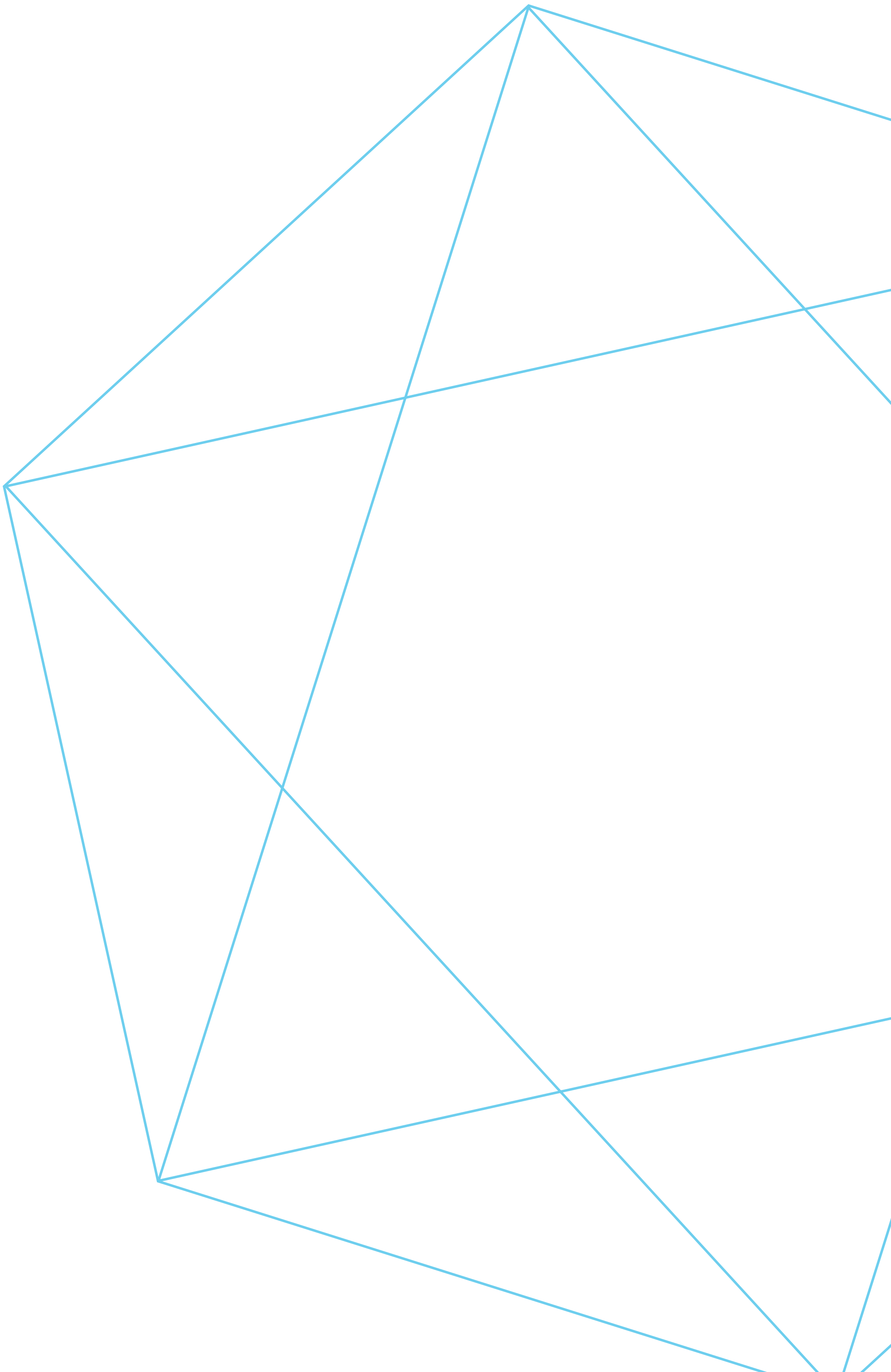
משרד ראש הממשלה
מערך הסייבר הלאומי

תורת ההגנה בסייבר לארגון

גרסה 1.0



משרד ראש הממשלה
מערך הסייבר הלאומי

תורת ההגנה בסייבר לארגון

גרסה 1.0

הדפסה שנייה // ניסן תשע"ח // אפריל 2018

// תוכן העניינים

פתח דבר **7**
תמצית מנהלים **10**

1. מבוא **12**
2. עקרונות תורת ההגנה **13**
3. מבנה תורת ההגנה **14**
3.1 תהליך ההגנה המחזורי 14
3.2 בקרות ההגנה מאוגדות על-פי NIST Cyber Security Framework 15
4. תהליך התכנון בראיית הארגון **17**
5. תורת ההגנה בעיני הארגון **18**
5.1 מימוש תורת ההגנה עבור ארגון מקטגוריה א' 19
5.2 מימוש תורת ההגנה עבור ארגון מקטגוריה ב' 23
6. פרקי הבקרות – לשלבי הביצוע והבקרה **32**
6.1 מבוא 32
6.2 כיצד להגן 33

נספחים

נספח א׳ - דוגמה לביצוע הערכת סיכון עבור נכס מידע 153
נספח ב׳ - עזרים עתידיים למימוש תורת ההגנה 154
נספח ג׳ - בקרות הגנה לארגון מקטגוריה א' – דגשים עבור איש המחשוב 156
נספח ד׳ - תאימות לתקנים 161
נספח ה׳ - בקרות הגנה קריטיות להשגת תוצאה גבוהה בזמן קצר 162
נספח ו׳ - בנק הבקרות 163
נספח ז׳ - התמודדות עם אירוע סייבר משמעותי 164
נספח ח׳ - ניתוח מצב מוכנות על בסיס סטטוס הטמעת והפעלת כלי הגנת סייבר 165
נספח ט׳ - מילון מונחים 167

מסמך זה פותח ע"י מערך הסייבר הלאומי לטובת הציבור. המסמך מהווה המלצה לכלל הארגונים במשק הישראלי. ניתן להשתמש בו לטובת העלאת החוסן בסייבר במשק באופן חופשי. מסמך זה נכתב עבור דירקטוריונים והנהלות של חברות, מנהלי הגנה בסייבר ומיישמים וספקי IT. המסמך מציג את דרישות ההגנה המינימאליות הנדרשות בהתאם לפוטנציאל הנזק. תכנית ההגנה לארגון הנגזרת ממסמך זה מותאמת למידת התלות של הארגון בסייבר. ארגונים נדרשים לבצע תהליך הערכת הסיכונים ויכולים לבנות תכנית הגנה מחמירה מדרישות מסמך זה. המסמך פונה לכלל המשק ונכתב בלשון זכר מטעמי נוחות בלבד. ההתייחסויות למסמך ניתן להעביר במייל tora@pmo.gov.il.

// פתח דבר

מנהלים, מומחי אבטחת מידע והגנת סייבר יקרים,

מרחב הסייבר הוא תולדה של קדמה טכנולוגית, קישוריות וחיבור גלובלי לרשת האינטרנט.

התלות הגוברת במרחב הסייבר מביאה עמה בשורות של חדשנות טכנולוגית ופיתוחים אדירים לאדם ולסביבתו.

לצד אלה מתפתח מרחב איומים, המשפיע על הרציפות התפקודית הארגונית, על שלמות תהליכי הייצור ועל סודיות המידע הארגוני.

מתקפות סייבר עלולות לפגוע בארגונים ואף להביא להפסקת תהליכי ייצור, לנזק כלכלי ולפגיעה במוניטין של הארגון.

מדינת ישראל עושה מאמץ לאומי בהגנת הסייבר במרחב האזרחי.

תורת ההגנה הארגונית הינה נדבך בתפיסת ההגנה הלאומית, המורכבת מרבדים שונים של הגנה על המשק הישראלי ועל הרציפות התפקודית שלו.

תורת ההגנה הלאומית רואה את הארגון כמכלול שלם ומאפשרת את העלאת רמת החוסן הארגוני באמצעות הטמעה רציפה של תהליכים, שיטות ומוצרי הגנה.

יישום תורת ההגנה הארגונית ישפר את החוסן הארגוני ואת העמידות הארגונית בפני מתקפות סייבר.

// תמצית מנהלים

מטרת תורת ההגנה הינה למזער את סיכוני הסייבר של ארגונים במשק הישראלי.

מסמך זה מגדיר מתודה סדורה אשר מובילה את נושא האחריות בארגון לבניית תכנית עבודה רב שנתית להגנה על הארגון.

באמצעות המתודה המובאת במסמך זה, הארגון יכיר את הסיכונים הרלוונטיים אליו, יגבש מענה הגנתי ויממש תכנית להפחתת הסיכונים בהתאם.

שלב א - הארגון יבין לאיזו קטגוריה הוא משויך:

- **קטגוריה א'** – ארגונים אשר פוטנציאל הנזק שלהם כתוצאה מאירוע סייבר **אינו** גדול.
- **קטגוריה ב'** – ארגונים אשר פוטנציאל הנזק שלהם כתוצאה מאירוע סייבר **הינו** גדול.

שאלון חלוקה לקטגוריות מופיע בעמוד 18.

שלב ב – בניית תכנית עבודה לארגון

לטובת בניית תכנית העבודה, הארגון יגדיר תחילה על מה הוא נדרש להגן, מהי רמת ההגנה הנדרשת, מהם פערי ההגנה אל מול המצב הרצוי ולבסוף יבנה תכנית עבודה לצמצום הפערים.

הסבר אודות אופן הגדרת יעדי ההגנה של הארגון ורמת ההגנה הנדרשת מובאים במסמך זה בעמודים 19-20 עבור ארגון מקטגוריה א' ובעמודים 23-25 עבור ארגונים מקטגוריה ב'.

בשלב זה, על הארגון להבין מהן הבקרות הנדרשות מהארגון עבור נכסיו השונים. בקרות אלו מובאות בעמוד 20 עבור ארגונים בקטגוריה א' ובעמודים 33-149 עבור מקטגוריה ב'.

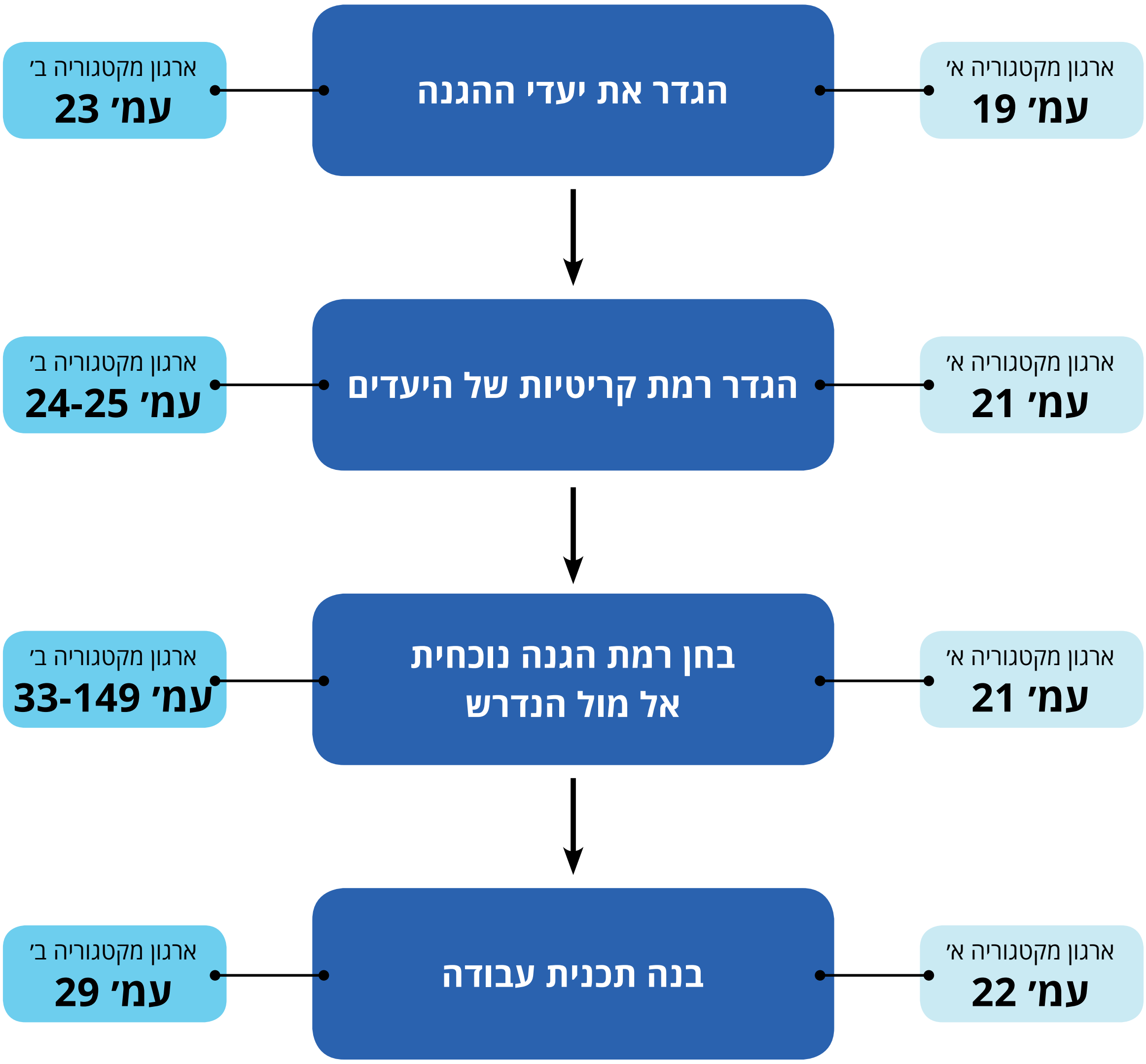
תוצר סופי לאור העבודה עם מסמך זה:

הארגון יבין מהן הבקרות הנדרשות למימוש לטובת הפחתת סיכוני הסייבר אליהם הארגון חשוף.

בקרות אלו יהוו את תכנית העבודה להפחתת סיכוני הארגון.

עבור ארגונים אשר מוכוונים מקצועית באמצעות מנחה ייעודי מטעם מערך הסייבר הלאומי, תכנית העבודה תבנה בהתאם להכוונת המנחה המגזרי.

תהליך העבודה עם מסמך זה נראה כך:



1 // מבוא

מרחב הסייבר הוא חלק בלתי נפרד מחיינו. ברמה האישית אנו מחפשים מידע באינטרנט, מנווטים את דרכנו בכביש באמצעות תוכנות ניווט, משוחחים בטלפון סלולרי, ולחלקנו יש קוצב לב או משאבת אינסולין, המחוברים לאינטרנט – כולם חלק ממרחב הסייבר. ברמה העסקית אנחנו משתמשים בכרטיסי אשראי, מנהלים בסיס נתונים של לקוחות, מנהלים ארגון גלובאלי על-ידי רשתות מחשוב, משווקים, קונים ומוכרים - והכול תוך התבססות על מרחב הסייבר.

לרבים מאיתנו, בחיי היומיום בכלל ובעסקים בפרט, מרחב סייבר זמין, נגיש ומהימן מהווה תנאי הכרחי. קל להבין זאת כאשר הללו נמנעים מאיתנו בצורה זמנית. איך תנהל את העסק ללא טלפון סלולרי? ללא הידע האגור ברשת הארגונית? ללא יכולת לבצע סליקת כרטיסי אשראי?

מרחב הסייבר הינו מרחב של אפשרויות והזדמנויות מצד אחד ומרחב של איומים וסיכונים מנגד.

במרחב זה מתנהלת פעילות ענפה של ריגול מדינתי, ריגול תעשייתי, פשע מאורגן ופשע מזדמן, פריצות למידע אישי וכד׳. הללו עלולים להשפיע על הביטחון הלאומי (למשל, באמצעות פגיעה במרחב הסייבר בתשתית לאומית קריטית כמערכת החשמל או המים), על התנהלות עסקית (למשל, ריגול מסחרי, סחיטה כלכלית) ועל פרטיות (למשל, באמצעות פרסום מידע ותמונות אישיות).

כיום, ארגונים שונים מגינים על עצמם מפני איומים אלו בצורות שונות. המידע הקיים באינטרנט על דרכי ההתגוננות מפני סיכוני סייבר רב ביותר ומורכב מאוסף של מתודולוגיות סדורות, שיטות עבודה מומלצות, כללי ״עשה ואל תעשה״ ועוד.

הגנה על ארגון מפני איומי סייבר דורשת ידע רב. ידע זה כולל מספר רב של התמחויות - טכנולוגיות, ארגוניות ותהליכיות.

ארגונים רבים בארץ ובעולם מתחבטים בשאלות כגון - ״האם אנחנו משקיעים די בהגנה בסייבר?״, ״האם אנחנו משקיעים נכון בהגנה בסייבר?״, ״האם אנחנו משקיעים בהגנה בסייבר בהתאם למקובל במשק/בענף שלנו?״ ארגונים רוצים להגן על עצמם באופן שיפחית את הסיכונים העיקריים שלהם במרחב הסייבר ויאפשר פעילות עסקית ללא פחד.

תורת ההגנה מסייעת לארגונים למפות את סיכוני הסייבר שהם חשופים אליהם, להבין את המשמעות העסקית של התממשות הסיכונים ולהגדיר אמצעי הגנה מידתיים להפחתת הסיכונים העיקריים. כמו כן, תורת ההגנה מגדירה הגנה נאותה לנכסים ארגוניים בעלי השפעה על מגזר או ברמה המדינתית.

מערך הסייבר הלאומי הוקם, בין היתר, על-מנת לעצב, ליישם ולהטמיע תורה לאומית להגנת הסייבר (החלטת ממשלה מס׳ 2444). במסגרת זו החליט המערך לפרסם תורת הגנה זו לארגונים במשק הישראלי, תחילה במשרדי הממשלה.

מערך הסייבר הלאומי פיתח תורת הגנה זו על-ידי שילוב תורות מובילות בעולם, ניסיון ישראלי בתחום האזרחי והביטחוני, התאמה לסביבה הישראלית והתאמה לתרבות העסקית הישראלית.

2 // עקרונות תורת ההגנה

העיקרון הראשי של תפיסת ההגנה אשר על בסיסה נכתבה תורת הגנה זו, הינו "הארגון כמכלול", כלומר ההכרה בכך שנדרש להגן על רציפות התפקוד של הארגון ולתמוך ביעדיו העסקיים.

תפיסה זו באה לידי ביטוי במסמך באופן הבא:

א. **אחריות הנהלה -** האחריות להגנה על המידע נמצאת בראש ובראשונה אצל הנהלת הארגון.

ב. **הגנה בהתאם לפוטנציאל הנזק –** ההשקעה בהגנה על כל נכס תהיה בהתאם לרמת הקריטיות שלו לתפקוד הארגון.

ג. **הגנה מבוססת ידע וניסיון ישראלי –** תורת ההגנה מאפשרת את המיקוד בסיכונים הרלוונטיים לכל ארגון וארגון. כחלק מפעילות מערך הסייבר הלאומי, מתבצעות ביקורות והערכות מודיעין עתיות למשק. פעולות אלו מאפשרות למקד ארגונים באזורים ספציפיים במעגלי ההגנה השונים.

ד. **הגנה פרואקטיבית –** בקרות ההגנה הוגדרו מתוך הבנה, כי על הארגון להשקיע מאמצים בנוסף על ההגנה הפאסיבית המסורתית. הדבר בא לידי ביטוי באמצעות הגדרת בקרות הגנה עבור שלבי המניעה, הזיהוי והתגובה והחזרה לשגרה.

ה. **הגנה רב-מימדית –** הגנה היא תהליך המשלב שלושה מימדים עיקריים: אנשים, טכנולוגיה ותהליכים (3 P's – People & Products & Processes). תורת ההגנה מגדירה מענה הגנתי נדרש בכל הרבדים הללו.

3 // מבנה תורת ההגנה

מאחר וארגונים פועלים בסביבה דינאמית, שינויים בטכנולוגיה, באופי החברה ובתחומי פעילותה משפיעים על האופן בו הארגון נדרש להגן על עצמו במרחב הסייבר.

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 בקרות נדרשות).

3.1 תהליך ההגנה המחזורי

תהליך ההגנה על-פי תורת ההגנה הוא תהליך מחזורי, הכולל שלושה שלבים עיקריים:

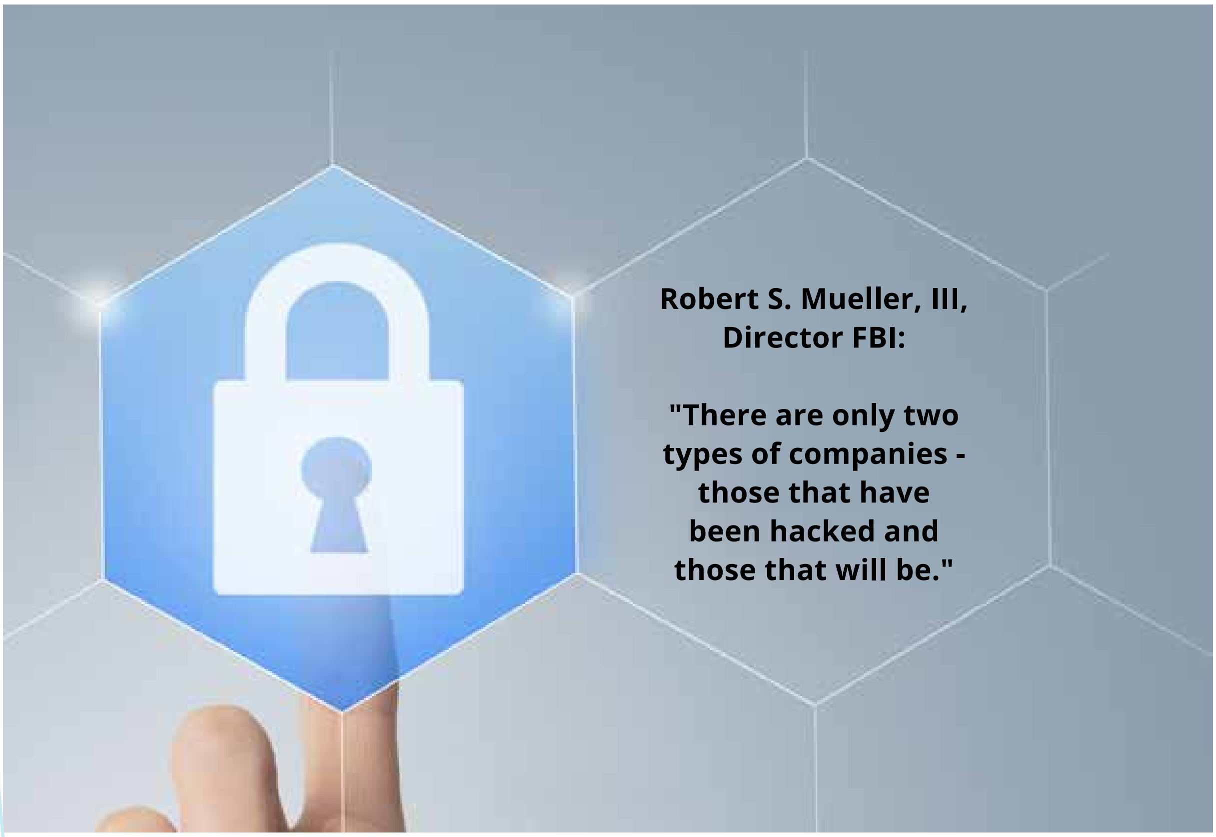
א. **תכנון והערכה -** עיקריו מיפוי יעדי הגנה בסייבר בארגון, הערכת סיכונים, בחינת אמצעי ההגנה (הבקרות הקיימים ובניית תכנית עבודה לסגירת פערי הגנה.

ב. **ביצוע** תכנית העבודה על-ידי בניית תהליכים ארגוניים, הטמעת כלים והטמעה ארגונית של הגנה בסייבר לארגון.

ג. **שמירה על עדכניות** ההגנה לאור דינאמיות מרחב הסייבר בארגון. התהליכים והטכנולוגיות המוטמעים בארגונים משתנים כל הזמן - מחשבים ורשתות חדשים מותקנים, תוכנות מתקדמות נרכשות, רכיבים חדשים מקושרים למרחב הסייבר (למשל Internet of Things), מוצעים שירותים חדשים (כגון מחשוב ענן) ועוד. מנגד, גם האיומים ושיטות התקיפה האפשריות על הארגון משתנים, ועקב כך – גם כלי ההגנה הנדרשים.

3.2 בקרות ההגנה, מאוגדות על-פי NIST Cyber Security Framework

לאורך השנים שמו תקני ההגנה דגש רב בנושא "כיצד להגן על ארגון", כלומר **למנוע** חדירה לארגון ולנכסי הסייבר שלו. **המציאות כיום שונה -** ארגונים מכל הגדלים והסוגים מותקפים, אך מזהים תקיפה חודשים רבים לאחר שזו התרחשה, אם בכלל. לאור זאת החליטו במכון התקנים האמריקני (NIST) לבנות תורת הגנה, אשר משקיעה הן בשלב היערכות וההגנה (המסורתיים) והן בשלבי האיתור, ההכלה וההתאוששות היה ותתרחש תקיפת סייבר. גישה זו מקבלת ביטוי במסגרת שנקראת NIST Cyber Security Framework. תורת ההגנה מאמצת את מסגרת NIST CSF ומאגדת תחתיה משפחות של בקרות הגנה. **בגישה זו מתבצעת הגנה על הארגון מפני תקיפה, לצד חיזוק יכולתו של הארגון לגלות תקיפה שהצליחה, להכילה ולהתאושש ממנה במינימום נזק לארגון.** בקרות אלו מבוססות על הידע הבינלאומי, אך בוצעו בהן התאמות רבות למאפייני המשק הישראלי, תוך הוספת דגשים ודוגמאות לטובת סיוע לארגונים למקד את המאמצים באופן יעיל יותר.



<u>זיהוי</u> (IDENTIFY)

משפחת בקרות:
- אחריות דירקטוריון והנהלה
- ניהול סיכונים והערכת סיכונים
- בקרה, ביקורת ותאימות

<u>הגנה</u> (PROTECT)

משפחת בקרות:
- בקרת גישה
- הגנה על המידע
- הגנה על שרתים ותחנות עבודה
- מניעת קוד זדוני
- הצפנה
- אבטחת רשת
- הפרדת סביבות
- אבטחה בענן
- הגנה על בקרים תעשייתיים
- אבטחת טלפונים סלולריים
- ניהול שינויים
- אבטחת מדיה
- אבטחת שרשרת אספקה ומיקור-חוץ
- אבטחה ברכש ופיתוח
- הגנה פיזית וסביבתית
- משאבי אנוש ומודעות עובדים
- הדרכות

<u>איתור</u> (DETECT)

משפחת בקרות:
- תיעוד וניטור
- סקרי הערכה של בקרות אבטחה
- הגנת סייבר פרואקטיבית

<u>תגובה</u> (RESPOND)

משפחת בקרות:
- ניהול אירועים ודיווח

<u>התאוששות</u> (RECOVER)

משפחת בקרות:
- המשכיות עסקית

4 // תהליך התכנון בראיית הארגון

שלבי התהליך

תהליך התכנון מורכב מהשלבים האינטואיטיביים הבאים:

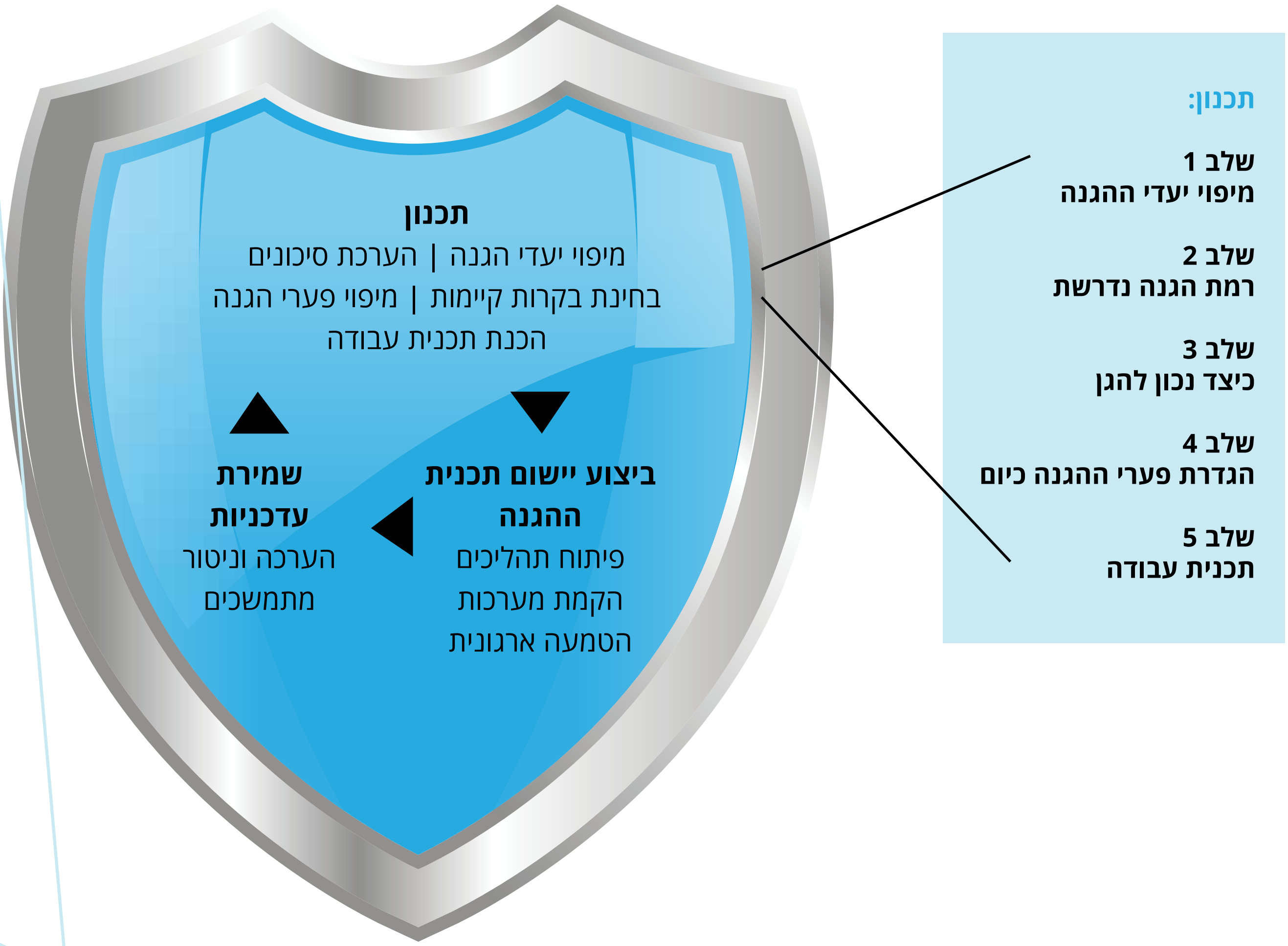
שלב 1: "על מה להגן?" – איתור נכסים/תהליכים עסקיים, הרגישים לפגיעת סייבר.

שלב 2: "כמה משפיע על יעדי הארגון?" – הבנת ההשפעה של פגיעת סייבר בנכסים/בתהליכים עסקיים על הארגון באמצעות מענה על שאלון ערכיות.

שלב 3: "כיצד נכון להגן?" - מתוך הבנת הערכיות שבשלב הקודם נגזרות הבקרות הנדרשות למימוש.

שלב 4: "רצוי מול מצוי" - איתור פערי הגנה קיימים כיום ביחס לבקרות הנדרשות.

שלב 5: "בניית תכנית עבודה" - להעלאת רמת ההגנה, על-מנת להגיע לרמת הסיכון הרצויה (כולל הבנה של מהות החשיפה לסיכון במידה שלא ממשים בקרות נדרשות).



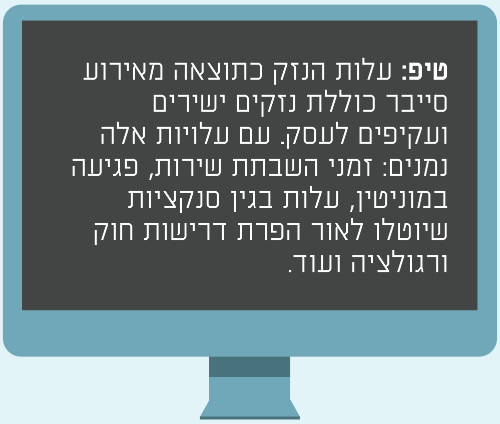
5 // תורת ההגנה בעיני הארגון

תורה זו מציגה שתי רמות שונות של המלצות, אשר נגזרות מפוטנציאל הנזק לארגון כתוצאה מאירוע סייבר:

- **ארגון בקטגוריה א׳ -** פוטנציאל נזק נמוך. הארגון יבצע תהליך פשוט של מיפוי יעדי הגנה ויבין במהירות את אופן ההגנה הנדרש.
- **ארגון בקטגוריה ב׳** – פוטנציאל לנזק משמעותי. ארגון הנשען בצורה משמעותית על מרחב הסייבר ונדרש לבצע תהליך מפורט יותר.

החלוקה מתבצעת לאחר מענה על השאלה הבאה:

במידה שיתרחש אירוע סייבר בארגונך,
האם עלות הטיפול באירוע לארגון
תהיה גבוהה מ-500,000 ש"ח?



בעת מענה על השאלה שלהלן, יש לקחת בחשבון את העלות הכוללת. ארגונים אשר השיבו בשלילה על השאלה הנ"ל, משויכים לקטגוריה א'. ארגונים אשר השיבו בחיוב, משויכים לקטגוריה ב'.

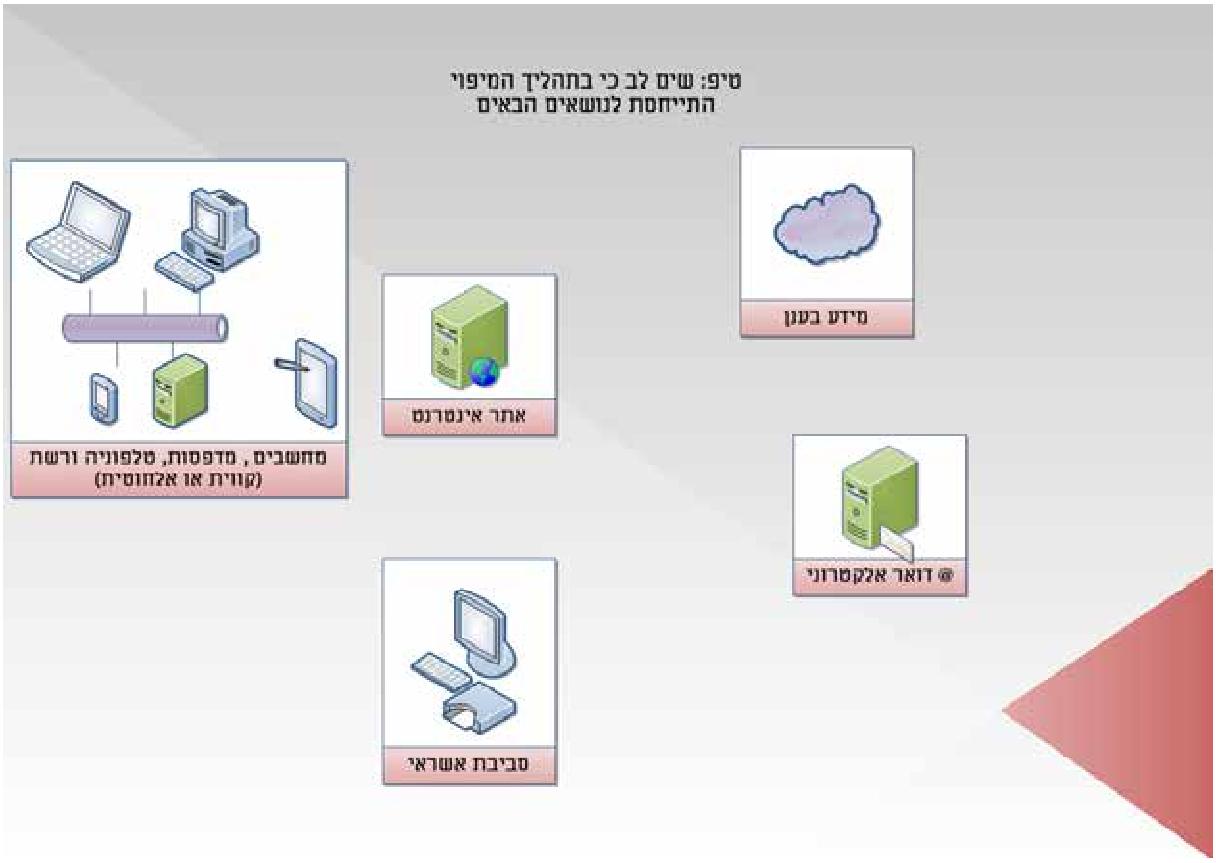
דרישות נוספות: במידה ועל הארגון חלות חובות נוספות מעצם היותו כפוף לרגולציות קיימות, הדבר עשוי להביא אותו למעבר מקטגוריה א' לקטגוריה ב'. כמו-כן, ארגון עשוי לדרוש מספקים שונים שלו לעמוד בהתאם לדרישות ארגונים מקטגוריה ב'.

5.1 מימוש תורת ההגנה עבור ארגון מקטגוריה א׳

תורת הגנה עבור ארגון בקטגוריה א׳ תחומות לעמודים 19-22 של מסמך זה.

שלב 1: מיפוי נכסים

יש לבצע מיפוי נכסים עיקריים. בדוק מול גורם התמיכה הטכנית את סוגי הציוד ונכסי המחשוב הנמצאים בשימוש הארגון.



שלבים 2 ו-3: רמת ההגנה הנדרשת וכיצד נכון להגן – עשרת הדיברות לארגון בקטגוריה א׳

ארגון בקטגוריה א׳ נדרש להגנה בהלימה לפוטנציאל הנזק. לכן, הארגון נדרש לממש בקרות בעלות אפקטיביות גבוהה במיוחד.

פירוט מלא של דרישות ההגנה נמצא בנספח ג' של מסמך זה.
בקרות אלו מחולקות לעשר קטגוריות ההגנה הבאות:

<table>
<tr><td colspan="3">1. אחריות הנהלה:
הבן את הסיכונים הקיימים לארגון במרחב הסייבר ובנה תכנית העבודה לסגירת פערי ההגנה בסייבר.</td></tr>
<tr><td>2. מניעת קוד זדוני:
עשה שימוש בטכנולוגיות לטיפול בפוגענים ובצע עדכוני אבטחה למערכות הארגון.</td><td>3. הצפנה:
הצפן ההתחברות מרחוק של עובדי הארגון וספקיו תוך שימוש במנגנוני הצפנה פשוטים מסחריים. הצפן גישה למידע רגיש תוך שימוש בתווך תקשורת מוצפן (הן בגלישה מהבית מרשת אלחוטית אל הארגון ומהארגון החוצה - אל לקוחות וספקים)</td><td>4. מחשוב ענן ורכש תוכנות:
קיים חוזה מול הספק, אשר דורש עמידה בסטנדרטים מקובלים להגנה על התוכנה והמידע.</td></tr>
<tr><td>5. הגנה על מידע:
הגדר מנגנוני ההגנה על אופן הוצאת מידע אל מחוץ לארגון.</td><td>6. הגנה על מחשבים:
הגדר רמת הגנה נדרשת על המחשבים. רמה זו כוללת החלפת סיסמאות ברירת מחדל של ציוד, הסרת תוכנות שאינן הכרחיות, חסימת חיבורים מיותרים והסרת משתמשים חזקים (Admin account) אשר אינם הכרחיים.</td><td>7. משאבי אנוש:
תדרך עובדים בעת קליטתם לעבודה והסר הרשאות של עובדים לאחר סיום העסקתם.</td></tr>
<tr><td>8. תיעוד וניטור:
נטר ותעד פעולות חריגות, אשר הארגון מעוניין לדעת אם הן התרחשו (ואשר מעידות על איום סייבר).</td><td>9. אבטחת רשת:
ודא בעיקר, כי הגישה אל הרשת נמצאת בבקרה של הארגון (ספקים ועובדים אינם יכולים להתחבר לרשת מרחוק מתי וכיצד שהם בוחרים) ושהרשת ערוכה מפני התקפות מניעת שירות.</td><td>10. המשכיות עסקית:
יכולת התאוששות במקרים של נפילת אתר, מחיקת מידע, נעילת קבצים.</td></tr>
</table>

שלב 4: הגדרת פערי הגנה

בדיקת מימושן של הבקרות המפורטות בנספח ג'.

קבלת המלצה לתכנית עבודה מתועדפת לטיפול בפערים מהגורם המטפל בנושאי המחשוב.

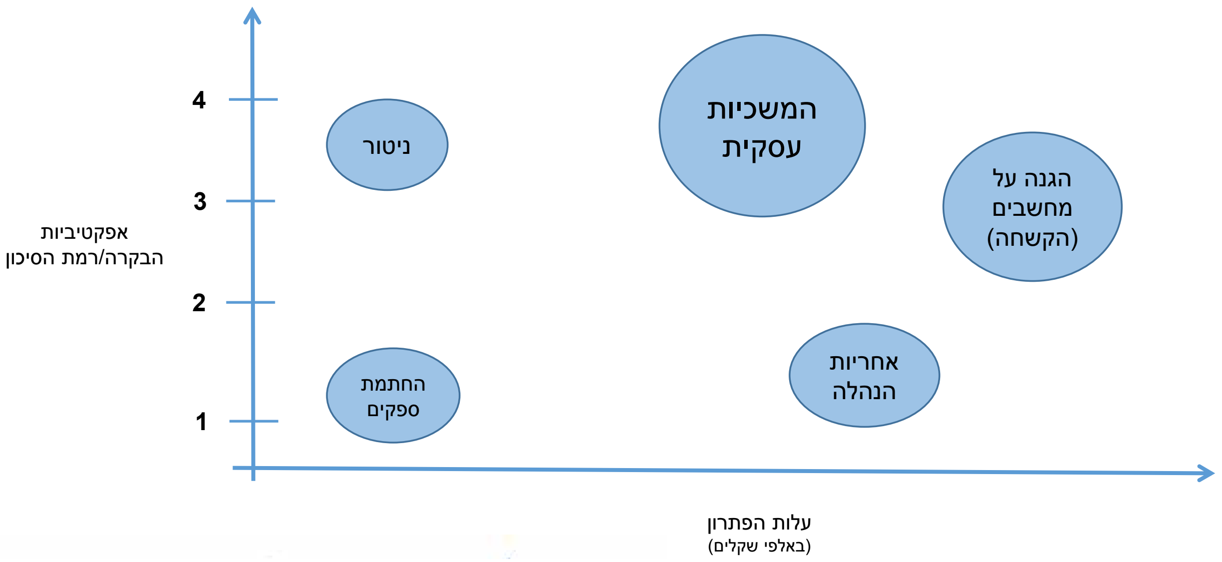
שלב 5: תכנית עבודה

כל בקרה בפרקי הבקרות מגינה מפני סיכון שנובע מפגיעת סייבר. הבקרה מקטינה את סיכון הסייבר, אשר עלול לפגוע ביעדי הארגון.

בבניית תכנית העבודה לסגירת פערי הבקרות, התכנית תיקח בחשבון:

- **אפקטיביות הבקרה** - תרומתה להפחתת הסיכון הארגוני.
- **עלות מימוש הפתרון** – מיוצג מטה באמצעות ציר "עלות הפתרון" (משך היישום, מורכבות המימוש, כוח אדם וציוד דרוש).
- **מהירות היישום** – מיוצג מטה באמצעות גודל העיגול.

דוגמה לשקלול הפרמטרים הנזכרים מעלה בארגון מסוים יכולה להיראות כך:



להלן תבנית עזר למילוי נתונים:

משפחת הבקרה	קיים/ לא קיים	אפקטיביות הבקרה	עלות מימוש	שקלול הנתונים/תעדוף
אחריות הנהלה				
מניעת קוד זדוני				
הצפנה				
מחשוב ענן ורכש תוכנות				
הגנה על המידע				
הגנה על מחשבים				
משאבי אנוש				
תיעוד וניטור				
אבטחת רשת				
המשכיות עסקית				

תבנית עזר לשימוש ארגונים מקטגוריה א' נמצאת באתר מערך הסייבר הלאומי.

