בעלי רמת סיכון משתנה הדורשת ניהול, תיעדוף ומתן מענה בהתאם לכך. משרד מבקר המדינה מדגיש כי באמצעות הגדרת קבוצות סיכון למכשור רפואי יוכל המוסד הרפואי לתעדף את השקעת המשאבים למתן הגנה ראויה על מכשירים שנקבעו ברמת הסיכון הגבוהה ביותר למוסד הרפואי, באופן שתשתפר ההגנה על מכשירים אלה מפני תקיפות סייבר אפשריות. על המוסדות הרפואיים שעדיין לא עשו זאת - להגדיר קבוצות סיכון למכשור רפואי. כמו כן מומלץ שמשרד הבריאות יבחן אם יש צורך להגדיר במישור הלאומי אילו מכשירים רפואיים יש לכלול ברמת הסיכון הגבוהה ביותר, שבהתאם לכך יש לתת להם את המענה ההגנתי המרבי.

מוסד ו מסר בתגובתו כי הוא יסווג קבוצות סיכון למכשור רפואי במסגרת תוכנית העבודה השנתית ויתעדף בהתאם לכך את השקעת המשאבים.

מוסד י"ז מסר בתגובתו כי יגדיר קבוצות סיכון בתחילת 2022.

מוסד ז מסר בתגובתו כי יגבש תוכנית בנושא בתחילת 2022.

מוסד י"ב מסר בתגובתו כי תגדיר את קבוצות הסיכון כאמור במסגרת סקר הסיכונים של המכשור הרפואי.

מוסד ב מסר בתגובתו כי הוא מקבל את המלצת משרד מבקר המדינה.

תוכנית להתאוששות מאסון והמשכיות עסקית

פרק זה מתבסס על תשובות המוסדות הרפואיים שהתבקשו להשיב על שאלון אבטחת המידע; הכללית השיבה בעניין זה בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה - כגוף אחד, שכן התוכנית להתאוששות מאסון והמשכיות עסקית של כל מוסדות הכללית מנוהלת באופן מרוכז ברמת מטה הכללית. לכן המספר הכולל של המוסדות בפרק זה הוא 17.

המשכיות עסקית היא יכולתו של ארגון להתכונן לאירועים המפריעים לפעילותו ולהגיב עליהם כדי להמשיך בפעילות הרגילה באופן ובהיקף שתוכננו מראש. מטרותיה העיקריות של תוכנית להמשכיות עסקית (Business Continuity Plan - BCP) הן להבטיח את שרידותו של הארגון, להגן על נכסיו החשובים, לאפשר להנהלתו שליטה על סיכונים וחשיפות, לקדם צעדים המונעים את התממשותם של חלק מאירועי החירום האפשריים, לאפשר פעולה יעילה ואקטיבית של הנהלת הארגון בשעת אירוע החירום וטיפול בהשבת הארגון לפעולה. גופים ציבוריים נדרשים אף להבטיח כי ביכולתם לספק שירותים חיוניים לציבור בעת אירוע חירום[86]. סיכונים לפגיעה בארגון עלולים לנבוע מגורמים שונים[87] ובהם פגיעות המבוססות על טכנולוגיה (למשל מתקפות סייבר על תשתיות מערכות המידע של המוסד הרפואי).

גיבוש תוכנית להמשכיות עסקית דורש תכנון, ובין היתר כולל ניתוח סיכונים, הצבעה על ההליכים הקריטיים שיש לשמור על זמינותם בעת אסון והגדרת המשאבים - האנושיים והחומריים, הנדרשים בעת אסון. תוכנית התאוששות מאסון (DRP - Disaster Recovery Plan) נוגעת לתהליכים במערכות מידע שארגון צריך לבצע כדי להתאושש מאסון ולאפשר המשכיות עסקית, תוך מתן דגש על אופן גיבוי המידע והסביבה (פיזית ולוגית) שבה הוא ישוחזר. במסגרת התוכנית להתאוששות מאסון הארגון קובע את ה-RPO (Recovery Point Objective), כמה מידע הוא מוכן לאבד במקרה של אסון, ואת ה-RTO (Recovery Time Objective), כמה זמן הארגון יכול להמתין עד חזרה לפעילות. כמו כן נדרש לקבוע אתר חלופי זמין לטובת המשך פעילות מערכות המידע במקרה של אסון - נזק או השבתה של האתר המרכזי (אתר DR - Disaster Recovery). אתר כזה יאפשר במקרה של אסון להעלות לשימוש באופן מהיר את מערכות המידע של המוסד הרפואי, לשחזר מידע על המטופלים ולהמשיך במתן השירותים הרפואיים.

86 ראו מבקר המדינה, **דוח שנתי 64א** (2013), "בניית תכניות להמשכיות עסקית של המערכת הפיננסית באירועי חירום", עמ' 51; ומבקר המדינה, **דוח שנתי 64ג** (2013), "היערכות שירותי הבריאות לעתות חירום - ממצאי מעקב", עמ' 717.

87 למשל אסונות טבע (רעידות אדמה, הצפות, סופות), אירועי לוחמה (למשל פגיעת טילים או פיגועי טרור), פגיעה בכוח אדם (מגפות, שביתות).

בשנת 2011 הורה מנכ"ל משרד הבריאות לכל בתי החולים הממשלתיים לגבש תוכנית להתאוששות מאסון עד סוף שנת 2013. כמו כן, תורת ההגנה בסייבר ממליצה לכל ארגון להכין וליישם מדיניות המשכיות עסקית שתגדיר כיצד הארגון מתנהל באופן שוטף ובעיתות חירום כדי להבטיח את ההמשכיות העסקית שלו, ובכלל זה להגדיר מדדים מקובלים כגון RTO במקרה שיתרחש אירוע סייבר. גם תורת ההגנה המעודכנת מדגישה את הצורך ביכולת התאוששות של ארגון במקרים של נפילת אתר, מחיקת מידע ונעילת קבצים, ומדגישה את הצורך בביצוע גיבויים למערכות המידע.

צוות הביקורת בדק אם קיימת בכל המוסדות הרפואיים תוכנית להמשכיות עסקית או תוכנית להתאוששות מאסון, האם קיים בהם אתר חלופי זמין לשם המשך פעילות מערכות המידע במקרה של אסון (אתר DR - Disaster Recovery) - בתוך כותלי המוסד או מחוצה לו; והאם תוכניות אלה עוסקות באופן הטיפול במכשירים רפואיים אם אלה נפגעו. להלן בלוח מוצג המענה של המוסדות בנושאים אלה:

לוח 6: **קיומה של תוכניות להמשכיות עסקית או להתאוששות מאסון, הקמת אתר חלופי זמין (DR), והתייחסות בתוכניות המוסדות לאופן הטיפול במכשירים רפואיים שנפגעו**

שם המוסד	תוכנית להמשכיות עסקית או תוכנית להתאוששות מאסון	אתר חלופי זמין (DR)	התוכניות עוסקות באופן הטיפול במכשירים רפואיים שנפגעו
מוסד י"ג	✓	✓ נותן מענה חלקי*	✗
מוסד ז	✓	✗	✗
מוסד י"ז	✓	צפוי לפעול באופן מלא בשנת 2022	✓
מוסד ד	✓	✓	✗
מוסד ט"ז	✗	✓	✗
מוסד ט	✗ (בשלבי כתיבה)	הכנת האתר בהליכים סופיים	✗
מוסד י"ד	✓	✓	✗
מוסד י"ב	✓	✓	✗
מוסד ו	✓	✓**	✗
מוסד י"א	✓	✓	✗
מוסד י	✓	✓	✓ (יש התייחסות לתשתיות המרכזיות שתומכות)

שם המוסד	תוכנית להמשכיות עסקית או תוכנית להתאוששות מאסון	אתר חלופי זמין (DR)	התוכניות עוסקות באופן הטיפול במכשירים רפואיים שנפגעו
מוסד ג	✓	✓	✓ (יש התייחסות לתשתיות המרכזיות שתומכות)
מוסד א	✓	✓	✗
מוסד ט"ו	✓	✓	✓ נותן מענה חלקי
מוסד ב	✓	צפוי לסיום בנייה בסוף 2021	✗
מוסד ה	✓	✓	✓
מוסד ח	✓	נותן מענה חלקי**	✗

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

* במוסד י"ג, באתר החלופי אין את כל מערכות המחשוב אלא רק עותק של מידע. בכוונת המוסד לפצל את חוות השרתים לשני חדרים נפרדים בשני בניינים שונים, וכך לשפר את שרידות מערך המחשוב ולצמצם את הסיכון ואת הצורך באתר גיבוי מרוחק לצורך ההמשכיות העסקית.

** מוסד ח הוסיף כי יש DR למערכות המנוהלות באופן מרכזי; כי במערכות מקומיות מתבצעים תהליכי שרידות וגיבויים; כי מוסד ח נמצא בשלבי תכנון למתן פתרון DR, וכי בימים אלה מוקם אב-טיפוס לדגם כדוגמה למימוש במערכות מקומיות.

מהלוח עולה כי לשני מוסדות רפואיים (מ-17 המוסדות הרפואיים שענו על שאלון אבטחת המידע): מוסד ט"ז ומוסד ט, אין תוכנית להתאוששות מאסון או תוכניות להמשכיות עסקית; ולשישה אין אתר חלופי (DR) זמין שנותן מענה מלא במקרה של אסון.

עוד עולה כי מרבית המוסדות הרפואיים - 13 מ-17 המוסדות (כ-76%) - לא שילבו בתוכניות שלהם להתאוששות מאסון או בתוכנית להמשכיות עסקיות את אופן הטיפול וההתאוששות של מערך המכשור הרפואי, מערך המורכב מאלפי מכשירים בכל ארגון, ובהם מכשירים החיוניים לשם אבחון קליני מדויק ולשם הצלת חיי אדם.

על מנת להבטיח את היכולת של המוסדות הרפואיים לחזור, בהקדם האפשרי, לפעילות תקינה וסבירה במקרה של אירוע אסון, נדרש שהמוסדות הרפואיים יקדמו הקמה של אתר חלופי (DR). בשל חשיבות הנושא, מומלץ כי משרד הבריאות, כמי שמנחה את המוסדות הרפואיים בכל הנוגע להגנה על מידע במערכות הממוחשבות שלהם ושעליו לפקח על יישום ההנחיות ולעקוב אחרי יישומן, יוודא כי למוסדות יש אתרי DR שיכולים לתת מענה מלא באירועי חירום.

כמו כן מומלץ שכלל המוסדות הרפואיים ישלבו בתוכניות שלהם להמשכיות עסקית והתאוששות מאסון התייחסות לאופן הטיפול והשחזור של מערך המכשור הרפואי, בהתאם לתיעדוף של המכשירים על פי מידת חשיבותם במסגרת פעילות המוסד הרפואי. זאת בהמשך להוראת מנכ"ל משרד הבריאות ולהמלצות תורת ההגנה בסייבר.

מוסד ו מסר בתגובתו כי ישלים את התוכנית להתאוששות מאסון, באופן שתכלול גם טיפול במכשירים רפואיים שנפגעו, בהתאם לסיווג חשיבותם לתפקוד המרכז הרפואי.

מוסד ז מסר בתגובתו כי לנוכח ממצאי הביקורת גיבש תוכנית הכוללת את אופן הטיפול וההתאוששות של מערך המכשור הרפואי במקרה של אסון.

מוסד י"ב מסר בתגובתו כי יגבש תוכנית להמשכיות עסקית אשר תעסוק גם באופן הטיפול במכשירים רפואיים במקרה של אסון.

מוסד ט"ז מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד ט"ז) כי הוא עובד בימים אלה על תוכנית להמשכיות עסקית העוסקת גם במכשור הרפואי.

מוסד ב מסר בתגובתו כי הוא מקבל את המלצת הביקורת.

מוסד ח מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד ח) כי עד סוף שנת 2022 תהיה תוכנית שלמה להמשכיות עסקיות.

משרד הבריאות מסר בתגובתו כי בשנת 2022 הוא יקדם מיזם בתחום ה-DR כדי להבטיח את ההמשכיות העסקית בכל מגזר הבריאות בישראל.

נוהל להתמודדות עם אירוע אבטחת מידע

תקן ISO קובע כי על ארגונים המעבדים מידע בריאותי אישי חלה החובה להגדיר תחומי אחריות ונהלים בנושא ניהול תקריות ביטחון מידע. תורת ההגנה בסייבר ממליצה להכין וליישם מדיניות תגובה לאירועים, וכן לבקר ולעדכן אותה תקופתית. חוזר מנכ"ל משרד הבריאות משנת 2015 קובע כי יש להגדיר נוהל טיפול במקרה של כשל אבטחתי במערכות.

מתשובות המוסדות על שאלון אבטחת המידע עלה כי אחד מ-17 המוסדות - מוסד ט"ז, לא השלים גיבוש של נוהל להתמודדות עם אירוע של אבטחת מידע או מתקפת סייבר. עוד עולה מהתשובות על השאלון כי הנוהל של מוסד ה נמצא בתהליך אשרור סופי.

על מוסד ט"ז לגבש נוהל להתמודדות עם אירוע אבטחת מידע, כנדרש בחוזר מנכ"ל משרד הבריאות משנת 2015. נוהל שכזה ישפר את יעילות המענה אם כשל שכזה יתממש.

ביטוח מפני תקיפות סייבר

בעשור האחרון גובר הביקוש לכיסוי ביטוחי מפני תקיפות סייבר. ביטוח סייבר כולל למשל כיסוי של הוצאות הקשורות לתגובה על אירוע סייבר; הוצאות רגולטוריות משפטיות; הוצאות הקשורות

לרכיבי אבטחת מידע; מחקר בנוגע לזהות התוקף; פגיעה בפרטיות; פגיעה בפעילות העסקית של הארגון; פגיעה במערכות הארגון; והחזר כספי במקרה של מתקפת כופר. עם זאת, מסקר שביצע מערך הסייבר הלאומי בשנת 2019 עולה כי רק ל-13% מהחברות במשק יש ביטוח סייבר[88]. לפי הערכת מערך הסייבר הלאומי, המורכבות שבקידום הנושא נובעת, בין היתר, מכך שמדובר בתחום ביטוחי חדש שלחלק מחברות הביטוח אין ידע מספק בו, ומהיעדר ביקוש בשל חוסר מודעות של ארגונים לסיכון.

"ענבל חברה לביטוח בע"מ", שהיא חברה ממשלתית, עוסקת בין השאר בתחומי מתן שירותי ניהול וייעוץ בתחום הביטוחי (להלן - חברת ענבל). למרכזים הרפואיים הממשלתיים כיסויים ביטוחיים באמצעות הקרן הפנימית לביטוחי הממשלה ובאמצעות פוליסות ביטוח משנה שענבל רוכשת או מנהלת עבורם, בגין אחריות מקצועית של הצוותים הרפואיים במרכזים הרפואיים הממשלתיים.

עלה כי נכון למועד סיום הביקורת לכל המרכזים הרפואיים הממשלתיים (הכלליים, הגריאטריים והפסיכיאטריים) אין ביטוח סייבר.

עוד עלה בנוגע לשאר המוסדות הרפואיים, כי לחלקם אין ביטוח המכסה את נושא אבטחת המידע והסייבר ולחלקם יש.

חברת ענבל מסרה לצוות הביקורת כי במסגרת תוכנית של החשב הכללי (החשכ"ל) לרכישת ביטוח סייבר ליחידות ממשלתיות, היא קידמה בשנת 2021 מהלך שיסייע לקידום פתרון ביטוחי למרכזים הרפואיים הממשלתיים. בתהליך שקידמה חברת ענבל בשיתוף משרד הבריאות (חטיבת המרכזים הרפואיים במשרד) בשנת 2021, נבחרו סוקרים לביצוע סקר אבטחת מידע בשלושה מרכזים רפואיים ממשלתיים: שיבא, רמב"ם ופורייה (מודל של מרכז רפואי גדול, בינוני וקטן). הסוקרים פעלו לכמת את אומדן הנזקים הכספיים והפיזיים שעלולים להיגרם ממגוון תקיפות סייבר. כמו כן ציינה חברת ענבל כי לאחר סיום הסקר בכוונתה לבחון בשיתוף החשכ"ל, משרד הבריאות וגורם שלישי שייבחר בהליך מכרזי את האפשרות לרכישת פוליסת ביטוח סייבר מרוכזת למרכזים הרפואיים הכלליים-ממשלתיים, הפסיכיאטריים והגריאטריים.

ענבל מסרה בתגובתה למשרד מבקר המדינה בינואר 2022 כי סקר אבטחת המידע בשלושת המרכזים הרפואיים הממשלתיים עדיין בשלבי ביצוע, ועם סיומו ניתן יהיה לקדם את ההליך לרכישת פוליסות הביטוח.

משרד מבקר המדינה ממליץ לחברת ענבל להשלים, בשיתוף משרד הבריאות, את הליך בחינת הכיסוי הביטוחי למרכזים הרפואיים הממשלתיים בתחום אבטחת המידע והסייבר ומדגיש את החשיבות שבסיום הליך זה.

88 מערך הסייבר הלאומי, "עבודת מטה של מערך הסייבר הלאומי מקדמת ביטוח ככלי לקידום חוסן המשק מפני תקיפות" (25.6.19). [קישור].

חלק מהמוסדות שאינם ממשלתיים מסרו בתגובתם למשרד מבקר המדינה כי בחנו שילוב של ביטוח סייבר, אך הוא אינו בהכרח משתלם או ישים בשל מחירו ותכולת הכיסוי שלו, וחלקם מסרו כי קיבלו את המלצת מבקר המדינה לרכישת ביטוח מפני תקיפות סייבר.

מומלץ גם כי הנהלות המוסדות שאינם ממשלתיים ואין להם ביטוח סייבר - ישקלו לשלב ביטוח כזה במסגרת ביטוחי המוסד הרפואי, וכי סוגיה זו תועלה לבחינה מחודשת מפעם לפעם.

