



תורת הגנה ארגונית אבטחת מידע

וסייבר מגזר הבריאות

גרסה 1.3

דצמבר, 2021

מספר גרסה	תאריך גרסה	הערות
1.0	2/2018	יצירת מסמך
1.1	7/2018	הגשת מסמך לאישור
1.2	1/2019	הפצה טיוטה ראשונית לקריאה
1.3	12/2021	אישור הנהלת משרד הבריאות והפצה

תוכן עניינים

9	1. מבוא
11	2. עקרונות תורת ההגנה למגזר הבריאות
13	3. מבנה תורת ההגנה
14	4. בקורות תורת ההגנה
15	פירוט פונקציות ומשפחות בקורות תורת ההגנה :
16	5. מימוש תורת ההגנה
16	שלב 1 : מיפוי יעדי הגנה – מיפוי תהליכים עסקיים וקליניים ומיפוי נכסי ההגנה
19	שלב 2 : קביעת רמת ערכיות, הסתברות הפגיעה ביעד ההגנה ורמת הסיכון הכוללת שלו
23	שלב 3 : כיצד נכון להגן
23	שלב 4 : הגדרת פערי הגנה
24	שלב 5 : תכנית עבודה
25	6. בקורות נדרשות למימוש תורת ההגנה
27	7. מוכנות ארגון למשבר סייבר
27	רקע
28	דגשים להיערכות מקדימה של הארגון לקליטת צוות IR
29	דגשים לצוות/שירות IR מיומן ומקצועי
29	המלצות כוח אדם
29	המלצות כלים/טכנולוגיות
29	המלצות מתודולוגיה
30	המלצות להיכרות מקדימה עם הארגון
30	SLA
30	ממשק צוותי IR עם הדוברים
32	8. הערכות וניהול מצב משבר
32	מבוא
32	החשיבות בהיערכות למצבי משבר בסייבר והנחות יסוד
32	הגדרות
33	מטרות התפיסה
33	מטרת התפיסה
33	מטרות משנה
33	מצבי הכוננות בסייבר ועקרונות לשינוי רמת כוננות
34	סרגל החומרה :רמזור
34	תבחינים לקביעת מצב הכוננות בסייבר :מה קורה במרחב הסייבר ובמרחב הפיזי
34	מצב שגרת הגנה בסייבר

34	מצב כוננות סייבר א'
35	מצב כוננות סייבר ב'
35	מצב כוננות סייבר ג'
35	עקרונות לשינוי רמת הכוננות בסייבר
35	העלאת רמת הכוננות בסייבר
36	הורדת רמת הכוננות בסייבר
36	צירים להכרזה על מצב הכוננות בסייבר
37	היערכות למצבי משבר : ארגז כלים
37	ידע מקצועי
37	כוח אדם
41	9. ניהול משבר סייבר
41	"מחזור החיים" של משבר סייבר
41	תפיסת הניהול של משבר סייבר : צוות ניהול המשבר
43	פעולות בניהול משבר סייבר
43	מצב שגרת הגנה בסייבר
43	מצב כוננות סייבר א'
44	מצב כוננות סייבר ב'
44	מצב כוננות סייבר ג'
45	התאוששות : חזרה למצב שגרת הגנה בסייבר
47	10. מודעות עובדים
47	רקע
47	עקרונות יסוד
47	אוכלוסיות היעד
47	הנהלה ומנהלים בכירים
48	סגל רפואי
48	אנשי טכנולוגיות
48	ספקים וקבלנים
48	כלל העובדים
48	תכנית הדרכה והעלאת המודעות
48	מרכיבי התכנית
48	הדרכה פרונטלית
49	מדידה, הערכה ודיווח
49	אחריות
51	11. תרגולי סייבר - מדריך לתרגול עצמי
51	רקע

51	תרחישי איום רלוונטיים למגזר הבריאות
51	מטרות תרגולי סייבר
51	רקע למדריך וזכויות יוצרים
51	משתתפים בתרגילים
51	ציפיות כלליות
52	מבנה התרגיל:
52	חוקי השתתפות
52	הנחיות עבור המשתתפים:
53	הנחיות עבור המנחה:
54	מהם 10 תחומי ההערכה?
55	תהליך התרגול
56	מורכבות התרגילים
56	תרחישים
56	תרגיל 1 *
56	תרגיל 2 *
57	תרגיל 3 *
58	תרגיל 4 *
58	תרגיל 5 *
59	תרגיל 6 *
59	תרגיל 7 **
60	תרגיל 8 **
61	תרגיל 9 **
61	תרגיל 10 ***
63	תרגיל 11 ***
63	תרגיל 12 ***
64	תרגיל 13 ***
64	תרגיל 14 ***
65	חזרה על תרחיש לדוגמה
65	תרגיל לדוגמה ***
67	תרגיל חזרה
67	מדגם של סוגיות ושאלות שזוהו במהלך התרגיל
69	12 אבטחת מידע והגנת סייבר במכשור רפואי
69	1. רקע/מבוא:
69	2. הגדרות:
69	2.1 אבטחת מידע - הגדרת ISO (ISO 27000:2014):

70	2.2 אבטחת מידע - הגנת סייבר (ה"ס) – לפי הגדרת ה-FDA :
70	2.3 אמ"ר (אבזורים ומכשירים רפואיים) :
70	2.4 הזדהות :
70	2.5 הזדהות חזקה :
70	2.6 הערכת סיכונים (לחלופין : אתור וחישוב הסיכון השורשי בהיבטי אבטחת מידע, דהיינו, זמינות-שלמות ואמינות-סודיות-C-I-A) :
70	2.7 הצפנה :
70	2.8 זיהוי חד ערכי :
70	2.9 זיהוי דו ערכי :
70	2.10 חתימה דיגיטלית (Digital Signature) :
70	2.11 לוג – Log :
70	2.12 מכשור רפואי –
71	2.13 נזק/פגיעה/חבלה - HARM (ISO/IEC 80001-1:2010) :
71	2.14 נתיב בקרה :
71	2.15 סיכון שיורי (ISO/IEC 80001-1:2010) :
71	2.16 סקר סיכונים :
71	2.17 תווד תקשורת ציבורי :
72	3. מסמכים ישימים :
72	3.1 חוקים והנחיות
72	3.2 תקנים בנושא אבטחת מידע
72	3.3 מסמכים והנחיות רלבנטיות מה-FDA
73	4. אחריות ליישום :
73	4.1 ליצרני מכשור רפואי :
73	4.2 למוסדות רפואיים המפעילים מכשור רפואי :
74	4.3 למשתמשים פרטיים של מכשור רפואי :
74	5. הסיכונים והאיומים למכשור רפואי הנובעים מכשל באבטחת המידע :
74	5.1 ניהול סיכונים
74	5.2 פגיעה בחיי אדם :
74	5.3 פגיעה בזמינות השירות המסופק באמצעות המכשור הרפואי :
74	5.4 פגיעה בסודיות הנתונים באחד ממרכיבי המכשור הרפואי או בעת העברת מידע מסווג בממשקי תקשורת (פנימיים או חיצוניים) :
75	5.5 פגיעה בשלמות ואמינות הנתונים באחד ממרכיבי המכשור הרפואי או בעת העברת מידע מסווג בממשקי תקשורת (פנימיים או חיצוניים) :
75	5.6 חדירה למערכות :
75	5.7 סיכוני אבטחת מידע טכנולוגיים :
76	6. ארכיטקטורה כללית של מערך המידע של המכשור רפואי וחיבורו לרשת התקשורת :

- 6.1. ניתן לחלק באופן כללי את עולם המכשור עפ"י החלוקה הבאה המתייחסת להיבטי איום וסיכון ומתן מענה להם : 76.....
- 6.2. ברמה העקרונית שימוש במכשור רפואי כולל את המרכיבים הבאים : 76.....
- 6.3. במקביל יידרשו מענים לדרכי הגישה הבאות : 76.....
7. הגדרות אבטחת מידע – רשימת תיוג עבור יצרן האמ"ר : 76.....
8. הנחיות למוסדות רפואיים בתהליך הטמעת אבטחת מכשור רפואי 83.....
- 8.1 תהליך קליטת מכשור 83.....
- 8.2 תהליך ניהול סיכונים : 83.....
- 8.3 בקורות אבטחת מידע 84.....
- 8.3.1 ניהול תקשורת ותפעול 84.....
- 8.3.1.1 נוהלי תפעול ואחריות תפעול 84.....
- 8.3.1.2 הגנה מפני ניסיונות פגיעה 85.....
- 8.3.1.3 זמינות נתונים ושירותים 85.....
- 8.3.1.4 תיחום השימוש בתשתיות מכשור רפואי 85.....
- 8.3.1.5 ניהול סביבת הרשת של המכשור הרפואי 85.....
- 8.3.1.6 ניהול סביבת המחשוב של המכשור הרפואי 86.....
- 8.3.1.7 תהליך העברת מידע רגיש בין סביבת המכשור הרפואי לרשת הארגון 86.....
- 8.3.2 בקרת גישה לוגית 86.....
- 8.3.2.1 אכיפת בקורות גישה 86.....
- 8.3.2.2 אמצעי זיהוי 87.....
- 8.3.2.3 ניהול הרשאות 87.....
- 8.3.2.4 בקרת גישה בין רשת הארגון לסביבת המכשור הרפואי 87.....
- 8.3.2.5 בקרת גישה מרשת האינטרנט/ רשת חיצונית לסביבת המכשור הרפואי 88.....
- 8.3.2.6 בקרת גישה ממכשור רפואי לרשת הארגון דרך רשת האינטרנט / רשת חיצונית 88.....
- 8.3.2.7 ניהול סיסמאות במכשור רפואי וברשת הארגון 89.....
- 8.3.3 בקורות ומנגנוני קריפטוגרפיה (Cryptography) 89.....
- 8.3.3.1 מדיניות שימוש בבקורות קריפטוגרפיה (Cryptography) 89.....
- 8.3.3.2 הצפנה (Encryption) 89.....
- 8.3.3.3 חתימה דיגיטלית (Digital Signature) 89.....
- 8.3.3.4 מנגנוני מניעת הכחשה (Non-Repudiation) 90.....
- 8.3.3.5 נתיב בקרה (Audit Trail) 90.....
- 8.3.3.6 קישור מכשור רפואי, עובדים ומערכות מידע המקושרות למכשור רפואי לאינטרנט 90.....
- 8.3.3.7 מידע במכשיר רפואי 91.....
9. נספח א' - מסמכים נוספים בנושא אבטחת מידע : 91.....
- 9.1 חוקים/דירקטיבות 91.....
- 9.2 תקנים 91.....

AUTO11 (Draft	9.1.1.1.
92 2)—Information Technology Security of In Vitro Diagnostic Instrument and Software Systems	
92..... נספח ב' - מהו מכשור רפואי, סוגי מכשור רפואי :	10.
92..... FDA 10.1	
92..... 10.1.1 כללי :	
92..... 10.1.2 הגדרת ה-FDA Medical Device – למכשור רפואי :	
10.1.3 מכשור רפואי הנו כלי (instrument), מכשיר (apparatus), מכונה (machine), מתקן (contrivance), אביזר (contrivance), שתל (implant), חומר המשמש לריאקציה כימית מחוץ לגוף (in vitro reagent), או משהו דומה (or other similar or related article), כולל רכיב או תוסף (including a component part, or accessory) אשר :	92.....
92..... 10.1.4 דוגמאות למכשור רפואי :	
93..... 10.1.5 ההגדרה מבטיחה :	
93..... 10.1.6 סוגי המכשור הרפואי עפ"י ה-FDA :	
93..... רמה 1 (Class I) – בקרות רגילות (general controls)	8.2.1.1.1
http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051530.htm	
93.....	
94..... 10.1.7 הגדרת ה-FDA עבור מערכת מידע מכשור רפואי – FDA Medical Device Data System (MDDS) :	
95..... 10.1.8 הגדרת ה-FDA ליישום רפואי נייד – FDA Mobile Medical Application (APPS) :	
96..... 10.2 מתוך חוק ציוד רפואי התשע"ב - 2012 – מדינת ישראל :	
10.2.1 "ציוד רפואי" – כל אחד מהמפורטים להלן, ולמעט תכשיר כהגדרתו בפקודת הרוקחים [נוסח חדש], התשמ"א – 1981 :	96.....
97..... נספח ג' – טופס דוגמה לבחינת ממונה הסייבר בארגון לרכש ציוד רפואי :	11.
98..... נספח ד' – טופס דוגמה לאישור ממונה סייבר בארגון לרכש ציוד רפואי :	12.
100..... נספח א : טבלת פירוט משמעויות למצבי כוונות	
104..... נספח ב' : הערכת מצב סייבר	
104..... תמונת מצב סייבר (דוגמה)	
104..... סוגיות לדיון בהערכת מצב (לדוגמה)	
105..... לסיכום	
106..... נספח ג' : שאלון מידת היערכות למצבי משבר בסייבר (TOP10)	
113..... 13 מדיניות ניהול סיכונים בסייבר בשרשרת אספקה	
113..... פרק א' : כללי	
113..... מטרות ויעדים	
113..... הגדרות	
114..... סמכויות ואחריות	
114..... באחריות הייעוץ המשפטי :	
114..... באחריות המערך הרפואי :	
115..... באחריות הרכש :	

116.....	באחריות גופים אלה, כל אחד בתחומו :
116.....	באחריות יחידת הסייבר המרכזית של משרד הבריאות :
117.....	מיפוי וסיווג ספקים
117.....	דרישות מגורמים בשרשרת אספקה
121.....	התקשרות עם ספקים בשרשרת אספקה
121.....	סקרי סיכונים בשרשרת אספקה
123.....	תרשים זרימה הזמנת רכש
124.....	חוקים, תקנות והנחיות רלוונטיות

1. מבוא

העידן הדיגיטלי הביא עמו הזדמנויות חברתיות וכלכליות אדירות, לפרטים, לעסקים ולמדינות אשר מכירים בהזדמנות ומעויזים לפרוץ דרך בעולם המשתנה במהירות. הבריאות הדיגיטלית, וביתר שאת בישראל, שינתה את האופן שבו ניתן טיפול רפואי ומביאה לחידושים רבים בעולם הרפואה: החל משימוש במערכות מידע לצורך שיפור האפקטיביות הקלינית והניהולית בארגוני הבריאות, דרך המכשור הרפואי עצמו שהוא, בעצמו כולל גם מרכיבי תקשוב ועד ההתפתחויות האחרונות במגזר, כגון ניטור רפואי אחר מצבם של מטופלים, יישומי רפואה מרחוק ושיתוף מידע רפואי לצרכי מחקר ופיתוח.

התוצאה של מהפכה זו היא, שכיום התהליכים הקליניים והאדמיניסטרטיביים במגזר הבריאות הישראלי תלויים באופן הדוק במערכות מבוססות מחשב. ברור אפוא שרתימת הטכנולוגיה לעולם הרפואה מאפשרת ליצור פלטפורמה לחדשנות ולקידום המענה אותו עולם הרפואה יכול להציע לשיפור הבריאות, תוחלת החיים ואיכות החיים. יחד עם זאת, לצד יתרונות אדירים אלה, השימוש במרחב הטכנולוגי והתלות הגוברת בפעילותו התקינה מביאים לכך שפגיעה במרחב הטכנולוגי משמעותה פגיעה בפעילותם התקינה של ארגוני הבריאות עצמם. על כן, על מנת לשמור על איכות הטיפול הרפואי, יש להתגונן כראוי מפני איומי הסייבר השונים.

איומי הסייבר הייחודיים למגזר הבריאות כוללים, בין היתר, פגיעה בתשתיות והשפעה על הרציפות התפקודית, פגיעה בחיי המטופלים באמצעות השבתת שירות ו/או ציוד רפואי שינוי במידע רפואי והשפעה על המטופל וגניבת מידע רפואי לצורכי מסחר.

על רקע חדירה הולכת וגוברת של האמצעים הטכנולוגים לפעילות הסדירה של המגזר, עולה צורך ברור לייצר מענה אל מול האיום המתפתח.

נקודת המוצא הינה שהאחריות להגן על ארגון בריאות מפני מתקפות סייבר הינה בראש ובראשונה על הארגון עצמו. במהלך השנים האחרונות ארגוני הבריאות החלו לטפל בסוגיות אבטחת מידע ואף הוסמכו לתקן ISO 27799, אולם באותו זמן המשיכה להתפתח מפת האיומים וחומרתם – במורכבות ובתדירות.

ע"מ לבצע "יישור קו" בתחומי הגנת הסייבר ולנסות לשנות את המגמה הנזכרת לעיל, בוצע ניתוח לרכיבי האיום ברבדים השונים ומולם המענה הטכנולוגי והכלים הזמינים כיום להתמודדות ראויה. בחוברת זו מוצגת בהתאם תפיסה סדורה לניהול סיכוני סייבר במגזר הבריאות בישראל.

תורת הגנה ארגונית אבטחת מידע

וסייבר

2. עקרונות תורת ההגנה למגזר הבריאות

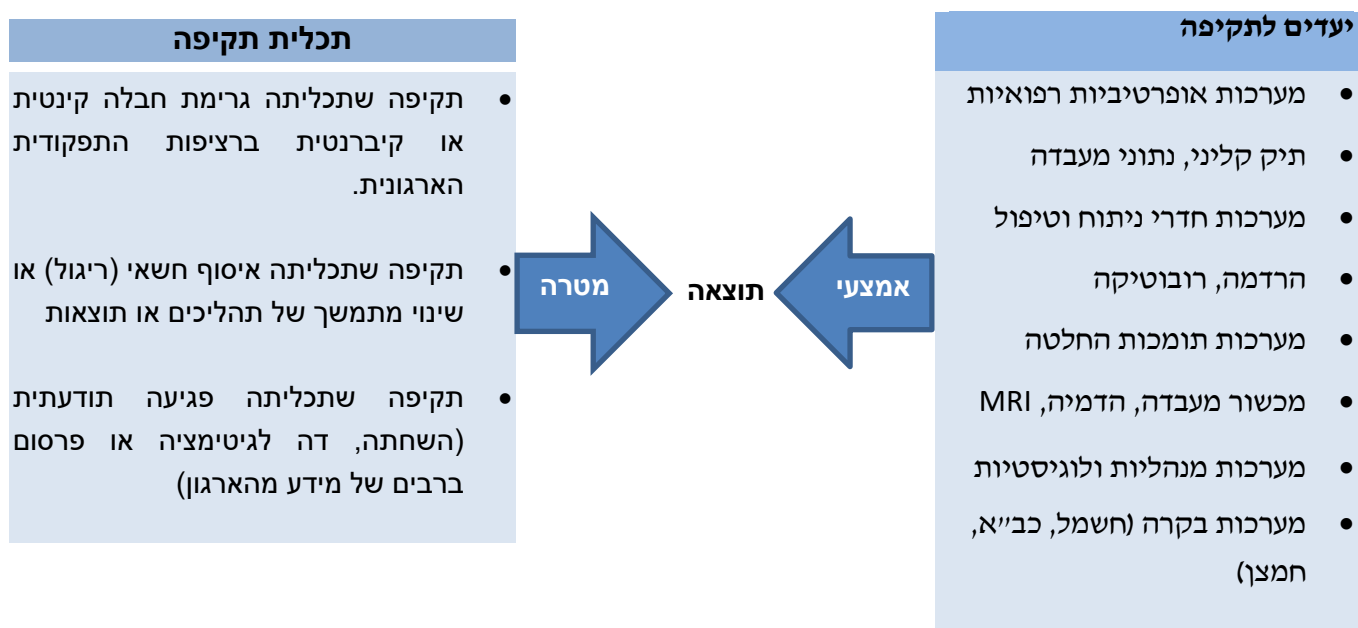
תורת ההגנה למגזר הבריאות מספקת לארגוני הבריאות, בתי חולים, לקופות החולים ולשרשרת האספקה של מוסדות אלה הנחיות כיצד לייצר מסגרת הגנה על כלל רכיבי הרציפות התפקודית של הארגון (דהיינו, היכולת לתפקד בספק שירותי רפואה חיוניים גם בהינתן מצב משברי כזה או אחר), ובכלל זה הגנת כלל מרחב הסייבר שלו – החל ממערכות בקרת המבנה, דרך מערכות המידע תומכות הרפואה של הארגון ועד המכשור הרפואי עצמו. בנוסף, מטרתה של התורה גם לסייע למוסדות אלה להגן על סודיות, אמינות וזמינות של המידע שנמצא ברשותם, ובכלל זה על מידע חסוי וחסוי ביותר. התורה מתבססת על מסמך תורת ההגנה בסייבר לארגון של הרשות הלאומית להגנת הסייבר, מרחיבה אותה כך שהיא תטפל בצרכים המיוחדים לניהול הגנת הסייבר של ארגונים במגזר הבריאות וסביבות התפעול הייחודית שלו.

כתורה מותאמת מגזר, בקורות תורת ההגנה הבריאותית מסונכרנות לתקן הגנת הסייבר לארגוני בריאות ISO 27799, להנחיות משרד הבריאות הרלוונטיות וכן לתקנות הגנת הפרטיות שנכנסו לתוקף במאי 2018.

מתאר האיומים על מגזר הבריאות השתנה במידה רבה עם השנים, ואף כי אף אחד מהם אינו ייחודי למגזר זה, מה שמייחד את תחום הבריאות הוא מערך הגורמים שיש לקחת בחשבון בעת הערכת איומים ופגיעויות. מטבעם, ארגוני הבריאות פועלים בסביבה שבה המבקרים והציבור הרחב לא יכולים להיות מופרדים לחלוטין ממערכות הארגון. במיוחד בארגוני בריאות גדולים דוגמת בתי חולים, כמות האנשים העוברים באזורים תפעוליים היא משמעותית. גורמים אלה מגבירים את הפגיעות של מערכות לאיומים פיזיים. בנוסף, ארגוני בריאות רבים נמצאים בפעילות 24 שעות ביממה, שבעה ימים בשבוע תחת לחץ משמעותי ועם מערכות שחלקן ותיקות ולפיכך מוגנות פחות מאיומי סייבר. גורמים אלו יכולים להגביר את הפוטנציאל לסוגים מסוימים של איומים ולהגביר את הפגיעות. מאידך גיסא, הטיפול הקליני כולל מגוון של צוות מקצועי, טכני, מינהלי, נלווה והתנדבותי, שהוא מוכשר ומיומן ושרבים רואים את עבודתם כיעוד לשירות הציבור. הנסיון מלמד כי נסיונם ומסירותם יכול לעתים קרובות להפחית באופן משמעותי את החשיפה לפגיעויות ולשמש כבקרה מפצה במקרה שאיום מתממש.

נכון לשנת 2018, איום הייחוס של מגזר הבריאות כולל מספר סיכונים:

- פגיעה ברציפות התפקודית
- פגיעה בחיי אדם
- פגיעה בשירות חיוני לציבור (רציפות תפקודית)
- נזק כלכלי
- פגיעה תודעתית
- זליגת מידע רגיש (שמובילה לפגיעה באינטרסים)



בהתאם, המטרה היא שעל בסיס תורת ההגנה של המשרד, הארגון יקיים מערך הגנת סייבר הנותן דגש לסיכונים הייחודיים של הארגון המונחה על רקע מאפייניו של מגזר הבריאות כמגזר פתוח אל הציבור, קיומן של מערכות ותוכנות לגאסי (legacy systems) יקרות; החשיבות בשימור דרגה גבוהה של זמינות של ציוד רפואי; כניסה ספורדית של ציוד מתקדם לארגוני הבריאות; השימוש ההולך וגובר בטכנולוגיות אלחוטיות ומבוססות אינטרנט באספקת שירותי הבריאות; החשיבות של הארגון לאספקת שירות חיוני לציבור ולשמירה על חיי אדם ובריאותו הנפשית.

בנוסף, הטמעת תורה זו מבוססת על שיתוף כלל הגורמים הרלוונטיים בארגון, ובכלל זה הצוותים הרפואיים, בגיבוש וביישום הגנת הסייבר, וכן בהטמעת תהליכי הגנת הסייבר בכלל המערכות הרלוונטיות של הארגון, ובכלל זה: מערכות המידע, המכשור הרפואי, מערכות הלוגיסטיקה התומכות, תהליכי העבודה של הארגון, מערכת כח האדם וכו'.

על רקע זה, הצפייה ממוסד הבריאות הינה שיצור מערך הגנה משולב כח אדם, תהליכים וטכנולוגיות במספר שכבות הגנה לטובת הקטנת משטח החשיפה לאיומי הסייבר, תוך שילוב יכולות מתקדמות, כגון הונאות ומלכודות, להתמודדות עם איומים קונקרטיים, ובחינה של טכנולוגיות חדשניות לטובת מימוש האמור, כדוגמת בלוקצ'יין.

על המוסד לתת דגש גם למקומו של איש הצוותי הרפואי כבקר מפקח ובמידת הצורך גם מעבר לפעילות "ידינית" מלאה, לטובת המשך אספקת שירות חיוני לציבור גם בהתקיים אירוע סייבר, וכן להטמעה של אמצעי הגנת הסייבר לטובת קידום הפעילות הקלינית של הארגון (למשל, על ידי הטמעת הזדהות חזקה מרחוק כדי ליעל את פעילות הארגון).

בעזרת כלל האמור לעיל, תורת ההגנה תאפשר לכל מוסד בריאות בישראל להעלות את רמת ההגנה שלו מפני כלל סוגי מתקפות הסייבר, למען שמירה על בריאות הציבור וצנעת המידע הרפואי אודותיו.

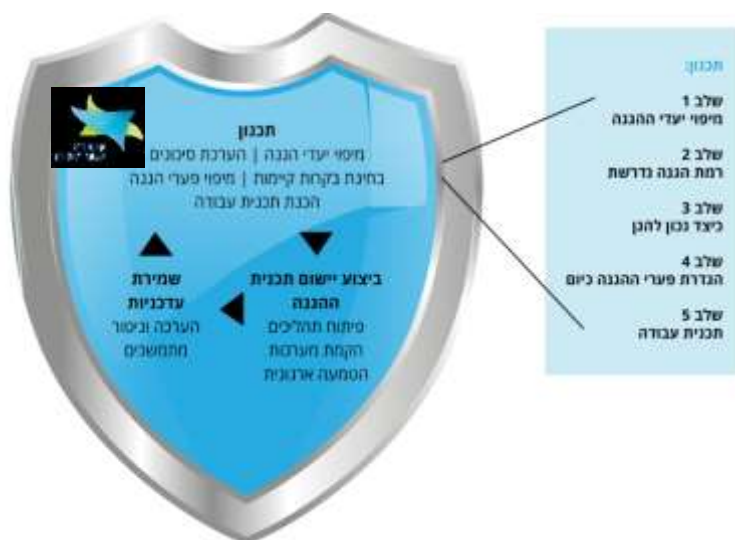
3. מבנה תורת ההגנה

תורת ההגנה למגזר הבריאות נבנתה על בסיס תורת ההגנה הארגונית שפורסמה ביוני 2017 ע"י הרשות הלאומית להגנת הסייבר. תורת ההגנה מסייעת לארגונים למפות את סיכוני הסייבר שהם חשופים אליהם ולהגדיר אמצעי הגנה מידתיים להפחתת הסיכונים העיקריים. תורת ההגנה פותחה זו על-ידי שילוב תורות מובילות בעולם, ניסיון ישראלי בתחום האזרחי והביטחוני, התאמה לסביבה הישראלית והתאמה לתרבות העסקית הישראלית.

תורה זו נבנתה באופן שלוקח בחשבון את העובדה, כי על הארגון לבצע תהליך הערכת סיכונים באופן תקופתי. הערכת סיכונים זו היא הבסיס לבניית תכנית עבודה רב שנתית למזעור הפערים (מימוש בקורות נדרשות). תהליך ההגנה על-פי תורת ההגנה הוא תהליך מחזורי, הכולל שלושה שלבים עיקריים:

- א. **תכנון והערכה** - עיקריו מיפוי יעדי הגנה בסייבר בארגון, הערכת סיכונים, בחינת אמצעי ההגנה (הבקורות) הקיימים ובניית תכנית עבודה לסגירת פערי הגנה.
- ב. **ביצוע** תכנית העבודה על-ידי בניית תהליכים ארגוניים, הטמעת כלים והטמעה ארגונית.
- ג. **שמירה על עדכניות** ההגנה לאור דינאמיות מרחב הסייבר בארגון ומאפייני האיומים השונים.

תהליך התכנון מורכב מהשלבים האינטואיטיביים הבאים:



4. בקורות תורת ההגנה

בקורות תורת ההגנה למגזר הבריאות נבנו על מסגרת הבקורות של תורת ההגנה הארגונית של רשות הסייבר. תורה זו אימצה את מסגרת ניהול הגנת הסייבר של מכון התקנים האמריקאי (NIST Cyber Security Framework), ובהלימה לבקורות הגנת הסייבר של תקני NIST SP 800-53 לצד ISO 27001. התוצאה היא בקורות "ישראליות" שמצד אחד מבוססות על הידע הבינלאומי, אך מצד שני בוצעו בהן התאמות רבות למאפייני המשק הישראלי, תוך הוספת דגשים לדוגמאות לטובת סיוע לארגונים.

בנוסף, כתורה מותאמת מגזר, בקורות תורת ההגנה למגזר הבריאות מסונכרנות לתקן הגנת הסייבר לארגוני בריאות ISO 27799, להנחיות משרד הבריאות הרלוונטיות וכן לתקנות הגנת הפרטיות שנכנסו לתוקף במאי 2018. הבקורות המוצגות בתורה זו זה הן אלה שזוהו כמתאימות בתחום הבריאות, והמתאימות ביותר לאור איום הייחוס על המגזר – לשמור על הרציפות התפקודית של המגזר, למנוע פגיעה בחיי אדם ולהגן המידע הבריאותי ולהבטיח שניתן יהיה לבדוק ולטפל בגישה למידע זה. בקורות אלו מסייעות להבטיח את המשכיות השירותים הרפואיים ולמנוע טעויות בתרגול הרפואי העלולות להיגרם כתוצאה מאי-שמירה על שלמות המידע הבריאותי, בכל מקרה יובהר כי בקורות תורת ההגנה מחייבות את כל ארגוני מגזר הבריאות, גם אין להם מקבילה בהנחיות מב"ר. במקרה של סתירה בין הוראות תורת ההגנה להנחיות קודמות, יגברו הוראות תורת ההגנה.

בקורות התורה נבנו על פי מסגרת NIST. בגישה זו מתבצעת הגנה על הארגון מפני תקיפה בשלב ההיערכות וההגנה המסורתיים, וזו לצד חיזוק יכולתו של הארגון לגלות אירוע סייבר, ובמידת הנדרש להכילה ולהתאושש ממנה במינימום נזק לארגון. **כל זאת, מתוך התפיסה כי הגנת הסייבר עוברת בשנים האחרונות מעולמות המניעה לעולמות ההתמודדות.**

הבקורות עצמן מצוינות בקובץ אקסל ובו רבדי מידע רלוונטיים. ביניהם (ראו המחשה בטבלה מטה):

מפני איזה סוג נזק מגינה הבקרה – סודיות, אמינות או זמינות.

השלב בשרשרת התקיפה שבה הבקרה ממלאת תפקיד (Cyber Kill Chain).

רמות הסיכון שבהן נדרש ליישם את הבקרה (בסולם של 1 עד 4).

סוג הבקרה – מנחה (כגון נוהל), מונעת (כגון מערכת סינון קוד עיון) או מגלה (מערכת ניטור)

תאימות לתקנים נפוצים

חלוקה לפי "פונקציות" ו"משפחות" הבקורות של NIST (ראו טבלה בעמוד הבא).

תוספת / חידוד דרישות של משרד הבריאות

1	1	1	2	5	3	5	4	7					6	6		
זמינות	אמינות	סודיות	Cyber Kill Chain	מיפוי לבקורות ISO מותאימות	רמת בקרה	מקור NIST	סוג הבקרה / מונעת / מגלה / מנחה / מותקנת / מאושרת	תוספת דרישות מגזר הבריאות	דוגמא ליישום הבקרה	הסבר משלים	הבקרה	כותרת	משפחה	פונקציה	מזהה פונקציה	

פירוט פונקציות ומשפחות בקורות תורת ההגנה:

פונקציה	מטרה	משפחות בקורות משויכות
זיהוי (IDENTIFY)	פיתוח ההבנה של הארגון על מנת לנהל סיכונים סייבר למערכות, נכסים, מידע ויכולות של הארגון	אחריות דירקטוריון ניהול סיכונים והערכת סיכונים בקרה, ביקורת ותאימות בקרת גישה הגנה על מידע הגנה על שרתים ותחנות עבודה מניעת קוד זדוני הצפנה אבטחת רשת הפרדת סביבות אבטחה בענן
הגנה (PROTECT)	פיתוח ויישום אמצעי ההגנה ההולמים על מנת להבטיח קיום השירותיים שהוגדרו כקריטיים עבור הארגון.	הגנה על בקרים תעשייתיים ומכשור רפואי אבטחת טלפונים סלולריים ניהול שינויים אבטחת מדיה אבטחת שרשרת אספקה ומיקור חוץ אבטחה ברכש ופיתוח הגנה פיזית וסביבתית משאבי אנוש ומודעות עובדים הדרכות תיעוד וניטור
איתור (DETECT)	פיתוח ויישום הפעילויות המתאימות על מנת לזהות ולאתר התרחשות של אירוע סייבר	סקרי הערכה של בקורות אבטחה הגנת סייבר פרואקטיבית
תגובה (RESPOND)	פיתוח ויישום הפעילויות המתאימות לתגובה לאירוע סייבר	ניהול אירועים ודיווחים
התאוששות (RECOVER)	פיתוח ויישום הפעילות המתאימות הנדרשות לשמר את חוסן הארגון ולשחזר את יכולות ושירותי הארגון שנפגעו עקב אירוע הסייבר	המשכיות עסקית

5. מימוש תורת ההגנה

שלב 1: מיפוי יעדי הגנה – מיפוי תהליכים עסקיים וקליניים ומיפוי נכסי ההגנה

לא ניתן להגן על נכסי הארגון ללא הבנה ומיפוי תחילה של הנכסים שלו ורגישותם להתממשות אירוע סייבר. לכן, כבסיס לתכנית הגנת הסייבר של כל ארגון במגזר הבריאות, יש לזהות את יעדי ההגנה ואת הטכנולוגיות שהארגון עושה בהן שימוש ומה רמת רגישותן לאיומי סייבר.

כיצד יודעים מהו "נכס הגנה"? כדי לענות על השאלה הזאת, על כל ארגון במגזר למפות את נכסיו (מערכות מחשב כאלה ואחרות), את קשרם לתהליכי הארגון ואת הממשקים מ/אל הנכס. שלב מיפוי הנכסים יקשור גם בין נכסים (פיזיים ואחרים) לתהליכים העסקיים המרכזיים בארגון. בסוף שלב זה יידע הארגון להגדיר מה הם הנכסים בעלי רמת ערכיות גבוהה לתפקוד הארגון ומה הם הנכסים המשניים. הגדרה זו תסייע להגן על הנכסים בהתאם לפוטנציאל הנזק, ותבוסס על כלים ייעודיים שהוכנו על ידי משרד הבריאות לטובת ארגוני המגזר.

כלים אלה, יחדיו עם עוזרים נוספים לחוברת זו, יסייעו לבצע את תהליך המיפוי באופן יעיל תוך שימוש במתודולוגיה אחידה, שפה ומדדים זהים וכן יספקו למשרד יכולת לגבש תמונת מצב רוחבית של רמת מוכנות המגזר להתמודדות עם אירועי סייבר.

כאמור, הדרך המיטבית למיפוי יעדי ההגנה הוא באמצעות מיפוי תחילה של התהליכים הליכטיים של הארגון. תהליכים אלה כוללים גם את התהליכים בהקשר לתחומים הבאים:

תהליכים בהקשר לתחומים עיקריים								ייעוד המערכת
אדמיניסטרציה כללית	הנה"ח וכספים	תקציב	ניהול מלאי	משאבי אנוש	IT	ביטחון	מח' משפטית	הנדסה
אדמיניסטרציה רפואית	רישום חולים	התחשבות רפואית	זימון חולים	רשומות רפואיות	ארכיב			
ניהול המידע הרפואי	הדמיה	מעבדות	חדרי ניתוח	תיק רפואי				
מערכות לצפייה ותחקור	BI	סטטיסטיקה	תחקור נתונים	Data Warehouse				
חציוד רפואי ורכיבי ה-SCADA	טיפול מניפולטיבי	שליטה ובקרה	תשתית	הדמיה	ביקורת וכיול			

כפי שניתן לראות בטבלה, אחד התהליכים המרכזיים בבית חולים הוא "ניהול המידע הרפואי", ולו מספר תתי תהליכים – ניהול מידע אודות הדמיה, ניהול מידע אודות התיק הרפואי וכו'. דוגמא אחרת לתהליך, שאיננו כולל מידע בהכרח, הוא התהליכים ההנדסיים-פיזיים בבית החולים, כשתתי התהליכים בו יכולים להיות לדוגמא שליטה ובקרה (למשל, על המעליות). עם השלמת תהליך מיפוי התהליכים, יהיה בידי כל ארגון טבלה מסודרת של כלל תהליכים הארגונים, על בסיס אקסל המיפוי הרלוונטי שנשלח ע"י משרד הבריאות:

מיפוי תהליכים מרכזיים ורמת רגישות						הערות
שם התהליך	תהליכי משנה	מנהל התהליך	מערכות מעורבות	תלות של המערכת בתהליך	רמת קריטיות התהליך	לרצף הטיפול

בהמשך ובהתאם למיפוי התהליכים, הארגון נדרש ליצור מיפוי מערכות התומכות בקיום התהליכים האמורים. יצוין כי מילוי המערכות ה"מעורבות" במסגרת מיפוי התהליכים (ראו טבלה מעלה) יכול לסייע לארגון, אך בכל מקרה נדרש לבצע מיפוי מערכות מלא בהתאם למפורט להלן.

בהכללה, מגזר הבריאות עושה שימוש במערכות ממוחשבות משלוש משפחות עיקריות:

א. **מערכות מידע (מערכות תומכות רפואה)** - מערכות המיושמות בארגוני בריאות אשר מעבדות, מאחסנות ומתקשרות מידע הקשור לתהליכים הרפואיים. המידע מופץ בצורה מאובטחת, בהתאם לצורך, בין הלקוחות, הספקים והגורמים השונים.

ב. **מכשור רפואי** - מכשור ייעודי המשמש לטיפול רפואי במטופלים, לשם אבחון, טיפול או ניתוח. המכשור הרפואי מהווה כיום חלק בלתי נפרד מהטיפול הרפואי, זמינותו ואמינותו הינם הכרחיים למתן שירותי הרפואה.

ג. **מערכות תשתית ובקרה (ICS/SCADA)** – מערכות המשמשות לשליטה, ניטור, בקרה ואיסוף מידע לצורך ניהול תשתיות ומתקנים כגון: חשמל, מים, דלק, גז, ביוב ועוד. מערכות אלו הכרחיות לשמירה על הרצף התפקודי של ארגון הבריאות

בהתאם, במסגרת פרויקט המיפוי של משרד הבריאות, נוצרו קבצי אקסל עבור כל אחת ממשפחות המערכות (מידע, מכשור רפואי ותשתית ובקרה). לטובת מיפוי המערכות במסגרת הטמעת תורת ההגנה, יש לעשות שימוש בקבצים אלה, בהתאם לסוג המערכת/הנכס. פירוט יופיע להלן.

בכל מקרה, יש לזכור כי מיפוי יעדי ההגנה הינו תהליך שדורש זמן ומשאבים. אחד הדרכים המומלצות לטובת ביצוע התהליך בצורה אפקטיבית היא להקפיד על הרזולוציה הנדרשת למיפוי ולדבוק בה. לדוגמה: מצד אחד, מובן שאין צורך לפרט את כל השרתים ואת כל עמדות הקצה של בית החולים, ומצד שני - הכללה גסה של כל השרתים כמקשה אחת עלולה לגרום למיפוי לא ממצה או אף לעלויות הגנה לא מידתיות.

בנוסף, ארגון אשר כתב תוכנית המשכיות עסקית, בין היתר באמצעות פרויקט מקביל שנערך על ידי המשרד, יוכל להסתייע בהערכת עצמת הנזק לארגון ולמידת התלות של תהליכי הארגון בנכסי המידע.

טבלת מיפוי נכסים תמולא על בסיס אקסל המיפוי של משרד הבריאות, תוך חלוקה למשפחות המערכות הרלוונטיות. להלן המחשות של הכלים (הבהרה: מדובר בהמחשה בלבד. יש למלא ע"ב האקסלים המקוריים):

מידע כללי (מערכות מידע)						
סוג מערכת	שם המערכת	תיאור כללי של המערכת	אחראי מערכת	שם ספק או פיתוח מקומי	תהליך נתמך/תחום נתמך (בחר מאשרימה לאחר בחירת תהליך)	תת תהליך נתמך (בחר מאשרימה לאחר בחירת תהליך)

מידע כללי (מכשור רפואי)								
סוג המכשור	שם המכשור	דגם המכשור	שם הספק	האם הציוד נתמך ע"י הספק (כן / לא)	שם היצרן	מס' יחידות ציוד	מיקום המכשיר	סוג הפעלה מערכת

מידע כללי (מערכות תשתית ובקרה)		
סוג מערכת	תיאור כללי	אחראי המערכת

בנוסף, יש לזכור כי על פי דרישות החוק להגנת הפרטיות והתקנות שהוצאו מכוחו - תקנות הגנת הפרטיות (אבטחת מידע), חייבת חובה למפות את מאגרי המידע כמשמעותם בחוק, ולהגדיר במסמך הגדרות המאגר נושאים כגון מטרת השימוש במידע, הסיכונים העיקריים של פגיעה באבטחת המידע וכו'. **לטובת מימוש האמור, קובץ אקסל המיפוי כולל גם גליון עבודה ייעודי (sheet) לנושא מאגרי המידע, ויש לבצע את המיפוי על בסיסו. להלן דוגמא של הכלי (הבהרה: מדובר בהמחשה בלבד. יש למלא ע"ב האקסלים המקוריים):**

מיפוי מאגרי מידע											
שם המאגר	מטרת השימוש במידע	מקורות המידע	מספר המאגר (אם רשום)	תאריך רישום המאגר	שם אחראי בארגון / מנהל המאגר	סוגי המידע שמכיל המאגר	מיקום המכשיר	האם מכיל מידע אודות מעל 100 אלף מטופלים	מהו מספר בעלי ההרשאה למאגר?	האם נעשה שיתוף של המאגר אל מחוץ לגבולות המדינה?	אופן ההתחברות למאגר

עם סיום מיפוי הנכסים, יוכל הארגון הרפואי להצביע על הנכסים המשמשים תהליכים שהוא מגדיר כקריטיים. השלב הבא יהיה לקבוע מי היא רמת הסיכון לנכס/מערכת ספציפית. יובהר: הן שלב מיפוי התהליכים ועדי ההגנה (שלב 1) והן שלב "קביעת רמת הסיכון" (שלב 2) מתבצעים על בסיס אותו קובץ אקסל מובנה של המשרד.