תכנית העבודה המוצעת תאושר על ידי מנהל הארגון.

ארגון מקטגוריה א׳
סיים את הקריאה של מסמך זה

5.2 מימוש תורת ההגנה עבור ארגון מקטגוריה ב׳

שלב 1: מיפוי נכסים

הארגון ימפה את נכסיו, את ייעודם ואת הממשקים מ/אל הנכס (API, Web services וכו׳). יש לכלול נכסים המאוחסנים בענן (XaaS).

שלב מיפוי הנכסים יקשור גם בין נכסי IT/OT לתהליכים העסקיים המרכזיים בארגון. בסוף שלב זה יידע הארגון להגדיר מה הם הנכסים בעלי רמת קריטיות גבוהה לתפקוד העסק ומה הם הנכסים המשניים.

הגדרה זו תסייע להגן על הנכסים בהתאם לפוטנציאל הנזק.

מיפוי הנכסים יכלול לפחות את הרשימה הבאה:

סוג הנכס	שם הנכס + יצרן	ייעוד הנכס	מקומי/ענן	ממשקים	הערות
אפליקציה ארגונית					**כגון ERP, CRM, DWH, WMS, מערכת שכר, פורטל ארגוני.**
תשתית					**כגון ציוד תקשורת, תשתית טלפוניה, דוא״ל ואחסון.**
רשת					**כגון קווית ואלחוטית אופטית, לוויינית.**
OT					**יכול לכלול, לדוגמה, טלוויזיה במעגל סגור, מערכות HMI, בקרים ועוד.**

טיפ: הנחת העבודה שלנו היא, כי דברים אשר אינך מודע לקיומם אינם מאובטחים כראוי. לטובת ביצוע מיפוי מקיף עבור נכסי ה-IT מומלץ לקבל רשימת נכסים מאגף מערכות מידע בארגון וכן לפעול מול מחלקת הרכש, שם קיימת רשימת ספקים של מוצרים ושירותים.

עבור מיפוי נכסי OT - מומלץ להיפגש עם מנהל התפעול ועם מנהל הביטחון (בפרט בארגונים תעשייתיים).

ארגון אשר כתב תכנית המשכיות עסקית, יוכל להסתייע בהערכת עצמת הנזק לארגון ולמידת התלות של תהליכי הארגון בנכסי המידע (שימוש ב BIA).

שים לב: רזולוציית מיפוי היעדים

מיפוי יעדי ההגנה הינו תהליך שדורש זמן ומשאבים. לטובת ביצוע התהליך בצורה אפקטיבית **יש להקפיד על הרזולוציה הנדרשת למיפוי.**

לדוגמה: מצד אחד, מובן שאין צורך לפרט את כל השרתים ואת כל עמדות הקצה, ומצד שני - הכללה גסה של כל השרתים כמקשה אחת עלולה לגרום לעלויות הגנה לא מידתיות.

שים לב: לעתים, מידע רגיש של הארגון נמצא אצל הספקים או מאוחסן בענן. כמו כן, לעיתים מידע רגיש מאוחסן בתוך קובץ ולא בתוך בסיס נתונים או מערכת מידע ייעודית. מיפוי טוב כולל גם נכסים מסוג זה. סקירת תהליכי הליבה של העסק היא דרך טובה לוודא כי המיפוי מביא בחשבון את כל הנכסים המהותיים.

שלב 2: רמת ההגנה הנדרשת

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.

טיפ: הטיות נפוצות בהערכת ערכיות הנכס
את ניתוח ערכיות-הנכסים נדרש לבצע בשיתוף הגורמים העסקיים. לעיתים עלולה להיווצר תחושת "עודף ערכיות" על-ידי בעל הנכס מהצד העסקי שסובר כי הנכס שלו הינו הנכס החשוב בארגון, אך היצמדות לתבחיני שאלון הערכיות אמורים לעזור לאמוד את המערכות על פני סקאלה אחידה נטולת הטיות.

בסיום שלב 2, יידע הארגון להגדיר את הנכסים החשובים ביותר לתפקוד העסק לעומת הנכסים המשניים.

על-מנת לענות על השאלות נדרש שיתוף פעולה צמוד של הצד העסקי בארגון, שמבין את המשמעות של הנכסים ואת מידת השפעתם על התפקוד העסקי.

שים לב:
מקובל בתחום הסייבר ואבטחת המידע לבחון את הנזק העלול להיגרם באמצעות שלוש קטגוריות:

- **פגיעה בסודיות הנתונים** – לדוגמה, תקיפת סייבר לצורך הדלפת פרטי לקוחות החוצה אל האינטרנט.
- **פגיעה באמינות (מהימנות) הנתונים** - לדוגמה, תקיפת סייבר, המשנה את נתוני הדו"ח הכספי של החברה כך שהם אינם מייצגים נכונה את מצבה.
- **פגיעה בזמינות הנתונים** – לדוגמה, תקיפת סייבר, הגורמת לכך שהמידע אינו זמין לחברה או ללקוחותיה (למשל, בעת נפילת אתר או נעילת קבצים/כופרה).

C

I

A

הגדר את רמת הערכיות עבור כל נכס באמצעות השאלון הבא:

שאלה	1	2	3	4
1. מהי רמת הנזק שייגרם לארגון **בעקבות חשיפת מידע מהנכס?** **C**	הנזק מוערך כאחד או יותר מהקריטריונים הבאים: א) עלות של עד 500,000 ש"ח לארגון. ב) השקעה של עד שני חודשי אדם לצורך טיפול באירוע.	הנזק מוערך כאחד או יותר מהקריטריונים הבאים: א) עלות לארגון של יותר מ-500,000 ש"ח, אך פחות מ-5,000,000 ש"ח. ב) השקעה של יותר מ-6 חודשי אדם, אך פחות מ-5 שנות אדם לצורך הטיפול באירוע. ג) הנכס מוגדר כמאגר מידע שחלה עליו רמת האבטחה הבינונית על פי תקנות אבטחת המידע של הרשות למשפט וטכנולוגיות מידע[1] ד) קיימת סכנה ברורה לבריאות הציבור. ה) המערכת משפיעה על שרשרת האספקה של חברה ממשלתית, או של ארגון המספק שירות חיוני לאזרחים (חשמל, מים, אנרגיה).	הנזק מוערך כאחד או יותר מהקריטריונים הבאים: א) עלות לארגון של יותר מ-5,000,000 ש"ח. ב) השקעה של יותר מ-5 שנות אדם לצורך הטיפול באירוע. ג) הנכס מוגדר כמאגר מידע שחלה עליו רמת האבטחה הגבוהה על פי תקנות אבטחת המידע של הרשות למשפט וטכנולוגיות מידע. ד) קיימת סכנה ברורה לחיי אדם.	ייגרם נזק משמעותי, אשר יכלול אחד משני התרחישים מטה: א) קיימת סכנה ברורה ומיידית לחייהם של אנשים רבים. ב) נזק כלכלי המוערך ביותר מ-20,000,000 ש"ח.
2. מהי רמת הנזק שייגרם לארגון **בעקבות שיבוש המידע הקיים בנכס?** **I**				
3. מהי רמת הנזק שייגרם לארגון **בעקבות השבתת הנכס לפרק זמן ממושך?** **A**				

ציון הערכיות לכל נכס הינו הציון הגבוה ביותר שהתקבל לשלוש השאלות (Impact = MAX 1-3).

ציון זה גם מכונה **העוצמה** של הסיכון (מסומן באות I). הציון מגדיר את פוטנציאל הנזק המקסימלי לארגון מנכס זה.

1 http://www.justice.gov.il/Units/ilita/MainDocs/shlav2.pdf

חישוב רמת הסיכון לנכס - אופן שקלול הנתונים:

יש לשקלל את עוצמת הנזק הפוטנציאלי (I) עם ההסתברות שאירוע סייבר יתרחש בנכס זה (Probability).

הסתברות (P) – מחושבת על-ידי הגדרת רמת החשיפה של הנכס (נכס שמחובר לאינטרנט ואין לו מנגנוני אבטחה חשוף מאוד לפגיעת סייבר, בעוד נכס מבודד תקשורתית בתוך חדר מאובטח חשוף פחות).

על-מנת להגדיר את רמת החשיפה לנכס יש לענות על השאלון הבא:

שאלה	1	2	3	4
1. כמה משתמשים קיימים במערכת?	1-10.	11-50.	51-500.	יותר מ-500.
2. מי הם משתמשי המערכת?	עובדים פנימיים בלבד.	ספקים חיצוניים קבועים.	ספקים חיצוניים מזדמנים.	הציבור הרחב.
3. כמה ממשקים קיימים למערכת?	ללא ממשקים.	1-5.	6-10.	יותר מ-10.
4. מהו אופי ממשק המערכת?	ללא ממשקים.	ממשקים פנים-ארגוניים.	ממשקים חיצוניים מול ספקים.	ממשקים לציבור הרחב.
5. מהו סוג המידע הקיים במערכת?	ללא רגישות עסקית.	מידע פנימי של החברה.	מידע רפואי או מידע של לקוחות.	מידע עסקי רגיש.
6. האם קיימת גישה מרחוק למערכת?	לא.	באמצעות 2FA.	באמצעות ערוץ מוצפן.	תוכנת השתלטות מסחרית.
7. מהי רמת מידור ההרשאות במערכת?	מידור מלא (הרשאות לפי קבוצות /תפקידים).	מידור פרטני (הרשאות פרטניות לעובד).	מידור בסיסי (מנהל ומשתמש).	ללא מידור (הרשאות זהות לכולם).
8. מהי רמת העדכניות של המערכת?	גרסה עדכנית ביותר.	עד 3 גרסאות אחורה.	מעל 3 גרסאות אחורה.	גרסאות שאינן נתמכות עוד על-ידי היצרן.
9. מהי מדיניות העדכונים וטלאי האבטחה?	התקנת עדכונים מלאים לפחות אחת לרבעון.	התקנת אבטחה בלבד לפחות אחת לרבעון.	עדכוני אבטחה קריטיים בלבד לפחות אחת לרבעון.	ללא תהליך עדכונים מסודר.
10. מהי רמת האבטחה הפיזית של המערכת?	נגיש לגורמים מורשים בלבד.	נגיש לכלל עובדי הארגון.	נגיש לקבלנים חיצוניים.	נגיש לכלל המבקרים בארגון.

ציון החשיפה לכל נכס הינו הציון הממוצע שהתקבל לעשר השאלות (P = Average 1-10).

ציון זה גם מכונה **ההסתברות** של הסיכון (מסומן באות P).

חישוב רמת הסיכון של הנכס (שקלול ציון עוצמה והסתברות)

על-מנת לקבל את רמת הסיכון לנכס, יש להציב בטבלה מטה את ערכי שאלון העוצמה וההסתברות (כפי שהתקבלו מהשאלונים מעמוד 25-26)

הערה: הערכים בתוך הטבלה מטה חושבו על פי הנוסחה - רמת הסיכון של הנכס = (I) *3+ (P)

הסתברות(P)/עוצמה (I)	4	3	2	1
4	[illegible]	13	10	7
3	[illegible]	12	9	6
2	14	11	8	5
1	13	10	7	4

לצפייה בחישוב רמת סיכון עבור נכס לדוגמה ראו נספח א'.

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 (הערך שהתקבל מעלה עבור רמת העוצמה I).

לצד כל בקרת הגנה בפרק 6 הוגדר האם היא נדרשת עבור נכס שציון העוצמה שלו הוא 1, 2, 3 או 4.

עבור כל נכס יש לממש את סך כל הבקרות שהערך שלהן קטן או שווה לציון העוצמה של הנכס. כך, לדוגמה, עבור נכס שציון העוצמה שלו הוא 3 נדרש ליישם את הבקרות שערכן הוא 1, 2 ו-3.

הגדרה זו מסייעת להתאים את הבקרות הנדרשות ליישום ביעד ההגנה, אל מול פוטנציאל הנזק.

שלב 4: הגדרת פערי הגנה

אל מול רשימת בקרות ההגנה המפורטות בפרק 6, בדוק מה מיושם כיום בארגון ומה נדרש לבצע. בסיום תהליך זה, הארגון יקבל רשימת פערים "רצוי מול מצוי".

מאחר שלא כל הבקרות 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 בקרות מיושמות בארגונים בצורה רוחבית, הרי שיש לא מעט מקרים, שבהם הבקרה לא יושמה במערכת ספציפית.

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

דוגמה להגדרת פערי הגנה:

הארגון מיפה את נכסיו ומצא כי שני הנכסים המהותיים לו הם: מערכת ניהול קשרי הלקוחות (CRM) ומערכת התשלום לספקים. לכן, לאחר שלב ההגדרה של פערי ההגנה, הארגון יחזיק ברשימה שיכולה להיראות כך:

בקרה	כלל הארגון	מערכת ה - CRM	מערכת תשלום לספקים
4.30: יש לממש multifactor authentication עבור התחברות חשבונות בעלי הרשאות יתר דרך הרשת	קיים חלקית	קיים	נדרש לממש
6.4: יש להגדיר ולהטמיע אמצעי אבטחה על מנת לאתר ולהתריע על שינויים בלתי מורשים בהגדרות תצורה	קיים תהליך מסודר בארגון	המערכת נמצאת בענן ואין לנו שליטה ישירה על דרישה זו	קיים
16.2: יש להשתמש בכלים חוזיים ומשפטיים בעת רכישת מערכת מידע או שירות מספקים	אין תהליך מסודר של החתמת ספקים בארגון	הספק הוחתם על הצהרה	מדובר בספק מחו"ל אשר אין באפשרותנו להחתימו. נבחן את הדרישות אל מול ההסכם הגנרי עמו

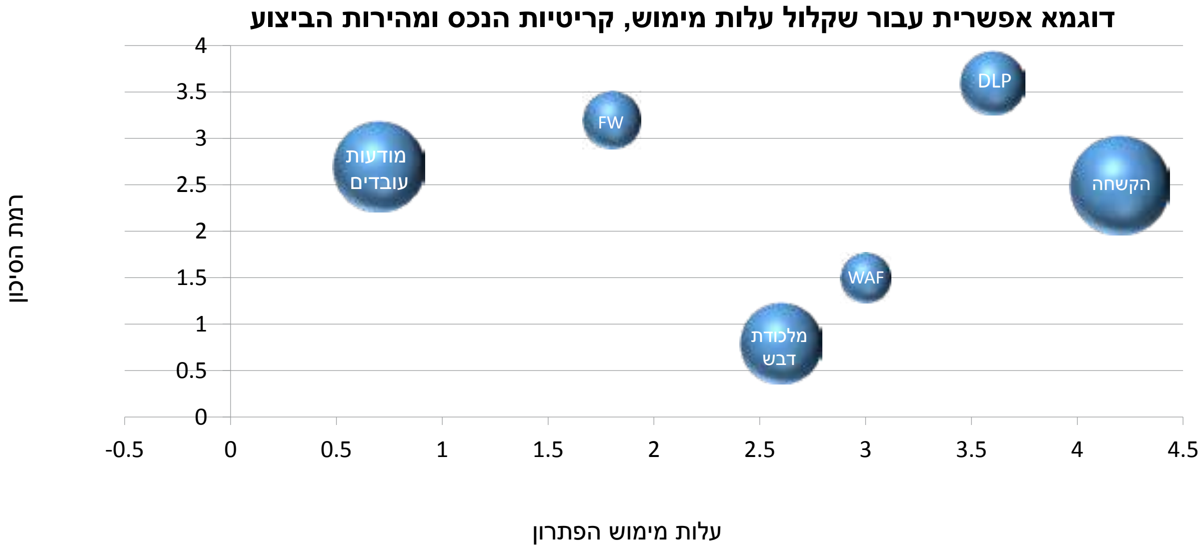
שלב 5: תכנית עבודה

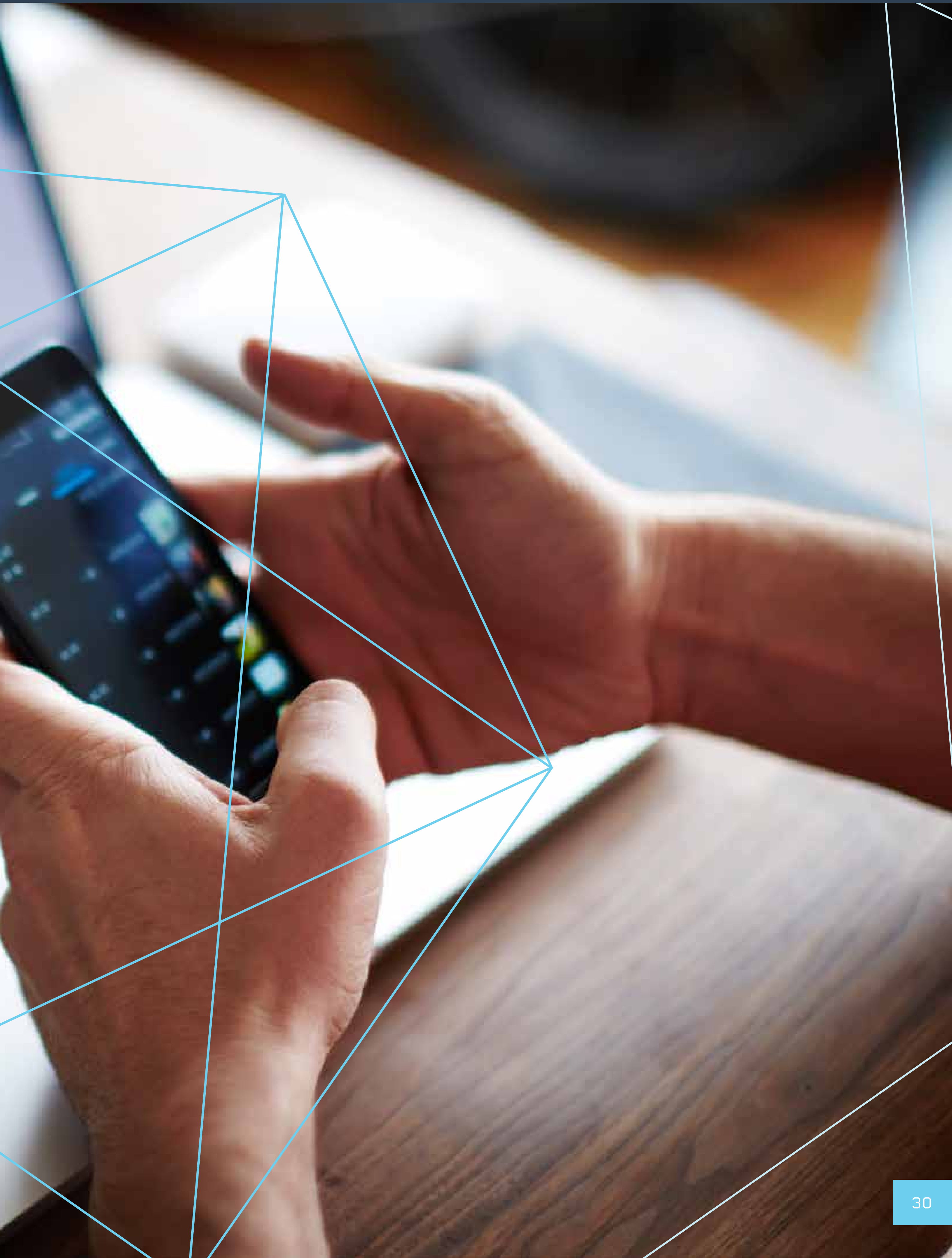
כל בקרה בפרקי הבקרות מגינה מפני סיכון עסקי, שנובע מפגיעת סייבר.

סדר העדיפויות של יישום הבקרות החסרות לארגון במסגרת תכנית העבודה ייקבע על-ידי שקלול **רמת הסיכון של הנכס, עלות הפתרון ומורכבות המימוש**.

סדר העדיפויות של יישום הבקרות בתכנית העבודה ייקבע על-ידי שקלול:

- **רמת הסיכון של הנכס** – ציר ה-Y בדוגמה מטה.
- **עלות מימוש הפתרון** – ציר ה-X בדוגמה מטה.
- **מהירות יישום הפתרון** – מבוטא באמצעות גודל העיגול בדוגמה מטה.





6 // פרקי הבקרות - לשלבי הביצוע והבקרה

6.1 מבוא

דרישות ההגנה מארגון מכונות בשפה המקצועית – בקרות. לטובת הגנה על הארגון בתחום הסייבר, הארגון נדרש לממש בקרות בתחומים שונים. בקרות אלו כוללות תהליכים, נהלים, מערכות הגנה וטכנולוגיות, אשר הארגון מיישם במטרה להפחית את הסיכון להתממשות אירוע במרחב הסייבר.

בקרות אלו מאוגדות על-פי הנושאים השונים, כגון בקרות להגנה על שרתים ותחנות קצה, בקרות על ניהול משתמשים, בקרות ניטור ועוד.

לצורך מיקוד, בקרות הגנה קריטיות (בעלות הערך "עלות מול תועלת" הגבוה ביותר) סומנו במסמך זה באמצעות אייקון מפתח.

לטובת בנייה של תורת הגנה פרופורציונלית, הבקרות במסמך זה סווגו לרמות שנעות בציר של 1-4, כאשר בקרות מרמה 1 הן הבקרות הבסיסיות ביותר ואילו בקרות מרמה 4 הן בקרות מורכבות וכאלו הדורשות השקעת משאבים רבים הבסיסיות ביותר, אשר נדרשות מכל ארגון ולכל נכס ואילו בקרות מרמה 4 הן כאלו אשר נדרשות עבור יעד הגנה שפוטנציאל הנזק שלו הינו 4.

6.2 כיצד להגן

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
זיהוי Identify					
1. אחריות דירקטוריון/אחריות הנהלה: נכסי סייבר מהווים כיום נכסים קריטיים, התומכים ביעדי הארגון. הגנה עליהם יכולה להיות חשובה כמו הגנה על נכסים פיזיים, כספים ועובדים. הגנה בסייבר הינה באחריות הנהלת הארגון. אחריות זו נדרשת להשתקף במפורש בארגון באמצעות תפיסת ההגנה בסייבר של הדירקטוריון, מדיניות ההגנה בסייבר של ההנהלה ונוהלי ההגנה בסייבר הארגוניים. כמו כל תכנית הגנה, הגנה בסייבר אינה הרמטית, וההנהלה נדרשת להחליט על רמת הסיכון שהיא מוכנה לקחת בהתחשב בעלויות המימוש של הבקרות למול מחירי התממשות הסיכון בתוך הארגון והשפעותיו על לקוחות, על ספקים ועל יעדים לאומיים. כמו כן, על הנהלת הארגון ליישם מנגנונים לטיפול באירועי סייבר שעלולים לקרות על-מנת לצמצם את הנזק לארגון.					
אחריות דירקטוריון	1.1	דירקטוריון הארגון יאשר את מדיניות אבטחת המידע והגנת הסייבר הארגונית אחת לשנה ויקצה משאבים נדרשים לטובת מימושה	אחת לשנה תוצג מדיניות אבטחת המידע והגנת בסייבר הארגונית, כנגזרת ממפת סיכוני הסייבר של הארגון לדירקטוריון. הדירקטוריון יאשר את מפת הסיכונים ואת המדיניות הנגזרת ממנה	מומלץ למנות בקרב חברי הדירקטוריון נציג אחד שיהיה מוקד ידע (ברמה הניהולית) בנושא. לטובת עמידה בדרישה זו, חשוב לוודא כי מפת הסיכונים מוצגת לחבר המנהלים בשפה העסקית לצד המענה הקיים כיום בארגון והפערים הנדרשים לטובת צמצום הפער והגעה לרמת סיכון מקובלת. חשוב כי מועצת המנהלים תגדיר את רמת הסיכון אותה הארגון מעוניין לקחת ("תיאבון הסיכון" - לדוגמה כפונקציה של איום ייחוס או של מבחן עלות/תועלת)	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אחריות הנהלה	1.2	יש לאשר אחת לשנה את מפת הסיכונים הנוכחית כפי שהיא עולה מסקר סיכוני סייבר ארגוני	הארגון ימפה את הסיכונים אליהם הוא חשוף בתחום הסייבר. הסיכונים ידורגו ויוצגו להנהלה לצד הגדרת המענה המתוכנן.	בארגונים בעלי נכסים מרמה 2 ניתן לבצע את הסקר עצמאית על ידי מיפוי הנכסים והתהליכים העסקיים הרגישים ועבודה על פי מתודת הערכת הסיכון של תורת ההגנה. בארגונים לטובת מימוש תחומי האחריות המובאים במסמך זה, הנהלת הארגון תגדיר את הגורם האחראי על הנושא בחברה (מנהל אבטחת מידע או בעל תפקיד אחר אשר יהיה אמון על תחום זה). עבור ארגונים בעלי יעדי הגנה מרמת ערכיות 3 ומעלה מומלץ להיעזר בגורם חיצוני לטובת ביצוע הסקר אחת לתקופה.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אחריות הנהלה	1.3	יש לזהות חקיקה והוראות מכח חוק הישימות לארגון	כל דרישה רלוונטית מתוקף חוק, תקן, חוזה כלפי הארגון, וכל האמצעים בהם הארגון נוקט על מנת לעמוד בדרישה, יוגדרו במפורש, יתועדו ויעודכנו עבור כל מערכת מידע ועבור פעילויות הגנה בסייבר לארגון בכללותו.	1. יש להכין רשימה של כל הדרישות החוקיות, רגולציות והתחייבויות חוזיות שזוהו. דוגמאות לדרישות חוקיות ורגולטוריות יכולות להיות עמידה בדרישות משרד המשפטים (רישום מאגרי מידע והגנה על הפרטיות), הגנה על כרטיסי אשראי בהתאם לדרישות תקן PCI , דרישות של ספקים ולקוחות לעמידה בנהלי ההגנה בסייבר שהארגון חתם עליהם 2. יש לבצע ולתעד מבדקי ציות אשר מראים כי הדרישות הנ"ל מבוצעות בארגון 3. יש להגדיר את הגורם בארגון אשר אמון על נושא אבטחת המידע כחלק מהגדרת תפקידו	2

2. ניהול והערכה של סיכונים:

תורת ההגנה בסייבר לארגון מתבססת על תהליך ניהול והערכה של סיכוני סייבר. זהו תהליך מחזורי, שיש לבצעו כאשר סביבת הסייבר של הארגון משתנה – הן בתוך הארגון (קליטת מערכות חדשות, שינויים טכנולוגיים, שינוי בתהליכים עסקיים וכד') והן מחוץ לארגון (שינוי מתמיד של מרחב האיומים בסייבר על הארגון). על-פי תורת הגנה זו, בניהול הסיכונים הארגון נדרש לזהות את יעדי ההגנה, להגדיר מה הן הבקרות הנדרשות על-מנת להגן עליהם ולבנות תכנית עבודה מתאימה.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
ניהול סיכונים והערכת סיכונים	2.1	יש להגדיר תהליך להגדרת גבולות הארגון, מיפוי יעדי ההגנה של הארגון, והערכת רמת הערכיות של יעדי ההגנה	מיפוי יעדי ההגנה יכול להתבצע על ידי מיפוי תהליכי עבודה בארגון, מערכות, מאגרים ותשתיות טכנולוגיות. רמת הערכיות של יעדי ההגנה נקבעת בהתאם להשפעות של פגיעה בחסיון, זמינות ושלמות על יעדי ההגנה.	הגדרת היעדים תכלול את כלל ההיבטים בהם על הארגון לבחון את רמת הסיכון הנוכחית אל מול הרמה הרצויה. יעדים אלו יכולים לכלול בין היתר רשימת מערכות, תשתיות, תהליכים עסקיים, אנשי מפתח וכל מה שהארגון הגדיר לעצמו כיעד להגנה בסייבר. יש לשים לב כי ישנם יעדי הגנה אשר נתווספו בשנים האחרונות וניתן בטעות שלא למפות אותם. מיפוי טוב יכלול לדוגמה גם את עולם ה- OT לרבות מצלמות אבטחה, מעליות ומדרגות חשמליות, פס ייצור ורכיבים נוספים "משולבי תוכנה" אשר לעיתים קרובות אינם מנוהלים על ידי אנשי המחשוב בארגון (אינם נכסי IT קלאסיים). נכסים אלו נמצאים פעמים רבות בלב העשייה של תפעול הארגון והם חשופים לא פחות למתקפת סייבר (כגון גלגל ענק בפארק שעשועים, משאבת דלק, מערכת המיזוג המרכזית, מערכת שו"ב על טורבינות ועוד)	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
ניהול סיכונים והערכת סיכונים	2.2	יש להגדיר וליישם תהליך תקופתי של הערכת סיכוני סייבר בהתאם למתאר האיומים של הארגון, לרמת החשיפה של יעדי ההגנה לאיומים, ולבקרות ההגנה המיושמות בארגון.	מטרת תהליך הערכת הסיכונים הינה לספק מפה עדכנית של סיכוני הסייבר בפועל (סיכונים שיוריים) במטרה להגדיר תכנית לטיפול בסיכונים. יש לבצע את הסקר באופן תקופתי ולעדכנו בעת שינויים בתהליכים ובמערכות הארגון.	ניתן לבסס את תהליך הערכת הסיכונים על תורת הגנת הסייבר.	2

3. בקרה, ביקורת ותאימות:

כל ארגון במשק נדרש להגן על נכסי הסייבר שלו על-מנת לעמוד בדרישות החוק הבסיסיות בהיבטי הגנה על זכויות יוצרים (למשל, לא להשתמש בתוכנות לא מורשות), להגן על רשומות ארגוניות ולהגן על מידע פרטיות שמצוי במאגרי החברה. כמו כן, מידע צופן, אם קיים, נשמר על-פי כללי המחוקק הרלוונטי. חלק מהארגונים נדרשים לעמוד בדרישות חוק נוספות. על הארגון לבנות מנגנוני בקרה על-מנת לוודא באופן שוטף, כי הוא עומד בדרישות החוק, הרגולציה הרלוונטית על-פי המגזר (בריאות, ביטוח, שוק ההון וכו'), תורת הגנה זו, מדיניות הדירקטוריון והחלטות ההנהלה בהיבטי ההגנה בסייבר.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרה, ביקורת ותאימות	3.1	יש לסקור את תהליכי המידע השונים תקופתית וזאת לצורך וידוא לעמידה בתקני אבטחה, מדיניות וכל דרישת אבטחת מידע	יש לבצע "סקר הנהלה" על התהליכים השונים לצורך וידוא ציות לתקנים ולדרישות אבטחת מידע. סקר זה יבחן את הפרמטרים השונים בתחום ההגנה בסייבר ויספק תמונת מצב להנהלה באשר לחוזקות ולחולשות של הארגון	סקר הנהלה נותן ראיה רוחבית על מצב הארגון מבחינת רמת ההגנה הנוכחית שלו. סקרים אלו יאפשרו להציג לארגון את התחומים בהם הוא נדרש להתמקד לעומת תחומים בהם הארגון יותר בשל (בדומה למודל הבשלות של CMMI). בין התחומים שהסקר יכול להתייחס אליהם ניתן להגדיר לדוגמא: פיתוח מאובטח, רמת מודעות, יכולות ניטור, רמת הבשלות של צוותי התגובה, נהלי הארגון וכו' חשוב לוודא כי התהליכים אשר הוגדרו קריטיים לארגון במסגרת התכנית להמשכיות עסקית של הארגון מקבלים מענה הגנתי ראוי	2
בקרה, ביקורת ותאימות	3.2	הארגון יוודא כתיבת מדיניות הגנה אשר תתייחס לכל ההיבטים המכוסים במסמך זה.	מטרת הבקרה הינה לוודא כי הנהלת הארגון הגדירה את הקווים המנחים שלה בהיבטי ההגנה עבור הנושאים השונים כגון מדיניות הגנה במשאבי אנוש, מדיניות הגנה בשרשרת אספקה, מדיניות ניטור ובקרה וכו'		2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרה, ביקורת ותאימות	3.3	יש לוודא כי מערכות המידע השונות עומדות בסטנדרט אבטחת המידע/הגנת סייבר הארגוני וכי הן מיושמות באופן מאובטח על בסיס קבוע - בהתאם למדיניות אבטחת המידע והגנת הסייבר הארגונית	יש לבצע סקרים תקופתיים במטרה לוודא כי מערכות המידע השונות עומדות בדרישות אבטחת המידע והגנת הסייבר שהארגון הגדיר וכי הן חסינות כנגד מתקפות	יישום נכון של בקרה זו יתבצע באמצעות כתיבת תכנית ארגונית שנתית או רב שנתית לביצוע סקרי סייבר תקופתיים על נכסי הארגון. הסקרים יכולים להיות במתכונת של קופסה לבנה/אפורה או שחורה כאשר יש לתת עדיפות לסקירת מערכות שקיבלו בשאלון הערכיות ציון גבוה. עבור מערכות מרמה 3 מומלץ כי הבדיקה תיעשה על ידי גורם חיצוני לארגון ובלתי תלוי	2
בקרה, ביקורת ותאימות	3.4	בדיקה אוטומטית של רמת ההגנה של הארגון	יש להשתמש בכלים ממוכנים אשר מדמים את פעילות התוקף באופן אוטומטי	מאחר וביצוע מבדקי חדירה הינה פעולה אשר מצריכה על פי רוב מעורבות אנושית, היכולת לכסות מערכות רבות ובזמן אמת הינה מוגבלת. לטובת מתן מענה על מגבלות הזמן והידע, קיימים מספר מוצרים אשר מאפשרים למנהל ההגנה לקבל חיווי באמצעות כלים שמדמים "משחק מלחמה" אשר תוקף את הארגון בשיטות שונות במטרה לזהות וקטורי תקיפה וחולשות לטיפול.	4
הגנה Protect					

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
4. בקרת גישה: גורמים רבים נדרשים לגשת למידע הארגוני לצורך תפקודם התקין – הן גורמים אנושיים (עובדי הארגון, לקוחותיו, ספקיו) והן גורמים טכנולוגיים (אפליקציות). הללו נדרשים לגישה למערכות ולסוגי מידע שונים. במטרה למנוע ניצול לרעה של גישות אלו, על הארגון להטמיע בקרות והגנות, אשר יבטיחו כי כל גורם יוכל לגשת אך ורק למידע שהוא זקוק לו, וכי אין הוא עושה בו שימוש שאינו מורשה. כמו כן נדרש לוודא, כי הגורמים הניגשים מזוהים ומאומתים באופן חד משמעי. לצורך כך נדרש לנהל את המשתמשים השונים (אנושיים ואפליקציות) באופן שוטף, להוסיפם, לבטלם ולשנות את הרשאותיהם על-פי הנדרש ולתעד את פעילותם. משנה זהירות נדרשת במתן הרשאות גבוהות לאנשים ולאפליקציות (תקיפות רבות עושות שימוש בהתחזות לגורמים בעלי הרשאות גבוהות) ולהזדהות מרחוק ברשת הארגונית. בקרת גישה היא אחד התחומים הבסיסיים בהגנת הסייבר של הארגון והוא דורש הקפדה על הפרטים.					
בקרת גישה	4.1	יש לפתח, לתעד וליישם מדיניות בקרת גישה.	מדיניות בקרת הגישה נועדה לוודא כי רק גורמים מורשים יכולים לגשת למידע ומערכות הארגון, לצפות ולבצע שינויים, וכל זאת בהתאם להגדרות תפקידם ובכפוף לפיקוח.	ניתן לכלול את מדיניות בקרת הגישה כפרק במדיניות אבטחת המידע הארגונית	2
בקרת גישה	4.2	יש להגדיר חשבונות משתמשים אשר תומכים בפונקציות העסקיות של הארגון	לכל הפחות, יש להפריד בין חשבון "מנהל" לחשבון "משתמש". כמו כן יש להגדיר משתמשים אשר מנהלים את פונקציות האבטחה במערכת (כגון יצירת משתמשים, ניהול הרשאות גישה ומערכת, ניהול מערכות אבטחת מידע ועוד)	יצירת משתמשים ארגוניים בתור משתמשים רגילים, חלוקת משתמשי "מנהל" לפי תפקיד מוגדר בלבד (מנהלי מערכת)	1

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.3	יש לסקור את רשימת המשתמשים על בסיס תקופתי ולעדכנה בהתאם	הארגון יסקור מדי תקופה מוגדרת את רשימת המשתמשים ויסיר משתמשים לא רלוונטיים בהתאם לצורך.	תהליך סקירת משתמשים תקופתי ותיעודו בנוהל בקרת גישה ארגוני, ביצוע מעקב שוטף באמצעות מערך ממוכן או ידני אשר יבוצע על ידי מנהלי המערכות. סקירה זו מתבצעת במטרה לאתר הן משתמשים לא פעילים/ כאלו שעזבו את הארגון והן לאשרר את רמת ההרשאות של המשתמשים הקיימים. כך לדוגמה במידה ועובד שינה תפקיד בארגון, במקרים רבים הוא "גורר עימו" את ההרשאות הקודמות. סקירה של מנהל המערכת מהצד העסקי עשויה להציף מקרים כאלו.	2
בקרת גישה	4.4	יש לנטרל/להסיר חשבונות זמניים באופן אוטומטי לאחר פרק זמן מוגדר	הארגון יגדיר תקופת זמן קבועה שלאחריה יחסמו חשבונות שמניים באופן אוטומטי.	במידת האפשר להגדיר חשבונות זמניים עם הקצבת זמן לכל מערכת המתממשקות לActive Directory או מערך ניהול זהויות (IDM), חשבונות אשר דורשים הארכה נדרשים באישור מיוחד.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.5	יש לנטרל/להסיר חשבונות לא פעילים באופן אוטומטי לאחר פרק זמן מוגדר	הארגון ינטרל / יסיר חשבונות לא פעילים לאחר תקופת זמן קצובה המוגדרת כחלק מהמדיניות.	יש להוציא דוחות תקופתיים לגבי פעילות Login של משתמשים במערכות המתממשקות ל Active Directory וכן חשבונות אשר ננעלו לפני תקופה ארוכה (כפי המוגדר בנוהל בקרת גישה). יש להסיר חשבונות אשר נמצאו.	3
בקרת גישה	4.6	יש לתעד ביומן רישום אוטומטי (רישום Log) כל יצירה, שינוי, אפשור, ניטרול והסרה של חשבון	הארגון יתעד כל שינוי בחשבונות משתמשים וינהל מעקב אוטומטי או ידני ביצוע התיעוד.	ניתן ליישם באמצעות הניטור (SIEM) אשר יתממשק למערכי ניהול ההרשאות בארגון - Active Directory, IDM, שרתים, מערכות אפליקטיביות וכן ציודי תקשורת ואבטחת מידע	3
בקרת גישה	4.7	יש לנטר פעילות חשבונות לזיהוי שימוש חריג, ולדווח על שימוש חריג לבעלי התפקידים המתאימים	דוגמאות לשימוש חריג: התחברות למערכת בימים ושעות מסויימות, התחברות מכתובות שאינן תואמות לתבניות השימוש הרגיל.	ניתן ליישם באמצעות מערכת SIEM לניטור משתמשים בקבוצות רגישות, איסוף המידע יעשה ממקורות כגון Active Directory, ציודי תקשורת ואבטחת מידע (חומת אש וכו')	3
בקרת גישה	4.8	יש להגדיר ולאכוף תנאים לחסימת שימוש בחשבונות	דוגמאות לתנאי חסימת כניסה: סופ"ש, שעות הלילה	ניתן להגדיר מגבלת כניסה בהגדרת משתמש בתוך חשבון הActive Directory, המגבלה לא תאפשר התחברות בשעות שאינן שעות פעילות.	4