ביקורת פנים בתחום אבטחת המידע

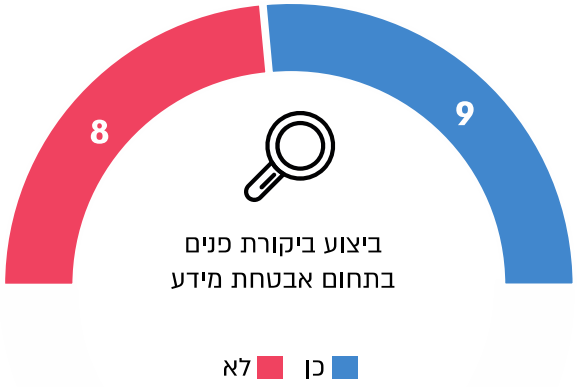
מבקרי פנים הם כלי בקרה חשוב בפעילות השוטפת של מוסדות רפואיים ונמנים עם שומרי הסף שבארגון; הם מעלים ליקויים חשובים ומניעים את הנהלת המוסדות לתקן ליקויים אלה. על פי החלטה של נציבות שירות המדינה משנת 2014, יש למנות מבקרי פנים בכל בתי החולים הכלליים[89].

תקן ה-ISO בנושא אבטחת מידע בתחום הבריאות קובע כי חלה על המוסדות הרפואיים חובה לקבוע תוכנית ביקורת שתכסה את כלל המרכיבים המצוינים בתקן, ובכלל זה את הסיכונים והביקורות המיושמות.

צוות הביקורת בדק במסגרת שאלון אבטחת המידע את ביצועה של ביקורת פנים בתחום אבטחת מידע במוסדות הרפואיים בשנים 2016 - 2021. פרק זה מתבסס על תשובות המוסדות הרפואיים שהתבקשו להשיב על שאלון אבטחת המידע; הכללית השיבה בעניין זה בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה - כגוף אחד, שכן ביקורת הפנים של כל מוסדות הכללית מנוהלת באופן מרוכז ברמת מטה הכללית. לכן מספרם הכולל של המוסדות בהם עוסק פרק זה הוא 17. להלן מוצג המענה של המוסדות בנושאים אלה והפרטים על המוסדות:

89 נציבות שירות המדינה, חוזר מס 8/2014 בנושא "מינוי מבקרי פנים בבתי החולים הממשלתיים" (23.3.14).

תרשים 10: **ביצוע ביקורת פנים בתחום אבטחת מידע, 2016 - 2021**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 7: **ביצוע ביקורת פנים בתחום אבטחת מידע, 2016 - 2021**

ביצעו ביקורת פנים בתחום אבטחת המידע	לא ביצעו
מוסד ז	מוסד ד
מוסד י"ז	מוסד ט
מוסד ג	מוסד י"ד
מוסד ב	מוסד ו
מוסד ח	מוסד י"א
מוסד ט"ו	מוסד א
מוסד ה	מוסד י
מוסד י"ב	מוסד ט"ז
מוסד י"ג	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה שכמחצית (שמונה) מהמוסדות הרפואיים לא ביצעו ביקורת פנים בתחום אבטחת מידע, ובהם מוסדות שהם מרכזים רפואיים גדולים - מוסד ט"ז ומוסד א.

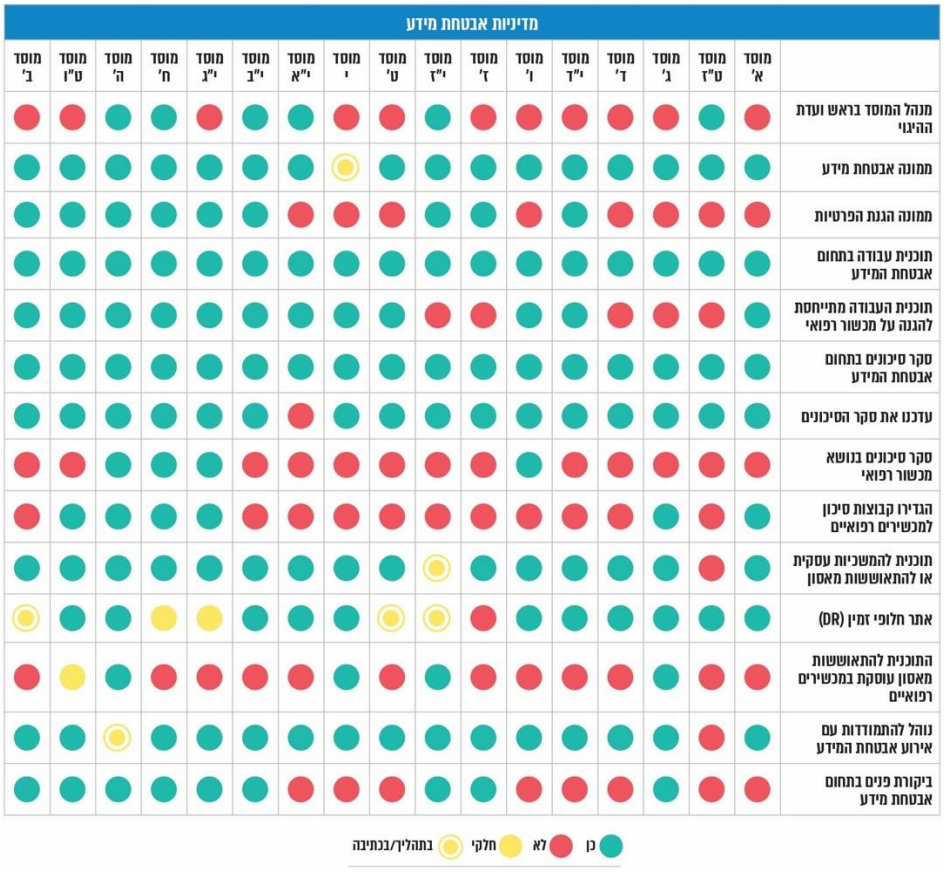
על המבקרים הפנימיים במוסדות הרפואיים להכין תוכנית ביקורת פנים שתשלב בחינה של נושאים בתחום אבטחת המידע כמפורט בתקן ISO, ובכלל זה ביקורות על מוכנות המוסדות להתמודדות עם תקיפות סייבר, עם זליגה של מידע רפואי אישי, עם פגיעה במכשור רפואי ועוד. מומלץ שמשרד הבריאות יוודא כי המוסדות הרפואיים מקיימים הנחיה זו.

מוסד ו מסר בתגובתו כי יכלול בדיקה של נושא אבטחת המידע במסגרת תוכנית העבודה של מבקר הפנים במוסד.

☆

להלן בתרשים מוצג ריכוז ממצאים מסוימים בנושא מדיניות אבטחת מידע במוסדות הרפואיים, כפי שעלו בפרק זה:

תרשים 11: **ריכוז ממצאים מסוימים בנושא מדיניות אבטחת מידע במוסדות הרפואיים**



כמו כן, עלו פערים נוספים בנושא מדיניות אבטחת מידע במוסדות הרפואיים.

אבטחת מידע בעת רכישת מכשיר רפואי חדש

לרוב גורמים רפואיים (או מחלקות הנדסה רפואית[90]) הם המבצעים רכש של מכשור רפואי ומתפעלים אותו, זאת להבדיל, למשל, מרכש מחשבים שממומן מתקציב מנהל מערכות המידע ומתבצע בשליטתו. גורמים אלה אינם מכירים, בדרך כלל, את שיקולי מערכות המידע וההגנה על מכשירים רפואיים, את סוגי ההתקפות האפשריות עליהם ואת ההגנה הנדרשת עליהם. על כן יש לערב את גורמי אבטחת המידע בהליך הרכש[91].

פרק זה מתבסס על תשובות המוסדות הרפואיים שהתבקשו להשיב על שאלון אבטחת המידע; הכללית השיבה בעניין זה בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה - כגוף אחד, שכן נושא הרכש של כל מוסדות הכללית מנוהל באופן מרוכז ברמת מטה הכללית. לכן מספרם הכולל של המוסדות בהם עוסק פרק זה הוא 17.

התייחסות להיבטי אבטחת מידע של מכשור רפואי בנוהלי הרכש של המוסדות הרפואיים

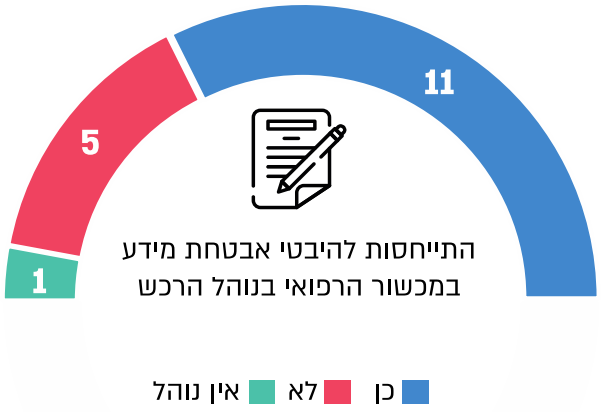
בעת רכש של מכשור רפואי נבחנים מדדים שונים של המכשיר על בסיס הצרכים של המוסד הרפואי, הן מדדים קליניים והן מדדים לוגיסטיים, ובפרט כשנרכש מכשור רפואי יקר ומורכב, כגון מכשיר דימות מסוג MRI שעלותו מסתכמת בכמיליון וחצי דולר לפחות (כחמישה מיליון ש"ח). על פי תורת ההגנה בסייבר, כיוון שבמסגרת תהליכי רכש ופיתוח מתווספים לארגון ציוד או תוכנות שעלולים להכיל פוגענים, נדרש לקבוע לשם כך מדיניות לרכש ופיתוח מערכות שישולב בה גם מרכיב הגנת סייבר, וכן נדרש לעקוב אחר יישומה ולעדכן אותה תקופתית. בתורת ההגנה המעודכנת נקבע כי על הארגון לדרוש מספקי השירותים לציית לדרישות האבטחה הארגוניות, לרגולציות, לסטנדרטים ולהנחיות. מהאמור עולה שעל כל ארגון לגבש את דרישות האבטחה, הסטנדרטים וההנחיות המתאימים לו.

ראו בתרשים ובלוח שלהלן את המוסדות הרפואיים שבנוהלי הרכש שלהם יש התייחסות להיבטי אבטחת מידע במכשור רפואי, והפרטים על המוסדות, כפי שעלה במענה על שאלון אבטחת המידע:

90 מחלקות אלה מעורבות לרוב בניהול ובתחזוקה השוטפת של המכשור הרפואי בארגון הרפואי.

91 נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי ממונה אבטחת מידע וסייבר יאשר רכש מכשיר רפואי קודם לקליטתו בארגון.

תרשים 12: **התייחסות להיבטי אבטחת מידע במכשור רפואי בנוהלי הרכש של המוסדות הרפואיים**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 8: **התייחסות להיבטי אבטחת מידע במכשור רפואי בנוהל הרכש של המוסד הרפואי**

כללו התייחסות להיבטי אבטחת מידע במכשור רפואי בנוהל הרכש	לא כללו
מוסד י"ג	מוסד ז
מוסד ד	מוסד י"ז
מוסד ט	מוסד ט"ז
מוסד י"ד	מוסד ו
מוסד י"ב	מוסד י"א
מוסד י	מוסד ב - אין נוהל רכש
מוסד ג	
מוסד א	
מוסד ט"ו	
מוסד ה	
מוסד ח	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עלה כי מבין 16 המוסדות הרפואיים שיש להם נוהל רכש, חמישה: מוסד ז, מוסד י"ז, מוסד ט"ז, מוסד ו, מוסד י"א - לא כללו בנוהלי הרכש שלהם התייחסות להיבטי אבטחת מידע במכשור הרפואי.

מוסד ב ציין בשאלון אבטחת המידע שאין לו נוהל רכש, אך במסגרת מכרזי הרכש שהוא מבצע יש התייחסות להיבטי אבטחת מידע.

מוסד ט"ז מסר בתגובתו כי במסגרת הליך הרכש של מכשור רפואי הספקים מקבלים מסמכי אבטחת מידע של מכשור רפואי מהמוסד הרפואי, ונדרשים גם להגיב על דרישות המוסד בנושא זה.

מומלץ שהמוסדות: מוסד ז, מוסד י"ז, מוסד ט"ז, מוסד ו, מוסד י"א ומוסד ב, יוודאו שנוהל הרכש שלהם יתייחס להיבטי אבטחת מידע של מכשור רפואי, בהתאם להמלצות של תורת ההגנה בסייבר, ובכלל זה - למעורבות בעלי תפקידים בתחום אבטחת מידע, עמידת המכשירים הרפואיים בתנאי סף שקבע המוסד הרפואי והבדיקות שיש לבצע מול הספק.

מוסד י"ז מסר בתגובתו כי יעגן בנוהל את התניית הרכש של מכשור רפואי באישור של ממונה אבטחת מידע.

מוסד ז מסר בתגובתו כי יטמיע נוהל כאמור עד סוף הרבעון הראשון של 2022.

מוסד ו מסר בתגובתו כי לנוכח ממצאי הביקורת עדכן בשנת 2021 את הנוהל באופן שיעסוק בהיבטי אבטחת מידע של המכשור הרפואי.

מוסד ב מסר בתגובתו כי הוא מקבל את המלצת משרד מבקר המדינה.

הליכי אבטחת מידע בעת ביצוע רכש של מכשור רפואי

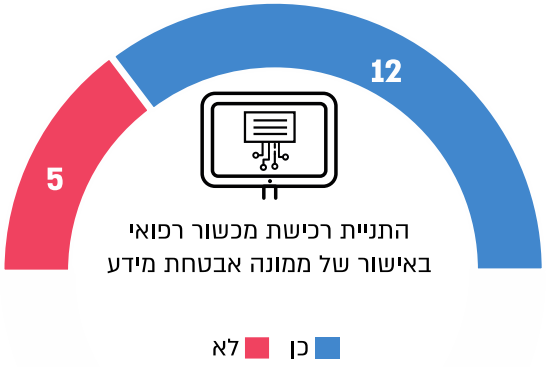
נוהל מכשור רפואי של משרד הבריאות משנת 2018 מחייב את המוסדות הרפואיים לקיים כמה הליכים הנוגעים לאבטחת מידע בעת ביצוע רכש של מכשור רפואי.

אישור ממונה אבטחת המידע לרכש

נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי ממונה אבטחת מידע וסייבר יאשר את רכש המכשיר קודם לקליטתו בארגון. המטרה של קביעה זו היא להבטיח שכבר בעת הליך הרכש - עובדי אבטחת המידע יהיו מעורבים ויבחנו היבטי אבטחת מידע הנוגעים למכשור רפואי, על מנת לצמצם קליטה של מכשירי רפואיים אשר עלולים להגביר את חשיפת הארגון לכשלים בתחום אבטחת המידע, ועל מנת לתת פתרונות אבטחה למכשירים אשר השימוש בהם מלווה בסיכון אבטחתי.

ראו בתרשים ובלוח שלהלן את המוסדות שהתנו את רכישת המכשור הרפואי באישור של ממונה אבטחת מידע, והפרטים על המוסדות, כפי שעלה מהמענה על שאלון אבטחת המידע:

תרשים 13: **התניית רכישת מכשור רפואי באישור של ממונה אבטחת מידע**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 9: **התניית רכישת מכשור רפואי באישור של ממונה אבטחת מידע**

התנו אישור של ממונה אבטחת מידע בביצוע רכש	לא התנו
מוסד י"ג	מוסד ז
מוסד ד	מוסד י"ז
מוסד ט	מוסד י"ד
מוסד י"ב	מוסד ו
מוסד י	מוסד י"א
מוסד ג	
מוסד א	
מוסד ט"ו	
מוסד ב	
מוסד ה	
מוסד ח	
מוסד ט"ז	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה שחמישה מ-17 המוסדות הרפואיים שענו על שאלון אבטחת המידע לא התנו את רכישת המכשור הרפואי בכך שממונה אבטחת המידע יאשר את ביצוע הרכש.

עוד עלה כי לעיתים גם בקרב מוסדות רפואיים שקבעו כי אין לרכוש מכשור רפואי בלי שהתקבל אישור של ממונה אבטחת המידע עדיין התבצע בפועל רכש בלי שהתקבל אישור לכך. למשל:

מוסד ט: ארבעה מ-37 המכשירים הרפואיים והמערכות החדשות שרכש המוסד הרפואי בשנת 2019 נרכשו בלא שממונה אבטחת המידע בחן אותם. כמו כן, אחד מ-23 המכשירים שרכש המוסד בשנת 2020, נבחן על ידי הממונה בדיעבד לאחר רכישתו.

מוסד ט"ו: מפרוטוקול ישיבתה של ועדת ההיגוי לאבטחת מידע וסייבר, שהתקיימה בנובמבר 2019, עולה כי המוסד רכש מכשיר רפואי שנאגר בו מידע ללא אישור התקנה של אגף טכנולוגיות מידע במוסד כנדרש. גם בישיבתה של ועדת ההיגוי ממאי 2020 עלה כי ברכישות קודמות של המוסד היו ליקויים דומים.

על המוסדות הרפואיים שטרם עשו זאת לשלב את ממונה אבטחת המידע בשרשרת האישורים של מכשור רפואי חדש, ועל כלל המוסדות להטמיע הליך זה בפעילות הרכש השוטפת שלהם. באופן זה ממונה אבטחת המידע יוכל להעלות סוגיות בתחום אבטחת המידע, לדרוש תשובות מהספקים או מהיצרנים, ובמידת הצורך - להכין מבעוד מועד את הבקרות המונעות והבקרות המפצות[92] שיש להטמיע.

מוסד י"ז מסר בתגובתו כי לנוכח ממצאי הביקורת מחלקות הרכש וההנדסה יודיעו ליחידת המחשוב על בקשת הרכש, עוד בשלב בחינת המכשיר, על מנת לבחון את התאמתו למדיניות אבטחת המידע של המוסד הרפואי. עוד מסר מוסד י"ז כי יתחיל להתנות רכש של מכשור רפואי באישור של ממונה אבטחת מידע.

מוסד ו מסר בתגובתו כי לנוכח ממצאי הביקורת הוא עדכן בשנת 2021 את נוהלי העבודה שלו וכעת נדרש אישור של ממונה אבטחת המידע בעת רכש של מכשור רפואי חדש.

מוסד ז מסר בתגובתו כי לנוכח ממצאי הביקורת צוות אבטחת מידע ישלח למחלקת הנדסה מסמך עם דרישות אבטחת מידע שעל הספק למלא, ולאחריו הצוות יאשר את הרכש.