שלב 2: קביעת רמת ערכיות, הסתברות הפגיעה ביעד ההגנה ורמת הסיכון הכוללת שלו

רמת ההגנה הנדרשת לכל נכס נגזרת מרמת הערכיות שלו לארגון. על-פי תורת ההגנה, הנכסים מדורגים לפי 4 רמות ערכיות. הציון 1 מציין רמת ערכיות נמוכה ו-4 מציין רמת ערכיות גבוהה. בהתאם, מותאמות לנכסות בקורות במדרג משתנה. בסיום שלב זה, יידע הארגון להגדיר את הנכסים החשובים ביותר לתפקוד העסק לעומת הנכסים המשניים. על בסיס אקסל המיפוי, ארגון יוכל לקבוע הן את רמת הערכיות של המערכת והן את ההסתברות לפגיעה במערכת. השאלון הותאם הן למגזר הבריאות ספציפית והן למשפחות מערכות כפי שהוגדר לעיל.

הערכיות של המערכת (Impact) תיקבע לפי הציון המקסימלי שקיבלה המערכת ע"י מענה לשאלות הערכיות. רמת חשיפת המערכת (הסתברות הפגיעה במערכת (Propbaility)) תיקבע לפי הציון הממוצע שקיבלה המערכת ע"י מענה לשאלות המסוכנות.

עבור מערכות מידע:

רמת ערכיות המערכת (Impact)												
השפעת המערכת על הארגון						סיווג המידע במערכת						
חשוב	תלות מה הנזק שגורמות מערכות אחרות בעת פגיעה במערכת זו?	סודיות מה הנזק בעת חשיפת מידע שמצוי במערכת?	שלמות מה הנזק בעת שיבוש הנתונים במערכת?	זמינות מה הנזק שיגרם בעת נפילת המערכת לפרק זמן ממושך?	זמינות תוך כמה זמן מעת נפילת המערכת הוגדר להעלות חזרה?	האם המערכת מכילה מידע תפעולי?	האם משולבת ציוד רפואי?	האם המערכת מכילה מידע עסקי רגיש?	האם המערכת מכילה מידע סטטיסטי ומידע מחקרי?	האם מדובר במערכת ייעודית למידע רפואי חסוי ביותר?	האם המערכת מכילה פרטי של מעל K100 מטופלים או/יש במערכת מעל ל-100 משתמשים?	האם המערכת מכילה מידע פרטי או רפואי מזהה?

כמו כן, השאלון הינו רב-ברירה ומחשב אוטומטית את הציונים.

לדוגמא:

זמינות מה הנזק שיגרם בעת נפילת המערכת לפרק זמן ממושך?	שלמות מה הנזק בעת שיבוש הנתונים במערכת?

רמת חשיפת המערכת (הסתברות הפגיעה במערכת / Propbaility)
אם לא ידועה התשובה נא לא לענות (להשאיר תא ריק)

חשוב	האם המערכת מכילה ממשק חיצוני לאינטרנט?	האם קיימת אופציה להתחברות מרחוק למערכת? כיצד?	האם סביבת ההתקנה של המערכת מוקשחת?	האם בוצע סקר סיכונים/ PT במערכת והאם הוטמעו הממצאים?	האם המערכת מתוחזקת ע"י גורם חיצוני (בהתחברות מרחוק או בגישה פיזית)?	כמות המשתמשים במערכת	האם למערכת עצמה נעשו עדכוני גרסה/אבטחה?	לאילו גורמים יש נישות פיזית למערכת?
------	--	---	------------------------------------	--	---	----------------------	---	-------------------------------------

גם בשאלון החשיפה, השאלון הינו רב-ברירה ומחשב אוטומטית את הציונים :

האם בוצע סקר סיכונים/ PT במערכת והאם הוטמעו הממצאים	האם המערכת מתוחזקת ע"י גורם חיצוני (בהתחברות מרחוק או בגישה פיזית)?	כמות המשתמשים במערכת	האם למערכת עצמה נעשו עדכוני גרסה/אבטחה?
בוצע וישמו הממצאים	אינה מתוחזקת ע"י גורם חיצוני	אלף ומעלה	נעשה עדכון בחצי שנה אחרונה
בוצע וישמו הממצאים	גישה באישור נקודתי לכל גישה	אלף ומעלה	נעשה עדכון בחצי שנה אחרונה
בוצע וישמו הממצאים	אינה מתוחזקת ע"י גורם חיצוני	בין 201 לאלף	נעשה עדכון בחצי שנה אחרונה

עבור מכשור רפואי :

רמת ערכיות המערכת (Impact)

חשוב	השפעת המערכת על הארגון				סיווג המידע במערכת שמפעילה את המכשור הרפואי			
	תלות מה הנוק שגורמות מערכות אחרות בעת פגיעה במערכת זו?	סודיות מה הנוק בעת חשיפת מידע שמצוי במערכת?	שלמות מה הנוק בעת שיבוש הנתונים במערכת?	זמינות מה הנוק שיגרם בעת נפילת המערכת לפרק זמן ממושך?	האם המערכת מכילה מידע סטטיסטי ומידע מחקרי?	האם המערכת מכילה מידע סטטיסטי ומידע מחקרי?	האם המכשור אוגר מידע פרטי/רפואי של מעל K100 מטופלים אורו יש במערכת מעל ל-100 משתמשים?	האם המכשור אוגר מידע פרטי מקומי או רפואי מזוהה?

רמת חשיפת המערכת (הסתברות הפגיעה במערכת / Propbaility)
אם לא ידועה התשובה נא לא לענות (להשאיר תא ריק)

חשוב	לאילו גורמים יש גישה פיזית למערכת?	האם למערכת עצמה נעשו עדכוני גרסה/אבטחה?	האם המערכת מתוחזקת ע"י גורם חיצוני (בהתחברות מרחוק או בגישה פיזית)?	האם בוצע סקר סיכונים / PT למכשור והאם הוטמנו הממצאים?	האם קיימת אופציה להתחברות מרחוק למערכת? כיצד?	האם המערכת מכילה ממשק חיצוני לאינטרנט?	האם המכשור מחובר או יכול להתחבר לרשת?
------	------------------------------------	---	---	---	---	--	---------------------------------------

עבור מערכות תשתית ובקרה :

רמת ערכיות המערכת (Impact)			
חשוב	תלות מה הנזק שגורמות מערכות אחרות בעת פגיעה במערכת זו?	שלמות מה הנזק בעת שיבוש הנתונים במערכת (לדוג' שינוי טמפר', שינוי לחץ גזים וכו')?	זמינות מה הנזק שנגרם בעת נפילת המערכת לפרק זמן ממושך (עד להפעלה ידנית)?

רמת חשיפת המערכת (הסתברות הפגיעה במערכת / Propbaility) אם לא ידועה התשובה נא לא לענות (להשאיר תא ריק)						
חשוב	לאילו גורמים יש גישה פיזית למערכת?	האם למערכת עצמה נעשו עדכוני גרסה/אבטחה? (מערכת הניטור/בקרה - אם לא קיימת מערכת כזו להשאיר ריק)	האם המערכת מתוחזקת ע"י ספק/טכנאי חיצוני (בהתחברות מרחוק או בגישה פיזית)?	האם קיימת אופציה להתחברות מרחוק למערכת? כיצד?	האם המערכת מכילה ממשק חיצוני לאינטרנט?	האם המערכת מנוטרת ע"י גורם הנדסה לבחינת תקלות בזמן אמת?

חישוב רמת הסיכון של הנכס (שקלול ציון עוצמה והסתברות)

לאחר שהגורם הרלוונטי בארגון מילא את השאלונים עבור כלל מערכותיו, יחשב האקסל באופן אוטומטי שלושה ערכים:

1. **ערכיות (Impact – למעשה "עוצמת" הפגיעה בארגון עקב הפגיעה במערכת):** ציון זה קובע את רמת הבקורות הנדרשת עבור המערכת הספציפית.

2. **חשיפה (Propability – למעשה מהי ההסתברות של המערכת למתקפות פוטנציאליות):** ציון זה רלוונטי לצורך קביעת רמת סיכון

3. **רמת סיכון המערכת (RISK):** בהתבסס על המכפלה ערכיות X חשיפה, ציון זה קובע את הדחיפות שיש לתת להטמעת בקורות הגנת הסייבר עבור מערכות ספציפיות, ומשמש לתעדוף בין פרויקטי הגנה של מערכות שונות.

יובהר: **רמת** הבקורות שיש להטמיע לכל מערכת תיקבע אך ורק עפ"י מענה לשאלות הערכיות. שאלת הסיכון נוגעת אפוא **למהירות הטמעת ויישום** הבקורות על פי תכנית העבודה וביחס לפרויקטי הגנה אחרים.

ניתן לצפות בכלל הציונים בגליון "ציונים לקביעת רמת בקורות תוה"ג". להלן המחשה כיצד נראה גליון כזה בהתייחס למערכת המידע של הארגון:

סינון רמת יישום בקורות		סינון רמת בקורות עפ"י CIA				
ציון סיכון כללי	האם יש צורך בבקורות הגנת הפרטיות?	ציון סודיות	ציון אמינות	ציון זמינות	רמת בקורות להטמעה	שם המערכת

עבור כל מערכת יתקבל ציון כללי של ערכיות (למעשה, רמת בקורות להטמעה).

לצד ציון כללי זה יפורטו הציונים הספציפיים שקיבלה המערכת ביחס לכל אחת מקבוצות הנזק (זמינות, אמינות וסודיות). ציונים אלה נועדו כדי להקל לזהות בשלב ההטמעה איזה סוגי בקורות נדרשות עבור המערכת. כך לדוגמא, עבור מערכת בקרה בה לא מצוי מידע (ואשר בשל כך תקבל היא ציון סודיות 0), לא יהיה צורך להטמיע בקורות שמטרתן מניעת זליגת מידע (להבדיל מבקורות שמטרתן מניעת השבתת המערכת).

כמו כן, ניתן לסנן את העמודה "רמת בקורות להטמעה" כך שכאשר רמת הבקורות להטמעה זהה בין מספר מערכות, ניתן לדעת באילו מערכות יש לתעדף טיפול עפ"י ציון סיכון כללי. לדוגמא, כאשר מדובר במספר מערכות ברמת בקורות 2 יש ל"טפל" ראשית במערכות עם רמות הסיכון הגבוהות יותר (הסיבה לכך היא שהסתברות הפגיעה בהן גבוהה יותר).

שלב 3: כיצד נכון להגן

בשלב 2 הגדרנו עבור כל נכס את מידת הערכיות (עוצמה) בסולם של 1-4. מידת ההגנה על כל נכס נגזרת ישירות ממידת הערכיות שלו.

לצד כל בקרת הגנה בפרק הבא הוגדר האם היא נדרשת עבור נכס שציון העוצמה שלו הוא 1, 2, 3 או 4. עבור כל נכס יש לממש את סך כל הבקורות שהערך שלהן ("רמת הבקרה", ראה מודגש באיור מטה) קטן או שווה לציון העוצמה של הנכס. כך, לדוגמה, עבור נכס שציון העוצמה שלו הוא 3 נדרש ליישם את הבקורות שערכן הוא 1, 2 ו-3. הגדרה זו מסייעת להתאים את הבקורות הנדרשות ליישום ביעד ההגנה, אל מול פוטנציאל הנזק.

זמינות	אמינות	סודיות	Cyber Kill Chain	מיפוי לבקורות ISO מתאימות	רמת בקרה	מקור NIST	סוג הבקרה (מונעת / מגלה / מנחה / מתקנת / מאוששת)	תוספת דרישות מגזר הבריאות	דוגמא ליישום הבקרה	הסבר משלים	הבקרה	כותרת	משפחה	פונקציה	מזהה פונקציה
--------	--------	--------	------------------	---------------------------	----------	-----------	--	---------------------------	--------------------	------------	-------	-------	-------	---------	--------------

שלב 4: הגדרת פערי הגנה

אל מול רשימת בקורות ההגנה המפורטות בפרק הבקורות, בדוק מה מיושם כיום בארגון ומה נדרש לבצע. בסיום תהליך זה, הארגון יקבל רשימת פערים "רצוי מול מצוי".

מאחר שלא כל הבקורות מיושמות באופן זהה בארגון, חשוב לוודא, כי עבור יעדי הגנה מהותיים לארגון מתבצעת בדיקה פרטנית. הסיבה לכך נעוצה בעובדה, שלא תמיד בקרה מסוימת מוטמעת בכל יעדי הארגון. הניסיון מראה, כי למרות שעל-פי-רוב בקורות מיושמות בארגונים בצורה רוחבית, הרי שיש לא מעט מקרים, שבהם הבקרה לא יושמה במערכת ספציפית.

מאחר שלא כל הבקורות נדרשות למימוש בכל נכס, היעזר ברמת הערכיות שהוגדרה לכל נכס בשלב 3 לטובת זיקוד רשימת הפערים.

רשימת פערים זו תהיה הבסיס לבניית תכנית העבודה של הארגון (שלב 5).

דוגמא להגדרת פערי הגנה:

בקרה	כלל הארגון	מערכת התיק הרפואי	מערכת צילומי רנטגן	מערכת ניהול המעבדות
4.16: יש לבצע נעילת חיבורים (Sessions) במקרה של חוסר פעילות זמני	קיים חלקית	קיים	לא קיים	קיים
16.2: ביצוע התקשרויות רק עם ספקים העומדים בתקן ISO 27001 או ISO 27799	קיים תהליך מסודר של החתמת ספקים	הספק עבר הסמכת ISO	הספק עבר הסמכת ISO	הספק עבר הסמכת ISO
22.3: יש לבצע מבדקי חדירה תשתיתיים ואפליקטיביים למערכות הארגון (בין אם הן פנימיות או	אין תהליך סדור של ביצוע מבדקי חדירה. נדרש לממש מול	בוצעה לפני מסירת המערכת מהספק	לא בוצע	לא בוצע

			מערכות ברמה 3 ומעלה	חיצוניות אבל מנוהלות על ידו אחת לתקופה
--	--	--	------------------------	---

שלב 5: תכנית עבודה

כל בקרה בפרקי הבקורות מגינה מפני סיכון עסקי, שנובע מפגיעת סייבר.
סדר העדיפויות של יישום הבקורות החסרות לארגון במסגרת תכנית העבודה ייקבע על-ידי שקלול רמת הסיכון של נכס, עלות הפתרון ומורכבות מימוש.

6. בקורות נדרשות למימוש תורת ההגנה

דרישות ההגנה מארגון מכונות בשפה המקצועית "בקורות" (ובאנגלית: controls). לטובת הגנה על הארגון בתחום הסייבר, הארגון נדרש לממש בקורות בתחומים שונים. בקורות אלו כוללות תהליכים, נהלים, מערכות הגנה וטכנולוגיות, אשר הארגון מיישם במטרה להפחית את הסיכון להתממשות אירוע במרחב הסייבר.

הבקורות המתועדות מבוססות על מסגרת אבטחת הסייבר של ארגון NIST אשר אומצה על ידי רשות הסייבר. הבקורות תואמות גם לדרישות התקן ISO 27799, אשר נדרש בארגוני הבריאות בישראל, ומסונכרנות עם הנחיות משרד הבריאות. הבקורות כוללות גם הפניות מפורטות אל ההנחיות או התקנים מהם ינקו את התכנים.

כך לדוגמא, בקורות הנוגעות להגנה על מידע בהתאם לסיווגו, מסונכרנות עם נהלי משרד הבריאות בנושא סיווג מידע במערכת הבריאות והוראות לטיפול ושימוש במידע לפי סיווגו; בקורות הנוגעות להגנה על מכשור רפואי, מסונכרנות עם מדיניות משרד הבריאות בנושא אבטחת מידע והגנת סייבר במכשור רפואי; ובקורות הקשורות להגנת מידע מוגן בהתאם לחוק הגנת הפרטיות, מסונכרנות עם תקנות הגנת הפרטיות (ראה דוגמא מטה בעמודה "תקנות הגנת הפרטיות" וב"הרכב המקרה המשוקללת"). כלל הבקורות כוללות (בעמודה "הרכב המקרה המשוקללת") גם הפניות מפורטות לסעיפים הספציפים בתקנים ובנהלים מהם ינקו הבקורות את המידע.

בהקשר זה תודגש החשיבות לנושא מודעות עובדים ותרגילים להעלאת המודעות הזו. במסגרת זו, גיבוש תכנית רב-ממדית הפונה לכל האוכלוסיות במשרד הבריאות ובמוסדות הבריאות, מופיעה בהנחיות משרד הבריאות (מדיניות בנושא מודעות עובדים לסיכונים אבטחת מידע והגנת סייבר וכן תרגולי סייבר במשרד הבריאות – מדריך לתרגול עצמי גרסא 1.0) ובהתאמה מופיעה בצורה מסונכרנת בקובץ הבקורות.

לטובת בנייה של תורת הגנה פרופורציונלית, הבקורות במסמך זה סווגו לרמות שנעות בציר של 1-4, כאשר בקורות מרמה 1 הן הבקורות הבסיסיות ביותר, אשר נדרשות מכל ארגון ולכל נכס, ואילו בקורות מרמה 4 הן כאלו אשר נדרשות עבור יעד הגנה שפוטנציאל הנוק שלו הינו 4 (ראה העמודה "רמת בקרה" בטבלה מטה).

מספר בקרה	כותרת	הבקרה	רמת בקרה	NIST 800-53 R. 4	ISO 27001 / 27799:2016	הנחיות המשרד	תקנות הגנת הפרטיות	הרכב המקרה המשוקללת
22.3	מבדקי חדירה	יש לבצע מבדקי חדירות למערכות על בסיס תקופתי	3	CA-8	-	-	סעיף 5(ד), מיפוי מערכות המאגר וביצוע סקר סיכונים	תוספת ע"ב סעיף 5(ד) לתקנות הגנת הפרטיות (מבדקי חדירה)

מוכנות ארגון למשבר סייבר

7. מוכנות ארגון למשבר סייבר

רקע

על פי התפיסה הלאומית בסייבר להיערכות ולניהול מצבי משבר, ועל פי תורת ההגנה בסייבר לארגון, כל ארגון נדרש להיערך להתרחשות של אירוע סייבר ומשבר סייבר, ולהגדיר תהליך מובנה לניהול במידה שהתרחשו במרחב אחריותו. תהליך זה נדרש להכיל הן את מדיניות הארגון בנושא והן את תוכנית הפעולה הארגונית בעת התרחשות אירוע/משבר סייבר. בהתאם לדרישות במסמכים שתוארו לעיל, יש להגדיר מה המענה שיש לארגון בהתחשב במשימותיו, בשרשרת הדיווח וביכולתו של הארגון להגיב בכלים העומדים לרשותו, ממשקים ארגוניים, משאבים נדרשים ועוד. מומלץ לפרט את תהליך הדיווח על אירוע/משבר סייבר הן בתוך הארגון והן מחוצה לו.

בתוך הארגון - חשוב ליידע נציג הנהלה בדרג, C-Level, CISO, יועץ משפטי, איש יחסי ציבור. נציג ההנהלה יחליט על הצורך בהתנתות צוות ניהול משבר סייבר (ראו להלן).

מחוץ לארגון - דיווח על פי חוק/רגולציה. דיווח ל CERT בריאות **[נספרי טלפון]** מומלץ להגדיר מראש צוות ארגוני, התומך בניהול משבר בסייבר. צוות ניהול משבר, בראשות מנהל בארגון, יכול אנשים בעלי ידע מהתחום הטכני, המשפטי, יחסי ציבור, מינהל ועוד. ארגונים שאינם בשלים לניהול עצמאי של משבר יכולים לשכור שירותים של גופים חיצוניים הנותנים שירותים אלו, אך הניהול והבקרה צריכים להישאר ברמת הנהלת הארגון.

לאור המהירות שבה מתפתח אירוע סייבר ופוטנציאל הנזק הגדול של אירוע סייבר לארגון, מומלץ להגדיר מראש תהליך ושרשרת קבלת החלטות בעת אירוע סייבר.

על מנת להתמודד עם אירועי משבר מומלץ להגדיר מראש את הממשקים ואת דרכי התקשורת הנדרשת של צוות ניהול המשבר בכל שלב של הטיפול בו – בתוך הארגון וכ מול גורמים חיצוניים (כולל דפי קשר בזמני חופשות/שבתות וכד').



- על מנת למזער את הנזק המשני של אירוע סייבר חשוב להכיר את הגורמים החיצוניים שעמם ייתכן כי יידרש קשר במהלך האירוע (למשל: משרד הבריאות – CERT בריאות, חברות נותנות שירותי סייבר, משרדים/רשויות ממשלתיות, גורמי יחסי ציבור, חברי דירקטוריון ועוד). חשוב כי המיפוי של הגורמים יבוצע מראש וכן כי יובנו הזיקות בעת התרחשותו של אירוע סייבר:
1. מומלץ להכיר את הגורמים הרשמיים במדינה בתחום הסייבר ואת תחום אחריותם, ובהתאם לכך לדווח על האירוע (משרד הבריאות CERT בריאות [מספר טלפון], מערך הסייבר, יחידת הסייבר המשטרתית, הרשות להגנת הפרטיות וכו').
 2. נדרש לעדכן את הרגולטור משרד הבריאות – CERT בריאות [מספר טלפון] על אודות האירוע והפעילויות שננקטו בהתאם להגדרות.
 3. על מנת למזער את הנזק של אירוע סייבר על גורמים/גופים אחרים חשוב לעדכןם בהקדם האפשרי, וזאת אם עשויה להיות השלכה של אירוע סייבר מתרחב (למשל, במידה שקיימת ארכיטקטורה המקשרת בין ארגונים, או שהארגון הוא חלק משרשרת אספקה לגופים אחרים).
- חשוב מאוד להכשיר את הצוות ולתרגל אותו ברמה שנתית על מנת לשמור על כשירותו.
- חשוב להגדיר נוהלי עבודה ארגוניים על מנת למנוע פעולות שגויות (מה מותר למחוק, לנתק ואיד). ...נהלים אלו חשובים ביותר על מנת למנוע פגיעה בדיני ראיות משפטיות לצרכים שונים:
1. בחשד לפלילים - על גורמים משטריים לבצע עבודה חקירתית (פורנזית) לגילוי התוקף.
 2. לצורך מזעור נזקים לארגון לאחר סיום האירוע - על גורמים משפטיים לפעול במישור המשפטי נגד התוקף או הגורמים שפעלו ברשלנות.

דגשים להיערכות מקדימה של הארגון לקליטת צוות IR

- א. צוות ניהול המשבר יידרש להסתייע בגורמים בעלי מומחיות בתחקור אירוע סייבר, שתפקידם להכיל את האירוע מבחינה טכנית ולעזור באומדן הנזקים ובמתן מענה טכנולוגי. זהו צוות ה- IR - צוות זה הינו חלק מהארגון, או שירות שהארגון שוכר מגוף מקצועי חיצוני.
- ב. על מנת להבטיח כי בסיס ההגנה של הארגון מיושם וכי קיימת מדיניות הגנה על הרשתות ועל המידע הארגוני, חשוב שהארגון יכיר ויישם את תורת ההגנה בסייבר לארגון.
- ג. בפרט, חשוב שהארגון ימפה את תהליכי הליבה שלו ואת נכסי הסייבר החיוניים התומכים בתהליכים אלו, וכן ינהל את הסיכונים שלהם. דרישה זו הינה גם אבן היסוד התפיסה הלאומית בסייבר להיערכות ולניהול מצבי משבר והיא מאפשרת לצוות ה- IR - לפעול במהירות, ביעילות ובאפקטיביות להכלת האירוע ולאומדן הנזקים (הפוטנציאליים).
- ד. חשוב לתחם באילו אזורים/תחומים יכול וצריך צוות ה- IR - לפעול ואילו אזורים/תחומים מוגדרים כמחוץ לתחום.
- ה. נדרש לקבוע עקרונות מקדימים להתערבות וממשקים של צוותי ה- IR - הן אם מדובר בצוות פנימי והן אם מדובר בצוותים חיצוניים. על הארגון לתחם את שלבי המעורבות של צוותי ה- IR.
- ו. חשוב מאוד להגדיר איש קשר **ייעודי וקבוע** של הארגון, המוגדר כמומחה תוכן ברשת הארגונית. זאת על מנת שניתן יהיה למקד את הצוות במקום הנדרש ולתת את הרקע הטכנולוגי הדרוש עם התפתחות האירוע. לאיש הקשר יהיה תיק הפעלה מעודכן ומתעדכן (מודפס), שירכזו בו כלל הנתונים ופרטי המידע הנדרשים לצוות ה- IR (כמפורט בסעיף הבא).
- ז. הארגון נדרש להכין מראש תיק הפעלה לצוות המיועד, אשר יוכן יחד עם צוות ה- IR - בשגרה, ויכיל את המידע הקריטי ביותר, הכולל: ארכיטקטורה, טופולוגיית רשת, סוגי חומרה, פיירוול, נתבים, מערכות תקשורת וכמובן מיפוי של התהליכים המרכזיים בארגון, וכן פרטי אנשי הקשר המרכזיים בעת אירוע.
- ח. רצוי שהארגון יכין עצמו בפן הלוגי לטיפול באירוע באופן שיסייע לצוות ה- IR - לעבודתו. למשל, על ידי איסוף ושמירה של לוגים ממערכות הפעלה וממערכות האבטחה הקיימות בארגון, הקלטה ושמירה של תעבורת רשת, הגדרה של PORT האזנה לחיבור מערכת הקלטה לתעבורת הרשת, יכולת לבצע הפצה של "סוכנים" בעמדות הקצה והשרתים וכד'.
- ט. חשוב להגדיר נוהלי עבודה פנימיים לצוותי ה- IT - בארגון במקרה של אירוע סייבר, על מנת למנוע פעולות שגויות, שיקשו על צוותי ה- IT - לפעול בצורה מיטבית (למשל: האם לנתק רשתות, האם להריץ כלי ניקוי/אנטי וירוס וכד').
- י. חשוב מאוד לשמר גם בשגרה כשירות בסיסית של צוות ה- IR - כולל עדכונים תקופתיים של מידע מודיעיני, היכרות עם תקיפות ויכולות טכנולוגיות חדשות, ביצוע תרגילים וסימולציות וכן ביצוע של מחקרי "כמעט ונפגע" על מנת להפיק לקחים מאירועים שלא התממשו.
- יא. מומלץ לקיים תרגול/סימולציה ארגונית אחת לשנה לפחות.
- יב. מומלץ לקיים תהליכי ניהול ידע, לרבות הפקת לקחים ולמידה מאירועים שהתרחשו בארגון.
- יג. יש להדגיש כי CERT בריאות עומד לרשות הארגון לסיוע ולמענה בכל שלב של האירוע.

דגשים לצוות/שירות IR מיומן ומקצועי

דגשים אלו הן דרישות מינימום לצוות IR איכותי. הדגשים הינם בקטגוריות האלה: כוח אדם, כלים וטכנולוגיות, מתודולוגיית עבודה והכרות מקדימה עם הארגון. כמו כן מובאים ככלי אצבע ל SLA - ולממשק עם הדוברים של הארגון. כמובן שבתחומים ייעודיים ידרשו יכולות נוספות/ ייעודיות על מנת לטייב את יכולות ה IR - של הארגון.

המלצות כוח אדם

1. בכל צוות IR יוגדר מוביל אירוע, שישמש כמרכז הנתונים ותמונת המצב עבור גורמי העניין, בארגון ומחוץ לו.
2. חברי הצוות יורכבו מבעלי ידע ומיומנות טכנולוגית:
 - א. באיסוף נתונים – כגון הקלטת תעבורת תקשורת, שכפול כוננים וזיכרון, איסוף לוגים וכו'.
 - ב. בניתוח וסינון הנתונים לאישוש או לזיכוי של אירוע.
 - ג. בביצוע שינויים לניקוי וחסימה של הפעילות הזדונית במערכות.
3. בנוסף על כך רצוי לשלב מומחי תוכן נוספים בהתאם לצורך ולמורכבות הנדרשת למתן פתרון: מומחי Malware Analysis ו- Reverse Engineering.
4. בדרישות מחברה המספקת שירותי IR חשוב לבחון:
 - א. האם אנשי הצוות מוסמכים בהתאם למסמך אסדרת המקצועות של מערך הסייבר הלאומי - מוסמך תחקור סייבר, או הסמכות אחרות בינלאומיות, אשר מוכיחות את הידע המקצועי הטכני של הצוות.
 - ב. האם ניתנת עמידה ב SLA - של 4 שעות לנוכחות של צוות ראשוני On Site.
 - ג. האם החברה יודעת לפעול לפי דין שימור ראיות, אשר יתאימו לדרישות רשויות החוק.
 - ד. האם החברה מחזיקה מומחי Malware Analysis ו- Reverse Engineering.

המלצות כלים/טכנולוגיות

1. למומחי הצוות נדרש "ארגז כלים" טכנולוגי, שיאפשר התמודדות עם האירוע. ארגז הכלים של הצוות יכול לכולל:
 - א. כלים טכניים ייעודיים לטיפול באירוע ולאיסוף הנתונים, בהם:
 1. "הסנפת" תעבורת הרשת.
 2. שכפול כוננים קשיחים Hard Disks וקבצים.
 3. הורדת הזיכרון הנדיף Memory Dump.
 - ב. כלים לניתוח ולאתור פעילות זדונית לפי חתימות, מזהים, התנהגות ואנומליה – ברמה של תעבורת רשת, תהליכים בזיכרון וקבצים.
 - ג. כלים לניתוח פורנזי של מערכות הפעלה לחקירה ולהצגה של הפעולות שבוצעו.
 - ד. כלים המאפשרים שחזור ואחזור של מידע שנמחק.
2. בדרישות מחברה המספקת שירותי IR חשוב לבחון קיום:
 - א. יכולת תמיכה בניטור 24/7 ובזמן אמת של מערכות הארגון (בין אם באתר או באופן מרוחק).
 - ב. התחייבות כי הכלים שבהם נעשה שימוש הינם "בטוחים" ולא יגרמו נזק לתשתיות הארגון.
 - ג. תיאור מוצר EDR ומגבלת פריסה.
 - ד. תיאור מוצר Network Analytics ומגבלת פריסה.
 - ה. תמיכת המוצרים במערכות הפעלה מבוססות Windows.
 - ו. תמיכת המוצרים במערכות הפעלה מבוססות Linux.
 - ז. יכולת תחקור סביבות מבוססות Mac.
 - ח. ביצוע שכפולים על פי סטנדרט קביל בבית משפט.
 - ט. ציוד טכני לביצוע ניתוח בתנאי שטח ומעבדה ניידת.
 - י. מעבדת Back Office לניתוח מתקדם של קבצים.
 - יא. יכולת ביצוע Reverse Engineering לקבצים.
 - יב. פורמט דו"ח להצגת הממצאים וסיכום הפעילות לרמת הנהלה.
 - יג. פורמט דו"ח מפורט ברמה טכנית מעמיקה, הכולל את כל הפעולות שבוצעו וכן המלצות לטיפול.

המלצות מתודולוגיה

1. הגם שכל תקיפת סייבר הינה ייחודית ודרכי הכלתה יהיו שונות, נדרשת מתודולוגיית עבודה סדורה לצוות על מנת לוודא עבודה איכותית ואפקטיבית - לצמצם את משך האירוע, למזער את הנזק לארגון ולבצע מינימום תקלות מול צוות ניהול המשבר.
2. בדרישות מחברה המספקת שירותי IR חשוב לבחון:
 - א. ניסיון בטיפול באירועי IR בארגוני Enterprise / SMB אירוע סייבר משמעותי בחברה.
 - ב. בדיקת דו"ח סיכום IR בארגון בגודל המתאים.
 - ג. בדיקת דו"ח תקציר מנהלים לארגון בגודל המתאים/או לחלופין לציין דרך התחברות לרשת החברה דרך התחברות לרשת החברה.
 - ד. בדיקת מתודולוגיית החברה לטיפול באירועי IR.

המלצות להיכרות מקדימה עם הארגון

1. אירוע סייבר מתפתח במהירות ועלול להידרדר לכדי משבר. היכרות מוקדמת של צוות ה-IR עם הארגון לו הוא מספק שירות יכולה לצמצם את משך האירוע, להכילו במהירות ולהקטין את הסיכוי להתפתחות משבר ולהחמרתו.
2. בדרישות מחברה המספקת שירותי IR חשוב לבחון:
 - א. האם קיימת בחברה היכרות קודמת עם רשת הארגון מפרויקטים מקבילים.
 - ב. האם החברה מקימה תיק עמדה.
 - ג. האם החברה מקימה עמדות תחקור On Site ולציין או לחילופין דרך התחברות לרשת החברה.
 - ד. באילו תדירויות מבוצעות פגישות הרענון בין הספק ללקוח.
 - ה. האם מבצע "סקר אתר" לאיתור לוגים רלוונטיים ולטיוב מוצרים טרום אירוע.
 - ו. האם כלול בהצעת המחיר בנק שעות ראשוני לטיפול בחשדות לאירועים בשוטף.

SLA

1. הארגון נדרש להגדיר את אופן הטיפול ואת זמני הטיפול באירוע, משלב הקריאה הטלפונית ועד ההגעה לאתר ותחילת הטיפול בשטח (למשל, עד חצי שעה מענה טלפוני מרגע פניית הארגון).
2. הארגון נדרש להגדיר זמני הגעה לאתר מרגע קבלת קריאה או החלטה על צורך בצוות בשטח) למשל, עד 4 שעות ברדיוס של 20 ק"מ מהחברה ועד 6 שעות במרחק גדול יותר).
3. בשל אופיים של איומי סייבר, נדרש להגדיר את זמינות הצוותים. במקרה של סיכון רב לארגון באירוע סייבר, הצוותים נדרשים לזמינות של 24/7 הן במצבי שגרה והן במצב חירום כללין לשים לב למצבי חירום במשק/לחימה וכו').

ממשק צוותי IR עם הדוברות

1. בעת ניהול משבר הנובע מאירוע סייבר קיימת חשיבות רבה לנושא של דוברות והסברה של האירוע ומשמעותו לגורמי עניין מחוץ לארגון. צוות הדוברות נדרש להסתמך על מידע שמתקבל מצוות ה-IR - חשוב שהמידע יבוסס על נתוני אמת ויתאר בשפה טכנית וניהולית מה קרה וכיצד פועל הארגון כדי להתמודד עם האירוע.
2. חשוב מאוד שצוות ה-IR יפעל על פי מדיניות הדוברות של הארגון ויכיר את הכללים והמגבלות. חשוב מאד להכין נוהל עבודה ודיווח בתחום הדוברות ויחסי הציבור, לרבות דיווח לבעלי המניות, לדירקטוריון, לרשויות ממשלתיות, לעיתונות ועוד.
3. חשוב שבצוות ה-IR -יוגדר איש קשר יחיד, שמרכז את המידע מול גורמי חוץ בכלל, והדוברות בפרט.
4. על מנת לסייע לדוברות, צוות ה-IR -נדרש לדיווח ראשוני מהיר ככל האפשר מרגע גילוי האירוע (כלל אצבע 12 -שעות) ודיווחים עתיים (כלל אצבע - כל 24 שעות עד להכלת האירוע).
5. על מנת להיערך לדיווחים, ראוי להכין מראש שאלות מובנות שצוותי ה-IR -יכירו, ובהתאם יידעו לתת מידע שוטף. מידע כזה יכול לכלול את הנתונים הבאים:
 - א. הממצאים הראשוניים מהתקיפה (כיצד קרה, תרחיש החדירה והתקיפה, האם ידועה זהות התוקף, אילו מערכות נפגעו, מהי הפגיעה).
 - ב. מה קרה? מתי קרה? האם מערכות האבטחה כשלו? האם מערכות האבטחה זיהו את התקיפה? כיצד הגיבו?
 - ג. מהם הצעדים הננקטים על מנת להכיל את האירוע ולהימנע מהרחבת האירוע.
 - ד. תוך כמה זמן ישובו השירותים לתפקד.
 - ה. האם נגרם נזק למידע של הארגון? איזה מידע?
 - ו. מי התוקף?

הערכות וניהול מצב משבר

8. הערכות וניהול מצב משבר

מבוא

בעשור החולף אנו עדים להתפתחות האדירה של מרחב הסייבר ולמגוון ההזדמנויות והאפשרויות שהוא מציע. בה בעת, הצמיחה המואצת של טכנולוגיות תקיפה והתגברות התלות בשימוש במערכות ממוחשבות, הובילו להפיכתו של מרחב הסייבר לתווך נרחב לפעילויות עוינות בעצמות גוברת ובהיקפים גדלים. נכסי סייבר, בדגש על תשתיות קריטיות, נעשו מטרה איכותית לתקיפות, מספר המטרות וסוגיהן גדל והולך, ועקב כך גם הסכנה הנשקפת לפרטים, לארגונים, למגזרים (סקטורים) ולמדינות.

לנוכח הפוטנציאל הנפיץ של איום הסייבר והנחיות הממשלה בנושא, מערך הסייבר הלאומי, משרד הבריאות, מוביל מאמץ להגנת מרחב הסייבר האזרחי ולשמירתו כמרחב בטוח. במוקד המאמץ נקטות פעולות להנחיה ולהכוונת הארגונים במשק ובמגזר הבריאות, על בסיס ההבנה כי במקרים רבים הם מושא התקיפה בסייבר ותווך שבו היא עוברת לארגונים אחרים. הפעולות באות לידי ביטוי בין היתר בהגברת המודעות לאיומים, בהנחלת נורמות, ובמתן כלים לניהול ולטיפול בהגנה מפני אירועי סייבר ולצמצום פוטנציאל התממשותם.

החשיבות בהיערכות למצבי משבר בסייבר והנחות יסוד

רוב אירועי הסייבר מקבלים מענה מספק על-ידי צוותי התגובה הטכנולוגיים הארגוניים, ואינם גורמים לנזק משמעותי וארוך טווח.

אולם מתקפות סייבר שהתרחשו ברחבי העולם והנזקים המשמעותיים וארוכי הטווח שגרמו, המחישו כי נדרש לפתח מענה שונה ויכולות מקיפות יותר, מעבר להטמעת טכנולוגיות הגנה ולפעולות להבטחת שגרת הפעילות באיומי סייבר ולהתמודדות עם אירועי סייבר נקודתיים. על כן נדבך משלים למאמץ להגנת מרחב הסייבר האזרחי הוא ההיערכות בסייבר למצבי משבר, שתסייע לצמצם את הסבירות להפיכת אירוע סייבר למשבר סייבר, ואם התממש המשבר תעזור לנהל אותו ביעילות.

בבסיס התפיסה שתי הנחות יסוד המדגישות את החשיבות שההיערכות בסייבר תעשה אל מול הנסיבות השוררות הן במרחב הסייבר והן במרחב הפיזי:

1. משבר סייבר עלול לגרום נזק של ממש ופגיעה ברציפות התפקוד, ולהסלים עד כדי מצב חירום לאומי. כך למשל, בדצמבר 2015 התרחשה מתקפת סייבר נגד רשת החשמל של אוקראינה, ושיבשה את אספקת החשמל למאות אלפי בתי אב למשך כמה שעות. באירוע אחר, במאי, 2017 פגעה קשות מתקפת הסייבר הבין-לאומית "WannaCry" במערך המחשוב של שירות הבריאות הלאומי בבריטניה. בשני האירועים הייתה הפגיעה בנכסי סייבר חיוניים, והעידה על קפיצת המדרגה בתעוזת התוקפים ועל התעצמות איום הסייבר.
2. מצבי חירום שנגרמו ממחולל פיזי שאינו סייבר (לדוגמה: מלחמה, טרור, תופעת טבע וכיו"ב) מגדילים את הסבירות להתרחשות משבר סייבר, מכיוון שיתעצמו בהם מאמצי התוקף בסייבר ובד בבד תגבר התלות בתפקודם התקין של נכסי סייבר חיוניים. כך למשל, במהלך העימות בין גיאורגיה ורוסיה שהחל באוגוסט 2008, ובסמוך אליו, נתקפו בסייבר ושותקו אתרי הממשל והתקשורת של גיאורגיה ורשת הטלפונים קרסה. תקיפת סייבר נוספת גרמה לפיצוץ בצינור המוביל נפט דרך גיאורגיה לאירופה (BTC) שלו תרומה אדירה לכלכלת המדינה. דוגמה אחרת הייתה במבצע "צוק איתן", באוגוסט, 2014 במהלכו נאלצה ישראל להתמודד עם מתקפת סייבר על מטרות צבאיות ואזרחיות, שהתגברה ככל שהפעילות הצבאית הורחבה והועמקה.

הגדרות

ההגדרות והמושגים להלן מתבססים על "מילון מונחי הסייבר" שגובש במערך הסייבר הלאומי, וכן על החלטות ממשלה ומסמכים העוסקים בהיערכות למצבי חירום, ונוסחו בהתאם למסמך זה.

מרחב הסייבר הגלובאלי (Global Cyberspace) - המארג של תשתיות המידע הטכנולוגיות, הכולל את האינטרנט, רשתות התקשורת, מערכות המחשוב וכל המעבדים והבקרים הממוחשבים המשובצים במערכות טכנולוגיות, המשתמשים של כל אלה.