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.9	יש להגדיר ולאכוף הרשאות גישה לוגיות למערכת ולמידע בהתאם למדיניות בקרת הגישה	בקרת הגישה יכולה להיעשות ברמה אישית (identity-based) או ברמת תפקיד (role-based), ומטרתה לשלוט בגישה של ישויות (משתמשים או תהליכי מחשב) לאובייקטים (קבצים, רשומות, מכשירים ועוד).	המשתמשים ינוהלו בצורה מרכזית באמצעות Directory ארגוני כגון Active Directory, OpenLDAP ועוד. מערך ההרשאות ימופה לפרופיל המשתמש.	1
בקרת גישה	4.10	יש להגביל את הרשאות המשתמשים למינימום ההכרחי הדרוש לביצוע תפקידם	הארגון יגדיר רמת הרשאות מינימלית לכל תפקיד וכן רמת הרשאות מינימלית למשתמש בסיס (ללא תפקיד מוגדר) אך נדרשת לו גישה למערכות הארגון.	הרשאות משתמשים יינתנו בהתאם לתפקידם, יוגדר פרופיל בסיסי אשר יינתן למשתמש והרשאות נוספות יינתנו בהתאם לצורך ובאישור ממונה ישיר - במידה וקיימת מערכת IDM ניתן למפות פרופיל בסיס וכן פרופילים אפליקטיביים. לאחר טיוב התהליך ההרשאות יינתנו בהתאם לתפקיד.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.11	יש להגדיר בעלי תפקידים, לבצע הפרדה בין תחומי אחריות Separation) (of duties ולהביא אותה לידי ביטוי במתן הרשאות למערכת	מטרת ההפרדה בין תחומי אחריות הינה להקטין את הפוטנציאל לשימוש לרעה של הרשאות. ההפרדה כוללת, לדוגמה, הפרדה של פונקציות עסקיות בין עובדים או בעלי תפקידים; וכן וידוא שצוות אבטחת המידע אשר מנהל את בקרת הגישה אינו מנהל גם את פונקציות הביקורת על בקרת הגישה.	יש לבצע מיפוי הרשאות אשר תומך במערך הפרדת סמכויות וליישם אותו בפרופילי הרשאות של משתמשים כגון: מפתח למול בודק תוכנה (לכל אחד מהם תהיה גישה לסביבה שונה, מפתח יעבוד על סביבת פיתוח - סביבה נמוכה, בודק יעבוד על סביבה גבוהה יותר - קדם ייצור) וכו'. מומלץ לבחון מימוש פתרון pim privileged identity management \ pam privileged access	3
בקרת גישה	4.12	הגישה אל מערכות ויישומים רגישים תתבצע אך ורק דרך רכיב תיווך ייעודי מוקשח (טרמינל)	לטובת החלקת מדיניות אחידה "מוקשחת" אל משאבים רגישים, יש לוודא כי הגישה אליהם תתבצע אך ורק לאחר מעבר דרך רכיב התיווך (כגון שרת פרוקסי או טרמינל)	ניתן לממש בקרה זו באמצעות הגדרת גישה ברכיב חומת האש כי התחברות אל נכסים רגישים תותר אך ורק מרכיב הקישור אשר כולל את הבדיקות והמדיניות הארגונית המחמירה (כגון מניעת יכולת ביצוע "העתק/ הדבק", מניעת יכולת הורדת קבצים, נעילת CLI וכו')	4
בקרת גישה	4.13	יש להגדיר מהם העובדים אשר מורשים לפרסם מידע במערכת נגישה ציבורית (כמו אתר אינטרנט), וליישם זאת הרשאה זו כחלק מתהליך מתן ההרשאות	הארגון יגדיר משתמשים אשר תפקידם דורש יכולת פרסום מידע במקורות פומביים ויתעד כחלק מנהלי הארגון את התפקידים הנ"ל	במערכות ניהול תוכן (CMS) יש לתת הרשאות עריכה ולמשתמשים ולאפשר הרשאות פרסום רק למנהלי התוכן	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.14	יש להגביל התחברות משתמש למערכת לאחר מספר ניסיונות התחברות כושלים, באמצעות נעילת האפשרות לביצוע התחברות במשך פרק זמן מוגדר או עד לשחרור ע"י מנהל מערכת	מטרת הבקרה היא להתמודד עם הסיכון של התקפות מניעת שירות. יש ליישם את הבקרה בן ברמת החיבור למערכת ההפעלה והן ברמת חיבור לאפליקציות ספציפיות.	ניתן להגביל את מספר הניסיונות הכושלים להתחברות בתוך ה Group Policy וה Domain Policy	2
בקרת גישה	4.15	יש להגביל את מספר החיבורים המותרים בו-זמנית של משתמש בודד ככל הניתן	מטרת הבקרה הינה לזהות התחברות משני מקומות שונים באמצעות אותם פרטי הזדהות. תרחיש כזה עלול להוות אינדיקציה לשימוש לא מורשה בחשבון המשתמש.	ניתן להגביל מספר התחברויות בו זמנית בתוך מדיניות ה Remote Logon ב Group Policy	3
בקרת גישה	4.16	יש לנעול חיבורים כתוצאה מחוסר פעילות זמני, ולא לאפשר את המשכיות החיבור עד להזדהות ואימות חוזר של המשתמש. כחלק מביצוע נעילת החיבור יש להסתיר מידע שהוצג על המסך טרם הנעילה.	בקרה זו מיושמת בדרך כלל ברמת מערכת ההפעלה, אך ניתן ליישמה גם ברמת האפליקציה. יש לציין כי נעילת חיבור אינה תחליף מקובל להתנתקות מהמערכת (Log-out).	ניתן לממש באמצעות הגדרת שומר מסך. במידת האפשר יש לוודא כי מערכות בפיתוח עצמי וכן מערכות מוצרי מדף יכללו מנגנון של Session time out.	3
בקרת גישה	4.17	יש לכתוב וליישם הגבלות שימוש ודרישות קונפיגורציה להתחברות מרחוק	נדרשת מדיניות העוסקת בחיבורים מרחוק אשר מגדירה את מגבלות השימוש בהתחברות מרחוק למשאבי הארגון וכן נדרש שימוש במערכות אשר מספקות גישה מרוחקת מאובטחת למשאבי הארגון	ניתן לממש גישה מאובטחת לארגון באמצעות מערכות כגון VPN או SSH אשר עומדות בקנה אחד עם המדיניות הארגונית להתחברות מרחוק למשאבי הארגון.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.18	יש לנטר התחברויות מרחוק	ניטור אוטומטי של חיבורים מרחוק מאפשר לארגונים לזהות התקפות סייבר, ובנוסף מאפשר לוודא ציות לנהלי הגישה מרחוק באמצעות בקרה על פעילויות המתבצעות במהלך החיבור המרוחק.	ניתן לממשק את מערכות הגישה מרחוק למערכות הניטור כגון ה SIEM ולוודא שאכן נרשמים אירועים על התחברות. יש לשים דגש מיוחד על התחברות ספקים חיצוניים לתוך הארגון מרחוק לצורך תחזוקה ותמיכה ולנטר את הפעילות שלהם בצורה אפקטיבית (כגון באמצעות כלי ניטור והקלטת מסכים)	3
בקרת גישה	4.19	יש לנתב את כל ההתחברויות מרחוק דרך מספר מוגדר של נקודות בקרת גישה מנוהלות managed network) access control (points	הקטנת מספר נקודות בקרת הגישה מצמצם את משטח התקיפה.	יש לבצע סקירה של נקודות הגישה לארגון (מיפוי שטח התקיפה) ולהעביר שרותים ארגוניים רגישים לאזור רשת אשר נמצא מאחורי חומת האש, יש לנתב את התעבורה אליו מכיוון רשת ה VPN, בגישה מתוך שרת הVPN. יש לבטל גישה ישירה מהעולם לשירותים אלו.	3
בקרת גישה	4.20	יש ליישם אמצעי הגנה נוספים בעת הרצה של פקודות רגישות באמצעות חיבור מרחוק	פקודות רגישות הן, למשל, אתחול שרת או ביטול טרנזקציה. יש לוודא כי לא ניתן להריץ פקודות אלו במסגרת התחברות רגילה למערכת.	גישה לשרתים רגישים וכן לניהול המערכות תתבצע מרשת הניהול שהיא מחוץ לטווח (Out Of Band) והגישה אליה מתבצעת באמצעות שרת ניהול ייעודי (הדורש הזדהות ואימות)	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.21	יש לאסור התחברות מרחוק למערכת לצורך ניהולה, וכן להגביל גישה למערכת מרשתות שאינן מנוהלות על ידי הארגון	הארגון לא יאפשר גישה ישירה מרחוק לממשקי ניהול אלא בצורה מאובטחת בלבד, לאחר אימות והתחברות לרשת ניהול.	יש למנוע Administrator Login בעת התחברות מרחוק למערכות (ניתן לבצע גם בלינוקס על ידי ביטול (PermitRootLogin	4
בקרת גישה	4.22	יש להגן על חיבור למערכת מרשת אלחוטית באמצעות אימות משתמשים/ מכשירים, שימוש בהצפנה והגדרת הגבלות שימוש	הארגון יאפשר חיבור לרשת אלחוטית רק עבור מכשירים המנוהלים/מאומתים על ידו וכן רק בעבור משתמשים מזוהים. מטרת הבקרה הינה למנוע שימוש לא לגיטימי ולא מזוהה ברשת האלחוטית.	הגישה אל הרשת האלחוטית תותר אך ורק לאחר הזדהות אל מול ה Access point.	2
בקרת גישה	4.23	יש לכייל את עוצמת השידור של האות האלחוטי על מנת להפחית את הסיכוי שאותות יקלטו מחוץ למתקן הארגון	הארגון יסקור את אותות השידור של הרשתות האלחוטיות ויוודא כי האות לא חורג מטווח המוגדר מראש.	ניתן לבצע מיפוי טווחי קליטה באמצעות סקירה מרחבית וכן ציוד ייעודי (Radio) בתיאום עם ספק המערכת האלחוטית, כמו כן ניתן לבצע עצמאית באמצעות Radio Analyzer וסריקה מסביב לשטח המבנה.	4
בקרת גישה	4.24	יש לאסור התחברות למערכות ארגוניות מתוך רשת אלחוטית	גישה למערכות הארגון תתאפשר רק עבור ציוד מחשוב המחובר באמצעות חיבור קווי לרשת הארגון.	אין לחבר את הרשתות האלחוטיות לרשת הארגון אלא אך ורק לנתב אינטרנט ייעודי לטובת גלישה בלבד, ניתן כמו כן ליישם שרת מתווך (פרוקסי) של הרשת האלחוטית	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.25	יש לכתוב וליישם הגבלות שימוש ודרישות תצורה של התחברות באמצעות מכשירים ניידים	הארגון יכתוב מדיניות ויישם בקרות אבטחת מידע על מכשירים ניידים הניגשים למערכות הארגון. על המדיניות להתייחס הן למכשירים המסופקים ומנוהלים על ידי הארגון וכן על מכשירים אישיים של עובדי ואורחי הארגון.	יש לכתוב מדיניות מכשירים ניידים אשר מגדירה מה הם גבולות השימוש במכשירים ניידים (כגון טלפונים סלולריים וטאבלטים) - מה ניתן לשמור או לגשת אליו בארגון באמצעות המכשיר הנייד	2
בקרת גישה	4.26	יש להטמיע הצפנה מלאה של המידע המאוחסן על מכשירים ניידים על מנת להגן על סודיות ושלמות המידע	הארגון יצפין את שטח הדיסק של המכשירים הניידים המתחברים למערכות שלו.	ניתן ליישם באמצעות Policy אשר יופץ למכשירים הניידים, באמצעות Mobile Device Management נתמך ברוב מכשירי האנדרואיד ואפל	3
בקרת גישה	4.27	יש לאסור על התחברות למערכת רגישה באמצעות מכשירים ניידים	הארגון יחסום ויאכוף באמצעות בקרות טכנולוגיות גישה למערכות ארגוניות רגישות באמצעות מכשירים ניידים.	ניתן ליישם באמצעות זיהוי הדפדפן במכשיר הנייד או לחלופין במערכות רגישות לא לחשפן לרשתות הנגישות למכשירים ניידים (גם לא מאחורי סגמנט ה VPN או לחלופין לחבר את המכשירים הניידים לסגמנט VPN שונה משאר המחשבים). הזיהוי יכול להתבצע גם באמצעות זיהוי ההתקן המתחבר על ידי בדיקת כתובת ה MAC של האמצעי המתחבר.	4

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.28	יש לזהות ולאמת באופן ייחודי את משתמשי המערכת	הארגון יאמת באופן חד ערכי משתמש המתחבר למערכות הארגון.	לכל משתמש מערכת יהיה שם משתמש ייחודי (אשר ימופה לאדם מסויים), משתמשים גנריים יצויין מי בעל המשתמש הגנרי, משתמשים אפליקטיביים יהוי בבעלות מנהל המערכת	2
בקרת גישה	4.29	יש לממש multifactor authentication עבור התחברות חשבונות בעלי הרשאות יתר דרך הרשת	הארגון ייישם הזדהות מקומית במספר אמצעי זיהוי (שניים או יותר) לחשבונות רגישים.	ניתן לדוגמה לממש באמצעות כרטיסים מגנטיים, טביעות אצבעות או מנגנונים אחרים הנתמכים על ידי Active Directory	2
בקרת גישה	4.30	יש לממש multifactor authentication עבור התחברות לוקאלית של חשבונות בעלי הרשאות יתר	הארגון ייישם הזדהות במספר אמצעי זיהוי (שניים או יותר) לחשבונות רגישים בהתחברות מקומית.	ניתן לממש באמצעות כרטיסים מגנטיים, טביעות אצבעות או מנגנונים אחרים הנתמכים על ידי Active Directory	3
בקרת גישה	4.31	יש לממש מנגנון אימות שהוא -replay resistant עבור התחברות של כל חשבון (בדגש על מנגנון אימות בעל אמצעי הצפנה)	הארגון ייישם מנגנון הזדהות חסין האזנה (כגון מנגנון זיהוי אשר מנפיק הזדהות חד פעמית) עבור כלל החשבונות	ניתן לממש באמצעות מנגנונים כגון כרטיס חכם או סיסמא חד פעמית.	4
בקרת גישה	4.32	יש לממש multifactor authentication לצורך התחברות מרחוק למערכת	הארגון ייישם הזדהות מרוחקת במספר אמצעי זיהוי (שניים או יותר) למערכות הארגון.	ניתן לממש באמצעות מנגנונים כגון כרטיס חכם או סיסמא חד פעמית בגישה מרחוק למערכות כגון VPN	2
בקרת גישה	4.33	יש לזהות ולאמת באופן ייחודי מכשירים מהם מתבצעת התחברות	הארגון יזהה באופן חד ערכי מכשירים אשר מתחברים לרשת הארגונית.	ניתן לממש באמצעות תעודות דיגיטליות המונפקות למחשבי קצה ומחשבים ניידים.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרת גישה	4.34	יש לנהל אמצעי הזדהות למערכת, לרבות: בחירת אמצעי זיהוי של עובד או בעל תפקיד, השמתם וחסימתם לאחר פרק זמן של חוסר שימוש	יש לנהל מאגר של אמצעי הזדהות והנפקתם, כמו כן ניתן לבצע ביטול אמצעי הזדהות באמצעות מערכת מרכזית	ניתן לממש באמצעות מערכת לניהול OTP במידה ונדרש אמצעי זיהוי חזק יותר מאשר הקיים במערכת	2
בקרת גישה	4.35	על הארגון ליישם אכיפת מדיניות סיסמאות באמצעים טכנולוגיים	על אכיפת המדיניות לכלול לכל הפחות: הגדרת מורכבות מינימלית, שונות מסיסמאות קודמות, זמן תפוגה מוגדר, דרישה להגדרת סיסמה חדשה לאחר התחברות ראשונית	ניתן לממש באמצעות Group Policy I Domain Policy	2
בקרת גישה	4.36	יש לוודא כי הפידבק ממערכת המידע במהלך תהליך האימות לא יספק מידע שעלול לגרום נזק במידה ויתגלה או יבוצע בו שימוש ע"י גורמים בלתי מורשים	יש להסוות את שדות האימות באמצעות הסתרת הסיסמא	ניתן לממש באמצעות מנגנונים מובנים במערכות ההפעלה וכמו כן ניתן לממש בדפי Web באמצעות הגדרת השדה כ Password	2
בקרת גישה	4.37	יש ליישם מנגנון אימות מוצפן	המטרה היא כי פרטי ההזדהות לא יהיו חשופים (Clear text). פרטי זיהוי חשופים ניתנים לגניבה במידה והם יועברו בתווך תקשורת אשר איננו מוצפן, לדוגמה במקרה של מתקפת MIDM.		2

5. הגנה על המידע:

בעידן הדיגיטלי שבו אנו חיים, המידע הינו אחד הנכסים המשמעותיים עבור רב הארגונים - בין אם מדובר במידע עסקי, בנתוני לקוחות או בכל נתון שנאסף ונשמר על-ידי הארגון לצורך פעילותו העסקית. בהתאם לכך, על הארגון לפעול לשמירה על המידע שלו מפני גניבה, שיבוש או מחיקה, ולעתים הוא אף מחויב לכך מתוקף הוראות חוק. בקרות אלו מתייחסות להגנה על המידע עצמו – סיווגו, אחסונו, ניודו וכד'.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
הגנה על המידע	5.1	יש למנוע העברת מידע לא מורשית או לא מכוונת דרך משאבי מערכת משותפים	על הארגון למנוע ולטפל בהעברת מידע לא מורשית באמצעות תיקיות משותפות, דואר אלקטרוני, מדיה נתיקה וכו'	יש להגביל את השימוש בתיקיות משותפות לצורך העברת מידע בייחוד כאשר ישנן הרשאות גם לגורמים שאינם מורשים. ניתן לעשות שימוש במערכת DLP על מנת למנוע העברת מידע אשר שמור בתיקיות משותפות. יש לצמצם למינימום האפשרי את השימוש בכוננים משותפים ולמחוק משם מידע רגיש מייד לאחר השימוש בו	1
הגנה על המידע	5.2	על הארגון לכתוב וליישם מדיניות ונהלים רלוונטים לצורך הגנה על מידע ולעדכנה באופן תקופתי	על המדיניות לכלול לכל הפחות התייחסות לסוגי המידע השונים הקיימים בארגון / מערכת. על המדיניות לכלול הגדרות ברורות לגבי הוצאת מידע אל מחוץ לגבולות הארגון ואופן הוצאת המידע בנוסף יש להתייחס לכלל הערוצים וציודי הקצה הקיימים בארגון: עמדות עבודה, שרתים, ציודים ניידים לרבות מחשבים, טאבלטים, טלפונים סלולריים וכן ציודי מחשוב לביש (שעונים חכמים וכו')	ניתן ליישם בקרה זו באמצעות כתיבת מסמך מדיניות בנושא הגנה על המידע בארגון. על המסמך לכלול הגדרות לסוגי המידע השונים בארגון, אילו סוגי מידע ניתן לשלוח אל מחוץ לכותלי הארגון. בנוסף יש לכתוב נהלים משלימים לגבי אופן שליחת המידע באופן מאובטח.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנה על המידע	5.3	על הארגון לכתוב וליישם מדיניות לסיווג מידע ארגוני ונהלי יישום לעובדי הארגון לצורך תיוג המידע	על מדיניות סיווג לכלול הגדרות ברורת כיצד ואיך לסווג כל סוג מידע שאופיין כמו כן יש להוסיף נוהל המנחה כיצד יש לטפל בכל אחד מסיווגי המידע	1. יש לאפיין את סוגי המידע הקיימים בארגון להבין את חשיבותם - בהתבסס על צרכים עסקיים, חוקים ורגולציות החלים על הארגון 2. יש לייצר מטריצה הכוללת את כלל סוגי הסיווגים - מה כולל כל סיווג (כלומר אילו סוגי מידע, לדוגמה: פרטי, עסקי, רפואי, ציבורי, בטחוני וכו') ואופני הטיפול השונים בסוגי המידע (אחסנה, העברה, השמדה, הגנה פיזית ולוגית וכו')	3
הגנה על המידע	5.4	יש לממש מנגנוני הגנה על מנת למנוע דלף מידע בעת העברת מידע לגורמים פנימיים או חיצונים	על הארגון ליישם מנגנונים להגנה על מידע בעת תנועה בין מערכות הארגון ובשליחתו אל גורמים מחוץ לארגון בהתאם למדיניות הגנת המידע הארגונית	ניתן ליישום בעזרת מס' טכנולוגיות אשר כל אחד עשויה למנוע תרחיש מסוים: 1. מערכת למניעת דלף מידע 2. מערכת להעברבת מידע מאובטחת כגון: מייל מאובטח / מוצפן, כספת אלקטרונית וכו'	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנה על המידע	5.5	יש ליישם מנגנוני הגנה לניטור ומניעה של גישה, שימוש או הוצאת מידע אשר הוגדר רגיש על פי הארגון אל גורמים שאינם מורשים בתוך ומחוץ לארגון	על הארגון ליישם מנגנונים להגנה על מידע בעת שמירתו במערכי האחסון הארגונים אשר עשויים להיות על שרתים פיזיים, וירטואליים ובענן, וכן בעת שמירתו על עמדות העבודה הארגוניות - יש לוודא שמנגנוני ההגנה לא יאפשרו שכפול, הדפסה, שליחה, מחיקה וכו' של מידע אשר הוגדר כמידע רגיש בניגוד למדיניות שהוגדרה עבור מידע זה	ניתן ליישום באמצעות שימוש בטכנולוגיות למניעת דלף מידע על מנת לנטר, להתריע ולמנוע פעולות אלו. ניתן לממש גם באמצעות פתרונות הגנה על מסמכים Document) (security וכן באמצעות הגבלת וניטור גישה לקבצים רגישים (כפי שמורחב בפרקי בקרת גישה וניטור)	3
הגנה על המידע	5.6	יש למנוע הפעלה מרחוק של עזרי מחשוב (מצלמות רשת, מיקרופונים, רמקולים, אוזניות וכל אביזר אשר עשוי להיות מחובר למחשב), ולספק אינדיקציה מפורשת לכך שעזרי המחשוב פעילים פיזית מול המשתמש	יש למנוע / לחסום / לנטר הפעלה מרחוק של מצלמות, מיקרופונים	רצוי לחסום באופן קבוע עזרי מחשוב שלא נעשה בהם שימוש במטרה לצמצם סיכון זה.	3
6. הגנה על תחנות עבודה ושרתים: תחנות עבודה ושרתים הינם ציוד המחשוב הבסיסי בכל ארגון, ההגנה על ציוד זה הינה בסיסית למניעת מתקפות על הארגון וההגנה על המידע הארגוני. בקרות הגנת תחנות עבודה ושרתים כוללות מס' שכבות הגנה - הקשחת שירותים (White/Black List), מניעת יצירת פרצות אבטחה בידי משתמשים הן בזדון והן בשוגג ועוד.					

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנת תחנות עבודה ושרתים	6.1	יש להגדיר, לתעד וליישם מדיניות הקשחה לתחנות עבודה ושרתים אשר מספקות מענה לדרישות אבטחת המידע של הארגון.	הארגון יגדיר דרישות הקשחה למערכות בארגון בדגש על מה הם דרישות הבסיס, תדירות העדכונים, רמת הסיווג ואז לתעד את הדרישות במסגרת על שתהווה בסיס לכתיבת נהלי ההקשחה. המדיניות תכלול בין היתר את ההתייחסות לעבודה עם תוכנות אשר אינן נתמכות על ידי היצרן (כגון מערכת הפעלה אשר הוכרזה במצב End Of Life)	ניתן להשתמש במסמכי Baseline של היצרנים הרשמיים ושל ארגוני תקינה כגון DISA, SANS וכו'. כמו כן יש להגדיר בנהלי הארגון מי אחראי על יישום ההקשחות בפועל ואיך מתבצעת הבדיקה השוטפת של הבקרות. מסמכי ההקשחה יכללו בין היתר התייחסות לשימוש בשירותים (Services) מורשים/ בטוחים, פורטים מאושרים, הסרת חשבונות לא פעילים וכו'. חשוב לוודא כי ההקשחה תתבצע בהתאם לפונקציונליות הרלוונטית של היישום (כגון הקשחת שרתי IIS מול TOMCAT, הקשחת שרת WEB מול הקשחת שרת DB וכו')	1
הגנת תחנות עבודה ושרתים	6.2	יש להטמיע מנגנונים לניהול מרוכז, יישום ואימות הגדרות התצורה של המערכת		מערכות חלונות ניתן להשתמש בכלים כמו Group Policy של Active Directory, במערכות לינוקס ניתן להשתמש לדוגמה בכלים של Red Hat או לחלופין בכלי ניהול והפצת תצורה אוטומטית כגון Chef	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנת תחנות עבודה ושרתים	6.3	יש להגדיר מדיניות לשליטה, אכיפה וניטור של התקנת תוכנות על מחשבי הארגון	מטרת הבקרה הינה לוודא כי תוכנות מותקנות על עמדות הקצה ועל השרתים רק באישור ולאחר בחינה של הצורך והסיכון הכרוכים בשימוש בתוכנה.	ניתן לממש בקרה זו באמצעות הגבלת חשבונות משתמש להתקנה/שינוי של תוכנות בעמדות הקצה וכן באמצעות שימוש בכלי Application control	2
הגנת תחנות עבודה ושרתים	6.4	יש להגדיר ולהטמיע אמצעי אבטחה על מנת לאתר ולהתריע על שינויים בלתי מורשים בהגדרות תצורה	שינוי בתצורת מערכת (קונפיגורציה) עלולה להוריד את רמת ההגנה על הנכס. כך לדוגמה שינוי של הגדרת אורך סיסמה או של הרשאה להתקנת תוכנות שלא בהתאם למדיניות הארגון חושפת אותו לסיכון.	ניתן לממש באמעות הגדרת חוקים רלוונטים במערכת ה SIEM, באמצעות השוואת דו"חות תקופתיים (קונפיגורציה נוכחית מול קודמת), באמצעות כלי ניטור ובקרה/ שו"ב ייעודיים אשר מספקים חיווי על שינוי קונפיגורציה וכו'. מומלץ לאמץ כלי CCM - Continuity control monitoring על מנת לקבל את החיווי בזמן אמת.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנת תחנות עבודה ושרתים	6.5	יש להגדיר את תצורת המערכת כך שתספק את הפונקציונלית המינימלית הנדרשת (תוך חסימת פונקציות, פורטים, פרוטוקולים שאינם נדרשים)	הארגון יגדיר נהלי הקשחה לכל סוג מערכת ושרת על בסיס פרקטיקות מקובלות כך שיכללו לכל הפחות: 1.הפחתה של שטח התקיפה של המערכת על ידי חסימת פורטים שלא נחוצים 2.כיבוי שירותים לא נחוצים 3.הסרת חשבונות משתמש אורח 4.העדפת שימוש בפרוטוקולים מאובטחים בתקשורת בין שרתים 5.קבלת עדכונים באופן מסודר 6.חסימת פונקציות רגישות של המערכת 7.שליחת לוגים על אירועי מערכת לשרת ניטור 8.חסימת התקנת תוכנה על ידי משתמשים לא מורשים	לטובת בניית תורת הגנה פרופורציונלית, הבקרות במסמך זה סווגו לרמות שנעות בציר של 1-4, כאשר בקרות מרמה 1 הן הבקרות הבסיסיות ביותר ואילו בקרות מרמה 4 הן בקרות מורכבות וכאלו הדורשות השקעת משאבים רבים הבסיסיות ביותר, אשר נדרשות מכל ארגון ולכל נכס ואילו בקרות מרמה 4 הן כאלו אשר נדרשות עבור יעד הגנה שפוטנציאל הנזק שלו הינו 4. ניתן להתבסס בכתיבת נהלי ההקשחה על פרקטיקות מקובלות כגון NIST פרסומי ה CERT הלאומי, CISI או על שירותי מומחה אשר יכין נהלי הקשחה לפי מערכות.	1
הגנת תחנות עבודה ושרתים	6.6	יש למנוע הרצה של תוכנות לפי הגדרת הארגון (Black List)	הארגון יגדיר רשימת תוכנות האסורות לשימוש (Black List).	הארגון יחסום תוכנות כגון: כלי תקיפה, תוכנות רוגלה, כלי אחסון בענן , כלי שיתוף קבצים ועוד. ניתן להגדיר רשימת תוכנות אסורות לשימוש באמצעות ה Active Directory או באמצעות כלי ניהול תצורה. חלק מכלי ההגנה על תחנות קצה ושרתים (Endpoint Protection) תומכים ביכולות הנ"ל.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנת תחנות עבודה ושרתים	6.7	יש להגדיר ולהשתמש ב-Whitelist של תוכנות מותרות לשימוש, ולחסום כל תוכנה אחרת	הארגון יגדיר את רשימת התוכנות מותרות לשימוש ויחסום התקנה ושימוש בכל שאר התוכנות באמצעות במערכת ניהול התצורה הארגונית או באמצעות כלי צד ג' ויחסום התקנה של תוכנות אלו.	ניתן להגדיר רשימת תוכנות המותרות לשימוש באמצעות ה Active Directory או באמצעות כלי ניהול תצורה.חלק מכלי ההגנה על תחנות קצה ושרתים (Endpoint Protection) תומכים ביכולות הנ"ל.	3
הגנת תחנות עבודה ושרתים	6.8	הארגון ינהל מעקב אחר שרתים ומערכות אשר הוחרגו (והחרגתם אושרה) מיישום תצורה מוקשחת.	לעיתים מסיבות עסקיות ו/או תפעוליות לא ניתן להחיל את רמת ההגנה על כל הנכסים באותה הצורה. במקרים אלו, הארגון נדרש ליישם תהליך אשר ידרוש אישור מיוחד להחרגת שרת או מערכת מסויימת מדרישות אבטחת המידע בעקבות צורך כלשהו, בתוך כך הארגון אחראי לספק בקרה מפצה במקום ההחרגה.	ניתן להגדיר ראש תחום או בעל תפקיד אשר יהווה "סמכות מאשרת" לחריגה מהמדיניות לטובת צרכי החרגה, הוא יבחן את הצורך התפעולי והעסקי להחרגה וימליץ על בקרה מפצה.	3

7. מניעת קוד זדוני:
קוד זדוני נמצא בשימוש גורמים עוינים לארגון ונועד לחדור לתוכו ללא אישור הארגון על-מנת לפגוע בו באמצעות מרחב הסייבר (גניבת מידע, שיבוש מידע, פגיעה במערכות מחשוב וכו'). קוד זדוני הינו מונח רחב, הכולל בתוכו סוגים רבים של פוגענים: וירוסים, תולעים, סוסים טרויאניים, Rootkits, Adware ועוד. למערך ההגנה מפני קוד זדוני חשיבות עליונה בהגנת הסייבר הארגונית. מערך ההגנה כולל מניעת חדירה של קוד זדוני מצד אחד (בנקודות הכניסה והיציאה של תקשורת לארגון, בשרתים ובנקודות קצה), וזיהוי ותהליכי לטיפול בקוד זדוני שחדר לארגון מצד שני.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
מניעת קוד זדוני	7.1	הארגון יפעיל כלים ומערכות בנקודות התקשורת החיצונית שלו, כלים אלו יסרקו ויזהו קוד עוין. הכלים יופעלו על תקשורת עם גורמים חיצוניים, דוא"ל ושרותי גלישה	מטרת בקרה זו הינה לזהות קוד עויין טרם כניסתו לארגון עוד ברמת ה - GW.	ניתן ליישם באמצעות שימוש בשרתי Proxy, במערכות NGFW ובכלים ייעודיים לפרוטוקולי תקשורת שונים כגון דואר אלקטרוני	2
מניעת קוד זדוני	7.2	הארגון יגדיר נהלים לטיפול בתחנות, שרתים או רשתות הנגועים בקוד זדוני	מטרת הבקרה הינה לוודא כי הארגון ערוך להתמודדות במידה ויתרחש אירוע של חדירת קוד עויין.	דוגמה לנהלים יכולה להיות נוהל זיהוי והסרה של נוזקה, נוהל התקנת מערכת הפעלה מחדש, נהלי זיהוי מגמות והסקת מסקנות במקרה של התפשטות והדבקה מסיבית בארגון	2
מניעת קוד זדוני	7.3	יש להטמיע כלים לזיהוי ומניעת קוד זדוני על תחנות קצה ושרתים בארגון, כלים אלו יופעלו במתכונת הגנה אקטיבית וכן יבוצעו סריקות תקופתיות	מאחר וחלק מהפוגענים עשויים לחדור את מנגנוני האבטחה, יש לוודא כי בקרות לטיפול בקוד זדוני ייושמו גם ברמת תחנות העבודה	ניתן להשתמש בכל כלי לזיהוי ומניעת קוד עויין (כגון אנטי וירוס) מיצרן מוכר.	1
מניעת קוד זדוני	7.4	הארגון יטמיע וינהל יכולות אלו כחלק מכלי ההגנה המופעלים על תחנות הקצה, או יטמיע כלים בעלי יכולות אלו בנוסף לכלי האנטי-וירוס הקיימים	מטרת בקרה זו הינה להעלות את רמת יכולת הזיהוי וטיפול בעמדות הקצה "מעבר" ליכולות הבסיסיות הקיימות במערכת האנטי וירוס.	ניתן להשתמש במוצרי HIPS עצמאיים או כיכולת נוספת של תוכנות ההגנה של מוצרי אנטי-וירוס	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
מניעת קוד זדוני	7.5	יש להפעיל בקרות מניעת קוד זדוני מתקדמות במערכות הפעלה של שרתים ותחנות הקצה	הארגון יפעיל מנגנונים במערכת ההפעלה המקשים על קוד עויין את הגישה לזיכרון או לפונקציות מערכת ההפעלה	ניתן לממש באמצעות פתרונות לזיהוי אנומליות ברמת מערכת ההפעלה	3
מניעת קוד זדוני	7.6	יש להטמיע כלי זיהוי נוזקות ברמת הרשת	הארגון יפעיל כלים אשר יוטמעו ברשת הארגון ומטרתם לזהות ולהתריע על נוזקות המתפשטות ברשת	דוגמה לכלים אלו יכולה להיות: Honeypots, טכנולוגיות Anti-Bot, רכיבי IDS ועוד	3
מניעת קוד זדוני	7.7	הארגון ינהל באמצעות מערכות מרכזיות את כלי מניעת הקוד הזדוני בארגון. כלי הניהול המרכזיים יאפשרו דיווח מרכזי שיאפשר זיהוי אירועים חשודים ואירועי מערכת (בעיות עדכון, הגנה לא-פעילה, הסרת רכיב וכו)	מטרת הבקרה הינה לנהל בצורה יעילה את מערך ההגנה של מניעת קוד זדוני. עבודה בתצורה של התקנה מקומית מקשה על היכולת להפיץ עדכונים, לוודא כיסוי מלא ולשלוט בתמונת ההגנה הכוללת	מרבית המערכות למניעת קוד זדוני מאפשרות שימוש בכלי ניהול בעלי ממשק ניהול מרכזי.	2
מניעת קוד זדוני	7.8	הארגון יפעיל אמצעים זיהוי ומניעה המתבססים על זיהוי התנהגות החורגת מהתנהגות מקובלת וסבירה בנוסף לשימוש בכלים מבוססי חתימות אלקטרוניות	מטרת בקרה זו הינה לאתר פעילויות אשר חורגות מהנורמה. הצפנה של קבצים רבים, מסמכים אשר מנסים לגשת לקבצי רג'יסטרי וכו' הינה אירועים לדוגמה אשר אמורים "להדליק" נורה בארגון.	ניתן להשתמש בכלים המנתחים היוריסטיקות (Heuristics), התנהגות משתמש או מערכת (behavioral)	3
מניעת קוד זדוני	7.9	יש להפעיל עדכון אוטומטי של כלל מערכות זיהוי ומניעת הקוד הזדוני בארגון	הארגון יפעיל עדכון אוטומטי משרת מרכזי המנוהל על ידי הארגון או על ידי ספק שירות מוכר. עדכונים אלה ישמרו על כלי ההגנה מעודכנים באופן תמידי	ניתן להשתמש בשרתי עדכון המוטמעים בתוך הארגון כחלק משרתי הניהול של מערכות אלו או לחלופין להשתמש בשרתי היצרן במידה ואין שרת עדכונים מרכזי ברשת הארגון (תקף גם לגבי שרותי ענן)	1

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
8. הצפנה: שימוש מושכל בהצפנה מסייע רבות להגנה על המידע ולמניעת חשיפתו גם במקרה שזה דלף, ובכך מפחית רבות את המשמעות העסקית של דליפת מידע. לכן חשוב להגדיר שימושים המצריכים הצפנה ואת סוג ההצפנה הנדרשת, בהתאם לחוקים, להנחיות, לנהלים, לרגולציה ולמחויבויות עסקיות ולכדאיות עסקית במסגרת ניהול הסיכונים. נדרש להגדיר הצפנה על מדיות שונות שהמידע עלול לדלוף מהן (זיכרונות, תווכי תקשורות וכד') וכן להגדיר מנגנוני ניהול ובקרה להצפנה (כגון ניהול מפתחות הצפנה ותעודות דיגיטליות בשלבים שונים). משנה חשיבות יש להצפנה על מדיה של התקנים ניידים (מחשבים ניידים, מכשירים סלולריים, טאבלטים ועוד).					
הצפנה	8.1	יש להגדיר שימושים אשר מצריכים הצפנה, ואת סוג ההצפנה הנדרשת בהתאם לחוקים, הנחיות, נהלים, רגולציה ומחויבויות עסקיות	הארגון יגדיר מהו המידע והמערכות שיש להצפינו ויתעד את תצורת הצפנת המידע, הדרישות יגזרו מדרישות החלות על הארגון או מדרישות השמירה על מידע.	דוגמה לדרישות יכולה להגיע מחוקי הגנה על פרטיות, PCI-DSS, דרישות בטחוניות ועוד.	1
הצפנה	8.2	יש לנהל ולהגן על מפתחות הצפנה בעת ייצור, הפצה, אחסון, גישה והשמדה	הארגון יגדיר נהלים וכן תהליכים להנפקה של מפתחות הצפנה, שמירה על מפתחות הצפנה פרטיים ושרתי הנפקת מפתחות ותעודות, נהלי הקשחה וכן נהלי החלפת מפתחות.	הקשחת ושמירה על שרתי Root Ca, שמירה באמצעות HSM, הפצת מפתחות הצפנה לעובדים ולמערכות, תפעול מערך PKI.	2
הצפנה	8.3	יש לוודא את זמינות המידע גם במקרה של אובדן מפתחות הצפנה	הארגון יטמיע מערך שחזור נתונים מוצפנים באמצעות יישום תהליכים מנוהלים וכלים מתאימים.	לדוגמה: מערך שחזור הצפנת דיסקים של מחשבים ניידים באמצעות כלי יצרן מערכת הצפנת הדיסק, ותהליכי שחזור מנוהלים.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הצפנה	8.4	יש לממש מנגנוני הצפנה למידע רגיש המועבר בין מערכות לבין ממשקי משתמש קצה על גבי תווך תקשורת ציבורי	הארגון יממש מערכי הצפנת נתונים למידע רגיש המוצג למשתמש באמצעות דפדפן, אפליקציית מובייל או מערכות אחרות המנגישות מידע באמצעות רשתות ציבוריות כגון רשת האינטרנט.	שימוש בתעודות SSL מאושרות ועדכניות בדפדפן	2
הצפנה	8.5	יש לממש מנגנוני הצפנה למידע רגיש המועבר בין מערכות בתוך הארגון	הארגון יממש תעבורה מוצפנת בממשקים בין שרתים ושירותים המעבירים מידע רגיש וכן יעדיף שימוש בפרוטוקולים המצפינים תעבורה.	ניתן ליישם באמצעות שימוש באמצעות פרוטוקולים כגון SSL, SSH, HTTPS ועוד.	4
הצפנה	8.6	יש לממש מנגנוני הצפנה למידע רגיש המועבר בין הארגון לבין ממשקים חיצוניים, ספקים, מערכות חיצוניות	הארגון יממש תקשורת מוצפנת אל מול ספקים ומערכות מחוץ לארגון.	ניתן ליישם באמצעות שימוש באמצעות פרוטוקולים כגון SSL, SSH, HTTPS, SFTP ועוד.	2
הצפנה	8.7	יש לממש מנגנוני הצפנה על מדיה של התקנים ניידים (מחשבים ניידים, מכשירים סלולריים, טבלטים ועוד)	הארגון יממש הצפנה של דיסקים קשיחים של התקנים ניידים ושל התקני מדיה ניידים.	במכשירים סלולריים וטבלטים ניתן להשתמש במערך הצפנת הדיסק של היצרנים. במערכות הפעלה אחרות ניתן להשתמש בכלים סל הספקים אשר מאפשרים הצפנת דיסק.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הצפנה	8.8	יש להשתמש במנגנוני הצפנה המתבססים על אלגוריתמי הצפנה מוכרים ובגדלי מפתח המתאימים למתאר האיום	הארגון לא ישתמש במנגנוני הצפנה בעלי חולשות ופגיעויות ידועות ויתאים את חוזק ההצפנה, לרבות גדלי מפתחות ההצפנה, למתאר האיום.	לדוגמא: לא להשתמש בשיטות הצפנה מיושנות כגון SHA1, SSLv1, SSLv2, או מפתחות הצפנה קטנים מ128Bit ועוד.	2
הצפנה	8.9	יש לנהל מערך הנפקה וביטול תעודות דיגיטליות ולהשתמש בתעודות דיגיטליות ממקור מהימן בלבד.	הארגון ינהל מערך הנפקת תעודות דיגיטליות ומערך ביטול תעודות (CRL), כמו כן ישתמש בתעודות חיצוניות אשר הונפקו על ידי מקורות מהימנים בלבד (Trusted CA)	ניתן לממש באמצעות מערך שרתי CRL מסודר ומעודכן, שימוש בתעודות חיצוניות של שרותים מאושרים (Trusted CA).	3
הצפנה	8.10	יש להגדיר תהליך לחידוש תעודות דיגיטליות בטרם מועד תפוגתן	הארגון יוודא כי התעודות הדיגיטליות אשר בשימוש קבוע יחודשו לפני מועד תפוגתן ובמידה והתעודות מוחלפות, התעודות הישנות מופצות לשרתי ביטול התעודות (CRL)		2
הצפנה	8.11	יש לבצע החלפה יזומה של מפתחות הצפנה רגישים מדי תקופה	הארגון יגדיר אורך חיי מפתחות הצפנה רגישים וידאג להחליפם בזמן, כמו כן יש ליישם תהליך להחלפה של מפתחות ההצפנה באפליקציות רגישות.		3

9. אבטחת רשת:

תשתית התקשורת בארגון מהווה גורם מרכזי, המחבר בין כלל משאבי המחשוב שברשותו - הן בינם לבין עצמם והן בינם לרשת האינטרנט ולארגונים אחרים. בארגונים רבים תשתית התקשורת היא קריטית לפעילותם היומיומית, והשבתתה או פגיעה בה היא בעלת משמעות מהותית על הארגון. כיוון שכך, רשת הארגון מהווה נקודת פתיחה לסוגים רבים של מתקפות על הארגון, ועל כן נדרש להגן עליה מפני איומים חיצוניים ופנימיים. הגנת הרשתות כוללת הפרדות פונקציונליות, טכנולוגיות, תהליכיות ונוהליות, בקרה וניטור של רשתות, סינון וחסימת מידע חשוד, ועוד. בקרות הרשת נרחבות, מכיוון שתקיפות רבות מבוצעות באמצעות הרשת הארגונית. חשיבות רבה ניתנת לבקרות שנועדו להגן על חיבור הרשתות הארגוניות בינן לבין עצמן, על צומתי התקשורת הארגונית וכמובן בינן לבין האינטרנט.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת רשת	9.1	יש לכתוב וליישם מדיניות הגנה על רשתות תקשורת, לבקר ולעדכן אותה תקופתית	על הארגון לכתוב וליישם מדיניות אבטחת רשת. מדיניות צריכה לכלול התייחסות לנושאים כגון: ערוצי הגישה לרשת האינטרנט הציבורי ותצורת ההגנה עליהם ובנוסף יש להתייחס להיבטי ההגנה בתווך התקשורת הפנים והחוץ ארגוניים	כתיבת מסמך מדיניות או שילוב כפרק במדיניות אבטחת המידע הארגונית	2
אבטחת רשת	9.2	יש להפריד בין פונקציונליות משתמש לשירותי הניהול של הרשת	ממשקי ניהול יופרדו ממשקי משתמש אחרים, במטרה לצמצם את החשיפה לגישה בלתי מורשית לממשקי הניהול	ניתן לממש באמצעות דף התחברות (login) נפרד עבור משתמשים ועבור מנהלי המערכת. רשת תקשורת נפרדת המשמשת להתחברות לממשקי ניהול ציוד. הגבלת כתובת IP מורשית גישה לממשק הניהול וכו'.	3
אבטחת רשת	9.3	הארגון יפעיל אמצעים טכנולוגיים על מנת להגן על שירותיו מפני התקפות מניעת שירות	יש להגן מפני התקפות מניעת שירות (DOS) מסוגים שונים כדוגמת: העמסה על משאבי מחשוב עד לקריסתם, העמסת רוחב פס התקשורת, העמסת אתר אינטרנט עד לקריסתו ועוד	ניתן ליישם את הבקרה באמצעות כלים כגון: מערכות חומת אש (באמצעות מודול IPS) מערכות לזיהוי חדירות (IPS), חומות אש אפליקטיביות (WAF), וכן הגבלות על כמויות נפח תעבור לכיוון מערכות מסויימות או הגבלת כמות שאילתות מבוצעות למערכות.	1
אבטחת רשת	9.4	יש לנתק חיבור רשת המקושר ל-session בעת סיום או לאחר פרק זמן מוגדר של חוסר פעילות	הארגון יכיל מגבלות על אורך חיי החיבור וכן ינטר וינתק חיבורי תקשורת ללא תשדורת	הבקרה ניתנת ליישום באמצעות חומת האש והגדרה אשר קובעת כי חיבורי רשת מקבלים Timeout לאחר תקופה קצובה של חוסר פעילות.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת רשת	9.5	יש להגדיר הנחיות לשימוש בטכנולוגית טלפוניית VOIP (IP) וכן לנטר ולבקר את השימוש בה	הארגון יגדיר מתי וכיצד מותר/אסור לבצע שימוש בשירותי VOIP (המוטמעים במערכות הארגון או כשירותי חיצוני) וכן יפעיל אמצעי אבטחת מידע על מנת לאכוף הגדרות אלו	ניתן ליישם באמצעות הפרדת רשת ה VOIP לרשת נפרדת מהרשת הרגילה, להגביל חיבוריות ציוד שאינו טלפוניה לרשת באמצעים כגון NAC, הזדהות של הציוד אל מול שרתי ה VOIP וכן שימוש בהצפנה והזדהות באמצעות SSL.	2
אבטחת רשת	9.6	יש לוודא כי שירות תרגום כתובות (DNS) מסופק על ידי שרת מהימן (פנים ארגוני וכן חוץ ארגוני)	הארגון יאפשר קבלת שירות תרגום כתובות (DNS) אך ורק משרת פנימי מאובטח. זאת במטרה למנוע ניתובי תקשורת שגויים (במזיד או בשוגג) אל יעדים עויינים	יוגדרו שרתי DNS פנימיים אשר יספקו מענה לשרתי הארגון, ניתן גם להגדיר שרתי DNS ייעודיים לאיזורים מאובטחים יותר של הרשת. שרתי הארגון יוגדרו כך שהפניה לשרות DNS תבוצע אך ורק לשרתים אלו.	1
אבטחת רשת	9.7	יש לוודא כי התשובות המתקבלות משרת תרגום הכתובות אמינות ולא שונו במהלך התשדורת	הארגון יוודא כי התשובות המוחזרות משרת תרגום הכתובות לא ניתנות לשינוי באמצעות מנגנונים כגון חיתום התשובות הנשלחות על ידי תעודה דיגיטלית	ניתן ליישם באמצעות שימוש בהרחבות DNSSEC של שירות ה DNS	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת רשת	9.8	יש להגן על אמינות התקשורת ברמת session בכך ששני קצוות ה-session יהיו בטוחים בנכונות זהות הצד השני (הגנה מפני MITM, session hijacking וכו')	הארגון יפעיל בקרות אמינות באמצעים טכנולוגיים כדוגמת תעודות דיגיטליות בעת יצירת חיבורי תקשורת בין השירותים והמערכות השונים.	ניתן להשתמש בתעודות SSL אשר מזהות את השירות ובאמצעות שרת CA פנימי מאובטח אשר מנפיק תעודות לשירותים השונים בארגון, השירות נתמך בתשתית ה Active Directory וכן שירותי Kerberos של מייקרוסופט. את בקרת ניהול השיחה (Session) ניתן ליישם באמצעות שימוש בבקרת Session ברמת השרת (כדוגמת IIS או Apache) או ברמת הרשת באמצעות Load Balancer	2
אבטחת רשת	9.9	יש לשלוט בתעבורת הרשת היוצאת/נכנסת לארגון	מטרת הבקרה הינה לוודא כי התעבורה אל תוך ומחוץ לארגון תתאפשר אך ורק בהתאם למדיניות שהוגדרה (גישה בפרוטוקולים מותרים, SERVICE מאושרים, ממקורות/אל יעדים מאושרים וכו')	ניתן לממש באמצעות יישום חומות-אש המבדילות בין רשת הארגון ובין רשתות חיצוניות.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת רשת	9.10	יש לנטר ולשלוט בצמתי תקשורת מרכזיים בתוך רשת הארגון	הארגון יחלק את הרשת שלו לתתי רשתות לפי רמת הסיכון / סיווג המידע במערכות	ניתן להפריד את הרשתות באמצעות חומת אש ארגונית בין הסביבות, הגדרת סביבות כגון איזור חיץ (DMZ) לטובת שירותים המוחצנים לרשת האינטרנט, רשתות ניהול אשר יחוברו מאחורי חיבור מאובטח, רשתות אשר יכילו שירותים רגישים ומערכות רגישות.	3
אבטחת רשת	9.11	יש להגביל את מספר ערוצי התקשורת החיצוניים למערכת	הארגון יצמצם ויאחד ערוצי תקשורת בכדי להבטיח שליטה טובה על החיבורים למערכת.	שימוש בשרת מסופים (Terminal Server) לצורך התחברות למערכת	2
אבטחת רשת	9.12	יש לחסום כברירת מחדל כל תעבורת רשת, ולאפשר ידנית כל תעבורה רצויה ע"י כלל חריגה	הארגון יגדיר את חוקי סינון תעבורת הרשת באופן החוסם בברירת מחדל כל תעבורה שלא הוגדרה במפורש כמותרת.	הגדרת "חוק אפס" בחומות האש החוסם את כל התעבורה שלא אופשרה באופן מפורש. יש לוודא כי הניתובים מוגדרים כך שכל התעבורה תנותב דרך חומות האש.	1
אבטחת רשת	9.13	יש למנוע ממכשירים ליצור תקשורת מקומיות על המערכת במקביל לתקשורת דרך חיבור חיצוני	הארגון יגדיר את מערכות המחשוב שלו כך שתחנות העבודה והשרתים יתקשרו מכרטיס רשת אחד בלבד או יותר המשויכים לרשת הפנימית או לרשת החיצונית בלבד.	ניתן להגדיר את תחנות העבודה עם מדיניות (Policy) הקובעת כי רק כרטיס רשת אחד יהיה פעיל בכל עת, ברמת השרתים, יגדרו חיבורים אך ורק לרכזות של הארגון, מאחורי חומת אש תוך כדי ביטול כרטיסי רשת נוספים (שלא מחוברים לרשת נדרשת בהגדרה כגון רשת אחסון) כדוגמת כרטיסי רשת קוויים ואלחוטיים.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת רשת	9.14	יש לנתב תקשורת מתוך הארגון לרשתות חיצוניות דרך שרתי פרוקסי מאומתים ומנוהלים	הארגון יגדיר כי כל התקשורת לרשתות חיצוניות תבוצע דרך שרתים מתווכים בלבד. זאת במטרה ליצירת תווך אשר ימנע תקשורת ישירה החופשת את משאבי הארגון אל רשת האינטרנט, וכן במטרה לאפשר יישום בקרות והגנות מרוכזות על ערוצי התקשורת אל מול רשת האינטרנט	ניתן ליישם באמצעות שרת מתווך (Proxy) אשר מחובר לעולם והגלישה מבוצעת דרכו בלבד, השרת המתווך יגודר כך שניתן להגביל את החיבורים לאתרים לא מורשים ולקטגוריות לא מורשות. כמו כן שרתים יוגדרו כך שתאופשר גישה לאינטרנט לטובת עדכונים בלבד דרך השרת המתווך (במידה ולא ניתן להשתמש בשרת עדכונים ייעודי של יצרן המערכת)	3
אבטחת רשת	9.15	יש ליישם מנגנונים למניעת חיבור פיזי בלתי מורשה לרשת הארגון	חיבור ציוד בלתי מורשה לרשת הארגון חושף את משאבי הארגון לפגיעה בסודיות, שלמות וזמינות משאבי מחשוב ומידע	ניתן ליישם באמצעות מערכות NAC	2
אבטחת רשת	9.16	יש ליישם מנגנונים המסננים תקשורת שאינה תואמת את מבנה הפרוטוקול/ המידע המצופה	יש ליישם מנגנונים אלו על מנת להתגונן מפני שימוש זדוני בפרוטוקולים שאינם מאובטחים / מורשיים. כמו כן יש לבצע ווידוא שמבנה חבילות התקשורת מגיעות בתצורה הנכונה וכי לא עברו שינוי לפני הגעתן ליעדם	לדוגמה: סינון תעבורה שאינה עומדת בסטנדרטים בפיירוולים, יישום XML Firewalls	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת רשת	9.17	יש לוודא כי במקרה של כשל תפעולי של אחד ממכשירי הגנת הגבולות (FW וכו') רמת אבטחת המערכת לא תפגע	יש להגדיר את ציוד אבטחת המידע כך שיחסום תקשורת בעת כשל.	מרבית ציודי אבטחת המידע ניתנים להגדרה כך שישנה יתירות לכיוון ציוד משני (חומת אש משנית לטובת יתירות, נתיב תקשורת מאובטח אחר ועוד) וכן במידה ואין יתירות הכשל יעביר את המערכת למצב Fail-Close.	2
אבטחת רשת	9.18	יש להשתמש במנגנוני הגנת גבולות כדי להפריד בין רכיבי מערכת אשר תומכים במשימות או שירותים עסקיים שהוגדרו ע"י הארגון ככאלה שדורשים הפרדה	הארגון יגדיר כי הפרדת הרשתות לאזורים מאובטחים תבוצע באמצעות ציוד אבטחת מידע ייעודי	ניתן להשתמש בכלים כגון חומת אש (Firewall), כלים כגון VPN אשר יאפשרו התחברות מאובטחת לרשתות ניהול, Access Control ברמת הנתבים, שרתים מתווכים (Proxy).	2
אבטחת רשת	9.19	יש להשתמש בכתובות רשת נפרדות (תת-רשת שונה) כדי להתחבר למערכות באזורי אבטחה שונים	הארגון יגדיר כי לכל תת רשת יהיה טווח כתובות נפרד אשר יפורסם לחומת האש ולנתבים.	ניתן ליישם באמצעות ניהול כתובות מרוכז על ממשק הניהול המרכזי של חומת האש או באמצעות רישום ידני (מנוהל ומבוקר) של כתובות הרשת השונות.	1
אבטחת רשת	9.20	יש ליישם מנגנונים לשמירה על שלמות וסודיות תעבורת רשת על גבי תווך ציבורי		לדוגמה: הצפנת תעבורה היוצאת מחוץ לארגון, הצפנת קווי תקשורת על גבי תווך ציבורי	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת רשת	9.21	יש להגדיר, לתעד וליישם מדיניות הקשחה לציודי תקשורת אשר מספקות מענה לדרישות אבטחת המידע של הארגון.	הארגון יגדיר דרישות הקשחה למערכות התקשורת בארגון בדגש על מה הם דרישות הבסיס, תדירות העדכונים, רמת הסיווג ואז לתעד את הדרישות במסגרת על שתהווה בסיס לכתיבת נהלי ההקשחה.	מסמכי Baseline וכן התייחסות לדרישות הקשחה במסמכי המדיניות. כמו כן יש להגדיר מי אחראי על יישום ההקשחות בפועל ואיך מתבצעת הבדיקה השוטפת של הבקרות. מסמכי ההקשחה יכללו בין היתר התייחסות לשימוש בשירותים (Services) מורשים/ בטוחים, פורטים מאושרים, הסרת חשבונות לא פעילים וכו'. חשוב לוודא כי ההקשחה תתבצע בהתאם להמלצות הייצרן המלצות הקשחה ניתן למצוא בתקנים מקובלים כגון DISA, SANS ובאתר הרשמי של היצרן.	3
אבטחת רשת	9.22	יש להטמיע מנגנונים לניהול מרוכז, יישום ואימות הגדרות התצורה של ציודי התקשורת		ניתן ליישום לפי סוג ציוד התקשורת ועל פי מנגנון הניהול המרכזי של כל יצרן. כמו כן ניתן ליישם את הקשחת רכיבי התקשורת השונים באופן ידני דרך ממשק הניהול של כל רכיב בנפרד	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
אבטחת רשת	9.23	מנגנון (מקומי או מרכזית) לניהול מדיניות FW	הארגון יגדיר את תצורת ניהול מדיניות מערכת "חומת האש" (FW) אשר תכלול התייחסות: תהליך הוספת / הסרת חוקי ניתוב במערכת כולל תהליך אישור להוספת / הסרת חוקים. כמו כן יש להגדיר את אופן התיעוד והפירוט לגבי כל חוק אשר נפתח ב FW לצורך ניהולו התקין	ניתן ליישום ישיר בממשק הניהול של המערכת. ניתן ליישם תהליך אישורים לפתיחת / הסרת חוקים וכן גם את יצירת והסרת החוקים בפועל במערכת באמצעות מערכות לניהול שינויים אוטומטיים	2
אבטחת רשת	9.24	טיוב חוקי FW	הארגון יבצע תהליך בדיקה וטיוב של חוקי מערכת ה FW ("חומת האש") לצורך שמירה על כשירות המערכת וכן לצורך ווידוא כי לא קיימים חוקים אשר עלולים לחשוף את הארגון שלא לצורך	ניתן ליישום באופן ממוכן באמצעות מערכות ממוכנות לניהול השינויים או לחילופין לבצע תהליך ידני של בחינת החוקים וההגדרות	3
אבטחת רשת	9.25	סריקת רשת תקופתית	מטרת הבקרה הינה לבחון אלו שירותי רשת פעילים ובאלו כניסות (PORT), איתור פגיעויות ברמת הרשת והאפליקציות ולמידה אודות מבנה הרשת בראיה חיצונית לארגון	ניתן לבצע באמצעות כלי סריקה חינמיים כגון NMAP, Superscan וכו'	2

10. הפרדת סביבות:

ברשת הארגון יכולות להתקיים כמה סביבות עבודה, כדוגמת: סביבת ייצור, סביבת פיתוח, סביבת בדיקות, סביבת מנהל ועוד. סביבות אלו לרוב מקושרות זו לזו, ובה בעת נבדלות זו מזו בסוג המידע הקיים בהן, ברמת הזמינות הנדרשת מהן, באופן ניהולן וברמת ההגנות ובקרות אבטחת המידע המוטמעות בהן. כיוון שכך, תוקפים מנצלים חולשות הקיימות בסביבה פחות מוגנת לצורך השגת דריסת רגל ברשת הארגון, ולנצלה לתקיפת הסביבות המאובטחות יותר. במטרה להגן על סביבות העבודה, על הארגון לייצר הפרדה וחציצה בין סביבות שונות, וזאת על-ידי הפרדה פיזית (ברמת התקשורת, האחסון, הווירטואליזציה, ניהול המפתחות וכו), בקרת מעבר מידע בין הסביבות, הפרדת משתמשים והרשאותיהם, תהליכי העברת מידע ותוכנה בין הסביבות, שילוב כלי אבטחה, מסננים וכלי ניטור.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הפרדת סביבות	10.1	יש לכתוב וליישם מדיניות להפרדת סביבות, לבקר ולעדכן אותה תקופתית	הארגון יכתוב ויישם מדיניות להפרדת סביבות כדוגמת סביבות ייצור, פיתוח, בדיקות, תמיכה, אינטרנט, רשת אורחים וכו'. מטרת ההפרדה הינה מניעת יכולת מעבר בין הסביבות על ידי ניצול הרשאות גישה או ניצול תשתיות משותפות.	המדינית צריכה להכיל הגדרה של סוגי הסביבות שיש להפריד, רמת ההפרדה הנדרשת (לדוגמה: הפרדה לוגית או פיזית) והפניה לנהלים מתאימים	2
הפרדת סביבות	10.2	יש להגדיר סביבות נפרדות לפיתוח, בדיקות וייצור	הארגון יגדיר ויתחם את הסביבות שיש צורך להפריד במטרה למנוע זליגת אירועי סייבר בין הסביבות במקרה של פגיעה באחת מהן	הגדרה של הסביבות השונות, מיפוי המערכות והתיחום הטכנולוגי (רשתות, שרתים ובסיסי נתונים) של כל סביבה	2
הפרדת סביבות	10.3	יש להגביל את השימוש בנתוני ייצור רגישים (נתונים של לקוחות או נתונים שהוגדרו על ידי הארגון כרגישים) בסביבות שאינן סביבות ייצור אם אינן מוגנות באותה מידה כסביבת הייצור	מאחר ולסביבות הנמוכות יותר ניגשים מפתחים ואנשי אבטחת איכות באופן פחות מבוקר, קיים חשש כי נתונים רגישים ידלפו החוצה. בנוסף על כך, רמת האבטחה על פי רוב בסביבות אלו נמוכה מרמת האבטחה בסביבת הייצור. לטובת צמצום החשיפה שבגישת המפתחים וגורמים נוספים אל סביבת הבדיקות והאינטגרציה יש למנוע העברת נתונים רגישים לסביבות אלו.	ניתן להשתמש בתהליכי אנונימיזציה (השמטה או ערבול של נתונים מזהים) או בנתוני טסט סינטתיים לצורך סביבות פיתוח ובדיקות	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הפרדת סביבות	10.4	יש להפריד בין הרשאות המשתמשים בסביבות השונות ולהגדיר את ההרשאות לכל סביבה בנפרד	ניתן לנהל את המשתמשים וההרשאות במערכת ניהול משתמשים אחת, אולם יש להגדיר רישום נפרד של ההרשאות לכל סביבה בנפרד, על מנת שסביבות המכילות מידע רגיש לא תהיינה חשופות לגישה בלתי מורשית במקרה של פריצת חשבון המשתמש או ניצול הרשאות לרעה.	הגדרת חשבון משתמש נפרד עבור אותו העובד, בכל סביבה בה הוא נדרש לפעול. הרשאות הגישה יוגדרו גם הן בנפרד עבור כל חשבון, בהתאם לצורך העסקי בפעילות העובד.	2
הפרדת סביבות	10.5	יש להגדיר תהליך אישור להעברת נתונים מסביבות הייצור לסביבות אחרות ולהגדיר תהליך לביצוע העברת הנתונים באופן מאובטח	העברת נתונים רגישים מסביבת הייצור לסביבות אחרות נדרשת לעיתים כחלק מתהליכי פיתוח ובדיקות. במטרה למנוע ניצול לרעה של תהליכים אלו, נדרש ליישם תהליך העברת נתונים מבוקר המחייב קבלת אישורים מתאימים טרם ביצועו.	ניתן ליישם באמצעות תהליך ממוכן הכולל אישור של גורם אבטחת מידע	2
הפרדת סביבות	10.6	יש להגדיר תהליך מבוקר של העברת רכיבי תוכנה מסביבות הפיתוח והבדיקות לסביבת הייצור	יש ליישם תהליך העברת רכיבי תוכנה לסביבת הייצור שמטרתו לוודא השלמת תהליכי בדיקות וקבלת האישורים המתאימים טרם ביצוע המעבר	ניתן ליישם במסגרת "ועדת עלייה לייצור" המרכזת שינויים בסביבת הייצור ואישורם, טרם ביצוע המעבר.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הפרדת סביבות	10.7	יש להפריד בין סביבות המיישמות רמת אבטחה שונה באופן הלוקח בחשבון את רמת האיום הנשקפת לסביבה ה"מוגנת יותר" מהסביבה ה"מוגנת פחות"	סביבות ייצור נוטות להיות מנוהלות בקפידה ובעלות בקרות ואמצעי הגנה נרחבים, בעוד סביבות פיתוח ובדיקות נוטות להיות בעלות ניהול רופף יותר ומכילות פחות בקרות ואמצעי הגנה. בכדי למנוע פגיעה בסביבת הייצור עקב ניצול חולשות בסביבות הנמוכות, יש להגדיר את רמות האבטחה של המערכות והסביבות השונות ולהפריד בין סביבות המיישמות רמת אבטחה שונה.		2
הפרדת סביבות	10.8	יש ליישם את ההפרדה בין הסביבות ברשת התקשורת, במערכות האחסון, וירטואליזציה, תהליכי ההזדהות וניהול מפתחות ההצפנה	הפרדה מלאה בין סביבות דורשת יישום רשתות פיסיות נפרדות ותשתיות נפרדות. שימוש בתשתיות משותפות דורש יישום מנגנוני הפרדה מספקים, המותאמים לרמת האיום ולאופי הסיכונים הנשקף לסביבה הטכנולוגית.		3
הפרדת סביבות	10.9	ממשקי תקשורת והעברת נתונים בין סביבות יישמו מנגנוני סינון דו-כיווניים המונעים מעבר קוד עוין, תקיפת חולשות, ניצול ממשקים אפליקטיביים והוצאה לא מבוקרת של מידע	הפרדה מלאה בין סביבות דורשת יישום רשתות פיסיות נפרדות ותשתיות נפרדות. שימוש בתשתיות משותפות דורש יישום מנגנוני הפרדה מספקים, המותאמים לרמת האיום ולאופי הסיכונים הנשקף לסביבה הטכנולוגית.	ניתן ליישם באמצעות טכנולוגיות סינון מתקדמות המיישמות מסנני תוכן וחוקי סינון מתקדמים	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
11. מחשוב ענן ציבורי: ארגונים רבים נסמכים בקצב הולך וגדל על שירותי ענן לצורך עיבוד מידע ואחסונו. לצד היתרונות של המהלך, הארגון נדרש לנהל את הסיכון שנוצר מכך שמידע בעל ערך עבור הארגון מועבר לידי צד ג' (ספק שירותי הענן). לכן מחובתו של הארגון לוודא, כי שירותי הענן לא יפגעו ברמת ההגנה בסייבר שלו, וזאת על-ידי הגדרת דרישות מתאימות מספק שירותי הענן. על הארגון להבין את חלוקת האחריות לאבטחת השירותים בין ספק השירות ובין הארגון וליישם את בקרות ההגנה בהתאם – הן ברמת הארגון והן ברמת הספק. הארגון נדרש לוודא, כי ספק שירותי הענן מתחייב לעמוד בתקנים וברגולציה הנדרשים מהארגון, לקיים את בקרות ההגנה בסייבר המתאימות לערכיות המידע ולהגדיר תהליכי בקרה ופיקוח מתאימים. תכנית ההמשכיות העסקית של הארגון נדרשת להביא בחשבון מצבים של שלילת יכולת הגישה לשירותי הענן. יש לוודא, כי ספק שירותי הענן מיישם מנגנונים לניטור אבטחת מידע ומדווח לארגון על אירועים חריגים.					

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
מחשוב ענן ציבורי	11.1	יש להבין את חלוקת האחריות לאבטחת השירות, בין ספק השירות ובין הארגון, וליישם את בקרות ההגנה בהתאם	בעת השימוש בשירותי ענן ציבוריים, ישנה חלוקת אחריות להגנת הסייבר, בין הנושאים שבאחריות הספק ובין נושאים הנשארים באחריות הלקוח. חלוקת אחריות זו תלויה באופי השירות ובמודל המימוש. על הארגון להבין מה הם הנושאים הנמצאים באחריותו, וליישם את ההשלכות של אחריות זו.	במקרה של שירותים מסוג תשתיות PaaS או IaaS, אחריות הלקוח הינה גם לניהול המשתמשים, לניטור השימוש על ידי המשתמשים, לניהול הנתונים ואבטחתם, לאבטחת היישומים והממשקים, ולעתים גם לאבטחת מערכות ההפעלה והתשתיות - כל זאת בהתאם לאופי השירות כמוגדר בהסכם עם הספק. בקרות אלו ניתנות ליישום באמצעות כלי שליטה ובקרה המסופקים בכחלק מהשירות, באמצעות כלים הקיימים בארגון או באמצעות ספקים חיצוניים המספקים שירותי אבטחת ענן. הסכם עם ספק שירותי הענן יכולים לכלול לדוגמה את ההיבטים הבאים: שמירת המידע והסודיות, התייחסות למקרים בהם הספק מחליט להפסיק את השירות או לשנות אותו,אופן הטיפול במקרים כמו דיסק תקול בו ספק שירותי הענן נדרש להחליף חומרה בה קיים מידע של הארגון.	1

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
מחשוב ענן ציבורי	11.2	יש לכתוב וליישם מדיניות שימוש והגנה על שירותי ענן ציבוריים, לבקר ולעדכן אותה תקופתית	על הנהלת הארגון להגדיר מדיניות וקווים מנחים לגבי התנאים והכללים לשימוש בשירותי ענן ציבורי ולגבי האופן שבו הארגון מיישם את הגנת הסייבר במקרה של שימוש בשירותי ענן ציבורי	מדיניות בנושא שימוש בשירותי ענן עוסקת, בדרך כלל, בנושאים הבאים: מהם השירותים המותרים לשימוש בארגון, מהן הדרישות הספציפיות של הארגון, נושאים שיש לכלול בהתקשרות עם ספקים, ניהול סיכוני פרטיות, פיקוח ובקרה. בעת כתיבת מדיניות זו, יש לקחת בחשבון את דרישות החוק בנושא מיקור חוץ אשר פורסמו על ידי הרשות למשפט וטכנולוגיות מידע (רמו"ט)	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
מחשוב ענן ציבורי	11.3	יש לוודא כי ספק שירותי הענן מתחייב לעמידה בתקנים וברגולציה הנדרשת, בהתאם לחובות הארגון ולתקנים שסוכמו עם הספק	ארגונים שונים כפופים להנחיות רגולטוריות המתייחסות לשימוש בשירותי ענן כגון הגנת פרטיות, רגולציה מגזרית או חבות חוזית לצדדים שלישיים. חובות אלה מכתיבות לעיתים כללים נוקשים לשימוש בשירותי ענן	לדוגמה: יישום הנחיות בנק ישראל, הפיקוח על שוק ההון, הנחיות רמו"ט, הנחיות התקשוב הממשלתי ואחרים. בעת ביצוע השוואה זו יש לבחון את כל היישומים אשר פעילים בענן בארגון. מיפוי זה יכול להתבצע בין היתר באמצעות בחינת היסטוריית הגלישה של המשתמשים השונים בארגון והשוואה אל מול רשימת ספקי התוכנה ובאמצעות בחינת החוקים הקיימים ברכיבי התקשורת הרלוונטיים (כגון FW, filtering וכו'). במקרים רבים תוכנות לניהול שכר, שיתוף מסמכים, בניית טפסים וסקרים ועוד נמצאות בענן והארגון איננו "מודע" לכך (Shadow IT)	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
מחשוב ענן ציבורי	11.4	יש להגדיר וליישם תהליכי פיקוח ובקרה תקופתיים על עמידת הספק בהתחייבויותיו	יישום הגנת סייבר בשירותי ענן מתבסס על מילוי קפדני של ספק השירות אחר התחייבויותיו. יש לנקוט בצעדי פיקוח במטרה לוודא כי הספק ממלא את אלו, בין אם באופן של פיקוח ישיר ובין אם באמצעות צד ג' בלתי תלוי הבודק את עמידת הספק בהתחייבויותיו באופן תקופתי	לדוגמה: משלוח שאלונים לספק, ביצוע ביקורות אצל הספק, שימוש בשירותי ביקורת חיצונית ואובייקטיבית המעידה על עמידת הספק בהתחייבויותיו. ספק השירות/תוכנה ישלח אל הלקוח תיעוד מפורט של אופן עמידתו ומימושו את הדרישות שהוגדרו בהסכם ההתקשרות. חריגות של הספק מההסכם יאושרו על ידי מנהל הגנת הסייבר בארגון. כך לדוגמא, במקרה של דרישה עקרונית במדיניות הארגון לעמידה ב SLA מסוים או למדיניות סיסמאות אותה ספק התוכנה איננו יכול לבצע, נדרש הליך פורמלי שבו הספק מסביר מדוע הוא איננו יכול לעמוד בדרישה זו והאם יש צפי לסגירת פער זה. נתונים אלו יועברו אל מנהל ההגנה בסייבר בארגון לאישור ולהגדרת בקרות מפצות להפחתת הסיכון.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
מחשוב ענן ציבורי	11.5	יש לבצע בדיקות אבטחת מידע בלתי-תלויות של ממשקים אל שירותי הענן, החשופים לרשת האינטרנט	בדיקה עצמאית של שירותי הענן על ידי הארגון, צד ג' שנשכר על ידו או גורם אובייקטיבי אחר, מאפשרת לזהות חשיפות אבטחת מידע ולטפל בהן, מבלי להסתמך על הספק באופן בלעדי	בין הבדיקות הרלוונטיות ניתן למנות: מבחני חדירה לממשקי משתמש, ממשקי ניהול וממשקים אפליקטיביים, ביצוע ביקורת בהתאם לסטנדרטים מקובלים, או ביצוע ביקורת המכסה נושאים ספציפיים שהוגדרו בהסכם ההתקשרות עם הספק	3
מחשוב ענן ציבורי	11.6	יש לוודא כי לא מועברים לשירותי הענן נתונים אשר על פי הרגולציה והמחויבויות של הארגון אסור להעבירם	ישנם נתונים אשר על הארגון אסור להעבירם לאחסון או עיבוד בשירותי ענן ציבוריים, משיקולים של רגולציה או התחייבות לצדדים שלישיים. בטרם העברת נתונים לענן, יש לוודא כי לא נשמרים או מועברים לשירות הענן נתונים מסוג זה	לדוגמה: בדיקה של שדות הנתונים אשר בכוונת הארגון להעביר לשירותי הענן, בטרם קבלת ההחלטה בנושא. ניתן גם לבצע על ידי מחיקה או החלפה של נתונים מסוג זה ברשומות המועברות לשירותי ענן. התייעצות עם גורם משפטי מוסמךבעת ביצוע בחינת והערכת רגישות הנתונים והאפשרות להעברתם לאיחסון בשירות ענן	1

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
מחשוב ענן ציבורי	11.7	על תכנית ההמשכיות העסקית של הארגון להביא בחשבון מצבים של שלילת יכולת הגישה לשירותי הענן	שירותי הענן הינם חיצוניים לארגון, ובדרך כלל התקשורת אליהם היא דרך תשתיות ציבוריות כגון רשת האינטרנט. יש להביא בחשבון, במסגרת תכנית ההמשכיות העסקית, מצבים בהם אין גישה לשירותי הענן, אם מסיבה של תקלה של הספק, או של התשתיות המאפשרות גישה אל הספק	לדוגמה, שיטות חלופיות למתן שירות ללקוחות במקרים של נתק משירות הענן, קבצי נתונים מעודכנים בארגון, המכילים את המידע הנמצא בשירותי הענן	2
מחשוב ענן ציבורי	11.8	יש להגדיר וליישם מנגנוני בקרת גישה המתאימים לממשקי הגישה לשירותי הענן, בהתאם לאיומים ולחשיפות הרלוונטיים לכל ממשק	לשירותי הענן ישנם בדרך כלל מספר סוגים של ממשקים: ממשקי משתמש, ממשקי ניהול ותחזוקה וממשקים אפליקטיביים. בדרך כלל, ממשקים אלה חשופים לרשת האינטרנט ולרשתות ציבוריות, ויש להגדיר מנגנוני בקרת גישה חזקים, המתאימים לאיומים הרלוונטיים לאופי הממשק, לרמת החשיפה הטכנולוגית ולמתאר האיומים	לדוגמה: הזדהות חזקה לממשקי ניהול, הגבלת גישה לממשקים רגישים לכתובות אינטרנט מסויימות	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
מחשוב ענן ציבורי	11.9	יש לוודא כי ספק שירותי הענן מיישם תהליכים של פיתוח מאובטח ומשלב בדיקות אבטחת מידע בשלבי פיתוח ותחזוקה	אחד מאיזורי החשיפה העיקריים של שירותי "תוכנה כשירות" (SaaS) בענן הינם ממשקי משתמש וממשקים אפליקטיביים. על מנת לצמצם חשיפות מסוג זה, על ספק שירותי הענן ליישם תהליכי פיתוח מאובטח ולשלב בדיקות אבטחה מתאימות בשלבי פיתוח ותחזוקה. על הארגון לוודא כי הספק מיישם באופן נאות תהליכים אלו	לדוגמה: הצהרה של הספק כי הוא מיישם תהליכי פיתוח מאובטח, הצגה של תוצאות בדיקות אבטחת מידע תקופתיות המבוצעות על מערכות הספק	3
מחשוב ענן ציבורי	11.10	יש לוודא כי ספק שירותי הענן מיישם מנגנוני ניטור אבטחת מידע ומדווח לארגון על אירועים חריגים	ישנם איזורי אחריות בתחום הגנת הסייבר המצויים בתחום אחריותו של ספק שירותי הענן. על הארגון לוודא כי הספק מבצע ניטור של איזורים אלה, ומדווח לארגון (לקוח השירות) על חשדות לאירועי סייבר, על מנת שהארגון יוכל לנקוט את צעדי ההגנה מצידו: הכלה והתאוששות	ניתן ליישם באמצעות עיגון הנושא בהסכם ההתקשרות עם הספק ודיווח תקופתי מצד הספק על מספר האירועים שהתרחשו וניתוחם	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
מחשוב ענן ציבורי	11.11	יש לקיים מנגנון ניטור אבטחת מידע במטרה לזהות אירועים סייבר בשירותי הענן	על מנת לקבל תמונה שלמה של אירועי סייבר ואירועים חשודים, על הארגון לנטר את הפעילות בשירותי הענן, ניטור זה יכול להתבצע באמצעות מערכות ספק שירותי הענן או על ידי חיבור מערכות הניטור של הארגון לרשומות לוג המופקות ממערכות ספק שירותי הענן	ניתן ליישם באמצעות קבלת פיד אירועים ממערכות הספק למערכות הניטור של הארגון או גישה לממשקי ניטור של הספק עצמו	3
מחשוב ענן ציבורי	11.12	יש להגדיר וליישם מנגנון המאפשר המשכיות תפקודית ומחיקה מלאה של הנתונים שנשמרו אצל ספק שירותי הענן במקרה של הפסקת הסכם השירות עם הספק	בעת סיום ההתקשרות עם ספק שירותי הענן, על הארגון לאפשר רציפות תפקודית ושמירה על רשומות השייכות לו, אשר נשמרו או עובדו באמצעות שירותי הענן. בנוסף, יש לוודא מחיקה של נתונים שנשארו אצל הספק והינם בבעלות או באחריות הארגון	ניתן ליישם באמצעות עיגון הנושא בהסכם ההתקשרות עם הספק	2

12. בקרים תעשייתיים:
בקרים תעשייתיים (ICS) אחראים לשליטה בפסי ייצור, במערכות בריאות, במערכות חשמל, במערכות לניהול מבנים (מעליות, דרגנועים וכו'), בתשתיות מים ועוד. עקב פשטות רכיבים אלו נהוג היה בעבר שלא לשייכם לרשימת המערכות שהארגון מגן עליהם מפני איומי סייבר. עם זאת, רכיבים אלו מהווים מטרה מועדפת עבור תוקפים, משום שפגיעה בהם עלולה להוביל לנזק חמור ביותר עבור הארגון ולקוחותיו. בהתאם לכך, הארגון נדרש לייחס חשיבות גבוהה להגנה על רכיבים אלו ולהקפיד במיוחד על הפרדתם ועל בידודם מרשתות תקשורת ככל האפשר. לצורך כך נדרש להגדיר מדיניות ארגונית בנושא הבקרים, להגן על התקשורת שלהם, לנהל את הגישה הפיזית, את מורשי הגישה אליהם ואת הפעולות המותרות לביצוע (עדכוני תוכנה, חיבור מדיה נתיקה וכד') וליישם מנגנונים המנטרים הפרעה בפעולתם באמצעות התקפת סייבר. בקרות אלו מתאימות גם למערכות משובצות מחשב (OT) בכלל.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרים תעשייתיים	12.1	יש לכתוב, לנהל ולבקר מדיניות ארגונית להגנה על סביבות בקרים תעשייתיים		ניתן ליישם באמצעות כתיבת מדיניות ונהלים תומכים אשר מגדירים הדרישות הייחודיות לסביבת הבקרים התעשייתיים ובהתייחס לאופי סביבת הבקרים (ייצור \ לוגיסטיקה \ בקרת סביבה \ ייצור כח ועוד) יש להתייחס להיבטים רגולטוריים הקיימים על סביבות אלו (לדוגמה, FDA, GXP, מערך הסייבר)	2
בקרים תעשייתיים	12.2	יוגדרו כללי שימוש נאות בציוד בסביבת הייצור ויוצב שילוט המסביר כללים אלו	הארגון יגדיר שילוט המסביר את נהלי אבטחת המידע בתחנות העבודה אשר שולטות ומבקרות את סביבת הייצור	השילוט עשוי לכלול את השימוש בתחנות העבודה המשותפות, שימוש בהתקני מדיה נתיקה, התנתקות משתמשים, ועוד	1
בקרים תעשייתיים	12.3	יש להגדיר את התהליכים הרגישים שבהם קיימות סביבות בקרה תעשייתיות לפי מידת רגישותם.	הארגון ימפה את התהליכים בהם קיימות סביבות בקרה ויגדיר את התהליכים העיקריים לעסק אשר מערבים בקרות אלו על מנת להבין את רמת הפגיעה העסקית והרגולטורית מכל סביבה כזו	מסמך מיפוי תהליכים וסביבות לפי רמת סיכון	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרים תעשייתיים	12.4	יש להפריד את רשתות הבקרה ממערכות אחרות ומרשתות חיצוניות	הארגון יבודד את רשתות הבקרה מרשתות משתמשים או שרתים לרשתות נפרדות באופן המגביל גישה ישירה בין הרשתות	ההפרדה יכולה להתבצע באמצעות שימוש בחומות אש ו-VLAN נפרדים לכל רשת בקרה. ההפרדה יכולה להתבצע באמצעות שימוש בחומות אש ו VLAN נפרדים לכל רשת בקרה. בהנתן האפשרות עדיף להפריד ע"י דיודה חד כיוונית ורק להוציא מידע מחוץ לארגון.	1
בקרים תעשייתיים	12.5	יש להפריד בין מערכת הניהול של בקרי ציוד תעשייתי ובין הרכיבים האופרטיביים של המערכת	יש ליישם הפרדה נאותה בין רשת הבקרים האופרטיביים ובין מערכת הניהול של הבקרים		2
בקרים תעשייתיים	12.6	אין לחבר התקנים שאינם בקרי סביבת ייצור לרשת בקרי הייצור	הארגון לא יתקין ציוד שאינו חלק ממערך רשת הבקרים התעשייתיים ברשת הבקרים. ציוד אשר נדרש לחברו יחובר לאיזור רשת נפרד ותקשורת תאופשר באופן פרטני	במידה ונדרש לחבר ציוד שונה אשר נדרש לחיבור לטובת ממשקים למערכות הייצור, יש לחברו בסגמנט רשת נפרד מאחורי חומת האש	1