הגשת טפסים עם מדדים טכניים ואישור הממונה על אבטחת המידע

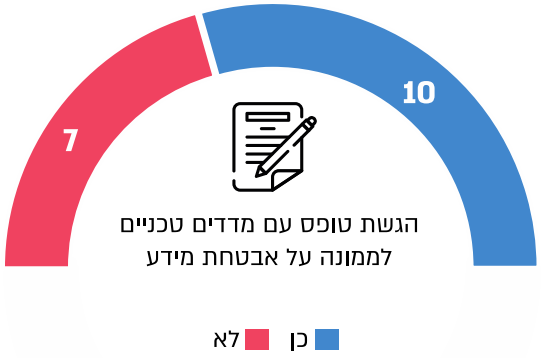
בנוהל מכשור רפואי של משרד הבריאות משנת 2018 נקבע כי עם בקשת האישור לממונה אבטחת המידע יוגשו לו טפסים עם מדדים טכניים הנוגעים לאבטחת המידע של המכשיר על מנת שהממונה יוכל לבחון את המכשיר ולתת את דעתו על רמת האבטחה שבו, על הסיכונים הכרוכים בשימוש בו ועל רמת האבטחה הנדרשת בהתאם לכך. מדדים אלה כוללים פרטים על

92 בקרה מפצה היא כלי שמוטמע בארגון לצורך אבטחת מידע (למשל לאבטחת מידע שבמכשיר רפואי) אם יש חולשות באבטחה שלא ניתן היה למנוע או לנטרל בכלים הקיימים בידי הארגון.

דרך החיבור של המכשיר לרשת, על אופן קבלתם או שליחתם של הנתונים מהמכשיר, האם נדרשת גישה מהארץ או מחו"ל למכשיר לצורך תחזוקה, והאם המכשיר אוגר מידע.

ראו בתרשים ובלוח שלהלן את המוסדות שהגישו טופס עם מדדים טכניים לממונה אבטחת מידע בשנים 2018 - 2021, והפרטים על המוסדות, כפי שעלה מהמענה על שאלון אבטחת המידע:

תרשים 14: **הגשת טופס עם מדדים טכניים לממונה אבטחת מידע, 2018 - 2021**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 10: **הגשת טופס עם מדדים טכניים לממונה אבטחת מידע**

מגישים טופס עם מדדים טכניים לממונה אבטחת מידע	לא מגישים
מוסד י"ג	מוסד ז
מוסד ט	מוסד י"ז
מוסד י"ד	מוסד ג
מוסד י"ב	מוסד ו
מוסד י	מוסד י"א
מוסד ח	מוסד ט"ו
מוסד א	מוסד ב
מוסד ה	
מוסד ד	
מוסד ט"ז	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי שבעה מ-17 המוסדות הרפואיים לא הגישו לממונה אבטחת המידע בשנים 2018 - 2021 טופס ובו המדדים הטכניים הנדרשים במסגרת הליך הרכש כנדרש בנוהל מכשור רפואי של משרד הבריאות משנת 2018.

על המוסדות הרפואיים למלא את הטופס כנדרש, ובכלל זה למלא את הפרטים על המדדים הטכניים הנוגעים למכשור הרפואי, על מנת להציגו לממונה אבטחת המידע במוסד ולקבל את אישורו. כך יוכל הממונה לבחון את המכשיר ולתת את דעתו עליו כאמור, וזאת על בסיס מידע מלא ושלם על המכשור הרפואי.

מוסד ו מסר בתגובתו כי יטמיע בחינה של מדדים טכניים בעת רכש של מכשור רפואי.

מוסד ד מסר בתגובתו כי אין הקפדה מלאה על מילוי טופס אבטחת המידע לפני הרכש, אך מילויו הוא תנאי לחיבור המכשיר לרשת. מוסד ד הוסיף כי יחדד את השימוש בטופס זה ואת חשיבות מעורבות מנהל אבטחת המידע בעת רכישת המכשיר.

מוסד ט"ו מסר בתגובתו למשרד מבקר המדינה מינואר 2022 (להלן - תגובת מוסד ט"ו), כי יסדיר בנוהל את המידע שעליו לשלוח לממונה אבטחת המידע.

מוסד ב מסר בתגובתו כי הוא מקבל את המלצת משרד מבקר המדינה.

הצהרות יצרן בנוגע לאבטחת מידע - בקשה לטופסי MDS²

ארגונים לא ממשלתיים בארה"ב[93] ומומחי אבטחת מידע ניסחו בשנת 2004 מסמך הקרוי MDS² (Manufacturer Disclosure Statement for Medical Device Security) ובו מפרט טכני מעמיק הנוגע למכשור רפואי, שאותו היצרן ממלא ומעביר לרוכש לצורך בחינה של מדדי אבטחת מידע ובטיחות הנוגעים למכשיר הרפואי, כדי להחליט אם המכשיר הרפואי עומד בתנאי אבטחת המידע המתאימים לרוכש. בטופס מציין היצרן, למשל, מהו אופן השמירה וההגנה על המידע הרפואי במכשיר, מהן בקרות הגישה למכשיר וכיצד נקבעות הרשאות הגישה למכשיר. טופסי MDS² הם מעמיקים ומפורטים יותר מאשר הטפסים שהמוסדות בישראל נדרשים למלא כאמור בהתאם לנוהל מכשור רפואי של משרד הבריאות משנת 2018. השימוש ב-MDS² אינו חובה, אולם בארה"ב נעשה בו שימוש בו הולך וגובר על ידי צרכנים אשר דורשים טופס שכזה מהספק או היצרן[94].

יצוין לחיוב כי שישה מ-17 המוסדות הרפואיים שענו על שאלון אבטחת המידע נהגו לבקש טופסי MDS² מהיצרנים (מוסד ט, מוסד י"ד, מוסד י, מוסד א, מוסד ט"ו ומוסד ה), ומומלץ ליתר המוסדות הרפואיים לנהוג כך.

מוסד ח מסר בתגובתו כי ידרוש לקבל את הטופס במסגרת סל הדרישות מהיצרנים.

93 העיקריים שבהם NEMA (National Electrical Manufacturers Association) וה-HIMSS (Health Information and Management Systems Society)

94 CyberMDX, "How MDS² Data Can Inform Smarter Medical Device Workflow", (17.10.19), [קישור].

בדיקות אבטחת מידע עם קבלת המכשיר וטרם הפעלתו

תורת ההגנה בסייבר מדגישה את החשיבות שבהטמעת בקרות בהליכי הרכש לצורך צמצום סכנות בתחום אבטחת המידע והסייבר. מטרת הבקרות - להקטין את הסיכוי כי הרכש של הרכיב החדש או המערכת יחדירו סיכוני סייבר לארגון. על פי תורת ההגנה בסייבר מומלץ, בין היתר, לבצע בדיקות אבטחת מידע ולטפל בחשיפות קודם להטמעת מערכות חדשות בארגון, ולכלול בבדיקות אלה לכל הפחות בדיקות אשר בוחנות את הישימות של אבטחת המכשיר וחשיפות אבטחה, וכן לממש שיטות למניעת הכנסה של רכיבי מערכת מזויפים לארגון, בין במתכוון ובין באמצעות הטעיה של גורם בשרשרת האספקה. תורת ההגנה המעודכנת מדגישה את הצורך לבחון באופן פרטני ועמוק את הבקרה על שרשרת האספקה בארגון. על פי המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי ראוי לבצע הליך של הקשחת[95] הרכיבים במכשיר, ובכלל זה יש להסיר מהמכשיר פונקציות שאינן נדרשות לתפעולו ולניהולו.

צוות הביקורת בדק אם המוסדות הרפואיים בודקים את הנושאים הבאים עם קבלת המכשיר וקודם להפעלתו:

1. נעילת הקונפיגורציה (תצורה) של המערכת באופן שנקבע בנוהל מכשור רפואי של משרד הבריאות משנת 2018, אשר לא יאפשר לשנות את תצורת פעולת המערכת אלא על ידי ספק או יצרן של המערכת בתיאום עם גורמי אבטחת המידע במוסד הרפואי. צעד שכזה יצמצם את האפשרות שגורמים שאינם מורשים לכך יבצעו שינויים טכניים במכשיר שיפגעו בפעילותו או לחלופין יחשפו אותו לאיומי סייבר או יגרמו לזליגת מידע רפואי.
2. גרסאות התוכנה של המכשיר או של רכיביו הן המעודכנות ביותר וכוללות עדכוני אבטחה תקפים הנותנים מענה לפרצות שעלולות לפגוע במכשיר (ראו גם להלן).
3. פונקציות (יישומים) שאינן נדרשות הוסרו מהמכשיר או נוטרלו.
4. בחינה ויישום של השבתת יציאות תקשורת שאינן נחוצות לצורך צמצום חשיפת המכשיר לפגיעות, למשל השבתת תווך תקשורת אלחוטי (WIFI).
5. החלפת שמות משתמש וסיסמאות ברירת מחדל אשר סיפק היצרן, כדי לשפר את האבטחה הכוללת של המכשיר מפני תקיפות סייבר וכדי להקשות את הפריצה למכשיר (ראו גם להלן).
6. סריקת המכשיר באמצעות כלי לזיהוי נוזקות, פוגענים וכן פעילויות חריגות (אנומליות) לאיתור מכשור בעייתי שלא ניתן להשתמש בו או לחברו לרשת.

95 Hardening, משמעו נקיטת פעולות שונות לצורך שיפור האבטחה במכשיר על ידי צמצום הפגיעות שלו.

משאלון אבטחת המידע עולה כי ניכרים פערים בין סוגי הבדיקות שביצעו המוסדות הרפואיים בעת רכישת מכשור רפואי ולפני התחלת השימוש בו ומספרן - שמונה מהמוסדות הרפואיים לא ביצעו יותר ממחצית מהבדיקות האמורות (ארבע בדיקות ומעלה), ושניים מהשמונה לא ביצעו שום בדיקה מבדיקות אלה. יצוינו לחיוב שני מוסדות שביצעו את כל הבדיקות המצוינות בעת רכישת מכשור רפואי וקודם להתחלת השימוש בו.

אחד המוסדות מסר בתגובתו כי לא ביצע את הבדיקות שציין משרד מבקר המדינה בשל הגדרות היצרנים והנזקים העלולים להיגרם למכשיר הרפואי.

על מנת להבטיח רמת הגנה נאותה על המכשירים ועל המידע שנאגר בהם מומלץ שהמוסדות הרפואיים ישלבו בדיקות מקיפות של המכשירים הרפואיים שהם רוכשים ולפני השימוש בהם, הדבר גם עולה מהמלצות תורת ההגנה בסייבר ומהמלצות מערך הסייבר הלאומי להגנה על מכשור רפואי. מומלץ שהמוסדות יקבעו גורם אחראי במוסד שיהיה אמון על ביצוע הבדיקות ועל תיעוד הביצוע.

מוסד אחד מסר בתגובתו כי יפעל להסדרת ביצוען של הבדיקות הנדרשות בעת הרכישה, וזאת הן באמצעות נקיטת הצעדים הנדרשים מול היצרנים והספקים בעת הרכישה, והן באמצעות מערכת לניטור ציוד רפואי שתאפשר לבצע חלק מהבדיקות.

מוסד שני מסר בתגובתו כי החל בשנת 2022 הוא יקפיד להחליף סיסמאות בעת קבלת מכשיר חדש, ולהשבית יציאות תקשורת לא חיוניות.

מוסד שלישי מסר בתגובתו כי יפעל לשפר את הבדיקות שהוא מבצע עם רכישת המכשיר.

מוסד רביעי מסר בתגובתו בנוגע להסרת פונקציות שאינן נדרשות מהמכשיר ולהחלפת שמות משתמש וסיסמאות ברירת מחדל כי במרבית המכשירים אין ביכולתו להסירן בשל הגדרות יצרני המכשור הרפואי שאינן מאפשרות זאת. עוד מסר כי בשנת 2022 ירחיב את היקף הסריקות של מכשירים רפואיים לשם איתור נוזקות, פוגענים ופעילויות חריגות לכלל המכשירים בקופה.

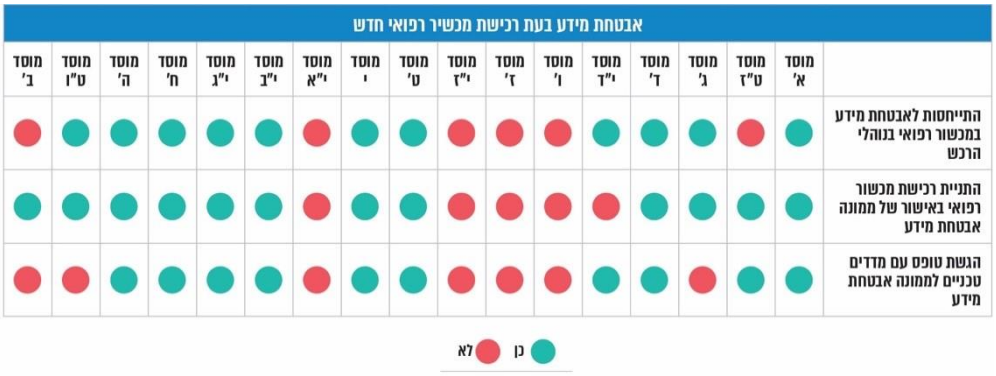
מוסד חמישי מסר בתגובתו כי יוסיף תהליך בקרה על הבדיקות שמבצעים ספקי המכשור הרפואי בהקשר זה, לפי רמת הסיווג של המכשיר.

מוסד שישי מסר בתגובתו כי הוא מקבל את המלצת משרד מבקר המדינה.

☆

להלן בתרשים מוצג ריכוז ממצאים מסוימים בנושא מדיניות אבטחת מידע בעת רכישת מכשיר רפואי חדש, כפי שעלו בפרק זה:

תרשים 15: **ריכוז ממצאים מסוימים בנושא אבטחת מידע בעת רכישת מכשיר רפואי חדש**



כמו כן, עלו פערים נוספים בנושא אבטחת מידע בעת רכישת מכשיר רפואי חדש.

הגנה על המכשירים הרפואיים בזמן השימוש בהם במוסד הרפואי

בעת השימוש השוטף במכשירים הרפואיים (ובפרט במכשירי דימות) על המוסדות הרפואיים לנקוט צעדים על מנת להגן על מכשירים אלה ועל המידע שנאגר בהם. פרק זה מתבסס על תשובות המוסדות הרפואיים שהתבקשו להשיב על שאלון אבטחת המידע; הכללית השיבה בעניין זה בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה - כגוף אחד, ולכן מספרם הכולל של המוסדות שבהם עוסק פרק זה הוא 17.

מיפוי של מערך המכשור הרפואי

לפי תורת ההגנה בסייבר, על ארגון בעל פוטנציאל נזק גבוה בעקבות אירוע סייבר למפות את נכסיו (ובהם יישומונים ארגוניים, תשתיות ממוחשבות ורשת הארגון), את ייעודם ואת הממשקים מהנכס ואליו (בכלל זה נכסים המאוחסנים בענן). בסוף שלב זה יידע הארגון להגדיר מה הם נכסים שחשיבותם רבה מבחינת תפקודו ואילו הם הנכסים המשניים, והדבר יסייע לארגון להגן על הנכסים בהתאם לנזקים האפשריים.

נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי ארגון רפואי יבצע תהליך מיפוי של המכשור הרפואי שברשותו ויתחזק את המיפוי באופן שוטף, זאת על מנת שמנהל אבטחת המידע יוכל ליזום סקרי אבטחת מידע של מערך המכשור הרפואי של המוסד. המיפוי גם יאפשר לארגון הרפואי לנהל את מערך המכשירים הרפואיים שברשותו; יאפשר לו לדעת בכל זמן נתון אילו מכשירים יש בארגון; ולהוסיף מדדים נוספים לאותו מיפוי לצורך ניהול אבטחתי ראוי. כאמור, משרד הבריאות הכין טבלה ובה רשימה המשמשת למיפוי המכשור הרפואי במוסד הרפואי והעביר אותה למוסדות רפואיים ככלי עבודה אפשרי.

מיפוי כללי של מכשור רפואי: עלה כי שישה מ-17 המוסדות הרפואיים שענו על שאלון אבטחת המידע - מוסד י"ד, מוסד י"א, מוסד ו, מוסד א, מוסד ב, ומוסד ה - לא מיפו באופן מלא את כל המכשירים הרפואיים שברשותם.

על המוסדות הרפואיים למפות את המכשור הרפואי שבבעלותם באופן מלא, כנדרש בנוהל מכשור רפואי של משרד הבריאות משנת 2018.

מוסד ו מסר בתגובתו כי ישלים בשנת 2022 את מיפוי המכשור הרפואי שבבעלותו.

מיפוי המכשור הרפואי בהיבטי אבטחת מידע: במסגרת שאלון אבטחת המידע בדק צוות הביקורת האם המוסדות הרפואיים כללו במיפוי של המכשור הרפואי שלהם מאפייני אבטחת מידע עיקריים, שהופיעו בטבלה שהכין משרד הבריאות.

הבדיקה העלתה כי לא כל המוסדות כללו במיפוי שלהם את כל המאפיינים. ראו בתרשים שלהלן את מספר המוסדות שהתייחסו למאפיינים אלה:

תרשים 16: **מאפייני אבטחת מידע שנכללו במיפוי המכשור הרפואי של המוסדות הרפואיים**

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מומלץ כי המוסדות הרפואיים ישלימו את מיפוי מערך המכשור הרפואי שלהם באופן שייכללו בהם מדדים נוספים הנוגעים לאבטחה של המכשירים הרפואיים, למשל בנוגע לתווך החיבור שלהם לרשת, לגרסת התוכנה המותקנת עליהם, למידע שהם אוגרים ולאופי התחזוקה שהם דורשים, זאת בהמשך לנוהל מכשור רפואי של משרד הבריאות משנת 2018 ולטבלה שהכין. באמצעות מיפוי מעודכן מסוג זה יכולים המוסדות לקבל תמונת מצב מקיפה על המכשור הרפואי שבבעלותם, ועל בסיס זה לתכנן את הצעדים הנדרשים לצורך ניהול אבטחתו באמצעות הבקרות המתאימות.