מרחב הסייבר האזרחי של מדינת ישראל (Israel's Civil Cyberspace) - מרחב הסייבר של כלל הגורמים הממלכתיים והפרטיים במדינת ישראל, למעט הגופים המיוחדים (צה"ל, משטרת ישראל, שב"כ, המוסד ומערכת הביטחון).

נכס סייבר (Cyber Asset) - מערכת תקשוב (לרבות חומרה ותוכנה), המשמשת בין היתר לאחסון, ניהול, עיבוד והעברה של מידע, ו/או לתפעול, שליטה ובקרה.

נכס סייבר חיוני (Vital Cyber Asset) - נכס סייבר שתפקודו התקין נדרש לשמירת רציפותו של תהליך ליבה.

תהליך ליבה (Core Process) - תהליך שמבצע ארגון על מנת לממש את יעדיו המרכזיים ו/או יעדים שהוגדרו לו.

שגרת הגנה בסייבר (Cyber Routine) - מצב שבו לא מסתמן נזק לתפקודם התקין של נכסי סייבר חיוניים.

אירוע סייבר (Cyber Incident) – התרחשות המעידה על פגיעה אפשרית בפעילות התקינה של נכס סייבר, שיש יסוד להניח כי היא נובעת מפעילות מכוונת במרחב הסייבר.

משבר סייבר (Cyber Crisis) – מצב שיש בו איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה בו בפועל, אשר עלול לגרום נזק קריטי לשגרת הפעילות ולתדמית, נזק כלכלי ופגיעה בחיי אדם. משבר סייבר נע במדרג רמות חומרה, ובמצב קיצון נגרם נזק ניכר לתהליכי ליבה ולרציפות התפקוד הארגוני/המשקית, והוא עלול להסלים עד כדי מצב חירום לאומי.

מחולל חירום (Emergency Trigger) – מהלך מלחמתי, תופעת טבע, משבר סייבר, פעולת טרור, תקלה וכיו"ב, שרמת הסיכון הטמונה בו מוערכת כעלולה לחולל מצב חירום.

מצב חירום לאומי (National State of Emergency) – מצב קשה ומסוכן ובו סיכון ממשי לפגיעה בציבור ו/או בחוסנה הלאומי של המדינה, המצריך פעילות רב תחומית ברמה הלאומית, לרבות הכרזה על-פי דין (לדוגמה "מצב מיוחד בעורף", "אירוע חירום אזרחי", הכרזת מלחמה).

מצב כוננות לאומי (National State of Alert) – נובע מאפשרות התרחשות מצב חירום שתוצאותיו חוצות ארגונים. העלאת מצב הכוננות הלאומי נועדה להקטין את הסבירות להתרחשות אירוע ואת פוטנציאל הנזק מהתרחשותו. מצב הכוננות הלאומי משפיע בהכרח על מצב הכוננות בסייבר.

מצב כוננות בסייבר (Cyber State of Alert) – קביעה רשמית של רמתה, מהותה והיקפה של ההיערכות הנדרשת בסייבר להתמודדות עם הנסיבות. מצב הכוננות בסייבר עשוי להשפיע על מצב הכוננות הלאומי.

מטרות התפיסה

התפיסה נובעת מההבנה כי ההיערכות וניהול של מצבי משבר מחייבים שילוב כוחות, תיאום ושיתוף פעולה ברמה הלאומית, ורק כך ישיגו את תכליתם. התפיסה מיועדת אפוא למשרדי הממשלה, לרגולטורים ולארגונים ממלכתיים העוסקים בתחום הסייבר, מכיוון שהם מובילים את המאמץ המדינתי המגנתי להכלת התקיפות והשלכותיהן ומנחים ומכוונים את ארגוני המשק.

מטרת התפיסה

לשמש מסמך יסוד המגדיר עקרונות ודרכים לפעולה בנושא היערכות וניהול מצבי משבר במרחב הסייבר

מטרות משנה

1. לייצר שפה משותפת ולהיות בסיס להעמקת שיתוף הפעולה והשיח בסייבר בנושא מצבי משבר, הן בין גורמים מדינתיים והן עם גורמים פרטיים.
2. לשמש כלי מסדר ומכווין לבניית תוכנית סייבר להיערכות ולניהול מצבי משבר, כל ארגון ברמתו, לשמירה על רציפות התפקוד וההמשכיות העסקית, ולסייע בבחינת מידת ההיערכות הארגונית בנושא.
3. לשמש בסיס למערך הסייבר הלאומי ולגורמים נוספים, לפיתוח עזרים עתידיים בנושא היערכות וניהול מצבי משבר בסייבר, דוגמת נהלים ושיטות עבודה, הרחבות מקצועיות ותהליכים. כל אלה יסייעו ביישום התפיסה ובהטמעתה במשק.

מאחר שמשבר סייבר עלול לפגוע קשות בשמו הטוב של הארגון, בנכסיו, בתפקודו או ביכולותיו להשיג את יעדיו המרכזיים (עד כדי סיכון עצם קיומו), ומכיוון שהוא מצריך התייחסות בקשת רחבה של היבטים ארגוניים ועסקיים, ההיערכות למשבר וניהולו הם באחריות הדרג הבכיר בארגון. על כן נכתבה התפיסה למועצות מנהלים (דירקטוריונים) ולהנהלות של ארגונים. התפיסה מיועדת גם לדרג המקצועי, בדגש על מנהלי ההגנה בסייבר והיערכות לחירום ולאחראים לניהול סיכונים, רציפות תפקוד והמשכיות עסקית.

מצבי הכוננות בסייבר ועקרונות לשינוי רמת כוננות

מצבי הכוננות בסייבר מהווים שפה משותפת לשיקוף מידת הדריכות וההיערכות הנדרשת אל מול הנסיבות השוררות במרחב הסייבר האזרחי ובמרחב הפיזי, ולקראת התרחשויות אפשריות בהם. הם ייקבעו כפוף להערכת מצב, שנועדה לסייע בפיתוח הבנת המשמעות של המתרחש על בסיס מידע ועובדות וחשיבה משותפת, ולאחר מכן הגדרת פעולות לביצוע. הכרזה על מצב כוננות סייבר התואם את המציאות ואת גודל האיום, והפעולות שיבוצעו בהתאם, יסייעו להקטין את הסבירות לפגיעה בנכסי חיוניים ולהתפתחות משבר סייבר, ואם כבר קרו - לצמצום הנזק שנגרם. לעומת זאת, אי הכרזה על מצב כוננות תואם תגרום נזק בהיקף רחב, נזק שהיה אפשר למנוע או לכל הפחות לצמצם.

סרגל החומרה: רמזור

כל עוד לא הוכרז אחרת ארגון נמצא במצב של "שגרת הגנה", מבצע פעילות הקשורה בהתנהלותו השוטפת ומתכוון למצבי משבר. במצב זה לא מסתמן נזק לתפקודם התקין של נכסי סייבר חיוניים של הארגון. איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה אפשרית בפעילותו התקינה (גם אם טרם הוכח כי היא נובעת מאירוע סייבר), הם ביטוי להסלמה ומגבירים את הסבירות להתרחשות משבר סייבר. במצב קיצון מתחוללת פגיעה רחבה וממושכת בנכס/סייבר חיוניים של הארגון, וגורמת נזק ניכר לתהליכי ליבה ולרציפות התפקוד הארגוני (המשכיות עסקית).

סרגל החומרה: רמזור

(מה קורה במערכות הארגון בזמן נתון)

מצב	תיאור
שגרת הגנה	ירוק: מצב שבו לא מסתמן נזק לתפקודם התקין של נכסי סייבר חיוניים
ביטוי להחמרה במצב מערכות הארגון	צהוב: איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה אפשרית בפעילותו התקינה
	אדום: פגיעה בנכס/סייבר חיוניים, שבגינה קיימת אפשרות לפגיעה משמעותית ברציפותו של תהליך ליבה
	שחור: פגיעה רחבה וממושכת בנכס/סייבר חיוניים המובילה לנזק משמעותי לתהליכי ליבה ולרציפות התפקוד הארגוני (המשכיות עסקית)

תבחינים לקביעת מצב הכוננות בסייבר: מה קורה במרחב הסייבר ובמרחב הפיזי

מצב הכוננות בסייבר יוגדר על-פי חומרת התבחינים והסבירות להתרחשותם, ובכך יסומן הצורך בהפעלה ובשימוש במשאבים ובכלים, ויוערך היקפם. מכיוון שבמצבי חירום שנגרמו ממחולל שאינו סייבר (לדוגמה מהלך מלחמתי, תופעת טבע, פעולת טרור, תקלה וכיו"ב) סביר שיתגברו מאמצי התוקף בסייבר, ובד בבד עולה חשיבות תפקודם התקין של נכסי סייבר חיוניים התומכים בתהליכי ליבה, מצב הכוננות בסייבר ייקבע לא רק לנוכח המצב במרחב הסייבר, אלא גם לנוכח המצב במרחב הפיזי.

שני דגשים חשובים בהקשר של המתאם (קורלציה) בין התבחינים ובין מצבי הכוננות:

- התממשותו של תבחין מסוים לא מכתיבה בהכרח קביעה של רמת כוננות סייבר ספציפית, אלא התבחינים הם כלי עזר להחלטה על הכוננות כפוף להערכת מצב.
- העלאת הכוננות בסייבר תיתכן גם טרם התרחש אירוע סייבר וכאשר אין ביטוי לפגיעה בנכסי סייבר חיוניים, למשל בעקבות מידע התרעתי או עקב התרחשויות שמגבירות את התלות בהם ואת חשיבות תפקודם התקין. כלומר ארגון יכול להיות במצב כוננות א' או ב' ובזמנית להיות במצב "ירוק" בסרגל החומרה.

להלן פירוט מצבי הכוננות בסייבר והתבחינים לקביעת כל אחד מהם:

מצב שגרת הגנה בסייבר

זהו מצב ברירת המחדל, ובו ההתרחשויות במרחב הסייבר ובמרחב הפיזי לא מצביעות על נזק לתפקודם התקין של נכסי סייבר חיוניים, או על הצורך בהגברת ההגנה עליהם. במצב זה אין ביטוי לתבחינים ברמות כוננות גבוהות יותר. תבחינים במרחב הסייבר: ללא התרחשות, או התרחשות אירועי סייבר שפוגעים בפעילותם התקינה של נכסי סייבר, אולם ללא פגיעה בנכסי סייבר חיוניים. תבחינים במרחב הפיזי: ללא התרחשות או התרעות כלליות לאירוע ביטחוני.

מצב כוננות סייבר א'

מצב כוננות סייבר א' ייקבע כפוף להערכת מצב וכאשר מתממש לפחות אחד מהתבחינים האלה:

תבחינים במרחב הסייבר : התרחשות אירוע סייבר שבו מסתמנת פגיעה אפשרית בתפקודו התקיין של נכס סייבר חיוני, קבלת מידע התרעתי; התרחשות אירוע סייבר מתוזמן (לדוגמה " OpIsrael "), התרחשות אירוע בחו"ל שטרם התפשט לישראל (לדוגמה " WannaCry ") אירוע סייבר המיוחס לישראל.

תבחינים במרחב הפיזי : תקלה תפעולית/טכנית בנכס סייבר חיוני ו/או במתקן המחזיק ב, התרעה לאירוע ביטחוני רחב היקף, התרחשות אירוע ביטחוני חריג (לדוגמה התגברות ירי לעבר ישראל, התרחשות תקיפה המיוחסת לישראל).

העלאת רמת כוונות בצה"ל, התרחשות אירוע חריג שעלולה להיות לו השפעה על מרחב הסייבר.

מצב כוונות סייבר ב'

מצב כוונות סייבר ב' ייקבע כפוף להערכת מצב וכאשר מתממש לפחות אחד מהתבחינים האלה :
תבחינים במרחב הסייבר : מידע התרעתי ממשי להתארגנות לתקיפה, פגיעה בנכס/ סייבר חיוני/ים ובעקבות זאת אפשרות לפגיעה ממשית ברציפותו של תהליך ליבה.
תבחינים במרחב הפיזי : פגיעה פיזית בשירותים חיוניים למשק (לדוגמה : הספקת חשמל, שירותי בריאות) התרחשות אירוע ביטחוני נרחב (לדוגמה :ירי רחב היקף, מבצע צבאי מוגבל)

מצב כוונות סייבר ג'

מצב כוונות סייבר ג' הוא המצב הגבוה ביותר של כוונות בסייבר, וההתרחשויות שבגינן הוכרז עלולות להסלים עד כדי מצב חירום לאומי. מצב כוונות סייבר ג' ייקבע כפוף להערכת מצב וכאשר מתממש לפחות אחד מהתבחינים האלה :
תבחינים במרחב הסייבר : פגיעה רחבה ו/או ממושכת בנכס/ סייבר חיוני/ים, המובילה לנזק ניכר לתהליכי ליבה ולרציפות התפקוד של המשק (לדוגמה :פגיעה חוצת מגזרים).
תבחינים בממד הפיזי : פגיעה פיזית רחבה ו/או ממושכת בשירותים חיוניים למשק, מלחמה או מבצע צבאי רחב היקף, הכרזה על "מצב מיוחד בעורף"/"אירוע חירום אזרחי".

שיגרה	מצב חירום לאומי	כוונות סייבר א'	כוונות סייבר ב'	כוונות סייבר ג'
תבחינים במרחב הפיזי	התרעות כלליות	תקלה תפעולית / טכנית בנכס סייבר חיוני ו/או במתקן המחזיק בו, התרעה לאירוע ביטחוני רחב היקף/חריג או התרחשות בפועל, העלאת רמת כוונות בצה"ל, התרחשות אירוע חריג	פגיעה פיזית בשירותים חיוניים למשק, אירוע ביטחוני נרחב	פגיעה פיזית רחבה ו/או ממושכת בשירותים חיוניים למשק, מלחמה/מבצע צבאי רחב היקף, הכרזה על "מצב מיוחד בעורף"/"אירוע חירום אזרחי"
תבחינים במרחב הסייבר	ללא התרחשות, אירועי סייבר ללא פגיעה בנכסי סייבר חיוני	אירוע סייבר בו מסתמנת פגיעה אפשרית בנכס סייבר חיוני, מידע התרעתי, אירוע מתחמך שניתן, אירוע בחו"ל שטרם התפשט לישראל, אירוע סייבר המיוחס לישראל	מידע התרעתי ממשי להתארגנות לתקיפה, פגיעה בנכס/ סייבר חיוני/ים ואפשרות לפגיעה משמעותית בתהליך ליבה	פגיעה רחבה ו/או ממושכת בנכס/ סייבר חיוני/ים, המובילה לנזק משמעותי לתהליכי ליבה ולשיבוש רציפות התפקוד של המשק

עקרונות לשינוי רמת הכוונות בסייבר

במסגרת כל אחד ממצבי הכוונות יבצע ארגון ברמתו הערכת מצב, יבחן את התבחינים במרחב הסייבר ובמרחב הפיזי, ובהמשך ייבחן הצורך בשינוי הכוונות.

העלאת רמת הכוונות בסייבר

המעבר לרמת כוננות סייבר גבוהה יותר נובע מאפשרות ממשית להסלמה בנסיבות השוררות או הסלמה בפועל, שמחייבת נקיטת פעולות שטרם ננקטו או הגדלה מתונה ככל האפשר בעצמות ובהיקף הפעולות שכבר ננקטו. פעולות אלו נועדו למנוע החמרה נוספת, או לפחות למזער את הנזק שייגרם. העלאת רמת הכוננות תיעשה בהתאם לתבחינים ובהדרגה, אולם לא בהכרח. כך למשל, במצב קיצון ייתכן כי יוכרז מצב כוננות סייבר ג' לפני שהוגדר מצב כוננות אחר.

הורדת רמת הכוננות בסייבר

המעבר לרמת כוננות נמוכה יותר ייעשה אם התבחינים שהובילו לקביעת רמת הכוננות חדלו מלהתקיים. הורדת רמת הכוננות תיעשה בהדרגה, כלומר ברמת כוננות אחת בכל פעם, עד לחזרה למצב שגרת הגנה בסייבר.

צירים להכרזה על מצב הכוננות בסייבר

- לאור המתודולוגיה שהוצגה לעיל, יש שלושה צירים מרכזיים להכרזה על מצב הכוננות במרחב הסייבר האזרחי:
- ברמה הלאומית, ברמת מגזרי המשק וברמת הארגון. לנוכח החשיבות הרבה בשיתוף מידע בסייבר ובהתחשב במהירות שבה מתרחשים אירועי סייבר, חיוני שכל גורם העושה שינוי בכוננות יעדכן על כך את כלל הגורמים הרלוונטיים, לרבות מערך הסייבר הלאומי, הרגולטור וארגונים מונחים (אם יש כאלה). לרוב ייעשה העדכון בחשאיות, וזו תאפשר לבצע "הגנה שקטה", כלומר מענה לאירוע הסייבר תוך כדי הקפדה על הסתרת פעולות המגן, כדי להכיל את המתקפה וללמוד את פעילותו ושיטותיו של התוקף.
 - ברמה הלאומית, על מצב הכוננות בסייבר יכריז ראש מערך הסייבר הלאומי, כמי שעומד בראש הארגון הממלכתי האמון על הגנת מרחב הסייבר האזרחי, או בעל תפקיד שהסמך לכך. כוננות סייבר זו מוכרזת בעקבות איום או התרחשות העלולים להסלים עד כדי מצב חירום לאומי. הכוננות בסייבר ברמה הלאומית מחייבת את כלל מגזרי המשק. מגזר יכול להגדיר לעצמו רמת כוננות סייבר גבוהה מזו שהוגדרה ברמה הלאומית, אולם לא נמוכה ממנה. מכיוון שבנקודת זמן נתונה מגזרים וארגונים עשויים להיות מושפעים מתבחינים בצורה שונה, וכן להפיק מהערכת המצב משמעויות שונות, פרט לרמה הלאומית יש עוד שני צירים להגדרת מצב הכוננות בסייבר, המבטאים סקטוריות ודיפרנציאליות אפשריות.
 - ברמת המגזר, על מצב הכוננות בסייבר יכריז מנכ"ל המשרד הממשלתי/הגורם הרגולטורי הרלוונטי או בעל התפקיד שהסמך לכך, בתיאום עם מערך הסייבר הלאומי או בעקבות המלצתו. ההכרזה מחייבת את כלל ארגוני המשק שבאחריות המגזר, או לחלופין ארגונים ספציפיים שהוגדרו נדרשים לכוננות. הכרזה על מצב כוננות סייבר במגזר מסוים אינה מחייבת מגזרים אחרים, אולם היא מסמנת נסיבות השוררות במרחב שאליו חשוך להתייחס.
 - ברמת הארגון, על מצב הכוננות בסייבר יכריז מנכ"ל הארגון או בעל התפקיד שהסמך לכך, בתיאום עם יחידת הסייבר המגזרית ו/או הגורם הרגולטורי, או בעקבות המלצתו/הנחייתו. ארגון יכול להגדיר לעצמו רמת כוננות גבוהה מזו שהוגדרה במגזר שאליו הוא שייך, אולם לא נמוכה ממנה.



היערכות למצבי משבר : ארגון כלים

לנוכח כל אחד ממצבי הכוננות בסייבר שתוארו לעיל, ינקוט כל ארגון ברמתו פעולות שיסייעו להקטין את הסבירות להתפתחות משבר סייבר, או לנהלו באופן שיפחית ככל הניתן את נזקיו והשלכותיו אם כבר התרחש. מדובר במימוש, לעיתים בפרק זמן קצר, של פעולות שבשגרת הגנה בסייבר מבוצעות באופן מצומצם, או שאינן מבוצעות כלל. על כן ככל שרמת הכוננות גבוהה יותר, יידרשו פעולות בעצימות ובהיקפים גדולים יותר כדי שארגון יוכל לבצע את הפעולות הנדרשות בזמן ניהול משבר, עליו להיערך אליהן כבר בשלב שגרת ההגנה. פעולות שלא יוכנו בעוד מועד לא יהיה אפשר לבצע בזמן משבר, או יהיה אפשר לבצען חלקית, באיחור ולא באופן מיטבי. לשם כך, נדבך משמעותי בהיערכות בסייבר למצבי משבר הוא בנייה מראש של "ארגון הכלים".

מאחר שמשבר סייבר אינו סוגיה טכנולוגית גרידא, ארגון הכלים שם דגש לא רק על משאבים טכנולוגיים, אלא גם על המרכיב האנושי ושיפור מיומנותיו ועל הטמעת ידע. כל אלה הם "מכילי כוח" בעבור הארגון. בכמה מהמרכיבים נעשה שימוש גם בשגרה (לדוגמה : הטמעת מערכות טכנולוגיות והדרכה ותרגול), ואחרים מופעלים רק לקראת התרחשות משבר, או בזמן התרחשותו בפועל (לדוגמה : ביצוע פעולות במערכות הממוחשבות והפעלת צוות לניהול משבר). כל ארגון אחראי על הכנת ארגון כלים משלו, לנוכח הערכת הסיכונים שביצע, איום ותרשיש הייחוס כלפיו בסייבר ובהתחשב בצרכיו ובמשאביו. הרכבו של ארגון הכלים ייקבע גם בעקבות היעדים ורמות השירות שנקבעו במשרדי הממשלה, המתייחסים למימוש חלקם באחריות המדינית להבטחת קיומם התקין של יעדי השירות הלאומיים. מכאן, הרגולטורים חשובים מאוד בהגדרת רמת רציפות התפקוד הנדרשת מהארגונים שבאחריותם, ולאורה יבנו הארגונים את ארגון הכלים, יקצו לו תקציב ייעודי וכן תקציב זמין נוסף לחירום, וישלבו אותו בתוכנית העבודה. את ארגון הכלים מומלץ לבנות תוך התייחסות לחמישה מכילי כוח : ידע מקצועי, כוח אדם, טכנולוגיות ואמצעים, הסתייעות בגורמים חיצוניים, הכשרה ותרגול. מאחר שהתפיסה מיועדת גם לארגונים ומוסדות ממלכתיים וגם לארגונים ציבוריים ופרטיים, כל ארגון יכול להיעזר בדוגמאות המפורטות להלן ולייצר לעצמו את ההתאמות הנדרשות.

ידע מקצועי

- א. הטמעת התפיסה המובאת במסמך זה, כמסגרת לשפה משותפת ולהעמקת שיתוף הפעולה והשיח, וככלי לבניית תוכנית סייבר להיערכות ולניהול מצבי משבר. תוכנית זו יכולה להיות פרק בתוכנית החירום הארגונית, או מסמך נפרד, ומומלץ שתיכתב בסיוע משרד הבריאות/מערך הסייבר או הגורם המנחה, ותאושר על-ידי הנהלת הארגון. ראוי לתקף ולעדכן את התוכנית אחת לשנה, ולרענן אותה עם העלאת הכוננות.
- ב. הטמעת תורת ההגנה בסייבר לארגון (תוה"ג), שפותחה במערך הסייבר הלאומי כדי למזער את סיכוני הסייבר של ארגונים במשק הישראלי. התוה"ג מגדירה מתודה סדורה שבאמצעותה כל ארגון יכול להכיר את הסיכונים הרלוונטיים לו, לגבש מענה הגנתי ולממש תוכנית להפחתת הסיכונים בהתאם. את התוה"ג וכן הרחבות מקצועיות בתחום הגנת הסייבר אפשר למצוא באתר האינטרנט של מערך הסייבר הלאומי.
- ג. הסתייעות בתורות, נהלים ושיטות עבודה מומלצות (Best Practices) בסייבר לארגון, שנכתבו על-ידי מערך הסייבר הלאומי, רגולטור רלוונטי או גורם מנחה מקובל בעולם (למשל מכוני תקנים), בדגש על היערכות וניהול מצבי משבר.

כוח אדם

- הגורם האנושי הוא חלק אינטגרלי בהיערכות ובניהול משבר סייבר, ולמצבי משבר יש השפעה על מצבת כוח האדם, בגלל הצורך לפעול בעצימות ובהיקפים גדולים יותר מבשגרה, או בעקבות גיוס מילואים והיעדרות עובדים. על כן נדרש להתייחס להפעלת כוח האדם במצבי משבר, להגדיר בעלי תפקיד חיוניים ותחומי אחריות, לבנות תוכנית לגיבוי ולתגבור כוח אדם חיוני בכל דרגי העבודה ולבחון דרכים ושיטות עבודה לתפקוד עם כוח אדם מצומצם.
- א. הקמת צוות היערכות וניהול משבר : מכיוון שהנהלת הארגון מחזיקה באחריות הכוללת להיערכות בסייבר למצבי משבר, והיא תנהל את המשבר אם יתממש, מומלץ שבראש הצוות יעמוד מנכ"ל הארגון או סגנו. משבר סייבר אינו עניין טכנולוגי גרידא, ולכן נוסף על מנהל אבטחת המידע והסייבר, רצוי שצוות ההיערכות וניהול המשבר יכלול גורמים בדרגה ניהולית בכירה, שמכירים את תהליכי העבודה בארגון זמן רב ומגיעים מתחומי ידע שונים (למשל סמנכ"ל תפעול, סמנכ"ל כספים, יועץ משפטי, מנהל הרכש והלוגיסטיקה, אחראי דוברות, קצין ביטחון). בזמן שגרה אחראי הצוות להיערכות, ובזמן משבר לניהולו על כל היבטיו : ריכוז תמונת מצב וביצוע הערכת מצב, הכרזה על מצב הכוננות ושינוי רמת הכוננות, ביצוע פעולות לנוכח מצב הכוננות, עבודה מול גורמים בתוך הארגון ומחוץ לו, ולבסוף התאוששות, חזרה למצב שגרה והפקת לקחים והטמעתם.
 - ב. הקמת צוות תגובה טכנולוגי : CSIRT צוות מקצועי שיעודו מניעה, זיהוי, התמודדות וטיפול באירוע סייבר והתאוששות מנזקיו. צוות זה כולל גורמי אבטחת מידע וסייבר וגורמי IT והוא יכול להיות מורכב מעובדי הארגון או ממומחי חוץ שבהם הארגון בוחר להסתייע. בעת משבר ידווח ישירות לצוות ההיערכות וניהול המשבר ויעבוד בהתייעצות ובתיאום עם נציגי יחידות אחרות בארגון ומחוץ לו.
 - ג. הצבות כוח אדם בחירום : על הארגון למפות את מצבת כוח האדם, את יכולותיו ואת כישוריו, ולבנות תמונת פערים בכוח אדם ובמיומנויות שלהן הוא זקוק להמשך רציפות תפקוד גם בזמן משבר. התהליך יסייע לארגון ליצור הצבות כוח אדם בחירום, כלומר שהתפקיד של חלק מהעובדים יהיה שונה בזמן משבר מהתפקיד שהם

- ממלאים בשגרה, ולסמן מקורות לתגבור (ויסות פנימי או הסתייעות בגורמים חוץ-ארגוניים). לבצוע מיטבי נדרש להכשיר ולתרגל את העובדים לנושא עוד בזמן שגרה.
- ד. הגדרת הארגון "מפעל חיוני": קבלת אישור "מפעל חיוני" מאפשרת בין היתר שני כלים חשובים להתמודדות עם מצבי משבר בהקשר של כוח אדם
1. "ריתוק משקי" של עובדים החיוניים להבטחת רציפות התפקוד של הארגון (לדוגמה גורמי אבטחת מידע וסייבר). עובד חייב שירות ביטחון, שאושר לריתוק משקי, יבצע בחירום את עבודתו במסגרת המפעל החיוני שאליו הוא שייך ולא ייקרא לשירות ביטחוני.
 2. איתור, הגדרה ואישור "מגויסי חוץ", שהם מי שאינם עובדים בארגון, ונקראים לעבוד בו בזמן משבר כמקור תגבור. חשוב לבסס את יחסי העבודה עם מגויסי החוץ עוד בשגרה.
 - ה. גיבוש עתודת מומחי סייבר: ארגון יכול לגבש עתודת מתנדבים המומחים במגוון תחומים בעולם הסייבר, ואלה יסייעו לארגון בשגרה ובזמן משבר, הן כצוות חשיבה וסיעור מוחות והן למתן פתרונות טכנולוגיים וניהוליים

טכנולוגיות ואמצעים

- על הארגון להצטייד בטכנולוגיות ובאמצעים שיסייעו לו להעלות את רמת ההגנה בסייבר, לחזק את יכולותיו לזהות תקיפה ולתת לה מענה, לנהל את המשבר ובה בעת לשמר תהליכי רציפות תפקוד והמשכיות עסקית.
- א. מערכות
 1. הטמעת טכנולוגיות הגנה (הזדהות, הצפנה, מניעת קוד עיון וכיו"ב)
 2. תשתיות תיעוד וניטור פעילויות במערכות לשם זיהוי אירועי סייבר ולטובת תגובה מהירה וצמצום הנזק (לדוגמה: הגדרת פעולות רצויות לשמירה בקובצי ה-LOG והטמעת מערכות SIEM)
 3. טכנולוגיות שיטוי, הטעיה וזיהוי וחקירה של תוקפים (לדוגמה "מלכודות דבש" Honeypots ו"ארגז חול" Sandbox)
 4. הטמעת מערכות גיבוי מידע ואחזור נתונים לטובת התאוששות מהירה, מערכות לתיעוד ולניהול אירועי משבר ולתחקור בסיומו (יומן מבצעים).
 5. קשר ישיר עם מערכת הסייבר של משרד הבריאות.
 6. את כלל המערכות הטכנולוגיות יש לעדכן עדכון שוטף, או לפי הנחיית הרגולטור/הגורם המנחה.
 - ב. אמצעים פיזיים: הקמת אתר חלופי DR מופרד ומרוחק פיזית מהאתר הראשי ועומד ברמת אבטחה גבוהה, באופן שיקטין את הסבירות ששני האתרים ייפגעו בו-זמנית ויאפשר גיבוי ושחזור מידע, הטמעת נהלים ובקורות כניסה למתקנים של הארגון, כדי למנוע חדירה לסביבת הסייבר באמצעים פיזיים.
 - ג. אמצעים לוגיסטיים: הצטיידות באמצעים לוגיסטיים ומנהלתיים שיסייעו לעבודה בזמן משבר (עבודה מרוחק, כלכלת עובדים, הסעות וכיו"ב) הצטיידות באמצעי מיגון פיזיים הנדרשים בזמן מצבי חירום ממחולל שאינו סייבר, בדיקה תקופתית של כשירות התשתיות והאמצעים.

הסתייעות בגורמים חיצוניים

- יש כיום גורמים מקצועיים רבים שיכולים לסייע בסייבר לארגון, הן במצב שגרה לטובת ההיערכות והן במצבי משבר.
- א. המגזר הציבורי: הסתייעות בכלים מקצועיים של מערך הסייבר הלאומי והרגולטורים המנחים את הארגון לדוגמה: ידע מקצועי, מענה לאירועי סייבר, הכשרות, הדרכות, תרגילים וביקורות ועוד.
 - ב. המגזר הפרטי: אם ארגון בוחר להסתייע בשירות של חברות פרטיות (לדוגמה: ייעוץ בנושא ניהול סיכונים, מענה לאירועי סייבר וניהול משבר סייבר, ביטוח וכיו"ב), הכרחי שבהסכמי השירות הנחתמים עימן תתווסף התחייבות שהמענה יינתן גם בזמן משבר SLA. חשוב שהגורם החיצוני שנותן שירות יכיר את תוכנית ההיערכות של הארגון למצבי משבר, ובמידת האפשר ישתתף בתרגילים הקשורים בה ויעודכן בעת התרחשות אירוע חריג. נוסף על כך ארגון יכול להסתייע בידע ובכלים המצויים בארגונים מקבילים בעולם.
 - ג. הסכמי שיתוף פעולה: ארגון יכול לפעול ליצירת הסכמים, בכתב או בעל-פה, עם ארגונים רלוונטיים אחרים (לדוגמה מאותו המגזר) לטובת סיוע הדדי ושיתופי פעולה בסייבר בשגרה ובדגש על מצבי משבר.

הכשרה ותרגול

- תוקפים רבים בסייבר מצליחים להתגבר על אמצעי ההגנה באמצעות שימוש בהנדסה חברתית (Social Engineering). כך הם מנצלים את הגורם האנושי, למשל דרך דיוג Phishing שבו התוקף מתחזה לגורם אחר. כאשר מתרחשים אירועי סייבר, הגורם האנושי הוא מרכיב אינטגרלי במתן המענה. על כן להכשרה ולתרגול יש חשיבות רבה בהיערכות בסייבר למצבי משבר ולהעלאת חוסנו של הארגון.
- א. הכשרות והדרכות: יינתנו לבעלי תפקידים בארגון, הן בנושאים כלליים לטובת העלאת המודעות ויצירת תרבות ארגונית לאיום הסייבר, והן בנושאים מוגדרים לטובת בנייה ושמירת כשירות. זאת כדי שהעובדים יבצעו את תפקידם בצורה מיטבית בשגרה ובחירום (בדגש על עובדים שמבצעים בחירום תפקיד שונה מהתפקיד שהם מבצעים בשגרה, בהתאם להצבות החירום). בדרג ההנהלה חשוב לכלול הכשרות והדרכות לחיזוק מיומנויות רכות, דוגמת יכולת קבלת החלטות, עבודת צוות והתנהלות תקשורתית.

ב. תרגילים וביקורות: יכולים להיות בהיקפים שונים (רמת פרט, כלל הארגון, מגזר שלם) ובשיטות שונות (תרגיל שולחני, אופרטיבי, סימולטור, ביקורת גלויה/סמויה, מבדקי חדירות). על התרגילים והביקורות להיות חלק מתוכנית העבודה השנתית, להקיף מספר רב ככל שניתן של בעלי תפקידים, כולל רמת ההנהלה וצוות ניהול המשבר, ולהתבצע בשיתוף גורמי חוץ שעימם יש לארגון ממשקים. נדרש שהתרגילים והביקורות יאתגרו ויביאו לידי ביטוי את תוכנית הסייבר להיערכות ולניהול מצבי משבר של הארגון, והמסקנות שיעלו בעקבותיהם יישמשו להפקת לקחים ולעדכונים נדרשים בתוכנית. במסגרת ארגז הכלים, מצורף בפרק הנספחים שאלון שנועד לשמש ככלי עבודה ומטרתו להעריך את מידת היערכותו של הארגון למצבי משבר בסייבר ולהציע תובנות הנוגעות לנושאים שנדרש לשפר (ראה נספח ג').



ניהול משבר סייבר

9. ניהול משבר סייבר

"מחזור החיים" של משבר סייבר

לכל משבר סייבר יש "מחזור חיים" ייחודי לו. יש משברים "מתפרצים" אשר מתרחשים בפתאומיות והשלכותיהם ניכרות מייד, ואילו משברים אחרים נבנים בהדרגה (אולם גם אם מסתמנת הסלמה הדרגתית ייתכן שבהמשך תגיע התפרצות). המידע הראשוני יכול להגיע מכמה מקורות: מערכות ניטור ובקרה, סימנים מעידים בנתונים או במידע עסקי, דיווח מגורם פנימי, או עדכון של גורם חיצוני (דוגמת מערך הסייבר הלאומי או רגולטור/גורם מנחה). לנוכח המהירות הרבה שבה משבר סייבר יכול להתפרץ והסיכון בהתרחבותו לארגונים ולמגזרים נוספים, על כל גורם המאתר חשד לאירוע סייבר, או מקבל דיווח בנושא, לעדכן מיידית את כלל הגורמים הרלוונטיים בארגון ומחוץ לו. את מחזור החיים של משבר סייבר, כשהליך שבו כמה שלבים, ניתן לשרטט כך:

זיהוי: גילוי כי מדובר בהתרחשות חריגה מבחינת השפעותיה על נכסי הסייבר החיוניים של הארגון ועל תהליכי הליבה שלו (איום או פגיעה בפועל), וגיבוש מהיר ככל האפשר של דפוס המענה הדרוש.

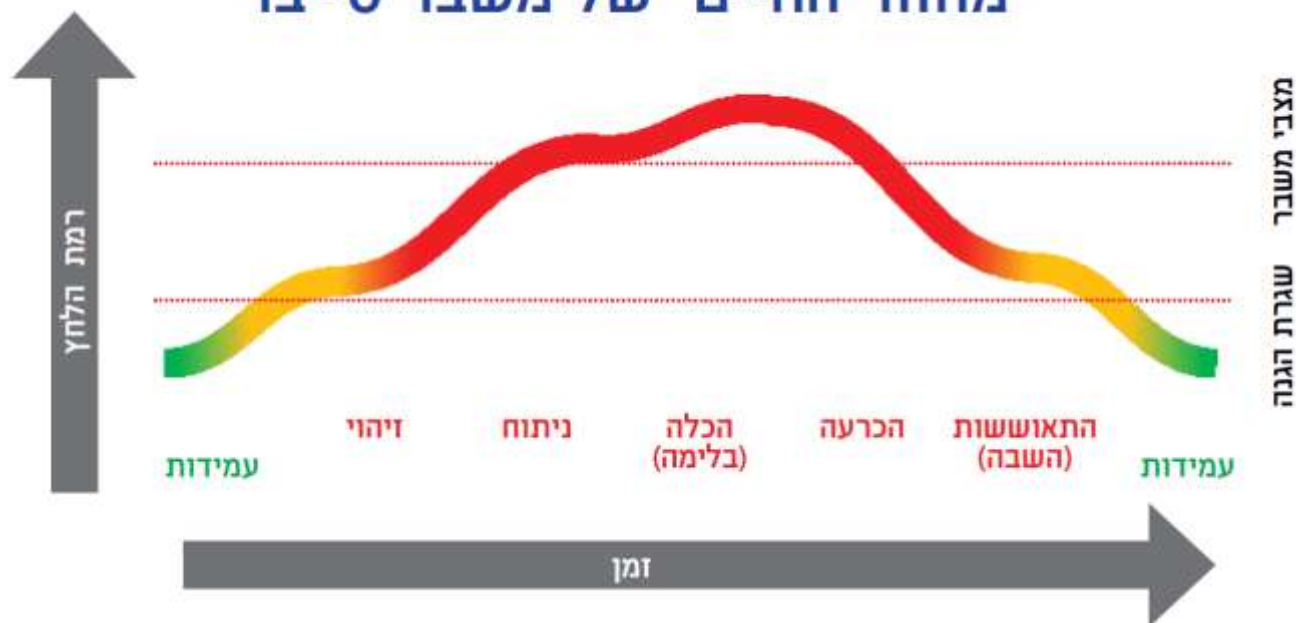
ניתוח: בירור מקיף ומעמיק של אופי ההתרחשות ובדיקה שאין פרצות נוספות, ובחינת השלכותיה על תפקוד הארגון מעבר להיבט הטכנולוגי.

הכלה (בלימה): חסימת התקיפה (השגת שליטה ראשונית) והתרחבותה לנכסי סייבר נוספים, ועצירת החמרת הנזק שהיא גורמת (המשכיות עסקית, תדמית, נזק כלכלי). עבודה לפי תוכנית ניהול משבר הארגונית.

הכרעה: נטרול רכיבי הפגיעה תוך כדי ניסיון לבטל או למזער ככל האפשר את הנזק שכבר נגרם.

התאוששות (השבה): חזרה מבוקרת לפעילות תקינה, הכרזה על סיום המשבר (מצב של שגרת הגנה בסייבר), תחקיר והפקת לקחים, והגדרת צעדים ליישום.

"מחזור החיים" של משבר סייבר



תפיסת הניהול של משבר סייבר: צוות ניהול המשבר

אפשר למנות כמה יעדים (תכליות) מרכזיים בניהול משבר סייבר:

למזער את הפגיעה התפקודית, העסקית-כלכלית והתדמיתית, לשמור על נכסי הסייבר החיוניים ועל נכסי מידע רגיש, להמשיך ולספק שירותים מיטביים גם בעת משבר, בדגש על שירותים חיוניים, לחזק את אמונם של בעלי עניין על-ידי הוכחת יכולת התמודדות טובה במצבי משבר, לסיים במהירות האפשרית את הטיפול בגורמי המשבר, להתאושש ולחזור לשגרה. נדרש שניהול משבר סייבר יתייחס לאיומים ולאתגרים בשני רבדים:

א. התמודדות עם גורמי המשבר: ההיבטים הטכנולוגיים הקשורים למתקפת הסייבר והשפעתם הישירה על נכסי הסייבר (בהובלת צוות התגובה הטכנולוגי). כפי שהוסבר בסעיף כוח אדם בפרק "היערכות למצבי משבר".

ב. התמודדות עם השלכות המשבר: להבדיל מאירוע סייבר, משבר סייבר דורש התייחסות מעבר לגבולות הטכנולוגיים, ויש לו השלכות בהיבט הפנים-ארגוני וחחוץ-ארגוני, דוגמת רציפות התפקוד של הארגון, השלכות עסקיות-כלכליות והשלכות תדמיתיות. ההתמודדות בשני הרבדים הללו מצריכה כלים שונים והיא גם באחריותם של גורמים ארגוניים שונים. עם זאת חשוב מאוד הסנכרון בטיפול בשני הרבדים, שכן יש זיקה ביניהם, ולהחלטות ברובד האחד עשויות להיות השלכות ברובד האחר. על כן, ומפאת השלכותיו החמורות של משבר הסייבר על תדמיתו של הארגון, נכסיו, תפקודו ו/או יכולותיו לממש את יעדיו המרכזיים, על משבר הסייבר להיות מנוהל על-ידי צוות ניהול משבר המורכב מדרג בכיר בהנהלת הארגון. צוות זה מנחה ומכוון

את פעילות הגורמים הרלוונטיים האחרים בארגון (בין היתר את צוות התגובה הטכנולוגי), וכן מנהל קשר עם בעלי העניין החיצוניים, שחשיבותם רבה בעת משבר.