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
בקרים תעשייתיים	12.7	גישת ספקי תמיכה לרשת הייצור תאופשר בהרשאה מראש וכן באמצעות תקשורת מאובטחת, מזוהה ואשר מאפשרת רישום פעולות הספק	הארגון יטמיע מערך תקשורת מאובטח לגישת ספקים ויבקר גישת הספק לארגון באמצעות מתן הרשאה מראש לכל התחברות ספק לרשת הבקרה	ניתן ליישם באמצעות מערך VPN לשרת ניהול ומשתמשים ייעודיים לכל ספק (בעדיפות למשתמש לכל עובד של הספק) אשר ינעלו בשוטף וייפתחו אך ורק במידת הצורך. מומלץ כי במידת האפשר, ספקים חיצוניים לא יתחברו ישירות לרשת הבקרה אלא לשרת מבודד אשר יש לו גישה ספציפית לרשת הבקרה עבור התחברות מרחוק ופעילות תחזוקה.	2
בקרים תעשייתיים	12.8	לא תאופשר גישה ישירה לאינטרנט מסביבת בקרים תעשייתיים וכן מסביבת ממשקי אדם מכונה		ניתן להגביל את רשתות הבקרה בחומת האש ולא לאפשר תקשורת ישירה לאינטרנט מרשתות אלו, שרתי עדכונים יאופשר מרשת חיץ באופן פרטני ולאחר מעבר דרך ציוד כגון PROXY	2
בקרים תעשייתיים	12.9	יוגבלו שירותים לא נחוצים בסביבת הייצור ובמערכות תומכות כגון ממשקי אדם-מכונה וחיישנים חכמים	הארגון יבטל ו\או יגביל שירותים לא נחוצים על כלל המערכות בסביבת הבקרה, בין אם ברמת מערכת הפעלה, רמת התקשורת והן רמת האפליקציה	ניתן להתבסס על מסמכי הקשחה של יצרני מערכת ההפעלה ואפליקציות ולכבות שירותים, לחסום פורטים, להגביל גישה אפליקטיבית לפונקציות מסויימות ועוד	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרים תעשייתיים	12.10	יש להשתמש בתקשורת אמינה בין ציודי הקצה לבקרים התעשייתיים במידת האפשר	יש להשתמש בפרוטוקולים אשר מאפשרים אימות המקור והיעד והצפנה של התווך בציוד תומך	בכל מקרה בו ניתן להשתמש בגרסאות מאובטחות של פרוטוקולים אלה יש להשתמש בגרסאות אלו (SFTP, HTTPS, SNMPv3 ועוד)	2
בקרים תעשייתיים	12.11	יוגדר מערך תקשורת חד-כיווני ממערכות ייצור לציוד החישה		יש להגדיר כלים להעברת תקשורת חד כיוונית בין חיישנים ומערכות בסביבות רגישות	4
בקרים תעשייתיים	12.12	רשתות אלחוטיות בסביבת הייצור יופרדו מרשתות אלחוטיות ארגוניות	הארגון יטמיע רשת אלחוטית ייעודית הנפרדת מהרשת האלחוטית הארגונית ומשמשת אך ורק לטובת תקשורת ברשת הבקרה, רשת זו לא תנותב לרשת הארגונית והפוך	יש להעדיף שלא להשתמש כלל ברשתות אלחוטיות ברשת הבקרה, אך במידה ונדרש לצורך העסקי, הקמת רשת זו תהיה בנפרד, ניהולה יהיה בנפרד והיא לא תוצמד לVLAN כלשהו של הרשת הפנימית	1
בקרים תעשייתיים	12.13	תקשורת אלחוטית בסביבת הייצור תוגבל באמצעות פרוטוקולים מאובטחים		יש להשתמש בWPA-2 PSK, במידת האפשר מומלץ להשתמש בגרסא מבוססת תעודות דיגיטליות לרשתות אלחוטיות אלו	1
בקרים תעשייתיים	12.14	יוגדר משתמש נפרד לכל לקוח קצה ברשת אלחוטית בסביבת הייצור	הארגון יגדיר משתמש נפרד לכל אדם ולכל ציוד ברשת האלחוטית	מומלץ לחבר את הרשת האלחוטית לשרת Radius ייעודי אשר יאמת משתמשים לרשת זו ויאפשר לנהל אותם	2
בקרים תעשייתיים	12.15	הגישה לממשקי אדם-מכונה תאופשר באמצעות משתמשים אישיים לכל מפעיל	הארגון יגדיר משתמש אישי לכל אדם העובד מול ממשק אדם מכונה. במידה והעמדה הינה עמדה שיתופית, ניתן להשתמש בהזדהות כרטיסים חכמים		2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרים תעשייתיים	12.16	הגישה לממשקי אדם-מכונה תאופשר באמצעות הזדהות חזקה	הארגון יגדיר הזדהות חזקה בגישה לממשק אדם-מכונה	ניתן להשתמש במגוון אמצעים כגון ביומטריה, כרטיסים חכמים, OTP ועוד	4
בקרים תעשייתיים	12.17	יותקנו מערכות ניטור ורישום פעילות על שרתי ניהול	הארגון יגדיר מערכות הקלטת פעילות \ רישום לוגים על שרתי הניהול של סביבת הבקרה	ניתן להשתמש במגוון אמצעים כגון כלים להקלטת מסכים ופעילויות משתמש, רישום לוגים של אפליקציה וכדומיהם	2
בקרים תעשייתיים	12.18	יותקנו כלי עזר כגון כלי זיהוי חדירות בסביבת רשתות הניהול של סביבת הייצור		ניתן ליישם באמצעות כלי IPS רשתי\ כלי HIPS וכלים דומים כגון Honeypots	3
בקרים תעשייתיים	12.19	יותקנו כלי ווידוא חתימות קבצים Integrity) (Checking לסריקת הקבצים המועברים לסביבת הניהול או אשר מותקנים בסביבת הניהול		ניתן ליישם באמצעות מגוון כלי File Integrity Checking	3
בקרים תעשייתיים	12.20	יותקנו כלים ייעודיים כנגד נוזקות בממשקי אדם-מכונה		ניתן ליישם באמצעות כלי anti-malware ייעודיים המתאימים לסוג המערכת	1
בקרים תעשייתיים	12.21	עדכוני תוכנה של היצרן יותקנו על סביבות נמוכות (סביבות בדיקה) טרם התקנתם בסביבת הייצור	הארגון יוודא בדיקה של עדכונים בסביבת בדיקות ויריצם לצרכי בדיקה לאורך זמן לצורך בדיקת יציבות המערכת והתהליך	ניתן ליישם באמצעות הקמת סביבה נמוכה (לפחות חלקית), הפניית התקשורת לסביבה זו בזמן חלון תחזוקה על סביבת הייצור ובדיקת התהליך	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרים תעשייתיים	12.22	יותקנו עדכוני מערכת הפעלה הנתמכים על ידי הספק בסביבת הייצור	הארגון יטמיע בתוך פרק זמן סביר עדכוני מערכת הפעלה ואפליקציה כפי שנתקבלו מיצרן המערכת וידרוש מהספק עדכוני אבטחה לליקויים חמורים המתפרסמים		1
בקרים תעשייתיים	12.23	כלי "נעילת תצורה" יותקנו על מערכות "סוף מחזור חיים" (End Of Life) ובהם מערכות הפעלה מיושנות	הארגון יטמיע כלים אשר נועלים את צורת המערכת לתצורה "נקייה" במידה ואין דרך לעדכן את הציוד		3
בקרים תעשייתיים	12.24	תוגבל היכולת להחדרת מדיה נתיקה לציודי הייצור ובכללם הבקרים, ממשקי אדם-מכונה וכן חיישנים		ניתן ליישם באמצעות ביטול התקני USB באופן פיזי (נעילת פורט) או באופן לוגי על ידי מדיניות מערכת הפעלה - GPO	2
בקרים תעשייתיים	12.25	העברת קבצים ממדיה נתיקה למערכות הייצור תבוצע לאחר "הלבנת" הקבצים המועברים	הארגון יטמיע מערך "הלבנת" קבצים ובדיקתם לעומק באמצעות מספר כלים טרם העברתם לסביבת הבקרים	ניתן ליישם באמצעות רכישת עמדות הלבנה ייעודיות או לחלופין באמצעות הקמת עמדה ייעודית הכוללת מספר מנועי סריקה שונים.	2
בקרים תעשייתיים	12.26	יתקיים מערך יתירות לרכיבים קריטיים בסביבת הייצור	הארגון יטמיע מערכת יתירות של שרתים וחיישנים קריטיים לסביבות הבקרה לצורך המשכיות התהליך	לצורך הקמת יתירות מומלץ להתייעץ בספק מערכת הבקרה	2
בקרים תעשייתיים	12.27	תוגבל גישה פיזית לפי צורך עסקי בלבד לסביבת הבקרים התעשייתיים וכן לציוד התקשורת בסביבה זו	הארגון יגביל גישה פיזית לארונות תקשורת, רכזות ועמדות ניהול של סביבת הבקרים	ניתן ליישם באמצעות הסבת חדרים ייעודיים לטובת ריכוזי תקשורת ושרתים ולבצע בקרת גישה באמצעות גישת תגים \ ביומטרי לסביבה זו	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
בקרים תעשייתיים	12.28	תוגבל גישה לוגית לפי צורך עסקי בלבד לסביבת הבקרים התעשייתיים וכן לציוד התקשורת בסביבה זו	הארגון יגביל גישת משתמשים ארגוניים אשר אין להם נגיעה עסקית למערך הבקרה וימנע גישתם לציוד ורשתות אלו		2
בקרים תעשייתיים	12.29	תוגבל במידת האפשר גישה לוגית (פונקציונלית) למערכות הייצור ובכללן ממשקי הבקרה, ממשקי הדגימה, ממשקי אדם-מכונה לפי תפקיד	גישה למערכות הניהול תוגבל לפי פרופיל משתמש, בקר מערכת לא ישנה הגדרות ופרמטרים של מערכת, שינוי פרמטרים יבוצע על ידי משתמש ניהולי	ניתן לוודא עם יצרן המערכת כי ישנה אפשרות להשתמש בפרופילי משתמש שונים במערכת	3
בקרים תעשייתיים	12.30	יש לבצע בדיקות אבטחת מידע ובכללן מבדקי חדירה בסביבות הייצור ובממשקי הניהול	הארגון יגדיר מתווה בדיקות כולל למגוון הרכיבים ברשת הבקרה בדגש על בדיקות אבטחת מידע מקיפות לכלל הרכיבים על מנת לשמור על רציפות תהליך עסקי	ניתן ליישם הן באמצעי בדיקת קונפיגורציה של הסביבות, הרצת סימולציות בזמן חלונות השבתה וכן ביצוע מבדקי חדירה לרשתות אלו במידת האפשר ו\או בזמן פעולות תחזוקה	2
בקרים תעשייתיים	12.31	יש להגדיר תרחישי ניטור ייחודיים לסביבת הייצור ולנטר אותם באמצעות מערך ניטור ארגוני	הארגון יגדיר מגוון תרחישי ניטור ייעודיים לסביבת הבקרה לפי מתאר האיום וחשיבות המערכת לתהליך העסקי	ניטור ברשתות בקרה שונה מניטור מערכות רגילות מאחר וסף הרגישות נמוך יותר, כל חריגה מכמות תקשורת רגילה בין הבקרים לממשקי הניהול והחיישנים עלולה להצביע על אירוע סייבר פוטנציאלי מאחר והפעילות רציפה ומונוטונית בסביבות אלו	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
13. אבטחת טלפונים סלולריים: טלפונים סלולריים הפכו להיות כלי מקצועי מרכזי – הם מכילים את אנשי הקשר, את תכתובות הדואר, אפליקציות ארגוניות שונות, סיסמאות ועוד. במקרים רבים הם מאפשרים גישה לרשת הארגונית וגם גלישה באינטרנט. מכאן, שהגדרה נכונה של הרשאות הטלפונים, השימוש העסקי שלהם וההגנה עליהם היא קריטית להגנה בסייבר של הארגון. נדרש להגדיר עבורם בקרת גישה, אבטחת תצורה, הטמעת כלי הגנה ייעודיים, אבטחת ערוצי התקשורת מהם לארגון, ניהול מרכזי - לרבות שליטה מרחוק למקרה של אובדן, ועוד.					
אבטחת טלפונים סלולריים	13.1	יש להגדיר מדיניות שימוש בטלפונים ניידים ולעדכנה באופן תקופתי	על הארגון להגדיר מדיניות שימוש בטלפונים ניידים לצרכי הארגון, לרבות גישה ליישומים ארגוניים ושמירה של נתונים רגישים של הארגון כל הטלפון		2
אבטחת טלפונים סלולריים	13.2	יש ליישם מנגנוני הגנה לבקרת גישה לטלפונים ניידים, כגון שימוש בסיסמה או באמצעי ביומטרי	על הארגון לקבוע את הפרמטרים לבקרת גישה למכשירים ניידים כגון שימוש בסיסמה באורך מסוים ונעילה אוטומטית	ניתן ליישם באמצעות שימוש בהגדרות מדיניות אוטומטיות המיושמות במכשיר בעת חיבורו לרשת הארגון	2
אבטחת טלפונים סלולריים	13.3	יש ליישם הגדרות אבטחה בטלפונים, המגבילים גישה לטלפון הנייד, שומרים על עדכניות התוכנה, מגבילים סיכונים של התקנת אפליקציות מסוכנות וכדומה	על הארגון לקבוע את הפרמטרים השונים ליישום במערכות ההפעלה של טלפונים ניידים, ולאכוף יישום הגדרות אלו במכשירים. הגדרות אלו כוללות אכיפה של עדכוני תוכנה, הגבלת שירותים מסוכנים, הגבלת התקנת תוכנות בלתי מוכרות או מסוכנות וכדומה.	ניתן ליישם באמצעות שימוש בהגדרות מדיניות אוטומטיות המיושמות במכשיר בעת חיבורו לרשת הארגון או באמצעות מערכת ניהול מרכזית	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת טלפונים סלולריים	13.4	יש ליישם הצפנה של נתונים רגישים הנשמרים על גבי מכשירים ניידים	נתונים רגישים של הארגון הנשמרים על המכשיר הנייד, כגון דואר אלקטרוני ארגוני, קבצים רגישים ויישומים רגישים, יוצפנו באמצעות מערכת ההפעלה של המכשיר או באמצעות יישומים ייעודיים	ניתן ליישם באמצעות הגדרות באפליקציות (יישומים) המבצעות הצפנה של המידע (יישום דואר אלקטרוני מאובטח, למשל) או באמצעות שימוש במחיצות המוצפנות באמצעות מערכת ההפעלה	2
אבטחת טלפונים סלולריים	13.5	יש ליישם כלי הגנה ייעודיים המזהים וחוסמים גישה בלתי מורשית ויישומים עוינים על גבי מכשירים ניידים	מכשירים ניידים, ובמיוחד כאלה הנמצאים בבעלות עובדי הארגון, חשופים במיוחד לחדירת תוכנות עוינות, בין אם כאלה שהוחדרו למכשיר ללא ידיעת בעליו ובין אם אלה מוסוות כיישום תמים. על מנת למנוע חדירת קוד עוין העלול לחשוף מידע רגיש של הארגון, יש להפעיל יישומים ייעודיים המזהים ומונעים הפעלה של קוד עוין.	ניתן ליישם באמצעות מערכות מסחריות המיועדות להגנה על מכשירים ניידים או באמצעות מכשירים מסחריים המיישמים יכולות הגנה מסוג זה	3
אבטחת טלפונים סלולריים	13.6	יש ליישם הצפנה של נתונים רגישים בתקשורת הנכנסת והיוצאת ממכשירים ניידים	תקשורת נתונים, הנכנסת ויוצאת מטלפונים ניידים, עושה שימוש ברשתות ציבוריות ובלתי-מאובטחות, על מנת להגן על המידע מחשיפה, יש להצפינה	ניתן ליישם באמצעות שימוש בפרוטוקולי הצפנה מקובלים ובאמצעות יישומים (אפליקציות) המבצעות הצפנה בעת הגישה לרשת הארגון	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת טלפונים סלולריים	13.7	יש ליישם אמצעי בקרת גישה לחיבור של מכשירים ניידים לרשת הארגון	מכשירים ניידים המתחברים לרשת הארגון, עושים שימוש בממשקי גישה מרחוק לרשת. על מנת לאבטח ממשק זה יש ליישם בקרת גישה כגון שימוש בטכנולוגיות תעודות דיגיטליות ובסיסמאות.		3
אבטחת טלפונים סלולריים	13.8	יש ליישם מערכת ניהול מרכזי, המנהלת את תצורת המכשירים הניידים ומאפשרת מחיקה מרוחקת של נתונים על המכשיר	אכיפת תצורה מאובטחת של טלפונים ניידים ושליטה מרחוק בנתונים רגישים הנשמרים על מכשירים ניידים מתאפשרת באמצעות מערכת ניהול מרכזית ורכיבי ניהול המיושמים על המכשירים.		2
אבטחת טלפונים סלולריים	13.9	יש ליישם מערכת ניטור אבטחת מידע מרכזית, המקבלת התרעות על אירועים חריגים על המכשירים הניידים ומאפשרת הכלה ותגובה לאירועים	על מנת לזהות אירועי תקיפה של מכשירים ניידים ולאפשר הכלתם ותגובה מתאימה, יש ליישם מערכת ניטור מרכזית המקבלת התרעות מרכיבים המיושמים על המכשירים הניידים.		3
אבטחת טלפונים סלולריים	13.10	יש לקבוע מדיניות להגנה או הגבלת שיחות המבוצעות באמצעות טלפונים ניידים	מכשירים ניידים עושים שימוש ברשתות ציבוריות ובלתי מאובטחות - על הארגון להגדיר כללי התנהגות וזהירות בעת ביצוע שיחות טלפון רגישות		4

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
14. ניהול שינויים: כחלק מתהליכי התפתחות הארגון והתעדכנותו, גם סביבת הסייבר של הארגון נדרשת לביצוע שינויים ועדכונים תקופתיים. הללו כוללים רכש חברות וחיבורן לתשתיות הארגון, שדרוגים טכנולוגיים, הוספה או שינוי של תהליכים עסקיים (למשל שרשרת אספקה) ועוד. תהליכי עדכון או שינוי אלו טומנים בחובם סיכון גדול לפגיעה במערכות הארגון ובמידע הקיים בהן. בהתאם לכך, על הארגון לנהל את השינויים באופן אשר יצמצם את הסיכון. ניהול זה כולל מדיניות לניהול תצורה של סביבת הסייבר בארגון, תיעודה ועדכונה השוטף.					
ניהול שינויים	14.1	יש לכתוב וליישם מדיניות לניהול תצורה, לבקר ולעדכן אותה תקופתית	מסמך המדיניות יכלול התייחסות לשינויי חומרה ותצורה והתייחסות לשינויי תוכנה	פרק ניהול שינויים בתוך מדיניות אבטחת מידע ארגונית ונהלים תומכים. פרק זה חשוב במיוחד עבור מערכות בקרה מאחר ובמערכות אלה כל שינוי מהווה סיכון לבטיחות תפעולית. לכן לפני ביצוע השינוי יש לבצע בדיקות קפדניות ולתעד כל שלב בביצוע השינוי. הנושא חשוב גם לצורך FORENSICS במקרה שהתרחש אירוע.	2
ניהול שינויים	14.2	יש לקבוע, לתעד ולעדכן בעת הצורך את התצורה הבסיסית הנדרשת של מערכת המידע	הארגון יתעד את תצורת מערכת המידע בעת הקמתה כולל תיעוד הרכיבים, תיעוד התקשורת, תיעוד הגדרות המערכת וכן נוהל התקנתה	ניתן ליישם במאצעות הכנת תיק מערכת	2
ניהול שינויים	14.3	יש לסקור את התצורה הקיימת של מערכות המידע על בסיס תקופתי, כאשר מתרחשים אירועים שהוגדו ע"י הארגון וכחלק אינטגרלי בתהליכי התקנה ועדכון גרסה	הארגון יתעד את השינויים במערכות המידע בעת שינוי תצורה משמעותי או אחת לתקופה (הקודם מביניהם)	ניתן ליישם באמצעות תהליך תיעוד שינויים	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
ניהול שינויים	14.4	יש ליישם מנגנונים אוטומטיים על מנת לשמור על עדכניות, שלמות ומוכנות הגדרות התצורה הבסיסית של מערכת המידע	הארגון יישם מערך של גיבוי ושחזור תצורה של מערכת המידע ורכיביה		3
ניהול שינויים	14.5	יש לשמור גרסאות קודמות של תצורת המערכת לצורך תמיכה בחזרה לאחור (Rollback)	הארגון יוודא כי קיימים כלים ושיטות לחזרה לאחור עבור שינויים שלא צלחו	ניתן ליישם באמצעות גיבוי המערכת באופן מלא לפני השינוי ובאמצעות שדרוג מדורג של רכיבים (סביבת בדיקות \ סביבת DR ועוד)	2
ניהול שינויים	14.6	יש לקבוע אילו שינויים במערכת מוגדרים כשינויי תצורה, לתעד בקשות לשינויי תצורה ואת הסטטוס שלהן (אושרו ובוצעו / נדחו) ולשמור אותן למשך פרק זמן שיוגדר	הארגון ינהל תהליך של אישרור השינויים לפני החלתם	ניתן ליישם באמצעות קיום ישיבות ניהול שינויים שבועיות ואשרור השינויים תוך הסבר על מהות השינוי	2
ניהול שינויים	14.7	יש ליישם מנגנון אוטומטי ל: תיעוד בקשות לשינויי תצורה, התראה לסמכות המאשרת ואיסור ביצוע שינויים עד שכל האישורים הנדרשים התקבלו	הארגון יתפעל מערכת מידע אשר תרכז את תהליך ניהול השינויים בכלל ותהליך אשרור השינויים בפרט.		4
ניהול שינויים	14.8	יש לנתח שינויים במערכת המידע על מנת לקבוע השפעות אבטחה פוטנציאליות לפני הטמעת השינוי (עקב חולשות, חוסר תאימות, כוונת זדון וכו')	הארגון ינהל תהליך של הערכת הסיכון כחלק מתהליך ניהול השינויים הארגוני. כחלק משלבי הגשת בקשת השינויים יתועדו ההשפעות הפוטנציאליות על זמינות ואמינות המערכת	ניתן ליישם באמצעות שאלון משלים לבקשת ניהול השינויים ובו מפורטים הסיכונים בעת ביצוע השינוי	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
ניהול שינויים	14.9	יש לנתח שינויי תצורה במערכת המידע בסביבת בדיקות נפרדת לפני יישום בסביבת הייצור	הארגון יבדוק את השינויים בסביבת בדיקות נפרדת לפני יישום השינויים בסביבת הייצור	ניתן ליישם באמצעות קיום סביבת בדיקות הדומה בגרסתה לסביבת הייצור.	2
ניהול שינויים	14.10	לאחר ביצוע שינוי תצורה במערכת המידע, יש לבדוק את פונקציות האבטחה על מנת לוודא כי הן פועלות כהלכה	הארגון יבדוק את כל המערכת ורכיביה בהתייחס להיבטי אבטחת המידע ובכללם: אימות, הרשאות, הצפנה, הקשחה וכל פונקציונליות אבט"מ אחרת הקיימת במערכת.	יש לבצע באמצעות סקירה של הבקרות הנדרשות ואף במידת הצורך באמצעות מבדקים כגון סקר בקרות ומבדקי חדירה	3
15. אבטחת מדיה: אמצעי מדיה (מגנטית, נתיקה, אופטית, מכנית) משמשים לצורך הכנסה והוצאה של מידע מהארגון. אמצעי המדיה משמשים לאחסון וניוד מידע הן בתוך הארגון והן החוצה ממנו. מידע זה עשוי להיות רגיש עבור הארגון, לקוחותיו או ספקיו, ועל כן נדרש להגן עליו מפני הגעה לידי גורם שאינו מורשה. כמו כן, אמצעי מדיה עלולים לשמש להכנסת פוגענים לתוך הארגון. לכן יש להגדיר וליישם מדיניות טיפול והגנה על מדיה (כולל גריטת המדיה).					

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת מדיה	15.1	יש לכתוב וליישם מדיניות הגנה על מדיה (מגנטית, נתיקה, אופטית, מכנית), לבקר ולעדכן אותה באפן שוטף אחת לתקופה	הארגון יכתוב ויישם מדיניות שימוש והגנה על מדיה הכוללת התייחסות לאופן שימוש במדיה, אחסון מדיה, ואופן השמדת המידע האגור במדיה ו\או השמדת המדיה עצמה בסוף השימוש (או סוף חיי המדיה)	המדיניות תתייחס לדוגמה לסוגי התקנים מאושרים לעומת כאלו שאסור לבצע בהם שימוש, האם מותר להשתמש במדיה (כגון מחשב/זכרון נייד, טלפון של העבודה) לצרכים פרטיים או שאסור, האם מותר לצאת עם מדיה זו מחוץ לגבולות הארגון וכיצד, מה עושים עם המדיה כאשר היא תקולה/ יצאה משימוש וכו' מדיניות זו תגזור את הנהלים הרלוונטיים לארגון כגון: תהליכים למיפוי מדיה וכן לניפוק המדיה (כגון רכש דיסקים מגנטיים לשרתים, מדיה אופטית) והגדרה כי גישה למדיה הנ"ל תסופק בהתאם לנהלי הארגון עבור בעלי תפקיד רלוונטיים (דוגמת גישה לדיסקים קשיחים רק לאנשי IT,גישה למדיה נתיקה לבעלי תפקיד הנדרשים לכך וכו')	2
אבטחת מדיה	15.2	יש לתייג את המדיה בהתאם לרמת סיווג המידע המוכל בה וכן לציין את אופן הטיפול במדיה בהתייחס להיבטי אבטחת מידע והגבלות ההפצה שלה	הארגון יגדיר נהלים ותהליכי תיוג המדיה וכן יתייג את המדיה עצמה בהתאם לרמת הסיווג המידע המוכל בו.	ניתן לתייג את המדיה באמצעות כלים כגון מדבקות על קלטות גיבוי, על אריזות למשלוח דיסקים קשיחים או על דיסקים אופטיים.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת מדיה	15.3	יש לאחסן מדיה באופן מאובטח	הארגון יגדיר את אופן אבטחת אחסון המדיה, לרבות התייחסות לסוגים שונים של מדיה (מגנטית / אופטית / נתיקה / פיסית)	ניתן לממש באמצעות תהליכים כגון הגנה פיזית על איזורי אחסון של מדיה פיזית, הצפנת הגיבויים ואחסון המדיה המגנטית אצל ספק אחסון מורשה, הגנה על ארונות תקשורת הכוללים שרתים ומערכי אחסון וכן דיסקים קשיחים, אחסון מדיה אופטית ורכיבי אחסון למערכי הצפנה (HSM) בכספות.	2
אבטחת מדיה	15.4	יש להגדיר תהליכי השחרה ו/או והשמדת מדיה	הארגון יגדיר נהלים ותהליכים להשחרת (השחרה = מחיקת כל מידע רגיש ממצע המידע טרם הוצאתו מרשות הארגון או ייעודו לשימוש אחר) והשמדת מדיה וכן ינהל מעקב שוטף אחר ביצוע תהליכי השחרה והשמדת המדיה. מטרת הבקרה הינה לוודא כי מידע רגיש לא יוצא מהארגון ללא בקרה.	ניתן לבצע השחרה של מדיה באמצעות תהליך ידני (כגון מחיקה פרטנית של המידע הרגיש, כגון נתוני כרטיס אשראי או פרטים מזהים של לקוחות וכו') או באמצעים טכנולוגיים (במקרים בהם ההשחרה מבצעת מחיקה שיטתית של תבניות ידועות מראש). השמדת מדיה יכולה להתבצע באמצעות גריסה / מגנוט / איפוס באמצעות כתיבה מרובה למדיה.	2
אבטחת מדיה	15.5	בעת חיבור מדיה נתיקה אל רשת הארגון, יש לבצע פעולות ניקוי בכדי לוודא שהמדיה איננה מכילה נוזקות או גורמים זדוניים אחרים	הארגון יגדיר תהליך של הלבנת המדיה (הלבנה = סריקה וניקוי מאיומי קוד עויין) לפני הכנסתה למערכות הארגון	ניתן לממש באמצעות עמדות הלבנה ייעודיות אשר יסרקו את המידע במדיה לפני חיבורה למערכות הארגון.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחת מדיה	15.6	יש להגדיר וליישם הגבלות שימוש במדיה תוך שימוש באמצעי אבטחה	הארגון יגדיר ויישם טכנולוגיות ושיטות להגבלת שימוש במדיה. זאת במטרה לצמצם איומי דלף מידע באמצעות מדיה נתיקה וכן איומי חדירת קוד עוין לרשת הארגון באמצעות מדיה נתיקה	ניתן למימוש באמצעות הקשחת תחנות העבודה בהתאם לסוג המערכת/עמדה או הרשאות של בעל התפקיד, כך שלא כל עובד יוכל לחבר התקן זכרון (כגון Disk On Key) למחשב. ניתן לממש הגדרה לפיה כל מידע שיוצא מתוך העמדה למדיה נתיקה יוודא יציאה אל התקן/תיקייה מוצפנת.	2
אבטחת מדיה	15.7	יש לממש מנגנוני הצפנה להגנה על מדיה דיגיטלית במהלך העברתה מחוץ למתקני הארגון	הארגון יחיל אמצעי הצפנה על מדיה אשר מיועדת להיות מועברת אל מחוץ לארגון או כזו אשר באופן שוטף בשימוש מחוץ לארגון (כגון מדיה נתיקה)	ניתן לממש באמצעות כלים כגון: הצפנת מדיה נתיקה, הצפנת קלטות גיבוי בעת הגיבוי וכו'.	3
אבטחת מדיה	15.8	יש לבדוק את הציוד להלבנת ולהשמדת המדיה באופן תקופתי על מנת לוודא את אפקטיביות הטכנולוגיה	הארגון יגדיר תהליך לבדיקת ציוד ותהליכי הלבנה והשמדת מדיה אשר יכללו בדיקה של אפקטיביות של התהליכים והטכנולוגיות המיושמות	ניתן לבדוק את מערכות ההלבנה / השמדה באמצעות בדיקות מדגמיות אחת לתקופה, כגון: באמצעות ניסיון הכנסת קובץ דמה, ניסיון הוצאת קובץ רגיש, ניסיון אחזור מידע רגיש ממדיה שהוצאה מכלל שימוש.	3

16. שרשרת אספקה ומיקור-חוץ:

פעילותם של ארגונים רבים תלויה בשירותים שהם רוכשים מספקים חיצוניים. שירותים אלו יכולים להיות קבלני משנה שמייצרים רכיבים ממוחשבים, ספקים של שירותי מחשוב שונים, אפליקציות שבשירות הארגון וכו'. שירותים אלו יכולים להיות בעלי קישוריות אל מערכות הארגון, ועל כן עלולים להוות ערוץ תקיפה כנגד הארגון. בהתאם לכך, על הארגון להגן על עצמו מפני פגיעה העשויה להגיע מצד ספקיו. הוא עושה זאת באמצעות דרישות משפטיות וחוזיות להגנה בסייבר מספק השירות, באמצעות סקרי ספקים לבחינת מנגנוני ההגנה בסייבר שלהם, באמצעות נוהלי עבודה מול הספק וכו'.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
שרשרת אספקה ומיקור חוץ	16.1	יש להתגונן מפני איומים של שרשרת האספקה על המערכת כחלק מאסטרטגיית "הגנה לרוחב" (Defense in Breadth)	הארגון ימפה ויזהה את האיומים והסיכונים הנובעים משימוש במערכת / שירות הספק על האספקטים הטכנולוגיים והתהליכיים הגלומים בהם, ויגלם את הסיכונים כחלק מתהליך ניהול הסיכונים והאיומים הארגוני. מומלץ להבחין בין סוגים שונים של ספקים כגון: מעבד/מחזיק מידע, ספק תמיכה/ פיתוח, ספק שירותים בענן	לצורך המיפוי ניתן להיעזר גם באיסוף מידע מודיעין סייבר אודות הספק כמטרה ולהשתמש במידע זה במכלול השיקולים וקבלת ההחלטות אודות ניהול הסיכון, כמו כן יש להתחשב במנגנונים ובקרות הקיימים בחצרות הספק ובתהליכיו בהשפעתם על התהליך העסקי (או התליכים העסקיים) שהמערכת / השירות תומכות בהם (לדוגמה בקרות אוטומציה והקמת שרתים ווירטואליים בפלטפורמת הספק בענן ואופן ההקשחה שלהם עלולים להשפיע על הארגון עצמו במידה והסביבות לא מוקשחות ו/או ספק שירותי הענן אינו מאובטח / נמצא במדינה עויינת ועוד)	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
שרשרת אספקה ומיקור חוץ	16.2	יש להשתמש בכלים חוזיים ומשפטיים בעת רכישת מערכת מידע או שירות מספקים	הארגון ישתמש במנגנונים חוזיים כגון מגבלות אחריות ומנגנונים משפטיים אחרים על מנת למזער את הסיכונים הנובעים מרכישת המערכת / השירות מהספק.	נוסף על סעיפי הגבלת אחריות וסעיפי פיצוי בעבור נזק, עמידה בדרישות רגולטוריות וחוקיות ניתן אף לעגן סעיפים כגון התראות מוקדמות בהפסקת שירות ו/או תמיכה מורחבת מעבר לתקופה אשר בה המערכת מוכרזת כEnd-Of-Life, הסכמי סודיות ושמירה על מידע בצורה מאובטחת או כל סעיף אחר המהווה גורם בקרה מפצה לסיכונים הגלומים בהקמת המערכת / רכישת השירות.	2
שרשרת אספקה ומיקור חוץ	16.3	יש לבצע סקר ספק לפני חתימה על חוזה רכישה של שירותים ומוצרים	הארגון יבצע סקר אודות אופי והתנהלות הספק טרם חתימת החוזה.	יבוצע סקר ספק אשר יכול לכלול: בשלות הספק, כמות הטמעות / לקוחות, יציבות הספק, יכולת עמידה ביעדי שירות, מערך ניהול האבט"מ, ההמשכיות העסקית של הספק ועוד.	3
שרשרת אספקה ומיקור חוץ	16.4	במקרים בהם יש חיבור לרשת הספק, יש ליישם בקרות מונעות אשר תפקידן למזער נזק המגיע מתשתיות הספק	הארגון ישתמש בבקרות הקיימות אצלו או בקרות יעודיות אחרות על מנת למזער את הנזק ממערכות / שירותי הספק.	בקרות כאלו יכולות להיות הפרדת סביבות, הפרדת ממשקים, סניטיזציה של הפלט המגיע ממערכות הספק, הפרדת התקשורת באמצעות שרת מתווך (Proxy) ועוד.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
שרשרת אספקה ומיקור חוץ	16.5	יש לבצע בדיקת מערכת / שירות בהיבטי אבטחת מידע לפני היישום בארגון	הארגון יבדוק את המערכת / השירות באמצעות כלים פנימיים וכן שימוש במבדקי חדירה טרם עליית המערכת / השירות לשלב הייצור.	ניתן לבדוק את המערכת הן באמצעי כלי ניהול פגיעויות והן באמצעות ביצוע סקרי סיכונים ומבדקי חדירה לפתרון הספק תוך כדי ווידוא שאין ממצאים חמורים אשר ישפיעו על הארגון ועל תהליכיו.	4
שרשרת אספקה ומיקור חוץ	16.6	יש להגדיר את רמת הקריטיות של המערכת / שירות בהתייחס להתליכים העסקיים המסתמכים עליה	הארגון יגדיר את מערכת כקריטית אם פגיעה בה או ברכיביה משפיעה על תהליך עסקי קריטי.	יש להוסיף את המערכת / שירות לרשימת המערכות הקריטיות בארגון ולהפעיל אמצעי ניטור ובקרה על המערכת/ השירות כדי לוודא שאין פגיעה ברציפות השירות.	3
17. אבטחה ברכש ופיתוח: במסגרת תהליכי רכש ופיתוח, הארגון מכניס מרכיבי סייבר לתוכני הארגון (למשל ברכישת תוכנה חדשה או בפיתוח מכשיר ייעודי). דרך תהליכי רכש ודרך שלבים שונים בתהליכי הפיתוח ניתן להכניס פוגענים לרשת הארגון. מנגד, דרך שלבים שונים בתהליכי פיתוח מוצר ניתן לשלב הגנות, שיקלו בעתיד על הארגון להתמודד עם איומי סייבר על מערכות ולארגון. מטרת הבקרות להקטין את הסיכוי כי הרכש או התוכנה/המערכת המפותחת יחדירו סיכוני סייבר לארגון. הבקרות כוללות כתיבת מדיניות בתחום, שתכווין את פעילות כלל הגורמים בארגון (רכש, משפטי, מנהלי פרויקט, מפתחים וכד'), דרישות הגנה לרכש/לפיתוח, ניהול סיכונים לרכש/לפיתוח, הגנות לאורך כל מחזור חיי התוכנה/מערכת וכו'.					
אבטחה ברכש ופיתוח	17.1	יש לכתוב וליישם מדיניות לרכש ופיתוח מערכות ושירותים, לבקר ולעדכן אותה תקופתית	מטרת הבקרה הינה לוודא כי כלל מערכות הארגון יעמדו ברף ההגנה שהגדיר הארגון. הן עבור מערכות אשר מפותחות באופן עצמאי והן מערכות אשר נרכשות כתוכנות מדף או כשירות בענן.	מדיניות זו תכלול בין היתר התייחסות לרמת SLA רצויה, עמידה בדרישות הגנה ברמות השונות (מדיניות סיסמאות, לוגים, הצפנה וכו'), גישה מרחוק, גישת מפתחים לייצור וכו'.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.2	עבור מערכות ברמת ערכיות 3 ומעלה, הארגון יוודא עמידה בדרישות התקן על ידי גורם חיצוני בלתי תלוי בארגון	הארגון יוודא כי נכסים אשר על פי שאלון הערכיות קיבלו ציון 3 ומעלה, עומדים בכל דרישות תורת ההגנה. וידוא העמידה בדרישות יהיה באמצעות סוקר חיצוני לארגון המפתח/ רוכש	במקרה של פיתוח עצמי, ניתן להיעזר בחברות ייעוץ/התעדה לטובת בחינת רמת ההגנה של המערכת בהתאם לדרישות התוה"ג. במקרה של רכש מספק חיצוני, נדרש לוודא כי המערכת עומדת בדרישות תורת ההגנה לנכסים מסוג 3 או לחילופין לדרוש מהפסק להציג אישור של עמידה בסטנדרטים מקובלים כגון /SOC1 SOC2 וכן בדרישות נוספות נדרשות (כגון עמידה ב PCI, HIPAA וכו' בהתאם לסוג המידע אותו המערכת שומרת/מעבדת). אישורים אלו יתועדו ויגובו בהסכם ההתקשרות מול גוף הפיתוח/הספק (כולל התחייבות לעדכן במידה וההסמכה נלקחת או שפג תוקפה)	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.3	ניהול סיכוני סייבר - יש להעריך את סיכוני הסייבר ואבטחת המידע הכרוכים בפיתוח ורכש מערכת או שירות חדש ולנהלם בהתאם לתהליכי ניהול הסיכונים הקיימים בארגון	מטרת הבקרה הינה לוודא כי היבטי ההגנה שולבו עוד משלב הייזום והתכנון, דרך הפיתוח ועד להעברה לייצור. הארגון יוודא כי ייזום רכש או פיתוח של מערכות ושירותים מבוצע לאחר סקירת הסיכונים הכרוכים בו ושילובם כחלק מניהול הסיכונים הארגוני.	מומלץ לבצע את הערכת הסיכונים הראשונית עוד בשלב היזום כך שהארגון יהיה ערוך להטמיע בקרות כחלק מתהליך הפיתוח, או לחלופין יהיה מוכן לקבל את הסיכונים שזוהו. לטובת מיפוי סיכונים ניתן להיעזר במתודות מוכרות של היצרנים כגון שיטות ל SSDLC, פרסומי SANS ו - OWASP. חשוב לשים לב למערכות אשר יהיו במיקור חוץ ו/או בענן מאחר והן כוללות סיכונים פרטניים אשר חלקם מכוסים במסמך זה ולטובת העמקה ניתן לבחון את ההמלצות של תקנים ייעודיים לאבטחת ענן כגון ISO 27017, תקן CSA וכו'.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.4	יש לדרוש ממפתחי המערכת לספק תיאור פונקציונלי של בקרות האבטחה שיושמו במערכת, ומידע אודות עיצוב ומימוש הבקרות	הארגון ידרוש תיעוד מלא של בקרות אבטחת המידע המוטמעות במערכת על מנת לוודא עמידה בדרישות אבטחת המידע ולצרכי תהליך ניהול הסיכונים והאיומים הארגוני)	מומלץ לקבל את מסמכי האפיון הפונקציונלי, מסמכי האפיון המפורט ואפיון (FD, DD/LLD, HLD) העל הכוללים את תיעוד הבקרות כחלק ממכלול תיעוד מנגנוני המערכת המלא. תיעוד זה יכלול לדוגמה את סוג ההצפנה, אופן וידוא בדיקת קלט, קבלת תסריטי הבדיקה בנושא הגנה בסייבר ועוד. הספק יתייחס במסגרת התיעוד לפיתוחים שלו וכן לשימוש בתוספים חיצוניים (ספריות חיצוניות, PLUG IN, תוכנות צד ג' ממשקים חיצוניים וכו'). מטרת בקרה זו הינה להבין לא האם הארגון מיישם את דרישות האבטחה אלא כיצד הוא מיישם אותן (פרוטוקול/תהליך/כלי תומך וכו')	3
אבטחה ברכש ופיתוח	17.5	ארכיטקטורה מאובטחת - יש להטמיע עקרונות ארכיטקטורה מאובטחת במסגרת האפיון, עיצוב, פיתוח, מימוש ושינוי מערכת המידע	הארגון יוודא כי בעת תכנון מערכות ושירותים מיושמת ארכיטקטורה מאובטחת, בין אם התכנון מבוצע על ידי הארגון, בתיאומו, בהנחייתו או בבקרתו של הארגון על עבודת ספק חיצוני.	עקרונות הארכיטקטורה המאובטחת יכולים להיגזר מבקרות המובאות בפרקים של מסמך זה, סטנדרטים מקובלים ועוד.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.6	פיתוח מאובטח - יש לדרוש ממפתחי המערכת שימוש בכלים ושיטות לפיתוח מאובטח כחלק אינטגרלי מתהליך הפיתוח	הארגון יטמיע מתודולוגיית פיתוח מאובטח ויוודא הטמעה של מתודולוגיה לפיתוח מאובטח אצל ספקי מערכות ושירותים המבצעים תהליכי פיתוח.	ספק התוכנה יעביר תיעוד על אופן מימוש עקרונות פיתוח מאובטח בפועל. התיעוד יפרט את הכלים בהם נעשה שימוש, המתודה איתה עובדים, סוגי הבקרות שיש לספק על רמת ההגנה של המערכת ועוד.	3
אבטחה ברכש ופיתוח	17.7	הפעלה בטוחה - יש להחזיק מדריך לניהול מערכת המידע אשר כולל את אופן הגדרת התצורה הטובה ביותר עבור היבטי אבטחה.	מדריך ההתקנה ותפעול המערכת יספקו את המידע הנדרש לטובת התקנת המערכת בתצורה (קונפיגורציה) בטוחה.	כחלק מתיעוד תצורת קנפוג המערכת יש לכלול - מדריך התקנה, הגדרות להקשחת התשתיות והאפליקציה, פריסה מומלצת, וכדומה. עבור מערכות ברמת ערכיות 3 ומעלה, נכון לאשר מראש את תצורת המערכת המומלצת כגון פורטים פתוחים, שימוש בשירותי רשת, עבודה בפרוטוקולים מאושרים, שינוי סיסמאות ברירת מחדל וכו' מאחר וסוגיית ניהול שינויים בתצורת המערכות הינו נושא אשר קשה לפיקוח ומעקב באופן ידני, עבור נכסים ברמה 3 יכללו מנגנון מפצה לבחינה אוטומטית של שינוי תצורה (חוקים בתוך ה SIEM, מערכת ניהול תצורה מרכזית Continuity control (monitoring	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.8	אבטחת שרשרת אספקה - יש לדרוש מספקי שירותים לציית לדרישות האבטחה הארגוניות, רגולציות, סטנדרטים והנחיות	הארגון יוודא כי ספקי שירות עומדים בדרישות הציות (Compliance) הארגוניות וכן דרישות הרגולטוריות החלות במדינות בהן פועל הארגון.	ניתן להגדיר את הדרישות הרגולטוריות של הארגון כחלק ממסך דרישות אבטחת מידע סטנדרטי, המיועד לספקי שירות חיצוניים.	1
אבטחה ברכש ופיתוח	17.9	יש לבצע בדיקות אבטחת מידע ולטפל בחשיפות שנתגלו בהן, בטרם הטמעת מערכות ושירותים. בדיקות אלו יכללו, לכל הפחות, בדיקת פונקציונליות האבטחה (מימוש הדרישות) ובדיקת חשיפות אבטחה.	הארגון יוודא כי בוצעו בדיקות אבטחת מידע בטרם העלאה לאויר של מערכת או שירות חדש או בעת ביצוע עדכונים למערכת.	במקרים בהם מתקבל שירות מספק חיצוני, ניתן להסתמך על מבדקים אשר בוצעו על ידי או עבור הספק. בדיקות אלו יכולות להתבצע באמצעות הפעלת כלי תקיפה אוטומטיים או באמצעות גורם אנושי. בדיקות אלו יכולות לכלול ניסיות להשיג גישה לא מורשית, להחדיר קוד עויין לבסיס נתונים ולממש תקיפות ידועות כגון SQLI, XSS, CSRF וכו'	2
אבטחה ברכש ופיתוח	17.10	יש לתעד את התהליך לטיפול בליקויים וחשיפות אבטחת המידע שנתגלו במהלך הבדיקות.	מטרתו של תיעוד תהליך הטיפול בחשיפות הינו לוודא שלמות ואפקטיביות הטיפול.	מטרת הבקרה הינה לוודא כי הליקויים שנמצאים מטופלים בהתאם למדיניות הארגון. מעקב זה יאתר ליקויים חמורים שפתוחים זמן רב, ליקויים רוחביים שלא מקבלים מענה, יסייע לבניית תכנית העבודה התקופתית של מנהל הגנת הסייבר ויוצגו להנהלה אחת לתקופה	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.11	יש לבצע ניתוח קוד סטטי (Static Code Analysis) כחלק ממבדקי אבטחת מידע למערכת/שירות חדש	הארגון יבחן מערכות ברמה 3 באמצעות כלים אוטומטיים אשר מהווים תחליף לסקירת קוד ידני (Code review).	ניתן לבצע בדיקות קוד בסיוע כלים ממוכנים אשר יודעים לקחת קטע קוד בתצורות שונות (Source code, קוד מקומפל, URL וכו') ולאתר פרצות קיימות בקוד. השימוש בכלי יעשה הן לפני רכישת המערכת והן בעת ביצוע שינויים בסביבת המערכת	3
אבטחה ברכש ופיתוח	17.12	יש לבצע תיקוף של הערכת הסיכונים והחשיפות של המערכת לאחר השלמת פיתוח המערכת	מטרת תיקוף הערכת הסיכונים היא לוודא את התאמת תמונת הסיכונים שבוצעה בעת תכנון המערכת למערכת כפי שפותחה	ביצוע סקר סיכונים למערכת בסיום הפיתוח ולפני כניסה לייצור	3
אבטחה ברכש ופיתוח	17.13	יש לבצע את בדיקות אבטחת המידע של המערכת על ידי גורם חיצוני בלתי-תלוי	הארגון יגדיר את התיחום של הסקר (Scope) אשר יבוצע על ידי הספק ואת סוג הבדיקה (כובע לבן/אפור/שחור) אך הבדיקה בפועל תתבצע על ידי גורם חיצוני לארגון	ביצוע PT באמצעות אנשי הארגון עלול לייצר מצב של ניגוד עניינים בתוך הארגון. שימוש בגורם חיצוני בלתי תלוי תסייע להעלות את רמת ההגנה של המוצר. במקרה של שימוש בכלים אוטומטיים, ניתן להביא גורם צד ג' אשר יבדוק כי אכן הכלי מבצע בדיקות חדירה אשר מכסות את התיחום של המערכת וכי גורם זה ינגיש את התוצרים לארגון (כתיבת הדו"ח המסכם של הבדיקה) הבדיקות יתבצעו בסביבה קרובה ככל הניתן לסביבת הייצור	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.14	יש לוודא כי בדיקות המערכת כוללות אימות כי בקרות אבטחת המידע שהוגדרו אכן מיושמות בהתאם לאפיון המקורי	יש לנהל רשימת תיוג של דרישות ההגנה שהוגדרו למערכת ולוודא כי אכן כל הדרישות מומשו על ידי אנשי הארגון והספק	בשלב המסירה יש לוודא אל מול רשימת הדרישות המוגדרות בתכנון המפורט כי אכן הוטמעו, וכן יש לתעד את מהות ותוצאות הבדיקה.	3
אבטחה ברכש ופיתוח	17.15	יש לדרוש מהספק לבצע ניתוח קוד דינמי Dynamic Code) (Analysis כחלק ממבדקי אבטחת מידע למערכת/שירות חדש	יש לדרוש מהספק לבצע ניתוח קוד דינמי Dynamic Code) (Analysis כחלק ממבדקי אבטחת מידע למערכת/שירות חדש	בדיקות הקוד הדינמיות יבוצעו על ידי כלים ייעודיים הקיימים על המדף או באמצעים כגון Fuzzing וכן בדיקות אוטומטיות של כלי סריקה בעת ריצה, הדוחות או הממצאים יבדקו אחת לתקופה על ידי הארגון באופן מדגמי כדי לוודא כי אכן מבוצעים תיקונים בהתאם.	3
אבטחה ברכש ופיתוח	17.16	יש לממש מנגנון למניעת שיבוש קבצים (tamper resistance) ברכיבי המערכת.	הארגון יוודא כי גוף הפיתוח (פנימי או חיצוני) מימש במערכת יכולת מניעת שיבוש קבצים	מנגנונים למניעת שיבוש יכולים להיות מיושמים באמצעות חתימת קבצים, הצפנה, יצירת העתקים ועוד.	4
אבטחה ברכש ופיתוח	17.17	יש לממש שיטות למניעת הכנסה של רכיבי מערכת מזויפים	מטרתם של מנגנונים אלה הינם למנוע הכנסה של רכיבי חומרה או תוכנה מזויפים לארגון, בין אם במתכוון או באמצעות הטעיה של גורם בשרשרת האספקה.	דוגמאות למגנונים מסוג זה הינם: בדיקת רכיבי חומרה, בדיקה ואימות של קבצי תוכנה נכנסים וכדומה. מנגנונים אלו יכולים להיות מרמות שונות של אבטחה החל מרמת מידור הגישה הפיזית למחשב, סיסמת BIOS, הצפנת הדיסק, הגדרה כי מערכת ההפעלה תוכל לבצע BOOT אך ורק מתוך ה HD, חוקים במערכת ה SIEM בנושא ועוד.	4