עדכון המיפוי של מכשור רפואי: כאמור, נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי ארגון רפואי יתחזק את המיפוי של המכשור הרפואי באופן שוטף, באופן שיוכל לדעת

בכל זמן נתון אילו מכשירים יש בארגון ולהוסיף מדדים נוספים לאותו מיפוי לצורך ניהול אבטחתי ראוי. הנוהל לא קובע את תדירות המיפוי הנדרשת או המומלצת.

בביקורת עלה כי שני מוסדות (מוסד ו ומוסד י"ד) מ-17 המוסדות שבהם היה מיפוי של המכשור הרפואי עדכנו את המיפוי בפעם האחרונה לפני יותר משנתיים, בשנת 2019; 15 מוסדות עדכנו את המיפוי לכל הפחות באמצע שנת 2020.

בהיעדר תמונת מצב מלאה ועדכנית בנוגע למיפוי המכשור הרפואי במוסד יתקשה צוות אבטחת המידע להגן על המכשור הרפואי הקיים ולהיערך כנדרש, באמצעות כלל האמצעים העדכניים, להתמודדות עם הנזקים האפשריים והסיכונים שהמכשיר חשוף אליהם. על המוסדות הרפואיים לעדכן את המיפוי באופן תדיר ושוטף. מומלץ גם שמשרד הבריאות יקבע את התדירות המזערית הנדרשת לצורך המיפוי.

משרד הבריאות מסר בתגובתו כי ישקול את הצורך בהגדרת תדירות לעדכון המיפוי של המכשור הרפואי במוסדות הרפואיים, וישנה את המדיניות בהתאם לכך.

הגנה פנימית באדריכלות הרשת של הארגון על מכשירים רפואיים

מערך התקשורת של מכשירים רפואיים נקרא IoMT (Internet of Medical Things). הגנה על רכיבי ה-IoMT משמעה הגנה על חלקיו הפיזיים השונים של המכשיר (למשל מסך, מקלדת), על היישומון (אפליקציה) שמותקן בו, על המידע שנאגר בו ומועבר באמצעותו ועל התקשורת שלו עם הרשת. מוסדות רפואיים יכולים להשתמש בכמה כלים כדי לאבטח את המכשור הרפואי ואת רכיביו בעת השימוש בו וכן את החיבור שלו לרשת הארגון. צוות הביקורת בדק אם 15 המוסדות הרפואיים[96] המשתמשים במכשירי MRI ו-CT הטמיעו ברשתות שלהם את אמצעי האבטחה האלה:

מערכת ניטור ובקרה ייעודית למכשור רפואי: מכשור רפואי פועל בתוך רשת, והיא סביבה משתנה (דינמית) שבה מתבצעות פעולות רבות באופן שוטף, ובכלל זה תקשורת מורכבת בין רכיבים שונים המעבירים ביניהם מידע ופקודות ביצוע. בשל ריבוי המכשירים הרפואיים במוסדות הרפואיים ומורכבותם - גובר בשנים האחרונות השימוש במערכות ניטור ובקרה ייעודיות למערך זה[97]. מערכות אלה כבר מוטמעות בחלק מהמוסדות הרפואיים בישראל ובעולם, והן מנטרות את הפעילות של המכשור הרפואי, אוספות מידע על פעולות שבוצעו ומזהות פעילות חריגה בתפקוד המכשור ובתקשורת אליו וממנו - דבר אשר עשוי להעיד על ניסיון תקיפה או זליגה של מידע (למשל תקשורת חריגה מבחינת סוג המידע שמועבר בין המכשיר לבין רכיביו וניסיונות של גורמים שאינם מורשים לכך לקבל גישה למידע). בעקבות ניטור הפעילויות יכול המוסד הרפואי

96 בלאומית ובמכבי אין שימוש במכשירי דימות מסוג MRI ו-CT; הכללית נספרה בנושא זה כגוף אחד הכולל הן את מרפאות הקהילה והן את בתי החולים שלה.

97 זאת לצד מערכות ניטור כללית יותר על כלל הרשת ומשתמשיה, כדוגמת מערכת אשר אוספת נתונים מהרשת (למשל לוגים המתעדים פעולות שבוצעו), מנתחת אותם ובאמצעותם מבצעת בקרת אבטחת מידע על תהליכים ברשת.

לזהות את מקור הפעילות החריגה, לפעול לעצירתה ולמנוע את התפשטותה לחלקים אחרים ברשת המוסד. טיפול בפעילות שמנוטרת בקביעות יכול להתבצע בכל שעות היממה באמצעות צוות האבטחה של המוסד, באופן פיזי או באמצעות טיפול מרחוק.

תווך תקשורת מוצפן בתוך הרשת: המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי כוללות המלצה לשימוש בתקשורת אמינה ומאובטחת הן בין רכיבי המכשור הרפואי עצמם והן בין הרכיבים לרשת הארגונית. בהינתן גישה לגורם עוין לרשת של המוסד הרפואי, הצפנת התקשורת תצמצם את הסיכון שאותו גורם יצליח לקבל גישה למידע שנשלח למכשיר הרפואי או מתקבל ממנו ולפענח את המידע, ובעקבות כך - תקשה על אותו גורם לעיין באותו מידע (למשל מידע רפואי אישי) או לחבל בו.

סגמנטציה (הפרדה) של מכשירי ה-MRI וה-CT ב-VLAN[98] נפרד ברשת: המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי מדגישות גם הן את החשיבות של תכנון אדריכלות הרשת לצורך הגנה, וממליצות לבחון לבודד את המכשירים ב-VLAN ייעודי לצורך צמצום ניצול מרחב התקיפה על המכשירים ושיפור הניטור שלהם.

הגנה על המכשור הרפואי באמצעות חומת אש ייעודית: חומת אש (firewall) היא מערכת היוצרת שכבת הגנה וירטואלית בין רשת הארגון לבין המרשתת; חומת האש חוסמת תקשורת ותעבורה בלתי רצויות, על בסיס כללים אשר בוחנים את המידע, את מקורו, את יעדו וכד'. חומת אש משמשת כלי מרכזי בהגנה הבסיסית הניתנת לרשת של ארגון. לצד התקנת חומת אש אשר מגינה על הרשת הכללית מפני איומי סייבר חיצוניים, ניתן להתקין חומות אש פנימיות בתוך הרשת (למשל על VLAN ייעודי), באופן שישפר את ההגנה על אותה סביבה מפני פוגענים אפשריים ביתר רשת הארגון. על פי המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי, חומת אש המותקנת על המכשיר הרפואי משמשת חוצץ הגנה וכלי להתמודדות עם מתקפת סייבר שמטרתה להשבית מערכות.

הפרדת שרתים: ארגונים עשויים להשתמש בשרת אחד לכמה ייעודים (למשל שימוש באותו שרת לצורך ייעודי, כמו ניהול משתמשים, גם לצורך תפעול ניהולי וגם לתקשורת במרשתת). מתכונת פעילות זו עלולה להגביר את החשיפה לסיכונים - חדירה לאותו שרת או פגיעה בו עלולה להיות נרחבת יותר מאשר לו הפגיעה הייתה בשרת ספציפי המיועד לצורך אחד; אשר לכך, יש מוסדות רפואיים שמייעדים שרת נפרד למכשירים הרפואיים הגדולים (MRI ו-CT) וכך מקטינים את הסיכון לפגיעה במערכות אחרות כאשר יש פגיעה בשרת של מכשירים אלו.

אמצעים חיוניים לצורך שיפור רמת האבטחה ואיתור פוגענים אשר עלולים לחדור את אחת משכבות ההגנה הם שילוב של כלים אלו - מיקום המכשור הרפואי ב-VLAN ייעודי, הגנה על סביבה זו באמצעות חומת אש ייעודית שתפריד בין המערכת לבין יתר הרשת וכן הפרדה מלאה בין השרתים הייעודיים למכשירים אלה לבין יתר השרתים.

98 Virtual Local Area Network - רשת מקומית וירטואלית.

בבדיקה של חמשת הרכיבים במערך ההגנה הפנימית באדריכלות הרשת של המוסדות הרפואיים עלה כי קיימים חֻסָרים מהותיים במערך ההגנה שהמוסדות הרפואיים הטמיעו לצורך הגנה על מכשור רפואי, וכי בחלק מהמוסדות יש שילוב של חֻסָרים המגביר את חשיפתם לסיכוני אבטחת מידע.

מומלץ כי כל המוסדות הרפואיים שבהם עלה חוסר באחד או יותר מהמרכיבים של ההגנה על מכשור רפואי ישלימו את החוסרים שנמצאו אצלם. המלצות אלו תואמות את המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי, ונוכח חשיבותן מומלץ כי המוסדות יאמצו אותן.

מוסדות מסוימים מסרו בתגובתם כי הם מקבלים את המלצת משרד מבקר המדינה ויפעלו בהתאם.

מומלץ כי משרד הבריאות יבחן המענה הנדרש לפערים שעלו בביקורת בתחום זה.

משרד הבריאות מסר כאמור בתגובתו כי הוא נערך לממש מיזם לאומי להגנה על מכשור רפואי במוסדות הרפואיים, שישפר את ההגנה של כל המוסדות הרפואיים. מיזם זה ממתין לאישור תקציבי לשנת 2022.

משתמשים, סיסמאות והרשאות גישה למכשירי דימות עיקריים

הרשאות גישה, ניהול רשימת משתמשים ומדיניות סיסמאות הם כלי מרכזי ביישום מדיניות אבטחת מידע בכל ארגון, וכך גם בנוגע להרשאות שימוש וגישה למכשירים רפואיים במוסדות רפואיים. כלים אלה משמשים בקרות שבאמצעותן ניתן להבטיח כי רק אלה הנדרשים לכך יכולים לגשת למכשור הרפואי, להפעילו ולעיין במידע שמעובד ונאגר בו. כך ניתן להבטיח הגנה על המכשיר עצמו ועל התפעול הטכני שלו, וכן על המידע הרפואי האמור.

בקרות הרשאה פיזית ולוגית

עוד קודם לביצוע כניסת המשתמש למכשיר הרפואי לצורך השימוש בו, עליו להגיע פיזית אל המכשיר ("הרשאה פיזית"). הגבלת הגישה הפיזית למכשיר משפרת את ההגנה עליו ומונעת גישה של גורמים לא מורשים למכשיר עצמו וכן למידע שמעובד ונאגר בו. מעבר לגישה הפיזית למכשיר, ניתן להגדיר בקרות גישה לוגיות לשימוש במכשיר ("הרשאה לוגית"), למשל הגדרת שם משתמש וסיסמה[99] וכן הגדרת מנגנון לעדכון הסיסמאות, לנעילת ההרשאה ולתיעוד פעולות

99 לצורך אבטחה ברמה גבוהה יותר ניתן אף להשתמש בשתי הרשאות לוגיות משולבות (מכונה "two factor authentication"), למשל שימוש בשם משתמש וסיסמה ובד בבד העברת כרטיס עובד. לעיתים במכשירים רפואיים המתקבלים מהיצרנים יש שם משתמש גנרי (דיפולטיבי - Default) - "ברירת מחדל". שינוי שם המשתמש והסיסמה הגנריים ישפר את רמת האבטחה הכוללת של המכשיר מפני תקיפות סייבר ויקשה את הפריצה למכשיר.

המשתמשים במכשור הרפואי. מכשיר רפואי שמוטמעות בו, בה בעת, בקרות פיזיות ובקרות לוגיות יהיה מאובטח יותר.

תקנות הגנת הפרטיות קובעות כי בעל מאגר מידע ינקוט אמצעים כדי לוודא שהגישה למאגר ולמערכות המאגר מתבצעת בידי בעל הרשאה המורשה לכך בלבד. חוזר מנכ"ל משרד הבריאות משנת 2015 קובע כי יש להקנות זכויות פעילות [הרשאות גישה] במערכת המידע על בסיס "הצורך לדעת" ולהתאימן לתפקיד שממלא העובד. נוהל מכשור רפואי של משרד הבריאות משנת 2018 עוסק גם הוא במתן הרשאות וקובע כי יש להגביל את מתן הרשאות הגישה למכשור רפואי ולפקח עליו, בהתאם לרגישות המכשור הרפואי ולרגישות השירותים ברשת הארגון שאליהם המכשור הרפואי מחובר.

מכשיר רפואי מרכזי הנמצא בסביבה פתוחה וללא בקרה לוגית הנדרשת לצורך הפעלתו חשוף לפגיעה בו ובבטיחותו, לגישה בלתי מורשית למידע רפואי אישי, ולהחדרת פוגענים למכשיר ולרשת הארגון.

צוות הביקורת בדק את ההיבטים האלה במסגרת בדיקתם של ארבעה מכשירי דימות:

1. "הרשאה פיזית": האם המכשיר הרפואי נמצא בחדר נעול או בסביבה פתוחה הנגישה לכול.
2. "הרשאה לוגית": האם יש הרשאות לוגיות (אחת או יותר) לשימוש במכשיר: שם משתמש וסיסמה, העברת כרטיס חכם או כרטיס עובד, מזהה ביומטרי ייחודי של העובד (למשל טביעת אצבע), או לחלופין גישה ישירה ללא דרישה להזדהות.

לוח 11: **בקרות הרשאה פיזית ולוגית במכשירי דימות**

	MRI		CT		רנטגן		אולטרסאונד נשים	
שם המוסד*	**בקרת הרשאה פיזית**	**בקרת הרשאה לוגית**	**בקרת הרשאה פיזית**	**בקרת הרשאה לוגית**	**בקרת הרשאה פיזית**	**בקרת הרשאה לוגית**	**בקרת הרשאה פיזית**	**בקרת הרשאה לוגית**
מוסד י"ג	✓	✓	✓	✓	✓	✗	✓	✗
מוסד ז	✓	✓	✓	✓	✓	✓	✓	✗
מוסד י"ז	✓	✓	✓	✗	✓	✓	✓	✓
מוסד ד	✓	✗	✓	✗	✓	✗	חלקי	✗
מוסד ט"ז	✓	✓	✓	✓	✓	✓	✓	✗
מוסד ט	✓	✓	✓	✓	✓	✗	✓	✗
מוסד י"ד	✓	✓	✓	✗	✓	✗	✓	✗
מוסד י"ב	✓	✓	✓	✓	✓	✓	✓	✗
מוסד ו	✓	✓	✓	✓	✓	✓	✓	✗
מוסד י"א	✓	✗	✓	✗	✗	✗	✓	✗
מוסד י	✓	✓	✓	✓	✓	✓	✓	✓
מוסד ג	✓	✗	✓	✗	✓	✗	✓	✗
מוסד א	✓	✓	✓	✓	✓	✓	✓	✓
מוסד ט"ו	✓	✗	✓	✓	✓	✗	✓	✗
מוסד ב	✓	✓	✓	✓	✓	✓	✓	✗
מוסד ה	✓	✓	✓	✓	✓	✓	✓	✓
מוסד ח	✓	✗	✓	✗	חלקי	✗	חלקי	✗

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

* יצוין כי גם מוסדות שאין להם MRI ו-CT סומנו ב-✓.

מהלוח עולה:

- בשלושה מ-17 המוסדות שענו על שאלון אבטחת המידע אין בקרת הרשאה פיזית לגישה לאחד מסוגי המכשירים לפחות. ב-14 מ-17 מוסדות אין בקרת הרשאה לוגית לגישה לאחד מסוגי המכשירים לפחות.
- ב-13 מ-17 המוסדות אין בקרת הרשאה לוגית לגישה למכשיר אולטרסאונד נשים, כלומר מתאפשרת גישה לנתונים השמורים במכשיר, וכך עלולה להיפגע פרטיות המטופלות.
- במוסד י"א אין בקרת הרשאה פיזית וגם לא לוגית על הגישה למכשירי הרנטגן שלו, כך גם בנוגע לחלק ממכשירי הרנטגן במוסד ח.
- במוסד ד, מוסד י"א, מוסד ג ובמוסד ח לא קיימת בקרת הרשאה לוגית בשום סוג של מכשירי הדימות שנבדקו.
- במוסד י"ד ובמוסד ט"ו אין בקרת הרשאה לוגית בשלושה סוגי מכשירים.
- במוסד ד ובמוסד ח לחלק ממכשירי אולטרסאונד נשים לא הייתה גם בקרת הרשאה פיזית וגם בקרת הרשאה לוגית[100].

מומלץ שכל המוסדות הרפואיים יוודאו כי קיימת בקרת הרשאה פיזית ובקרת הרשאה לוגית על הגישה למכשירי הדימות כנדרש בהתאם לתקנות הגנת הפרטיות, לחוזר מנכ"ל משרד הבריאות משנת 2015 ולנוהל מכשור רפואי של משרד הבריאות משנת 2018. הטמעת בקרות אלה חשובה במיוחד בקרב מוסדות שבהם יש מכשירי דימות ללא בקרת הרשאה לוגית ופיזית, שכן בהיעדר בקרה כאמור עלולים להתבצע גישה לא מורשית למכשירים אלה על השלכותיה השונות.

מוסד י"ג מסר בתגובתו למשרד מבקר המדינה בינואר 2022 (להלן - תגובת מוסד י"ג) כי בכוונתו להוסיף את בקרת ההרשאה הלוגית במכשירים אם יתאפשר לבצע זאת מהבחינה הטכנולוגית, וכי יגבש נוהל בנושא וכן יבחן מינוי גורם אחראי לתחום בקרות ההרשאה.

מוסד י"ב מסר בתגובתו כי יפעל להגדיר בקרת הרשאות כניסה לוגית בכל מכשיר שבו ניתן להגדיר בקרה שכזאת. מוסד י"ב הוסיף בתגובתו כי יפעל לשנות את הסיסמאות במכשירים הרפואיים בתדירות קבועה וכן יבחן את האפשרות לנעול את המכשירים לאחר כמה ניסיונות כניסה כושלים בהתאם למאפייני המכשיר. כמו כן מוסד י"ב יבחן את ישימות השימוש בהרשאות אישיות במכשירים רפואיים.