תפיסת הניהול של משבר סייבר



כשמאגדים יחד את המרכיבים שתוארו לעיל, המתווה הכולל של ניהול משבר סייבר נראה כך :



פעולות בניהול משבר סייבר

בשלב זה של הפרק יפורטו פעולות לביצוע בניהול משבר סייבר. לנוחות הקורא, הפעולות מחולקות לפי מצבי הכוננות בסייבר. אין זה אומר שהכרזה על מצב כוננות מכתבה בהכרח מימוש של פעולות ספציפיות, אלא שמצבי הכוננות הם כלי עזר להחלטה על פעולות. על כן במצב כוננות סייבר נתון יבצעו ארגונים פעולות שונות זה מזה, לנוכח הסכנה הנשקפת להם והערכת המצב ובהתחשב בכלים ובמשאבים העומדים לרשותם או בהנחיית הרגולטור מאחר התפיסה מיועדת הן לארגונים ומוסדות ממלכתיים והן לארגונים ציבוריים ופרטיים, כל ארגון יכול להיעזר בדוגמאות מפורטות להלן ולליצר לעצמו את ההתאמות הנדרשות. כפי שהוסבר בפרק הקודם, פעולות שלא יוכנו בעוד מועד לא יתאפשר לממשן בזמן משבר, או יתאפשר לממשן חלקית ולא באופן מיטבי. טרם החלטה על פעולה נדרש להביא בחשבון את השלכותיה האפשריות להלן פירוט הפעולות האפשריות בכל אחד ממצבי הכוננות בסייבר, בחלוקה לפעולות פנים-ארגוניות וחוף-ארגוניות.

מצב שגרת הגנה בסייבר

במצב שגרת הגנה בסייבר, פרט לפעולות הנעשות להבטחת שגרת הפעילות באיומי סייבר ולהתמודדות עם אירועי סייבר נקודתיים, נערך הארגון לפעולות שינקוט במצבי משבר. כלומר, הארגון עושה פעילות שוטפת תוך בניית יכולות והעלאת כשירות, ושמירה על גמישות לקראת מעבר למצב כוננות סייבר גבוה יותר, כפי שפורט בפרק הקודם שעסק בארגז הכלים.

מצב כוננות סייבר א'

פעולות אפשריות במצב כוננות סייבר א' :

פנים-ארגוני : הגברת עירנות, עדכון כלל הגורמים הרלוונטיים בתוך הארגון בהעלאת הכוננות והגברת זמינות, ויסות ו/או תגבור כוח אדם לריכוז מאמץ, איש/תגבור מרכז השליטה הארגוני, הערכות מצב שוטפות, עדכון תמונת המצב ומאמץ המודיעין, הכנת הודעות לתקשורת ("נצורות"), רענון תוכנית הסייבר לניהול משבר וידידא מוכנות למעבר למצב כוננות גבוה יותר, נקיטת פעולות נדרשות במערכות הממוחשבות (לדוגמה : בדיקת תקינות, עדכוני אבטחה, הגברת פעילות הניטור במערכות ההגנה השונות, גיבויים ועוד), ביצוע פעולות נדרשות הקשורות באבטחה הפיזית

(לדוגמה הגברת עירנות לאירועים חריגים בארגון ודיווח מידי, החמרת נוהלי הכניסה לארגון ובדיקת תקינות אמצעי האבטחה ועוד).

חוץ-ארגוני: עדכון הרגולטור/הגורם המנחה, מערך הסייבר הלאומי, שותפים וכלל הגורמים הרלוונטיים במצב הכוננות ובתמונת המצב בסייבר, לצורך שיתוף מידע וידע וקבלת הנחיות והמלצות לפעולה, מתן הנחיות לגורמים שהארגון מנחה, איסוף מידע מגורמים פנימיים וחיצוניים רלוונטיים, עדכון ובדיקת קשר עם נותני שירותים שהארגון קשור עימם.

מצב כוננות סייבר ב'

במצב כוננות סייבר ב' יבוצעו כל הפעולות שביצע הארגון במצב כוננות סייבר א', וכן :
פנים-ארגוני: הפעלה ותגבור צוותים מקצועיים רלוונטיים (לדוגמה צוותי תגובה טכנולוגיים, צוות ניהול משבר), איש מלא של מרכז השליטה ועבודה לפי שיעון פעילות ארגוני, מוכנות להפעלת תוכנית הצבות כוח אדם חירום, פעילות דוברות, ביצוע פעולות נדרשות במערכות הממוחשבות (לדוגמה : הפסקת הכנסת קבצים, הקפאת תצורה ובחינת הצורך בניתוק קישורים לא הכרחיים עם מערכות משיקות, צמצום פעילות למינימום, איתור רכיבים שהותקפו, בידוד הסגמנט שבו זוהתה התקיפה, חסימת התקיפה, בדיקה כי אין פרצות נוספות, תיעוד), חלוקת אמצעי מיגון והעלאת המוכנות למעבר למתקן חלופי ובדיקת המערכות הנמצאות בו (רלוונטי כאשר ההסלמה קשורה במחולל חירום פיזי, ואם קיים) נקיטת פעולות נדרשות הקשורות באבטחה הפיזית (לדוגמה : סריקות עיתיות, עיבוי אבטחה והגבלת כניסת מבקרים רק במקרים דחופים ובליווי), צמצום פעולות שאינן חיוניות.
חוץ-ארגוני: מימוש התקשרויות עם גורמים מקצועיים חיצוניים לקבלת סיוע (לדוגמה חברות אבטחת מידע וסייבר, וניהול משבר) מימוש הסכמים שנחתמו לשיתוף פעולה עם ארגונים מקבילים, מתן התראה להגברת זמינות למגויסי החוץ העומדים לרשות הארגון, הפעלת עתודת מומחים בסייבר.

מצב כוננות סייבר ג'

במצב כוננות סייבר ג' יבוצעו הפעולות שנקט הארגון במצב כוננות סייבר ב', וכן :
פנים-ארגוני: הפעלת תוכנית הצבות כוח אדם בחירום, הפעלת ריתוק משקי (בארגונים שאושרו כ"מפעל חיוני"), איש מתקן חלופי, ביצוע פעולות נדרשות במערכות הממוחשבות (לדוגמה ניתוק כלל הקישורים החיצוניים למערכת), ביצוע פעולות נדרשות הקשורות באבטחה הפיזית (לדוגמה איסור כניסת מבקרים).
חוץ-ארגוני: עבודה לפי שיעון פעילות לאומי, הפעלת מגויסי חוץ.

פעולות אפשריות לנוכח כל אחד ממצבי הכוננות (דוגמה)

מצב כוננות סייבר א'		מצב כוננות סייבר ב'		מצב כוננות סייבר ג'	
עדכון כלל הגורמים הרלוונטיים	ויסות ו/או תגבור כוח אדם	הפעלת צוותים מקצועיים פנים ארגוניים	איוש מלא של מרכז השליטה הארגוני	עבודה בהתאם לשעון פעילות לאומי	הפעלת תוכנית הצבות כוח אדם בחירום
תגבור מרכז השליטה הארגוני	ביצוע הערכות מצב שוטפות	עבודה לפי שעון פעילות	מוכנות להפעלת תוכנית הצבות כוח אדם בחירום	הפעלת ריתוק משקי	הפעלת מגויסי חוץ
עדכון תמונת מצב ומאמץ המודיעין	הכנת הודעות "נצורות" לתקשורת	פעילות דוברות	מיגון ולוגיסטיקה	איוש מתקן חלופי	מיגון ולוגיסטיקה
רענון ועבודה לפי תוכנית ההיערכות בסייבר למשברים	יידוא מוכנות למעבר למצב כוננות גבוה יותר	מימוש התקשרויות עם נותני שירותים	מימוש הסכמי שיתוף פעולה עם ארגונים מקבילים	ביצוע פעולות במערכות הממוחשבות	ביצוע פעולות להגברת האבטחה הפיזית
ביצוע פעולות במערכות הממוחשבות	ביצוע פעולות להגברת האבטחה הפיזית	ביצוע פעולות במערכות הממוחשבות	ביצוע פעולות להגברת האבטחה הפיזית		

התאוששות: חזרה למצב שגרת הגנה בסייבר

- על חזרה למצב שגרת הגנה בסייבר יכריז מנכ"ל הארגון, או בעל התפקיד שהסמיך לכך (למשל ראש צוות ניהול המשבר). עם ההכרזה על חזרה למצב של שגרת הגנה בסייבר יש לעדכן את כל הגורמים הרלוונטיים בתוך הארגון ומחוץ לו. על הארגון להגדיר יעדי התאוששות, להעריך את הנזקים שנגרמו ולפעול לצמצמם, ולהפיק לקחים מהתנהלותו במשבר בהקדם, כדי לשפר את איכות המענה העתידי למצבי משבר. חשוב לדון בין היתר בנושאים האלה:
- סקירה כרונולוגית של האירועים והפעולות שבוצעו, החל בהחלטה על העלאת הכוננות בסייבר וכלה בחזרה לשגרת הגנה.
 - הערכת התנהלות הארגון ויעילות הפעולות שננקטו בתגובה לאירועים בכלל התחומים (טכנולוגי, ניהולי, לוגיסטי, דוברות ועוד) כולל נושא ההסתייעות ושיתוף הפעולה עם גורמים חיצוניים.
 - הערכת יעילות ההכנות שבוצעו בשגרה ("ארגז הכלים").
 - זיהוי נושאים לשיפור ולשימור והערכת צרכים עתידיים. גיבוש לקחים, הטמעתם והפצתם לבעלי העניין בתוך הארגון ומחוץ לו.
 - תיקוף תוכנית ההיערכות בסייבר למצבי משבר.

מודעות עובדים

10. מודעות עובדים

רקע

כחלק ממערך הגנת הסייבר במסגרת ארגוני הבריאות בישראל יש לפעול ליישום מיטבי של הדרכת עובדים והעלאת המודעות. מקומו של הגורם האנושי באבטחת המידע והגנת הסייבר של ארגון הינו מרכזי. בכוחו של הפרט להתריע על אירוע סייבר ובכך לצמצם נזקים פוטנציאליים כתוצאה ממנו, אך בכוחו גם לחולל אירוע, במזיד או בשוגג. עובדי הארגון עלולים להיות גורם משמעותי באמצעותו ניתן יהיה לחדור לארגון, תוך שימוש בהנדסה חברתית ודיוג, התחזות לביצוע פעולות לא מורשות, גניבת הרשאות והונאה. תכנית הדרכה והעלאת המודעות מהווה נדבך חשוב בצמצום הסיכון של ניצול החולשה האנושית במטרה לפגוע בארגון. תקני אבטחת המידע והגנת הסייבר המחייבים את ארגוני הבריאות בישראל, לרבות תקן ISO-27799, מדגישים את הצורך לביצוע הדרכות כלליות להעלאת מודעות וכן הדרכות ספציפיות לבעלי תפקידים רגישים ונושאי משרה ובכלל זה את הצורך לתרגל באופן שוטף. להבדיל מהדרכה, בה מועבר ידע על ידי הצגתו ונדרש ללמוד ולשנן את החומר, תהליך הגברת המודעות נועד ליצור שינוי התנהגותי באמצעות תכנים המותאמים לאופי הארגון ולדרישות התפקיד. השינוי, בין אם הוא ההתפתחות של יכולות או יצירת הנעה, צריך להיעשות באופן הדרגתי ומבוקר. התכנית המוצגת להלן מתאימה לאופיים המיוחד של ארגוני הבריאות ומסייעת בזיהוי האיומים ודרכי ההתמודדות עמם.

עקרונות יסוד

- תמיכת ההנהלה הבכירה – על התכנית לקבל את תמיכת ההנהלה הבכירה, הן במשרד והן בארגוני הבריאות. זהו תנאי הכרחי להצלחתה. על ההנהלה להדגיש לעובדים את חשיבות הנושא, למדוד את רמת ההשתתפות ויעילות ההדרכה וכן ולהקצות משאבים הולמים לנושא.
- שיתוף גורמי מפתח – על מנת ליצור שפה משותפת והתאמת התכנים לאוכלוסיות השונות, יש לשתף בהובלת התכנית יחידות ארגוניות כגון: הגופים הרפואיים המקצועיים, ניהול סיכונים, משאבי אנוש, יחידות ה-IT, הנדסה, בטחון, ייעוץ משפטי וכדומה.
- התאמה לאוכלוסיות הרלוונטיות – על מנת ליצור תכנית הדרכה אפקטיבית, יש לזהות את אוכלוסיות היעד השונות. מסמך זה מגדיר את קהלי היעד במגזר הבריאות.
 - התכנים צריכים להשתמש במושגים המקובלים אצל קהל היעד;
 - הדוגמאות המוצגות למשתתפים יהיו מעולם התוכן שלהם;
 - הנושאים יותאמו לסוגי התפקיד של המשתתפים;
 - תהליכי העבודה, המשימות, האילוצים והכלים בהם הם עושים שימוש יילקחו בחשבון;
 - ההדרכה תותאם לרמת ההבנה והמיומנות הטכנולוגית של המשתתפים;
- יצירת עניין – יש לשאוף כי כל אחד ממרכיבי התכנית ייצור עניין ומוטיבציה למשתתפים על מנת לסייע בהפנמת המסרים.
- שיתוף פעיל – על התכנית למצוא דרכים מאתגרות אשר יגרמו לקהל היעד להשתתף באופן פעיל.
- מדידה – על מנת לקבל חיווי על אפקטיביות התכנית יש למצוא דרכים לכמת את הצלחתה.

אוכלוסיות היעד

על מנת לעמוד בעקרונות היסוד, הוגדרו אוכלוסיות יעד על פי המאפיינים הבאים:

- רמת האחריות ובכירות בארגון
- מכנה משותף כגון: תפקיד, תהליכי עבודה
- סוג המידע אשר האוכלוסייה חשופה אליו ורגישותו
- רמת הידע הטכנולוגי של האוכלוסייה.

כמו כן, על מנת להתמקד ולשמור על אפקטיביות גבוהה, אוכלוסיות היעד לא הוגדרו על פי המכנה המשותף הנמוך ביותר.

להלן אוכלוסיות היעד:

הנהלה ומנהלים בכירים

מקבלי ההחלטות בארגון נדרשים להוביל את נושא הטיפול באירועי סייבר ולהנחיל את הצורך והדרכים לשמירה על שלמות המידע ועל פרטיותו בקרב המנהלים בדרגי הביניים ובקרב כלל העובדים.

המנהלים עצמם נדרשים להכיר בחובות ובדרכי השמירה על המידע אליו הם נחשפים לרבות מידע רפואי אישי, עסקי ומסחרי.

סגל רפואי

הסגל הרפואי חשוף במהלך עבודתו למידע רפואי, אישי ופרטי. יש לוודא כי הסגל מודע לצורך והדרך להגן על מידע זה. בנוסף, אנשי הסגל הרפואי עושים שימוש במכשור רפואי לאבחון ו/או לטיפול בחולה, דבר המשפיע באופן ישיר על מצבו הרפואי של המטופל. נדרשת מודעות לפגיעות במכשור זה כתוצאה מהתקפות סייבר והדרך לצמצם את הפגיעה כתוצאה מכך.

אנשי טכנולוגיות

באוכלוסייה זו נכללים אנשי מערכות המידע להם השפעה על מערכות המידע, אמינותן וזמינותן; עובדי הנדסה רפואית להם חשיפה למכשור הרפואי, בעלי השפעה על תפקוד המכשור, אמינותו וזמינותו; ומשתמשים/מתפעלים של ציוד בקרה (SCADA) של תשתיות הארגון.

ספקים וקבלנים

אנשי מקצוע בתחומי הפעילות השונים במגזר הבריאות ובמערכות התמך. ביניהם כאלו הנחשפים למידע רגיש של הארגון והמטופלים, מערכות הליבה, המכשור הרפואי והתשתיות. נדרש להתייחס באופן ממוקד לסיכון זה בתהליך ההתקשרות ולדרוש הדרכות מסודרות הן על ידי הספק והן על ידי גורם שלישי וכן לאפשר יכולת בקרה על קיום תהליכים אלה ויעילותם.

כלל העובדים

נדרש תהליך הדרכה והעלאת מודעות לנושא שמירה על המידע בכל שלבי ההעסקה של כל עובד בארגון באשר הוא. על העובדים להכיר את היבטי אבטחת המידע בדרישות החוק בנושא הגנה על המידע והפרטיות, נהלי העבודה של הארגון, צורת הדיווח על אירועים חריגים.

תכנית הדרכה והעלאת המודעות

מרכיבי התכנית

התכנית מורכבת מהרכיבים המפורטים להלן. שימוש בכל אחד מהאמצעים ייבחן על פי יעילותו בהשגת היעדים לשיפור המודעות והתאמת האמצעי לאוכלוסיית היעד:

הדרכה פרונטלית

העברת ידע, הנחיות והוראות לאדם או לקבוצה, ישירות באמצעות מדריך.

- הדרכה כללית המתאימה לכלל העובדים;
- הדרכה פרטנית מותאמת לכל אחת מן האוכלוסיות שאופיינו לעיל.
- לומדה – תוכנת מחשב שמטרתה הקניית ידע ומיומנויות למשתמש בה. מומלץ לעשות שימוש בתוכנה כללית וכן לשקול, בנוסף, פיתוח לומדות ייעודיות לאוכלוסיות השונות.
- "מסע פרסום" (קמפיין) – סדרה של הודעות אשר חולקות רעיון, נושא אחיד ומטרה משותפת (המושג "קמפיין" אומץ מעולם השיווק).
- הכלים באמצעותם ניתן ליישם את מסע הפרסום מגוונים, לדוגמא: שלטים, כרזות, קליפים ועוד. למעשה כל דבר שיביא את הנושא המרכזי למודעות קהל היעד, יחשוף אותו למידע ויניע אותו לפעול בדרך הרצויה.
- תקשורים חודשיים** – הודעות קצרות שמטרתן יצירת עניין. הודעות אלו כוללות נושאים כגון דיווח על אירוע שהתרחש והלקחים ממנו או המלצה מקצועית על דרך התנהגות במצבים משתנים.

תרגילים – דימוי מבויים של מצב או סדרת מצבים אשר המתורגל צריך להגיב להם. ביניהם:

- "דיוג" (פשינג) – הדמיה של תקיפה דרך שליחת דואר אלקטרוני
- הנדסה חברתית – הדמיה של תקיפה העושה שימוש בחולשה אנושית.
- תרגילי הנהלה – הדמיה של רצף אירועי סייבר המוצגים להנהלת הארגון במטרה לתרגל את גורמי ההנהלה בניתוח ותגובה על אירועים באופן מיטבי.
- יחידת הסייבר של מב"ר מנחה לגבי מטרות ודרכי התרגול. כמו כן מסייעת היחידה בביצוע תרגילים תוך הכנת הארגונים להתמודדות עצמאית עם תרגולים אלה.
- תרגול טכנולוגי – הדמיה של תקיפה העושה שימוש בחולשה טכנולוגית. בחינת יכולת הזיהוי, ההגנה, הבידוד, עובדה במערך חירום, יכולת ההתאוששות והחזרה לשגרה.

מדידה, הערכה ודיווח

על מנת לוודא כי הפעילות להעלאת מודעות העובדים היא יעילה, נכונה ומשיגה את המטרה, נדרש כי יבוצעו מדידה, הערכה ורישום של יעילות התוכנית.

ניתן לעשות שימוש באחד או יותר מאמצעי המדידה הבאים, באופן ידני או בכלים טכנולוגיים :

- שאלון ידע לפני ואחרי קיום הדרכה ;
 - מדידת כמות דיווחי האירועים המתקבלים מהעובדים והשוואתם לדיווחים שהתקבלו בתקופה קודמת ;
 - דו"ח סיכום תרגיל וחווה הדעת של המשתתפים וגורמי הבקרה.
 - בתרגיל "דיוג" (פשינג) ניתן לקבל מדדים ע"פ פעולות שהמשתמש ביצע ורמת החשיפה לארגון לדוגמה : פתיחת מייל, כמות לחיצות על קישורים, באם התקיים דיווח לגורמי אבטחת המידע והסייבר הארגוני.
- יש לאסוף נתונים מכל האמור לעיל ולנתחם, על מנת לגבש תמונת מצב ארגונית על רמת המודעות, למדוד את האפקטיביות ומגמות השיפור על פני התקופה ולשפר באופן מתמיד את יעילות התכנית. יש לדווח להנהלת הארגון באופן שוטף על יעילות התוכנית, מימוש יעדיה. במידה והתגלו פערים בתהליך ההדרכה והעלאת המודעות יש לדון עם ההנהלה על דרכי הפעולה.

אחריות

מנהלי בתי חולים, מנהלי מרפאות, מנהלי קופות חולים אחראים להגנה על המידע הרפואי הנוצר ונאגר במוסד ובכלל זה על הדרכה והעלאת המודעות של העובדים.

אחריות מנהלים, על המנהל האחראי לוודא כי קיימת ומיושמת בארגונו תכנית הדרכה ברמה השנתית. ההנהלה הבכירה תאשר מדי שנה את תכנית ההדרכה העדכנית.

תרגולי סייבר - מדריך לתרגול עצמי

11. תרגולי סייבר - מדריך לתרגול עצמי

רקע

תרחישי איום רלוונטיים למגזר הבריאות

- גישה בלתי מורשית לרשומות הרפואיות EMR
- גניבת מידע רפואי - לצורכי מסחר וסחיטה
- שיבוש מידע רפואי - השפעה על המטופל
- פגיעה בתשתיות - השפעה על הרציפות התפקודית
- פגיעה בצידוד רפואי - השבתת שירותים ופגיעה בחיי אדם

מטרות תרגולי סייבר

מטרת התרגיל הינה לשפר את רמת מוכנותם של ארגוני בריאות להתמודדות עם מקרה אמת. כמו כן, התרגיל יסייע להגברת המודעות ושיתוף פעולה בין הגופים בארגון בנוסף יבחן את אפקטיביות ההתמודדות של בית החולים עם ניהול אירוע סייבר, באמצעות:

- הטמעת המודעות לאחריות הנהלת הארגון להגנת הסייבר.
- הערכת מוכנות הארגון להתמודד עם אירועי סייבר ושל יכולתו להכיל אירוע סייבר.
- שיפור של המוכנות של תכנית ההתמודדות עם אירוע סייבר על ידי בחינת הישימות שלה.
- הגברת המודעות לאבטחת הסייבר בארגון והטמעת כללי התנהגות נדרשים.
- הרחבת שיתוף הפעולה בנוגע לאבטחת הסייבר במגזר הבריאות.

רקע למדריך וזכויות יוצרים

המשרד משתף פעולה עם עמיתים בהגנת הסייבר מסמך זה מבוסס על תכנית CyberRX שנעשתה על ידי, DHHS HITRUST וארגונים התנדבותיים כדי לשפר את התקדמות אבטחת הסייבר בתחום תעשיית הבריאות. התכנית נוצרה כתגובה לחששות והאיומים הגוברים על תעשיית הבריאות. כפי שהוכח מתגובות של ארגונים רבים לפרצות אבטחה, אופן התגובה של ארגון לאירועי סייבר חשוב לא פחות מהאופן בו הארגון מגן על עצמו מסיכונים אבטחה.

יתרונות המדריך:

- הערכת מוכנות התגובה של הארגון לתקרית ואת יכולות ניהול משברים בתגובה לאירועי ואיומי סייבר אמתיים ורלוונטיים.
- שיפור התקדמות תכנית אבטחת הסייבר על ידי הפקת לקחים שנלמדו מתרגילי הסימולציה
- הגברת המודעות לאבטחת סייבר ברחבי הארגון הבריאות המתורגל.
- שילוב והדרכת המנהלים באבטחת סייבר.
- הקמת והרחבת שותפויות וקשרים בתעשיית הבריאות כדי להגביר את שיתוף הפעולה לעמידה באתגרים שמציבה אבטחת סייבר.

משתתפים בתרגילים

מטרות הסימולציה והתרחישים הנבחרים, יקבעו את הגורמים המשתתפים בתרגילים. המשתתפים משתנים ועשויים לכלול את מנהל רפואי, המנהל האדמיניסטרטיבי, מנהל מערכות מידע, מנהל אבטחת מידע, אנשי מחלקות פרטיות, משפטיות, ניהול סיכונים, ביקורת פנימית, ניהול סיכונים, דוברות, מעבדות, ביטחון ואחרים בהתאם לצורך.

ציפיות כלליות

הכנה: נדרש מתאם ארגוני כדי לתכנן ולהתכונן לתרגיל. כמו כן מומלץ, אך לא נדרש, כי המשתתפים יהיו בקיאים היטב בהליכי ותכניות תגובת הארגון שלהם לתקרית סייבר. על המשתתפים להיות מוכנים לתרום לתרגול ולמקסם את ערך הלמידה של כל תרחיש.

התחייבות/משך: בהתאם לרמת ההשתתפות הרצויה, כל תרגיל ינוע בין מספר שעות ליום שלם.

מבנה התרגיל:

1. המנחה יציג את התרחישים הנבחרים למשתתפים יחד עם הנחות, הצגות וסימולציות כלשהן על מנת להבטיח שהתרגיל יהיה ריאלי ככל האפשר.
2. הנציגים בארגון ידונו כיצד לטפל בבעיה, כולל נהלי תגובה ספציפיים לתקרית באופן מדי/קרוב, תקשורת נדרשת (פנימית וחיצונית), אחריות פיקוח (לדוגמה, מי יוביל), מידע/משאבים נוספים נדרשים, השלכות משפטיות או השלכות רגולטוריות אחרות, תכנון/פעולות לטווח ארוך שיש לשקול ותכניות מגירה אפשריות.
3. על פי הצורך, המנחה יספק נקודות לסייע על מנת שהתרחיש יתקדם.
4. יתקיים דיון מדי על מה עבד היטב ומה היו חלק מהלקחים שנלמדו יבוצע מיד לאחר האירוע.
5. דוח לאחר פעולה ("תחקיר אירוע") ינוסח ויופץ למשתתפים לאחר מכן כדי להבין באופן רשמי את הלקחים שנלמדו מהתרחיש ואת שיטות העבודה המומלצות. ראה פרטים נוספים בהמשך :

שלב : 1 להתכונן ולתכנן

- קבע מטרות ויעדים לניהול התרגיל (לדוגמה, להשתמש בו כדי להעלות מודעות אצל המנהלים, להעריך את יכולות תגובת הסייבר ו/או תכנית אבטחת סייבר מתקדמת).
- השג תמיכה ארגונית והסכמה לניהול התרגיל.
- בחר מנחה/משקיף היכול להוות צד אובייקטיבי כדי להעריך אם הושגו מטרות ויעדים.
- התחל לתכנן את התרגיל על ידי בחירה/התאמה אישית של תרחישים ממדריך זה.
- בחר מיקום ואמצעי לניהול התרגיל (מיקום פיזי ו/או שיחת ועידה).

שלב : 2 ניהול התרגיל

- המנחה הנבחר ינהל את התרגיל על ידי הצגת התרחישים המוסכמים ומתן מידע נוסף בנקודות, וישמור על המשתתפים "במסלול".
- על המשתתפים מהארגון להיות מעורבים באופן פעיל באמצעות הפנית שאלות, זיהוי השלבים הבאים וכו', כאילו שהתרחיש "אמיתי".
- המנחה ירשום הערות על נקודות חוזקה ואתגרים שנצפו במהלך התרגיל.

שלב : 3 זיהוי לקחים שהופקו

- הקבוצה עורכת תחקיר על תצפיות ולקחים שנלמדו.
- זיהוי שיפורים בתכנית אבטחת הסייבר.
- המנחה שולח סיכום של התרגיל שבוצע והלקחים שהופקו במסמך רשמי.

שלב : 4 שיפור תכנית אבטחת סייבר

- בהתבסס על לקחים והזדמנויות שזוהו לשיפור תכנית אבטחת סייבר, יש לבצע תיקונים כפי שניתן ליישם אותם.
- תכנית לסימולציה נוספת למדידת ההתקדמות לשמירת נושא אבטחת הסייבר על סדר היום.

חוקי השתתפות

תרגילי "על הנייר" יכולים להיות יעילים כאשר הם מיושמים בקבוצות קטנות של עובדים בכירים המטפלים בנושא או בעיה ממוקדים. בהתאם למספר התסריטים שהארגון שלך מחליט להריץ, ניתן לבצע תרגילים כאלו ביום אחד, חצי יום או מספר שעות (למשל 2-4 שעות), עם תרחישים המתמקדים בפרקי זמן מוגבלים לטיפול בבעיות מפתח (למשל, שלב הכנה ותגובה מידית) הנה כמה הנחיות מומלצות :

הנחיות עבור המשתתפים:

- המשתתפים יכולים לכלול נציגים ממחלקות: אבטחה, מערכות מידע, המחלקה המשפטית, ומשתתפים פוטנציאליים אחרים ממחלקות יחסי ציבור, משאבי אנוש ואזורים אחרים, בהתאם לארגון ולתרחישים שנבחרו.
- פורמט תרגיל "על הנייר" מתמקד בפעולות הנדרשות בנקודות זמן מסוימות, סוגיות מפתח, דילמות או נקודות החלטה נדרשות. מטרת הפורמט היא לאפשר לארגון להתעמק בתהליכים הרוחביים ולזהות פעולות נחוצות, החלטות או לקחים שהופקו.

דברים שחשוב לזכור:

- כמשתתף בתרגיל זה, המשתתפים יתבקשו להשעות את המציאות ולא "להיאבק בתרחיש". לעתים קרובות יש אירועים בעולם האמיתי שאינם מתרחשים כפי שניתן לצפות. הכוונה של תרגיל "על הנייר" היא לא להתווכח האם משהו יכול לקרות, אלא כדי לחקור כיצד המשתתפים יפעלו/יגיבו אם זה אכן קרה.
- כמו בעולם האמיתי, המשתתפים עשויים להידרש לקבל החלטות עם מידע מוגבל. המשתתפים יידרשו להשתמש במידע שיש להם בהישג יד ולקבל את ההחלטה הטובה ביותר שהם יכולים לקבל.
- ע"מ לקיים תרגיל אפקטיבי יש צורך להתבסס על כך שהצוות פעל ע"פ פרוטוקול רפואי והארגון מתמודד בצורה עצמאית בהתאם ליכולת בשיגרה וחירום.

הנחיות עבור המנחה:

תפקידו של המנחה הוא לתאר את התרחיש, לענות על שאלות למשתתפים מרכזיים ולזהות סוגיות נוספות. עם זאת, המנחה אינו מספק למשתתפים או לארגון "תשובות" כלשהן לתרגיל. לעתים קרובות אין תשובה אחת נכונה. קביעת הגישה והתגובה הטובות ביותר תלויה בארגון.

ציפיות ספציפיות מהמנחה כוללות:

- תפקידו של המנחה בתרגיל "על הנייר" הוא משולש: מנחה, יועץ ואנליסט. בתור מנחה, עליו לעקוב אחר הישגי האירועים הקשורים ליעדי התרגיל, להציע עצות, לשמור על הדיון במסלול הנכון, ולהבטיח שהקבוצה המשתתפת אינה מבזבזת זמן על נושאים משיקים לדיון.
- המנחה הוא היחיד המעניק תשומת לב מלאה לתהליך. יש לזכור שתפקידו של המנחה אינו עוסק בהנחלת מידע, אלא בהפקת מידע מהמשתתפים על-ידי הצגת השאלות הנכונות.
- **הדרכת תרחיש:** המנחה ידריך את תוכן התרחיש ואת מטרות התרגיל הרצויות למשתתפים ויציע מידע מעודכן המבוסס על "ספר המהלכים" של התרחיש. לכל תרחיש יהיו שאלות לדיון, שיציגו החלטות מפתח ואת הפעולות הנדרשות מההשתתפות. חשוב יותר להבין את התהליך ואת הרציונל המוביל ל"מדוע" התקבלה פעולה/החלטה כלשהי מאשר ההחלטה בפועל עצמה. על המנחה להשתמש בשאלות אלו כדי להניע את הדיון.
- **דיון קבוצתי:** אנו ממליצים לתת לקבוצה זמן להסתגל לדיון במסגרת תרגיל "על הנייר" ולאחר מכן למקד את הדיון בהחלטות מפתח הקשורות לסדר היום. עם זאת, חשוב כי המשתתפים בכלל זה הנהלת הארגון (לא המנחים) יקבעו מתן עדיפות להחלטות במסגרת התרגיל.

דברים שחשוב לזכור:

- המנחה לא ישתתף בתרגיל זה. הוא/היא משקיף ניטרלי, ולכן חשוב כי המנחה ישאר ללא דעות מוקדמות, יתבונן, ויעמוד בפיתוי להתערב עם פתרונות/דעות משלו/משלה. בעת ביצוע התרגיל, על המנחה:
- לזכור כי שתיקה והפסקות בשיחה יכולות להיות דבר טוב כיוון שהן עשויות לעודד משתתפים לדבר.
- להתחיל את הדיון עם שאלות רחבות, ולאחר מכן לצמצם את השאלות בהן צריך לטפל במהלך.
- להכניס את עצמו/עצמה לדיון רק כדי:
 - להבהיר נקודות ספציפיות בתרחיש עצמו
 - להבטיח כי הצוות שוקל את כל ההיבטים של הנושא
 - למנוע מהתרחיש מלשקוע.
- להרתיע משתתפים מלקבוע מסקנות מבלי לספק את הרציונל עבורם.
- לבקש מהמשתתפים להסביר כיצד התגובה שלהם תעבוד על ציר זמן נתון ומי יהיה אחראי על כל החלטה או פעולה.
- המנחה יכול/ה לענות על שאלות בסיסיות למשתתפים, אך אינו/ה יכול/ה לייפות את תשובתו/ה. כל קריאת ביניים צריכה להיות כללית בטבעה על מנת להוביל לדיון ושאלות עמוקות יותר של המשתתפים.
- על המנחה לרשום הערות במהלך התרגיל על ההבחנות שלו/ה, כדי לזהות את השיטות/הלקחים הטובים ביותר שהופקו. תיעוד המנחה הן על מה נעשה והן על מה שלא נעשה על ידי המשתתפים הוא קריטי לתהליך. תצפיות אלה חיוניות להגשמת התועלת המלאה של התרגיל.
- על המנחה לעודד את המשתתפים ליהנות ולשמור על מצב הרוח. אנו צופים שכאשר הארגון יתרגל את מערכות וקישורי התקשורת הללו, נמצא פערים בתהליכים שלו. אף אחד לא צריך להרגיש רע בקשר לתוצאות. המטרה היא לשפר את האבטחה בנכס הלאומי הקריטי הזה הנקרא שירותי בריאות.

מהם 10 תחומי ההערכה?

ממשל/אנשים	האם הארגון מסוגל לזהות ולהביא את האנשים המתאימים כדי לפקח או לתקן את תקרית הסייבר (למשל, נציגים ממחלקת מדיניות, אבטחה, יחסי ציבור, משפטית, משאבי אנוש וכו')?	• האם תפקידי המפתח והאחריות מוגדרים ומובנים? • האם הייתה תקשורת של חלוקת אחריות זו מחוץ לקבוצת האבטחה או קבוצה אחרת האחראית לתפקידים אלו)?
מדיניות ו/או הנחיות לתגובה לתקרית	האם הארגון כתב תהליכים או הנחיות לתגובה ראשונית לתקרית, פיקוד ובקרה, תגובה לפריצה, דיווח, הודעה על התקרית, רשויות ותיקון/החלטה לטווח ארוך?	• האם התהליכים והגורמים האחראיים לדיווח והודעה ברורים? • האם תהליך התייעוד היה ברור? • האם המדיניות תואמת לדרישות האחרונות של כלל אומניבוס (למשל, מבחן 4 נקודות לאי-חשיפה)?
תקשורת פנימית והסלמה "אסקלציה"	על מנת להבטיח תיאום ושיתוף פעולה, האם התקרית הועברה בצורה נכונה ברחבי הארגון (למשל, למחלקת מדיניות, משפטית, ציות) והועברה להנהלה הבכירה והעסקית?	• לעתים קרובות, התקשורת מחוץ לאבטחה מתעכבת. האם זה המקרה בתרגיל זה? • האם ההתקשרות הובנה במלואה בקרב המשתתפים? • האם נעשה דיון שמערב את הצוות המשפטי, לצורך שמירה על זכויות משפטיות?
הדרכה	להעברת ציפיות, האם לארגון יש תכנית הדרכה כתובה לזיהוי אירוע סייבר, דיווח ותיקון מיד?	• האם נראה כי משתתפי הארגון הוכשרו להגיב לתקרית?
שיתוף מידע	לעזור לצפות איומים כלליים וספציפיים לתעשייה, האם הארגון רשום ו/או משתמש במודיעין לאיומי סייבר?	• האם הארגון מקבל וממנף מידע על איום ספציפי למגזר הבריאות להבנה טובה יותר של הסיכונים על מנת לנקוט בפעולות המתאימות?
ניהול איומים ופגיעות	למזער חדירות ותקריות, האם הארגון מבצע בדיקות חדירה ותקיפה תקופתיות, בדיקות סייבר,	• האם הארגון מתייחס או ממנף מידע מתהליכי ניהול הפגיעות שלו במהלך משחק המלחמה והתגובה?

- האם הארגון מבצע סריקות איום מתמשך ומתקדם (ATP) וזיהוי חולשות?

זיהוי פריצה, או בדיקות דומות אחרות?

האם יש לארגון תהליך הדורש בדיקה כזו?

- האם יש לארגון והאם הוא ממנף מאגר מלאי על מנת לבצע הערכה סיכוניים, השפעה, ו/או ביצוע ניתוח נוסף במהלך התרגיל?

להעריך האם הארגון יכול להיות מושפע מאיום, האם הארגון שומר מלאי נכסים של מאגרים/מערכת מרכזיים, כולל מכשירים ניידים, מכשירים רפואיים המכילים נתונים אישיים (PHI) יחד עם האדם האחראי לדעת את מיקומם?

ניהול נכסים ומלאי נתונים/נכסים

- האם יש לארגון תכנית הערכת ספק כחלק מתכנית הסייבר שלו?
- האם ספקים כלולים בתהליכי התגובה של הארגון?
- האם הספקים מודעים

זיהוי סיכונים פוטנציאליים של צד שלישי, האם יש לארגון מלאי של ספקים מרכזיים ויש לו הסכמי שותפות עסקית אתם? האם לארגון יש תהליך לשמירה על מלאי כזה?

הערכת הספק

- האם הארגון עורך דיון ומנסה להפיק לקחים מהתרגיל?

לזהות ולמנוע אירועים חוזרים ופגיעות פוטנציאליות, האם הארגון

הפקת לקחים

מתעד תקריות/פריצות ועורך תהליך הפקת לקחים?

- האם הארגון דן בעדכון ההדרכות או בתכנית האבטחה שלו כדי לשקף לקחים שנלמדו מתקרית זו ו/או תקריות קודמות?

לטפל ולהגיב לשינויים בפעילות העסקית, בטכנולוגיה ו/או איומי סייבר חדשים, האם יש לארגון תהליך לסקירה ועדכון שנתיים של תגובות לתקריות ותכניות סייבר/אבטחה, מדיניות

עדכון תכניות ומדיניות

- עשרת תחומי ההערכה הבאים כוללים : פעולות, מדיניות או מוצרים מרכזיים לחיזוק יכולות אבטחת הסייבר של ארגון.
- כל תחומי ההערכה עשויים שלא לחול ישירות על תרחיש שנבחר. עם זאת, קריטריונים להערכה ניתן להעריך באופן ישיר או עקיף בהתאם לתרחיש שנבחר (לדוגמה, אם התרחיש מדבר על התפשטות של נזקה במכשיר, ניתן להעריך את סמן מספר 7 בהתבסס על השאלה האם מתייחסים למלאי הנכסים בבדיקת זיהומים ופגיעות פוטנציאליים על מכשירים אחרים במהלך התרגיל). השאלות הן דוגמאות, ותהיה גם מעורבות של שיקול דעת.

תהליך התרגול

תרגולי סייבר מיועדים להשפיע על כל משתתף ובמקרים מסוימים דורשים מעורבות מנהיגותית בכירה. התרגילים מכוונים את ארגוני הבריאות ואת השותפים העסקיים שלהם מסוגים וגדלים שונים, בייחוד המשתתפים הבאים :

- ספקים - בתי חולים, מרפאות, מרכזי שיקום, סיעוד, בתי אבות, אשפוז.
- יום, ניתוחים ומרכזי רפואה דחופה.
- בתי מרקחת קמעונאים ובהזמנה בדואר.
- מנהלי הטבות פרמצבטיות (PBM).
- תכניות בריאות.
- ארגוני מחקר רפואי וניסויים קליניים.
- שותפים עסקיים.

- ארגון בריאות כללי.

מורכבות התרגילים

תרגילי סייבר מדורגים על פי המורכבות, החל מהמורכבת הנמוכה ביותר, כוכב אחד (*), ועד למורכבות הגבוהה ביותר, שלושה כוכבים (***).

תרחישים

תרגיל 1 *

סיפור רקע: בית החולים שלך משתמש במערכת רישום רפואית ממוחשבת לניהול הטיפול בחולה. במהלך השבוע האחרון, למספר חולים הייתה תגובה חמורה לתרופה בזמן אשפוזם בבית החולים. מספר המקרים נראה גבוה מהרגיל באופן משמעותי.

תיאור

מצב

חלק 1 : במהלך בדיקה נקבע כי ברשומות הרפואיות הממוחשבות של החולים לא נרשמו האלרגיות שלהם לתרופות.

חלק 2 : רופאים מדווחים גם הם כי האלרגיות לתרופות אינן מופיעות במערכת הממוחשבת והתיעוד מראה כי נתונים אלו כן הוכנסו למערכת לפני 11 יום.

חלק 3 : לאחר בדיקה נקבע כי הרשומות הרפואיות הממוחשבות של החולה שונו, אך מספר זיהוי המשתמש ביומן השינויים ריק.

חלק 4 : לאחר בדיקה נוספת, אתם מוצאים גם אי התאמות לא מוסברות של נתונים אחרים ברשומות הרפואיות הממוחשבות.

חלק 5 : ה CERT -הלאומי מפרסם דוח המציין כי האקטיביסט הסורי מתמקד בארגוני בריאות במטרה לשבש את פעילותם ולפגוע באמון הצרכן על ידי שיבוש המידע הרפואי.