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.18	יש לוודא כי מערכות נרכשות/מפותחות מיישמות מנגנוני אימות קלטים	מערכות מפותחות יישמו מנגנונים שמטרתם לוודא סינון של קלטים בלתי צפויים כגון קלט באורך/פורמט בלתי צפוי, העלולים להוביל לתוצאה בלתי-צפויה ולפגיעה בחסיון, שלמות או זמינות המערכת בהתאם לרמת ערכיות המערכת	ניתן לבצע עבור מערכות ברמה 2 על ידי קבלת הצהרה מהיצרן לגבי ביצוע בדיקות קלט ושימוש בספריות תוכנה סטנדרטיות המסננות קלטים בהתאם לאופי הקלט הצפוי. עבור מערכות ברמת ערכיות 3 נדרש לממש פתרון טכנולוגי (כגון WAF) ברמה הרשתית או לוודא מנגנון מקביל ברמת האפליקציה. יש לוודא בשלב ביצוע תיחום סקר מבדק החדירה כי נושא בדיקות הקלט מכוסה בצורה מקיפה (OWASP יכול להוות נקודת ייחוס טובה) וכן בהתאם למדיניות הארגון בנושא.	2
אבטחה ברכש ופיתוח	17.19	יש לוודא כי מערכות נרכשות/מפותחות מיישמות מנגנוני טיפול נאות בשגיאות	מערכות מפותחות יישמו מנגנונים שמטרתם לכידה נכונה של שגיאות והצגה מבוקרת של תוצאות שגיאת מערכת באופן שלא חושף מידע רגיש. בכל מקרה, יש לוודא כי מנגנון השגיאות איננו חושף מידע רגיש של המערכת כגון שמות טבלאות או משתמשים בבסיס הנתונים, שפת כתיבת המערכת, גרסאות של תוכנות וכו'	ניתן לבצע על ידי יישום הטמעת מנגנון ניהול שגיאות המציג שגיאה סטנדרטית בקרות שגיאה	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
אבטחה ברכש ופיתוח	17.20	יש לוודא כי מערכות נרכשות/מפותחות מיישמות מנגנוני אימות פלט	מערכות מפותחות יישמו מנגנונים שמטרתם לוודא סינון של תוצאות (פלטים) בלתי צפויות, העלולות להיגרם מהתקפה על המערכת ולחשוף מידע רגיש מתוך המערכת	ניתן לבצע על ידי שימוש בספריות תוכנה סטנדרטיות המסננות תוצאות בהתאם לאופי הפלט הצפוי. כמו"כ ניתן למימוש באמצעות מערכות לאיתור אנומליות אשר מבוססות על התנהגות המערכת/משתמש/ מערכת הפעלה וכו'	3
אבטחה ברכש ופיתוח	17.21	יש לוודא כי מערכות נרכשות/מפותחות מיישמות מנגנוני Session מהימנות	מערכות מפותחות יישמו מנגנונים שמטרתם לוודא מניעה של מתקפות על מנגנון ניהול חיבור כגון חטיפת חיבור (session hijacking) או man-in-the-middle	ניתן לבצע על ידי ניהול נכון של session, מחיקת של חיבור בתום פעילות משתמש, אקראיות של מזהי חיבור (Tokens) וכדומה	2
18. הגנה פיזית וסביבתית: ההגנה הפיזית והסביבתית הינה נדבך חשוב בהגנת הסייבר של הארגון, שנועדה למנוע מתוקף לחדור לסביבת הסייבר באמצעים פיזיים. פעילות מונעת כוללת, בין היתר, מתן גישה פיזית רק לגורמים מורשים במתקני הארגון, הגנה פיזית על התשתיות הדרושות למרחב הסייבר, כגון חשמל, מיזוג, הגנה מפני נזקי מים וכד'. בנוסף, מערך הגנה פיזי יעיל ימנע גם מקרים של פגיעה בזדון בציוד וכן יתריע במקרה של פגיעה כזאת לגורמים השונים בארגון. פרק זה לא מכסה את כלל הפעילויות בתחום ההגנה הפיזית של הארגון, אלא מוגבל לנדרש לטובת הגנת הסייבר בלבד.					
הגנה פיזית וסביבתית	18.1	יש לכתוב וליישם מדיניות הגנה פיזית וסביבתית, לבקר ולעדכן אותה תקופתית	מטרת הבקרה הינה להגדיר את ראיית הארגון בנושאים כגון נעילת משרדים בסוף יום, מצלמות אבטחה, כניסת אורחים וכניסת עובדים חיצוניים למתחמי החברה ולאיזורים רגישים, הגנה נאותה על חדרי השרתים וחדרי הבקרה וכו'		2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנה פיזית וסביבתית	18.2	יש לכתוב וליישם נהלים אשר יסייעו בהטמעת מדיניות הגנה פיזית וסביבתית והבקרות הרלוונטיות	יש לכתוב נהלי בקרת גישה פיזית למתקן הארגון לרבות: 1. נוהל גישה פיזית 2. נוהל אורחים במתחם הארגון 3. נוהל גישה לחדר מחשב / חדר תקשורת		2
הגנה פיזית וסביבתית	18.3	יש להגדיר ולתחזק רשימת מורשי גישה למתקן בו נמצא הנכס, לנפק אמצעי הזדהות לצורך גישה למתקן, לסקור את הרשימה תקופתית ולהסיר ממנה אנשים כאשר הרשאת הגישה אינה נדרשת יותר	יש לתחזק את רשימת מורשי הגישה למתקני החברה ולעל הארגון להחזיק רשימה עדכנית	הנפקת תעודת עובד / מבקר לצורך זיהוי	2
הגנה פיזית וסביבתית	18.4	יש לאכוף בקרת גישה פיזית בנקודות כניסה/ יציאה למתקן	יש ליישם בקרת גישה פיזית בכל הכניסות / יציאות ממתקני הארגון	דלת + קורא כרטיסים, מנעול, קורא ביומטרי, שומר, קודן וכו'	2
הגנה פיזית וסביבתית	18.5	יש לשמור לוגים של גישה פיזית למתקן	יש לתעד ולשמור את רישומי (לוגים) של כלל הכניסות והיציאות של כלל המבקרים	רישום כלל הכניסות והיציאות במסד נתונים / לוגים או רישום ידני באמצעות שומר	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנה פיזית וסביבתית	18.6	יש לבקר, לתעד לאבטח ולאכוף בקרת גישה פיזית לאזור ריכוזי תקשורת / מחשוב (חדרי שרתים / ארונות תקשורת)	יש להגביל את הגישות הפיזיות של גורמים שאינם מורשים לאזורי ריכוז של תקשורת / מחשוב (חדרי שרתים ותקשורת). על הארגון להגדיר רשימת מורשי גישה לאזורים הללו ולאכוף את הגישה בהתאם וע"פ נהלי הארגון	1. יש להגדיר הרשאות גישה (פיזית ולוגית) מתאימות עבור הגורמים המורשים 2. יש לתעד באמצעות רישום לוגים או רישום יומן נוכחות בעת הגישה לחדרי מחשוב. במידה ולא ניתן למכן את תיעוד הגישה לארונות התקשורת וחדרי השרתים, יש לבחון הגנה פיזית עליהם באמצעות מנעול אשר ימנע מגורמים בלתי מורשים להתחבר אל ציוד זה	2
הגנה פיזית וסביבתית	18.7	יש לשלוט בגישה פיזית למכשירי פלט של המערכת על מנת למנוע מגורמים בלתי מורשים להשיג את הפלט (לדוג': מדפסות ופקסים)	מטרת הבקרה הינה לוודא כי המידע מגיע לבעליו המקורי. בקרה זו חשובה בפרט במקומות שבהם ישנו מידע פרטי כגון פקסים אשר כוללים מידע רפואי או ביטוחי, הדפסה של פרטים אישיים של עובדים וכו'. במקרים אלו, חשוב לוודא כי המידע נחשף אך ורק למי שאמור להיחשף אליו.	ניתן ליישם במספר תצורות: 1. ניתן ליישם ע"י מערכת בקרת הדפסה אשר דורשת קוד או כרטיס עובד לפני קבלת הפלטים 2. מיקום המדפסות בחדר סגור אשר הגישה אליו מוגבלת 3. במקרה של פקס, ניתן לבצע שימוש בשירותים כגון FAX2MAIL או לכל הפחות לוודא הימצאות ליד הפקס לפני קבלתו 4. מומלץ לוודא בסוף יום כי אמצעי פלט אשר ממוקמים באזורים ציבוריים/מרובי משתמשים יהיו "נקיים" וכי מידע אישי לא יהיה נגיש למי שאיננו אמור להיות חשוף אליו.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנה פיזית וסביבתית	18.8	יש לנטר את הגישה הפיזית למתקן בו נמצא הנכס על מנת לגלות ולהגיב לאירועי אבטחה, ולסקור את הלוגים על בסיס תקופתי	מטרת הבקרה הינה למנוע גישה מגורמים בלתי מורשים אל אזורים רגישים. גישה כזו יכולה לאפשר לגורמים עויינים לסצע פעולות זדוניות כגון חיבור אמצעי האזנה, התחברות לרשת, גניבת חומרה ועוד. מטרת הבקרה הינה לוודא כי כל מי שניגש לאזורים אלו עושה זאת לאחר שהארגון הגדיר כי הוא מורשה לבצע זאת.	יש לנטר את כלל הגישות הפיזיות לאזורים רגישים כגון חדרי שרתים, ארונות תקשורת וכו' באמצעות רישום של הנכנסים והיוצאים	3
הגנה פיזית וסביבתית	18.9	יש לנטר ולהתריע על כל גישה פיזית לנכס שלא בשעות העבודה המקובלות או בימים שאינם ימי עבודה	יש לעשות שימוש באמצעי ניטור והתרעה לצורך זיהוי גישות שאינם מורשות בשעות ובזמנים שאינם מוגדרים ימי ושעות עבודה מקובלות לצורך זיהוי גישות שאינם מורשות	ניתן לעשות שימוש מערכת אזעקה ו/או שימוש במוקד בטחון לצורך ניטור והתרעה מפני גישה שאינה מורשית למתקן	3
הגנה פיזית וסביבתית	18.10	יש להגדיר ולקיים מערך תגובה עבור גישות שאינן מורשות למתקן הארגון בעת זיהוי		ניתן ליישם באמצעות שימוש בכונן מהארגון (קב"ט), מוקד בטחון חיצוני / חברת שמירה וכו'	3
הגנה פיזית וסביבתית	18.11	יש להטמיע מצלמות וידאו למעקב אחר גישה פיזית לנכס ולשמור את ההקלטות בפרק זמן שיוגדר	יש להתקין מצלמות אבטחה במעגל סגור לצורך ניטור שוטף של כלל הכניסות הפתחים המאפשרים גישה למתקן הארגון, כמו כן יש לנטרם באופן שוטף ורצוף על ידי איש בטחון		4

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנה פיזית וסביבתית	18.12	יש לתעד רשימת אורחים למתקן	יש לתעד ולתחזק את רשימת האורחים למתקני הארגון	רישום ביומן מבקרים / תיעוד כלל המקרים במערכת ייעודית לזימון אורחים למתקני הארגון	2
הגנה פיזית וסביבתית	18.13	יש לשמור על ציוד החשמל וכבלי החשמל של המערכת מפני נזק	יש להקפיד על סלילה נכונה ותיוג נכון של כלל כבלי החשמל בחדרי השרתים ובארונות התקשורת	יש לסמן כלל כבל בקצוות שלו על מנת שעובדי הארגון יוכלו לזהות בקלות לאיזה שרת / מערכת הוא שייך ולמנוע ניתוק בשוגג	2
הגנה פיזית וסביבתית	18.14	על הארגון להיות בעל יכולת לספק חשמל לטווח קצר באופן שאינו ניתן לשיבוש על מנת לאפשר כיבוי מסודר של המערכת או העברתה לספק כח חלופי		ניתן ליישם מערך UPS's לצורך אבטחת הורדה מסודרת של המערכות בעת מצב שבו אין זרם חשמל קבוע	2
הגנה פיזית וסביבתית	18.15	על הארגון להיות בעל יכולת לספק חשמל למשך זמן ממושך באופן שאינו ניתן לשיבוש על מנת לאפשר המשך פעילות עסקית סדירה		ניתן להשתמש בגנרטור לצורך יישום הבקרה	3
הגנה פיזית וסביבתית	18.16	יש ליישם ולתחזק תאורת חירום אוטומטית אשר תופעל באירוע של הפסקה או שיבוש חשמל, ותכלול יציאות חירום ונתיבי פינוי במתקן			1
הגנה פיזית וסביבתית	18.17	יש ליישם ולתחזק אמצעים/מערכות לזיהוי וכיבוי אש עבור מערכת המידע אשר נתמכות במקור אנרגיה עצמאי			1
הגנה פיזית וסביבתית	18.18	יש לשמור ולנטר רמות טמפרטורה ולחות מקובלות במתקן בו נמצא הנכס		בקרה זו רלוונטית בעיקר בחדרי שרתים	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנה פיזית וסביבתית	18.19	יש להגן על הנכס מפני נזק כתוצאה מדליפת מים באמצעות האופציה ל-master shutoff או שסתומי בידוד			2
הגנה פיזית וסביבתית	18.20	יש לאשר, לנטר ולשלוט ברכיבי מערכת אשר מוכנסים ומוצאים מהמתקן		ניתן לממש לדוגמה באמצעות נוהל הוצאת רכיבי תוכנה / חומרה מהארגון, הנוהל צריך להתייחס להיבטי הוצאת רכיבי חומרה / תוכנה אשר עשויים להכיל מידע רגיש. הניטור והבקרה אחר מידע שיצא מהארגון יכול להתבצע באמצעות מעקב אחר חומרה שיצאה מהארגון (כגון מחשבים ניידים שחולקו לספקים או התקני זכרון שחולקו). הרישום והמעקב יהיו תקופתיים ויכללו למי ניתנה החומרה, לכמה זמן, לאיזו סיבה ותאריך החזרה משוער.	2
הגנה פיזית וסביבתית	18.21	יש ליישם בקרות אבטחה באתרי העבודה החלופיים (כגון אתר DR) ולהעריך את מידת האפקטיביות שלהן		רמת האבטחה הפיזית באתר חלופי כגון אתר ה DR תהיה ברמה מקובלת והולמת את המידע המאוחסן שם. מימוש הבקרה באמצעות תמיכת הנושא בנוהל ובחוזה ההתקשרות מול האתר אליו פורסים בחירום וכן באמצעות ביקורת תקופתית של הנושא	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנה פיזית וסביבתית	18.22	יש למקם את רכיבי המערכת במתקן בו פוטנציאל הנזק כתוצאה ממפגע יהיה מינימלי, והאפשרות לגישה בלתי מורשית תהיה מינימלית	במידת האפשרי יש למקם את המערכות (חדרי השרתים / תקשורת) במיקום מוגן ככל שניתן במרכז המבנה ולא בצמוד לקירות חיצוניים או בקירוב למקורות מים (כולל צינורות)		3

19. משאבי אנוש:

עובדי הארגון מהווים נדבך חשוב בהגנת הסייבר הארגונית. מצד אחד, יש ביכולתם לזהות ולהתריע על אירועים חשודים מיד עם התרחשותם, ומנגד הם עשויים להוות נקודת תורפה, אשר תוביל לאירוע סייבר בשוגג (בעקבות טעות או תוך ניצולם על-ידי תוקף), או בכוונה. בהתאם לכך, על הארגון להקפיד לשלב בתהליכי הגיוס בדיקות מתאימות למועמדים, על-פי רגישות התפקידים, ליידע את עובדיו בדבר איומי הסייבר השונים, כיצד להתגונן מפניהם ולמי עליהם לדווח. על הארגון להגדיר את כללי ההתנהגות של עובדיו במרחב הסייבר החיצוני (רשתות חברתיות, חשיפת מידע פנים-ארגוני באינטרנט וכד'), שיכול להשפיע על רמת ההגנה של הארגון. בתהליך העזיבה על הארגון לבטל את ההרשאות של העובד.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
משאבי אנוש ומודעות עובדים	19.1	יש להעריך את רמת רגישות התפקידים השונים בארגון ולגבש קריטריונים מתאימים לתהליכי מיון בקבלת עובדים	יש לגבש דרישות מינימום להתליכי הגיוס וכן דרישות נוספות עבור תפקידים רגישים במיוחד	דרישות מינימום לדוגמה יכולות לכלול בדיקות רקע ואימות נתונים, דרישות נוספות יכולות לכלול מבחני אמינות או פוליגרף. מומלץ לייצר מטריצה אשר מגדירה מול בעלי התפקידים השונים את סוג הבדיקה הרצוי כך שתהיה מידתיות ושימוש מותאם סיכון בכלי האבחון הקיימים. לדוגמה הגדרה כי כל עובד בחברה נדרש להמצאת ר.פ מהמשטרה (לא חוקי), ביצוע של סיווג בטחוני אם נדרש, ביצוע מבדק אמינות, ביצוע פוליגרף, אימות נתונים אשר נמסרו על ידי המועמד, בדיקת ממליצים של מקומות עבודה קודמים. עובדי התמיכה הטכנית נדרשים למבחן אמינות ממוחשב, בעלי הרשאות גבוהות (כגון ADMIN) נדרשים לתחקיר במכון אבחון חיצוני וכו'	2
משאבי אנוש ומודעות עובדים	19.2	יש לבצע בדיקות רקע למועמדים בעת גיוס ומעבר לתפקיד בעל רמת רגישות שונה	יש לבצע בדיקות רקע למועמדים /עובדים במעבר תפקיד בהתאם לתפקידים בטרם מתן הרשאת גישה למערכות המידע.	בדיקות רקע למועמדים/עובדים יכולות לכלול: אימות נתוני רקע, שיחות עם ממליצים, מבדקי אמינות ו/או פוליגרף, בדיקות רקע כלכליות ואחרות, מבדק בטחוני	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
משאבי אנוש ומודעות עובדים	19.3	יש להחתים את העובדים על הצהרה לגבי מחוייבות המשתמש להקפיד על דרישות הסייבר של הארגון	העובד חותם על הצהרות כי הוא מודע לכך שמערכות הארגון מכילות מידע חסוי עסקית ואין להוציאו או לניידו ללא אישור מפורש בהתאם לנהלי הארגון	ניתן ליישם באמצעות החתמת כלל העובדים על טופס ייעודי אשר ישמר בתיק העובד. בנוסף ניתן ליישום באמצעות מערכת לניהול זהויות (IDM) אשר תאפשר תהליך אשרור תקופתי אוטומטי אשר יוודא כי העובד חתם על ההצהרות וההסכמים	2
משאבי אנוש ומודעות עובדים	19.4	יש להחתים את העובדים על הצהרה לגבי מחוייבות לשמירה על סודות הארגון לאחר סיום ההעסקה	העובד חותם על הצהרה כי הוא איננו ימסור מידע רגיש של הארגון לגורמים שאינם מורשים וכי איננו לקח עימו מסמכים או אמצעי אוגר מידע אשר מכיל מידע עסקי של הארגון	ניתן ליישם באמצעות נוהל/מסמך עליו חותם העובד. ניתן גם לבצע ביקורת מדגמית כתהליך משלים להחתמה על הטופס התחייבות. ביקורת זו יכולה להתבצע באמצעות ניטור פעילות המשתמש ברשת לאיתור אנומליות (נסיונות גישה לתיקיות שאינן שלו, ניסיונות להעתיק כמות מידע גדולה וכו').	2
משאבי אנוש ומודעות עובדים	19.5	יש להגדיר דרישות אבטחה לספקים וגורמי צד ג'	הארגון יגדיר דרישות אבטחת מידע כחלק ממדיניות ההתקשרות עם ספקים, הדרישות יכללו הגבלות לגבי שיתוף מידע, הסכמי סודיות, הכרה של נהלי אבטחת המידע בארגון, הדרכות לספקים ועוד.	ניתן ליישם כסט נהלים ולהחתים את עובדי הספק על ההסכמים המתאימים בעת תחילת עבודתם, כמו כן יש לבצע ריענון של הנהלים מדי תקופה	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
משאבי אנוש ומודעות עובדים	19.6	יש להגדיר כללי התנהגות בעבודה מול מערכות המידע בארגון, כללים אלו מגדירים את תחומי האחריות וכללי השימוש הנאות במערכות המידע בארגון ובדגש על מערכות רגישות	הארגון יגדיר נהלי התנהגות בהתייחס למערכות המידע ויפיצם לכלל העובדים.	ניתן ליישם באמצעות נוהל אשר מגדיר לדוגמה את מדיניות ההורדות בארגון, גלישה לאתרי שיתוף קבצים, גלישה ועבודה עם כתובת המייל הפרטית/העסקית, וכו'. ניתן לממש באמצעות תהליך ארגוני אשר מתעד את נהלי השימוש או באמצעות לומדות אשר ניתנות לעובדים חדשים וכן באמצעות כלים מיכוניים כגון: Appliction control & URL filtering	1
משאבי אנוש ומודעות עובדים	19.7	יש להגדיר נהלים והגבלות המתייחסים לשימוש ברשתות החברתיות.	יש להגדיר נהלים והגבלות המתייחסים לשימוש ברשתות החברתיות הכוללים: הגבלות על אופן פרסום מידע ארגוני ברשתות החברתיות ובאתרים ציבוריים, ייצוג הארגון ברשתות חברתיות ואופן הגישה לרשתות חברתיות ממערכות הארגון.	נהלי שימוש ברשתות חברתיות יכולים לכלול התייחסות לאופן בו הארגון מצפה מעובדיו לייצג את הארגון במדיה זו, למידע שמותר/אסור לחשוף בעת השימוש במדיה ולכללי זהירות בעת גישה לרשתות חברתיות ממערכות הארגון.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
משאבי אנוש ומודעות עובדים	19.8	יש להגדיר וליישם תהליך הטלת סנקציות על עובדים שלא צייתו לנהלי אבטחת מידע	הארגון יחליט על נהלים משמעתיים לטיפול באירועי אבטחת מידע שביצעו עובדים או קבלנים, יתעד וינהל רישום של צעדים משמעתיים אשר ננקטו.	לדוגמה: עובד שפעל הניגוד להנחיות מפורשות יזומן, יחד עם מנהלו, לשיחת בירור עם גורמי אבטחת מידע/בטחון. במקרים מסוימים יש טעם בהערות משמעתיות, סנקציות שונות ועד לסיום עבודתו של העובד. יש לשים לב למקרים בהם יש לערב ייעוץ משפטי או להודיע לרשויות החוק.	3
משאבי אנוש ומודעות עובדים	19.9	יש לבחון ולעדכן את הרשאות הגישה של עובד בעת ניוד עובד מתפקיד לתפקיד	יש להגדיר תהליכים של עדכון על ניוד העובד ושל עדכון ההרשאות בהתאם לתפקיד החדש (הסרת ההרשאות המיותרות והקמת ההרשאות הנדרשות לתפקיד החדש)	יישום תהליך עדכון ההרשאות יכול להתבצע באופן ידני, על ידי העברת הודעה מתאימה לגורם המנהל את ההרשאות במערכות המידע או באופן אוטומטי, במקומות בהם ישנם ממשקים ממוכנים לניהול ההרשאות, המשולבים במערכות משאבי האנוש (כגון מערך ניהול זהויות ממוכן). בעת מעבר תפקיד, ישנה עדיפות להסרה מלאה של ההרשאות הישנות והגדרת ההרשאות הנדרשות לתפקיד החדש, על מנת שלא תיוותרנה הרשאות עודפות כתוצאה מתפקיד קודם.	1

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
משאבי אנוש ומודעות עובדים	19.10	יש לבטל הרשאות גישה ולחסום חשבונות משתמש בעת סיום העסקה	יש להגדיר תהליכים של עדכון על עזיבת עובד צפויה, ושל טיפול בחסימת הרשאותיו וחשבון המשתמש	יישום תהליך חסימת חשבון משתמש והרשאות יכול להתבצע באופן ידני, על ידי העברת הודעה מתאימה לגורם המנהל את חשבונות המשתמשים וההרשאות במערכות המידע או באופן אוטומטי, במקומות בהם ישנם ממשקים ממוכנים לניהול ההרשאות, המשולבים במערכות משאבי האנוש (כגון מערך ניהול זהויות ממוכן). בעת סיום ההעסקה יש לחסום את ההרשאות ואת חשבון המשתמש ולהקפיאו לתקופה מתאימה, שבסופה יש למחוק את חשבון המשתמש.	2

20. הדרכות:

תרבות של הגנת סייבר בארגון חשובה לצמצום סיכוני התקיפה של הארגון. התקפות רבות משתמשות כיום בהנדסה חברתית (Social Engineering) על-מנת לתקוף את הארגון – למשל, חדירה לארגון או ביצוע תקיפת כופרה (Ransomware) דרך מייל Phishing, התחזות לצורך ביצוע פעולות מורשות (כגון העברת כספים) וכו'. עובדי החברה מהווים כלי משמעותי בידי התוקף, ולכן הדרכות והעלאת מודעות הן כלי ארגוני חשוב להתמודד עם סיכונים אלו. הארגון נדרש לבצע הדרכות לעובדים בנושא הגנה בסייבר בכל הרמות ובאופן עתי - הן הדרכות כלליות של העלאת מודעות והן הדרכות ספציפיות לבעלי תפקידים רגישים ונושאי משרה - ולתרגלם באופן שוטף.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
הדרכות	20.1	יש לפתח, לתעד וליישם מדיניות הדרכות מודעות בנושא אבטחת מידע	הארגון יגדיר מדיניות הדרכות בנושאי מודעות אבטחת המידע ובה יפרט מה הוא פרק הזמן שבו יש לרענן את ההדרכות, מי יודרך ובאילו תחומים, כיצד יש לבצע מעקב אחר ביצוע ההדרכות	ניתן ליישם באמצעות כתיבת מדיניות הדרכות הכוללת את הגדרת הסמכויות לביצוע ומעקב אחר ביצוע ההדרכות והתכנים המועברים. מדיניות זו תגדיר את אוכלוסיות היעד השונות (עובדים חדשים, בעלי תפקידי מפתח, עובדים שהעסקתם הסתיימה), התייחסות לספקים וגורמים חיצוניים, הגורם המעביר את ההדרכות, אופן הפיקוח והבקרה (החתמה על הצהרה/מבחן וכו'), הישגים נדרשים, תדירות ההדרכות ונושאים חיוניים אשר חייבים להיכלל בהדרכות.	2
הדרכות	20.2	יש לבצע הדרכה בסיסית לעובדים בנושא אבטחת מידע	הארגון יכיל הדרכה בסיסית אשר תתייחס לשימוש נאות במידע, כללי אבטחת מידע בארגון, איומים פנימיים וחיצוניים הכוללים את הסימנים המזהים לאיומים.	ניתן ליישם באמצעות לומדה פנימית ו/או לומדה חיצונית אשר תותאם לצרכי הארגון (בהתייחס למדיניות הארגון)	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הדרכות	20.3	יש לבצע הדרכה ייעודית לבעלי תפקידים ונושאי משרה בעלי גישה למשאבים רגישים בנושא אבטחת מידע	הארגון יכיל הדרכות ראשוניות ותקופתיות אשר יכללו (בהתאם לתפקיד): בקרות אבטחה סביבתיות ותפעולן במידת הצורך, בקרות אבטחה פיזית ותפעולן, תרגולים מעשיים לגבי תפעול אירועי אבטחת מידע וסייבר , התנהגויות חשודות של מערכת וזיהוי התנהגות קוד זדוני.	ניתן ליישם באמצעות לומדה פנימית ו/או לומדה חיצונית אשר תותאם לצרכי הארגון ובהתאם להגדרות התפקיד (בהתייחס למדיניות הארגון)	3
הדרכות	20.4	הארגון יעלה את המודעות לנושא ההנדסה החברתית בקרב העובדים	יש לוודא כי בעלי התפקיד השונים מכירים את איום ההתחזות וניסיונות לשיטוי מצד תוקפים פוטנציאלים	ניתן לבצע באופן עצמאי או באמצעות חברה חיצונית. ניסיונות אלו יכולים לכלול בדיקת בקשות "לא לגיטימיות" מאנשי התמיכה, בקשה לקבלת מידע בשם גורם אחר, ניסיונות לבצע פעולה ללא אימות המבקש, ייזום בקשות ברשתות החברתיות או באמצעות הדוא"ל ועוד.	4

איתור Detect

21. תיעוד וניטור:

תורת ההגנה מניחה, כי על אף תהליכי ההגנה - יהיו תקיפות שיחדרו לארגון. כחלק מההתמודדות עם אירוע סייבר על הארגון להיות מסוגל לזהותו ולטפל בו. לצורך כך, הארגון נדרש לתעד פעילויות רלוונטיות במערכותיו, העשויות להוות אינדיקציה לאירוע סייבר. נוסף על כך, על הארגון לנטר תיעוד זה באופן שיאפשר לו לזהות אירועים אלו בהקדם האפשרי, לצורך תגובה מהירה וצמצום הנזק ככל האפשר. הבקרות נועדו להגדיר את האירועים ולייצר תשתיות תיעוד וניטור אפקטיביות.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
תיעוד וניטור	21.1	יש לכתוב וליישם מדיניות תיעוד וניטור, לבקר ולעדכן אותה תקופתית		מדיניות ארגונית בנושא ניטור ובקרה וכן נהלים תומכים, כגון נהלי מוקד ניטור אבט"מ, נהלי איסוף אירועים ועוד	2
תיעוד וניטור	21.2	יש לקבוע אירועים אותם המערכת תתעד (כלומר תרשום אודותיהם לוגים), לתעד כיצד רשומות בקרה אלה מתאימות לתחקור אירועים ותקריות אבטחה וכן להגדיר את פרק הזמן שיש לשמור נתונים אלה. בנוסף יש להגדיר באילו מערכות יש להפעיל auditing (שרתים, רכיבי תקשורת, אפליקציות, מסדי נתונים וכו')	הארגון יקבע אילו אירועים יאספו ממערכות הארגון למערך ניטור אבטחת המידע וכן יגדיר רשימת חוקי ניטור אשר ישתמשו באירועים אלו. יש להגדיר את פרק הזמן המינימלי לשמירת הנתונים, במיוחד במקרים ישנה דרישה רגולטורית המגדירה את פרק הזמן האמור	ניתן ליישם באמצעות ביצוע אפיון וסקירה של אירועים נפוצים והמתקבלים והגדרת חוקים לפי סוגי האירועים הנדרשים לאיסוף לצורך תיחקור אירועים ותקלות לאחר התרחשותם	2
תיעוד וניטור	21.3	יש לבחון באופן תקופתי את הגדרת האירועים המתועדים ואת אפקטיביות מערך הרישום	יש לבחון באופן תקופתי את הנחות העבודה ואת השינויים במערכות הארגון במטרה לבדוק את שלמות הניטור. כמו כן יש לסקור תקופתית את תקינות האירועים הנרשמים והתאמתם להגדרות ולצרכי הארגון	בחינה תקופתית של מנגנוני רישום הלוגים והתאמתם למערכות הארגון. במקרה של מערכת ניטור מרכזית ניתן להפעיל מנגנונים אוטומטיים המוודאים את פעילות ותקינות מערכת רישום האירועים	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
תיעוד וניטור	21.4	יש להפעיל מנגנון המייצר רשומות בקרה אודות אירועים במערכות הארגון. יש לרשום, לכל הפחות, אירועים ממערכות המכילות מידע רגיש של לקוחות, מערכות קריטיות לתפקוד הארגון ומערכות ליבה (שרתים, רכיבי תקשורת, אפליקציות, מסדי נתונים וכו')	הארגון יוודא כי מערכות תשתית ומערכות אפליקטיביות מפעילות מנגנון רישום אירועים, וכי הרשומות נשמרות לפרק זמן שהוגדר על ידי הארגון. רשומות הבקרה יכילו מידע כגון: סוג האירוע, מתי התרחש, מקור האירוע, שם המשתמש. בכל מקרה, יש לנטר את המערכות המעבדות מידע רגיש, מהוות חלק מהתשתית הקריטית של הארגון או מנהלות את תהליכי הליבה של הארגון	בדרך כלל, ניתן להפעיל מנגנוני רישום קיימים במערכות תשתית. במקרה של מערכות אפליקטיביות, יש לוודא כי המערכת מאפשרת רישום פעילויות. ניתן גם להפעיל מנגנוני רישום מרכזיים המחוברים למערכות הארגון, ואוספים את רשומות האירועים ממערכות אלו למאגר מרכזי	1
תיעוד וניטור	21.5	הארגון יגדיר מידע נוסף אשר נדרש כחיוני לרישום בלוג המתקבל מהמערכות הארגוניות, לרבות מזהה ייחודי של הפעולה, פקודות ושאילתות שבוצעו	יומן הפעילות (לוג) הבסיסי במערכות השונות איננו מכיל בהכרח את כל המידע הנדרש לתטובת תחקור אירוע. לטובת קבלת מידע חיוני זה, על הארגון להגדיר את הפעולות/מידע הרצוי לשמירה בקבצי ה - LOG. במערכות רגישות יש צורך בתיעוד מעמיק ומפורט של הפעולות שבוצעו במטרה ליצור התרעות איכותיות	יש להגדיר את השדות הנדרשים לניטור במערכות השונות. לעתים יש צורך בהגדרת הניטור בשלבי הפיתוח של מערכות או בהרחבת מאגרי הניטור במטרה לאסוף מידע מפורט זה	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
תיעוד וניטור	21.6	הארגון יישם מערכת מרכזית לניטור והתרעה	יש לאפיין ולהטמיע מערכת ניטור והתרעה מרכזית בארגון, המקבלת אירועים ממערכות הארגון השונות ומרכזת את תהליכי הניתוח, ההתרעה והטיפול באירועים חשודים	לדוגמה, יישום מערכת SIEM, המרכזת את מכלול תהליכי הניטור וההתרעה על אירועי אבטחת סייבר	3
תיעוד וניטור	21.7	מנגנוני הרישום יכללו, לכל הפחות, מידע אודות אופי הפעולה שבוצעה, חתימת זמן, מקור ויעד הפעולה, מזהה משתמש, מזהה תהליך, כשלון/הצלחה, שם קובץ מעורב		עבור ארגון מרמה 1 יש לבקש מספק התוכנה/ המפתח כי הלוגים יכללו לכל הפחות את השדות המוגדרים בבקרה זו. עבור ארגונים מרמה 2 - יש לוודא כי לוג הפעילות אכן כולל את המידע הנדרש. בדרך כלל, ניתן להפעיל מנגנוני רישום קיימים במערכות תשתית. במקרה של מערכות אפליקטיביות, יש לוודא כי המערכת מאפשרת רישום פעילויות	1
תיעוד וניטור	21.8	יש להקצות שטח אחסון מספק עבור רשומות הבקרה	הארגון יוודא כי שטח האחסון המוקצה לרשומות הלוג ולמערך הניטור עונה לצרכיו לאורך זמן כפי שהוגדר	יש לבצע תכנון מקדים של דרישות אחסון הנתונים וכן לבצע תכנון קיבולת תקופתי	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
תיעוד וניטור	21.9	יש לייצר מנגנון של קבלת התראה במידה של הפסקת כתיבת נתונים ללוגים/ייצור לוגים		הארגון יוודא כי מערך ניטור אבטחת המידע מנוטר ומתריע כאשר לא מתקבלים אירועים לאורך זמן ממערכת מידע המחוברת למערך הניטור. ניתן להגדיר כחוק והתרעה כאשר לא מתקבלים אירועים ממקור מידע במרבית מערכות הניטור ואיסוף הלוגים (SIEM ו-Log Management)	200%

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
תיעוד וניטור	21.10	יש להגדיר פעילויות רגישות אותן הארגון מעוניין לנטר.	מטרת הבקרה הינה לוודא כי הארגון הגדיר לעצמו את התרחישים אותם הוא רוצה לנטר וכי הוא מסוגל לקבל מידע זה	ניתן לבצע באמצעות פגישה עם הגורמים העסקיים לטובת הבנת תהליכי העבודה והתנהלות חריגה עבור איתור פעילות לא מורשית. ניתן להגדיר אירועים ותרחישים לניטור באמצעות פגישה עם מחלקת IT במטרה לזהות התנהגות חריגה ברשת כגון גישה לקבצים רגישים, ניסיונות הזדהות רבים שכשלו, העתקת קבצים רבים להתקן אחסון/תיקייה מקומית, התנהלות לא לגיטימית של ספק או עובד מיקור חוץ ועוד. לטובת מימוש ניטור אירועים אלו ניתן להיעזר הן במערכת SIEM והן בדו"חות מקומיים, פלטים ממערכות שונות, מצלמות, תשאול עובדים ועוד.	2
תיעוד וניטור	21.11	יש לסקור ולנתח תקופתית את רשומות הבקרה ולדווח את הממצאים לבעלי תפקידים מתאימים שהוגדרו	הארגון יפיק דוחות על אירועי אבטחת מידע וטרנדים וידווח על ממצאים להנהלה או לגורם המוגדר לכך	ניתן להפיק דוחות מרוכזים מכל מערכת ניטור אבטחת מידע כגון SIEM	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
תיעוד וניטור	21.12	הארגון יישם מנגנוני גילוי וחקירה אוטומטיים לזיהוי אירועים החשודים כאירועי סייבר ואיסוף ראיות, מתוך רשומות הניטור ומידע פורנזי	על מנת לאתר אירועים חשודים, יש להפיק התרעות ואינדיקציות מתוך נתוני הניטור והמידע הפורנזי הנאספים ממערכות הארגון. יש להתייחס לאירועים שהארגון הגדיר כחשודים, בהתאם למתאר האיומים הארגוני	ניתן ליישם באמצעות דוחות, שאילתות וחוקים או מנגנונים אנליטיים אוטומטים המיושמים על מאגר נתוני הניטור או במערכות ניטור ייעודיות כגון SIEM ומערכות פורנזיקה	2
תיעוד וניטור	21.13	מערכת הניטור תרכז רשומות בקרה ופורנזיקה ממקורות מידע שונים ותפעיל מנגנונים אנליטיים על מנת להשיג תמונת מצב ארגונית שלמה	הארגון יישם "מנוע קורלציה ואנליטיקה" שמטרתו שילוב נתונים ממקורות מידע שונים (מערכות שונות) באופן שמאפשר זיהוי אירועים רוחביים ותקיפות מתקדמות על מערכות הארגון	לדוגמה, שילוב נתונים ממערכות סיסטם ותקשורת, שילוב מידע ממערכות תשתית ומערכות אפליקטיביות, שילוב נתונים ממערכות בקרת גישה פיסית, סריקת פגיעויות והזנות ממקורות מודיעין סייבר.	4
תיעוד וניטור	21.14	יש להגן על רשומות הבקרה מפני גישה בלתי מורשית, שינוי או מחיקה	הארגון יאבטח את שטח האחסון וכן יקשיח את מערך הניטור כך שלא ניתן יהיה לשנות רשוומות לוג לאחר כתיבתן	ניתן ליישם על ידי הגבלת גישה למערך אחסון רשומות הניטור והגבלת הגישה לשרתים עצמם	2
תיעוד וניטור	21.15	יש לגבות את רשומות הבקרה על בסיס תקופתי ולשמרו בנפרד ממערך הניטור עצמו		הארגון יגדיר גיבוי שוטף הן של הגדרות מערך הניטור (גיבוי החוקים וקונפיגורציית מערכת הניטור) וגיבוי של הלוגים שנאספו	3
תיעוד וניטור	21.16	יש להשתמש במנגנונים קריפטוגרפים על מנת להגן על שלמות רשומות וכלי הבקרה	מערך הניטור יחתום באמצעות מנגנוני חתימות דיגיטליות ו-Hashing של קבצי הלוג שנאספו על מנת לוודא שלא בוצעו שינויים בקבצים אלו	מרבית מערכות ה-SIEM והפורנזיקה תומכות בפונקציונליות זו - יש לוודא את הפעלתה התקינה	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
תיעוד וניטור	21.17	יש לוודא שניתן לאחזר רשומות בקרה ופורנזיקה, ותוצאות אנליטיקה, שנשמרו לטווח ארוך	הארגון יוודא מדי תקופה כי ניתן לאחזר ו/או לחפש רשומות מתקופה איחסון ארוכה ככל הניתן	ניתן להוציא דוח על אירועים מהקמת המערכת לדוגמה על מנת לוודא כי אכן אירועים אלו קיימים במערכת הניטור	4
תיעוד וניטור	21.18	יש ליישם מנגנון להקלטה ומעקב של פעילות המשתמשים (User Session) במערכות המידע	יש להגדיר את מנגנון ההקלטה וכן את כללי השימוש במנגנון זה לרבות המקרים בהם יש להקליט, כללי זהירות בנושא פרטיות משתמשים בהקשר זה והרשאות הגישה למערכת ההקלטה	ניתן ליישם מנגנון הקלטה באמצעות הפעלת מערכת על תחנות המשתמשים, התקנה על שרתי טרמינל או שרתי אפליקציה	4
תיעוד וניטור	21.19	יש ליישם מנגנונים המזהים ומתריעים בזמן אמת בפני נסיונות התקפה	מנגנוני התרעה יזהו ויתריעו בשל חשד להתקפה. מנגנונים אלו ייושמו על ומסביב למערכות המידע ומערכות התשתית של הארגון.	ניתן ליישם באמצעות הגדרת חוקים המערך ה-SIEM אשר יתריעו על אירועי מתקפה ואירועי אבט"מ, כמו כן ניתן להפעיל צוות אנליטים (SOC) אשר ינתחו את האירועים	3
תיעוד וניטור	21.20	יש לנטר תעבורת תקשורת יוצאת ונכנסת לזיהוי פעילות בלתי שגרתית או בלתי מורשית		ניתן ליישם על ידי חיבור חומת האש הארגונית, ה-IPS ולבצע קורלציה מול Feeds חיצוניים על מנת לזהות תקשורת לשרתים חשודים	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
תיעוד וניטור	21.21	יש להטמיע אמצעי ניטור ספציפיים על פעילות משתמשים אשר מהווים רמת סיכון גבוהה (למשל, משתמשים בעלי רמת הרשאות גבוהה)	הארגון יאפיין פונקציות ארגוניות רגישות ויוודא כי חלים עליהן חוקי ניטור פרטניים בהתייחס לפעולות רגישות במערכות הארגון	ניתן להשוות הן מול קבוצה של משתמשים רגישים בתוך הActive Directory או לחלופין להנפיק רשימה ידנית של משתמשים אלו ולטעון אותה למערך ה SIEM. לדוגמה ניתן לייצר התראה על כל יצירת משתמש ADMIN חדש בתוך ה-DC	3
22. סקרי הערכת בקרות אבטחה: סקרי הערכת בקרות האבטחה נועדו לבחון את מימוש הבקרות בפועל על-פי תורת הגנה זו וכן לבחון את אפקטיביות ההגנה. רצוי לבחון את העמידה בבקרות הנדרשות על-ידי גורם עצמאי בארגון או גורם חיצוני. את העמידה באפקטיביות ניתן לבחון על-ידי מבדקי חדירות, בחינת פגיעויות, Red Teams וכד'. הבקרות נדרשות לבחון באופן תקופתי, כי מערכות הגנת הסייבר הקיימות בארגון אכן מוגדרות כראוי ומעודכנות בהתאם לשינויים שחלו בארגון ובאיומי הסייבר האפשריים.					
סקרי הערכת בקרות אבטחה	22.1	מדיניות - יש לכתוב ולייסם מדיניות לניהול פגיעויות וחשיפות אבטחת מידע, וכן לבקר ולעדכן אותה תקופתית	הארגון יגדיר מדיניות בנושא ניהול חשיפות בארגון הכולל: זיהוי פגיעויות וחשיפות והערכתן, תיקון החשיפות והפגיעויות, אחריות לביצוע המשימות ומעקב שוטף		2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
סקרי הערכת בקרות אבטחה	22.2	נוהל - יש לכתוב תכנית לניהול פגיעיות וחשיפות אבטחת מידע הכוללת את תהליך ההערכה ותיקון הליקויים שנתגלו	הארגון יכתוב תיק נהלים ותכנית ליישום ותפעול מערך ניהול הפגיעויות בדגש על הטמעת מערכות לזיהוי, הפעלת כלים וסוקרים, הפעלת ספקי משנה ועובדים לטיפול בממצאים. כמו כן יש לכלול בתכנית ניהול הפגיעויות וחשיפות האבטחה אחת או יותר מהבדיקות הבאות: סריקת פגיעויות, בדיקת משתמש זדוני, הערכת איום פנימי ובדיקות ספציפיות אחרות שיוגדרו ע"י הארגון	תכנית הערכת אבטחת מידע וניהול הפגיעויות תכלול מגוון נהלים ותהליכים אשר נועדו לתפעול מערך זיהוי הפגיעויות, מעקב שוטף אחר תהליכים ומנגנונים לתיקון הליקויים, ממשקים לתהליכים מקבילים (ניהול עדכוני אבטחת מידע, ניהול תצורת מערכות אבטחת מידע, פיתוח מאובטח וכו') כמו כן יש לשלב בתכנית שימוש במערכות לסריקת פגיעויות, ביצוע של מבדקי חדירה אשר מדמים משתמש ארגוני פנימי ו/או תוקף חיצוני, וכן מערכות לסקירת תצורה וכו'	2
סקרי הערכת בקרות אבטחה	22.3	יש לבצע מבדקי חדירות למערכות על בסיס תקופתי	הארגון יבצע מבדקי חדירה תשתיתיים ואפליקטיביים למערכות הארגון (בין אם הן פנימיות או חיצוניות אבל מנוהלות על ידו) אחת לתקופה.	הארגונים הפיננסיים לדוגמה מנהלים תכנית לביצוע מבדקי חדירה על כלל מערכות הארגון ברמה שנתית ואף רב-שנתית כך שניתן לבצע מעקב שוטף אחר הממצאים ותיקונם.	3
סקרי הערכת בקרות אבטחה	22.4	יש למנות גורם עצמאי/ בלתי-תלוי לביצוע מבדקי החדירות	הארגון יעסיק בודקי אבט"מ חיצוניים (לביצוע מבדקי חדירה)	ניתן לפעמים לבצע את המבדקים על ידי צוות פנימי אשר אינו כפוף למערכות המידע אלא לגוף אבטחת המידע, כך שאינו אחראי לתיקון הליקויים עצמם.	4