מוסד ז מסר בתגובתו כי במכשירים ישנים לא ניתן להגדיר בקרת הרשאה לוגית. מוסד ז ציין כי יבצע מיפוי של המכשור הרפואי שניתן להוסיף לו בקרת הרשאה לוגית, ינחה להגדיר סיסמאות

100 המוסדות לא ציינו במענה על שאלון אבטחת המידע את מספר המכשירים שאינם נעולים בחדר סגור.

אישיות ולהחליפן אחת לתקופה במכשירים שבהם ניתן לעשות זאת, ופעילות זו תתבצע בשנת 2022. מוסד ז הוסיף כי יבצע גם בקרה על החלפת הסיסמאות האישיות בפרקי זמן שייקבעו.

מוסד ו מסר בתגובתו כי בדק היתכנות להגדרת שם משתמש וסיסמה אישיים ומצא כי הגדרה כזאת תפגע ברצף הפעילות של השימוש במכשירים הרפואיים.

מוסד א מסר בתגובתו כי לא ניתן להגדיר הרשאת גישה אישית לכניסה למערכות הדימות.

מוסד ח מסר בתגובתו כאמור כי במרבית המכשירים אין ביכולתו להחליף שמות משתמש וסיסמאות ברירת מחדל, וזאת בשל הגדרות יצרני המכשור הרפואי.

מוסד ט"ו מסר בתגובתו שבמכשירים רפואיים, כדוגמת מכשירי דימות, שבהם יש קושי טכנולוגי להגדיר בקרת גישה לוגית, הוא הנחה לבצע מחיקה של המידע הנשמר על המכשירים אחת לשבועיים כדרך להתגבר על הקושי.

מוסד ב מסר בתגובתו כי יבחן את האפשרות להוסיף בקרת הרשאה לוגית מהבחינה הטכנולוגית.

מומלץ כי כלל המוסדות הרפואיים ישפרו את מערך הבקרה הלוגית במערך מכשירי הדימות שלהם, ואם קיימת מגבלה להגדרת בקרה כזאת, מומלץ שיטמיעו בקרות מפצות בסביבת עבודה כזאת, על מנת לצמצם את הסיכונים הנלווים לשימוש במכשירים אלה.

עדכון רשימת המשתמשים בעלי הרשאות לוגיות למכשור הרפואי

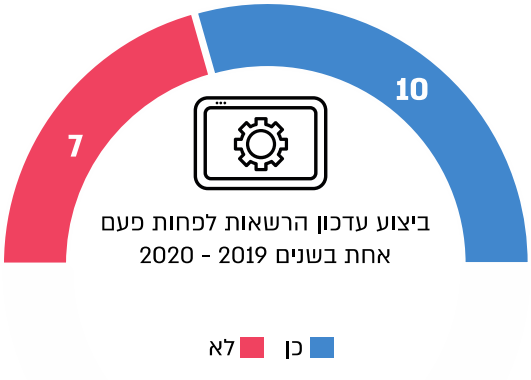
הפעילות הרפואית במוסדות הרפואיים משתנה במהלך הזמן. למשל - רופאים, מתמחים ואחיות פורשים ומגיעים חדשים, עובדים מחליפים תפקיד, צוות המינהלה מתחלף, מכשור רפואי חדש נכנס לשימוש במקום מכשור ישן ועוד. בשל כך יש צורך לעדכן, מפעם לפעם, את רשימת המשתמשים שיש להם הרשאות לשימוש במכשירים הרפואיים וכך להבטיח שתינתן הרשאת הגישה למכשור הרפואי רק למי שנקבע כי היא נדרשת עבורו.

תקנות הגנת הפרטיות קובעות כי בעל מאגר ידאג לביטול הרשאות של משתמש שסיים את תפקידו. בחוזר מנכ"ל משרד הבריאות משנת 2015 נקבע כאמור כי יש להקנות זכויות פעילות [הרשאות גישה] במערכת המידע על בסיס "הצורך לדעת" ולהתאימן לתפקיד שממלא העובד. עוד קובע החוזר כי נדרשת ביקורת תקופתית על פרטי רישום המשתמשים בכל מערכות המידע, על מנת לוודא את שלמותם ודיוקם, וכי עדיין נדרשת גישה למשתמשים הקיימים. נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי הרשאות הגישה לכל העובדים והמכשירים הרפואיים ייבחנו לפי שיקול דעתה של ההנהלה, ויש לבצע בחינה של הרשאות אלה במערכות בעלות סיווג גבוה אחת לשישה חודשים.

צוות הביקורת בדק אם בשנים 2019 - 2020 המוסדות הרפואיים ביצעו לפחות פעם אחת עדכון של רשימת המשתמשים בעלי הרשאות לוגיות למכשירים הרפואיים.

ראו בתרשים ובלוח שלהלן את המוסדות שביצעו עדכון הרשאות לפחות פעם אחת בשנים 2019 ו-2020, והפרטים על המוסדות:

תרשים 17: **ביצוע עדכון הרשאות לפחות פעם אחת, 2019 ו-2020**



לוח 12: **ביצוע עדכון הרשאות לפחות פעם אחת, 2019 ו-2020**

ביצעו עדכון הרשאות בשנים 2019 ו-2020	לא ביצעו
מוסד י"ג	מוסד ז
מוסד י"ז	מוסד ט
מוסד י"ד	מוסד ו
מוסד י"ב	מוסד י"א
מוסד י	מוסד ט"ו
מוסד ג	מוסד ח
מוסד ב	מוסד ד
מוסד ט"ז	
מוסד ה	
מוסד א	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי שבעה מ-17 מוסדות רפואיים לא ביצעו לפחות פעם אחת עדכון של רשימת המשתמשים בעלי הרשאות לוגיות למערך המכשור הרפואי בשנים 2019 - 2020.

אי-ביצוע עדכון של רשימת המשתמשים כאמור במשך שנתיים במערך המכשור הרפואי, הכולל אלפי מכשירים ובכלל זה מכשירים רגישים בעלי חשיבות רבה לפעילות השוטפת של המוסד הרפואי, עלול להגביר את חשיפת המכשירים לאיומי אבטחת מידע וסייבר.

מוסד ח מסר בתגובתו כי אין לו הרשאת גישה לחלק מהמכשור הרפואי לצורך ביצוע עדכון הרשאות.

מומלץ שבהמשך להנחיה שנקבעה בנוהל מכשור רפואי משנת 2018, המוסדות הרפואיים יקבעו בנוהליהם פרקי זמן קבועים לביצוע עדכון של רשימת המשתמשים המורשים במכשור הרפואי ויפעלו לעדכון ההרשאות בהתאם לכך. אשר למכשור רפואי שהוגדר כבעל סיווג גבוה, עליהם להקפיד על עדכון ההרשאות אחת לשישה חודשים, כנדרש בנוהל מכשור רפואי. עוד מומלץ שהמשרד יוודא כי המוסדות מבצעים את עדכון ההרשאות למכשירים המוגדרים בעלי סיווג גבוה על פי הקבוע בנוהל.

מוסד ז מסר בתגובתו כי יגבש נוהל שיחייב כל מנהל יחידה רפואית לבקר את רשימת המשתמשים המורשים להשתמש במכשירים הרפואיים.

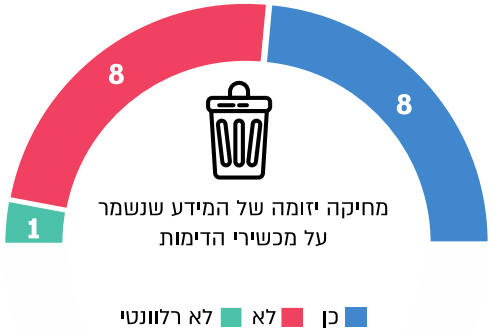
המידע הרפואי הנאגר במכשירי הדימות

מידע רפואי אישי הנאסף במכשירים הרפואיים נשמר בו לפרק זמן מסוים התלוי, בין היתר, בנפח האחסון של המכשיר; המידע גם מועבר בד בבד, או לאחר פרק זמן מסוים, למערכת ארכיב דיגיטלית (PACS, ראו להלן) ובמידת הצורך גם למערכות נוספות ברשת המוסד הרפואי, באופן שאין צורך לשמור לאורך זמן את המידע גם על המכשירים עצמם; אם גיבוי הקובץ נכשל או נפגם - ניתן לחזור לקובץ המקורי השמור במכשיר; בחלק ממכשירי הדימות המפענחים ניתן לעיתים לבצע פעולות פיענוח מורכבות רק בקובץ הצילום המקורי, השמור במכשיר עצמו, ולא בהעתקים שהועברו ממנו אל ה-PACS או אל רשת המוסד.

על פי המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי, יש למחוק מידע ונתונים שנאגרים במכשירים רפואיים, לאחר שימוש במכשיר ועיבוד המידע בו או בעת החלפת המשתמש במכשיר.

ראו בתרשים ובלוח שלהלן את המוסדות שביצעו מחיקה יזומה של המידע שנשמר במכשירי הדימות שלהם, ופרטים על המוסדות האלה:

תרשים 18: **מוסדות שביצעו מחיקה יזומה של המידע שנשמר במכשירי הדימות**



לוח 13: **מוסדות שביצעו מחיקה יזומה של המידע שנשמר על מכשירי הדימות**

מחקו	לא מחקו	לא רלוונטי
מוסד י"ד	מוסד י"ג	מוסד ב*
מוסד א	מוסד י"ז	
מוסד ט"ו	מוסד ד	
מוסד ז	מוסד ט"ז	
מוסד ט	מוסד י"א	
מוסד י	מוסד י"ב	
מוסד ג	מוסד ו	
מוסד ה	מוסד ח	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

* מוסד ב ציין כי מכשירי הדימות שברשותו לא אוגרים מידע.

מהתרשים ומהלוח עולה כי שמונה מ-17 המוסדות הרפואיים שענו על שאלון אבטחת המידע לא מחקו באופן יזום ותדיר מידע שנשמר במכשירי הדימות שהפעילו.

מוסד ח מסר בתגובתו כי מחיקת המידע מהמכשירים הרפואיים עלולה לגרום לאובדן מידע רפואי חשוב הנדרש לעיתים, עד להגעתו בצורה תקינה לארכיב. מוסד ח הוסיף כי קיים קושי תפעולי למחוק מידע מהמכשירים הרבים שברשותו.

מוסד י"ב מסר בתגובתו כי במכשירי ה-MRI וה-CT שברשותו לא ניתן לבצע מחיקה יזומה, וכי הוא יבחן ביצוע מחיקה כזאת במכשירי הרנטגן והאולטרסאונד.

נוסף על המחיקה המובנית המתבצעת בחלק ממכשירי הדימות, המושפעת מנפח האחסון הקיים במכשירים, מומלץ כי המוסדות הרפואיים יסדירו את התהליך לניהול המידע האגור במכשירים הרפואיים, ובכלל זה במכשירי הדימות, ויקבעו את תדירות בדיקת המידע, מהו המידע שנדרש להמשיך לשמור אך ניתן להעבירו למערכות אחסון אחרות, מהו המידע שניתן למחוק ואיזה מידע חשוב שימשיך להישמר במכשיר, וזאת בהמשך להמלצות מערך הסייבר הלאומי להגנה על מכשור רפואי. מומלץ כי פעולה זו תהיה מוסדרת בנוהל אשר יגדיר את בעלי התפקידים שיהיו אחראים לביצוע המחיקה וכן את תדירות ביצועה.

מוסד י"ג מסר בתגובתו כי יגבש נוהל בנושא אשר יסדיר את מחיקת המידע שנשמר במכשירי דימות.

מוסד י"ז מסר בתגובתו כי יבחן את הנושא במסגרת תוכנית העבודה שלו לשנת 2022.

ניהול עדכוני גרסאות תוכנה (Patch Management)

במכשירים רפואיים רבים משולב מחשב עם מערכת הפעלה. בדומה למחשבים אחרים, היצרנים מפרסמים, מפעם לפעם, עדכוני גרסה לתוכנה, באמצעות "טלאים" (אשר מכונים "Patches"), שאותם יש להתקין במכשור הרפואי. חלק מהעדכונים נוגעים לתחום אבטחת מידע, שמטרתם טיפול בפרצות שהתגלו. יש חשיבות עליונה להתקנת עדכוני תוכנה ללא שיהוי הן על מנת לשפר את איכות התפעול של המערכות והן על מנת למנוע פגיעה במערכות ובמידע עד להתקנת העדכונים. סיכון נוסף נשקף גם בשל ניצול לרעה של פרק הזמן שנוצר בין מועד פרסום הצורך בעדכון התוכנה לבין המועד שבו העדכון מתבצע בפועל - תקיפות על ידי פצחנים שיכולים לפגוע בפרצות האבטחה

שה"טלאי" אמור לתת לו מענה.

דוח שפרסם משרד מבקר המדינה בבריטניה בשנת 2018[101] בדק את תגובת שירות הבריאות הלאומי בבריטניה (NHS - National Health Service) על מתקפת סייבר שאירעה במאי 2017 ושמה WannaCry, וממצאיו ממחישים את החשיבות שבביצוע עדכוני תוכנה. במתקפה זו נפגעו 80 מרכזים רפואיים (בתי חולים ומרפאות), והיא הובילה למניעת גישה של צוות שירותי הבריאות לתיקים רפואיים ולנעילה של מכשור רפואי, דבר ששיבש את הפעילות של מכשירי דימות ומכשור מעבדתי. בדיקת מבקר המדינה בבריטניה העלתה כי בחודשיים שקדמו לתקיפה צוות אבטחת המידע בשירותי הבריאות הלאומי התריע לפני המרכזים הרפואיים כי יש להתקין "טלאי" אבטחת מידע כדי למנוע פגיעה באמצעות פרצת האבטחה שאכן נוצלה בפועל במתקפת WannaCry. בדוח צוין שמרכזים רפואיים רבים לא ביצעו את העדכונים הנדרשים, ובעקבות כך מערכות המידע במרכזים אלה הותקפו בהצלחה והפעילות בהם שובשה.

בעקבות מתקפת סייבר על המרכז הרפואי הלל יפה באוקטובר 2021, פרסם מערך הסייבר הלאומי המלצות לארגונים, על מנת שיוכלו לזהות מתקפה דומה ולמנוע התרחשותה. המערך

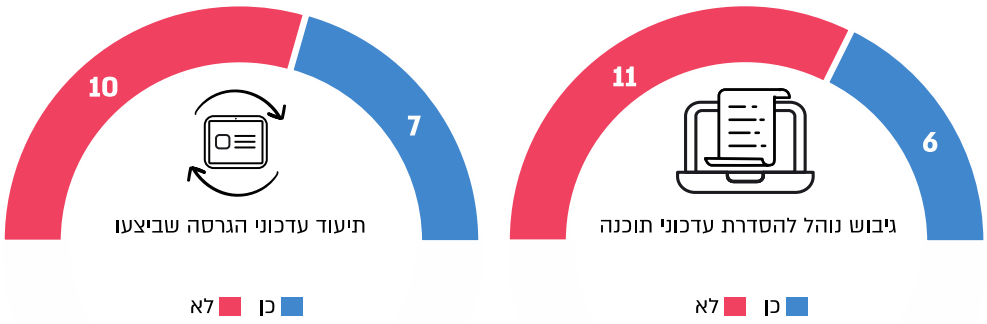
101 National Audit Office ,(NAO) ;"Investigation: WannaCry cyber attack and the NHS", 2018

המליץ, בין היתר, לוודא כי כלל שרתי הדואר האלקטרוני (דוא"ל) וה-VPN[102] משודרגים לגרסאות עדכניות, וליזום החלפת סיסמאות גורפת לכל המשתמשים בשרתים אלו, למקרה שהתוקף השיג אחיזה בהם[103].

על פי המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי ראוי שהארגונים ישלטו בתהליכי עדכוני התוכנה, שיוגדרו במדיניות הארגון לביצוע בתדירות סבירה או ייקבעו על פי מידת דחיפותם, לצורך צמצום הסיכונים שבהם. נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי על מנת להבטיח פעולה רציפה ובטוחה של המכשור הרפואי יש צורך בעדכון מתמיד של גרסאות היצרן העדכניות. על מנת לעמוד בדרישה זו יש להגדיר מדיניות ותהליכים ולהתייחס לניהול מבוקר של שינויים בתפעול, בתשתיות ובמערכת, ולקיים תהליך לביצוע עדכונים ו"טלאים" מאומתים למערכות הפעלה או לתוכנת המכשיר הרפואי, בהתאם לצרכים.

להלן בתרשים מוצגים המוסדות הרפואיים על פי פעולותיהם בתחומים אלה: גיבוש נוהל המגדיר את מדיניותם בנושא עדכון תוכנה ותיעוד עדכוני הגרסאות במכשירים, וכן מוצגים בתרשים פרטים על המוסדות:

תרשים 19: **גיבוש נוהל להסדרת עדכוני תוכנה ותיעוד של עדכוני הגרסאות שבוצעו**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

102 Virtual Private Network - רשת וירטואלית פרטית המשמשת כתווך תקשורת מאובטח.

103 מערך הסייבר הלאומי - התרעות, "מתקפת כופרה כנגד גוף במגזר הבריאות בישראל" (13.10.21). [קישור].

לוח 14: **גיבוש נוהל להסדרת עדכוני תוכנה ותיעוד עדכוני הגרסאות שבוצעו**

שם המוסד	האם המוסד גיבש נוהל להסדרת עדכוני תוכנה	האם המוסד תיעד את עדכוני הגרסה שביצע במכשירים הרפואיים
מוסד י"ג	✓	✓
מוסד ז	✗	✓
מוסד י"ז	✗	✓
מוסד ד	✗	✗
מוסד ט"ז	✓	✗
מוסד ט	✗	✓
מוסד י"ד	✗	✗
מוסד י"ב	✗	✗
מוסד ו	✗	✗
מוסד י"א	✗	✗
מוסד י	✗	✓
מוסד ג	✓	✓
מוסד א	✗	✗
מוסד ט"ו	✓	✗
מוסד ח	✓	✗
מוסד ב	✓	✗
מוסד ה	✗	✓

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשימים ומהלוח עולה ש-11 מ-17 המוסדות הרפואיים לא גיבשו נוהל המסדיר את האופן שבו על המוסד הרפואי לעדכן תוכנה, לרבות במכשירים רפואיים, וכי עשרה מהמוסדות לא תיעדו את עדכוני גרסאות התוכנה שביצעו במכשירים הרפואיים. מוסד ד, מוסד י"ד, מוסד י"ב, מוסד ו, מוסד י"א ומוסד א לא גיבשו נוהל כאמור ולא תיעדו את עדכוני גרסאות התוכנה שביצעו.

