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 2021 - 2018

2 מתקפות מסוג Distributed Denial Of Service Attack - DDOS, 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 מאוישׁ 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.

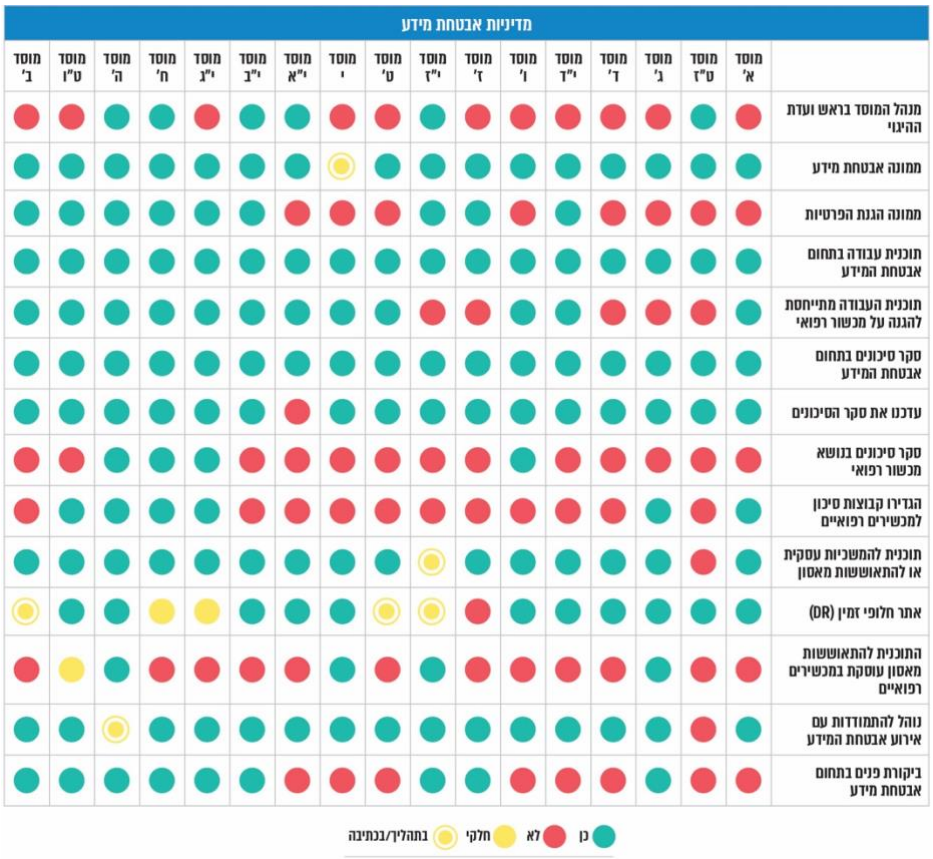
- **מדיניות אבטחת מידע במוסדות הרפואיים - ועדת היגוי ובעלי תפקידים** - ב-19 מוסדות רפואיים מ-25 המוסדות הרפואיים שענו על שאלון אבטחת המידע מנכ"ל המוסד לא עמד בראש ועדת ההיגוי לתחום הגנת המידע; שמונה מ-25 המוסדות הרפואיים לא מינו ממונה הגנה על הפרטיות.

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.

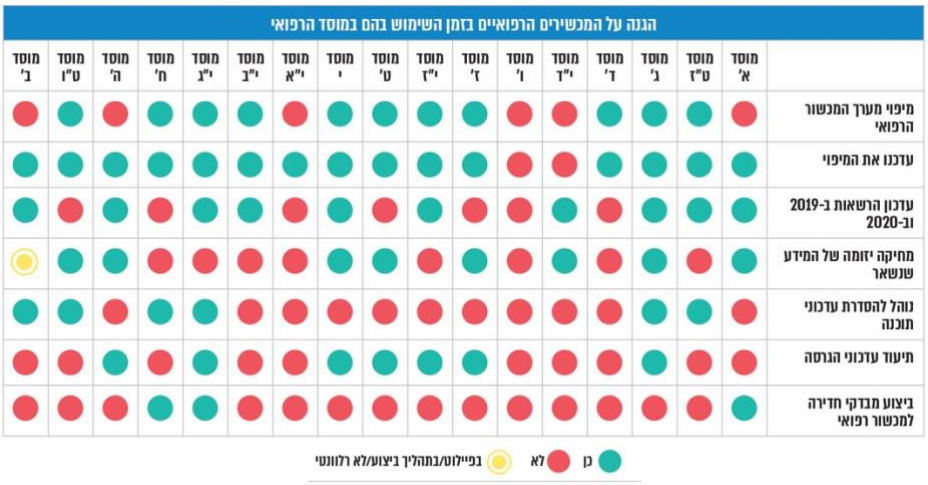
8 החלטת הממשלה בנושא לא עסקה במרכזים רפואיים ציבוריים או בקופות החולים, ולכן המוסדות הרפואיים שנבדקו בפרק זה היו 11 מרכזים רפואיים כלליים-ממשלתיים.

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.



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

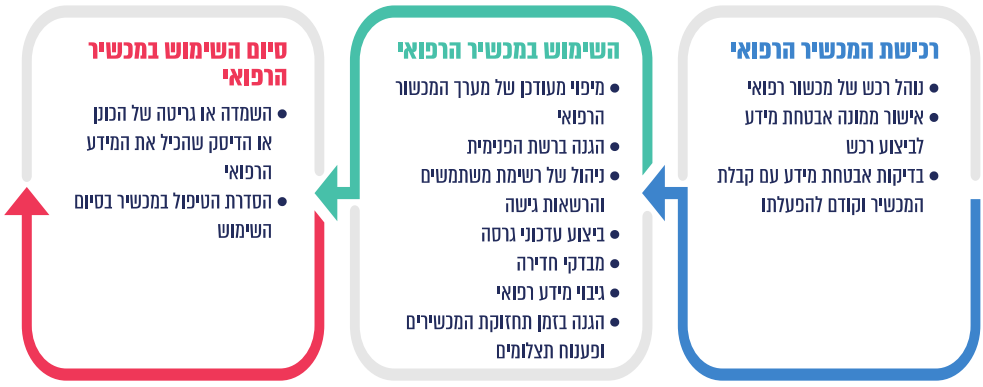
9 DR - Disaster Recovery - אתר חלופי זמין לטובת המשך פעילות מערכות המידע במקרה של אסון - נזק או השבתה של האתר המרכזי. אתר כזה יאפשר במקרה של אסון להעלות לשימוש באופן מהיר את מערכות המידע של המוסד הרפואי, לשחזר מידע על המטופלים ולהמשיך במתן השירותים הרפואיים.

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.