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
סקרי הערכת בקרות אבטחה	22.5	על הארגון להפעיל קבוצה עצמאית לביצוע מבדקי חדירה, ולהפעיל תרגילי Red Team על מנת לדמות ניסיונות של תוקפים לסכן את הנכס	הארגון יעסיק קבוצת בודקי אבט"מ חיצוניים אשר ידמו ניסיונות פגיעה בנכסים על מנת לבחון הן את הבקרות והן את יכול התגובה של הארגון.	ניתן לבחון על ידי בקרה זו את יכולת התגובה של צוותי הניטור והן את יכולת אנשי התשתיות ואבטחת המידע לחסום מתקפות שזוהו בזמן אמת.	4
סקרי הערכת בקרות אבטחה	22.6	יש לבצע סריקת פגיעויות באופן שוטף ובהתאם לתהליך ניהול הפגיעויות הארגוני, באמצעות כלי יעודי למטרה זו על מערכות המידע של הארגון (פנימיות וחיצוניות)		ניתן לממש באמצעות התקנה של כלי לסריקת פגיעויות ותזמון סריקות אחת למספר שבועות, חודש, או מספר חודשים (ניתן גם להגדיר תזמון שונה לכל סביבה)	2
סקרי הערכת בקרות אבטחה	22.7	יש לוודא כי כלי סריקת הפגיעויות מעודכן באופן שוטף ומכיל את הפגיעויות החדשות אשר מתגלות ומדווחות	יש לוודא שכלי הסריקה בעל יכולת עדכון שוטף, בעל רשיון בתוקף (על מנת לקבל עדכונים לגבי פגיעויות חדשות) וכן אכן מתבצע עדכון של הפגיעויות שהכלי מסוגל לזהות.	ניתן לוודא לפי תאריכי עדכון של הפגיעויות ולוודא שישנה תקשורת לאתר העדכונים של ספק המערכת (או שקיים אתר מראה פנימי לעדכונים)	2
סקרי הערכת בקרות אבטחה	22.8	על הארגון לתקף את החולשות והפגיעויות שזוהו על ידי המערכת האוטומטית באמצעות תהליך פנימי אשר כולל סקירה של הימצאות החולשות והפגיעויות שזוהו במערכות נוספות	הארגון יגדיר תהליך תיקוף אשר מתייחס לכל הפחות לחולשות ולפגיעויות קריטיות וגבוהות שזוהו ומוודא בדיקה באופן ידני או באופן ממוכן הימצאות של החולשות והפגיעויות במערכות נוספות	לדוגמה במידה ונמצאה פגיעות קריטית במערכת הפעלה של חלונות או בבסיס הנתונים של המערכת, ניתן לבצע סקירה של השרתים הלא מעודכנים אשר מריצים את אותה גרסה	4

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
סקרי הערכת בקרות אבטחה	22.9	יש לבצע סריקות עם משתמש מערכת (Credentialed Scan) בכלי סריקת הפגיעויות	הארגון יגדיר משתמש מערכת לכלי סריקת הפגיעויות אשר יאפשר התחברות למערכת עצמה וסריקה של התהליכים והעדכונים המותקנים עליה. כאשר המטרה לזהות גם חולשות בהגדרות ההקשחה של המערכת הנבדקת	מרבית כלי סריקת הפגיעויות הקיימים בשוק מכילים מצב סריקה Credentialed Scan	4
סקרי הערכת בקרות אבטחה	22.10	יש לוודא כי קיים כלי אוטומטי המשווה בין תוצאות סריקת הפגיעויות בעבר לתוצאות נוכחיות לטובת בקרה וניתוח מגמות	הארגון ינהל מעקב אוטומטי על מצב הפגיעויות שזוהו לאורך תקופה על מנת לזהות מערכות אשר מהוות סיכון באופן חריג או לחלופין מערכות שיישום הבקרות בהן אינו מספק.	ניתן לממש הן באמצעות כלי הסריקה עצמם והן על ידי ממשק למערכות צד ג' (כדוגמת SIEM)	4
סקרי הערכת בקרות אבטחה	22.11	יש לוודא כי קיימת התאמה בין תוצאות כלי ניהול פגיעויות שונים אשר מוטמעים בארגון לצורך קבלת תמונת מצב שלמה על מגוון הפגיעויות במערכת	יש לוודא כי מגוון כלי סריקת הפגיעויות ו/או כלי הניטור מחוברים למערך מרכזי על מנת לקבל תמונת מצב אחידה של מצב הפגיעויות והבקרות.	ניתן לבצע על ידי ממשוק כלי ה Vulnerability Scanning, כלי ה Patch Management לממשק מרכזי כגון ה SIEM או מערכת Data Analytics\BI על מנת להוציא דו"ח מרכז ואחיד של מצב הפגיעויות.	4
סקרי הערכת בקרות אבטחה	22.12	יש להטמיע מנגנון אוטומטי לניהול מרוכז של תהליך תיקון הליקויים	הארגון יטמיע מערכת מרכזית לניהול החשיפות שזוהו ומאמצי התיקון.	ניתן לממש על ידי הקמת ממשקים בין מערך ניהול החשיפות לבין מערכת הקריאות הארגונית או לחלופין להשתמש במערכת ייעודית לצורך זה (כלי GRC)	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
סקרי הערכת בקרות אבטחה	22.13	יש לבקר את תהליך תיקון הפגיעויות ולהחיל יעדים ברי מדידה לתיקון הפגיעויות לפי רמת חומרתן	הארגון יגדיר יעדים SLA לטיפול בחשיפות לפי רמת חומרתן. בנוסף יש להגדיר התראות לגבי סטייה מלוחות הזמנים של תיקון החשיפות לפי המדדים והיעדים שהוגדרו (SLA)	לדוגמה חשיפות קריטיות יתוקנו בתוך מספר ימים, חשיפות ברמה גבוהה בתווך של עד חודש, בינוני עד שלושה חודשים וכו'. בנוסף יש לממש התראות SLA לקריאות הנפתחות ממערך ניהול הפגיעויות והוצאת דוחות על חריגות מיעדים אלו.	3
23. הגנת סייבר פרואקטיבית: בקרות סייבר פרואקטיביות מאפשרות לארגון להתגונן מפני תקיפות באופן שמשתנה עם השתנות התקיפה. במסגרת זו הארגון יאסוף מידע עדכני לגבי איומי הסייבר שלו ודרכי התמודדות מולם ומידע הנוגע לנוכחותו הדיגיטלית ויתרגם אותם לבקרות יישומיות אד-הוק. בנוסף, הארגון יישם מערך "שיטוי והטעיה" של תוקפים פוטנציאליים (כגון מלכודות דבש, או טכנולוגיות שיטוי והטעיה נוספות) על-מנת לבלבל את התוקף, להקטין את המוטיבציה שלו לתקיפה, לגלותו במהירות במידה שחדר לארגון ועוד. הארגון יטמיע בקרות המבוססות על ניתוח דפוסי התנהגות (מערכת ומשתמש) בסביבות רגישות.					
הגנת סייבר פרואקטיבית	23.1	הארגון יגדיר תכנית בנושא הגנת סייבר פרואקטיבית ויעדכן אותה תקופתית	תכנית הגנת סייבר פרואקטיבית תעסוק בזיהוי איומים חדשים, התאמת הבקרות לאיומים שזוהו, אחריות לאיסוף מידע מודיעיני ואחר, סקירת בקרות חדשות ועוד.		3
הגנת סייבר פרואקטיבית	23.2	הארגון יאסוף מידע עדכני לגבי איומי סייבר ודרכי התמודדות מולם	הארגון ילמד ממקורות מידע פומביים לגבי איומי סייבר חדשים הנוגעים לעסקי הארגון ולטכנולוגיות המיושמות בו והשפעותיהם עליו.	ניתן ללמוד ממידע המפורסם במקורות מידע מקצועיים גלויים כגון: metasploit, אתרי חברות אבטחה אשר מפרסמות פגיעויות, חולשות וכו' וכן להתקשר עם חברות מתמחות המספקות שירותי מודיעין מסוג זה.	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
הגנת סייבר פרואקטיבית	23.3	הארגון יאסוף מידע הנוגע לנוכחותו הדיגיטלית (פעילות עסקית, מידע אודות לקוחות, מידע לגבי משתמשים פנימיים)	מטרתו של איסוף המידע היא לזהות מקרים של חשיפת מידע רגיש של הארגון ברשת האינטרנט לרבות ב"רשת האפלה".	ניתן להשתמש בשירותים של חברות המתמחות בכך.	3
הגנת סייבר פרואקטיבית	23.4	הארגון יפרוט את המידע לגבי איומי הסייבר לבקרות יישומיות או לטובת טיוב בקרות קיימות	הארגון ימפה את השינויים הנדרשים להגדרות מערכות אבטחת המידע וכן הבקרות התשתיותיות והאפליקטיביות של הארגון על מנת להתמודד עם איומים חדשים.	שינויים יכולים להיות בהגדרת רשתות, חומות אש, מערכות וממשקים אפליקטיביים, ועוד. יש לעדכן את נהלי המערכות בהתאם לאחר עדכון ההגדרות.	3
הגנת סייבר פרואקטיבית	23.5	הארגון יישם מערך "שיטוי והטעיה" של תוקפים פטנציאליים	הארגון יטמיע מערכות טכנולוגיות אשר מטרתן היא לבלבל ולעכב תוקף פוטנציאלי על מנת לשפר את יכולות הזיהוי וההתמודדות עם האיומים.	מערכות כגון Honeypots, שרתים וירטואליים ייעודיים מנוטרים, חתימת קבצים ועוד. ניתן לממש במספר רב של דרכים כגון הגדרת משתמשים פיקטייביים, אובייקטים בתוך ה DC אשר מטרתם היא למשוך את התוקף, הטמנת קבצים בעלי שמות ומאפיינים "חמידים" כגון "סיסמאות"/"משכורות"/ חסוי וכו'	3
הגנת סייבר פרואקטיבית	23.6	הארגון יטמיע בקרות המבוססות על ניתוח דפוסי התנהגות (מערכת ומשתמש) בסביבות רגישות	הארגון יטמיע מערכות לזיהוי אנומליות הן ברמת השרת והן ברמת הרשת בסביבת שירותים ומידע רגיש.	מערכות מסוג זה יכולות להיות הן מערכות ברמת השרת וכן ברמת הרשת.	3

תגובה Respond

<table>
<tr><th>משפחה</th><th>זיהוי</th><th>הבקרה</th><th>הסבר משלים</th><th>דוגמה לישום הבקרה</th><th>רמת בקרה</th></tr>
<tr><td colspan="6">24. ניהול אירועים ודיווח:
על הארגון להיות מסוגל לנהל אירוע סייבר שמתרחש בצורה שתאפשר מזעור הפגיעה, נטרול האיום וחזרה לשגרה באופן המיטבי. זאת לצד תחקור האירוע, הפקת מסקנות ולקחים וביצוע התאמות במערך ההגנה בהתאם. בקרות אלו נועדו לתכלית זו. במסגרת זו, הארגון יגדיר את תהליכי הטיפול שלו באירוע סייבר, את ערוצי הדיווח לעובדים על חשד לאירועי אבטחה, יגדיר את הגורם המקצועי (בתוך הארגון או מחוצה לו), שתפקידו לספק ידע מקצועי, תמיכה וליווי בנושאי ניטור, זיהוי, חקירה ותגובה לאירועי סייבר, הגדרת דיווחים במהלך התרחשות אירוע הסייבר ובסיומו (למשל ל-CERT הלאומי ולרגולטור) ועוד. יש לבדוק את יכולת התגובה לאירועים על בסיס תקופתי תוך שימוש במבדקים שיגדיר הארגון.</td></tr>
</table>

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
ניהול אירועים ודיווח	24.1	יש לכתוב וליישם מדיניות תגובה לאירועים, לבקר ולעדכן אותה תקופתית	הארגון יכתוב ויישם מדיניות תגובה לאירועי אבטחת מידע כחלק ממדיניות אבט"מ הארגוני, הארגון יבדוק וירענן את התכנית אחת לתקופה	בכתיבת מידיניות טיפול באירועים יש להגדיר בעלי תפקידים וצוותי תגובה, רמות חומרה של אירועים וכן דרכי תקשורת עם רשויות במידת הצורך (משטרת ישראל, רמו"ט, מערך הסייבר הלאומי, רגולטור ישיר וכו'). התכנית תגדיר מי מנהל את האירוע במידה והוא מתרחש (ניתן להגדיר כי במקרים שונים בעלי תפקיד שונים לוקחים את האחריות לניהול האירוע כגון הבדל בין ניהול ארוע של בקשת כופר לשחרור מחשבים ארגוניים לבין איום לפרסום נתוני לקוחות רגישים החוצה). חשוב כי המדיניות תיכתב בשיתוף עם גורמי צד ג' שרלוונטיים לארגון כגון רגולטור, ספקים בדגש על מערכות שבענן, עובדי מיקור חוץ וכו'. מומלץ כי המדיניות תגדיר מתי פותחים חדר מצב, עבור אילו אירועים נדרש לערב את ההנהלה וכיצד, תדירות דיווח, פניה ל-CERT/מערך הסייבר הלאומי, הכרזה על חזרה לשגרת עבודה וכו'	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
ניהול אירועים ודיווח	24.2	יש לפתח תכנית לטיפולי באירועי סייבר ואבטחת מידע	הארגון יכתוב תכנית לזיהוי, טיפול ותגובה לאירועי סייבר ואבטחת מידע אשר כוללת: מתווה למימוש יכולת תגובה לאירועי אבטחה, הסבר-על כיצד יכולות הארגון מתאימות לטיפול באירועים, מענה לדרישות הארגון בהתחשב במשימותיו וגודלו, תגדיר תקריות אשר נדרשות בדיווח, תספק אמצעי מדידה ליכולת הארגון להגיב לאירועים ותגדיר את המשאבים ותמיכת ההנהלה הנדרשת לתחזוקה ושיפור יכולת התגובה לאירועי אבטחה	ניתן ליישום באמצעות מיפוי התהליכים הארגוניים והגופים בארגון שיהוו צוותי תוגבה, בהתבססות על יכולותיהם, התממשקות עם הצוותים שמתחזקים את מערכות הניטור הארגוניות על מנת לוודא שניתן לתרגל ולבדוק אירועים	2
ניהול אירועים ודיווח	24.3	יש לפתח יכולת לטיפול באירועי סייבר ואבטחת מידע אשר כוללת הכנה, זיהוי וניתוח, בלימה והתאוששות	מטרת הבקרה הינה לחזיק בידע והכלים הנדרשים מארגון לטובת תחקור אירוע, הכלתו, ניהולו בצורה יעילה והתמודדות עם ההשלכות שלו.	ניתן ליישם באמצעות יישום התכנית לטיפול באירועי אבטחת מידע בדגש על גיוס אנשי מקצוע אשר יהוו את הבסיס למוקד זיהוי האירועים והתגובה, הכשרת הצוות לטיפול באירועים מסוגים שונים (כגון התפשטות וירוס, כופרה, התמודדות עם DDOS, התמודדות עם מידע שדלף מחוץ לארגון וכו'). ניתן לממש באמצעות שימוש בכלי חקירה או באמצעות התקשרות מול צוותי "ניהול אירועים" (ERT).	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
ניהול אירועים ודיווח	24.4	יש להטמיע מנגנונים ממוחשבים לתמיכה בתהליך הטיפול באירועים	ניהול אפקטיבי של אירועים וחשד לאירועים (התראות) רבים במקביל הינו תהליך מורכב. לטובת מעקב אחר סטטוס ההתראות, הפעולות הנדרשות לביצוע, מעקב אחר החלטות וכו נדרש למכן את החלקים שניתן בתהליך ניהול האירועים.	ניתן לממש באמצעות חיבור מערכות השו"ב למערכות ניטור וזיהוי האירועים, כמו כן ניתן להגדיר מראש שנהלי התגובה ישולבו בתוך קריאות השו"ב. ניתן גם למימוש באמצעות מערכות תומכות החלטה, מערכות ניהול Work Fllow או מערכת ניהול קריאות (Ticketing). מומלץ כי הכלים יסייעו לארגון לאתר אירועים אשר פתוחים זמן רב, אירועים חמורים אשר הטיפול בהם איננו "מתקדם" ומצבים אשר דורשים התערבות מיידית.	3
ניהול אירועים ודיווח	24.5	יש לתעד אירועי אבטחת מידע, את תהליכי הטיפול באירוע לרבות איסוף מידע, פעולות שבוצעו ומסקנות	הארגון ינהל דיווח מרוכז וכן ניהול אירועים מרוכז לטובת קבלת תמונה אחידה ומלאה לגבי אופי האירועי והערכת הסיכונים	ניתן לממש בצורה מרוכזת תחת מוקד ניטור אבט"מ (SOC) אשר יאסוף, יתעד וירכז את המידע המוזן מהם	2
ניהול אירועים ודיווח	24.6	יש להגדיר ערוצי דיווח לעובדים לצורך דווח על חשד לאירועי אבטחה לגורמים הממונים	הארגון יכיל נהלים המחייבים דיווח ואת אופן הדיווח לגבי אירוע המוגדר כארוע סייבר	ניתן לממש גם באמצעות ההדרכות אשר יסבירו לעובדים מהם אירועי אבטחת מידע וכיצד לדווח עליהם. מומלץ לפנות אל ה - CERT הלאומי לטובת קבלת סיוע תגובה והתאוששות.	1

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
ניהול אירועים ודיווח	24.7	יש להגדיר גורם שתפקידו לספק ידע מקצועי, תמיכה וכן ליווי מקצועי בנושאי ניטור, זיהוי, חקירה ותגובה לאירועי אבט"מ	הארגון יגדיר גורם מקצועי שתפקידו להוות מקור ידע מקצועי לזיהוי וחקירה של אירועי אבט"מ	הגורם יכול להיות גורם פנימי או לחלופין גורם חיצוני בעל נסיון בזיהוי, חקירה ותגובה לאירועים, הגורם ינחה ויתדרך את הצוותים המתפעלים את האירועים, יהווה מקור ידע מנסיונו בנושא אירועי סייבר ואבט"מ ותגובה לאירועים מסוג זה	3
ניהול אירועים ודיווח	24.8	יש להטמיע מנגנון אשר מנגיש מידע לגבי תגובה וטיפול בארועי סייבר ואבטחת מידע	הארגון ינגיש תיק נהלים אשר מכילה את נהלי הזיהוי והתגובה לאירועי סייבר ואבטחת מידע	ניתן לממש סעיף באמצעות כל מערכת לניהול ידע או מערכת לניהול מסמכים או בעותק מודפס	2
ניהול אירועים ודיווח	24.9	יש לבצע הדרכות בנושא תגובה לאירועי אבטחה לבעלי תפקידים רלוונטיים	הארגון יבצע הדרכות בנושא זיהוי ותגובה לאירועי אבט"מ לכל הגורמים אשר אמונים על תפעול ארועים אלה. יש לרענן הדרכות אלו אחת לתקופה	ניתן לבנות את תיק ההדרכות כך שיכילו את נהלי התגובה, וכן את Best Practice הכלים בהם הארגון משתמש על מנת להנגיש את המידע הנ"ל בזמן אירוע אמיתי	2
ניהול אירועים ודיווח	24.10	יש לשלב סימולציות לאירועים במסגרת ההדרכות על מנת לשפר את אפקטיביות התגובה של הצוות במצבי משבר	הארגון ידמה תרחישים של אירוע אבט"מ על מנת לבחון את מוכנותו ולהיערך בהתאם	חלק מהסימולציות ניתן לבצע בתור "תרגול יבש" אשר ידמה ארוע מונחה ותגובת הצוותים תמדד על ידי בקר התרגיל וחלק מהסימולציות ידמו אירועים בסביבות חיות עם אמצעים אמיתיים כגון שירות תרגול phising	3

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה ליישום הבקרה	רמת בקרה
ניהול אירועים ודיווח	24.11	יש ליישם מנגנונים אוטומטיים על מנת לספק סביבת הדרכות מעמיקה ומציאותית יותר	הארגון ידמה התנהגות של ארוע אבט"מ תוך דגש על שימוש בסביבות המדמות את הסביבה הארגונית	ניתן לדמות מקרים בסביבות סגורות (סביבת בדיקות) או במעבדות חיצוניות ייעודיות (כדוגמת מעבדת סייבר מקצועית)	4
ניהול אירועים ודיווח	24.12	יש לבדוק את יכולת התגובה לאירועים על בסיס תקופתי תוך שימוש במבדקים שיגדיר הארגון, ובכלל זאת באמצעות סימולציה של אירוע אמת, על מנת לקבוע אפקטיביות. יש לתעד את תוצאות הבדיקה התקופתית	הארגון ידמה מתקפות אמיתיות, בין היתר באמצעות כלי תקיפה אוטומטיים, לטובת מדידת יכולת התגובה לאירועי אבט"מ. הארגון יתעד ויפיק לקחים מתרגילים המבוצעים לצורך זיהוי ובקרה, הארגון יפיק דו"ח תחקיר ארוע בסיום התרגיל	ניתן למדוד באמצעות הכנת תסריט האירוע ומדידה של כמות הארועים שזוהו וכן מדידת איכות התגובה (מזעור הנזקים לארגון, תקשורת בין גורמים, ריכוז והפעלה, חזרה לשגרה) ניתן לשלב את זיהוי הארועים עם אמצעים כגון מבדק חדירה אמיתי המבוצע על האגון. חלק מהבדיקה תהיה על ידי שימוש בכלי תקיפה אמיתיים.	3

התאוששות Recover

25. המשכיות עסקית:

מטרתו של ארגון לקיים המשכיות עסקית ולמזער את הנזק הנגרם לו בהתרחש אירוע סייבר משמעותי. בקרות ההמשכיות העסקית נועדו לצורך כך. על הארגון לוודא יכולת שחזור מהירה של תשתיות הסייבר של הארגון לרמה נאותה, עליו להיערך מבחינת תשתיות חלופיות באם נדרשות (כולל זמינות ויתירות), לבדוק את תכנית ההמשכיות העסקית באופן עתי ואף לתרגל אותה. הנושא של גיבויים אפקטיביים, אמינים וזמינים קריטי לתהליך המשכיות עסקית יעיל ונדרש לתרגל אותו באופן שוטף.

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
המשכיות עסקית	25.1	יש לכתוב וליישם מדיניות המשכיות עסקית, בהיבטי הגנת סייבר, לבקר ולעדכן אותה תקופתית	הארגון יכתוב ויישם תכנית המשכיות עסקית אשר נגזרת מיעדי הארגון ומיישמת בקרות ותהליכים על מנת לעמוד ביעדים אשר הוגדרו. התכנית תתחשב בתרחישי האסון השונים ובתהליכים הקריטיים למימוש יעדי הארגון. הארגון יגדיר אילו נכסים תומכים בפעילות של משימות ופונקציות עסקיות קריטיות (פיזיים ודיגיטליים). הארגון יגדיר את פרק הזמן המקסימלי הנסבל להשבתה של שירותים חיוניים בטרם החזרתם לפעילות תקינה (במתכונת חירום). הארגון יגדיר במסגרת תכנית ההמשכיות את פרק הזמן שבו משימות חיוניות יחזרו לפעילות, מרגע הפעלת התכנית	הארגון יכתוב ויישם מדיניות המשכיות עסקית, יש לעדכן מדיניות זו באופן תקופתי. מדיניות זו תגדיר כיצד הארגון מתנהל בשוטף ובחירום במטרה להבטיח את ההמשכיות העסקית (כולל הגדרת מדדים מקובלים כגון RTO) במידה ומתרחש אירוע במרחב הסייבר. ניתן להיעזר בכתיבת המדיניות בחומרי עזר כגון בתקן ISO 22301 , המכילים כלי עזר לניהול ההמשכיות העסקית בארגון.	2
המשכיות עסקית	25.2	יש לבצע תכנון קיבולת הנחוצה לפעילות למקרה אסון (לדוג' כח עיבוד, תקשורת, שירותי תמיכה)	הארגון יוודא כי המערכות והתשתיות המיועדות להמשכיות הפעילות במצבי אסון תומכות בקיבולת הנחוצה להיקפים ולפרקי הזמן הנדרשים.	ניתן ליישם לאחר מיפוי השירותים הקריטיים וכן לאחר הגדרת יעדי ההתאוששות והשרידות לכל שירות, הארגון בד"כ מבצע מדידה של הקיבולת הנדרשת באתר החלופי מבחינת תשתיות תקשורת, תשתיות סיסטם וכן אפליקציות כולל רישוי מתאים.	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
המשכיות עסקית	25.3	יש לבצע הדרכה לעובדים בנושא המשכיות עסקית	הארגון יבצע הדרכות לעובדים בהתייחס לנהלי ההמשכיות העסקית	בתוך כך יש להתייחס לתפקידם של העובדים במערך ההתאוששות, מקומות התכנסות זמניים, לוגיסטיקה, הפעלה וכן יעדי ההתאוששות עצמם ברמת כל צוות והארגון	2
המשכיות עסקית	25.4	יש לבצע תרגול של תכנית ההמשכיות העסקית באופן תקופתי	הארגון יתכנן ויבצע תרגילי מוכנות לשם בדיקת אפקטיביות תכנית ההמשכיות העסקית	ניתן ליישם באמצעות "תרגיל יבש" המכיל מספר תרחשים ובכך לבדוק את מוכנות העובדים. מומלץ כי התרגול יכלול הן את היבטי ה IT של תכנית ההמשכיות העסקית כגון רצף עבודה של טלפוניה ותקשורת מחשבים והן צדדים משלימים כגון עמידת ספקים חיצוניים ושירותים (בענן ומקומיים) בהנחיות תכנית ה BCP. כמו כן חשוב לוודא כי הארגון מבצע מהלכים של העלאת מודעות בחירום כגון בחינת נחיצות ודחיפות העברת גרסאות לסביבת הייצור, הקפדה על ליווי אורחים, ניסיונות לשחזור קבצים, תרגול ניהול אירוע סייבר וקבלת החלטות של ההנהלה כולל תחקור והפקת לקחים ועוד	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
המשכיות עסקית	25.5	יש לבצע תרגול של תכנית ההמשכיות העסקית באמצעות סימולציה של הפעלת התכנית, באופן תקופתי	הארגון ישתמש בסימולציות והפעלת העובדים המעורבים ביישום התכנית לבדיקת מערך ההתאוששות	על מנת לבצע סימולציה הקרובה למציאות ככל האפשר ("תרגיל רטוב"), יש להכין תסריטים של תרחישי אסון, להפעיל את התכנית (במתכונת מצומצמת) בסביבת האמת (סביבת DR) ולבחון את תפקוד התכנית	3
המשכיות עסקית	25.6	יש לבדוק את תכנית ההמשכיות על בסיס תקופתי ולתקן פערים שהתגלו	הארגון יבקר ויתקן את תכנית ההמשכיות העסקית באופן תקופתי	לדוגמה: תכנית בדיקות המבצעת הפעלה חלקית של מעבר לסביבת החירום באופן תקופתי ולמערכות שונות במטרה לוודא את תקינות תהליכי המעבר	2
המשכיות עסקית	25.7	יש לבדוק את תכנית ההמשכיות באתר החלופי, על מנת שצוות ההמשכיות יכיר את מתקן ומשאבי האתר החלופי וכדי להעריך את יכולת האתר החלופי לתמוך בפעילויות הדורשות המשכיות	הארגון יכין נהלים ותהליכים לתרגול והכרת אתר הגיבוי כחלק מתרגול ההמשכיות העסקית	ניתן לבצע באמצעות סיורים לאתר הגיבוי, ריענון הידע לגבי המערכות המאוחסנות בו והפעלת המעבר לאתר המשני	2
המשכיות עסקית	25.8	יש להשתמש בכלים אוטומטיים כדי לבדוק באופן מעמיק ואפקטיבי את תכנית ההמשכיות	הארגון ישתמש בכלים אוטומטיים אשר יאפשרו בקרה ובדיקה של אפקטיביות התכנית	דוגמה לכלים כאלה היא בקרה של מערך הגיבויים והתראות על גיבויים שכשלו, בקרה על תצורות שרידות (HA) בין האתר הראשי למשני, ניטור של קווי התקשורת בין האתרים ועוד	4

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
המשכיות עסקית	25.9	יש לבצע שחזור מלא של המערכת למצב מוכר כחלק מבדיקת תכנית ההמשכיות	הארגון יבצע נסיון שחזור מלא עבור המערכות אשר הוגדרו חלק מתכנית ה -DR מגיבוי אחת לתקופה	לדוגמה: ביצוע שחזור מלא של מערכת לסביבת הגיבוי; לאחר סיום פעולת השחזור יש לבצע בדיקות קבלה במטרה לוודא כי המערכות מתפקדות, הכוללות: השוואת נתונים, בדיקת תצורה ונסיון עבודה מול המערכות המשוחזרות	3
המשכיות עסקית	25.10	יש להקים אתר אחסון ועיבוד חלופי אשר יאפשר גיבוי ושחזור מידע, ויהיה באותה רמת אבטחה כמו האתר הראשי	הארגון יקים ויחזיק אתר משני אשר יכיל עותקים של מערכות, מערכות אבט"מ, ואחסון אשר יתמכו בהתאוששות והמשכיות עסקית של תהליכים קריטיים	ניתן ליישם באמצעים כגון שכפול שרתים, סביבות שרידות באמצעות הכפלה של השרתים והצבתם באתר המרוחק, טכנולוגיות ווירטואליזציה ועוד.	2
המשכיות עסקית	25.11	יש לוודא שאתר האחסון החלופי מופרד מהאתר הראשי (באופן פיזי ולוגי) על מנת לצמצם את הסיכון לפגיעה בו-זמנית בשני האתרים		הארגון יוודא מרחק פיזי נאות בין האתר הראשי לאתר הגיבוי וכן הפרדה מספקת של רשתות מחשבים ותשתיות תומכות	2
המשכיות עסקית	25.12	יש להגדיר את את אתר האחסון החלופי באופן שיאפשר עמידה ביעדי תכנית השחזור	הארגון יגדיר את המערכות וקווי התקשורת באתר המשני כך שניתן יהיה לבצע התאוששות מהירה ואפקטיבית	ניתן ליישם בקרה זו באמצעות מערכות התומכות בשרידות (High Availability) בתצורות שונות המאפשרות שכפול של מידע באופן מהיר ואף זמינות של שירותי חזרה מגיבוי אשר פועלים באתר המשני	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
המשכיות עסקית	25.13	יש לזהות בעיות נגישות פוטנציאליות לאתר האחסון החלופי במקרה של אסון אזורי, ולנקוט בפעולות מנע מתאימות	הארגון יוודא כי אתר הגיבוי נגיש במקרה של אסון	מומלץ לוודא כי קיימות מספר דרכי גישה, כי אתר הגיבוי נמצא במבנה עמיד לרעידות אדמה וכי ישנה דרך לתפעל את האתר מרחוק במידת הצורך במלי להגיע פיזית	2
המשכיות עסקית	25.14	יש להכין הסכמים לתשתית אתר חלופי אשר מכילים סעיפי "עדיפות שירות" (priority-of-service) בהתאם ליעדי ההתאוששות של הארגון	הארגון יוודא כי בהסכמי השירות שלו מול ספק אתר הגיבוי יהיו סעיפים המחייבים את הספק לזמני שירות ותגובה התואמים את יעדי הארגון	ניתן לוודא כי בהסכמי השירות (SLA) אל מול ספק אתר הגיבוי זמני התגובה של אנשי הסיסטם והזמן לטיפול בתקלות לא פוגעים ב-RTO של השירות, כמו כן לדרוש עדיפות מהספק בהתאוששות של שירותים קריטיים	2
המשכיות עסקית	25.15	יש לוודא מוכנות של אתר העיבוד החלופי לעבודה כאתר המבצעי ובתמיכה במשימות חיוניות ופונקציות עסקיות	הארגון יוודא כי השירותים והמערכות (כולל מערכות התמך והתשתיות) באתר הגיבוי יהיו מוכנות וזמינות בכל זמן נתון לטובת מעבר ועבודה שוטפת מול אתר הגיבוי	ניתן לוודא באמצעות הכנת רשימות תיוג מפורטות למערכות התמך והתשתיות, לוודא את תקינות המערכות באופן תקופתי וכן לבדוק את תקינותן במסגרת ביצוע תרגילים	2
המשכיות עסקית	25.16	יש ליצור גיבוי לרשתות תקשורת ולוודא קיום שירותי תקשורת חלופיים על מנת להקטין את התלות בתשתית יחידה (Single point of failure)	הארגון יוודא כי קיימת תשתית תקשורת חלופית בין האתר הראשי לאתר הגיבוי וכן כפילות תקשורת לאתר הראשי	ניתן לוודא באמצעות רכישת קווי גיבוי מספק אחר והפעלתם בשוטף, ע"י כך למעשה למזער התלות בקו תקשורת יחיד	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
המשכיות עסקית	25.17	יש לדרוש מספקי השירות, הרלוונטיים לתרחישי החירום, תכנית המשכיות עסקית הנבדקת באופן תקופתי	הארגון יוודא מול ספקי השירות כי יעדי ההתאוששות שלהם תואמים את יעדי ההתאוששות של הארגון	ניתן לקבל מספקי השירות את עיקרי תכניות החירום שלהם, לרבות יעדי ההתאוששות של השירותים המסופקים לארגון	2
המשכיות עסקית	25.18	יש לבצע גיבויים ברמת משתמש, מערכת ותיעוד המערכת ולהבטיח את הגנת הגיבויים	הארגון יבצע גיבוי של כלל המידע הקריטי במערכות המידע התומכות בתהליכים העסקיים ויבטיח שמירה על זמינות, שלמות וסודיות הגיבויים	ניתן לבצע באמצעות גיבוי לקלטות, לדיסקים או לענן	1
המשכיות עסקית	25.19	יש לוודא את אמינות הגיבויים וזמינותם	הארגון ישמור ויוודא כי הגיבויים מתבצעים אופן אמין וזמינים להתאוששות	ניתן לבצע באמצעות בדיקה תקופתית של שחזור גיבויים	2
המשכיות עסקית	25.20	יש לשמור עותק גיבוי של מידע קריטי באתר נפרד מהאתר הראשי	הארגון יוודא כי עותקים של גיבויים נשמרים באתר מרוחק ובאופן המוגן מאסונות סביבתיים (כגון שריפה)	ניתן לבצע על ידי גיבוי ישירות לאתר גיבוי מרוחק או שינוע שוטף של מדיית הגיבוי לאתר מרוחק	2
המשכיות עסקית	25.21	יש לממש מנגנון לשחזור טרנזקציות למערכות מבוססות טרנזקציות	הארגון יגדיר מנגנון אשר ישחזר טרנזקציות שלא הושלמו בעקבות כשל מערכת או מעבר למערכת גיבוי	ניתן לממש במגוון תצורות, תצורה של כתיבה כפולה (שתי טרנזקציות במקביל לשתי מערכות - לראשית ולעותק) תצורה של אישור הטרנזקציה לאחר השליחה ושמירה ותיוג של הטרנזקציות שכשלו, במערכות אשר מבוססות תורים ניתן להעתיק את תוכן התור לגיבוי כך שטרנזקציות אשר לא נשלפו קיימות בתור גיבוי	2

משפחה	זיהוי	הבקרה	הסבר משלים	דוגמה לישום הבקרה	רמת בקרה
המשכיות עסקית	25.22	יש לוודא יכולת לשחזור רכיבי מערכת למצב מבצעי ידוע	יש לוודא מנגנונים המאפשרים שחזור נתונים או תצורת מערכת למצב ידוע כגון תצורה שהוקפאה במועד מסוים או מצב נתונים ממועד מסוים	ניתן לבצע על ידי גיבוי תצורה בנקודת זמן (כגון בטרם ביצוע שינויים) וכן על ידי קביעת נקודת שחזור נתונים ומנגנון גלגול לאחור (Rollback)	3
המשכיות עסקית	25.23	יש לוודא יתירות שירותים ותשתיות קריטיות	הארגון יוודא כי קיימת יתירות לשירותים ומערכות תשתית קריטיות במטרה לצמצם את התלות בנקודת כשל יחידה	ניתן ליישום על ידי יתירות של תשתיות קריטיות כגון ציודי תקשורת, שירותי רשת עיקריים, מערכות אבטחה, מערכות אחסון וכדומה	3

נספח א' //
דוגמה לביצוע הערכת סיכון

בדוגמה מטה החישוב הינו: Risk =3I+P =3X3+2

טופס מלא עבור מערכת לדוגמא

	שאלה	תשובה לדוגמה	ציון משוקלל
שאלון רמת ערכיות (עוצמה) שאלון זה מופיע בעמוד 26 במסמך	מהי רמת הנזק שיגרם לארגון בעקבות **חשיפת מידע** מהמערכת? C	2	הערך המקסימלי 3
	מהי רמת הנזק שיגרם לארגון בעקבות **שיבוש מידע** הקיים במערכת? I	1	
	מהי רמת הנזק שיגרם לארגון בעקבות **השבתת** המערכת לפרק זמן ממושך? A	3	
שאלון רמת חשיפה (הסתברות) שאלון זה מופיע בעמוד 28 במסמך	כמה משתמשים קיימים במערכת?	2	הערך הממוצע 2
	מי הם משתמשי המערכת?	4	
	כמה ממשקים קיימים למערכת?	1	
	מהו אופי ממשקי המערכת?	1	
	סוג המידע הקיים במערכת	3	
	גישה למערכת מרחוק	1	
	רמת מידור הרשאות משתמשי המערכת	2	
	עדכניות תשתית	3	
	עדכונים וטלאי אבטחה	4	
	אבטחה פיזית	2	
	ציון משוקלל למערכת		3*3+2=11

לאחר מענה על השאלון הנ"ל עבור כלל הנכסים של הארגון, מתקבלת רשימה כזו:

הסתברות(P)/עוצמה (I)	4	3	2	1
4	[illegible] מערכת א'	13	10 מערכת ג'	7
3	[illegible]	12	9	6
2	14	11 מערכת ב' מערכת ד'	8	5 מערכת ה
1	13	10	7	4

נספח ב' //
עזרים עתידיים למימוש תורת ההגנה

על-מנת לעזור במימוש תורת ההגנה ובהנגשתה לקהלי יעד שונים יפותחו כמה עזרים בהובלת המערך. בנוסף, ייתכן שיפותחו עזרים נוספים על-ידי גופי משק שונים, כמקובל בעולם במקרים דומים.

העזרים שהמערך מתכנן לפתח בקרוב הם:

1. תהליך של מיכון תורת ההגנה באמצעות פלטפורמה טכנולוגית נוחה ויעילה, שתהווה כלי עבודה.
2. טפסים ונהלים גנריים מוכנים לשימוש הארגון, כמו דוגמה למסמך מדיניות ארגונית בהיבטי הגנה בסייבר, נוהל לבקרות תורת ההגנה, תבנית לטפסים שונים ועוד. על הארגון **להתאים** דוגמאות ותבניות אלו לצרכיו.
3. מחשבון להערכת הסיכון, שימכן כמה נוסחאות פשוטות בתורת ההגנה.
4. טבלאות עם דוגמאות למיפוי יעדים.
5. מידע מעשיר נוסף עבור פרקי הבקרות.
6. Best Practices עבור בקרות נבחרות.
7. ערכות הדרכה לקהלי יעד שונים.

העזרים התומכים בתורת ההגנה יוצגו על-פי ההיררכיה הבאה:

- **תפיסה לאומית** - שעל בסיסה אנו כותבים את תורת ההגנה לארגון.
- **תורת ההגנה** - מציגה את נושאי ההגנה השונים ברמה הבסיסית (לדוגמה: ניטור, מודעות, הפרדת רשתות, ניהול שרשרת אספקה ועוד).
- **Best Practices** - על בסיס תורה זו נכתוב יחד איתכם הנחיות פרטניות לטכנולוגיה/שירות וכו', כגון Best practice להקשחת שרתי DB מסוג מסוים, או לעבודה נכונה עם מערכת הפעלה Windows 10 וכו'.
- **הרחבות מקצועיות** - לצד תורת ההגנה יהיו מסמכי הרחבה, המספקים מידע נוסף שאינו תלוי טכנולוגיה ספציפית (Best Practice), אך עם זאת, הוא מקיף ומפורט יותר מדרישות הבסיס של תורת ההגנה ("הרחבה מקצועית").

המידע הנ"ל יונגש לשטח בצורות שונות (מדריכים, לומדות מקוונות, One pager לעסקים קטנים, הדרכות וקורסים ועוד).

Best Practice A

Best Practice B

Best Practice C

Best Practice D

Best Practice E

תורת הגנה לארגון / תקן הגנה בסייבר

תפיסה

הרחבות מקצועיות:

לדוגמא, פיתוח מאובטח, עבודה בסביבת ענן, מיקור חוץ ושרשרת אספקה, המשכיות עסקית ועוד.

נספח ג' //
בקרות הגנה לארגון מקטגוריה א' - דגשים עבור איש המחשוב

בקרות אלו מפרטות את הדברים הבסיסיים הנדרשים מארגון לטובת הגנה בסיסית על נכסיו.

הבקרות מפרטות את הנדרש מהארגון בפרק 5.1 בחלק של "עשרת הדברות" להגנה על ארגון מקטגוריה א'.

משפחה	כותרת	הבקרה	הסבר משלים
אחריות הנהלה	ממשל תאגידי	יש לבחון תקופתית את גישת הארגון לניהול אבטחת המידע והגנת הסייבר ואת אופן יישומה.	יש לבחון במסגרת בקרה זו - את בקרות האבטחה המיושמות בארגון, מדיניות אבטחת המידע, והגנה על תהליכים עסקיים קריטיים לארגון.
מניעת קוד זדוני	זיהוי ומניעת קוד זדוני על תחנות קצה ושרתים בארגון	יש להטמיע כלים לזיהוי ולמניעת קוד זדוני על תחנות קצה ושרתים בארגון. כלים אלו יופעלו במתכונת הגנה אקטיבית וכן יבוצעו סריקות תקופתיות.	מאחר שחלק מהפוגענים עשויים לחדור את מנגנוני האבטחה, יש לוודא כי בקרות לטיפול בקוד זדוני יוישמו גם ברמת תחנות העבודה.
מניעת קוד זדוני	עדכונים אוטומטיים	יש להפעיל עדכון אוטומטי של כלל המערכות לזיהוי ולמניעת קוד זדוני בארגון.	הארגון יפעיל עדכון אוטומטי משרת מרכזי המנוהל על-ידי הארגון או על-ידי ספק שירות מוכר. עדכונים אלה ישמרו על כלי ההגנה מעודכנים באופן תמידי.
הצפנה	קריטריונים להצפנה	יש להגדיר שימושים המצריכים הצפנה ואת סוג ההצפנה הנדרשת, בהתאם לחוקים, להנחיות, לנהלים, לרגולציה ולמחויבויות עסקיות.	הארגון יגדיר מהו המידע והמערכות שיש להצפין ויתעד את תצורת הצפנת המידע. הדרישות ייגזרו מדרישות החלות על הארגון או מדרישות השמירה על המידע.
הגנת תחנות עבודה ושרתים	מדיניות הקשחה	יש להגדיר, לתעד וליישם מדיניות הקשחה לתחנות עבודה ושרתים, המספקת מענה לדרישות אבטחת המידע של הארגון.	הארגון יגדיר דרישות הקשחה למערכות בארגון, בדגש על דרישות הבסיס, תדירות העדכונים ורמת הסיווג, ואז לתעד את הדרישות במסגרת-על, שתהווה בסיס לכתיבת נוהלי ההקשחה.