- הנחות הארגון בזמן התרגיל: יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- תחומים לשימור: יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- תחומים לחיזוק ושיפור: יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 2 *

סיפור רקע: הארגון שלך מקבל הודעה מגורם חיצוני על כך שדיאגרמות הרשת של הארגון שלך (כולל כתובות IP, רשימת בקרת גישה וכללי firewall) פורסמו באתר GlueBin הציבורי.

תיאור

מצב

חלק 1 : כתובת ה IP- שתועדה באתר GlueBin היא של אתר נופש זר.

חלק 2 : במהלך סריקה של קבצים ביומן, אתה מזהה חיבור לקוח לדואר אלקטרוני מאותה כתובת IP. הדואר האלקטרוני של הארגון שלך דורש סיסמה קשה כדי להיכנס.

חלק 3 : לחבר בכיר בצוות יש שיתוף זמן באתר נופש זה והוא משתמש לעתים קרובות במרכז העסקים שלהם. אתה מראיין אותו ומגלה כי הוא היה באתר הנופש בזמן הפרסום ב-GlueBin, אך הוא אומר כי הוא לא פרסם דבר לאתר GlueBin.

חלק 4 : חבר הצוות הבכיר אומר גם כי הוא התחבר לרשת האלחוטית החינמית של אתר הנופש עם המחשב הנייד של העבודה.

חלק 5 : אתה ממשיך לעקוב אחר אתר GlueBin ורואה מידע ארגוני נוסף מפורסם שם בשימוש באותה כתובת IP.

חלק 6 : אתה גם קובע כי כל הקבצים שפורסמו באתר GlueBin הופיעו בקבצים מצורפים בתיבת הדוא"ל של חבר הצוות לפני נסיעתו לאתר הנופש.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 3 *

סיפור רקע: מנהל בית החולים מקבל שיחת טלפון מנשיא תוכנת Softco המודיע לו כי מחשבים מבית החולים בצעים התקפות על אתר Softco Software בשני סופי השבוע האחרונים Softco. מבקשים הסבר לכך לפני נקיטת פעולה בעניין זה.

תיאור

מצב

חלק 1 : לאחר בדיקה של יומן הרשת נמצאה תנועה רבה המכוונת כלפי אתר Softco Software.

חלק 2 : לאחר בדיקת אחד המחשבים הפנימיים המזוהה ביומן הרשת נמצאה תכנה לא מזוהה אשר רצה במחשב המחובר לכתובת IP בקנדה ביציאת TPC 6667 (IRC).

חלק 3 : לאחר ביצוע בדיקה על המחשב הנגוע התגלה כי התוכנה הזו נוצרה חודש לפני שתוכנה בשם "super gem sorter vision quest.exe" יצאה לפועל.

חלק 4 : הבדיקה מציגה כי התוכנה נמחקה, אך במקור היא הורדה למחשב מקובץ מצורף בדוא"ל.

חלק 5 : הארגון מאתר את הודעת הדוא"ל עם הקובץ המצורף ושורת הנושא שלו היא: "משחק ממש כיפי וזכור להעביר אותו לכל החברים שלך". דוא"ל זה הגיע מגירסת cc של הדומיין שלך שנראית כמו כתובת הדוא"ל של מנהל מערכות המידע שלך.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.

- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 4 *

סיפור רקע: מנתח גזים בדם מצביע על קריאות נתרן גבוהות עבור מספר גדול של חולים. מכשיר זה מבודד ולא מחובר לרשת.

מציב	תיאור
	חלק 1: טכנאי מעבדה מזהה קריאות חריגות של רמות נתרן גבוהות במהלך בדיקות גזים בדם ומוציא את המכשיר משירות.
	חלק 2: אתה מבצע הליכי פתרון בעיות, אך לא מוצא דבר שיסביר את הקריאות השגויות.
	חלק 3: אתה בודק גם את רשומות התחזוקה והן מראות כי המכשיר עבר בדיקה ראשונית כאשר הגיע לראשונה. המכשיר גם תוקן לאחרונה ומערכת ההפעלה והתוכנה שלו מעודכנות.
	חלק 4: אתה מתקשר לספק וטכנאי שטח נשלח אל מיקומך. הטכנאי קובע כי ישנה נזקה על המכשיר העצמאי. תאריך היצירה והתיקון האחרון של הנוזקה מתאים לתאריך התיקון האחרון במנתח הגזים בדם.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 5 *

סיפור רקע: הארגון שלך משתמש בתוכנה מותאמת אישית לניהול בריאות וחיוב עבור המטפלים שלו בשטח. לחבילת תוכנה זו יש דף אינטרנט בקצה קדמי ושרת SQL בקצה האחורי. בשבועיים האחרונים כל הגשות החיוב שלהם ל-Medicare נדחו בשל קודי נוהל חסרים.

מציב	תיאור
	חלק 1: אתה מתקשר לספק התוכנה, שם מסבירים לך כי קודי הנוהל הם שדות חובה וכל קודי הנוהל מקודדים בצורה חזקה לדף האינטרנט.
	חלק 2: אתה בודק את טבלת SQL ומגלה כי כל הרשומות בטבלת קוד הנוהל נמחקו. אתה מסתכל גם בטבלת הביקורת והיא כוללת רק רשומות של השבועיים האחרונים.
	חלק 3: במהלך בדיקת שרת SQL אתה מוצא קובץ גדול המכיל את טבלאות החולים מאוחסן בשורש כונן c:
	חלק 4: אתה בודק את דף האינטרנט ומגלה כי שדה שם הכניסה של המטפל אינו מבצע אימות נתונים ומאפשר לדוחות SQL להישלח לשרת SQL.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.

- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 6 *

סיפור רקע: הארגון שלך בודק את הרשומות הפיננסיות שלו ומגלה כי חסרים \$100,000 מחשבון רכש הציוד הרפואי שלו.

תיאור

מצב

חלק 1: מחלקת הנהלת חשבונות סוקרת את כל ההזמנות שאושרו לאחרונה והבדיקה מאשרת כי חסרים \$100,000 בחשבון.

חלק 2: מחלקת הנהלת החשבונות יוצרת קשר עם הבנק של הארגון ומגלה 10 תשלומים של \$10,000 לחשבונות בנק לא מאושרים בחו"ל. כל התשלומים בוצעו על ידי אותו מנהל רכש.

חלק 3: אתה בודק את מנהל הרכש שלך, שטוען כי מעולם לא ביצע את התשלומים הללו.

חלק 4: אתה מבצע בדיקה משפטית של מחשב מנהל הרכש. במהלך הבדיקה, אתה מגלה כי הדפדפן במחשב לא הוגדר לקבלת עדכונים והמחשב נגוע בנוזקה.

חלק 5: אתה מגלה גם כי הנוזקה הגיעה מאתר אינטרנט מזויף המעוצב כמו אתר מדיה חברתית פופולרי של תעשיית הבריאות בשם [AwesomeHealthSpace.com](https://www.AwesomeHealthSpace.com) בנוסף, אתה מוצא הודעת דוא"ל עם קישור לאתר המזויף, שנמצא גם הוא במחשב בתוך תיבת הדוא"ל של מנהל הרכש.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 7 **

סיפור רקע: הארגון שלך ביצע מיקור חוץ לקידוד ואירוח האפליקציה שלו לנייד, לספק צד שלישי פופולרי המתמחה באפליקציות בריאות בנייד. אתה שומע בחדשות כי הייתה פריצה לרשת של הספק (כלומר, ספק אפליקציית הבריאות לנייד), אך הספק עדיין לא פנה אליכם.

תיאור

מצב

חלק 1: אתה קורא דוח על בלוג אבטחה אליו נסוגו הנתונים של לקוחות הארגון במשך חודשים ולאנשים זרים הייתה גישה מלאה לנתונים האישיים הללו. אתה מתקשר לספק, שם מבטיחים לך כי הרשתות שלהם מאובטחות.

חלק 2: ספק הצד השלישי פותח בבדיקה, בה מתגלה כי אחד המפתחים השתיל דלת אחורית בספריית קוד אפליקציות שכיחה, בה משתמשים במוצרים רבים שלהם, כולל המוצר בו משתמש הארגון שלך.

חלק 3: יוצרים אתך קשר מ-DHHS Cyber Threat Analyst Center -והם

מודיעים לך כי הם זיהו את הבלוגר כחבר קבוצת האקטיביסטים סינית.

חלק 4 : כמה כלי תקשורת מפרסמים את טענת הבלוגר.

חלק 5 : הארגון שלך מתחיל לקבל תלונות מלקוחות וכך גם DHHS והמשרד לזכויות האזרח (OCR) בנוגע לפריצה.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 8 **

סיפור רקע : הארגון שלך מתמחה בשירותי מרפאות חוץ ומקבל הודעה כי הושגה גישה ל 150,000 -רשומות הנוגעות ל 100,000 -מטופלים על ידי צד לא מורשה באמצעות חילופי מידע בריאות (HIE).

תיאור

מצב

חלק 1 : התקשורת המקומית מפיצה את החדשות על הפריצה ומבקשת את תגובת הארגון שלך.

חלק 2 : הארגון שלך מקבל הודעת דוא"ל הדורשת העברה של מיליון דולר בתוך שמונה שעות לחשבון זר, או שהפורץ ישחרר את המידע.

חלק 3 : אתה מבצע בדיקה מהירה של ההודעה. אתה קובע כי קבלן זר לשעבר נכנס לרשומות מסוימות כנראה בשימוש חשבון מנהל שהיה משותף בקרב אנשי IT בתמיכה ב – HIE.

חלק 4 : אתה מגלה כי הקבלן הזר אינו נמצא יותר בארצות הברית ונמצא כרגע במדינה ללא הסכם הסגרה.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 9 **

סיפור רקע : הארגון שלך מקבל התראה כי תמונות רפואיות של המטופלים שלכם מתחילים להופיע בלוח הדיונים 5chun.

תיאור

מצב

חלק 1 : אתה יכול לקבוע כי בכל הרשומות מופיע אותו הרופא.

חלק 2 : אתה קובע כי המידע שדלף כולל 50 רשומות של מטופלים מתחת לגיל 18.

חלק 3 : אתה שואל את הרופא והוא אומר כי הוא מחבר את הטאבלט למחשב העבודה שלו עם סנכרון אוטומטי מופעל, כדי לצפות בנתוני המטופלים וכי היה סנכרון של למעלה מ-2000 רשומות.

חלק 4 : במהלך השיחה עם הרופא, הוא מספר כי הוא לא מוצא את הטאבלט שלו ונראה כי הוא נעלם. מערכת ניהול הנכסים שלכם מראה כי הטאבלט שלו הוצפן עם סיסמה. אתה שואל את הרופא כמה הסיסמה שלו הייתה חזקה והוא אומר לך כי השתמש בסיסמה "PASSWORD".

חלק 5 : יומני הרשת שלכם מראים כי הטאבלט מאותת בבית ונמצא כעת קרוב מאוד לשם.

- הנחות הארגון בזמן התרגיל: יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- תחומים לשימור: יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- תחומים לחיזוק ושיפור: יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 10 ***

סיפור רקע : רשות אכיפת החוק מודיעה לארגון שלך כי עותק של מסד הנתונים של הרשומות הרפואיות הממוחשבות (EHR) של הארגון נמצא במערכת שהשתלטו עליה.

תיאור

מצב

חלק 1 : המערכת עליה השתלטו מכילה גם קוד מקור למערכת הרשומות הרפואיות הממוחשבות (EHR).

חלק 2 : האפליקציה והנתונים הנמצאים בסיכון מתארחים בספק שירותי ענן (CSP) ואינם נמצאים בתוך הרשת שלכם. ספק שירותי הענן מספק אירוח מסוג תשתית כשירות (IaaS).

חלק 3 : ספק שירותי הענן טוען כי אין לו אחריות כלשהי להודעת הפריצה או הניטור כיוון שהפריצה התרחשה ברמת האפליקציה. הספק מספק את יומני הגישה של מסוף הניהול. ישנם חיבורים לא מוסברים ממקור מחוץ לרשת שלכם.

חלק 4 : במהלך בדיקה משפטית של מערכת הרשומות הממוחשבות המתארחות בשירותי ענן, אתה מגלה מספר ניסיונות כניסה למערכת שנכשלו מלפני 3

חודשים לקצה הקדמי של הרשת ולקצה האחורי של אפליקציית, EHR ולאחר מכן ישנה ירידה דרמטית במספר ניסיונות הכניסה.

הבדיקה המשפטית הראשונית של התמונות במכשיר המתארחות בספק שירותי ענן חושפת כי למסוף הניהול של ספק שירותי הענן ולשרת הקצה האחורי של הרשת ישנה סיסמה משותפת.

חלק 5 : ישנו חיבור ישיר מהרשת שלכם לספק שירותי הענן. הבדיקה המשפטית שלכם מגלה כי היו ניסיונות גישה לא מאושרים לרשת שלכם מסביבת התשתית כשירות של ספק שירותי הענן.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 11 ***

סיפור רקע : שלושה מטופלים שעברו טיפולי הקרנות בארגונכם מתחילים מיד להראות סימנים לסימפטומים של מחלת קרינה חמורה לאחר קבלת טיפולים מהארגון שלכם. רופא הוזמן לבדוק את חולים אלו והוא קבע כי כולם קיבלו רמות קרינה לא בטוחות במהלך הטיפול שלהם.

תיאור

מצב

חלק 1 : מחלקת האונקולוגיה שלכם מפעילה בדיקה דיאגנוסטית שאינה מזהה בעיות כלשהן, אך בדיקה ידנית מראה רמות טיפול לא בטוחות. היצרן שולח טכנאי שאינו מוצא בעיה כלשהי במערכת, אך חושד בחבלה ומודיע ל-משרד הבריאות לניהול חקירה.

חלק 2 : חקירת ה CERT -בריאות מעלה את העובדה כי המסוף של מערכת ניהול הטיפול ששימש את ציוד ההקרנות לשמירת נתוני המטופלים וניהול המינון פעל על מערכת הפעלה מעבר למחזור התיקונים שלה. הארגון שלכם לא עדכן או תיקן את המערכת לאחרונה.

חלק 3 : החברה שיצרה את מערכת ניהול הטיפול היא הספק היחיד לתיקוני המערכות. מערכת ניהול הטיפול יכלה גם לעבוד רק על מערכת ההפעלה הנוכחית שלה. המערכת לא תוקנה מרגע שהותקנה.

חלק 4 : הבדיקה שלכם מגלה כי מערכת ניהול הטיפול לא נרשמה באף רשימת נכסי אבטחה ולא נבדקה לנקודות רגישות.

חלק 5 : ה CERT -בריאות מזהה נזקה בציוד טיפול ההקרנות. הנזקה הייתה בעלת תכונות של הימנעות/השבתת, AV שגם השביתה אמצעי ביטחון אחרים של המערכת, מה שהוביל לחשיפת יתר לקרינה. אף אחד מהתיקונים המסופקים על ידי הספק לציוד יכול היה למנוע מהנזקה להשבית את אמצעי הביטחון.

- הנחות הארגון בזמן התרגיל: יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- תחומים לשימור: יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- תחומים לחיזוק ושיפור: יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 12 ***

סיפור רקע : פגיעות/ניצול של אפליקציית רשת פורסמו ב DefCon -עבור תוכנת מקור פתוח נפוצה המהווה את הבסיס לכלי אבטחה רבים ואפליקציות תוכנה. התוכנה משמשת לקלט נתונים עם חיבורים מוצפנים קבועים.

תיאור

מצב

חלק 1 : תוכנת קוד פתוח פגיעה משולבת בפתרונות המסופקים על ידי ספקי אבטחה רבים. אחד מחברי הצוות שלכם, שהיה ב-DefCon בודק את המערכות שלכם ומוצא כי רבים משרתי הרשת, רשתות VPN ו firewall - משתמשים בכלי זה.

חלק 2 : הפגיעות הייתה שם למשך שנתיים לפחות, אך רק לאחרונה הובאה לידיעת הציבור.

חלק 3 : הצוות שלך ממליץ להעביר את שרתי הארגון למזלג אבטחה מתחרה, אך אין באפשרותך לאבטח את ה VPN -וה firewall -שני אלו תלויים ביצרן לעדכונים.

חלק 4 : firewall מתחיל לאתר מספר התקפות גבוה על ה, VPN -המנסות

לנצל את הפגיעות שלו.

חלק 5 : firewall עברה את תקופת התמיכה והיצרן כבר לא מעדכן את מערכת ההפעלה.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 13 ***

סיפור רקע : התקבלה התראה אוטומטית כי בוצעה גישה למסד נתונים רפואיים בין השעות 1:00 ל 3:00 -לפנות בוקר. לא היה טיפול תחזוקה מתוכנן למשך הלילה.

תיאור

מצב

חלק 1 : אתה מוצא קובץ יומן המראה כי בוצעה גישה למסד הנתונים באמצעות חשבון ברירת המחדל של מנהל המערכת.

חלק 2 : מנהל מערכת מסד הנתונים קובע כי שם החשבון היה "administrator" והסיסמה הייתה "admin2014"

חלק 3 : מסד הנתונים מכיל מרשמים ומידע דמוגרפי על מספר גדול של מטופלים.

חלק 4 : מסד הנתונים כולל גם מידע פיננסי של ארגון שלך אין הרשאה או סיבה לגיטימית לאסוף. איסוף המידע היה מנוגד למדיניות הפרטיות של הארגון, והציבור אינו מודע לכך שמידע נוסף זה נאסף.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל 14 ***

סיפור רקע : ערכת SIEM לניהול אירועים ואבטחת מידע בארגון שלך מתריעה על חיבור ועל העברה של כמויות גדולות של מידע ל- StopBox שירות אחסון בענן. ההעברה נמשכת.

תיאור

מצב

חלק 1 : מנהל הרשת מנסה לחסום את StopBox אך מגלה כי StopBox

זהה לתוכנת VOIP בעלת טכנולוגיה להימנעות מ . firewall -התנועה ב-

StopBox מוצפנת ויכולה להשתמש בתקשורת עמית לעמית (P2P) מנהל

הרשת מגלה גם כי מנהלים מסוימים השתמשו ב - StopBox

חלק 2 : אתה בודק לאחר את התנועה ומזהה כי אחת המתמחים הייתה אחראית להעברת הנתונים. המתמחה השתמשה בנתוני מידע המאפשר זיהוי אישי (PII) למחקר במחשב הביתי. אתה מתעמת עם המתמחה. היא מתנצלת ומבטיחה למחוק את כל הנתונים מ- StopBox. היא גם אומרת שתמחק את הנתונים מהמחשב הביתי שלה ברגע שתקבל אותו בחזרה מטכנאי NerdHerd המתקנים אותו.

חלק 3 : StopBox הוא בעל תכונת שחזור לקבצים מחוקים שלא ניתן להשבית.

חלק 4 : המתמחה מודיעה לך כי NerdHerd היו חייבים לבצע שחזור מלא של המערכת עקב נזקה שהם מצאו במחשב.

חלק 5 : אתה מקבל מידע כי מטופל עם שם ייחודי שיש עליו התראות גוגל על שמו קיבל הודעות כי נתוני ה- PII שלו פורסמו. הוא פונה לארגון שלכם להבהרות.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

חזרה על תרחיש לדוגמה

בסעיף זה נחזור על תרחיש לדוגמה. דוגמה זו נועדה לעודד מחשבה ולגרום לארגון שלכם לחשוב על הסיכונים, על הסוגיות ועל הצדדים המעורבים, אשר כל תרחיש ייחודי עשוי לשאת עמו. אין לחשוב על דוגמא זו כקו מנחה להפעלת התרגיל. אנו מעודדים ארגונים להביא את המיומנויות והניסיון הייחודיים שלהם, כדי להבטיח כי הייחודיות של הארגון תבוא לידי ביטוי בתרגיל. סעיף זה כולל רשימת פעולות לתכנון התרגיל וטבלה של נושאים ושאלות לדוגמא שעשויים להיות מזהים במהלך התרגיל לדוגמא המוסבר להלן.

תרגיל לדוגמא ***

סיפור רקע : ביום שני בבוקר מוקד תמיכת ה- IT שלכם מקבל שיחת טלפון מד"ר גלית בה היא מודיעה להם כי המחשב הנייד המוצפן שלה נגנב מהבית שלה במהלך פריצה. בנוסף היא אומרת כי היה כונן USB במחשב הנייד, אבל היא לא זוכרת מה נמצא עליו. כמו כן, היא מספרת כי היא רשמה את שם המשתמש והסיסמה שלה על פתק ליד המחשב הנייד.

תיאור

מצב

חלק 1 : מוקד תמיכת IT רושם את מקרה המחשב הגנוב בכלי הכרטוס ומודיע על כך למחלקות אבטחת מידע, ציות ומדיניות.

חלק 2 : מחלקת פרטיות מודיעה למשטרה, שם מאשרים כי אכן קיבלו שיחה מד"ר גלית שדיווחה על פריצה לביתה בשעה 2:00 לפנות בוקר בשבת.

חלק 3 : אתה מבצע הערכת סיכונים החושפת כי המחשב הנייד הכיל נתונים ספציפיים על מטופלים כמו בדיקות מעבדה ונתוני אבחון וטיפול, הקשורים למשפט חדש בעניין תרופה.

חלק 4 : אתה קובע כי במחשב הנייד היו גם מספרי ביטוח לאומי ופרטים אישיים ניתנים לזיהוי אחרים, שלא היו אמורים להיאסף, על 10,000 - מטופלים. לד"ר גלית לא הייתה הרשאה למידע כזה.

- **הנחות הארגון בזמן התרגיל:** יש לפרט את המסקנות המתקבלות במהלך ביצוע התרגיל.
- **תחומים לשימור:** יש לפרט את התהליכים שבוצעו כראוי במהלך התרגיל.
- **תחומים לחיזוק ושיפור:** יש לפרט את התחומים ותהליכים אשר דרשו שיפור במהלך התרגיל.

תרגיל חזרה

שלב

ניהול התרגיל

תיאור

הקדמה

הערות

תן למשתתפים להציג את עצמם ואת תפקידם בתרגיל.	■	
הסבר את התרגיל.	■	הסבר למשתתפים
בלי לחץ של זמן.	■	
אין תשובות נכונות ולא נכונות.	■	
התרגיל מתוכנן לעורר דיון.	■	
התייחסו אליו כאל תרחיש אמיתי.	■	
המנחה מציג את התרגיל.	■	התחלת התרגיל
תן לדיונים להתפתח בטבעיות.	■	
זהה סיכונים ובעיות, צעדים שיש לבצע וכו'.	■	
זהה משתתפים פנימיים וחיצוניים בתרחיש.	■	
השתמש בשאלות לא מובילות כדי לעורר שיחה. למשל, "מה היית עושה במצב כזה"?	■	
המנחה יספק הזרקות לפי הצורך.	■	
רשום הערות במהלך הדיון.	■	תיעוד התרגיל
הכן בסיס לסקירה לאחר התרגיל.	■	
שים לב לתחומים הזקוקים לחקירה נוספת.	■	
סכם נקודות שיש לקחת.	■	
תעד את הסוגיות שזוהו.	■	
תן למשתתפים 10 עד 15 דקות הפסקה.	■	סקירה לאחר התרגיל
בדוק את מטרות התרגיל פעם נוספת.	■	
בקש משוב מהמשתתפים.	■	
תעד מסקנות או החלטות מהתרגיל.	■	
תעד את רמת ההתקדמות של הארגון	■	
עקוב אחר פעולות מתקנות.	■	פעולות לאחר התרגיל
תעד את התיקון והלקחים שהופקו.	■	פיתוח תכנית פעולה מתקנת מעקב אחר פעולה מתקנת מעקב אחר לקחים שהופקו
שמור את התוצאות עבור תרגילי הסייבר הבאים.	■	

מדגם של סוגיות ושאלות שזוהו במהלך התרגיל

סוגיות/שאלות לדוגמה

1. כיצד קיבלו את ההודעה מחלקות אבטחת מידע, ציות ופרטיות? באמצעות דוא"ל, טלפון סלולרי, הודעת טקסט?
2. האם מחלקות אבטחת מידע, ציות ופרטיות ידעו מה לעשות ברגע שקיבלו הודעה?
3. מי לוקח את ההובלה בארגון כאשר מתרחש אירוע?
4. מהו זמן התגובה הפנימי למתן שירות בתוך הארגון לתגובה לפריצה?
5. האם יש לארגון עץ קריאות בזמן תגובה לתקרית המסופק למוקד התמיכה?
6. האם תכנית התגובה של הארגון לתקרית יצאה לפועל?
7. האם הצוות נפגש בצורה וירטואלית או פנים אל פנים?
8. באיזו תדירות מתכנסת הקבוצה מחדש כדי לדון בפריצה?
9. האם מחשב נייד זה היה רשום במלאי הנכסים?
10. האם המחשב הנייד היה מוצפן? כיצד זה נקבע?
11. האם התקן ה-USB היה מוצפן? כיצד זה נקבע?
12. כיצד אומתו הנתונים שהיו על המחשב?
13. האם ניתן למחוק מרחוק את המחשב הנייד?
14. האם יש למחשב הנייד התקן מסוג LoJack?
15. מדוע לקח לד"ר גלית כל כך הרבה זמן להודיע לארגון על הפריצה? מהי מסגרת הזמן הדרושה לדיווח על פריצה?
16. האם הייתה סיבה עסקית לגיטימית לכך שלד"ר גלית יהיו מידע רפואי חסוי (PHI) במחשב הנייד שלה?

17. מתי הייתה הפעם האחרונה שד"ר גלית עברה הכשרה למודעות לאבטחה?
18. האם יש הסכם עובד חתום עבור ד"ר גלית, בו היא מסכימה לציית למדיניות הארגון ולנהליו?
19. האם לארגון שלך יש מדיניות סנקציות לעובדים?
20. האם ד"ר גלית ממושמעת על פי מדיניות הסנקציות של העובדים?
21. מה היה תפקיד אכיפת החוק בפריצה זו?
22. אלו הודעות לגבי הפריצה נשלחו על ידי הארגון?
23. אלו ארגונים חיצוניים קיבלו הודעה על הפריצה?
24. האם פרקליט פנימי ו/או חיצוני קיבלו הודעה ומעורבים בתגובה לפריצה?

12 אבטחת מידע והגנת סייבר במכשור רפואי

1. רקע/מבוא:

- 1.1. אבטחת המכשור הרפואי מהווה כיום אתגר מיוחד במינו. הנושא נמצא בהתפתחות ושינויים תכופים לנוכח פוטנציאל האיומים העלולים לפגוע בבריאות הציבור ושרידות התהליכים הרפואיים מחד ומאידך התלות ההולכת וגוברת בפיתוחים טכנולוגיים בתחומי הרפואה ותועלות בשימוש בחדשנות הטכנולוגית.
- 1.2. אחת הסיבות העיקריות לצורך באבטחת המידע במכשור רפואי הינה השימוש בתשתיות מחשוב תקניות (דהיינו, מערכות הפעלה כדוגמת חלונות ולינוקס, ופרוטוקול תקשורת תקני וגם פרוטוקולי תקשורת ייעודיים) המפעילות יישום או מכשור ייחודי, לעיתים פולשני לגוף האדם המטופל.
- 1.3. המכשור הרפואי מהווה כיום חלק בלתי נפרד מהטיפול הרפואי וזמינותו הינה חיונית למתן מגוון רחב מאד של שירותי רפואה.
- 1.4. המכשור הרפואי הולך ותופס חלק נכבד מתהליכי האבחון והטיפול במטופלים ומחייב קישור בזמן אמת לרשתות תקשורת ארגוניות, ובה בעת לגישה מרחוק למטרות הענקת שירותי רפואה למרחוק, וכן לצורך מתן מענה מקצועי ומהיר לתמיכה ע"י יצרני המכשור וספקי תמיכה ותחזוקה בארץ ומח"ל.
- 1.5. ייצור שיווק ושימוש בציוד רפואי במדינת ישראל:
 - 1.5.1. ציוד רפואי מיוצר, משווק, ומותר לשימוש במדינת ישראל על בסיס רישומו בפנקס הציוד הרפואי, המנוהל באגף הציוד הרפואי (אמ"ר) שבמשרד הבריאות.
 - 1.5.2. התהליך לרישום ציוד רפואי באגף לציוד רפואי כולל בחינת מסמכים, אישורים, והצהרות של גופים רגולטוריים מוכרים. האגף רשאי לדרוש גם מסמכים ומידע נוסף שאינו נכלל בבקשה, וכן דוגמאות של הציוד הרפואי, ולהציג שאלות בכל עניין מן העניינים הנוגעים לרישום הציוד הרפואי.
 - 1.5.3. להלן רשימת הרשויות הרגולטוריות המוכרות שעל אישורם נסמך האישור במדינת ישראל:
 - 1.5.3.1. מנהל המזון והתרופות של ארה"ב (FDA).
 - 1.5.3.2. האישור האירופי (CE Marking), שניתן בידי גופים פרטיים (Notified Bodies) שהוסמכו לכך בידי הרשויות הממשלתיות.
 - 1.5.3.3. הרשות המוסמכת בקנדה (Health Canada).
 - 1.5.3.4. הרשות האוסטרלית (TGA).
 - 1.5.3.5. הרשות היפנית (PMDA).
 - 1.5.4. במידה והוכחה בטיחות ויעילות הציוד הרפואי ובמידה והמסמכים שהוצגו בפני האגף ענו על כל הדרישות המפורטות בחוק הציוד הרפואי ובהנחיות המפורטות באתר האינטרנט של האגף, יונפק אישור רישום הציוד הרפואי בפנקס הציוד הרפואי במשרד הבריאות.

2. הגדרות:

2.1 אבטחת מידע - הגדרת ISO (ISO 27000:2014):

שימור סודיות (Confidentiality), שלמות ואמינות (Integrity), וזמינות (Availability) של מידע. כאשר:

- 2.1.1 סודיות: תכונת אי זמינות/חשיפת מידע לבלתי מורשים (יחידים, ישויות או תהליכים).
- 2.1.2 שלמות ואמינות: תכונת הגנת דיוק ושלמות.
- 2.1.3 זמינות: תכונת הנגישות והשימושיות עפ"י דרישה ע"י ישות מורשית.

2.2 אבטחת מידע - הגנת סייבר (ה"ס) – לפי הגדרת ה-FDA:

תהליך של מניעת שינוי בלתי מורשה, שימוש לרעה או שלילת השימוש, או שימוש בלתי מורשה של מידע האגור, מעובד או מועבר מהמכשיר הרפואי ליעד חיצוני. הגנת סייבר מחולקת לשלושה נושאים:

- 2.1.4 סודיות: נתונים, מידע או מבנה המכשיר נגישים רק לעובדים וישויות מורשות ומופעלים בזמנים מורשים ובאופן מורשה.
- 2.1.5 שלמות ואמינות: נתונים ומידע הנם מדויקים ושלמים ולא שונו באופן בלתי הולם.
- 2.1.6 זמינות: נתונים, מידע ומערכות מידע נגישים ושימישים באופן המצופה, בזמן ובמקום שהוא דרוש.
- 2.1.7 בטיחות: אביזרים ומכשירים רפואיים מצופה להבטיח שימוש נאות במכשירים ובריאותם ובטיחותם של החולים והמטפלים.

2.3 אמ"ר (אביזרים ומכשירים רפואיים):

אגף במשרד הבריאות (צידוד רפואי) העוסק ברישום אמ"ר במדינת ישראל, מתן היתרי יבוא מסוגים שונים לאמ"ר, מעקב אחר שיווק אמ"ר והנפקת מסמכים המסייעים ליצוא אמ"ר. האגף מפעיל מנגנון רישום, פיקוח ובקרה על ייצור, יבוא ושיווק אמ"ר.

2.4 הזדהות:

שיטה להבטחה שתכונה לגבי ישות הינה נכונה. הכוונה היא בד"כ לזיהוי אדם מול מערכת ממוחשבת ולא לזיהוי בין מערכות. פרטי המידע שנותנים את הוודאות המסויימת ומשמשים גורם אימות מתחלקים לארבעה מאפיינים: נתון שהאדם יודע (סיסמא, קוד), נתון שהאדם מחזיק (כרטיס חכם, מכשיר נייד), נתון שהוא האדם (תווי פנים, טביעת אצבע), נתון שהאדם עושה (דפוס התנהגותי) הגדרת ברירת המחדל תהיה באמצעות שני גורמי אימות. 2FA

2.5 הזדהות חזקה:

מימוש תהליך הזדהות ליישות מול שני גורמי אימות לפחות שאחד מהם הוא משהו שבידי האדם או משהו שהוא האדם (כרטיס חכם או ביומטריה).

2.6 הערכת סיכונים (לחלופין: אתור וחישוב הסיכון השורשי בהיבטי אבטחת מידע, דהיינו, זמינות-שלמות ואמינות-סודיות-C-I-A):

תהליך של הערכת רמת הסיכון של המערכות השונות בארגון. התהליך ממפה את האיומים השונים הנובעים מהפעילות במערכות השונות. תוצר הערכת הסיכונים הנו מסמך המדרג את רמת המסוכנות של המערכות השונות לארגון. מסקנות מסמך זה משמשות לגזירת פעילויות אבטחת המידע השונות.

2.7 הצפנה:

תהליך המרה של מידע גלוי (Clear Text) למידע מקודד (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

2.8 זיהוי חד ערכי:

ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

2.9 זיהוי דו ערכי:

ערך ייחודי נוסף על הערך המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי

2.10 חתימה דיגיטלית (Digital Signature):

פריט מידע ייחודי הנוצר כפונקציה קריפטוגרפית של פריט מידע אחר, כך שהוא מזהה את התוכן בצורה מדויקת ומאפשר לזהות שינוי בו.

2.11 לוג – Log:

קובץ התייעוד של נתיב בקרה.

2.12 מכשור רפואי –

ראה פירוט בפרק 6.

2.13 נזק/פגיעה/חבלה - HARM (ISO/IEC 80001-1:2010):

פגיעה פיזית או נזק לבריאותו הגופנית או הנפשית של המטופל, או נזק לציוד. או לסביבה, או צמצום ביעילות, או פגיעה באבטחת המידע האגור במכשיר או במערכת. הותאם מההגדרה בתקן ISO 14971:2007.

2.14 נתיב בקרה:

תיעוד פעולות המתבצעות במערכות מידע. קובץ התיעוד מקשר את הפעולה לנתונים נוספים כגון: שם מבצע הפעולה, המועד, הפעולה עצמה ועוד.

2.15 סיכון שיורי (ISO/IEC 80001-1:2010):

הסיכון הנותר לאחר שאמצעי בקרה לסיכון יושמו. הגדרה 2.15 תקן ISO 14971:2007.

2.16 סקר סיכונים:

סקר המאתר איומים/חשיפות הקשורות באבטחת מידע במערכות שונות והמערך את רמת הסיכון שלהם לארגון.

2.17 תווך תקשורת ציבורי:

תשתיות תקשורת המשרתות/משתפות מספר רב של צרכנים ואינן שייכות לאחד מהם. תשתיות אינטרנט מוגדרות כתווך תקשורת ציבורי.

3. מסמכים ישימים:

3.1 חוקים והנחיות

3.1.1 מדינת ישראל

3.1.1. חוק ציוד רפואי התשע"ב–2012.

3.1.2 הנחיות להגשת בקשה לרישום ציוד רפואי (אמ"ר) במשרד הבריאות- באתר האינטרנט.

https://www.health.gov.il/Services/ImportAndBusinessLicensing/AMR/regitation/Documents/AMR_reg_guidelines.pdf

<https://www.health.gov.il/Services/ImportAndBusinessLicensing/AMR/Pages/default.aspx>

3.2 תקנים בנושא אבטחת מידע

ISO 3.2.1

- סדרת תקני IEC_80001
- IEC_80001-1:2010
- IEC/TR 80001-2-1:2012
- IEC/TR 80001-2-2:2012
- IEC/TR 80001-2-3:2012
- IEC/TR 80001-2-4:2012
- IEC 27002-ISO 27799:2016

3.3 מסמכים והנחיות רלבנטיות מה-FDA

3.3.1 מכשור רפואי- MEDICAL DEVICE :

<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm>

3.3.2 Medical Device Data System :

<http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/MedicalDeviceDataSystems/ucm251906.htm>

3.3.3 יישומים רפואיים ניידים – Mobile Device Applications (23.9.2013)

<http://www.fda.gov/medicaldevices/productsandmedicalprocedures/connectedhealth/mobilemedicalapplications/default.htm>

3.3.4 טיוטת הנחיה (14.6.2013) CYBER SECURITY FOR MEDICAL DEVICES–

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft
Guidance for Industry and Food and Drug Administration Staff

<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf>

3.3.5 הנחיה נוספת שה-FDA מפרסם ב-28.12.2016 :

<https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>

[Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff](#)

FDA Safety Communication: Cyber security for Medical Devices and Hospitals Networks 3.3.6
(14/6/2013)

[http://wayback.archive-](http://wayback.archive-it.org/7993/20170722144747/https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm)
[it.org/7993/20170722144747/https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm](https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm)
<https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm>

National Electrical Manufacturers Association/Healthcare Information – HIMSS/NEMA 3.3.7
and Management Systems Society

Manufacturer Disclosure Statement for Medical Device Security (MDS²)

<http://www.nema.org/Standards/ComplimentaryDocuments/MDS2%20form%20HN%201-2013.xlsx>

4. אחריות ליישום:

משרד הבריאות מגדיר במסמך זה את דרישות אבטחת המידע שיש לכלול בתהליכי שילוב מכשור רפואי במדינת ישראל באופן הבא:

4.1 ליצורני מכשור רפואי:

באמצעות הגדרת דרישות סף מקומיות בתהליך הרישום, (המנוסחות במסמך זה, בפרק 7) הנסמכות על תהליכים תקיניים המקובלים בעולם. כדוגמת MDS² המעודכן (גרסת 10/2013), נחיות אבטחת מידע למכשור רפואי של ה-FDA (אוקטובר 2014 ודצמבר 2016) וכיו"ב.

4.2 למוסדות רפואיים המפעילים מכשור רפואי:

- על בסיס ניהול סיכונים חיבור והפעלת מכשור רפואי האוגר/לא אוגר מידע מקומי (במכשיר) ומתחבר/אינו מתחבר לרשת המוסד הרפואי, תוך הסתייעות בתקינה מאושרת לנושא זה בעולם (סדרת תקני IEC_80001), ובשילוב הגישות שנקטו ע"י המפקח על הבנקים בכותבו את הנחייתו לניהול תקין של טכנולוגיית המידע

(נב"ת 357)², בשנת 2003, וע"י המפקח על הביטוח באגף שוק ההון במשרד האוצר בכתיבת: "הוראה לניהול סיכונים אבטחת המידע של הגופים המוסדיים"³ בשנת 2006. אלו מצוינים בפרק 8.6 במסמך זה.

- בשנת 2017, וע"י הרשות הלאומית להגנת הסייבר במשרד ראש הממשלה נכתבה תורת ההגנה בסייבר לארגונים 4
- חקיקה רלוונטית לדיון בהצעת חוק ההוצאה לפועל – סעיפים 7א ו-7ב חוק הגנת הפרטיות, תשמ"א-19815
- ביום 21.3.2017 אישרה וועדת חוקה, חוק ומשפט בכנסת ישראל את תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-62017, שקבעה שרת המשפטים, המפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות הישראלי על כל גורם המנהל או מעבד מאגר של מידע אישי. התקנות שהן יוזמה של הרשות להגנת הפרטיות שהיא גם הגוף המפקח על יישומן,

4.3 למשתמשים פרטיים של מכשור רפואי:

כחלק מאישור רישום של מכשור רפואי שיירכש ע"י צרכן פרטי ישירות ממשווק, יידרש יצרן המכשור הרפואי לספק למשתמש הנחות אבטחת מידע. דומה להסדר הקיים היום בעת שיווק תרופות, כאשר לכל אריזת תרופה נלווה מסמך מאושר ובו הנחיות לשימוש, תופעות לוואי וכד'.

* לחשיבה לגבי תהליך עתידי. אין התייחסות לנושא זה במסמך הנוכחי.

5. הסיכונים והאיומים למכשור רפואי הנובעים מכשל באבטחת המידע:

5.1 ניהול סיכונים

ההגנה בסייבר מתבססת על תהליך ניהול והערכת סיכונים בסייבר. זהו תהליך מחזורי שנדרש להתבצע כאשר משתנה סביבת הסייבר של הארגון – הן בתוך הארגון (קליטת מערכות חדשות, שינויי טכנולוגיה, שינוי בתהליכים עסקיים וכד') והן מחוץ לארגון (שינוי מתמיד של מרחב האיומים בסייבר על הארגון, הארגון נדרש לזהות את יעדי ההגנה, להגדיר מהן הבקורות הנדרשות על מנת להגן עליהן ולבנות תכנית עבודה מתאימה בכדי לתת מענה לכלל האיומים). ההנהלה נדרשת להחליט על רמת הסיכון שהיא מוכנה לקחת בהתחשב בעלויות מימוש הבקורות למול מחירי התממשות הסיכון בתוך הארגון והשפעותיו על הרצף הטיפולי ושמירה על חיי המטופלים. כמו כן על הנהלת הארגון ליישם מנגנונים לטיפול באירועי סייבר העלולים להתרחש על מנת לצמצם את הנזק.

5.2 פגיעה בחיי אדם:

שינויי כיוול או שינוי כלשהו בנתוני מכשור רפואי (בין בשגגה ובין בזדון) שתוצאותיו הינן תוצאות שגויות שמפיק המכשיר אשר עלולות לגרום לפגיעה בחיי אדם. פעולה זו יכולה להתבצע על ידי גורם אנושי או על ידי קובץ זדוני.

5.3 פגיעה בזמינות השירות המסופק באמצעות המכשור הרפואי:

- גרימת נזק לרכיבי התוכנה של המכשור הרפואי, נזק שעלול לגרום להשבתתו המלאה/החלקית ובכך לפגוע בזמינות השירות שהמכשור מספק למטופלים באמצעות מכשור זה.