מומלץ שכלל המוסדות הרפואיים ישלימו גיבוש של נוהל המסדיר את התהליך לעדכוני התוכנה במוסד הרפואי, בהתאם לנוהל מכשור רפואי של משרד הבריאות משנת 2018 ולהמלצות מערך הסייבר הלאומי להגנה על מכשור רפואי. במסגרת זו מומלץ לקבוע את התדירות הנדרשת לביצוע העדכונים, לקבוע אילו גורמים האחראים לכך ולפרט את הדרך לביצוע העדכונים בפועל, בשים לב לכך שיש לצמצם במידת האפשר מפגיעה בפעילות השוטפת של המרכז הרפואי. מומלץ גם שהמוסדות יתעדו את כל עדכוני הגרסאות שביצעו במערכות המחשוב, ובכלל זה במערך המכשור הרפואי.

מוסד ו מסר בתגובתו כי יגבש נוהל המסדיר את תהליך עדכוני התוכנה וכן את תיעודם.

מוסד י"ז מסר בתגובתו כי יקדם את הנושא במסגרת תוכנית העבודה שלו לשנת 2022.

מוסד ז מסר בתגובתו כי יגבש נוהל בתחילת שנת 2022.

מוסד י"ב מסר בתגובתו כי יגבש נוהל להסדרת עדכוני תוכנה ויתעד את עדכוני הגרסה שהוא מבצע במערכת ניהול המכשירים.

מוסד ח מסר בתגובתו כי יקפיד לתעד את עדכוני הגרסה במכשירים הרפואיים.

מוסד ב מסר בתגובתו כי יתעד את כל עדכוני הגרסאות שהוא מבצע.

מוסד ט"ו מסר בתגובתו כי רכש מערכת לניטור ולמיפוי של ציוד רפואי שתמפה, בין היתר, גם את מצב עדכוני הגרסה בכל מכשיר שמחובר לרשת, וכך יוכל לתעד את עדכוני הגרסאות.

מבדקי חדירה למכשירים רפואיים

מבדקי חוסן הם מבדקים שנועדו לאתגר את מערכות האבטחה של הארגון ולאתר פרצות אבטחה וסיכונים אפשריים. ראו בתרשים שלהלן את סוגי מבדקי החוסן שניתן לבצע:

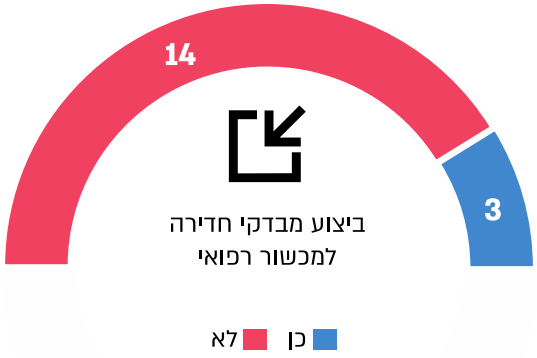
תרשים 20: **סוגי מבדקי החוסן שניתן לבצע בארגון**

מבדק חדירה (Penetration Test - PT): מבדק חדירה הוא הליך שבמהלכו מתבצעת תקיפה מבוקרת ומתוכננת של המערכת הממוחשבת של הארגון על מנת לאתר בה חולשות. המבדק יכול להתבצע בכמה סביבות עבודה של המערכות הממוחשבות, ובהן סביבה "נקייה" שאפשר לבצע בה בדיקות עם סיכון נמוך לגרימת נזק למערכות המידע (סביבת בדיקה - Testing), או לחלופין במערכות הממוחשבות עצמן (סביבת ייצור - Production) באופן שמאפשר לבחון באופן מדויק יותר את החולשות במבדק החדירה, אך הכרוך בסיכון גדול יותר לפגיעה במערכות אלה.

מבדקי חדירה - המלצות מערך הסייבר הלאומי: על פי המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי, יש לבצע מבדקי חדירה תקופתיים על רכיבי המכשור הרפואי כדי לוודא את חוסנה של הרשת ושל הרכיבים. רצוי כי מבדקים אלה יתמקדו בשינויים שניתן לבצע ברשת בסביבת המכשירים, בתפקודם של המכשירים וביכולות לתקוף מהרשת את הרכיבים ולתקוף מהרכיבים את הרשת.

נוהל מכשור רפואי: נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי מנהל אבטחת המידע בארגון ייזום מבדקי חדירה למערך המכשור הרפואי הן ברמת התשתית והן ברמת היישום (אפליקציה), במידת האפשר בשיתוף ספקי המכשור והנציגים של יצרני המכשור, או לחלופין במבדקים שיבצעו יצרני המכשור. הנוהל קובע שעל מבדקים אלה לדמות ניסיונות פריצה שפצחנים יכולים לבצע מתוך המוסד או מחוצה לו. עוד נקבע בנוהל כי גורם מקצועי, עצמאי, בלתי תלוי וחיצוני למוסד הוא זה שיבצע את מבדקי החדירה. להלן בתרשים ובלוח מוצגים המוסדות על פי ביצוע מבדקי חדירה למכשור רפואי בשנים 2018 - 2021, וכן פרטים על המוסדות:

תרשים 21: **המוסדות שביצעו מבדקי חדירה למכשור רפואי, 2018 - 2021**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 15: **ביצוע מבדקי חדירה למכשור רפואי בידי המוסדות**

ביצעו מבדק חדירה	לא ביצעו
מוסד י"ג	מוסד ד
מוסד א	מוסד י"ד
מוסד ח	מוסד י"ב
	מוסד ו
	מוסד י"א
	מוסד ט"ו*
	מוסד ט"ז**
	מוסד ב
	מוסד ז
	מוסד י"ז
	מוסד ט
	מוסד י
	מוסד ג
	מוסד ה

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

* מוסד ט"ו מפעיל באופן קבוע שתי מערכות המדמות תקיפה ברשת, כדי לאתר חולשות וקווי תקיפה, בין היתר למערכות, לציוד רפואי ולמערכת ההדמיה עצמה (PACS).

** מוסד ט"ז ציין שלא ביצע בדיקת חדירה ממוקדת למכשור, אך בדק גישה למכשור רפואי במסגרת בדיקת חדירה כללית למוסד הרפואי.

מהתרשים ומהלוח עולה שרובם המוחלט של המוסדות הרפואיים - 14 מוסדות (כ-82%), לא ביצעו מבדקי חדירה שכללו תקיפה של מכשור רפואי בשנים 2018 - 2021. רק מוסד ח, מוסד י"ג ומוסד א ביצעו בתקופה זו מבדקי חדירה למכשור רפואי.

את המבדקים בשלושת המוסדות האמורים ביצעו חברות חיצוניות שהמוסדות התקשרו עימן, ובמוסד ח בוצעו חלק מהבדיקות בידי צוות אבטחת המידע של המוסד. הבדיקות כללו ניסיון חדירה למכשירים באופן שפגע באמינות ובזמינות שלהם, ניסיונות להזליג מידע מהמכשירים או מהשרתים שלהם ואף ניסיונות חדירה למכשירי דימות גדולים כמו MRI ו-CT.

מוסד י"ז מסר בתגובתו כי מבדקי חדירה שביצע לא כללו את נושא המכשור הרפואי עקב עלותם הגבוהה.

על המוסדות הרפואיים לפעול בהתאם לנוהל ולשלב בתוכניות העבודה שלהם מבדקי חדירה עיתיים למכשור רפואי הן ברמת התשתית והן ברמת היישום. מומלץ כי המבדקים יבוצעו על בסיס סקר סיכונים שיכינו המוסדות ויאפשר לזהות את המכשירים הרפואיים החשופים לסיכון האבטחתי הגבוה ביותר, וכי בהתאם לכך תיקבע שיטת המבדק.

מוסד ו מסר בתגובתו כי יבצע מבדקי חדירה למכשור רפואי בהתאם לסיווג רמת הסיכון של המכשירים.

מוסד ז מסר בתגובתו כי יבצע מבדקי חדירה במסגרת תוכנית העבודה שלו לשנת 2022.

מוסד י"ב מסר בתגובתו כי יבחן את האפשרות לבצוע מבדק חדירה במכשור רפואי.

מוסד ב מסר בתגובתו כי הוא מקבל את המלצת משרד מבקר המדינה אך הוסיף כי ייתכן שיהיה קושי לבצע מבדקי חדירה במכשירים רפואיים בשל הסיכון לפגיעה במכשיר הרפואי והחשש לביטול אחריות הספק או היצרן למכשיר.

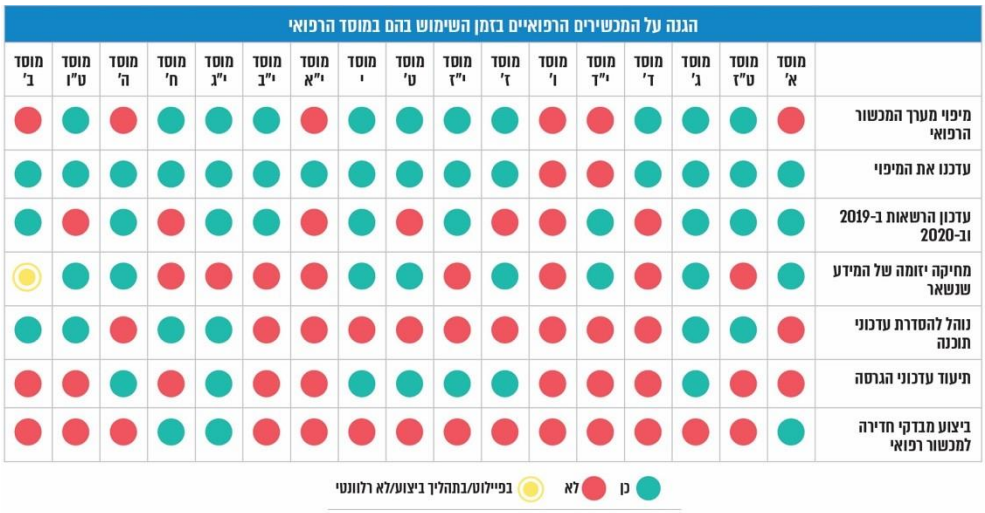
בשל סיכוני הסייבר ההולכים ומתעצמים ובשל החשיבות בביצוע מבדקי חדירה למכשירים רפואיים לצורך איתור חולשות בהם, מומלץ שמשרד הבריאות יעקוב אחר ביצוע מבדקי חדירה שביצעו המוסדות הרפואיים במכשירים הרפואיים.

משרד הבריאות מסר בתגובתו כי יבחן את האפשרות לבצע מעקב אחר מבדקי חדירה למכשור רפואי, וכי ישנה את המדיניות אם ימצא לנכון.

☆

להלן בתרשים מוצג ריכוז ממצאים מסוימים בנושא הגנה על המכשירים הרפואיים בזמן השימוש בהם במוסד הרפואי, כפי שעלו בפרק זה:

תרשים 22: **ריכוז ממצאים מסוימים בנושא הגנה על המכשירים הרפואיים בזמן השימוש בהם במוסד הרפואי**



כמו כן, עלו פערים נוספים בתחום זה.

על המוסדות הרפואיים והנהלתם מוטלת האחריות לפעול להגן על מערכות המידע של מוסדותיהם ובכלל זה על המכשור הרפואי, בין היתר באמצעות הקפדה על הנחיות אבטחת המידע של משרד הבריאות ונוהלי האבטחה שלו. תקן ISO, תורות ההגנה של מערך הסייבר ונוהלי משרד הבריאות הם חלק מההנחיות המכוונות את פעילות המוסדות בתחום אבטחת המידע, ובפרט בנוגע להגנה על מכשירים רפואיים. בפרק זה הועלו ליקויים הנוגעים להגנה על המכשירים הרפואיים במוסדות הרפואיים בזמן השימוש בהם, ובפרט בנוגע להגנה על מכשירי דימות. בשל איומי הסייבר הגוברים ובשל מורכבותם, מומלץ שמשרד הבריאות יבחן את הפערים שעלו במוסדות הרפואיים מבחינת ההגנה על כלל מכשיריהם הרפואיים, יגבש הנחיות ונוהלי עבודה בנושאים שבהם ניכרת חולשה בפעילות אבטחת המידע במוסדות, ויבצע בקרה על פעילות המוסדות הרפואיים בכל הנוגע לתחומי אבטחת המידע. עוד מומלץ כי המוסדות הרפואיים יגבשו נוהלי עבודה פנימיים בתחום אבטחת מידע, ובכלל זה בנוגע להגנה על מכשירים רפואיים, ויטמיעו אותם בעבודתם השוטפת.

הגנה על מערכת הארכיב של צילומי ההדמיה - ה-PACS

טכנולוגיית PACS (Picture Archiving and Communication System) היא ארכיב דיגיטלי של צילומי דימות ממכשירי דימות, ובהם MRI ו-CT. מוסדות רפואיים יכולים לרכוש טכנולוגיה זו מספקים שונים המייצרים סביבת עבודה של PACS הכוללת תשתיות, מערכות ושרתים ייעודיים. ה-PACS עשוי לשמור כגיבוי תצלומים למשך תקופות ארוכות, וכפועל יוצא מכך נאגר בו במשך השנים מידע רפואי אישי של מאות אלפי מטופלים.

במשך השנים נחשפו מקרים שבהם זלגו צילומים משרתי ה-PACS שלא אובטחו כראוי. למשל, חברת אבטחת מידע מגרמניה תיארה בשנת 2019 כיצד איתרה שרתי PACS המחוברים למרשתת והצליחה להשיג גישה למאות מיליוני תצלומים רפואיים ובהם פרטים אישיים[104]. במסגרת ההגנה על ה-PACS יש לתת את הדעת, בין היתר, על גיבוי המידע השמור בשרתים אלה, על אפשרות הגישה לתצלומים הנשמרים בשרתים אלה ועל מתן מענה להתרעות אבטחה הנוגעות ל-PACS.

גיבוי ארכיב ה-PACS של מכשירי ה-MRI וה-CT

חשוב מאוד לגבות לטווח הרחוק את תצלומי הדימות הנאגרים ב-PACS, וזאת, בין היתר, מסיבות אלה: רופאים עשויים להידרש בעתיד לבחון מחדש תצלום לצורך מתן אבחנה קלינית ומעקב טיפול; ושמירת המידע מייתרת ביצוע בדיקה נוספת שעלולה לגרום אי-נוחות למטופל או חשיפה לקרינה מיוננת (ב-CT).

תקנות הגנת הפרטיות: על פי תקנות הגנת הפרטיות מידע רפואי מסווג כאמור כמידע שחלה עליו רמת אבטחה בינונית (לכל הפחות)[105], ובעליהם של מאגרים שבהם שמור מידע מסווג ברמה זו נדרש לקבוע נהלים לגיבוי מידע זה באופן תקופתי.

חוזר מנכ"ל משרד הבריאות: חוזר מנכ"ל משרד הבריאות משנת 2015 קובע כי יש להכין עותקי גיבוי של מידע של מערכות מידע ולבדוק מידע זה באופן סדיר, לפי מדיניות גיבוי מוסכמת.

נוהל מכשור רפואי של משרד הבריאות: נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי הנהלת הארגון תגדיר דרישות לגיבוי מידע של מכשור רפואי שהוגדר כחיוני בתהליך הערכת סיכונים, מנהל אבטחת המידע יהיה אחראי לבקרה על איכות הגיבויים, ואלה יישמרו במקום מרוחק, מאובטח ומוגן מפני פגיעה.

בישראל אירע לפחות מקרה אחד שבו נמחקו תצלומים מה-PACS. בשנת 2014 מרכז רפואי דיווח למשרד הבריאות על שני אירועים שבמהלכם נמחקו ממערכת ה-PACS שלו כ-2,700 תצלומים של מטופלים שלא היה ניתן לשחזרם, כיוון שה-PACS לא היה מגובה. בסיכום של תחקור האירוע

104 "Update Issued on Unsecured PACS as Exposed Medical Image Total Rises to 1.19 Billion", HIPPA Journal website.

105 בהתאם לתנאים שנקבעו בתוספת הראשונה והשנייה לתקנות.

משנת 2014 הדגיש משרד הבריאות כי מרכזים רפואיים נדרשים לגבות מידע ממוחשב כפי שקבע חוזר מנכ"ל משרד הבריאות בשנת 2012[106], ואף ציין כי האירוע דווח ל-FDA.

ביצוע גיבוי יומי ל-PACS

נמצא כי 15 המוסדות הרפואיים שנבדקו ומשתמשים במכשירי MRI או CT[107] - השתמשו ב-PACS.

בביקורת עלה כי כל המוסדות מבצעים גיבוי ל-PACS לפחות פעם ביום, פרט למוסד י', שלא ביצע גיבוי של ה-PACS, ובמועד סיום הביקורת נמצא בתהליך הטמעה של מערכת גיבוי.

שמירת העתקי גיבוי של PACS

נמצא כי 14 מ-15 המוסדות שהשתמשו ב-PACS שומרים לפחות העתק אחד של הגיבוי כדי להבטיח את שרידותו.

עלה כי במוסד י"ז אין גיבוי מלא של צילומי הדימות במערכת ה-PACS.

מוסד י"ז מסר בתגובתו כי הסיבה לכך היא עלויות גבוהות של הפעולה.

משרד מבקר המדינה ממליץ למוסד י"ז לשפר את שרידות הצילומים ב-PACS באמצעות שמירה של העתק גיבוי אחד לפחות, וכך להבטיח כי אם ייפגע הגיבוי הקיים בעת מתקפת סייבר או תקלה טכנית, תהיה אפשרות לשחזר את התצלומים. זאת בהתאם לנוהלי משרד הבריאות.