משפחה	כותרת	הבקרה	הסבר משלים
הגנת תחנות עבודה ושרתים	יישום הקשחה	יש להגדיר את תצורת המערכת כך שתספק את הפונקציונליות המינימלית הנדרשת (תוך חסימת פונקציות, פורטים, פרוטוקולים שאינם נדרשים).	הארגון יגדיר נוהלי הקשחה לכל סוג מערכת ושרת על בסיס פרקטיקות מקובלות, כך שיכללו לכל הפחות: 1.הפחתה של שטח התקיפה של המערכת על-ידי חסימת פורטים לא נחוצים. 2.כיבוי שירותים לא נחוצים. 3.הסרת חשבונות משתמש אורח. 4.העדפת שימוש בפרוטוקולים מאובטחים בתקשורת בין שרתים. 5.קבלת עדכונים באופן מסודר. 6.חסימת פונקציות רגישות של המערכת. 7.שליחת לוגים על אירועי מערכת לשרת ניטור. 8.חסימת התקנת תוכנה על-ידי משתמשים לא מורשים.
מחשוב ענן ציבורי	אחריות משותפת	יש להבין את חלוקת האחריות לאבטחת השירות בין ספק השירות ובין הארגון וליישם את בקרות ההגנה בהתאם.	בעת השימוש בשירותי ענן ציבוריים, יש חלוקת אחריות להגנת הסייבר בין הנושאים שבאחריות הספק ובין נושאים הנשארים באחריות הלקוח. חלוקת אחריות זו תלויה באופי השירות ובמודל המימוש. על הארגון להבין מה הם הנושאים הנמצאים באחריותו וליישם את ההשלכות של אחריות זו.
מחשוב ענן ציבורי	שיתוף מידע רגיש	יש לוודא, כי לא מועברים לשירותי הענן נתונים אשר על-פי הרגולציה והמחויבויות של הארגון אסור להעבירם.	יש נתונים שעל הארגון נאסר להעבירם לאחסון או לעיבוד בשירותי ענן ציבוריים בשל שיקולים של רגולציה או התחייבות לצדדים שלישיים. טרם העברת נתונים לענן, יש לוודא כי לא נשמרים או מועברים לשירות הענן נתונים מסוג זה.

משפחה	כותרת	הבקרה	הסבר משלים
הגנה על המידע	הגנת המידע השמור במשאבים משותפים	יש למנוע העברת מידע לא מורשית או לא מכוונת דרך משאבי מערכת משותפים.	על הארגון למנוע ולטפל בהעברת מידע לא מורשית באמצעות תיקיות משותפות, דואר אלקטרוני, מדיה נתיקה וכו'.
אבטחת רשת	ניהול חיבורים (Sessions) - ברמת רשת	הארגון יפעיל אמצעים טכנולוגיים על-מנת להגן על שירותיו מפני התקפות מניעת שירות	יש להגן מפני התקפות מניעת שירות (DOS) מסוגים שונים כדוגמת: העמסה על משאבי מחשוב עד לקריסתם, העמסת רוחב פס התקשורת, העמסת אתר אינטרנט עד לקריסתו ועוד
אבטחת רשת	אמינות חיבור (Sessions)	יש לוודא כי שירות תרגום כתובות (DNS) מסופק על-ידי שרת מהימן (פנים ארגוני וכן חוץ ארגוני)	הארגון יאפשר קבלת שירות תרגום כתובות (DNS) אך ורק משרת פנימי מאובטח. זאת במטרה למנוע ניתובי תקשורת שגויים (במזיד או בשוגג) אל יעדים עוינים
אבטחת רשת	גבולות רשת	יש להגביל את מספר ערוצי התקשורת החיצוניים למערכת	הארגון יצמצם ויאחד ערוצי תקשורת בכדי להבטיח שליטה טובה על החיבורים למערכת.
אבטחת רשת	גבולות רשת	יש לחסום כברירת מחדל כל תעבורת רשת, ולאפשר ידנית כל תעבורה רצויה על-ידי כלל חריגה	הארגון יגדיר את חוקי סינון תעבורת הרשת באופן החוסם בברירת מחדל כל תעבורה שלא הוגדרה במפורש כמותרת.
אבטחת רשת	גבולות רשת	יש להשתמש בכתובות רשת נפרדות (תת-רשת שונה) כדי להתחבר למערכות באזורי אבטחה שונים	הארגון יגדיר כי לכל תת רשת יהיה טווח כתובות נפרד אשר יפורסם לחומת-האש ולנתבים.
בקרת גישה	ניהול משתמשים	יש להגדיר חשבונות משתמשים אשר תומכים בפונקציות העסקיות של הארגון	לכל הפחות, יש להפריד בין חשבון "מנהל" לחשבון "משתמש". כמו כן יש להגדיר משתמשים אשר מנהלים את פונקציות האבטחה במערכת (כגון יצירת משתמשים, ניהול הרשאות גישה ומערכת, ניהול מערכות אבטחת מידע ועוד)

משפחה	כותרת	הבקרה	הסבר משלים
בקרת גישה	ניהול הרשאות	יש להגדיר ולאכוף הרשאות גישה לוגיות למערכת ולמידע בהתאם למדיניות בקרת הגישה	בקרת הגישה יכולה להיעשות ברמה אישית (identity-based) או ברמת תפקיד (role-based), ומטרתה לשלוט בגישה של ישויות (משתמשים או תהליכי מחשב) לאובייקטים (קבצים, רשומות, מכשירים ועוד).
משאבי אנוש ומודעות עובדים	כללי התנהגות עובדים	יש להגדיר כללי התנהגות בעבודה מול מערכות המידע בארגון. כללים אלו מגדירים את תחומי האחריות ואת כללי השימוש הנאות במערכות המידע בארגון, בדגש על מערכות רגישות.	הארגון יגדיר נוהלי התנהגות בהתייחס למערכות המידע ויפיצם לכלל העובדים.
משאבי אנוש ומודעות עובדים	ניהול הרשאות בעת גיוס/ניוד/ עזיבה	יש לבחון ולעדכן את הרשאות הגישה של עובד בעת ניוד עובד מתפקיד לתפקיד.	יש להגדיר תהליכים של עדכון על ניוד העובד ושל עדכון ההרשאות בהתאם לתפקיד החדש (הסרת ההרשאות המיותרות והקמת ההרשאות הנדרשות לתפקיד החדש).
אבטחה ברכש ופיתוח	דרישות אבטחה ברכש ופיתוח מערכות	אבטחת שרשרת אספקה - יש לדרוש מספקי שירותים לציית לדרישות האבטחה הארגוניות, לרגולציות, לסטנדרטים ולהנחיות.	הארגון יוודא כי ספקי שירות עומדים בדרישות הציות (Compliance) הארגוניות וכן בדרישות הרגולטוריות החלות במדינות שבהן פועל הארגון.
הגנה פיזית וסביבתית	תאורת חירום	יש ליישם ולתחזק תאורת חירום אוטומטית, אשר תופעל באירוע של הפסקה או שיבוש באספקת חשמל ותכלול יציאות חירום ונתיבי פינוי במתקן.	
הגנה פיזית וסביבתית	הגנה מפני שריפות	יש ליישם ולתחזק אמצעים/ מערכות לזיהוי וכיבוי אש עבור מערכות המידע אשר נתמכים במקור אנרגיה עצמאי.	

משפחה	כותרת	הבקרה	הסבר משלים
תיעוד וניטור	מנגנון תיעוד	יש להפעיל מנגנון המייצר רשומות בקרה על-אודות אירועים במערכות הארגון. יש לרשום, לכל הפחות, אירועים ממערכות המכילות מידע רגיש של לקוחות, ממערכות קריטיות לתפקוד הארגון וממערכות ליבה (שרתים, רכיבי תקשורת, אפליקציות, מסדי נתונים וכו').	הארגון יוודא, כי מערכות תשתית ומערכות אפליקטיביות מפעילות מנגנון רישום אירועים, וכי הרשומות נשמרות לפרק זמן שהוגדר על-ידי הארגון. רשומות הבקרה יכילו מידע, כגון סוג האירוע, מתי התרחש, מקור האירוע, שם המשתמש. בכל מקרה, יש לנטר את המערכות המעבדות מידע רגיש, המהוות חלק מהתשתית הקריטית של הארגון, או המנהלות את תהליכי הליבה של הארגון.
תיעוד וניטור	מנגנון תיעוד	מנגנוני הרישום יכללו, לכל הפחות, מידע על אופי הפעולה שבוצעה, חתימת זמן, מקור ויעד הפעולה, מזהה משתמש, מזהה תהליך, כישלון/הצלחה, שם קובץ מעורב.	
ניהול אירועים ודיווח	טיפול באירועי סייבר ואבטחת מידע	יש להגדיר ערוצי דיווח של עובדים לגורמים הממונים לצורך דיווח על חשד לאירועי אבטחה.	הארגון יחיל נהלים על אירועים המחייבים דיווח ואת אופן הדיווח לגבי אירוע המוגדר כאירוע סייבר.
המשכיות עסקית	זמינות משאבים	יש לבצע גיבויים ברמת משתמש, מערכת ותיעוד המערכת ולהבטיח את הגנת הגיבויים.	הארגון יבצע גיבוי של כלל המידע הקריטי במערכות המידע התומכות בתהליכים העסקיים ויבטיח שמירה על זמינות, שלמות וסודיות הגיבויים.

נספח ד' //
תאימות לתקנים

תורת ההגנה שואבת את בסיס הידע שלה מתקנים בינלאומיים מקובלים, דוגמת NIST 800-53 ו-ISO 27001. לטובת הקלה על ארגונים לאמץ את הבקרות המופיעות במסמך זה, מערך הסייבר הלאומי מיפה את הבקרות הקיימות אל הבקרות המקבילות להן בתקנים הנזכרים לעיל. בפרט, ארגון העומד בתורת ההגנה ונדרש להסמכת תקן ISO 27001 יכול להשתמש בנספח תאימות לתקן.

בהמשך, ובמקביל להתפתחות תורת ההגנה הארגונית, ימפה המערך את הבקרות אל מול תקנים מקומיים ובינלאומיים מובילים. בין התקנים החשובים שימופו בקרוב אפשר למנות את:

- חוזר ניהול בנקאי תקין 357 + 361
- חוזר ניהול סיכוני סייבר של רשות שוק ההון
- תקנות הרשות למשפט וטכנולוגיות מידע (רמו"ט)
- ISO 27032

תאימות לתקן ISO 27001

לאור העובדה שתקן זה נבנה תוך הישענות רבה על תקנים בינלאומיים בכלל ותקן ISO 27001 בפרט, ההשלמה הנדרשת מארגון המממש תורת הגנה זו לטובת עמידה מלאה בדרישות לקראת מבדק התעדה אינה גדולה.

על-מנת להקל על ארגונים אשר מוסמכים או שוקלים להתחיל מהלך של התעדה לתקן ISO 27001, נכתבה טבלת המרה, המשקפת את בקרות תורת ההגנה אל מול הצהרת הישימות של התקן (Statement Of Applicability). טבלה זו מצויה באתר מערך הסייבר הלאומי.

נספח ה' //
בקרות הגנה קריטיות להשגת תוצאה גבוהה בזמן קצר

תורת ההגנה מגדירה תהליך של ניהול סיכונים, ולפיו דרישה למימוש בקרות במסגרת תכנית עבודה. מנגד, אצל חלק מהארגונים קיים צורך למקד את הפעילויות הראשונות לביצוע. פעילויות אלו כוללות, למעשה, את הבקרות בעלות הערך "עלות מול תועלת" הגבוה ביותר.

ארגון ה-SANS נחשב לאחד המובילים בעולם בתחום הגדרת בקרות הגנה קריטיות, שהן הבקרות האפקטיביות ביותר (CSC - Critical Security Controls). מימוש הבקרות, אשר מכסות 20 נושאים, מספק לארגון מענה מפני 88% מהמתקפות הידועות[1].

הבקרות במסמך זה נבנו על בסיס אותו ההיגיון, אך הן אינן מייצגות בהכרח את בקרות המפתח של ארגון ה- SANS. לעיתים, שיקולים כמו קלות ואפקטיביות הבקרות השפיעו על בחירת הבקרות אשר סומנו על ידינו באמצעות אייקון ייעודי כבקרות "מפתח".

ארגון המעוניין לקבל תמונת מצב מהירה של מוכנות ההגנה שלו יכול לעבור על בקרות ההגנה הקריטיות, אשר מסומנות באמצעות סימן של מפתח בפרק 6 במסגרת משפחות הבקרה השונות.

משפחה	זיהוי
ניהול סיכונים והערכת סיכונים	2.1
בקרת גישה	4.2, 4.4, 4.17
הגנה על המידע	5.1
הגנת תחנות עבודה ושרתים	6.5
מניעת קוד זדוני	7.1 ,7.2 ,7.3 ,7.9
הצפנה	8.6
אבטחת רשת	9.1 , 9.9, 9.12, 9.24, 9.25
הפרדת סביבות	10.2, 10.4
מחשוב ענן ציבורי	11.4, 11.6
אבטחת מדיה	15.7
שרשרת אספקה ומיקור חוץ	16.2
אבטחת ברכש ופיתוח	17.14
הגנה פיזית וסביבתית	18.6
הדרכות	20.2
תיעוד וניטור	21.1
סקרי הערכת בקרות אבטחה	22.6
ניהול אירועים ודיווח	24.12
המשכיות עסקית	25.1, 25.19

1 https://www.sans.org/critical-security-controls/history

נספח ו' //
בנק הבקרות

בנק הבקרות מהווה מרכיב משמעותי בתורת ההגנה. הבנק, שנבנה על סמך תקינה עולמית מקובלת, מכיל מרכיבים רבים, שנועדו להעשיר את ההבנה של הארגון המגן במימוש הבקרה.

משיקולי נוחות ויעילות, בגוף מסמך זה הוכנסו רובדי המידע ההכרחיים לטובת מימוש תורת ההגנה. לצד זאת הוגדרו ונכתבו רובדי מידע מעשירים נוספים על-אודות כל בקרה. בין רבדים אלו אפשר למנות כיום את:

1. CIA - היבטי אבטחת המידע שעליהם הבקרה מגינה - זמינות, שלמות או חיסיון.
2. Cyber Kill Chain - השלב בשרשרת התקיפה שבה הבקרה ממלאת תפקיד.
3. קטגוריות הנכסים שעבורן הבקרה רלוונטית - IT, OT, שירותים או מאגרי מידע.
4. רמות הסיכון שבהן נדרש ליישמה - ככל שרמת הסיכון של נכס גבוהה יותר, תידרשנה בקרות המספקות רמת הגנה גבוהה יותר, המותאמת לסיכונים הרלוונטיים לנכס (רמות 1-4 הנגזרות מהשלב השלישי בתהליך ניהול הסיכונים שבמסמך זה).
5. סוג הבקרה - בקרה יכולה להיות בקרה מנחה (כגון נוהל), בקרה מונעת (כגון מערכות לסינון קוד עוין), או מגלה (כגון מערכות ניטור והתראה).
6. תאימות הבקרה לתקנים נפוצים (בשלב הראשון של פרסום תורת ההגנה הבקרות ממופות אל התקנים ISO 27001 ו-NIST 800-53).

מידע מורחב ומשלים על-אודות פרקי הבקרות ניתן למצוא באתר מערך הסייבר הלאומי.

נספח ז' //
התמודדות עם אירוע סייבר משמעותי

תורת ההגנה מניחה, כי אי אפשר להבטיח הגנה מלאה מפני פגיעת סייבר בארגון. אי לכך, פרקי הבקרות נועדו להכין את הארגון להתמודד עם אירועי סייבר ולהתאושש מהם בנזק קטן. מנגד, לאור הניסיון שנצבר בשנים האחרונות אנו יודעים, כי ניהול אירועי סייבר משמעותיים הינו תחום מקצועי, הדורש ידע ייחודי, כלים, תשתיות והכשרה מקצועית ייעודית, שאינם קיימים בכל ארגון. לטובת סיוע לארגונים בהתמודדות עם אירועים כאלו הוקם ה-CERT הלאומי שתחת מערך הסייבר הלאומי. ייעודו של ה-CERT הוא לחזק את החוסן של המשק הישראלי בסייבר באמצעות מתן סיוע ראשוני וטיפול באיומי סייבר, וכן לרכז ולקבל מידע רלוונטי מכלל הגופים בישראל ובעולם.

תפקידים ותחומי פעילות של ה-CERT:

- טיפול באירועים (Incident Handling) - החל משלב הדיווח, עבור בסיוע ובתיאום הטיפול באירוע סייבר ועד לסיוע בהתאוששות ובתחקור.
- טיפול בחולשות ופוגענים (Vulnerabilities and Artifacts Handling) - החל משלב קבלת הפוגענים, עבור בביצוע מחקר להבנתם ועד הפצת המתודולוגיות והדרכים להתמודדות עמם.
- התמודדות ומניעה של איומי סייבר – באמצעות פעילות פרואקטיבית לגילוי, לזיהוי ולחקירה שלהם.
- פיתוח ידע להתגוננות והפצתו לקהל היעד – לרבות כלים וטכנולוגיות לשיתוף מידע.
- הסברה והעלאת מודעות – לקהל הרחב, לקהלים ייעודיים ולקהל המקצועי העוסק באבטחת סייבר.
- פיתוח קשרים עם גופים מקבילים בעולם וטיפוחם – חילופי מידע, מתודולוגיות התגוננות ועוד.

פנייה לקבלת עזרה בציר ההתאוששות ניתנת, בין היתר, באמצעות הדרכים הבאות:

א) שליחת מייל לכתובת team@cert.gov.il.

ב) התקשרות לטלפון מס' 0723990800.

ג) פנייה באמצעות טופס מובנה באתר ה-CERT בכתובת:

https://www.gov.il/he/Departments/General/contact

נספח ח' //
ניתוח מצב מוכנות על בסיס סטטוס הטמעת והפעלת כלי הגנת סייבר

לטובת קבלת תמונת מצב מהירה וכללית אודות רמת ההגנה הנוכחית של הארגון, נבנה "שאלון הערכה עצמית".

שאלון זה נועד לקבלת מידע כללי ברמת "High Level" על רמת אבטחת המידע בארגון ולסייע בבניית תכנית עבודה מעשית בהתאם לתורת ההגנה הארגונית.

השאלון בנוי מארבע קטגוריות:

1. **ראשי** - הכוללת נתונים כלליים על הארגון.
2. **תכנית הגנה IT** - הכוללת את רכיבי הגנה הקיימים ברשת ה IT (מנהלה) בארגון ורמת הטמעתם.
3. **תכנית הגנה ICS** - הכוללת את רכיבי הגנה הקיימים ברשת התפעול (רשת של הרכיבים התעשייתיים ורכיבי בקרה) בארגון ורמת הטמעתם.
4. **תכנית הגנה או"ש** - הכוללת את התהליכים, שיטות ומערכות מנהל וארגון בנושאי סייבר ואבטחת המידע.

לצפייה בשאלון הערכה עצמית המלא יש להיכנס לאתר מערך הסייבר הלאומי.

דוגמה מתוך שאלון הערכה עצמית: (המסמך המלא נמצא באתר המערך)

			לא רלוונטי	לא קיים 0%	הטמעה טכנולוגית (התקנת המוצר) 30%	הטמעה לוגית הגדרות (עפ"י הגדרות יצרן) 60%	פרישה בארגון (אחוז הפרישה בכלל הארגון) 80%	מבדקי חדירה והגדרות פרטניות מותאמות לארגון - אופטומיזציה 90%	תחזוקה שוטפת 100%
כלי ניהול שליטה וניטור									
	SIEM	האם קיימת מערכת ניטור ?							
	הגדרת Log במערכות	רמת הגדרת לוגים במערכות							
	System Change Management	האם קיימת מערכת לניהול שינויים (שינוי תוכנה / גרסאות וכד')							

	דלף מידע - DLP	האם קיימת מערכת למניעת דלף מידע ?							
	מערכות לזיהוי אנומליות	האם קיימת לזיהוי אנומליות ברשת / במערכות ?							
	ניהול גיבויים של מערכות אבטחת מידע וכו'	האם קיימים גיבויים להגדרות מערכות ההגנה?							
	תחקור סייבר	האם קיימת מערכת לתחקור אירוע סייבר ?							
הגנה חיצונית									
	Firewall	האם קיימת מערכת "חומת אש" בארגון?							
	Anti Spam / Email Protection	האם קיימת מערכת להגנה על דואר נכנס (פוגענים וכד)?							
	Web filtering	האם קיימת מערכת לסינון אתרים ?							
	SSL VPN	האם קיימת מערכת לגישה מאובטחת לארגון?							
	WAF	האם קיימת מערכת "חומת אש אפליקטיבית" בארגון?							
	SandBox	האם קיימת מערכת הלבנה לקבצים נכנסים לארגון?							
רשת									
	IPS / IDS	האם קיימת מערכת לזיהוי / חסימה של מתקפות בארגון?							
	NAC	האם קיימת מערכת בקרת גישה לרשת?							
	Segmentaion	האם קיימת הפרדת רשתות בארגון ?							
	AntiVirus	האם מוטמעת מערכת אנטי וירוס בארגון?							
	VA Scanning	האם מבוצעות סריקות ברשת לאיתור חולשות אבטחת מידע?							

נספח ט' //
מילון מונחים

מונח	באנגלית	הגדרה	דוגמאות/הסברים
CERT	CERT® Computer/ Cyber Emergency Response/ Readiness Team	גוף מקצועי שייעודו לסייע לארגונים להתמודד עם אירועי סייבר. הוא מספק את השירותים הנחוצים להתמודדות עם אירוע סייבר, ומסייע בהתאוששות מנזקיו.	המונח משמש כיום במדינות שונות לייצג גופים בעלי תחומי אחריות ויכולות שונים. שם אלטרנטיבי – CSIRT [Computer Security Incident Response Team]
אחיזה	Hold	מצב שבו לתוקף יש יכולת לבצע פעולות בנכס סייבר.	
איום סייבר	Cyber Threat	צירוף של כוונות ויכולות לתקיפה במרחב הסייבר שטרם התממש.	ראה, להבדיל, אירוע סייבר.
אירוע סייבר	Cyber Incident	התרחשות אשר מעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, שקיים יסוד להניח, כי היא נובעת מפעילות מכוונת במרחב הסייבר.	אירוע סייבר אינו בהכרח מעיד על תקיפת סייבר, אך קיים יסוד סביר להניח שכן.
אִפְחוּת	Mitigation	מכלול האמצעים שבהם נוקטים כדי להקטין את הסיכוי להתממשות אירוע סייבר, או כדי להפחית ככל הניתן את נזקיו והשלכותיו, אם כבר התממש.	
הבנה מצבית בסייבר	Cyber Awareness	היכולת לייצר הבנה טובה של המתרחש במרחב הסייבר ושל השלכותיו על רציפות התפקוד בארגון/ משק.	
הגנה שקטה	Observable/ Manifest Defence	שלב במהלך ניהול אירוע סייבר שנועד לסלק את התקיפה ו/או לגרום לתוקף לנקוט בפעולות שאותן לא היה מבצע אלמלא נחשף, וכל זאת, תוך הבנה שהפעילויות הנעשות במהלכו יכולות להיחשף לתוקף.	

מונח	באנגלית	הגדרה	דוגמאות/הסברים
הגנה רועשת	Non Observable/ Covert Defence	שלב במהלך ניהול אירוע סייבר המבוצע תוך הקפדה על הסתרת פעולות המגן מהתוקף, מתוך מטרה להכיל את המתקפה וללמוד את פעילותו ושיטותיו של התוקף.	
הגנת סייבר	Cyber Defense	כל הפעולות שתכליתן להגן על נכסי הסייבר של ארגון מפני תקיפת סייבר.	הגדרה זו מחליפה את המונח אבטחת מידע ומרחיבה אותו. הגנת סייבר אמנם מגינה על המידע ברובד הנמוך שלה אך עושה זאת מתוך פרספקטיבה של הגנת הארגון ו/או התהליך ו/או המערכת, המתבססים על מערכות התקשוב שלהן.
הכוונה (בהיבטי סייבר)	Guidance	מכלול הפעילויות המדינתיות שתכליתן להשפיע על המשק להעלות את רמת החוסן שלו בהיבטי הגנת הסייבר. פעילויות אלו יכולות לכלול בין היתר: הנחיה (Direction) ישירה ועקיפה של ארגונים במשק. הסברה (Publicity) אסדרה (Regulation) של שוק הסייבר תמרוץ ארגונים (Incentivization) שיתוף מידע (Information Sharing and Dissemination) הכשרה ושמירת כשירות (קורסים, השתלמויות, ימי עיון, תרגילים) (Training)	הכוונת המשק בהיבטי ההגנה בסייבר מתבצעת ע"י גורמים שונים במערך הסייבר הלאומי ובגופי רגולציה נוספים. ההכוונה כוללת כלי רגולציה שונים למימושה.
הכלה	Containment	השתלטות על תהליכי גרימת הנזק המתחוללים באירוע סייבר, שמניבה אחד - או יותר - מהתוצאים הבאים: תחימת היקפו של תהליך גרימת הנזק במונחים של מרחב או אמצעים פיסיים; הגבלת רמת החומרה של הנזק הנגרם אל מתחת לסף מסוים; עצירתו של תהליך גרימת הנזק	אין מדובר בנטרול של מחוללי התהליך, אלא במניעת המשך התחוללותם של הנזקים שהוא גורם.

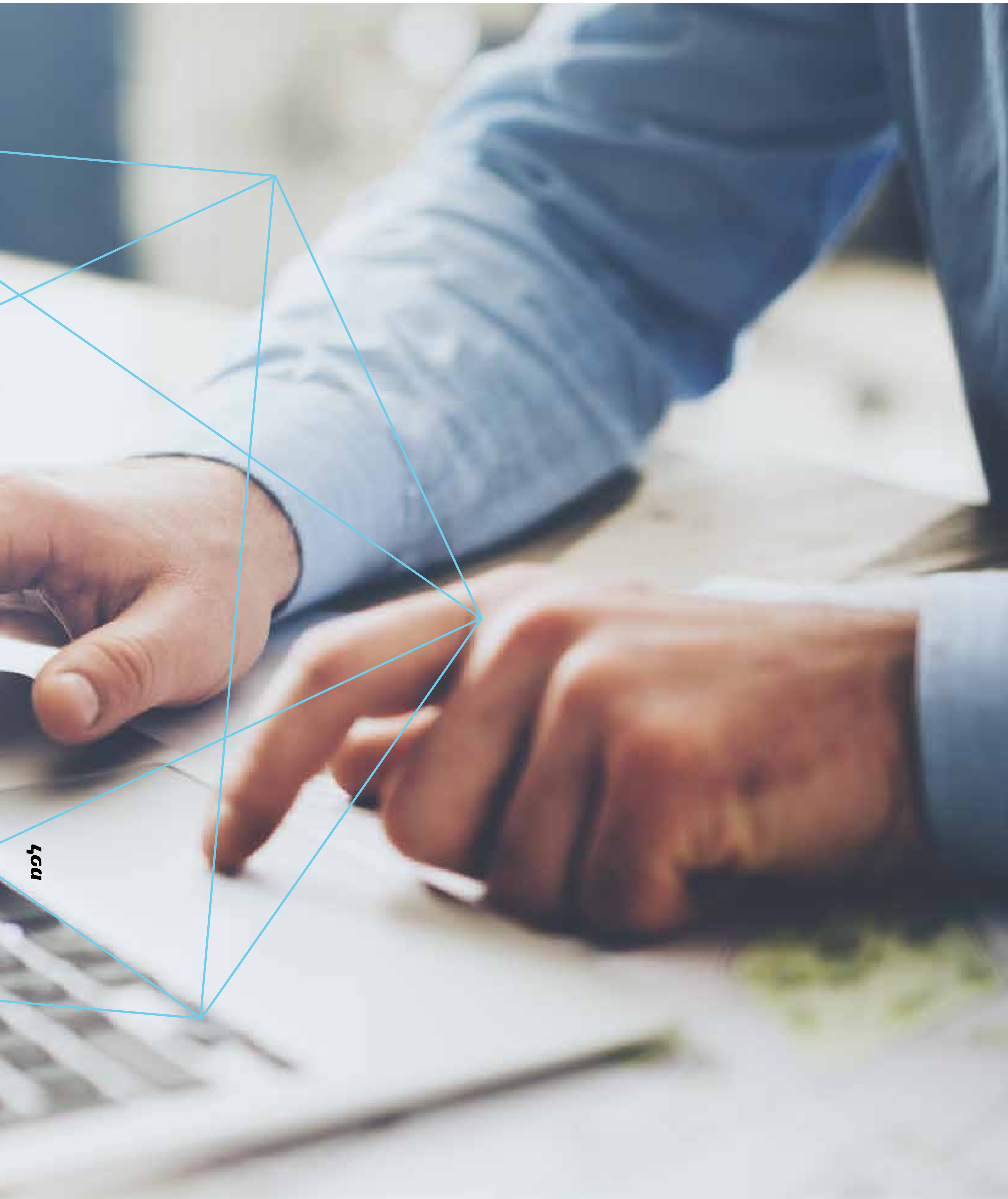
מונח	באנגלית	הגדרה	דוגמאות/הסברים
המרכז הלאומי לניהול אירועי סייבר - "ה-CERT הלאומי"	CERT-IL	אגף במערך הסייבר הלאומי, שייעודו לסייע למשק התמודד עם אירועי סייבר במרחב הסייבר הלאומי. הוא מספק את השירותים הנחוצים להתמודדות עם אירוע סייבר, ומסייע בהתאוששות מנזקיו.	ממוקם בבאר שבע. פרטי התקשרות: 0723990800 מייל: team@cert.gov.il https://cert.gov.il/ContactUs/Pages/ContactUs.aspx
הרשאת גישה למערכת מידע	Accessibility rights	הבטחת אפשרות לגישה למערכת ממוחשבת ולמידע המצוי בה באופן בלעדי למוסמכים לכך.	
מערך הסייבר הלאומי	NCSA [National Cyber Security Authority]	יחידת סמך במשרד ראש הממשלה המכווינה ומקדמת את פעילות ההתגוננות האזרחית בהיבטי עמידות וחוסן לאומי, וכן מנהלת, מפעילה ומבצעת את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר.	
התאוששות (של מערכת בהיבטי סייבר)	Recovery	החזרת מערכת שניזוקה מתקיפת סייבר לרמת פעולה המאפשרת את המשך קיומה של רציפות התפקוד של הארגון.	התאוששות מערכת יכולה להיות לרמת פעילות חלקית, אך מספיקה לצרכי הארגון.
הַתְקָפַת אֶפֶס ימים	Zero-day attack	תקיפת סייבר המנצלת פרצת אבטחה במערכת תקשוב, והמתרחשת בטרם הוכן והופץ תיקון לחסימת פרצת האבטחה, או בסמוך מאוד להכנה ולהפצה של התיקון הדרוש.	התקפות אפס ימים אפקטיביות גם זמן ארוך לאחר גילויין והפצת התיקון שלהן עקב פערי הטמעה של התיקון בארגונים רבים.
התרעה	Alert	הודעה על אירוע סייבר ודרכי ההתמודדות המומלצות עמו, המיועדת לקבוצת נמענים מוגדרת מראש, ומכילה מידע בעל ערך אבטחתי.	התרעות מערך הסייבר הלאומי יכולות להיות מופצת במספר אמצעים, בין היתר דרך תשתית CyberNet.
חולשה	Vulnerability	נקודת תורפה במערכת ממוחשבת או ברכיב שלה או בנוהל הקשור אליה אשר ניתן לנצלה כדי לחולל אירוע סייבר.	
יומן מופעים	Log	רשימה כרונולוגית של מופעים אשר זוהו במערכת תקשוב ותועדו בה אוטומטית.	מושג טכני.

מונח	באנגלית	הגדרה	דוגמאות/הסברים
יחידה להגנת הסייבר בממשלה (יה"ב)	Governmental Cyber Defence Unit	יחידה ברשות התקשוב במשרד ראש הממשלה שייעודה להכוון ולהנחות מקצועית בתחום הגנת הסייבר את כלל משרדי הממשלה ויחידות הסמך שלהם (למעט הגופים המיוחדים).	מתוקף החלטת ממשלה.
יחידת הכוונה מגזרית	Sectorial Guidance Unit	יחידה של אנשי מקצוע בתחום הגנת הסייבר במשרד ממשלתי, שתפקידה להסדיר את הגנת הסייבר במגזרים שבתחומי אחריותו ולסייע למערך בהכוונתו.	מתוקף החלטת ממשלה המנחה המקצועי שלה הוא מערך הסייבר הלאומי.
לָחְמַת סייבר	Cyber warfare, CW	לחמה שבה משתמשים בכלים, באמצעים ובשיטות של סייבר.	יכולה להתלוות ללוחמה קונבנציונלית כממד לחימה נוסף, או כזירת לוחמה עצמאית.
מאגר על	Critical Data Base	מאגר מידע שהוכרז כנכס לאומי חיוני.	רשימת התבחינים מוגדרת במסמך מדיניות של מערך הסייבר הלאומי. דוגמאות: מרשם האוכלוסין, מאגר רישוי נשק ועוד.
מאמץ תקיפה מתמיד	Advanced Persistent Threat [APT]	תקיפת סייבר, שהגורם המבצע אותה מפעיל מאמץ מתמשך לשם מימושה. אופייני שבמתקפה מתמשכת ישתמש התוקף בשיטות ואמצעים טכנולוגיים מתקדמים.	הדגש לרוב הינו התמשכות המאמץ של התוקף. אמנם תוקפים מתוחכמים משתמשים גם בשיטות ואמצעים טכנולוגיים מתקדמים. אולם גם באמצעים פשוטים ניתן כיום במתקפה מתמשכת למצוא ולנצל בהצלחה חולשות בגופים רבים.
מבצע סייבר	Cyber Operation, CO	מבצע העושה שימוש ביכולות סייבר, במטרה להשיג יעדים במרחב הסייבר או באמצעותו.	הגנתי או התקפי.
מגזר (במרחב הסייבר הלאומי)	Sector	כלל הארגונים הפועלים במסגרת תחום מקצועי או ענף משקי ומצויים במסגרת אחריות של מאסדר סייבר.	מתוקף החלטת ממשלה. המאסדר שבהגדרה מאפשר לבצע פעילות אסדרה במגזר.
מופע סייבר	Cyber Event	התרחשות הניתנת לגילוי במערכת תקשוב.	דוגמאות: רישום מופע ב-LOG,

מונח	באנגלית	הגדרה	דוגמאות/הסברים
מושא תקיפה	Object of Attack	ארגון שתקיפת סייבר מתחוללת בו, או שקיימת הערכה כי יש איום להתרחשות אירוע שכזה בו.	אירוע סייבר יכול להתרחש בארגון כאשר מושא התקיפה הוא ארגון שלישי.
מושא תקיפה משני	Secondary Object of Attack	נכס סייבר שתוקף עושה בו שימוש כדי לממש את תקיפתו, ושאינו מהווה יעד תקיפה כשלעצמו.	למשל ספק תקשורת שבאמצעותו מגיעים למושא התקיפה.
מידע בעל ערך אבטחתי	Actionable Information	כל אחד מאלה: 1. סממן (Indicator) להתרחשות אירוע סייבר; 2. חולשה (Vulnerability) בנכס סייבר; 3. איום (Threat) להתרחשות אירוע סייבר; 4. נוזקה (Malware).	מונח משפטי שנועד להגדיר את סוגי המידע המינימליים שמאפשרים לטפל באירוע סייבר מבלי לחשוף מידע מוגן
מידע מוגן	Sensitive Information	כל אחד מאלה: 1. מידע שחוק הגנת הפרטיות, התשמ"ה 1981, חל עליו לעניין יחיד 2. מידע אודות ארגון שאינו נחלת הכלל 3. סודות מסחריים לפי חוק עוולות מסחריות.	
ממונה הגנת סייבר	CISO [Chief Information Security Officer]	מתכלל את מאמצי ההגנה על מערכות התקשוב הארגוניות בסייבר בארגון.	ה-CISO נדרש להבנה של האינטרסים העסקיים של הארגון ושל הביטוי שלהם בנכסי הסייבר שלו. הוא מנהל את סיכוני הסייבר ואת כלל מאמצי ההגנה על נכסי הסייבר הארגוניים, על מנת לספק הגנת סייבר מיטבית לארגון.
ממצא	Artifact	פריט מידע גולמי (נוזקה, קובץ, לוג, וכו') המשמש לחקירת פעילות התוקף.	
מערכת בקרה תעשייתית	ICS [Industrial Control System]	מערכת מבוססת מחשוב, המנטרת ומבקרת תהליכים המתחוללים בתוך מערכת ייצור תעשייתית.	
מערכת מידע	Infosystem	מערכת המכילה מחשבים, רכיבי תקשורת המקשרים ביניהם ומידע האגור בהם.	

מונח	באנגלית	הגדרה	דוגמאות/הסברים
מערכת סקאדה	SCADA [Supervisory Control And Data Acquisition]	מערכת בקרה תעשייתית, המטפלת בתהליכים רחבי היקף המתרחשים באתרים מרובים שלרב מצויים בפיזור גיאוגרפי גדול.	סוג של ICS.
מצב כוננות לאומי בסייבר	National Cyber Stateof Alert	קביעה פומבית ומעוגנת בחוק של רמתה, מהותה והיקפה של ההיערכות הלאומית הנדרשת להתמודדות עם משבר סייבר לאומי. מצב כוננות לאומי נקבע, בדרך של הכרזה, על ידי גורם ממלכתי המוסמך לכך.	מושג מתחום החירום בסייבר.
מצב שגרה בסייבר	Cyber Routine	אחד משני מצבי היסוד במרחב הסייבר הלאומי. מצב, תלוי הכרזה לאומית, שבו לא מסתמן נזק לתפקודם התקין של נכסי סייבר חיוניים כתוצאה מתקיפת סייבר.	מושג מתחום החירום בסייבר.
מרחב הסייבר הגלובאלי	Global Cyberspace	המארג הגלובאלי של תשתיות המידע הטכנולוגיות, הכולל את המרשתת (אינטרנט), רשתות התקשורת, מערכות המחשוב וכל המעבדים והבקרים הממוחשבים המשובצים במערכות טכנולוגיות.	
מרחב הסייבר הישראלי	Israeli Cyber Space	מכלול מרכיביו של מרחב הסייבר הגלובאלי, שלמדינת ישראל יש בהם זכויות.	כולל אלמנטים מחוץ לגבולות הלאומיים.
מרכז ניהול אירועי (מנ"א) סייבר	CSOC [Cyber Security Operations Center]	מרכז לניהול כלל פעילות ההגנה בסייבר של ארגון או מגזר.	דוגמאות – מנ"א ממשלתי, מנ"א פיננסי. נהוג לקצר ל-SOC, בהקשר של הגנת סייבר.
משבר סייבר לאומי	National Cyber Crisis	אירוע סייבר שהשלכותיו בכוח או בפועל מחייבות התערבות מיידית של המדינה כדי למנוע אותן, ואם כבר קרו - להכיל אותן ולתקן את נזקיהן.	למשל פגיעה מצרפית במגזר, פגיעה תשתית קריטית במדינה וכד'

מונח	באנגלית	הגדרה	דוגמאות/הסברים
נגישות (בסייבר)	Accessibility	יכולת של תוקף לחדור לתוך נכס סייבר.	במילים אחרות, נגישות היא פועל יוצא של השגת גישה (של התוקף לנכס הסייבר). בדרך כלל, נגישות מבוססת על ניצול חולשה בנכס הסייבר.
נכס סייבר	Cyber Asset	מערכת תקשוב.	משמש לביטוי הערכיות של מערכת תקשוב בהיבטי הגנה בסייבר.
נכס סייבר חיוני (נס"ח)	Vital Cyber Asset	נכס סייבר שתפקודו התקין נדרש לשם הבטחת רציפות התפקוד של נכס לאומי חיוני.	דוגמאות - תמ"ק, מאגר על וכד'.
נִצְלוּל/תִפְלוּד	Exploit	טכניקה המנצלת חולשה בנכס סייבר על מנת להשיג גישה אליו.	A technique to breach the security of a network or information system in violation of security policy.
סל חירום בסייבר	Cyber Emergency Reserve	המענה הכולל המצוי בידי ארגון, מגזר או המדינה לטיפול במצב חירום בסייבר. הוא מורכב ממשנה מקצועית כתובה (מדיניות, נהלים, תפיסות הפעלה, חקיקה) וממשאבים הנחוצים כדי ליישמה (סמכויות, תקציב, כ"א, אמצעים, זמן ומרחב).	
סממן	Indicator of Compromise (IOC)	נתון אשר ממנו או מכמה שכמותו ניתן להסיק כי התרחש, מתרחש או עלול להתרחש אירוע סייבר.	
שוק הגנת הסייבר	Cyber Security Market	אוסף הארגונים העוסקים בהספקת ידע, מוצרים ושירותים בהגנת סייבר לארגונים.	כולל בין היתר חברות, יצרנים, ספקים, מוסדות ההכשרה והסמכה, בעלי מקצוע, אקדמיה, ספקי מודיעין וכו בתחום הסייבר.
שרשרת תקיפה	Cyber Kill Chain	התהליך שבאמצעותו מבוצעת תקיפת סייבר.	קיימים מספר מודלים לשרשרת תקיפה, כגון המודל של LM.
תקיפת סייבר	Cyber Attack	תקיפה במרחב הסייבר שמסכנת נכסי סייבר או מערכות ותשתיות הנתמכות על ידם.	

מונח	באנגלית	הגדרה	דוגמאות/הסברים
תקנון רמזור	Traffic Light Protocol	שיטה לסיווג מידע על פי מידת רגישותו במובן של קניין רוחני, צנעת הפרט, וכו. היא משמשת להסדרה של שיתוף במידע בין גורמים שונים, ומתבססת על תיוג כל פריט מידע באמצעות אחד מארבעת הצבעים הבאים: ״לבן״: מידע שווה לכל נפש, שאין כל מגבלה לשתף בו, לפרסמו או להפיצו בכפוף לחוקי זכויות יוצרים והגבלים. "ירוק״: מידע שהשיתוף בו מוגבל לקהילה מסוימת ומוגדרת של בעלי עניין. אין להפיצו מחוץ לקהילה זו, ובכל מקרה, אין לפרסמו באינטרנט. ״כתום״: בדומה למידע ״ירוק״, ניתן לשתף במידע שכזה חברים בקהילה מסוימת, אולם, הוא לא יופץ באופן אוטומטי לכל חברי הקהילה הנוגעת בדבר, אלא לקבוצה נבחרת של גורמים מתוכה, שלחבריה יש ״צורך מוכח לדעת אותו״ [need-to-know" basis"]. ״אדום״: מידע שהשיתוף בו מצומצם להפצה על בסיס אישי בלבד.	משמש גופים כגון ה-CERT הלאומי בבואו להפיץ מידע.
תשתית מדינה קריטית (תמ"ק)	CCI (Critical Cyber Infrastructure)	נכסי סייבר חיוניים הנקבעים ע"פ תבחינים ומתווספים לחוק הסדרת הבטחון.	תמ"ק משמש באופן חופשי לציין גם את הגוף המונחה (ג"מ) המכיל את הנכס כגון חברת החשמל, רש"ת וכו'. אולם ההגדרה המדויקת של התבחינים ושל הסמכויות מול תמ"ק היא ברמת הגנת הנכס.

משרד ראש הממשלה
מערך הסייבר הלאומי