² <https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/357.pdf>

³ <http://mof.gov.il/hon/Documents/%D7%94%D7%A1%D7%93%D7%A8%D7%94-%D7%95%D7%97%D7%A7%D7%99%D7%A7%D7%94/mosdiym/memos/2006-9-06.pdf>

https://www.gov.il/BlobFolder/generalpage/tohag-dir/he/Cyber-Accessibility_0.pdf

⁵ http://www.google.co.il/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=5&ved=0ahUKEwii9vSew-TZAhuUEPsAKHchOAIsQFghDMAQ&url=http%3A%2F%2Fknesset.gov.il%2Fcommittees%2Fheb%2Fmaterial%2Fdata%2FH06-05-2007_13-39-48_seifim.doc&usq=AOvVaw2cpcyqdXBUMsgl0z_17wmU

⁶ https://www.nevo.co.il/law_html/law01/501_600.htm

- שינויי כיוול או שינוי כלשהו בנתוני מכשור רפואי (בין בשגגה ובין בזדון) שתוצאותיו הינן תוצאות שגויות שמפיק המכשיר ובכך לגרום להשבתת השימוש במכשיר באופן מלא או חלקי.

5.4 פגיעה בסודיות הנתונים באחד ממרכיבי המכשור הרפואי או בעת העברת מידע מסווג בממשקי תקשורת (פנימיים או חיצוניים):

- גניבת נתוני מטופלים (כולל מידע רפואי אישי) מהמכשור הרפואי עצמו או דרך אחד מהקישורים של המכשור (למשל ע"י יישום תקיפת Man-in-the-Middle) באחד מממשקי המכשור הרפואי או מערכת הניהול שלו, או על ידי ציתות לתווך התקשורת).
- גניבת נתונים מרשומה רפואית ממוחשבת האגורה במערכות המידע של המוסד שבו מופעל המכשור הרפואי ומחובר אליו בתקשורת, ע"י חדירה למערכת המידע של המוסד הרפואי תוך שימוש במכשור הרפואי שאיננו מאובטח כיאות/בממשק שבין המכשור הרפואי ומערכת ניהול התהליך הרפואי (שהמכשיר מהווה חלק ממנו) שאיננו מוגן באופן מספק/בממשק הגישה מרחוק אל המכשור הרפואי.

5.5 פגיעה בשלמות ואמינות הנתונים באחד ממרכיבי המכשור הרפואי או בעת העברת מידע מסווג בממשקי תקשורת (פנימיים או חיצוניים):

- שינוי בלתי מורשה של נתוני מטופלים (כולל מידע רפואי אישי) במכשור הרפואי עצמו או דרך אחד מהקישורים של המכשור (למשל על ידי יישום תקיפת Man-in-the-Middle באחד מממשקי המכשור הרפואי או מערכת הניהול שלו).
- גרימת נזק לרכיבי התוכנה של המכשור הרפואי, נזק שעלול לגרום לפגיעה באמינות/שלמות הנתונים בתהליך העבודה עם המכשור הרפואי.
- שימוש שלא כדין במכשור הרפואי שעלול לגרום לפגיעה באמינות/שלמות הנתונים.

5.6 חדירה למערכות:

- שימוש שלא כדין במכשור הרפואי במטרה לחדור למערכות אחרות בארגון.
- שימוש שלא כדין במכשור הרפואי על מנת לחדור באמצעותו למערכות המידע של יצרני/ספקי המכשור דרך הקישור מרחוק שמספק הלקוח של המכשור הרפואי ליצרן/ספק/מטמיע המכשור.
- שימוש שלא כדין במערכות בארגון במטרה לחדור למכשור רפואי.

5.7 סיכוני אבטחת מידע טכנולוגיים:

- ציתות לרשת התקשורת בממשקים פנימיים (לדוגמא בין תוכנת ניהול המכשיר הרפואי לבין רכיב הבקרה) או חיצוניים (למשל בין תוכנת ניהול המכשור הרפואי לתוכנות אחרות). פעילות זו עלולה לאפשר (בין היתר):
 - חשיפה של מידע רפואי של מטופלים לגורמים לא מורשים.
 - חשיפה של פרטי הזדהות והתחזות לגורמים מורשים.
- גישה של גורם לא מורשה לרכיבי המכשור הרפואי תוך עקיפת מנגנוני בקרה תשתיתיים או אפליקטיביים (לדוגמא קיום חולשות מערכת הפעלה או שירותים, התחזות של גורם לא מורשה למשתמש מורשה, עקיפת מנגנון הזדהות על ידי Brute-Force, עקיפת מנגנון הרשאות, גישה פיזית ללא הרשאה).
- גישה של גורם תחזוקה מורשה לרכיבי המכשור הרפואי, מרשת חיצונית⁷, ברמת הרשאה כזו העלולה לאפשר לו גישה למערכות מידע/רכיבים אחרים ברשת, ללא כל הרשאה.
- חדירה/החדרה מכוונת של קובץ זדוני לרכיבי המכשור הרפואי מתחנות/שרתים ברשת או רשתות מקושרות אליה תוך עקיפת מנגנוני בקרה (הקשחת מערכת הפעלה, אנטי וירוס).
- חדירה/החדרה מכוונת של קובץ זדוני מרכיבי המכשור הרפואי לתחנות/שרתים ברשת או רשתות מקושרות אליהם תוך עקיפת מנגנוני בקרה (דוגמאות למנגנוני בקרה: הקשחת מערכת הפעלה, אנטי וירוס).
- התחזות לתוכנת ניהול מכשור רפואי או למכשיר רפואי או לתוכנה חיצונית אחרת הקשורה לתהליך הרפואי.
- ביצוע שינויים בהגדרות שונות במכשור הרפואי ללא כל הרשאה.

⁷ תקיפה המאפשרת התחזות לגורם מורשה בתווך התקשורת, חשיפת מידע לגורם לא מורשה ואף שינוי של מידע ללא הרשאה.
⁸ שאינה מפותחת על ידי גורם במערך הבריאות

■ הסיכונים שהוצגו בסעיפים שלעיל עלולים לאפשר (בין היתר):

1. פגיעה בזמינות המכשור הרפואי.
2. שיבוש מידע רפואי של מטופלים.
3. שיבוש של מידע חיוני לביצוע טיפול ולכן שיבוש הטיפול עצמו.
4. חשיפה של מידע רפואי של מטופלים לגורמים לא מורשים.

6. ארכיטקטורה כללית של מערך המידע של המכשור רפואי וחיבורו לרשת התקשורת:

6.1 ניתן לחלק באופן כללי את עולם המכשור עפ"י החלוקה הבאה המתייחסת להיבטי איום וסיכון ומתן מענה להם:

- מכשור שאיננו אוגר מידע באופן מקומי - ואיננו מחובר לרשת תקשורת.
- מכשור שאיננו אוגר מידע באופן מקומי - ומחובר לרשת תקשורת.
- מכשור שאוגר מידע באופן מקומי - ואיננו מחובר לרשת תקשורת.
- מכשור שאוגר מידע באופן מקומי - ומחובר לרשת תקשורת.

הערות:

- א. המונח "מחובר לרשת" כולל גם שידור/קליטה ברשת אלחוטית/סלולרית.
- ב. ככל שאנו מתקדמים בחומרת הסיכון כך גדלים האיומים ומתרחב עולם הפתרונות (הבקורות) שנדרש ליישם.
- ג. מכשור רפואי גם אם איננו מחובר לרשת הארגונית עשוי להידרש לחיבור גישה מרחוק למטרת תחזוקה, שדרוגי תוכנה כיול וטיפול בתקלות ע"י היצרן (בארץ או בחו"ל) או ספק התחזוקה (בארץ או בחו"ל).
- ד. על הארגון לנהל את רמות הסיכון אליהן הוא חשוף בסייבר לבקר את תהליכי ההתחברות של ספקים לארגון ופוטנציאל פגיעה בתקינות פעולת המכשור הרפואי והמערכות התומכות.

6.2 ברמה העקרונית שימוש במכשור רפואי כולל את המרכיבים הבאים:

- מכשור רפואי המבצע אבחון, טיפול או שניהם, כדוגמת מכשיר מעבדה, מכשיר דימות, מכשירי בדיקה פולשניים⁹, כולל מחשב צמוד או משובץ מחשב¹⁰.
- רכיב ניהול ההליך הרפואי, כדוגמת מערכת ניהול מעבדות, מערכת ניהול צילומי דימות וכיו"ב.
- מערכת ארגונית/מערכות ארגוניות המאפשרות/גישה למידע הנוצר במכשור הרפואי או בתהליך הרפואי שבו המכשור הרפואי נוטל חלק הן למטפל והן למטופל.

6.3 במקביל יידרשו מענים לדרכי הגישה הבאות:

- גישה מקומית ומרוחקת של משתמשים לכל אחת משלושת סוגי המערכות הנ"ל.
- גישה מרחוק על גבי האינטרנט של יצרני/תומכי שלושת המערכות הנ"ל.
- ממשקי תקשורת פנימיים וחיצוניים שבהם מועבר מידע באופן דו כיווני בין שלושת המערכות הנ"ל.

7. הגדרות אבטחת מידע – רשימת תיוג עבור יצרן האמ"ר:

מקרא לטבלה:

נושא בקרה: המרכיב הראשי שלגביו ייושמו בקורות.

⁹ המכשיר הרפואי עצמו מבוקר על ידי בקר אלקטרוני, שהוא מהווה רכיב ייעודי ונפרד בעל ממשקי תקשורת משלו.
¹⁰ מתואר במסמך זה כתוכנת הניהול של המכשיר או של הבקר.

תיאור הבקרה: הסבר מפורט מהי הבקרה הנדרשת לכל נושא ראשי של בקרה יוצמדו אחד או יותר בקורות.

חשיבות הבקרה:

- בקרה חיונית: כשמה כן היא, חיוני שתתקיים.
- בקרה חשובה: מומלץ שתתקיים, אך איננה חיונית.

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע
1.	כללי	קיום תיעוד של ניתוח סיכוני הגנת סייבר במכשור הרפואי ובממשקים בינו לבין מרכיבים חיצוניים תוך התייחסות לנזק / פגיעה / חבלה (HARM) במרכיבים הבאים בניתוח סיכוני הגנת הסייבר שלהם: • הערכת ההשפעה של האיומים והפגיעות על תפקוד המכשיר ועל בריאות המטופל. • הערכה של ההסתברות לניצול לרעה של איום או פגיעות. • הגדרת רמות סיכון ואסטרטגיות מתאימות לצמצום. • הערכת הסיכון השיווי וקריטריונים לרמות סיכון סבירות.	חשובה	X	X	X	X
2.	כללי	המכשיר הרפואי לא יחשוף מידע פנימי שאינו נדרש למשתמש בעת תקלה.	חשובה	X	X	X	X
3.	הגבלת	קיום מנגנונים המגבילים גישה למכשירים באמצעות תהליך הכולל הזדהות ווידוא ההזדהות של ישויות (יחידים, תהליכים, מכשירים). לדוגמה:	חיונית	X	X	X	X

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע
	גישת למשתמשים מורשים	שם משתמש וסיסמה, כרטיס חכם, ביומטרי).					
4.		קיום מנגנון אוטומטי לסגירת session של משתמש על בסיס מרכיב זמן מתוכנן מראש באופן מותאם לסביבת הפעלת המכשיר.	חשובה	X	X		X
5.		קיום מנגנון עצמאי ושכבתי להענקת הרשאות שמבוסס על רמות הרשאה שונות עפ"י תפקיד דורש ההרשאה (לדוגמה: אפליקציה רפואית, ספק שירות רפואי, מנהל).	חיונית	X	X		X
6.		קיום מנגנוני נעילה פיסית ולוגית של ממשקים במכשירים ובציוד קישוריות, לצמצום הסיכון לחבלות.	חיונית	X	X		X
7.		גישת פריווילגית למכשיר (לדוגמה: למנהלנים, טכנאי שירות, אנשי תחזוקה) מחייבת שימוש ב-Multi Factor Authentication ("הזדהות חזקה").	חשובה	X			X

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ולא אוגר מידע
8.		קיום אמצעים המאפשרים הימנעות משימוש בסיסמאות מקודדות מראש (Hardcoded Passwords). קיום מנגנונים המאפשרים הגבלת גישה ציבורית לסיסמאות שבהן נעשה שימוש לגישה פריווילגית למכשיר.	חיונית	X	X	X	X
9.		קיום מנגנוני הזדהות לפני ביצוע פעילויות רגישות: לפני אישור של עדכון תוכנה או קושחה.	חשובה	X	X	X	X
10.	הבטחת תוכן בר אמן	קיום מנגנונים המאפשרים אימות של קודים (Authenticated code) לעדכוני תוכנה או קושחה.	חשובה	X	X	X	X
11.		אפשרות שימוש בתהליכים שיטתיים למשתמשים מאושרים להוריד גרסת תוכנה/קושחה ברת זיהוי מהיצרן.	חשובה	X	X	X	X
12.		קיום מנגנונים המבטיחים מניעה של שינוי של מידע רפואי על ידי גורם לא מורשה כשהוא שמור במכשור הרפואי. קיום מנגנונים המבטיחים את פרטיות המידע של המטופלים כשהוא שמור במכשור הרפואי, כשהוא מודפס וכשהוא מוצג לקהל (באמצעות המכשיר	חיונית	X	X		

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
		עצמו). יש להשתמש לשם כך במנגנונים קריפטוגרפים.					
13.		קיום של מנגנונים המבטיחים מניעה של שינוי של מידע רפואי על ידי גורם לא מורשה בתהליך העברתו. קיום מנגנונים המבטיחים את פרטיות המידע של המטופלים בתהליך העברתו, כולל בעת הדפסתו והצגתו לקהל באמצעות החיבור הרשתי. יש להשתמש לשם כך במנגנונים קריפטוגרפים.	חיונית	X	X		
14.		באם ניתן לשמור מידע רפואי אישי במכשיר הרפואי נדרשת יכולת להציג בפני המשתמש את רמת סיווג המידע הנגיש, בהתאם לתקן 27799.	חשובה	X	X		
15.	מנגנוני אל כשל והתאוששות	קיום של מנגנוני אל כשל המגנים על תפקודים חיוניים של המכשיר, אפילו באם אבטחת המכשיר הועמדה בסיכון.	חשובה	X	X	X	X
16.		קיום של מנגנונים המאפשרים אתור, תיעוד ותגובה למצבים בהם אבטחת המכשיר מועמדת	חיונית	X	X	X	

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
		בסיכון Security (Compromises).					
17.		קיום יכולת לאושש את הגדרות המכשיר ע"י מנהלן מערכת מאומת.	חיונית	X	X	X	X
18.	ממשקים	מכשירים רפואיים שאינם נדרשים בקישוריות לא יכילו ממשקי תקשורת.	חיונית		X		X
19.		ממשקי תקשורת אלחוטיים יכילו אמצעים לפעולות לפחות בהתאם לתקנים הבאים, בהתאמה : WPA2, Bluetooth 2.1.	חיונית	X	X		
20.	תיעוד במסמכי טרום שיווק (להלן: מט"ש)	ניתוח סיכונים (Hazard analysis), אמצעי צמצום / הקלה / הפגה (Mitigations), ושיקולי תכנון המתייחסים לסיכוני הגנת סייבר מכוונים ("זדוניים") ושאינם מכוונים ("בשוגג"), הנלווים למכשיר, כולל: • רשימה מפורטת של כל סיכוני הגנת סייבר אשר נשקלו בתכנון של המכשיר. • רשימה מפורטת ומנומקת של כל הבקורות שיושמו עבור המכשיר.	חיונית	X	X	X	X

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
21.		מטריצת מעקב המקשרת בין בקורות הגנת סייבר בפועל לסיכוני הגנת סייבר שנשקלו.	חיונית	X	X	X	X
22.		אפיון של תוכנית שיטתית לאספקת עדכונים וטלאים מאומתים למערכות הפעלה, או לתוכנת המכשיר הרפואי, בהתאם לצרכים.	חיונית	X	X	X	X
23.		מענה לכלל השאלות המופיעות בקובץ MDS ²	חיונית	X	X	X	X
24.		הצהרה כי המכשיר מסופק כשהוא נקי מתוכנות זדוניות.	חיונית	X	X	X	X
25.		רשימת כלל התקנים הטכנולוגיים שעל פיהם פועל המכשיר הרפואי, לרבות תקנים הקשורים לממשקים במכשיר הרפואי.	חיונית	X	X	X	X
26.		הוראות הפעלה למכשיר ומפרט המוצר בהתייחס לתוכנת אנטי ווירוס מומלצת ו/או FIREWALL ו/או כל מנגנון אבטחת מידע המתאים לסביבת השימוש.	חיונית	X	X	X	X

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
27.		ממצאי בדיקות אבטחת מידע שבוצעו למכשור הרפואי ובקורות שיושמו לצמצום סיכונים, אם אלו נתגלו.	חשובה	X	X	X	X

8. הנחיות למוסדות רפואיים בתהליך הטמעת אבטחת מכשור רפואי

8.1 תהליך קליטת מכשור

8.1.1 דרישות אבטחת מידע וסייבר

הוראות אלו עניינן דרישות אבטחת מידע וסייבר למכשור רפואי

8.1.2 גופי ביצוע

הנדסה רפואית, מערכות המידע, ממונה אבטחת מידע וסייבר, ניהול הסיכונים ומנהלי הרכש במוסדות הבריאות.

8.1.3 שיטה

- כל מכשור רפואי חדש יובא לאישור הממונה אבטחת מידע וסייבר טרם אישור קליטתו בארגון. יחד עם בקשת האישור יש לצרף את כל המסמכים הרלוונטיים על-פי נספחים מצורפים לנוהל זה (ראה נספחים ג-ד).
- על הספק המכשור הרפואי להשיב ולהתייחס על כל סעיף וסעיף בקטגוריה הרלוונטית. **סעיף אשר לא תתקבל לגביו התייחסות, המכשיר לא יאושר.**
- בתהליך האישור יימצא אישור הציוד מבחינת הגנת המידע בחתימת הממונה על אבטחת המידע וסייבר או מי מטעמו יתקיים תיעוד מתאים להרשאות וסקרי סיכונים.
- החברה המספקת את המכשור על פי אחד מהסיווגים מהטבלה לעיל **תנעל את קונפיגורציה של המערכת** כך שלא יהיה ניתן לשנות את תצורת פעולת המערכת אלא על ידי ספק / יצרן המערכת בתאום עם גורמי אבטחת המידע והסייבר בארגון.

8.2 תהליך ניהול סיכונים:

מטרה: להבטיח הטמעת מכשור רפואי במוסד רפואי תוך שילוב ניהול סיכונים.

- הארגון הרפואי יבצע תהליך מיפוי מכשור רפואי ויתחזק המיפוי באופן שוטף. המיפוי יתייחס (בין היתר) לקבוצות הסיכון כפי המתוארות בסעיף ג' להלן.
- הערה: מוסד שבצע את הפעילות כחלק מתהליך הסמכתו לתקן אבטחת מידע בבריאות (27799), יסתמך על המיפוי שבצע ויוסיף התייחסות ע"פ סעיף ג' להלן.
- מוסד רפואי יבצע תהליך ניהול סיכונים עבור הטמעה של מכשור רפואי ברשת בהתאם לתקן IEC 80001, בנושאים הבאים:
- הגדרת ותיעוד תפקידים והרשאות.

(א) הגדרת ותיעוד מדיניות ותהליכים בניהול סיכונים.

- תכנון, יישום ותיעוד תהליך ניהול סיכונים.
- תכנון, יישום ותיעוד תהליך ניהול שינויים וניהול הגדרות.
- תכנון, יישום ותיעוד תהליך ניהול ניטור ואירועים.
- יישום תהליך בקרה של תהליכים במחזור החיים של רשת המשלבת מכשור רפואי.

(ב) בתהליך ניהול הסיכונים יש להתייחס לקבוצות הבאות של מכשור רפואי :

- מכשור שאיננו אוגר מידע באופן מקומי ואיננו מחובר לרשת תקשורת.
- מכשור שאוגר מידע באופן מקומי ואיננו מחובר לרשת תקשורת.
- מכשור שאיננו אוגר מידע באופן מקומי ומחובר לרשת תקשורת.
- מכשור שאוגר מידע באופן מקומי ומחובר לרשת תקשורת.
- סקרי סיכונים אבטחת מידע ומבחני חדירה מבוקרים לבקרת הרשת

מטרה: להבטיח עמידת מכשור רפואי וקישורו לרשת בדרישות מדיניות אבטחת המידע של המוסד ושל מתודולוגיות אבטחת מידע מקובלות בעולם.

(ג) מנהל אבטחת המידע ייזום סקרי אבטחת מידע של מערך המכשור הרפואי של המוסד.

א. מכשור רפואי בעל סיכון גבוה ייסקרו לפחות אחת ל – 18 חודש.

ב. לגבי מכשור רפואי אחר ההנהלה תקבע את תדירות הסקרים בהתאם לרגישות המערך.

- הסקרים יבחנו את נושאי הניהול ואת יעילות אמצעי ההגנה (כולל אמצעים פיזיים ולוגיים) שיושמו במוסד ואת רמת הגדרות אבטחת המידע במכשור הרפואי הן ברמת התשתית (ציוד ותווד תקשורת, מערכות הפעלה, בסיסי נתונים) והן ברמת האפליקציה (ברמת קוד מקור או חבילות תוכנה).
- המוסד יערוך סקרי אבטחת מידע לפני הטמעת שינויים משמעותיים במכשור הרפואי שהוגדר ע"י המוסד כבעל סיכון גבוה לפי הערכת הסיכונים, כאשר חלו שינויים משמעותיים במכשור רפואי זה או לפני הכנסת מכשור רפואי זה לשימוש תפעולי (Production).
- מנהל אבטחת המידע ייזום מבחני חדירה (Penetration Tests) הן ברמת התשתית והן ברמת היישום (אפליקציה) במידת האפשר בשיתוף ספקי המכשור והנציגים של יצרני המכשור או לחליפין שיתוף במבדקים שנעשים ע"י יצרני המכשור, המדמים ניסיונות פריצה ע"י פורצים מתוך ומחוץ למוסד, הן כמשתמש קיים והן כפורץ ללא חשבון קיים, למערך המכשור הרפואי. תדירות מבחני החדירה תיקח בחשבון את רגישות המערך. מכשור רפואי הפתוח לתווד תקשורת ציבורי, יעבור מבחני חדירה לכל הפחות אחת ל – 18 חודש.
- סקרי אבטחת המידע ומבחני החדירה התקופתיים ייערכו ע"י גורם מקצועי, עצמאי, בלתי תלוי וחיצוני למוסד.
- הנהלת המוסד תקיים דיונים על תוצאות סקרי אבטחת המידע ומבחני החדירה ותפעל למימוש המלצותיהם תוך פרק זמן סביר.

8.3 בקורות אבטחת מידע

8.3.1 ניהול תקשורת ותפעול

8.3.1.1 נוהלי תפעול ואחריות תפעול

מטרה: להבטיח פעולה רציפה ובטוחה של מכשור רפואי.

על מנת להבטיח פעולה רציפה ובטוחה של המכשור הרפואי יש צורך לעדכון מתמיד של גרסאות היצרן העדכניות. על מנת לעמוד בדרישה זו נדרש להגדיר מדיניות ותהליכים יש להתייחס לניהול מבוקר של שינויים בתפעול, בתשתיות ובמערכת. קיום תהליך להכנסת עדכונים וטלאים מאומתים למערכות הפעלה, או לתוכנת המכשיר הרפואי, בהתאם לצרכים.

יש ליישם תהליכים מבוקרים של תפעול המכשור הרפואי ואמצעי הקישור שלו לרשת הארגון ולתעדס בנוהל המתייחס בין היתר לנושאים הבאים: תהליכים, חלוקת אחריות, בקורות, טפסים.

8.3.1.2 הגנה מפני ניסיונות פגיעה

מטרה: להגן על שלמות, חיסיון ואמינות המידע והמכשור הרפואי ולמנוע פגיעה במטופלים.

- (א) על מנת להגן על סביבות המחשוב והתקשורת יבוצעו הפעולות הבאות:
1. הארגון יתקין, בנקודת הקישור של המכשור הרפואי לרשת, אמצעים מקובלים ונאותים המצמצמים את החשיפה לניסיונות פגיעה (כולל איתור, זיהוי ומניעת ניסיונות אלה). אמצעים אלו (אמצעי הבקרה) יגנו מפני פגיעה בשירותי המכשור הרפואי מפגיעה שמקורה ברשת הארגון ובשירותים ברשת הארגון מפני פגיעה שמקורה במכשור הרפואי, שימוש לא תקין במידע, במכשור הרפואי ובבסיסי הנתונים. דוגמא לאמצעים המצמצמים את החשיפה לניסיונות פגיעה הינה קיומן של מערכות לניהול בקרת גישה לרשת (NAC), לאיתור ניסיונות חדירה מהאינטרנט ומתוך רשת הארגון (IDS/IPS), מערכות לסינון תכנים (Content Filtering) וכדומה.
 - הארגון יעדכן את גרסאות מערכת ההפעלה של המחשבים השייכים למכשור הרפואי וגרסאות תוכנות ההפעלה של המכשור הרפואי בהתאם להוראות יצרן מערכת ההפעלה, להוראות יצרן המכשור הרפואי והערכת סיכונים אבטחת המידע.
 2. הארגון יעדכן את גרסאות טלאי אבטחת המידע של מערכת ההפעלה של המחשבים השייכים למכשור הרפואי ושל תוכנות ההפעלה של המכשור הרפואי בהתאם להוראות יצרן המכשור הרפואי ובהתאם להערכת סיכונים אבטחת המידע.
 3. הארגון יעדכן את גרסאות החומרה והתוכנה של אמצעי הבקרה השייכים לסביבת המכשור הרפואי בהתאם להוראות יצרן המכשור הרפואי ובהתאם להערכת סיכונים אבטחת המידע.
 - (ב) הארגון רשאי להשתמש באמצעי בקרה מקובלים ונתונים אחרים, ובלבד שמהות אבטחת המידע הנדרשת בסעיף זה לא תפגע.
 - (ג) על הארגון להתאים את אמצעי הבקרה המקובלים והנאותים בהתאם להתפתחויות הטכנולוגיות שישררו באותה עת, ולאיומים ולחשיפות הרלוונטיים לאותה תקופה, תוך התבססות על הוראות יצרן המכשור הרפואי.

8.3.1.3 זמינות נתונים ושירותים

מטרה: להבטיח זמינות של מידע חיוני, שירותי עיבוד מידע ושירותי תקשורת.

- (א) הארגון יישם כלים להבטחת זמינות מידע של מכשור רפואי, שירותי עיבוד מידע ושירותי תקשורת שהוגדרו כחיוניים בתהליך הערכת הסיכונים.
- (ב) לצורך כך ישקול הארגון שימוש בשירותי של מערכות ומכשור רפואי, ציוד קישוריות, אמצעי בקרה וכדומה, באמצעים מקומיים או דרך שירותים של ארגון אחר.
- (ג) הנהלת הארגון תגדיר דרישות גיבוי למידע של מכשור רפואי שהוגדר כחיוני בתהליך הערכת הסיכונים.
- (ד) מנהל אבטחת המידע יהיה אחראי על בקרת איכות הגיבויים.
- (ה) אמצעי הגיבוי ישמרו במקום מרוחק, מאובטח ומוגן בפני פגיעה באמצעים ובתוכנם.

8.3.1.4 תיחום השימוש בתשתיות מכשור רפואי

מטרה: להגדיר ולתחם את השימוש המבוצע בתשתיות מחשוב ותקשורת המספקות שירותים למכשור רפואי.

- (א) השירותים שיופקו על ידי ציוד מחשוב ותקשורת בסביבת המכשור הרפואי יוגבלו לשימוש במכשור הרפואי בלבד.
- (ב) אמצעי הבקרה בסביבת המכשור הרפואי יאפשרו צמצום החשיפה לפגיעה ברשת הארגון שמקורה בסביבת המכשור הרפואי וגם צמצום החשיפה לפגיעה בסביבת המכשור הרפואי שמקורה ברשת הארגון.

8.3.1.5 ניהול סביבת הרשת של המכשור הרפואי

מטרה: להבטיח את הגנת המידע והשירותים בסביבת הרשת של המכשור הרפואי.

- (א) קישור גורמים חיצוניים אל סביבת הרשת של המכשור הרפואי יתבצע באופן ריכוזי, דרך נקודות כניסה מבוקרות. לא תאושר התחברות אחרת.
- (ג) קישור של סביבת המכשור הרפואי לרשת הארגון יתבצע באופן ריכוזי, דרך נקודות כניסה מבוקרות. לא תאושר התחברות אחרת. ייושם מידור בין הסביבות השונות ברשת באמצעות חלוקה לוגית או פיזית של הרשת והגבלת אפשרות הקישור בין סביבות הרשת השונות. רמת המידור תיקבע בהתאם לרמת הרגישות של המכשור הרפואי, בהתאם **לתהליך הערכת סיכוני אבטחת מידע**.
- (ד) תיושם בקרה וסינון של תקשורת יוצאת ונכנסת אל סביבת המכשור הרפואי על פי הגדרות הארגון.
- (ה) תיושם בקרה על הפעילויות המתבצעות בסביבת התקשורת של המכשור הרפואי לאיתור אירועים חריגים כגון: חיבור לא מרשה, הכנסת התקנים חיצוניים וכו'. בנוסף לבקרה בדיעבד, תיושם בקרה בזמן אמת.

8.3.1.6 ניהול סביבת המחשוב של המכשור הרפואי

מטרה: להבטיח את הגנת המידע והשירותים בסביבת המחשוב של המכשור הרפואי ואת הגנת התשתית התומכת.

- (א) חיבור של התקן חיצוני למחשב של מכשור רפואי יבוצע בהתאם להוראות יצרן המכשור הרפואי בלבד. ממשקי התקנים חיצוניים במחשבים של המכשור הרפואי יבוקרו. לא יאושר כל חיבור של התקן חיצוני למחשב של מכשור רפואי שלא דרך ממשקי כניסה מבוקרים אלו.
- (ב) תיושם בקרה וסינון של מידע וקבצים יוצאים ונכנסים אל סביבת המכשור הרפואי על פי הגדרות הארגון.
- (ג) תיושם בקרה על הפעילויות המתבצעות בסביבת המחשוב של המכשור הרפואי לאיתור אירועים חריגים. בנוסף לבקרה בדיעבד, תיושם בקרה בזמן אמת.

8.3.1.7 תהליך העברת מידע רגיש בין סביבת המכשור הרפואי לרשת הארגון

מטרה: להגדיר את רמת האבטחה המינימלית הנדרשת להעברת מידע על פי סיווגו.

- (א) בהתייחס לרמות סיווג המידע שהוגדר בארגון בהתאם **לתהליך סיווג נכסי מידע**, יגדיר הארגון את דרישות אבטחת המידע ההכרחיות ליישום בתהליך העברת מידע השייך לסביבת מכשור רפואי.
- (ב) מידע רפואי המועבר יוגן באמצעים הולמים לשמירה על שלמות ואמינות הנתונים.
- (ג) קישוריות להעברת מידע בין רשת הארגון לסביבת המכשור הרפואי, או בכיוון השני, תבוקר באמצעי בקרה מקובלים על מנת לוודא כי המידע מועבר ליעדו בלבד.
- (ד) במידה והעברת המידע מבוצעת בתווך תקשורת ציבורי או בתווך אלחוטי:
1. מידע בעל סיווג יוגן באמצעים מקובלים לשמירת סודיות, אמינות ושלמות הנתונים.
 2. מידע רפואי אישי ומידע שסווג כבעל סיווג גבוה, בהתאם **לתהליך סיווג נכסי מידע**, יוגן במנגנוני הצפנה סטנדרטיים לשמירה על סודיות, אמינות ושלמות הנתונים.

8.3.2 בקרת גישה לוגית

8.3.2.1 אכיפת בקרות גישה

מטרה: לאכוף מדיניות בקרות גישה מ/אל המכשור הרפואי.

- (א) ייושמו מנגנונים ממוכנים לניהול בקרות גישה מ/אל סביבת המכשור הרפואי ומ/אל מערכת הניהול שלו.
- (ב) בקרות גישה יורכבו מאמצעי זיהוי ובקרת הנתבי בין גורם מורשה לסביבה.
- (ג) מדיניות בקרת גישה תיקח בחשבון מידור מתאים של הרשאות.
- (ד) יש לבנות מנגנוני התראה במטרה להתריע על גישה בלתי מורשית למכשור הרפואי בטווח הזמן האפקטיבי למענה

8.3.2.2 אמצעי זיהוי

מטרה: לזהות באופן חד ערכי כל מורשה גישה למכשור הרפואי.

- (א) ייקבעו אמצעי זיהוי למכשור הרפואי ולשירותים לצורך זיהוי חד ערכי (Unique User ID) של הגורם מורשה הגישה.
- (ב) אמצעי הזיהוי יהיו אישיים ולא יותר שיתוף של אמצעי הזיהוי.
- (ג) אמצעי הזיהוי יוחלו הן על מערכות, הן על עובדי הארגון והן על משתמשים אחרים (ספקים וכדומה) המתחברים למכשור הרפואי ומהמכשיר הרפואי לשירותים ברשת הארגון.
- (ד) לכל הפחות, אמצעי הזיהוי יורכבו משילוב של שם משתמש (User Name) וסיסמא, ממולת לשלב אימות 2FA.
- (ה) נתוני הזיהוי יישמרו חסויים (הן בתווך התקשורת והן במערכות השונות).
- (ו) למכשור רפואי מוגדר כבעלות סיכון גבוה, בהתאם להערכת סיכוני אבטחת מידע, הארגון יסקול שימוש באמצעי זיהוי חזק כמוגדר בנספח מונחים. יש להשתמש בטכנולוגיה המונעת אפשרות העתקה או שחזור הפריטים.
- (ז) ייקבע פרק זמן של אי פעילות (Session Time Out) במכשור הרפואי ובשירותים שאליו מתחבר המכשור הרפואי שלאחריו יופעל מנגנון ניתוק תקשורת שיחייב זיהוי מחדש של הגורם הניגש. במידה ומנגנון הניתוק מטיל מגבלה על פעילות בעלת אופי רציף, יש להתריע לפני ניתוק התקשורת.

8.3.2.3 ניהול הרשאות

מטרה: לוודא שהרשאות הגישה מ/ אל המכשור הרפואי מאושרות, מוקצות ומתוחזקות כראוי.

- (א) יוגדר תהליך רישום וביטול רישום להרשאות גישה למכשור הרפואי ולשירותים וכן להרשאות גישה מהמכשיר הרפואי לשירותים ברשת הארגון.
- (ב) מתן הרשאות גישה מ/אל מכשור הרפואי ושירותים יוגבל ויפוקח בהתאם לרגישות המכשור הרפואי ורגישות השירותים ברשת הארגון אליהם המכשור הרפואי פונה, ובהתאם להערכת סיכוני אבטחת מידע. חובה לנהל טבלת הרשאות לעובדים בהתאם לתפקידם ולמידע הנדרש להם לצורך ביצוע תפקידם. חובה לנהל טבלת הרשאות למכשור רפואי בהתאם לדרישות התפקוד התקין שלו ולמידע הדרוש לתפקודו התקין.
- (ג) הרשאות הגישה לכל העובדים והמכשירים הרפואיים ייבחנו לפי שיקול דעת ההנהלה. לכל הפחות, הפעילות תתבצע אחת לשישה חודשים במערכות בעלות סיווג גבוה.
- (ד) ניהול ההרשאות ייעשה ע"י מנגנון ממוכן לניהול הרשאות.
- (ה) יוגדר תהליך סקירת הרשאות גישה למכשור הרפואי ולשירותים וכן להרשאות גישה מהמכשיר הרפואי לשירותים ברשת הארגון תקבע מדיניות אחידה עבור סקירת גישות המשתמשים בארגון.
- (ו) יש לבחון את תהליכי הבקרה אחת לשנה כחלק מתהליך ניהול הסיכונים הכולל

8.3.2.4 בקרת גישה בין רשת הארגון לסביבת המכשור הרפואי

מטרה: לאכוף מדיניות בקרת גישה חזקה בגישה בין מכשור הרפואי לרשת הארגון.

- (א) בגישה מרשת הארגון לסביבת המכשור הרפואי, או בכיוון השני, נתוני ההזדהות ומידע רפואי אישי יוגנו בפני ציתות (הצפנה מקצה לקצה).
- (ב) בגישה מרשת הארגון לסביבת המכשור הרפואי, או בכיוון השני, תיושם בקרת גישה לוגית לסביבה, שתורכב מאמצעי זיהוי ובקרת הנתבי בין גורם מורשה לסביבה, תוך לקיחה בחשבון מידור מתאים של הרשאות.
- (ג) מחשבים ברשת הארגון המאפשרים בגישה לסביבת המכשור הרפואי יכילו אמצעים מקובלים ונאותים המצמצמים את החשיפה לניסיונות פגיעה בסביבת המכשור הרפואי (כולל איתור, זיהוי ומניעת ניסיונות אלה).

(ד) מחשבים בסביבת המכשור הרפואי המאופשרים בגישה לרשת הארגון יכולו אמצעים מקובלים המצמצמים את החשיפה לניסיונות פגיעה ברשת הארגון (כולל איתור, זיהוי ומניעת ניסיונות אלה) ובכפוף להוראות יצרן המכשור הרפואי.

8.3.2.5 בקרת גישה מרשת האינטרנט / רשת חיצונית לסביבת המכשור הרפואי

מטרה: לאכוף מדיניות בקרת גישה חזקה בגישה למכשור הרפואי דרך האינטרנט/תשתית תקשורת ציבורית.

- (א) נתוני ההזדהות למכשור הרפואי ומידע רפואי אישי יוגנו בפני ציתות (הצפנה מקצה לקצה).
- (ב) תיושם בקרת גישה לוגית לסביבת המכשור הרפואי, שתורכב מאמצעי זיהוי ובקרת הנתיב בין גורם מורשה לסביבה, תוך לקיחה בחשבון מידור מתאים של הרשאות.
- (ג) בגישה למכשור הרפואי לצורך ביצוע פעולות מהותיות ייעשה שימוש באמצעי זיהוי חזק, **לפי עקרונות אמצעי זיהוי**.
- (ד) בקישור עובדים, נותני שירות או סביבות תקשורת לסביבת התקשורת של המכשור הרפואי, תוודק התקשורת יאובטח בפני ציתות וזליגת מידע. במקרה של חיבור עובדים תאובטחנה גם תחנות הקצה.
- (ה) לא תותר גישה ישירה מרשת האינטרנט / רשת חיצונית לסביבת מכשור רפואי של הארגון, אלא דרך מערכת שער (Gateway) מאובטחת, הממוקמת באזור מפורז מחוץ לסביבת המכשור הרפואי, שתיזום את ההתקשרות לסביבת המכשור הרפואי בשם הגורם הפונה.
- (ו) הארגון יממשאופן הגישה מרחוק בהתייחס להערכת סיכוני אבטחת מידע, בהתאם לרגישות והסיכון לגישה מרחוק ובהתאם לגורם העושה שימוש (בהתאם למפורט במסמך). בקרת הגישה תכלול אמצעי זיהוי חזקים, הצפנת התוודק מקצה לקצה, הקפדה על מדיניות הרשאות נוקשה ויישום בקרות למניעה ואיתור של חריגות.
- (ז) במקרה והמכשור הרפואי מכיל אופן גישה מרחוק מובנה, על הארגון לבחון את אופן הגישה בהתאם **להערכת סיכוני אבטחת המידע** ולפעול בהתאם.
- (ח) כל הגורמים הניגשים יזוהו באופן חד ערכי מול סביבת המכשור הרפואי (בהתאם **לעקרונות אמצעי זיהוי**).
- (ט) ארגונים יעגנו בהתקשרויות, כי גורמים הניגשים מרחוק למכשור הרפואי יפעלו לאבטחת המחשבים שלהם, על מנת למנוע פגיעה במכשור הרפואי, וכן ינקטו אמצעים לצמצום הפגיעה משימוש באינטרנט ובקרות גישה.

8.3.2.6 בקרת גישה ממכשור רפואי לרשת הארגון דרך רשת האינטרנט / רשת חיצונית

מטרה: לאכוף מדיניות בקרת גישה חזקה בגישה ממכשור רפואי לרשת הארגון דרך האינטרנט / תשתית תקשורת ציבורית / רשת אלחוטית / רשת סלולרית.

- (א) נתוני ההזדהות ומידע רפואי אישי יוגנו בפני ציתות (הצפנה מקצה לקצה).
- (ב) תיושם בקרת גישה לוגית לרשת הארגון, שתורכב מאמצעי זיהוי ובקרת הנתיב בין גורם מורשה לסביבה, תוך לקיחה בחשבון מידור מתאים של הרשאות.
- (ג) בגישה של המכשור הרפואי לרשת הארגון לצורך ביצוע פעולות מהותיות ייעשה שימוש באמצעי זיהוי חזק, **לפי עקרונות אמצעי זיהוי**.
- (ד) תוודק התקשורת יאובטח בפני ציתות וזליגת מידע. במקרה של חיבור מכשור ארגוני הוא יאובטח.
- (ה) לא תותר גישה ישירה של מכשור רפואי מרשת האינטרנט / רשת חיצונית / רשת אלחוטית / רשת סלולרית לרשת הארגון, אלא דרך מערכת שער (Gateway) מאובטחת, הממוקמת באזור מפורז מחוץ לסביבת רשת הארגון, שתיזום את ההתקשרות לסביבת רשת הארגון בשם הגורם הפונה.
- (ו) הארגון יגדיר אופן גישה מאובטח בהתייחס **להערכת סיכוני אבטחת מידע**, בקרת הגישה תכלול אמצעי זיהוי חזקים, הצפנת התוודק מקצה לקצה, הקפדה על מדיניות הרשאות נוקשה ויישום בקרות למניעה ואיתור של חריגות.
- (ז) כל הגורמים הניגשים יזוהו באופן חד ערכי מול רשת הארגון (בהתאם **לעקרונות אמצעי זיהוי**).