הפצת התרעות בנוגע לפרצות באבטחת מידע במכשור רפואי וברכיביו

כלי מרכזי לשיפור ההגנה מפני תקיפות סייבר הוא מודיעין איכותי הכולל מידע על כוונות תקיפה של פצחנים ברחבי העולם, על טכניקות העבודה של גורמים אלה ועל חולשות חדשות שהתגלו במערכות מידע. בהחלטת הממשלה בנושא הגנת הסייבר משנת 2015 נקבע שאחד מתפקידי היחידה המגזרית הוא לגבש ולהפעיל תהליכי שיתוף מידע פנימיים וחיצוניים בתוך המגזר, וכן להגדיר נהלים ושיטות להעברת מידע בין הגופים במגזר.

משרד הבריאות מפעיל כאמור SOC שהוא חמ"ל לניטור, אירועי אבטחת מידע וסייבר במגזר הבריאות, לשליטה ולבקרה עליהם, ובמסגרת פעילותו הוא משתף מידע עם המוסדות הרפואיים

106 משרד הבריאות, חוזר מנכ"ל מס' 18/12 בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות" (13.9.12). קיים נוסח מעודכן לחוזר - חוזר מנכ"ל משרד הבריאות משנת 2015.

107 ללאומית ולמכבי אין מכשירים כאלה.

ומוסר להם התרעות. מידע זה יכול להתקבל ממגוון מקורות: ממחקרים שמבצעים אנליסטים בתחום הסייבר העובדים ב-SOC, ממוסדות רפואיים אחרים, מיצרנים וספקים של מכשור רפואי, מכתבות חדשותיות, ממערך הסייבר הלאומי, מגורמי ביטחון נוספים ומשיתוף ידע עם ארגונים בחו"ל.

לנוכח החולשות שהתגלו ב-PACS, בשנים 2018 - 2021 פרסמו הרשויות האמריקניות הנחיות והתרעות הנוגעות לטיפול בחולשות אלה: בדצמבר 2020 ביצע המכון הלאומי לתקנים וטכנולוגיה בארה"ב[108] סקר סיכונים מקיף לחולשות של ה-PACS ופרסם מסמך מנחה ובו מפורטות הדרכים להתמודד עם חולשות אלה[109]; בשנים 2018 ו-2021 כמה סוכנויות ממשל בארה"ב פרסמו התרעות על פרצות אבטחה ב-PACS במכשירי דימות ספציפיים[110].

היות שהתרעות אלו היו רלוונטיות גם למוסדות הרפואיים בישראל שיש בהם מערכת כזאת, צוות הביקורת בדק אם הגורמים הלאומיים - מערך הסייבר הלאומי ומשרד הבריאות - הפיצו אותן למוסדות הרפואיים.

מערך הסייבר הלאומי מסר לצוות הביקורת כי בשנים 2019 - 2021 הוא לא הפיץ התרעות בנושא מכשירי דימות ובכלל זה התרעות בנוגע לפגיעה אפשרית בטכנולוגיות ה-PACS. משרד הבריאות מסר לצוות הביקורת כי התרעות אלה לא הגיעו לידיו. מוסד י"ד ומוסד ג, שבידיהם מכשירי דימות ו-PACS שבהם עסקו ההתרעות האמורות, מסרו לצוות הביקורת כי הם לא קיבלו התרעות אלה ממערך הסייבר הלאומי ומהמשרד.

משרד הבריאות הוסיף וציין כי לפי עמדתו, מערך הסייבר הלאומי הוא שאחראי לריכוז כלל ההתרעות בתחום המכשור הרפואי, ובכלל זה לביצוע חיפושים יזומים לאיתור חולשות בתחום זה, וכי המערך מפעיל כמה כלים לטובת הנושא. המשרד הוסיף כי הוא התקשר עם חברה חיצונית המפעילה עבורו אנליסט בתחום הסייבר, אולם התקשרות זו מבוצעת בהתאם לתקציב המשרד ובהיקף משרה חלקי.

היעדרה של התרעת האבטחה בנושא ה-PACS מעורר חשש שמערך הסייבר הלאומי ומשרד הבריאות אינם מנטרים את כל ההתרעות החושפות פגיעה אפשרית במערכות המידע הרפואיות, ובפרט התרעות קריטיות הנוגעות למכשור רפואי.

מומלץ כי משרד הבריאות ומערך הסייבר הלאומי יפעלו להעשרת מקורות המידע המשמשים אותם לצורך איסוף התרעות אבטחת מידע הנוגעות למכשור הרפואי, לרבות מהגופים הרלוונטיים בעולם, ויפיצו אותן למוסדות הרפואיים בהתאם לכך.

משרד הבריאות מסר בתגובתו כי הוא פועל לשפר את מקורות המידע המשמשים אותו.

108 National Institute of Standards and Technology - NIST.

109 Securing Picture Archiving and Communication System (PACS), NIST 1800-24A, 2020

110 Cybersecurity and Infrastructure Security Agency, 2018, ICS Advisory (ICSMA-18-037-02), [קישור] ; Picture Archiving Communication Systems (PACS) Vulnerabilities, 2021, HHS Cybersecurity Program

הגנה על המכשירים ועל המידע שבהם בעת תחזוקתם ובעת פיענוח תוצאות

תחזוקת מכשירי דימות

מכשירי דימות משמשים מוסדות רפואיים שנים רבות (לעיתים אף עשרות שנים), ולפיכך נדרשת תחזוקה שוטפת בעת השימוש בהם. יש ארבע דרכים לביצוע התחזוקה: באמצעות טכנאים עובדי המוסד הרפואי, באמצעות טכנאים חיצוניים המגיעים למוסד הרפואי עצמו לתיקון המכשירים, באמצעות התחברות מרחוק של אנשי תחזוקה למכשיר, או באמצעות הוצאת המכשיר אל מחוץ לכותלי המוסד לביצוע תחזוקה חיצונית. פרק זה מתבסס על תשובות המוסדות הרפואיים שהתבקשו להשיב על שאלון אבטחת המידע; הכללית השיבה בעניין זה בשם כל שמונת המרכזים הרפואיים הכלליים שלה ומרפאות הקהילה - כגוף מרוכז אחד, ולכן מספר המוסדות הכולל הוא 17.

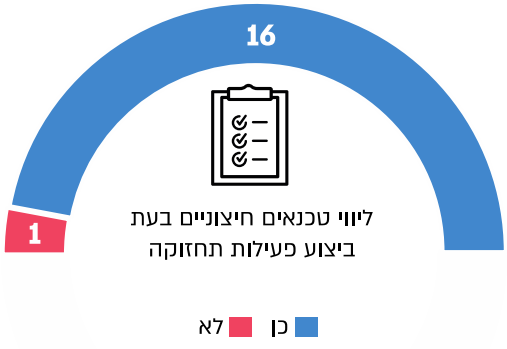
טכנאים המבצעים עבודת תחזוקה במכשירים הרפואיים במוסד הרפואי

ב-17 המוסדות הרפואיים שענו על שאלון אבטחת המידע מתבצעת תחזוקה של מכשירים באמצעות טכנאים המגיעים למוסד הרפואי.

על פי המלצות מערך הסייבר הלאומי להגנה על מכשור רפואי, יש למנוע באופן ממשי גישה לא מורשית למכשור הרפואי ולרכיביו או למנוע ביצוע שינויים בסביבות המכשור הרפואי ורכיביו, למשל באמצעות ליווי של הטכנאים על ידי עובדים מטעם המוסד הרפואי.

ראו בתרשים ובלוח שלהלן את המוסדות בהם עובדי המוסד הרפואי מתלווים לטכנאים החיצוניים בעת ביצוע פעילות התחזוקה במכשירים הרפואיים, והפרטים על המוסדות:

תרשים 23: **המוסדות שבהם עובדי המוסד הרפואי מתלווים לטכנאים החיצוניים בעת ביצוע פעילות התחזוקה במכשירים הרפואיים**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 16: **המוסדות שבהם עובדי המוסד הרפואי מתלווים לטכנאים החיצוניים בעת ביצוע פעילות התחזוקה במכשירים הרפואיים**

המוסדות בהם עובדי המוסד מתלווים לטכנאים	המוסדות בהם עובדי המוסד לא מתלווים לטכנאים
מוסד ז	מוסד י"א
מוסד י"ז	
מוסד ג	
מוסד ד	
מוסד ט	
מוסד י"ד	
מוסד ב	
מוסד י"ב	
מוסד י"ג	
מוסד י	
מוסד א	
מוסד ט"ז	
מוסד ו	
מוסד ח	
מוסד ט"ו	
מוסד ה	

על פי מענה המוסדות הרפואיים לשאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

עלה כי במוסד י"א אנשי המוסד הרפואי מלווים את הטכנאים החיצוניים רק בחלק מזמן הימצאותם במוסד ואינם עוקבים אחר פעילות התחזוקה המתבצעת בפועל, ולא מתבצע תיעוד מלא של ביקורי הטכנאים.

בהמשך להמלצות מערך הסייבר הלאומי להגנה על מכשור רפואי, מומלץ כי מוסד י"א יוודא כי טכנאים חיצוניים המבצעים עבודות תחזוקה במוסד הרפואי יגיעו למוסד רק לאחר תיאום עם הגורמים הרלוונטיים, וכי במסגרת עבודתם הם ילוו כל העת בעובד המוסד. כך ניתן יהיה לפקח על עבודתם ולצמצם את חשיפת המכשור הרפואי לסיכוני אבטחת מידע - חשיפת מידע רפואי אישי והעתקתו, החדרת פוגענים למכשיר, ביצוע שינויים במידע שנאגר על המכשיר או ברכיבי המכשיר, חבלה מכוונת או שאינה מכוונת ועוד.

מוסד י"א מסר בתגובתו כי במסגרת תוכנית העבודה שלו לשנת 2022 הוא יפעל לתיעוד ביקורי הטכנאים החיצוניים במוסד הרפואי.

חתימה על הסכם סודיות

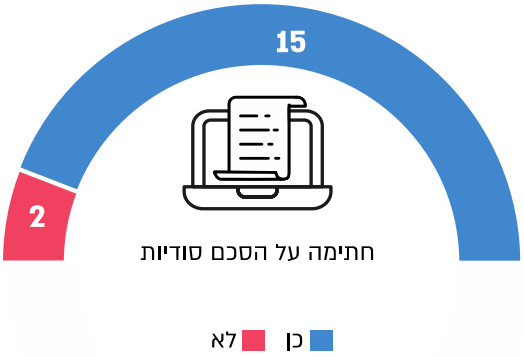
על פי תקן ISO מוסדות רפואיים הנעזרים בשירותיהם של צדדים שלישיים, כאשר שירותים אלה כוללים עיבוד של מידע רפואי אישי, חייבים להשתמש בחוזים המפרטים, בין היתר: צעדי ביטחון שיש ליישם, ההגבלות החלות על צדדים שלישיים לעניין הגישה לשירותים הרפואיים וצעדי ענישה שיינקטו נגד כל גורם שלא יעמוד בתנאי החוזה. עוד נקבע בתקן ISO כי כאשר צד שלישי אינו מעבד מידע רפואי אישי [למשל כאשר טכנאים מבצעים עבודת תחזוקה במכשירים הרפואיים במוסד הרפואי], "ייתכן ועדיין יהיה מקום לנסח קטע מתאים" מתוך סעיפי החוזה האמור, וכי מומלץ ליישם הסכם המפרט את בקרות אבטחת המידע באספקת שירות על ידי צד שלישי.

על פי תקנות הגנת הפרטיות, בעל מאגר מידע המתקשר עם גורם חיצוני לצורך קבלת שירות הכרוך במתן גישה למאגר המידע יקבע במפורש בהסכם עם הגורם החיצוני, בין היתר, את חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם.

במכתב ששלח ממונה אבטחת מידע במשרד הבריאות למוסדות הרפואיים הוא ציין כי במסגרת מדיניות ההתקשרות עם ספקים חיצוניים, יש להגדיר דרישות אבטחת מידע לספקים אלה ולגורמי צד שלישי, בין היתר באמצעות דרישות להגבלת שיתוף מידע ולחתימה על הסכמי סודיות.

ראו בתרשים ובלוח שלהלן את המוסדות שהחתימו את החברות הנותנות שירותי תחזוקה למכשירים הרפואיים, או את טכנאי חברות אלו, על הסכם סודיות, והפרטים על המוסדות:

תרשים 24: **המוסדות שהחתימו את החברות הנותנות שירותי תחזוקה למכשירים הרפואיים, או את טכנאי חברות אלו, על הסכם סודיות**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 17: **החתמת החברות הנותנות שירותי תחזוקה למכשירים הרפואיים, או טכנאי חברות אלו, על הסכם סודיות**

המוסדות שהחתימו על הסכם סודיות	המוסדות שלא החתימו על הסכם סודיות
מוסד י"ז	מוסד ד
מוסד י"א	מוסד ט
מוסד ט"ז	
מוסד ו	
מוסד י"ד	
מוסד י	
מוסד י"ב	
מוסד י"ג	
מוסד ג	
מוסד ב	
מוסד ח	
מוסד ט"ו	
מוסד ה	
מוסד א	
מוסד ז	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי שני מוסדות רפואיים מ-17 המוסדות שענו על שאלון אבטחת המידע: מוסד ד ומוסד ט, לא החתימו את החברות הנותנות שירותי תחזוקה למכשירים הרפואיים, או את טכנאי חברות אלו, על הסכם סודיות.

מומלץ כי מוסד ד ומוסד ט יגבשו הסכם סודיות כאמור ויחתימו את החברות הנותנות שירותי תחזוקה למכשירים הרפואיים או את טכנאי חברות אלו על הסכם כזה, על מנת לשמור על חסיון המידע הרפואי.

תחזוקה מרחוק של מכשירי MRI ו-CT

מכשור רפואי עשוי להידרש לעיתים לגישת חיבור מרחוק למטרת תחזוקה, שדרוגי תוכנה, כיול, טיפול בתקלות ועוד; את הטיפול יכול לבצע היצרן או ספק התחזוקה של המכשיר מהארץ או מחו"ל[111].

על פי תורת ההגנה בסייבר יש לקבוע מדיניות להתחברות מרחוק, את ההגבלות להיקף השימוש בכלי זה ואת דרישות התצורה הנדרשות לשם כך. בתורת ההגנה המעודכנת נקבע כי על הארגון להכין תוכנית עבודה לצמצום פערי ההגנה בארגון, ובין היתר לוודא כי הגישה אל הרשת נתונה לבקרה של הארגון, באופן שההתחברות של ספקים ועובדים מרחוק לרשת הארגון תהיה מבוקרת.

הסדרת אופן ההתחברות מרחוק לצורך תחזוקה

ל-14 מ-15 המוסדות הרפואיים המפעילים מכשירי MRI ו-CT יש גישה ליצרני המכשירים, המאפשרת להתחבר למכשיר מרחוק לצורך תחזוקה (יצוין כי במוסד ח - המוסד ה-15, לא מתבצע חיבור כזה מטעמי אבטחת מידע).

ראו בתרשים ובלוח שלהלן את המוסדות שהסדירו את אופן ההתחברות מרחוק באמצעות נוהל, והפרטים על המוסדות:

111 נוהל מכשור רפואי של משרד הבריאות משנת 2018.

תרשים 25: **המוסדות שהסדירו את אופן ההתחברות מרחוק באמצעות נוהל**

על פי מענה המוסדות הרפואיים לשאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 18: **הסדרת אופן ההתחברות מרחוק באמצעות נוהל**

הסדירו את אופן ההתחברות באמצעות נוהל	לא הסדירו
מוסד י"ג	מוסד ט
מוסד א	
מוסד י	
מוסד ד	
מוסד י"ד	
מוסד ג	
מוסד ו	
מוסד ט"ז	
מוסד ט"ו	
מוסד ז	
מוסד י"ז	
מוסד י"ב	
מוסד י"א	

על פי מענה המוסדות הרפואיים לשאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי מוסד ט לא הסדיר את אופן ההתחברות מרחוק באמצעות נוהל.

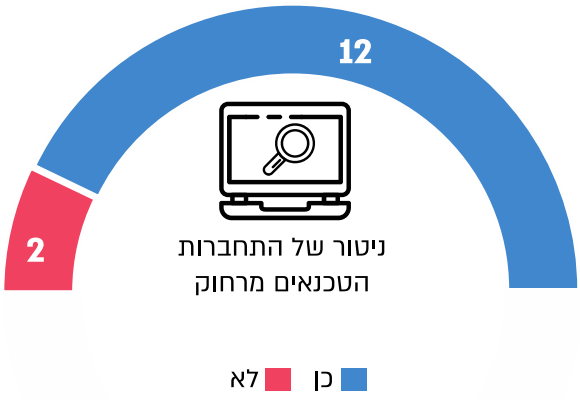
נוכח החשיפה למידע רפואי וסיכוני אבטחת המידע הנלווים לפעילות התחזוקה המתבצעת באמצעות חיבור מרחוק, מומלץ שמוסד ט יסדיר בנוהל את אופן ההתחברות מרחוק.

בקרות על פעילות התחזוקה מרחוק וניטורה

תקנות הגנת הפרטיות קובעות כי במערכות של מאגר מידע ברמת אבטחה בינונית או גבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר. על פי תורת ההגנה בסייבר מומלץ לנטר התחברויות מרחוק לצורך תחזוקה, למשל ניטור פעולות באמצעי כלי ניטור או הקלטת מסכים. על פי תורת ההגנה המעודכנת מומלץ לבצע ניטור שוטף של התשתיות והמערכות בארגון. נוהל מכשור רפואי של משרד הבריאות משנת 2018 קובע כי על המוסד הרפואי לבקר את תהליכי ההתחברות של הספקים למוסד הרפואי תוך התייחסות לפוטנציאל הפגיעה במכשור הרפואי, בהתאם לסיכונים שהגדיר המוסד.

ראו בתרשים ובלוח שלהלן את המוסדות שביצעו ניטור של התחברות הטכנאים מרחוק, והפרטים על המוסדות:

תרשים 26: **המוסדות שביצעו ניטור של התחברות הטכנאים מרחוק**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 19: **ניטור של התחברות הטכנאים מרחוק**

ביצעו ניטור של ההתחברות מרחוק	לא ביצעו
מוסד י"ג	מוסד ט
מוסד א	מוסד י"א
מוסד י	
מוסד ד	
מוסד י"ד	
מוסד ג	
מוסד ו	
מוסד ט"ז	
מוסד ט"ו	
מוסד ז	
מוסד י"ז	
מוסד י"ב	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי שני מוסדות רפואיים - מוסד ט ומוסד י"א - מתוך 14 המוסדות שבהם טכנאים מתחברים מרחוק לצורך תחזוקת מכשירי הדימות, לא ביצעו ניטור של התחברות מרחוק, למשל באמצעות רישום הפעולות או הקלטת ההתחברות.