- (ח) ארגונים יעגנו בהתקשרויות, כי מכשור רפואי ארגוני הניגש מרחוק לרשת הארגון יופעל בסביבה מאובטחת, על מנת למנוע פגיעה במערכות המידע של הארגון, וכן ינקטו אמצעים לצמצום הפגיעה מקישוריות לאינטרנט ובקורות גישה.
- (ט) גישה של מכשיר רפואי לרשת הארגון דרך רשת אלחוטית תמומש בהתאם להוראות משרד הבריאות בנושא קישוריות אלחוטית במוסדות רפואיים.

8.3.2.7 ניהול סיסמאות במכשור רפואי וברשת הארגון

מטרה: לאכוף שימוש בסיסמאות חזקות שתמנענה גישה של משתמשים לא מורשים אל המכשור הרפואי או גישה של מכשירים לא מורשים לרשת הארגון.

- (א) הארגון יגדיר מדיניות סיסמאות ויחילה בסביבת המכשור הרפואי וברשת הארגון.
- (ב) הסיסמא תהיה ידועה אך ורק למשתמש.
- (ג) הסיסמא הראשונית תוגדר ע"י המשתמש או תימסר לידי באופן חסוי. בכל מקרה, הסיסמא לא תימסר דרך רשת האינטרנט, רשת אלחוטית או דרך התשתית לה נדרשת הסיסמא להזדהות.
- (ד) במידה וסיסמא נמסרת למשתמש, יש לאמת ראשית את זהות המשתמש. המשתמש יחויב לשנות את הסיסמא בהתחברות הראשונה למערכת.
- (ה) סיסמאות לא ישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.
- (ו) סיסמא תבוטל מידית בכל מקרה של חשש לפגיעה בחשאינותה. לא יתאפשר לשחזר את הסיסמא.
- (ז) מורכבות הסיסמא, תוקפה ותחולתה לפי סוגי הקהל – עובדים, נותני שירותים וכדומה – ייקבעו בהתאם לתקנים מקובלים (כגון ת"י 1495). לדוגמא: הסיסמא תורכב משילוב של אותיות וספרות, לא יאופשר שימוש בתווים זהים רצופים, תוקפה יפוג לאחר 60 יום, המערכת תינעל לגישה לאחר 4 ניסיונות גישה כושלים וכדומה.
- (ח) סיסמאות ברירות המחדל בגישה לסביבת מכשור רפואי תשוננה בהתאם למדיניות הסיסמאות הארגון.

8.3.3 בקורות ומנגנוני קריפטוגרפיה (Cryptography)

מטרה: להגן על החיסיון, המהימנות או השלמות של המידע.

8.3.3.1 מדיניות שימוש בבקורות קריפטוגרפיה (Cryptography)

- (א) הארגון יפתח ויישם מדיניות שימוש במנגנוני קריפטוגרפיה (Cryptography) להגנה על מידע רגיש.
- (ב) הארגון יגדיר את סוגי המידע השונים הדורשים שימוש במנגנוני קריפטוגרפיה בהתאם לתהליך סיווג המידע שהארגון ביצע.

8.3.3.2 הצפנה (Encryption)

- (א) הארגון ישקול יישום מנגנוני הצפנה להגנה על חיסיון מידע בעל סיווג גבוה האגור באמצעי אחסון (קובץ, בסיס נתונים וכדומה), בהתאם לתהליך סיווג נכסי מידע.
- (ב) הארגון יישם הצפנה להגנה על חיסיון מידע בעל סיווג גבוה בתווך התקשורת מחוץ לארגון, בהתאם לתהליך סיווג נכסי מידע.
- (ג) בכל מקרה, יוצפנו כל סיסמאות הגישה לכל המכשור הרפואי וגם כל המידע הרפואי האישי (קצה לקצה).

8.3.3.3 חתימה דיגיטלית (Digital Signature)

- (א) הארגון ישקול יישום חתימה דיגיטלית להגנה על מהימנות ושלמות של מידע רפואי ומידע בעל סיווג גבוה, בהתאם לתהליך סיווג נכסי מידע.

- (ב) החתימה תיושם באופן שיאפשר לגופים מחוץ לארגון לזהות את בעלי החתימה הדיגיטלית באופן המקובל בסטנדרטים בין-לאומיים.
- (ג) בכל מקרה של ביצוע פעולות מהותיות ושינוי פרטים מהותי בסביבת המכשור הרפואי, על גבי האינטרנט/תשתית תקשורת ציבורית/אלחוטית, תיושם חתימה דיגיטלית באופן המבטיח את אימות זהות המשתמש.
- (ד) בכל מקרה של ביצוע פעולות מהותיות ושינוי פרטים מהותי ברשת הארגון על ידי מכשור רפואי, על גבי האינטרנט/תשתית תקשורת ציבורית/אלחוטית, תיושם חתימה דיגיטלית באופן המבטיח את אימות זהות המשתמש.

8.3.3.4 מנגנוני מניעת הכחשה (Non-Repudiation)

- (א) מנגנוני מניעת הכחשה ייושמו בכדי ליישב מחלוקות לגבי התרחשות או אי-התרחשות של אירועים או פעולות, כפי שיוגדר במדיניות אבטחת המידע של הארגון.
- (ב) בכל מקרה של ביצוע פעולות מהותיות הכולל מידע בעל סיווג גבוה דרך האינטרנט וחברות צד שלישי, יבוצע שימוש בשירות זה באופן המבטיח את אימות זהות המבצע.

8.3.3.5 נתיב בקרה (Audit Trail)

מטרה: לגלות פעילויות לא מורשות ולזהות את מקורן.

- (א) הארגון יקיים מנגנון נתיב בקרה לניטור ומעקב אחר ביצוע פעולות ושאליות במכשור רפואי וברכיבי תשתית שעליו הוא פועל, הן מתוך הארגון והן מחוצה לו.
- (ב) הארגון יקיים מנגנון נתיב בקרה לניטור ומעקב אחר ביצוע פעולות ושאליות במערכות ברשת הארגון על ידי מכשור רפואי, הן מתוך הארגון והן מחוצה לו.
- (ג) על ה-Log להכיל את הנתונים הרלוונטיים, כך שיתאפשר לגלות ניסיונות גישה ופעולות לא מורשות ולזהות את מקורן. נתיב הבקרה יכלול מידע לפחות על מהות הפעולה, מקור הגישה וזמן הגישה.
- (ד) פרק הזמן לשמירת קבצי התיעוד ייקבע בהתאם לרגישות המכשור הרפואי ולמערכות ברשת שאליו ניגש המכשור הרפואי כפי שנקבעה בתהליך הערכת סיכוני אבטחת מידע.
- (ה) כל ניסיון גישה כושל וחריג למכשור הרפואי או למערכות ברשת שאליו ניגש המכשור הרפואי ינוטר ויתועד במנגנון אירועים.
- (ו) הארגון יידע את עובדיו וספקיו בדבר ביצוע רישום פעילויותיהם בקובץ לוג.
- (ז) על שעון מנגנון הניטור להיות מסונכרן עם מקור שעון מדויק לצורך דיוק התיעוד.
- (ח) קבצי ה-Log יאובטחו בפני מחיקה, שינוי או קריאה בלתי מורשים.

8.3.3.6 קישור מכשור רפואי, עובדים ומערכות מידע המקושרות למכשור רפואי לאינטרנט

מטרה: למנוע חשיפת מידע רגיש אל מחוץ לסביבת המכשור הרפואי ולצמצם יכולת פריצה של גורמים לא מורשים אל סביבת המכשור הרפואי.

- (א) הנהלת הארגון תגדיר את השימושים המותרים למכשור רפואי, לעובדים ולמערכות מידע המקושרות למכשור רפואי לקישור לאינטרנט.
- (ב) למערכות מידע ולעובדים המקושרים למכשור רפואי, וצריכים להיות מקושרים לאינטרנט, הקישור לאינטרנט יתאפשר באחד מן האופנים הבאים:
1. רשת ייעודית מנותקת לוגית או פיזית מסביבת המכשור הרפואי – תתאפשר הורדת קבצים ברשת ייעודית, תוך נקיטת אמצעי בקרה נאותים בלבד. הארגון יגדיר במסגרת מדיניות אבטחת המידע את סוגי הקבצים המורשים להורדה באופן קישור זה.
 2. ממחשב שאינו מחובר לרשת (Stand Alone) – במקרה זה תתאפשר הורדת קבצים באופן מאובטח.
- (ג) הקישור לאינטרנט יאובטח בפני גישה בלתי מורשית מהאינטרנט, תוכנות זדוניות ושימוש בלתי תקין.

8.3.3.7 מידע במכשיר רפואי

מטרה: למנוע חשיפת מידע רגיש לגורמים לא מורשים בעלי גישה למכשור הרפואי.

- (א) יש לוודא עמידה בדרישות חוק הגנת הפרטיות
- (ב) במכשור רפואי המכיל מידע רפואי אישי יש ליידע את המשתמשים לגבי רמת סיווג המידע הנגיש.
- (ג) המכשור הרפואי לא יחשוף מידע פנימי שאינו נדרש למשתמש בזמן תקלה.
- (ד) באם ניתן לשמור מידע רפואי אישי במכשיר הרפואי נדרשת יכולת להציג בפני המשתמש את רמת סיווג המידע הנגיש, בהתאם לתקן ISO 27799.
- (ה) תובטח פרטיות המידע הרפואי האישי השמור במכשור הרפואי, כשמידע רפואי מודפס וכשמידע רפואי מוצג לקהל.

9. נספח א' - מסמכים נוספים בנושא אבטחת מידע:

9.1 חוקים/דירקטיבות

9.1.1 ארה"ב

9HIPAA 9.1.1.1

HIPAA - OMNIBUS 9.1.1.2

9.2.1 אירופה

9.2.1.1 לא נכתב עדיין

9.2.1.2 אסיה (סין, יפן, אוסטרליה)

9.2.1.3 לא נכתב עדיין

9.2 תקנים

ISO 9.2.1

9.2.2.1. תקנים נוספים.

Clinical Laboratory Standards Institute - CLSI 9.2.2

AUTO09-A:Remote Access to Clinical Laboratory Diagnostic 9.2.2.1

Devices via the Internet; Approved Standard

This document provides a standard communication protocol for instrument system vendors, device manufacturers, and hospital administrators to allow remote connections to laboratory diagnostic devices. The remote connections can be used to monitor instruments' subsystems; collect diagnostics data for remote system troubleshooting; and collect data for electronic inventory management.

<http://shopping.netsuite.com/s.nl/c.1253739/it.A/id.963/.f>

AUTO11-A: IT Security of In Vitro Diagnostic Instruments and Software 9.2.2.2 Systems; Approved Standard

This document provides technical and operational requirements as well as technical implementation procedures related to security of IVD systems (devices, analytical instruments, data management systems, etc.) installed at a healthcare organization.

<http://shopping.netsuite.com/s.nl/c.1253739/it.A/id.955/.f>

AUTO11 (Draft 2)—Information Technology Security of In Vitro 9.1.1.1 Diagnostic Instrument and Software Systems

מסמך הטיוטה איננו נגיש (12/11/2013).

10. נספח ב' - מהו מכשור רפואי, סוגי מכשור רפואי:

FDA 10.1

10.1.1 כללי:

1. מכשור רפואי, לפי הגדרת ה-FDA, כולל גם מערכת מידע מכשור רפואי – Medical Device Data System

(MDDS), וכן אפליקציות רפואיות לניידים – Mobile Medical Applications (25.9.2013)

הגדרות:

10.1.2 הגדרת ה-FDA למכשור רפואי – FDA Medical Device:

<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm>

10.1.3 מכשור רפואי הנו כלי (instrument), מכשיר (apparatus), מכונה (machine), מתקן

(contrivance), אביזר (contrivance), שתל (implant), חומר המשמש לריאקציה כימית מחוץ לגוף (in vitro reagent), או משהו דומה (or other similar or related article), כולל רכיב או תוסף (including a component part, or accessory) אשר:

- מוכרת ב: official National Formulary, or the United States Pharmacopoeia, or any supplement to them
- מיועד לשימוש בתהליך אבחון של מחלה, או מצבים אחרים, או בריפוי, טיפול, הקלה או מניעה של מחלה, באדם או חיות אחרות,
- מיועד להשפיע על המבנה או כל פונקציה של גוף אדם או כל חיה אחרת, ואשר איננו משיג את מטרתו הראשונית באמצעות פעילות כימית בתוך הגוף או על גוף אדם או חיה אחרת, ואשר איננו תלוי בביצוע חילוף חומרים על מנת להשיג ולו אחת ממטרותיה הראשוניות.

10.1.4 דוגמאות למכשור רפואי:

- דוחק לשון (Tongue depressor)
- קוצבי לב
- מתקני לייזר לניתוח
- מכשור מעבדה
- ציוד אבחון אולטרה סאונד
- ציוד רנטגן (כיום קרויות CR-Computerized Roentgen)

- ליזרים למטרות שימוש ברפואה.

10.1.5 ההגדרה מבטיחה:

- הבחנה ברורה בין מכשיר רפואי (Medical Device) והמוצרים האחרים אשר ה-FDA מהווה עבורם רגולטור, כדוגמת סמים/תרופות (Drug).
- במידה ומטרת השימוש הראשונית/העיקרית במוצר מושגת באמצעות פעילות כימית או באמצעות חילוף חומרים עם הגוף, המוצר מוגדר בדרך כלל כסם/תרופה (Drug).

10.1.6 סוגי המכשור הרפואי עפ"י ה-FDA:

<http://www.fda.gov/medicaldevices/deviceregulationandguidance/overview/classifyyourdevice/default.htm>

10.1.6.1 ה-FDA הגדיר סיווג לכ-1,700 סוגים גנריים שונים של מכשירים וקיבץ אותם ל-16 קבוצות רפואיות המכונות פאנלים ("panels").

10.1.6.2 כל אחד מ-1,700 הסוגים הגנריים של מכשירים מוגדר לאחד משלוש רמות סיכון (Regulatory classes) עפ"י הסכנה הנשקפת לבריאות הציבור בעקבות תקלות בציוד או כשלים בבטיחות הציוד. רמת הסיכון של הציוד הרפואי קובעת את הכללים והבקורות שיחולו על הציוד כדלהלן:

8.2.1.1.1 רמה 1 (Class I) – בקורות רגילות (general controls)

8.2.1.1.1 כולל פטורים (With Exemptions)

- ללא פטורים (Without Exemptions)

8.2.1.1.2 רמה 2 (Class II) – בקורות רגילות (general controls) ובקורות מיוחדות (Special Controls)

- כולל פטורים (With Exemptions)

- ללא פטורים (Without Exemptions)

8.2.1.1.3 רמה 3 (Class III) – בקורות רגילות (general controls) ואישור טרם שיווק (Premarket Approval).

10.1.6.3 רמת הסיכון אליה משתייך המכשיר מגדירה (בין היתר) את תהליך הטרם שיווק הנדרש מהיצרן על מנת לקבל את אישור ה-FDA למכשיר. עבור רמות 1 ו-2 ללא פטורים, נדרש מילוי טופס 510(k). למכשירים ברמה 3 נדרש אישור טרם שיווק (PMA-PreMarket Approval Application). החלוקה לרמות מבוססת סיכונים שהמכשיר מציב למטופל או למשתמש בו. הסיכון מהווה מרכיב חשוב מאד בקביעת הרמה אליה משויך המכשיר. רמה 1 כוללת את המכשירים המציבים את הסיכון הקטן ביותר, ואילו רמה 3, את המכשירים המציבים את הסיכון הגבוה ביותר.

10.1.6.4 הקבוצות רפואיות הן:

<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051530.htm>

Medical Specialty (Panels)

- 1 Anesthesiology
- 2 Cardiovascular
- 3 Chemistry & Toxicology
- 4 Dental
- 5 Ear, Nose, and Throat
- 6 Gastroenterology and Urology
- 7 General and Plastic Surgery
- 8 General Hospital
- 9 Hematology & Pathology
- 10 Immunology & Microbiology
- 11 Neurology
- 12 Obstetrical and Gynecological
- 13 Ophthalmic
- 14 Orthopedic
- 15 Physical Medicine
- 16 Radiology

10.1.6.5 מכשיר המסווג לרמה 1 (Class I) הכולל פטורים עדיין מחויב בבקורות רגילות הכוללות (בין היתר) רישום (Registration & Listing), תיוות (Labeling) ונהלי ייצור תקינים (Good Manufacturing Practice, למעשה - Quality System, מערכת הבטחת איכות).

10.1.7 הגדרת ה-FDA עבור מערכת מידע מכשור רפואי – FDA Medical Device Data System (MDDS):

10.1.7.1 מערכת מידע מכשור רפואי (MDDS) הנה מכשור המיועד לספק אחד או יותר מהשימושים הבאים, ללא בקרה או שינוי הפונקציות או הפרמטרים של מכשירים רפואיים מקושרים:

1. העברה אלקטרונית של נתוני מכשור רפואי,
2. אגירה אלקטרונית של נתוני מכשור רפואי,
3. הסבה אלקטרונית שנתוני מכשור רפואי מתבנית אחת לתבנית אחרת בהתאם קלסיפיקציות מוגדרות.
4. הצגה אלקטרונית של נתוני מכשור רפואי.

MDDS 10.1.7.2 עשוי לכלול תוכנה, חומרה חשמלית או אלקטרונית כגון: תווך פיזי לתקשורת (כולל תווך פיזי אלחוטי), מודמים, ממשקים, ופרוטוקול תקשורת. הגדרה זו איננה כוללת מכשירים שייעודם לפעול בהקשר של ניטור חולים אקטיבי.

MDDS 10.1.7.3 באופן מעשי, הינו מכשור רפואי המיועד לספק אחד או יותר מהפונקציות הבאות:

1. העברה או החלפה אלקטרונית של נתוני מכשור רפואי ממכשור רפואי, ללא שינוי בפרמטר או בפונקציונאליות של מכשור רפואי מקושר כלשהו. לדוגמה, סעיף זה יכול לכלול תוכנה האוספת נתונים ממכשיר לגבי רמות CO₂ אצל חולה ומשדרת את הנתונים למאגר נתונים מרכזי.
2. אחסון ואחזור אלקטרוני של נתוני מכשור רפואי, ללא שינוי בפרמטרים או פונקציונאליות של המכשור. לדוגמה: תוכנה האוגרת את היסטוריית רישומי לחץ הדם לבחינה מאוחרת יותר ע"י מטפל.
3. הסבה אלקטרונית של נתוני מכשור רפואי מתבנית אחת לאחרת בהתאם להגדרות שנקבעו מראש. לדוגמה, תוכנה הממירה נתונים דיגיטליים שיוצרו ע"י מכשיר oximeter לתבנית נתונים דיגיטליים שנתן להדפיסם.
4. הצגה אלקטרונית של נתוני מכשור רפואי, ללא שינוי של פונקציונאליות או פרמטרים במכשור רפואי. לדוגמה: תוכנה המציגה את הקרדיוגרם הקודם של חולה.

MDDS 10.1.7.4 ישנו הסבר מפורט מה איננו MDDS. הדוגמה הבולטת הנם רכיבי IT רגילים שבהם נעשה שימוש במערכת הבריאות ואשר לא שונו או הותאמו מעבר להנחיות של יצרניהם. אלו אינם נחשבים MDDS גם באם בתהליך העבודה הם מאחסנים, מעבדים, מעבירים בתקשורת או מסבים נתוני מכשור רפואי בנוסף למידע אחר. דוגמאות הנם: נתבים, האבים, נקודות גישה אלחוטיות, NAS, SAN, תוכנת PDF, צג מחשב, מסך גדול ועוד.

MDDS 10.1.7.4 הנו מכשור רפואי מרמה 1 (CLASS I) ופטור מהודעת טרום שיווק premarket (510(k) notification). המשמעות הנה שכל התוכנות והחומרות הכלולות בהגדרת MDDS עדיין מחויבים בבקורות רגילות הכוללות (בין היתר) רישום (Registration & Listing), תיוות (Labeling) ונהלי ייצור תקינים (Good Manufacturing Practice), למעשה - Quality System - מערכת הבטחת איכות.

10.1.8 הגדרת ה-FDA ליישום רפואי נייד – FDA Mobile Medical Application (APPS):

10.1.8.1 יישומים ניידים הנם תוכנות המורצות על טלפונים חכמים ומכשירי תקשורת ניידים אחרים. הם יכולים להיות גם אביזרים נלווים (accessories) המתחברים לטלפונים חכמים או מכשירי תקשורת ניידים אחרים או כשילוב של תוספת ותוכנה.

Mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software.

יישומים רפואיים ניידים הנם מכשירים רפואיים (Medical Devices) שהנם יישומים ניידים, עומדים בהגדרת מכשירים רפואיים, והנם תוספת (Accessory) למכשירי רפואי הנתון למשטר רגולטורי או הופכות פלטפורמה ניידת ומכשיר רפואי במשטר רגולטורי.

Mobile medical apps are medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device.

10.1.8.2 כיצד יפעל ה-FDA על מנת לנהל את היישומים הרפואיים הניידים? ה-FDA יפעיל גישת ניהול סיכונים מדורגת המתמקדת בקבוצה קטנה יחסית של יישומים ניידים העונים להגדרה של "מכשיר" וגם:

1. מיועדים לשימוש כאביזר נלווה למכשיר רפואי המצוי במשטר רגולטורי של מכשיר רפואי, או
 2. הופכים פלטפורמה ניידת למכשיר רפואי המצוי במשטר רגולטורי.
- מדיניות ה-FDA איננה מחייבת מפתחי יישומים רפואיים ניידים לפנות לקבלת הערכה מחודשת עבור שינויים מינוריים במוצר.

FDA's mobile medical apps policy does **not** require mobile medical app developers to seek Agency re-evaluation for minor, iterative product changes.

10.1.8.3 על קבוצת המוצרים הבאה, המהווה סיכון מינימלי למטופל, ה-FDA יפעיל תהליך של enforcement discretions ללא דרישה מהיצרנים להעביר מידע קדם שיווקי או רישום מוקדם ב- רישומי ה-FDA:

- מסייעים לחולים/משתמשים לנהל את מחלתם/מצבם באופן עצמאי ללא אספקה של הנחיות או עצות טיפוליות,
 - מספקים לחולים כלים פשוטים לארגן ולעקוב אחר מצבם הרפואי,
 - מספקים גישה קלה למידע הקושר למצב רפואי או טיפול,
 - מסייעים לחולים לתעד, להציג או להעביר בתקשורת מצבים רפואיים אפשריים לספקי שירות רפואי,
 - ממכנים פעולות פשוטות של ספקי שירות רפואי,
 - מאפשרים למטופלים או ספקים לקיים אינטראקציה עם מערכות רשומה רפואית אישית או רשומה רפואית אלקטרונית.
- Help patients/users self-manage their disease or condition without providing specific treatment suggestions;
 - Provide patients with simple tools to organize and track their health information;
 - Provide easy access to information related to health conditions or treatments;
 - Help patients document, show or communicate potential medical conditions to health care providers;
 - Automate simple tasks for health care providers; or
 - Enable patients or providers to interact with Personal Health Records (PHR) or Electronic Health Record (EHR) systems.

10.2 מתוך חוק ציוד רפואי התשע"ב - 2012 – מדינת ישראל:

10.2.1 "ציוד רפואי" – כל אחד מהמפורטים להלן, ולמעט תכשיר כהגדרתו בפקודת הרוקחים [נוסח חדש], התשמ"א-111981:

- (1) מכשיר המשמש לטיפול רפואי, וכן מכשיר או תוכנת מחשב הנדרשים להפעלת מכשיר כאמור; לעניין זה, "מכשיר" – לרבות אבזר, חומר כימי, מוצר ביולוגי או מוצר ביוטכנולוגי;

¹¹ דיני מדינת ישראל, נוסח חדש 35, עמ' 694.

(2) עדשות מגע;

(3) מכשיר חשמלי הפולט קרינה מייננת או בלתי מייננת המשמש לטיפול קוסמטי.

11.נספח ג' – טופס דוגמה לבחינת ממונה הסייבר בארגון לרכש ציוד רפואי:

בקשת אישור הגנת מידע וסייבר לציוד רפואי		
סימוכין – מס' בקשה:	שם ודגם המכשיר:	ממלא הטופס:
סוג הבקשה:	רמת מכשור:	
☐ פתיחת מספר בקשה למכשור בארגון ☐ התנסות ללא חיבור לרשת/שמירת מידע דמוגרפי ☐ התנסות עם חיבור לרשת/שמירת מידע דמוגרפי	☐ משקי ☐ מעבדתי ☐ טיפולי/דיאגנוסטי	
כללי		
תאריך:	שם יצרן:	שם ספק:
פרטי איש הקשר אצל הספק:		
שם:	כתובת מייל:	טלפון:
חיבור לרשת – סמן אחת או יותר מהאפשרויות הבאות:		
☐ המכשיר מיועד להתחבר לרשת בחיבור (Tcp/Ip): ☐ RJ45 – Ethernet ☐ USB ☐ Wifi ☐ Bluetooth ☐ Infra-Red ☐ אחר, פרט:	☐ המכשיר מיועד להתחבר בעזרת חיבור סיריאל (RS232) בלבד ל: ☐ Terminal Server ☐ מערכת מעבדות ☐ IMD Soft ☐ למכשיר יש יותר מיציאת תקשורת אחת. פרט סוגי יציאות וייעודן:	☐ המכשיר שולח/מקבל נתונים מ: ☐ PACS /RIS ☐ דמוגרפיה ☐ WebService ☐ תיק רפואי ☐ מערכת מעבדות ☐ אחר. פרט:

☐ המכשיר אינו מתחבר לרשת כלל ☐ המכשיר אינו מתחבר לרשת <u>כיום</u> אך קיימת אופציה לכך בעתיד. פרט:	☐ נדרש קישור אינטרנט לצורך תחזוקה: ☐ מהארץ ☐ מחו"ל
נתוני מטופלים – סמן אחת או יותר מהאפשרויות הבאות	
☐ המכשיר אינו מחזיק נתוני מטופלים מקומית וגם שולח אותם לרשת PACS ☐ ☐ תיקיית רשת ☐ תוכנה ייעודית ☐ אחר. פרט:	☐ המכשיר אינו מחזיק נתוני מטופלים מקומית ולא שולח אותם לרשת ☐ המכשיר שומר נתוני מטופלים מקומית בלבד
☐ המכשיר אינו מחזיק נתוני מטופלים מקומית וכן שולח אותם לרשת PACS ☐ ☐ תיקיית רשת ☐ תוכנה ייעודית ☐ אחר. פרט	

12. נספח ד' – טופס דוגמה לאישור ממונה סייבר בארגון לרכש ציוד רפואי:

אישור/דחייה – הגנת מידע וסייבר	
☐ המכשיר מאושר מבחינת הגנת מידע וסייבר (יש למלא את סעיף גורמים מאשרים)	☐ המכשיר אינו מאושר מבחינת הגנת מידע וסייבר
☐ המכשיר מאושר מבחינת הגנת מידע וסייבר בהתניות נוספות:	
☐ גורמים מאשרים הנדרשים לחתימה):	
שם מנהל מערכות מידע: _____ תאריך אישור הבקשה: _____	
שם ממונה אבטחת מידע וסייבר: _____ תאריך אישור הבקשה: _____	

שם מנהל סיכונים _____ תאריך אישור הבקשה: _____.
לתשומת לבכם:
• אישור זה נוגע רק לקונפיגורציה המפורטת מעלה. • בכל שינוי קונפיגורציה יש לפנות לאישור מחדש.
• אישור זה הוא אישור הגנת מידע בלבד. • לצורך חיבור לרשת הארגון יש לפנות לגורמי המחשוב המתאימים

נספח א: טבלת פירוט משמעויות למצבי כוונות

קטגוריה	מפרט תבחין	מצב כוונות א'	מצב כוונות ב'	מצב כוונות ג'
מרחב סייבר	התרעה סייבר	רענון נהלים לעובדים		
	כללית ו/או אירוע	הפעלת סיוע חיצוני –		
	סייבר שמיוחס	חברת מודיעין סייבר		
	לישראל			
מרחב סייבר	תקיפת סייבר	רענון נהלים לעובדים		
	מתוזמנת על ישראל	צמצום חשיפה		
מרחב סייבר	תקיפת סייבר בעולם	לאינטרנט		
	שיתכן שתזלוג	דריכת סיוע חיצוני IR		
	לישראל			
מרחב סייבר		הודעה לעובדים ורענון		
		נהלים		
		צמצום חשיפה לאינטרנט		
		למינימום הכרחי		
		ניטור מוקפד של נכסים		
		חיונים, כניסות/יציאות		
		מהרשת, מאפייני תעבורה		
		ברשת והקלטות ושמירת		
		לוגים ונתונים בהתאם		
		לנוהל היערכות למצב		
		סייבר		
		הפעלת הגנה פרואקטיבית		
		(Hunting)		
	התרעת סייבר	כוונות צוותים מקצועיים		
	קונקרטי	(אבטחת מידע/הגנת		
		סייבר, תשתיות תקשורת		
		ו-IT, אחרים) ב-פ' 1+		
		להגעה + זמינות כלל		
		המנהלים		
		רענון נהלי חירום סייבר –		
		כינוס צוות ניהול אירוע,		
		רענון ערוצי דיווח ושיטת		
		עבודה		
		מימוש הערכת מצב יומית		
		לפחות בראשות ר'		
		הארגון.		

		היערכות לחירום – חלוקת אמצעי תקשורת ופרטי תקשורת עדכניים, וידוא מצאי ציוד ומכשור חירום רפואי, מכשור רפואי מדגמי מנותק מהרשת רענון תכנית BCP ארגונית בדיקת תקינות ועדכניות הגיבוי (DRP) והכנת עזרים ידניים (אם נדרש) תדרוך צוותים רפואיים על היותם "בקרה מפצה" הפעלת סיוע חיצוני – חברת מודיעין סייבר דריכת כוננות של סיוע חיצוני IR כל האמור לעיל ובנוסף:
מרחב סייבר	פגיעת סייבר בנכס/ים חיוני/ים	הפעלת צוות IR בארגון וטיפול באירוע כל הצוותים המקצועיים בנוכחות 24/7 צוות ניהול אירוע בפעילות 24/7 עד לסיום. פעילות בהתאם להמלצות צוות IR והנחיות צוות ניהול אירוע (לדוגמא - ניתוק מלא מהאינטרנט / ניתוק כלל המכשור הרפואי / סיוע מארגונים רפואיים סמוכים). כל האמור לעיל עפ"י מצב כוננות ב' בתרחיש פגיעת סייבר בנכס חיוני ובנוסף: הפעלה מלאה של תכנית ה- BCP הארגונית סיוע והסתייעות בארגוני בריאות אחרים במגזר – על פי הנחיות משרד הבריאות מעבר לעבודה בנוהל חירום מלא לפי הנחיות משרד הבריאות
מרחב פיזי	פגיעה רחבה ו/או ממושכת בנכס/ים חיוני/ים תקלה פיזית בנכס חיוני	רענון נהלים לעובדים

מרחב פיזי	התרעה לאירוע ביטחוני רחב היקף	הפעלה עפ"י הנחיה של משרד הבריאות:
מרחב פיזי	אירוע ביטחוני חריג	רענון נהלים לעובדים צמצום חשיפה
מרחב פיזי	העלאת כוונות בצה"ל	לאינטרנט דריכת סיוע חיצוני IR
מרחב פיזי	פגיעה פיזית בשירותים חיוניים למשק	הודעה לעובדים ורענון נהלים צמצום חשיפה לאינטרנט למינימום הכרחי
מרחב פיזי	אירוע ביטחוני רחב היקף	ניטור מוקפד של נכסים חיונים, כניסות/יציאות מהרשת, מאפייני תעבורה ברשת והקלטות ושמירת לוגים ונתונים בהתאם לנוהל היערכות למצב סייבר
		הפעלת הגנה פרואקטיבית (Hunting)
		הפעלת סיוע חיצוני – חברת מודיעין סייבר
		כוונות צוותים מקצועיים (אבטחת מידע/הגנת סייבר, תשתיות תקשורת ו-IT, אחרים) ב-פ' + 1 להגעה + זמינות כלל המנהלים
		רענון נהלי חירום סייבר – כינוס צוות ניהול אירוע, רענון ערוצי דיווח ושיטת עבודה
		מימוש הערכת מצב יומית לפחות בראשות ר' הארגון.
מרחב פיזי	פגיעה פיזית רחבה ו/או ממשוכת בשירותים חיוניים למשק	כל האמור לעיל במצב חירום ב' ברמה הפיזי ובנוסף – היערכות לחירום – חלוקת אמצעי תקשורת ופרטי

תקשורת עדכניים, וידוא מצאי	מלחמה	מרחב פיזי
ציוד ומכשור חירום רפואי, מכשור רפואי מדגמי מנותק מהרשת		מרחב פיזי
רענון תכנית BCP ארגונית	מצב מיוחד בעורף / אירוע חירום אזרחי	
בדיקת תקינות ועדכניות הגיבוי		
(DRP) והכנת עזרים ידניים (אם נדרש)		
תדרוך צוותים רפואיים על היותם "בקרה מפצה"		
דריכת כוננות של סיוע חיצוני IR		

נספח ב': הערכת מצב סייבר

תכלית הערכת המצב בסייבר היא לסייע בפיתוח הבנת המשמעות של המתרחש על בסיס מידע ועובדות וחשיבה משותפת, ולאחר מכן הגדרת פעולות לביצוע. הערכת המצב תהיה בראשות הדמות הבכירה בארגון, או מי שהסמך לכך, במועד שנקבע מראש (למשל אחת לשבוע) או לנוכח הנסיבות, בהשתתפות דרג ניהולי בכיר (בדרך כלל צוות היערכות וניהול משבר) וגורמי מקצוע רלוונטיים אחרים. על הדיון עצמו להיות תמציתי ותכליתי. פורמט דיון הערכת מצב אמור להיות קבוע, תוך התאמות נדרשות למאפייני המצב. חלקו הראשון מורכב מהצגת תמונת המצב של כל המידע הכמותי והאיכותי הרלוונטי, הידוע בזמן נתון על המתרחש במרחב הסייבר ובמרחב הפיזי, והשלכותיו על הארגון. על מנת לייעל את הדיון, תמונת המצב צריכה להיות מתואמת עם הגורמים השונים לפני ביצועה, והיא כוללת שני רבדים:

א. תמונת מצב טכנולוגית: יעדי התקיפה ומועדיה, גורמי התקיפה ככל שידועים, נכסי סייבר שנפגעו (בדגש על נכסי סייבר חיוניים), השפעות על תהליכי ליבה ושירותים, סטטוס ההתמודדות עם התקיפה, קשר עם גורמים חיצוניים מקצועיים.

ב. בתמונת מצב לגבי היבטי המעטפת: לרבות השלכות על רציפות התפקוד והמשכיות עסקית, השלכות עסקיות-כלכליות, היבטי תקשורת ודוברות, היבטים משפטיים ועוד.

תמונת מצב סייבר (דוגמה)

דו"ח נכון לתאריך שעה _____		
נושא הדווח	תמונת מצב	פעולות שנקטו / מתוכננות
מועד התקיפה		
הגורם התוקף		
סוג המתקפה		
נכסי סייבר שנפגעו		
מטרות ודרישות התוקפים		
מידע ונתונים שזלגו		
שירותים/תהליכים שנפגעו		
פרסום ופומביות		
ממשקים עם גורמים מחוץ לארגון		
היבטי מעטפת		

בחלקו השני של הדיון, אל מול תמונת המצב, ייבחנו המשמעויות והחלופות ויתקבלו החלטות והמלצות לפעולה. לאחר מכן ייכתב סיכום של ההחלטות שהתקבלו ויופץ לגורמים הרלוונטיים, בדגש על משימות לביצוע.

סוגיות לדיון בהערכת מצב (לדוגמה)

היכולת להתמודד עם האירוע	סיוע מקצועי נדרש (ספקים/יועצים/ מומחים)	פעולות נדרשות מול גורמים חיצוניים, בדגש על רגולטור/ גורם מנחה	פעולות נדרשות מול לקוחות

משמעויות בהקשר היבטי כוח אדם	החלטות לגבי פעולות הקשורות באבטחה הפיזית	החלטות לגבי פעולות במערכות הממוחשבות (בדגש על נכסי סייבר חיוניים)	סדרי עדיפויות לאישוש תהליכי ליבה ושירותים
היבטים משפטיים	תקשורת ודוברות כלפי חוץ	הנחיות בהיבטי אבטחת מידע וביטחון	עדכון עובדים

פעולות לביצוע

לסיכום

דיון הערכת מצב

- תמציתי ותכליתי
- פורמט הדיון וההצגות בו מוגדרים מראש
- דגש על שינויים שאירעו מאז הדיון הקודם

עקרונות

שלבים

על מנת לייעל את דיוני הערכת המצב, תמונת המצב צריכה להיות מתואמת עם הגורמים השונים לפני דיון הערכת המצב

עדכון והבהרת משמעויות (פורמט קבוע מראש)

1. הצגת תמונת מצב טכנולוגית: ראש צוות ה- CSIRT / מנהל חדר מצב
2. השלמות בתחומים עיקריים: מנהלים מקצועיים רלוונטיים, דוברות, ייעוץ משפטי

1

קבלת החלטות

1. הצגת ההחלטות הנדרשות בנושאים העומדים על הפרק, והחלופות העיקריות
2. דיון על החלופות
3. קבלת החלטות על דרכי הפעולה

2

- סיכום מהיר בכתב של ההחלטות שהתקבלו
- הפצת הסיכום והמשימות לגורמים הרלוונטיים

3

נספח ג' : שאלון מידת היערכות למצבי משבר בסייבר (TOP10)

השאלון להלן מבוסס על התפיסה המובאת במסמך זה, והוא כלי עבודה להנהלת הארגון לבחינת מידת ההיערכות הארגונית למצבי משבר בסייבר. תוצאות השאלון מאפשרות לדרג את היערכות הארגון וללמד מהן הפעולות שעליו לעשות כדי לשפר את היערכותו.

אפשר להשתמש בשאלון כפי שהוא, או לבצע בו התאמות, כל ארגון ברמתו, ומומלץ שיבוצע על-ידי הגורמים האחראים בארגון לרציפות תפקוד והגנה בסייבר, לניהול סיכונים ולהיערכות לחירום. אפשרות נוספת היא להסתייע בגורם חיצוני אובייקטיבי שיבצע את תהליך הבחינה.

בהתאם לאופי הארגון מומלץ להגדיר פרק זמן לביצוע הבחינה (במוצע אחת לשנה), ובעקבותיה לבנות תוכנית לשיפור. השאלון מתבסס על רשימת נושאים ראשיים, ובהם חלוקה לנושאי משנה. על מנת להקל את מילוי התשובות ולאפשר צפייה נוחה בתשובות המתקבלות (כולל בצורה גרפית), אפשר לבנות את השאלון ב Excel - או בכלי אחר. הסבר על אופן חישוב הציון נמצא בסוף השאלון.

שאלון מידת היערכות למצבי משבר סייבר		תאריך	1/1/2019			
ר	מספר שאלה	שאלה	תשובה	ערך שאלה	ערך תשובה	ציון סופי של הנושא
ות ת ות ות ית ר ר	1	האם הוגדרו בארגון בעלי תפקידים ותחומי אחריותם להיערכות בעת שגרה, לקראת מצב משבר סייבר?	א. כן, בדרגים מקצועיים ובדרגי הנהלה	3.34%		0.00%
			ב. כן, בדרג מקצועי בלבד	1.66%		
			ג. כן, בדרג הנהלה בלבד	1.66%		
			ד. לא הוגדרו	0.00%		
	2	האם הוגדרו בארגון בעלי תפקידים ותחומי אחריותם בעת התרחשות משבר סייבר (פגיעה אפשרית בנכס סייבר הנובעת מפעילות מכוונת)?	א. כן, בדרגים מקצועיים ודרגי הנהלה	3.34%		
			ב. כן, בדרג מקצועי בלבד	1.66%		
			ג. כן, בדרג הנהלה בלבד	1.66%		
			ד. לא הוגדרו	0.00%		
	3	האם הוגדרו "תהליכי ליבה" בארגון (תהליכים שמבצע ארגון על מנת לממש את יעדיו המרכזיים ו/או יעדים שהוגדרו לו על ידי הרגולטור)?	א. הוגדרו תהליכי ליבה באופן מלא	3.34%		
			ב. הוגדרו תהליכי ליבה באופן נקודתי / חלקי	1.66%		
			ג. כן, בדרג הנהלה בלבד	0.00%		
4	האם הוגדרו נכסי סייבר החיוניים לארגון (על ידי הארגון או על ידי הרגולטור)?	א. הוגדרו נכסי הסייבר החיוניים באופן מלא	5.00%		0.00%	
		ב. הוגדרו נכסי הסייבר החיוניים באופן נקודתי / חלקי	2.50%			
		ג. לא הוגדרו כלל נכסי הסייבר החיוניים	0.00%			

		5.00%	א. מבוצעות באופן מלא, כולל תיקופן מעת לעת	האם מבוצעות בארגון בדיקות של ספקים ונותני שירות, לצורך זיהוי אימים וסיכונים על נכסי סייבר חיוניים ממערכות/שירותי הספקים?	5	
		2.50%	ב. מבוצעות באופן נקודתי / חלקי (רק בעת תחילת עבודה עם ספק חדש, או רק עבור חלק מהספקים)			
		0.00%	ג. לא מבוצעות כלל			
0.00%		5.00%	א. מבוצע לפחות פעם בשנה	באיזו תדירות מבוצע תהליך של ניהול סיכונים בסייבר בארגון?	6	
		3.33%	ב. מבוצע פעם ב-2-3 שנים			
		1.66%	ג. מבוצע פחות מפעם ב-3 שנים			
		0.00%	ד. לא מבוצע כלל			
		5.00%	א. מיושמות במידה רבה מאוד	שאלת בונוס: במידה שמבוצעים תהליכי ניהול סיכונים בסייבר (סעיפים א'-ג') בשאלה 6 באיזו מידה מיושמות ההמלצות של תהליכי ניהול הסיכונים?	7	
		3.75%	ב. מיושמות במידה רבה			
		2.50%	ג. מיושמות במידה בינונית			
		1.25%	ד. מיושמות במידה מועטה			
		0.00%	ה. לא מיושמות כלל			
		5.00%	א. במידה רבה מאוד	באיזו מידה ארגון נערך לפי תרחישי ייחוס לתקיפה עוינת בסייבר (תסריטים לפעילות נגד הארגון ואופן מימושם)?	8	
		3.75%	ב. במידה רבה			
		2.50%	ג. במידה בינונית			
		1.25%	ד. במידה מועטה			
		0.00%	ה. כלל לא			
0.00%		10.00%	א. מוגדרים באופן מלא	האם מוגדרים בארגון מצבי כוננות בסייבר?	9	
		5.00%	ב. מוגדרים באופן חלקי/נקודתי			
		0.00%	ג. לא מוגדרים כלל			
		2.50%	א. מוגדרים באופן מלא	שאלת בונוס: במידה שמוגדרים מצבי כוננות סייבר (סעיפים א'-ב' בשאלה 9), האם הוגדרו הסמכויות הניהוליות להכרזה ו/או לעדכון מצבי הכוננות?	10	
		1.25%	ב. מוגדרים באופן חלקי/נקודתי			
		0.00%	ג. לא מוגדרים כלל			
		2.50%	א. מוגדרים באופן מלא	שאלת בונוס: במידה שמוגדרים מצבי כוננות סייבר (סעיפים א'-ב' בשאלה 9), האם הוגדרו פעולות הנדרשות לביצוע בכל מצב כוננות?	11	
		1.25%	ב. מוגדרים באופן חלקי/נקודתי			
		0.00%	ג. לא מוגדרים כלל			

0.00%		3.33%	א. כן	12	האם ארגון עושה שימוש ב"תפיסה הלאומית להיערכות ולניהול מצבי משבר בסייבר" (מסמך שנכתב על ידי מערך הסייבר הלאומי)?
		0.00%	ב. לא		
		3.33%	א. כן	13	האם ארגון עושה שימוש בתורת הגנה בסייבר (כגון מסמך ה"תורה"ג" שהופץ על ידי מערך הסייבר הלאומי, או בתו"ל ייעודי אחר)?
		0.00%	ב. לא		
		3.33%	א. במידה רבה מאוד	14	באיזו מידה ארגון עושה שימוש בתקנים ושיטות עבודה מומלצות ("Best Practices") מטעם ארגון רשמי, כגון תקני ISO, GDPR, NIST, תקנות הגנת הפרטיות?
		2.50%	ב. במידה רבה		
		1.66%	ג. במידה בינונית		
		0.83%	ד. במידה מועטה		
		0.00%	ה. כלל לא		
		3.33%	א. כן, באופן מלא	15	אם ארגון מוגדר "משק לשעת חירום" או "מפעל חיוני", האם בוצע "ריתוק משקי" של עובדים אשר חיוניים להבטחת רציפות התפקוד שלו (המשכיות עסקית)?
		1.66%	ב. כן, באופן חלקי/נקודתי		
		0.00%	ג. לא בוצע		
		0.00%	ד. לא רלוונטי - לא מוגדר כמשק לשעת חירום/מפעל חיוני		
0.00%		3.33%	א. כן (אם ארגון אינו "משק לשעת חירום" או "מפעל חיוני" סכום תן את הציון 5% ולא 3.33%)	16	האם הוגדר בארגון צוות ייעודי בדרג ההנהלה לצורך היערכות וניהול משבר סייבר?
		0.00%	ב. לא		
		3.33%	א. כן (אם ארגון אינו "משק לשעת חירום" או "מפעל חיוני" סכום תן את הציון 5% ולא 3.33%)	17	האם הוגדר בארגון צוות תגובה בדרג המקצועי-טכנולוגי (Incidence Response Team) למתן מענה במקרה של משבר סייבר? (יכול להיות צוות פנימי או במיקור חוץ)
		0.00%	ב. לא		

0.00%		2.50%	א. רציפה או יומית	באיזו תדירות מבוצע גיבוי של נתונים?	18
		1.66%	ב. שבועית		
		0.83%	ג. חודשית ומעלה		
		0.00%	ד. כלל לא מבוצע גיבוי		
		2.50%	א. כן	האם לארגון יש טכנולוגיות לתיעוד וניטור פעולות במערכותיו הממוחשבות?	19
		0.00%	ב. לא		
		2.50%	א. כן	האם לארגון יש אתר DR (התאוששות מאסון) מופרד ומרוחק באופן פיזי מהאתר הראשי (לטובת גיבוי מערכות, מידע, והמשכיות עסקית)?	20
		0.00%	ב. לא		
		2.50%	א. במידה רבה מאוד	באיזו מידה ארגון ערוך ברמה הלוגיסטית לתמוך בכ"א הדרוש לטיפול במשבר סייבר (לדוגמה עבודה מרחוק, כלכלת עובדים ומזון, הסעות, דרכי תקשורת חלופיות וכו')?	21
		1.88%	ב. במידה רבה		
		1.25%	ג. במידה בינונית		
		0.63%	ד. במידה מועטה		
		0.00%	ה. כלל לא		
0.00%		2.50%	א. כן	לצורך מתן מענה לאירועי סייבר?	22
		0.00%	ב. לא		
		2.50%	א. כן	לצורך הכשרות והדרכות כוח אדם?	23
		0.00%	ב. לא		
		2.50%	א. כן	לצורך תרגול הארגון?	24
		0.00%	ב. לא		
		2.50%	א. כן	ביצוע ביקורות?	25
		0.00%	ב. לא		
0.00%		3.33%	א. כן, באופן תדיר (כולל רענונים)	האם מבוצעות הכשרות והדרכות לבעלי תפקידים בארגון (עובדים והנהלה), בנושאי העלאת מודעות ויצירת תרבות ארגונית?	26
		1.66%	ב. כן באופן מזדמן / נקודתי בלבד (לדוגמה בעת קליטת עובדים)		
		0.00%	ג. לא מבוצעות		
		3.33%	א. מבוצעים לפחות פעם בשנה	באיזו תדירות מבוצעים בארגון תרגילי סייבר?	27
		2.22%	ב. מבוצעים אחת ל-2-3 שנים		
		1.11%	ג. מבוצעים פחות מפעם ב-3 שנים		
		0.00%	ד. לא מבוצעים כלל		

		2.00%	א. כן	שאלת בונוס: אם מבוצעים תרגילי סייבר, האם דרג ההנהלה משתתף בתרגילים אלו?	28	
		0.00%	ב. לא			
		2.00%	א. כן	שאלת בונוס: אם מבוצעים תרגילי סייבר, האם גורמים מקצועיים טכנולוגיים משתתפים בתרגילים אלו?	29	
		0.00%	ב. לא			
		2.00%	א. כן	שאלת בונוס: אם מבוצעים תרגילי סייבר, האם גורמי חוץ משתתפים בתרגילים אלו?	30	
		0.00%	ב. לא			
		3.33%	א. מבוצעות לפחות פעם בשנה	באיזו תדירות מבוצעות בארגון ביקורות (פנימיות או חיצוניות), בנושא סייבר?	31	
		2.22%	ב. מבוצעות פעם ב-2-3 שנים			
		1.11%	ג. פחות מפעם ב-3 שנים			
		0.00%	ד. לא מבוצעות			
	0.00%		3.33%	א. כן	האם לארגון יש תוכנית כתובה (נוהל) לניהול משברי סייבר?	32
			0.00%	ב. לא		
			3.33%	א. כן	האם הוגדרו בארגון אנשי קשר לדיווח במקרה של התפתחות משבר סייבר (מיהם האנשים שעמם יוצרים קשר בתוך הארגון ומחוץ לו – רגולטור, שותפים, לקוחות, ואיך ליצור את הקשר)?	33
			0.00%	ב. לא		
			3.33%	כן	האם מוגדרות בארגון פעולות לחזרה לשגרה והפקת לקחים בעת התאוששות ממשבר סייבר (אופן גיבוש לקחים והטמעתם)?	34
			0.00%	לא		
0.00%		ציון מסכם:				

ציון מקסימלי אפשרי כולל בונוס: 116%

אופן חישוב הציון

הציון המרבי בשאלון הינו $100\% + 16\%$ "בנוס" = 116% .

החישוב בכל חלק מתבצע על ידי סכימה של ערך התשובה אותה הארגון מדין (עמודה H).

הערה: בנושא "כוח אדם", יש שאלה לגבי "משק לשעת חירום" ו"מפעל חיוני" (שאלה 15) עם תשובה אפשרית של "לא רלוונטי". אם א לשעת חירום" או "מפעל חיוני", יש לבצע סכימה לפי שתי השאלות הנותרות (16+17 בלבד), והניקוד המרבי לכל אחת מהן הוא 5% . אם לשעת חירום" או "מפעל חיוני", תבוצע סכימה של סך הנקודות עבור כל שלוש השאלות בסעיף (15-17), וכל שאלה מקבלת ניקוד כדי לקבל את הציון הכללי לשאלון, סוכמים את כלל האחוזים, על פני כלל הסעיפים (מחושב אוטומטית).

הסבר לדוגמה, סעיף מצבי כוננות בסייבר (שאלות 9-11 בשאלון)

סעיף "מצבי כוננות בסייבר" מקנה לכל היותר $10\% + 5\%$ בנוס. לכן בעבור הבחירות המתוארות מטה (מסומנות בצהוב), יקנה הסעיף $1.25\% + 1.25\%$

9. האם מוגדרים בארגון מצבי כוננות בסייבר?

א. מוגדרים באופן מלא $[10\%]$

ב. מוגדרים באופן חלקי/נהדתי $[5\%]$

ג. לא מוגדרים כלל $[0\%]$

10. שאלת בנוס: במידה שמוגדרים מצבי כוננות בסייבר (סעיפים א'-ב' בשאלה 9), האם הגדרו הסמכויות הניהוליות להכרזה ו/או

א. הגדרו באופן מלא $[2.5\%]$

ב. הגדרו באופן חלקי/נהדתי $[1.25\%]$

ג. לא הגדרו $[0\%]$

11. שאלת בנוס: במידה שמוגדרים מצבי כוננות בסייבר (סעיפים א'-ב' בשאלה 9), האם הגדרו הפעולות המדרשות לביצוע בסייבר

א. הגדרו באופן מלא $[2.5\%]$

ב. הגדרו באופן חלקי/נהדתי $[1.25\%]$

ג. לא הגדרו $[0\%]$

ניהול סיכונים סייבר בשרשרת אספקה

13 מדיניות ניהול סיכונים סייבר בשרשרת אספקה

פרק א': כללי

קהל יעד

- 1.1. מנהלי ארגוני בריאות בישראל.
- 1.2. מחלקת משאבי אנוש, הייעוץ המשפטי, הרכש, שעת חירום, התשתיות וההנדסה הרפואית וגורמי הרפואה הרלוונטיים בארגוני הבריאות ויחידות הסמך
- 1.3. מנהלי מערכות מידע בארגוני הבריאות ויחידות הסמך.
- 1.4. מנהלי אבטחת מידע והגנת הסייבר בארגוני בריאות ויחידות הסמך.

מטרות ויעדים

בשנים האחרונות חל גידול משמעותי במספר תקיפות הסייבר ועוצמתם על ארגונים. מקורן של חלק משמעותי מתקיפות אלו, הוא בשרשרת האספקה של הגוף המותקף.

- מערך הבריאות עושה שימוש רחב בשירותיהם של גופים חיצוניים. דבר המעמיד את הארגון אל מול סיכונים ואיומים חדשים הכוללים, בין היתר:
- גישה של עובדים של חברות זרות לנכסים ארגוניים, דליפה או שיבוש של מידע;
- שיבוש פעולתה של מערכות או ציוד רפואי על ידי גורמים בלתי מורשים;
- השפעה על מערכות תשתית בכללן מערכות שליטה ובקרה, כיבוי, שיבוש והשחתה;
- השפעה על מלאים, פגיעה בתהליכי המשכיות עסקית ומערך שעת חירום
- הכנסה של קוד עוין בשלבי פיתוח תוכנה או בשלבי עדכוני תוכנה;
- שימוש בשרשרת האספקה כווקטור תקיפה בשוגג או בזדון.

מסמך זה מתווה את מדיניות משרד הבריאות בנושא ניהול סיכונים סייבר בשרשרת האספקה.

על כל ארגון רפואי לגבש מדיניות ונהלים התואמים למתווה המוצג במסמך זה.

הגדרות

3.1 **שרשרת אספקה** – קבוצת משאבים ותהליכים הקשורה לספקים, רוכשים וקבלני ביצוע הדרושים לתהליך הפיתוח, הייצור, הטיפול, האחסנה והמשלוח של מוצרים ושירותים לארגון הבריאות וטיפול בהם בכל מקום במחזור החיים שלה בכללם ביצוע תהליכי הגריטה וגריטה של אמצעים מגנטיים, מחשוב וציוד רפואי, ספק ישיר של שירות או מוצר לארגון רפואי וכל ספק או יצרן הקשור בעקיפין לשירות ו/או המוצר המסופקים לארגון הרפואי בין אם בחצרות הארגון או מחוצה לו.

3.2 **ספק מהותי/קריטי** – ספק המספק שירותים כגון: תמיכה ו/או תחזוקת מערכות מידע, אחסון נתונים רגישים מחוץ לחצרות התאגיד, שירותי מיקור חוץ טכנולוגיים, וכד' (נב"ת 363 ס' 7) כזה שפגיעה בו עלולה לגרום לנזק מהותי עבור הארגון - כל ספק של שירות ו/או מוצר, שהפרעה באספקתו הסדירה, בתחזוקה שלו, בשדרוגו או בפעולתו התקינה (עד כדי השבתה) עלולה לשבש תהליכים מהותיים בארגון הרפואי. החלטה על הגדרת ספק כמהותי נתונה לשיקול דעתו בהתאם לפוטנציאל הנזק לארגון (המחושב לפי טבלה בסעיף 5.4 במסמך זה).

סמכויות ואחריות

פרק זה מפרט את הגורמים העיקריים המעורבים בניהול תהליכי העבודה עם ספקים, ובמסגרתו מפורטים הסמכות והאחריות של כל גורם בכל אחד משלבי בחירת הספק, קביעת דרישות אבטחת המידע והגנת הסייבר בהתאם לרמת הסיכון הנובע משילוב הספק בתהליכי העבודה בארגון הרפואי.

על כל ארגון להתאים את הגדרת הגורמים, הסמכויות והאחריות לאופיו, דרכי פעולתו ובעלי התפקידים בו.

מנהל הארגון

למנהל הארגון אחריות כוללת לשמירה על הרציפות התפקודית וטיפול בסיכוני סייבר לרבות של שרשרת האספקה בשגרה ובחירום.

לשכה משפטית

באחריות הייעוץ המשפטי:

- להעניק יעוץ וליווי משפטי להסדרת תהליכי שרשרת האספקה בארגון.
- לוודא עמידת הארגון בדרישות החוק והתקנות הרלוונטיות (ראה נספח חוקים, תקנות והנחיות, ראה נספח בסעיף 10 ובהתאם לעדכונים מעת לעת)
- לנסח לבקר ולאכוף את חוזי הרכש ואספקת השירותים לוודא קיומן של דרישות אבטחת מידע והגנת הסייבר כחלק מכל מכרז והסכם עסקי עם כל גורם בשרשרת האספקה.
- לסייע בהסדרת התקשרויות וחוזים קיימים ובחינת הפערים ליישום התהליך בארגון
- לוודא קיום התחייבות חוזית לזמינות הספק (SLA- Service Level Agreement) בהתאם לסוג השרות ודרישה לזמינות והגעה לתחזוקה ועדכון גרסאות תוכנה, השלמת מלאים של מוצר מתן שירותים, כ"א וכדומה בהתאם לדרישות הארגון.
- לוודא קיום אפשרות שיתוף סקרי הספקים (שאלונים ותוצאות בודק) – עם משרד הבריאות וגורמים נוספים במגזר הבריאות העשויים להיות מושפעים מאותו ספק בין אם קיימת התקשרות חוזית או קיימת כוונה להתקשרות עתידית
- לוודא קיום התחייבות חוזית בנושא תהליכי דיווח על אירועי אבטחת מידע וסייבר בטווח הזמן הסביר הנדרש לארגון לקיום תהליכי תגובה וצמצום החשיפה.
- לוודא התחייבות חוזית לביצוע בדיקות וסקרי אבטחת מידע וסייבר עצמאיים וכן היתר לביצוע סקרים ובקרה עצמית באמצעות הארגון או מי מטעמו בכפוף להודעה מוסכמת.

המערך הרפואי

באחריות המערך הרפואי:

- לסייע בביצוע ניתוח של רמת התלות בספקי המערך הרפואי וסיווג רמת הקריטיות לשמירת הרציפות התפקודית וכחלק מתהליך ניהול סיכונים;
- להכיר את תהליכים ונהלי העבודה שיוגדרו בארגוני הבריאות בשגרה ובחירום.

רכש

באחריות הרכש :

- לוודא קיומן של דרישות אבטחת מידע והגנת הסייבר כחלק מכל התקשרות בין אם במכרז ואו בכל הסכם עסקי עם כל גורם בשרשרת האספקה.
- הגדרה וסיווג של ספקים מהותיים בסיוע אבטחת מידע והגנת הסייבר בהתאם לקריטריונים ולרמת הנזק הפוטנציאלי משיבוש או פגיעה במימוש השירותים הניתנים ע"י הספק
- לוודא עמידת הספקים בתקן אבטחת מידע-ISO 27001 בהתאם להוראות חוזר המנהל הכללי של משרד הבריאות, מס' 3/15. וכן עמידה באישור גופי ההסמכה מטעם מערך הסייבר לשרשרת האספקה כתנאי לתחילת תהליך ההתקשרות.
- לוודא זמינות הספק (SLA- Service Level Agreement) בהתאם לסוג השרות ודרישה למלאים של מוצר, שירותים, כ"א וכדומה.
- לנהל תהליך סדור של מיפוי כלל הספקים בארגון

דירוג הספק	רמת הנזק הצפוי לארגון מהספק	פגיעה ברציפות עסקית	רגישות המידע הנגיש לספק	נוק כלכלי לארגון	סבירות להתממשות אירוע
C	נמוך	התאוששות מאירוע אצל הספק תיקח מספר שעות	מידע בעל רמת רגישות נמוכה	עשרות אלפי שקלים	תלות נמוכה בסייבר.
B	בינוני	התאוששות מאירוע אצל הספק תיקח מספר ימים	מידע בעל רגישות בינונית	מאות אלפי שקלים	תלות בינונית בסייבר בהתקשרות עם הספק
A	גבוה	התאוששות מאירוע אצל הספק תיקח מספר שבועות	מידע עסקי/מידע רפואי	מעל מיליון ₪	ספק בעל תלות גבוהה בסייבר.

הווה אומר, ספק אשר קיבל בקריטריון אחד לפחות רמת סיכון A, יוגדר כספק מהותי והארגון והספק יפעלו בהתאם לרמת סיווג זו.

- **ספקים אשר דורגו ברמה A** – יידרשו להוכיח את רמת ההגנה שלהם עפ"י דרישות שאלון הספקים באמצעות בודק ספקים/גורם בדיקה מוסמך. לצפייה ברשימת גורמי הבדיקה המוסמכים, ראה רשימה באתר המערך ובמודול האסדרה.
- **ספקים אשר דורגו ברמה B** – יידרשו לענות על השאלון לרבות צירוף הראיות הנדרשות בשאלון. את הראיות הספק יעביר ללקוח בערוץ בטוח שיסוכם בין הצדדים.

- **ספקים אשר דורגו ברמה C** – ימלאו את שאלון הספקים ויחתימו עורך דין או את מנכ"ל החברה על הצהרת הספק לגבי רמת עמידתו בדרישות ההגנה שבשאלון.

טכנולוגיות מידע והנדסה רפואית

באחריות גופים אלה, כל אחד בתחומו:

- לוודא כי כל ציוד או שירות חדש הניתן לצוות עובר תהליך אישור של הגוף האחראי על אבטחת המידע והגנת הסייבר;
- להוות קשר מקצועי עם ספקי הציוד, המחשוב או התמיכה ולוודא כי העבודה מתבצעת בהתאם להנחיות אבטחת המידע;
- לדרוש עדכון שוטף מיצרנים ספקים ונותני שירות בנוסף בכל אירוע או לחליפין עדכון תוכנה או חומרה נדרש לבצע תהליך ניהול שינויים מתואם עם הנהלת ביה"ח ואבטחת המידע והסייבר.
- לעדכן באופן שוטף בדבר התקשרות עם ספק חדש או קבלת מוצר / שירות חדש מספק קיים.
- להצביע על ספקים חליפיים לציוד הרפואי

אבטחת מידע והגנת הסייבר

- הגדרת מדיניות ונהלים מפורטים לגבי סיווג ספקים ודרישות ספציפיות לאבטחת המידע;
- סיווג הספקים וקביעת פוטנציאל הנזק בסיוע הרכש, מערכות מידע ו/או הנדסה רפואית, תשתיות שליטה ובקרה (ICS), גורמי הנהלה ושע"ח (בהתאם לטבלה מצורפת בגוף ההנחיה);
- ביצוע סקרי ספקים בהתאם למדיניות ודרישות חוזר מנכ"ל לעמידה בתקנים ISO- 27001, ISO- 27799 וכן תהליכי ההתעדה שגובשו במערך הסייבר הלאומי במטרה להסדיר את תהליך ניהול סיכונים סייבר הנובעים משרשרת האספקה.
- ביצוע מעקב אחר תיקון ליקויים המתגלים בסקרי ספקים ודיווח ליחידת הסייבר המגזרית וגורמים נוספים בהתאם לאופי הליקויים והשפעתם (יעוץ משפטי, הרשות להגנת הפרטיות ומערך הסייבר).
- בנייה ותיקוף תכונות עבודה בנושא הסדרת שרשרת האספקה הארגונית והדרישות להתעדה בכפוף למתודולוגיה של מערך הסייבר הלאומי, בהתאם ללוחות הזמנים המפורטים בגוף ההנחיה ודיווח ליחידת הסייבר המגזרית של משרד הבריאות לגבי התקדמות התוכנית וממצאים.
- דיווח ל CERT משרד הבריאות ורשות להגנת הפרטיות לגבי כל חשד לאירועי סייבר הקשורים במישרין או בעקיפין לספקי הארגון ועשויים לחשוף את הארגון לפגיעת סייבר בטווח הזמן המידי.

יחידת הסייבר המגזרית במשרד הבריאות

באחריות יחידת הסייבר המרכזית של משרד הבריאות:

- לפרסם מדיניות והנחיות מקצועיות בנושא ניהול סיכונים סייבר בשרשרת האספקה;

- לרכז את הידע המקצועי בנושא התמודדות עם סיכונים סייבר בשרשרת האספקה, להפיץ ולשתף את הגופים השונים בידע זה;
- קבלה, איסוף וניתוח של מידע רוחבי לגבי ספקים מרכזיים של המגזר.
- קיום תהליכי אכיפה לספקים קיימים ותמיכה בתהליכי ההתעדה עבור ספקים הנמצאים בהתקשרויות עם ארגונים.
- החרגה של מועדי הגשה בהתאם לפנייה של הנהלות הארגונים לאחר הגשה של ניתוח הסיכונים ותוכניות העבודה באשר למימוש תהליכי ההסדרה.

מיפוי וסיווג ספקים

יש לזהות את הספקים הקריטיים שהארגון עובד איתם ולקבוע קריטריונים לסיווגם. להלן סיווג אפשרי:

- ספקי שירותי כוח אדם שלעובדיהם אין גישה ישירה למידע רגיש;
- ספקי שירותי כוח אדם שלעובדיהם גישה למידע ו/או שירות טכנולוגי רגיש (בתוך הארגון);
- ספקים חיצוניים מוצר, שרות, ענן אשר כשל או הפרה בהם עלולים לגרום להשפעה מהותית על הפעילות של ארגון הבריאות או לפגיעה בלקוחות הארגון (באופן ישיר או עקיף);
- ספקים אשר יש להם גישה מרחוק למערכות הארגון.
- בעלי נגישות למידע רגיש (רפואי/אישי)
- בעלי נגישות Online למערכות רפואיות ו/או למערכות המידע
- בעלי נגישות למידע שאינו רגיש
- בעלי נגישות Offline (ללא חיבור לארגון ובאחזקת הספק) למערכות רפואיות/מידע
- בעלי נגישות למערכות אחרות שאינן מחוברות למערכות רפואיות/מידע
- חסרי מידע ו/או חסרי נגישות

דרישות מגורמים בשרשרת אספקה

מסגרת ניהול אבטחת מידע

- על כל ספק קריטי למנות גורם האחראי לאבטחת המידע;
- על כל ספק קריטי להגדיר וליישם מדיניות אבטחת מידע והגנת הסייבר.
- עבודה מול ספקים קריטיים תתבצע רק מול גורמים העומדים בתקן בינלאומי לאבטחת מידע - ISO 27001 ואו בתקן אבטחת מידע במוסדות בריאות ISO 27799 בהתאם להוראות חוזר המנהל הכללי של משרד הבריאות, רגולציית יסוד להגנת סייבר במערכת הבריאות בישראל..
- עמידה בדרישות מתודולוגיה לניהול סיכונים בשרשרת אספקה של מערך הסייבר הלאומי לגבי סיווג והסמכת ספקים עבור גופי תשתית מדינה קריטית (תמ"ק) וגופי הנחיה מגזריים ויחידות סמך.
- יש למפות כלל הספקים ולדרגם בהתאם לטבלה המצורפת בסעיף 7.7.102022.
- עמידה בדרישות המדיניות הלאומית להזדהות בטוחה.

- ספקים אשר עומדים לפני חידוש שירות או ספקים אשר עומדים לפני חתימה על חוזה עבודה מול הלקוח יהיו בעדיפות ראשונה לסקר ובחינת הדרישות המפורטות בהנחיה.
- בכל התקשרות, מכרז עתידי ובפרט לגבי כל התקשרות שתתבצע מתאריך 31.12.2020 תידרש עמידה מלאה בתהליכי ההתעדה בהתאם לדירוג הספק ע"י הארגון (להלן סעיף 7.1.5).
- דירוג סיווג הספק יתבצע לפי רמת הקריטיות הגבוהה ביותר של אותו ספק, הציון הסופי של ספק (מבין שלוש הרמות C/B/A), ייגזר מפוטנציאל הנזק המרבי. לדוגמה, ספק אשר בקריטריון אחד נמצא ברמה A, וביתר הקריטריונים נמצא ברמה C, יסווג כספק ברמת פוטנציאל נזק A.
- ספק שאינו מהותי ואינו בשרשרת האספקה של הארגון בהיבטי סייבר אין חובה לערוך לו סקר.
- בהתאם ללוחות הזמנים שנקבעו לעיל, תדווח ליחידת הסייבר המגזרית של משרד הבריאות תכנית העבודה הכוללת טבלה המכילה את מיפוי כלל הספקים בהתאם לשדות הנדרשים הבאים:

דירוג ספקים	מיפוי ספקים				
	שם הספק	סוג השירות/מוצר אותו הוא מספק	איש קשר מהצד העסקי בארגון אל מול הספק	פרטי התקשרות מול נציג הספק לשאלות בנושא סייבר	סוג השירות הניתן (שירות מבוסס ענן/פיתוח תוכנה/גישה מרחוק/שירות שכולל חשיפת מידע של הלקוח ו-או אפשרות לפגיעה בתהליכים ו-או מערכות בארגון או בלקוחותיו)
A/B/C					

בקרה על המשאב האנושי

- במסגרת ההתקשרות של מוסד רפואי עם ספק או גורם חיצוני אשר ייחשף למידע רפואי ו/או יורשה לגשת למכשור תומך תהליך רפואי - ינוסח הסכם סודיות בהתאם לטיב המידע המשותף, הסכם שמירת סודיות זה יחול על כל אחד מעובדי הספק אשר יבואו במגע עם מידע ומכשור מסוג זה.
- עובדי ספק חיצוני אשר מעורבים בעיבוד ותחזוקה של מידע רפואי אישי במסגרת עבודתם יידרשו בנוסף, לחתום על הנחיות סודיות ואבטחת המידע לעובד של משרד הבריאות לפני תחילת העבודה במוסד הרפואי.
- הספק החיצוני יידרש לבצע בדיקות לאימות רקע של עובד שלו בהתאם לרמת החשיפה ובדרך שתקבע הנהלת הארגון בכפוף לדרישות החוק הפרטיות והחוק למניעת העסקה של עברייני מין (לדוגמה - תעודת יושר ממשטרת ישראל, העדר רישום עברות מין, מבחני אמינות, אימות של תעודות, רישום פלילי וכדומה). יעוד לביצוע הבדיקה יוצג בתחילת הליך אישור ההתקשרות של המוסד הרפואי עם הספק החיצוני.
- הספק יחויב ליידע את המוסד הרפואי בכל שינוי בהרכב העובדים, וכי לא יבצע שינויים כאמור ללא אישור מראש של מנהל אבטחת המידע במוסד הרפואי.

- לצורך הגברת המודעות לסיכוני הסייבר במגזר הבריאות, יקיים הספק הדרכות ייעודיות בנושאי אבטחת מידע בקרב עובדיו. יעביר את התכנים ונוהלי הארגון הרלוונטיים לאבטחת המידע והגנת הסייבר וכן יקיים תיעוד לביצוע הדרכות יישמר ויוצג לביקורת התקופתית שתבוצע על ידי המוסד הרפואי.

בקורות טכנולוגיות

- במידה ומתבצעים שמירה, עיבוד או שידור של מידע של הארגון הבריאות באתר הספק (או באתר חיצוני של גורם שלישי כגון ענן) על ארגון הבריאות לוודא כי הוטמעו ומנוהלות בקורות אבטחת מידע טכנולוגיות הולמות בכפוף לדרישות שהוגדרו ויעדכנו במתווה שיוגדר על ידי מערך הסייבר הלאומי כחלק מהמאמצים לאסדרת שרשרת האספקה. יש להגדיר את סוג השרות ולהתאים רשימה של הבקורות.

דוגמאות:

- תכנון ויישום ארכיטקטורה מאובטחת של הפתרון ;
- ניהול הרשאות, בפרט הרשאות אדמיניסטרטיביות ;
- אבטחה אפליקטיבית ;
- ניהול תצורה, עדכונים וניהול שינויים ;
- הפרדה בין אזורים בעלי רגישות שונה ;
- הצפנה של מידע רגיש ;
- ניטור של פעולות המתבצעות על המידע.

גישה מרחוק

- גישה מרחוק תאושר אך ורק במקרים בהם אין זה מעשי לספק את השירות הנדרש על ידי עובדי המוסד הרפואי או בגישה ישירה של הספקים למערכות הארגון מחצרותיו.
- ככל מומלץ לא לאפשר גישת ספקים קבועה יש לאפשר גישה מרחוק בכפוף לצורך ובזמן הנדרש לתיקון או תחזוקה בהתאם לאישורים מתאימים מגורם ניהולי מקצועי.
- גישה מרחוק תוגבל להתחברות לציוד שעל הספק להתחבר אליו, ללא יכולת להתחבר לציוד אחר ותותנה בעמידה בדרישות אבטחת המידע, והסכמה חוזית מצד הספק לעמידה בבקורות טכנולוגיות בכללן אפשרות לביצוע ניטור, הקלטות וכו' בהתאם לסוג המידע ואופי ההתחברות כפי שיקבעו על ידי מנהל אבטחת המידע.
- מערכת ההזדהות לגישה מרחוק תהיה ברף מינימלי של רב"א 3 בגישה של עובדי הספק למערכות הממוחשבות בהן נעשה שימוש במגזר הבריאות.

גישה פיזית לציוד

- יש להגדיר תהליך לליווי ופיקוח על ספק שירות של חברה חיצונית אשר ימנע חשיפה, שינוי או מחיקה של מידע רפואי אישי לגורם שאינו מורשה בכללן השפעה על ציוד רפואי וממערכות שו"ב (שליטה ובקרה ICS).

- כל גורם חיצוני אשר יזומן לגשת למערכות ו/או ציוד רפואי של המוסד הרפואי יידרש לעבור תהליך הזדהות בפני הגורם המזומן. מתן האישור לתחילת העבודה יינתן רק לאחר ביצוע זיהוי ואימות הגורם החיצוני. במקרים בהם קיים ספק בזהותו של נותן השירות אין לאפשר את עבודתו עד לסיום הבירור.
- המוסד הרפואי ינהל רשימה של אזורים בהם מנוהל מידע רגיש ו/או ציוד רפואי קריטי. הגישה לאזורים אלו תמודר בפני ספקים חיצוניים והציבור. יש להימנע ככל האפשר מכניסת גורמים חיצוניים לאזורים הרגישים ולקיים תהליכי בקרה נאותים למניעת גישה פיזית למתקנים ומערכות שיוגדרו ע"י הארגון.
- גישה פיזית של עובדי ספק חיצוני לאזורים רגישים תתואם, תאושר מראש ותתבצע בנוכחות עובד המוסד הרפואי בכדי למנוע שימוש לרעה במידע או כניסה למידע שאינו רלוונטי לתהליך העבודה
- תנוהל רשימה עדכנית של ספקים חיצוניים המורשים לגשת לאזורים רגישים.

זמינות והמשכיות בשרשרת אספקה

- בחינה והגדרת דרישות זמינות והמשכיות עסקית יחייבו את כל הגורמים המעורבים בשרשרת האספקה של כל תהליך בהתאם לחיוניותו לתהליכים העסקיים של הארגון מתוך בחינה על ההשפעה מתוך ההבנה כי פגיעה בו תפגע ביכולות הארגון לספק שרות.
- תוגדר מחויבות חוזית לעמידה בדרישות אלה וכן יתבצעו ביקורות תקופתיות.

טיפול באירועי אבטחת מידע

- כל ספק מחויב להתריע מידית לארגון הבריאות על כל חשד לאירוע אבטחת מידע וסייבר שמתרחש אצלו בין אם האירוע קשור באופן ישיר לארגון הבריאות ובין אם לאו.
- למול כל ספק קריטי יש להגדיר את חלקו בניהול אירועי אבטחת מידע וסייבר על ארגון הבריאות לבצע הערכה של רמת האיום הנובעת מפגיעה בספק ופגיעה בארגון במימוש תקיפה דרך הספק.
- יש לבצע התקשרות מוקדמות עם חברות אבטחה מידע וסייבר למטרת מתן תגובה לאירועי סייבר ותהליכי התאוששות בכפוף להתחייבות הספק ובהתאם להיקף האירוע, יש לקיים הערכות מצב משותפות ועבודה משותפת להתמודדות יעילה וחזרה לשגרה מפוקחת.
- באחריות הספק וארגון הבריאות לקיים דיווח במקביל בהתאם לדרישות הרשות להגנת הפרטיות לגבי כל חשד לפגיעה במאגר מידע תקנה 11(ד)(1) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: "התקנות") קובעת כי בעל מאגר מידע שחלה עליו רמת אבטחה בינונית או גבוהה (כהגדרתן בתקנות) מחויב להודיע לרשות להגנת הפרטיות באופן מיידי על אירוע אבטחה חמור (כהגדרתו בתקנות), וכן ידווח לרשות על הצעדים שנקט בעקבות האירוע.
- ככלל, על הדיווח להיעשות תוך 24 שעות ממועד גילוי של אירוע האבטחה החמור, ובכל מקרה לא יאוחר מ-72 שעות מאותו מועד.

התקשרות עם ספקים בשרשרת אספקה

- בכל מכרז לשירותים חיצוניים יש לוודא קיום התעדה מתאימה בהתאם לדירוג הספק ולצרף נספח אבטחת מידע שיהווה חלק בלתי נפרד ממנו, עמידה בדרישות אלה תהווה תנאי הכרחי לעמידה במכרז.
- בכל התקשרות חוזית עם ספק יש לאמת את קיום תוקף ההתעדה ולצרף נספח אבטחת מידע שיהווה חלק בלתי נפרד מההסכם.
- בבחינת ספקים יקבע "מפל איכות", תינתן עדיפות לעמידה בדרישות שרשרת אספקה והסמכה ע"פ דירוג הספק ובהתאם לעמידה בבקורות הרלוונטיות ומידת יישומן ע"י הספק בהתאם לסוג השרות ואופיו עבור הארגון.
- ספקים אשר לא יעמדו בדרישות ההתעדה בין אם התהליך ימשך מעבר לזמן שנקבע לצורך קיום תהליכי ההתעדה או יתגלו פערים שאין בכוונת הספק לתקנם, הן ספקים קיימים והן ספקים חדשים ידרשו לתהליך שימוע ולמתן הבהרות ליחידת הסייבר במשרד הבריאות ולגורמים ביעוץ המשפטי בשיתוף מערך הסייבר והרשות להגנת הפרטיות בהתאם לצורך.
- ספקים אשר יעברו תהליך שימוע יעודכנו כי התהליך הינו שקוף לכלל המגזר הבריאות ובהתאם למדניות מערך הסייבר לכלל המגזרים המוסדיים, ארגוני הבריאות יעודכנו לגבי התהליך וידרשו להקפיד התקשרויות עתידיות כאשר לגבי התקשרויות קיימות עם אותם ספקים תידרש קיום הערכות מיוחדות לצמצום נזק פוטנציאלי (חשיפה למחוללי האיום)
- יתקיים תהליך לאישור החרגה ובחינת דחיית ההתעדה של ספקים בכפוף לקיום סקרים והערכת הסיכונים ולאחר קיום תהליך בשילוב גורמים במשרד הבריאות ומערך הסייבר הלאומי.

סקרי סיכונים בשרשרת אספקה

- יש להגדיר את תדירות וצורת סקרי הסיכונים בהתאם לקריטריון הספק ורגישות התהליך הנתמך בכפוף לתהליכי האסדרה של שרשרת האספקה ובחינת עמידה בדרישות בצורה עיתית בכפוף לרגולציה שתקבע ע"י מערך הסייבר הלאומי.
- לכל הפחות, על כל ספק למלא ברמה שנתית שאלון המתייחס לכל הבקורות שהוגדרו על ידי ארגון הבריאות. שאלון זה ייחתם על ידי גורם מוסמך מטעם הספק לאחר שמולאו דרישות תהליך ההתעדה בשרשרת האספקה. (C)
- בגופים בהם יוגדרו שאלונים עם הוכחת עמידה הספק יידרש להציג ראיות לקיום הבקרה ועמידה בדרישות (B) במערכת שתוגדר ע"י מערך הסייבר הלאומי
- לספקים שיוגדרו כבעלי סיכון גבוה (A) תתבצע בקרה בשטח על ידי בודקים מאושרים ע"י מערך הסייבר לסקר שרשרת האספקה ויימסר דיווח ליחידת הסייבר המגזרית;
- באחריות מנהל אבטחת המידע והגנת הסייבר של הארגון לעקוב אחר תיקון הליקויים המתגלים במסגרת סקרי הסיכונים ולוודא עמידה וקיום היעדים בתוכניות העבודה השנתית.
- "מערכת יוב"ל" (יעדים ובקורות לארגון) – הינה מערכת לניהול סיכונים סייבר ואבטחת מידע. המערכת פותחה באמצעות המערך הלאומי להגנת הסייבר, לטובת הציבור. המערכת מורכבת ממספר מודולים, כגון מודול שרשרת אספקה, מודול התעדה, מודול תורת הגנה ועוד. מודול התעדה במערכת, מסייע לאבחן את רמת הגנת המידע המיושמת על ידי הספק. רמת הגנת המידע נקבעת על ידי מילוי שאלון

סגור הכולל שאלות ממגוון תחומים באבטחת מידע. לאחר מילוי השאלון הספק יקבל ציון המשקף את רמת הגנת המידע של שירות/מוצר ספציפי. במקרים מסוימים יידרש הספק לעבור בדיקת התעדה, באמצעות גורם בדיקה מורשה, אשר רק לאחריה יקבל אישור על רמת ההגנה בארגונו.

המערכת מסייעת בין היתר בדברים הבאים:

- הנגשת שאלון רמת ההגנה לספקים במשק בצורה מקוונת.
- מע' ההתעדה הנגישה באתר מערך הסייבר הלאומי, מאפשרת את הנגשת רשימת הגורמים במשק אשר סיימו את תהליך ההסמכה בהתאם למתודה הלאומית בנושא (ספקים, ובודקים מוסמכים). כל ארגון במשק יוכל לבצע חיפוש במערכת, ולקבל פילוח מתאים של חברות העומדות בסף הסיכון שקבע הארגון. על סמך מידע זה יוכל הארגון לבחור את הספק המתאים ולחתום עמו חוזה התקשרות להבטחת עמידת הספק ברמת הסיכון שנקבעה.
- פלטפורמה עבור הספק להפיק דו"חות להצהרה על רמת העמידה שלו בדרישות ההגנה של מתודה זו, לצד יכולת לנהל את הליקויים שעלו אצלו בתהליך (Remediation). בנוסף, הספק רשאי בכל זמן נתון לעדכן את פרטיו במערכת ובהתאם יופק למוצר/שירות ציון חדש.
- המערכת זמינה למשק באתר מערך הסייבר ובאמצעות הקישור הבא:
- <https://grc.cyber.gov.il>

חוקים, תקנות והנחיות רלוונטיות

- חוק המחשבים, התשנ"ה – 1995 ;
- הוראות ותקנות משרד הבריאות ;
- חזור מנכ"ל משרד הבריאות 3/2015 בעניין הגנה על מידע במערכות ממוחשבות ובמערכות בריאות ;
- חוק הגנת הפרטיות התשמ"א – 1981 ;
- תקנות הגנת הפרטיות (אבטחת מידע) 7809, התשע"ז – 2017 ;
- תקנים להגנת מידע ISO 27001 , ISO 27799 ;
- אסדרת שרשרת אספקה מערך הסייבר
- תקנים וולונטריים לניהול סיכונים ISO27005 , ניהול אירועי סייבר ISO 27032
- המדיניות הלאומית להזדהות בטוחה