יש חשש שמוסדות אלה יתקשו לעקוב אחר פעולות התחזוקה שבוצעו בנוגע למכשירים שלהם, וכי יתקשו לאסוף מידע עובדתי ההכרחי לתחקור כל תקלה במכשיר, פגיעה בו או אירוע אבטחת מידע שהתרחש לאחר פעילות התחזוקה.

מומלץ שמוסד ט ומוסד י"א יטמיעו תהליכי בקרה על פעילות התחזוקה מרחוק שיכללו תיעוד של פעולות התחזוקה שביצעו ספקים אלה, לצורך צמצום הסיכונים הקיימים, ויטמיעו זאת בנוהל המסדיר תחזוקה מרחוק של מכשירים רפואיים.

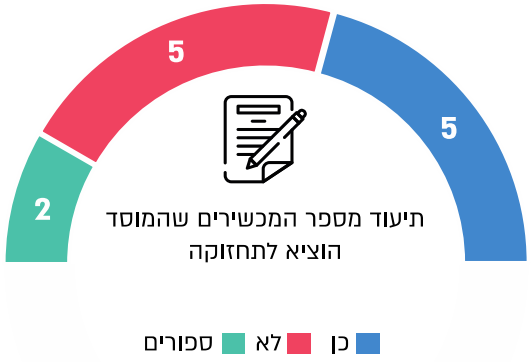
הוצאת מכשירים רפואיים לתיקון מחוץ למוסד הרפואי

לעיתים לצורך תחזוקת המכשירים הרפואיים, לדוגמה מכשיר אולטרסאונד נשים, נדרש להוציאם לתיקון מחוץ לכותלי המוסד הרפואי. 12 מ-17 המוסדות הרפואיים שענו על שאלון אבטחת המידע הוציאו מכשירים רפואיים לתיקון בשנת 2020.

על פי תקן ISO החל על בתי חולים, קופות חולים ומרפאות, חובה על ארגונים המעבדים מידע רפואי אישי לתעד את נכסי מידע הבריאות ולעקוב אחריהם.

ראו בתרשים ובלוח שלהלן את המוסדות שתיעדו כמה מכשירים רפואיים הוציאו לתחזוקה מחוץ למוסד, והפרטים על המוסדות:

תרשים 27: **המוסדות שתיעדו כמה מכשירים רפואיים הוציאו לתחזוקה מחוץ למוסד**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

לוח 20: **המוסדות שתיעדו כמה מכשירים רפואיים הוציאו לתחזוקה מחוץ למוסד**

יודעים כמה מכשירים הוציאו לתחזוקה	לא יודעים כמה מכשירים הוציאו לתחזוקה	ציינו כי הוציאו לתחזוקה מכשירים ספורים
מוסד ז	מוסד י"ג	מוסד י"ד
מוסד י"ב	מוסד ד	מוסד ט"ו
מוסד ג	מוסד ט"ז	
מוסד ט	מוסד ה	
מוסד ו	מוסד ח	

על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים ומהלוח עולה כי ל-7 מ-12 המוסדות שהוציאו מכשור רפואי לתחזוקה מחוץ למוסד הרפואי לא היה מידע מדויק בנוגע למספר המכשירים שהוצאו לתחזוקה בשנת 2020 ולזהותם: חמישה מוסדות ציינו כי "אינם יודעים" (מוסד י"ג, מוסד ד, מוסד ט"ז, מוסד ה ומוסד ח) ושניים (מוסד י"ד ומוסד ט"ו) ציינו כי הוצאו מכשירים ספורים אך לא ציינו מספרם.

על המוסדות הרפואיים לנהל רישום מלא של כל המידע הנחוץ קודם להוצאת המכשירים הרפואיים לתחזוקה מחוץ למוסד, ובכלל זה עליהם לציין במסגרת הרישום אם המידע הרפואי השמור במכשירים נמחק לפני הוצאתם לתחזוקה.

מוסד י"ג מסר בתגובתו כי יטמיע נוהל להסדרת הנושא.

מוסד ח מסר בתגובתו כי יתעד באופן שוטף את רשימת המכשירים שהוצאו מחוץ למוסד.

סיום השימוש במכשיר רפואי

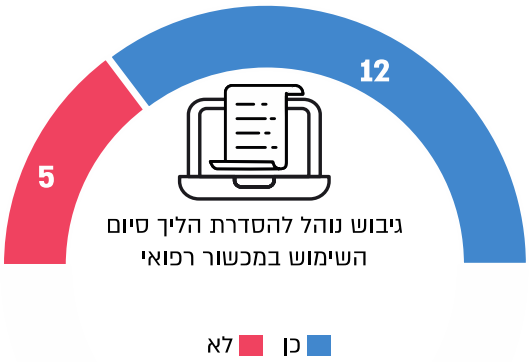
עם סיום השימוש של המוסד הרפואי במכשיר - בין שהמכשיר נזרק (נגרט), ובין שהוא נמכר לצד שלישי, על המוסד לבצע הליך לסיום השימוש במכשיר - הוא נדרש למחוק את המידע הרפואי ששמור עליו.

תקן ISO מתייחס להליך סיום השימוש במכשור רפואי, וקובע כי חלה חובה על ארגונים המעבדים מידע רפואי אישי לשכתב [למחוק] באופן בטוח רשומות קודמות, או לחלופין להשמיד כל מדיה הכוללת מידע רפואי אישי, כאשר המדיה אינה נדרשת עוד לשימוש. יצוין כי נוהלי משרד הבריאות, ובפרט נוהל מכשור רפואי משנת 2018, אינם עוסקים בנושא זה.

ממענה המוסדות הרפואיים על שאלון אבטחת המידע עלה שבמסגרת הליך סיום השימוש במכשור הרפואי כל 17 המוסדות הרפואיים ביצעו השמדה או גריטה של הכונן או הדיסק שהכיל את המידע הרפואי.

ראו בתרשים שלהלן את המוסדות שגיבשו נוהל המסדיר את הליך סיום השימוש במכשור רפואי, והפרטים על המוסדות:

תרשים 28: **המוסדות שגיבשו נוהל המסדיר את הליך סיום השימוש במכשור רפואי**



על פי מענה המוסדות הרפואיים על שאלון אבטחת המידע, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי חמישה מ-17 המוסדות לא גיבשו נוהל המסדיר את הליך סיום השימוש במכשור רפואי.

בביקורת עלה כי גם מוסד רפואי שאימץ נהלים להסדרת הליך סיום השימוש במכשור רפואי הוציא מכשור רפואי ישן מכותלי המוסד בלי שמחק את המידע הרפואי שהכיל המכשיר.

מומלץ שכלל המוסדות הרפואיים יגבשו נוהל המסדיר את הפעולות שיש לבצע בעת סיום השימוש במכשיר רפואי, לפני השמדתו, גריטתו או מכירתו, ואת בעלי התפקידים האחראים לביצוע כל פעולה. צעד כזה יצמצם את הסיכון שמידע רפואי אישי יגיע לידי מי שאינם מורשים לכך.

מומלץ גם שמשרד הבריאות יגבש קווים מנחים למוסדות הרפואיים להליך הטיפול במכשירים רפואיים עם סיום השימוש בהם, ובכלל זה למחיקת המידע ששמור עליהם ולתיעוד המחיקה, זאת בדומה לנהליו בנושא אבטחת המידע בעת רכש של מכשור רפואי.

אבטחת מידע אצל ספקים חיצוניים המבצעים בדיקות דימות

ארבע קופות החולים (הכללית, מכבי, מאוחדת ולאומית) מפנות את חבריהן לביצוע בדיקות דימות גם במכונים חיצוניים (להלן - ספקים חיצוניים) ובמרכזים הרפואיים. ברשות הספקים החיצוניים קיים מכשור רפואי המעבד ואוגר מידע רפואי אישי במהלך ביצוע בדיקות הדימות - מכשירי MRI, CT, רנטגן ואולטרסאונד.

תורת ההגנה בסייבר ממליצה להשתמש בכלים חוזיים ומשפטיים בעת רכישת שירותים מספקים, על מנת למזער את הסיכונים מהשירות שניתן.

חוזר מנכ"ל משרד הבריאות משנת 2015 קובע כי החל מינואר 2016 יש לבצע התקשרויות רק עם ספקים חיצוניים העומדים בתקני אבטחת מידע: ISO27001 (תקן בין-לאומי לניהול אבטחת מידע) או ISO27799 (תקן לאבטחת מערכות מידע בתחום הבריאות). זאת כדי לצמצם את הסיכונים הכרוכים בהתקשרות של המוסד עם גורמים חיצוניים המחזיקים מידע רפואי אישי.

המכונים החיצוניים מעבדים ומנהלים מאגרי מידע רפואי של המטופלים הנבדקים בהם, ולכן עליהם לפעול גם על פי כללי תקנות הגנת הפרטיות. הרשות להגנת הפרטיות הדגישה את הבקרה שיש לבצע על גורמי-חוץ בהנחיה משנת 2011[112] וציינה כי נושא אבטחת המידע חייב להיות תנאי יסוד בכל התקשרות לצורך ביצוע שירות מיקור חוץ; כי יש להגדיר מסמך אבטחה מחייב (למשל תקן ISO) שיעסוק בכללי אבטחת המידע שעל אותו גורם חיצוני לעמוד בהם; כי על מזמין השירות לבצע מעקב ובקרה שוטפים בעניין קיום הוראות החוק והחוזה בידי אותו גורם חיצוני.

יצוין כי לפי תשובות הקופות על שאלון אבטחת מידע, ארבעתן עיגנו בהסכמי ההתקשרות שלהן עם מכונים חיצוניים שמבצעים בדיקות דימות את חובת המכונים לעמוד בתקני אבטחת מידע: ISO27001 או ISO27799.

עם זאת עלה כי לא היה ברשות הקופות מכבי והכללית מידע בנוגע למספר הספקים החיצוניים אשר מחזיקים בפועל בתקני ISO תקפים. הכללית הוסיפה בתשובתה כי היא מבצעת בחינה מחודשת לכל ספקי הדימות החיצוניים במחוזות כדי לוודא שהם עומדים בפועל בתקן ISO; מכבי הוסיפה בתשובתה כי בדיקת העמידה בתקני ISO בקרב הספקים החיצוניים מבוצעת במסגרת תהליך ההתקשרות החוזי עם כל ספק חדש החל בשנת 2019, והם נדרשים להציג בו תעודת ISO עדכנית. עוד ציינה מכבי כי היא התקשרה עם ספקים חיצוניים רבים לפני שהחלה פעילות מחלקת אבטחת מידע והגנת סייבר (בתחילת שנת 2019), ולכן לא ביצעה בדיקה עימם.

112 הנחית רשם מאגרי מידע מס' 2011/2 - "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי" (10.6.12).

בדומה למידע הרפואי השמור במכשירים רפואיים במוסדות הרפואיים, גם מידע רפואי המעובד ונאגר במכונים שמפעילים ספקים חיצוניים עשוי להיות יעד לתקיפות סייבר. מכאן החשיבות לעמידה של ספקים חיצוניים אלה בתקני אבטחת המידע האמורים, וזאת על מנת להבטיח את קיומה של רמת אבטחה בסיסית הנדרשת לשמירה על המידע הרפואי.

מומלץ כי נוסף על הדרישה מהספקים החיצוניים לעמוד בתקני ISO לאבטחת מידע במסגרת ההתקשרות עימם, יבצעו מכבי והכללית מעקב ובקרה שוטפים בעניין מידת עמידתם של הספקים החיצוניים בתקנים אלה, וישלימו בחינה בנושא של כלל הספקים שהן עובדות עימם.

סיכום

המוסדות הרפואיים מפעילים אלפי מכשירים רפואיים המשמשים לצרכים רפואיים שונים. המוסדות פועלים ללא הפסקה ונדרשים לתת שירות בעת חירום; פעילותם נעשית בסביבה שבה הצלת חיי אדם חשובה יותר מכול וכללי אבטחת מידע הופכים לעיתים למשניים; הם נגישים לציבור ובחלקם מבקרים בכל יום אלפי אנשים העוברים ליד מכשירים רפואיים ותשתיות מחשוב; שמור בהם מידע רפואי רב וכן מידע על מחקרים רפואיים. המידע בעל ערך רב לפצחנים, לחברות מסחריות ולמדינות עוינות. כל אלה הופכים את המוסדות ואת המכשור הרפואי שלהם לפגיעים במיוחד בפני תקיפות סייבר שמטרתן לרוב גנבת מידע, שינוי מידע, סחיטה או פגיעה פיזית.

בביקורת עלו ליקויים המעידים על היעדר הסדרה של סמכויות מערך הסייבר הלאומי כלפי היחידות המגזריות במשרדי הממשלה ושל הפער בין סמכויות המאסדרים. ההמלצות המופיעות בתורת ההגנה בסייבר והמלצות מערך הסייבר הלאומי להגנה על מכשור רפואי, המוצעות לארגונים במשק הישראלי, כוללות התייחסות לצורך בהגנה על מכשור רפואי, ובפועל חלק מהמוסדות הרפואיים שנבדקו אימצו את ההמלצות וחלקם לא. מצד משרד הבריאות, הבקרה על תחום אבטחת המידע במוסדות הרפואיים חלקית בלבד, ובשנים 2019 ו-2020 המשרד לא ביצע בקרה בתחום המכשור הרפואי. עוד עלו ליקויים במערך אבטחת המידע במוסדות. וכן עלה כי משרד הבריאות אינו עוקב אחר תיקון הליקויים שהועלו בביקורות שהוא עושה, וגם אינו דורש מהמוסדות לדווח לו על כך. יחד עם זאת, יש לציין לחיוב את יוזמת משרד הבריאות להקמת ה-SOC המגזרי הנותן שירות לכלל המוסדות הרפואיים.

בביקורת עלו ליקויים בתחום אבטחת המידע של מכשור רפואי ב-25 מוסדות רפואיים שנבדקו: 11 המרכזים הרפואיים הכלליים-ממשלתיים, שני מרכזים רפואיים ציבוריים, ארבע קופות החולים ושמונת המרכזים הרפואיים של הכללית. עלו ליקויים במוסדות הרפואיים, לרבות במוסדות רפואיים גדולים. הליקויים נוגעים להיבטי הניהול של תחום אבטחת המידע, למשל הקצאת תקציב בסכום קטן מהנדרש ותוכניות עבודה שלא נידון בהן כלל נושא שיפור ההגנה על מכשור רפואי ואבטחתו; להיבט התפעולי בהגנה על המכשירים, למשל חוסר באמצעי אבטחה קריטיים שהיה על המוסדות הרפואיים להטמיע ברשת לצורך הגנה על מכשירי דימות; בחלק מהמוסדות היו מכשירים שהופעלו ללא בקרות הרשאה פיזיות ולוגיות, רוב המוסדות הרפואיים לא ביצעו מבדקי חדירה אשר כללו הדמיה של תקיפת מכשור רפואי. בתחום הלוגיסטי - רכש וסיום חיי המכשיר, עלה שבמסגרת רכש של מכשור רפואי לא נבחן נושא אבטחת המידע, וכי והליך סיום השימוש במכשור רפואי אינו מוסדר. גם בהיבט התחזוקה של מכשירי הדימות עלו ליקויים, ובין השאר לא בוצע ניטור בעת התחברות מרחוק, ולעיתים לא היה ליווי לטכנאים חיצוניים שהגיעו למוסד הרפואי לצורך תחזוקת המכשור הרפואי.

מומלץ שמערך הסייבר הלאומי יקדם את תהליך האסדרה של סמכויותיו כלפי היחידות המגזריות במשרדי הממשלה, ובכללן כלפי מגזר הבריאות, ושל הפער בין סמכויות המאסדרים. על משרד הבריאות להמשיך לפעול כמאסדר על מנת לסייע במישור הלאומי למוסדות הרפואיים להתמודד עם אתגרי אבטחת המידע במכשור הרפואי. על המוסדות הרפואיים לפעול על מנת לתקן את הליקויים שעלו בדוח זה ולהטמיע אמצעי אבטחת מידע ובקרות ראויות בכל מסלול חייו של המכשיר הרפואי - טרם רכישתו, בעת קליטתו במוסד הרפואי, במהלך השימוש השוטף בו ותחזוקתו ובעת סיום השימוש בו. מתן מענה על ליקויים אלה יצמצם את סיכוני אבטחת המידע שאליהם נחשפים המוסדות הרפואיים בעת השימוש השוטף במכשירים רפואיים. עוד עלה בביקורת כי כל המוסדות הרפואיים שאותם בדק דוח זה עמדו בתקן ISO 27799, וכולם מבצעים סקרי סיכונים בתחום אבטחת המידע.

איומי הסייבר על מערכת הבריאות הולכים ומתרבים, הם ממשיים ואינם רק בגדר איום. ניסיונות תקיפה של פצחנים מתבצעים כל העת, לעיתים הם מצליחים, כמו המתקפה שהתקיימה בתקופת הביקורת (אוקטובר 2021) על המרכז הרפואי הלל יפה והשביתה את מערכותיו. תקיפות כאלה עלולות להוביל לשיבוש בפעילות השוטפת של המוסדות הרפואיים, לזליגה של מידע רפואי של מטופלים ולגרימת נזק למכשירים רפואיים חיוניים. ואולם לא מדובר רק בניסיונות תקיפה של פצחנים אלא גם בניסיונות מצד גורמים בעלי עניין שיש להם גישה למערכות ולמכשור ומעוניינים לפגוע בהם או לשבש את פעילותם. נוסף על כך, אף פעילות שגרתית ותמימה עלולה להביא לפגיעה במערכות המידע, במאגרי המידע ובמכשור רפואי. איומים אלה מחייבים את משרד הבריאות ואת הנהלות המוסדות הרפואיים לשים את הדגש הראוי על סיכוני אבטחת המידע הכרוכים בשימוש במכשירים רפואיים ועל הדרך הראויה להתמודדות עימם.