

הנחיות המשרד
להגנת הסביבה
אגף חירום
יחידת הגנה על
מידע וסייבר
בתעשייה

המשרד להגנת הסביבה



الوزارة لحماية البيئة
Israel Ministry of Environmental Protection

הוראות לעמידה בתנאי היתר רעלים בתחום ההגנה על מידע וסייבר גרסה 0.9



2017



1. הקדמה

- 1.1. ביום 15.02.2015 התקבלה החלטת הממשלה מס' 2443 (להלן: החלטת הממשלה), שכותרתה "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר". החלטה זו היא המשך להחלטת הממשלה מספר 3611 מיום 07.08.2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי".
- 1.2. באותו מועד התקבלה גם החלטת ממשלה 2444 בעניין "קידום ההיערכות הלאומית להגנת הסייבר". במסגרת זו החליטה הממשלה על מדיניות כוללת בתחום הגנת הסייבר ועל הקמת רשות לאומית להגנת הסייבר במסגרת מערך הסייבר הלאומי במשרד ראש הממשלה.
- 1.3. החלטה זו נועדה לקדם את התפיסה הלאומית להגנת הסייבר, לטובת העלאה שיטתית ורציפה של רמת ההגנה במרחב הסייבר במדינת ישראל. ההחלטה מובילה לאסדרה לאומית בהגנת הסייבר ולהובלה ממשלתית בהגנת הסייבר כחלק מיישום האסדרה הלאומית וכמהלך של דוגמה לציבור ולמשק.
- 1.4. בהתאם להחלטת הממשלה, הכוונה והנחיה מקצועית בתחום הגנת הסייבר במשק ישראלי ישתלבו במערך הרגולציה הממשלתי. משמעותה של קביעה זו היא כי הגנה מפני מתקפות סייבר, העלולות לגרום לפגיעה בסביבה או בבריאות הציבור ובחיי אדם, תתבצע באמצעות כלי הרגולציה (לדוגמה – היתר רעלים שניתן מכוח חוק החומרים המסוכנים).
- 1.5. כדי לקבוע הוראות בתחום ההגנה מפני מתקפות סייבר, העלולות לגרום לפגיעה בסביבה, בבריאות הציבור או בחיי אדם, הוקמה במשרד להגנת הסביבה יחידת הגנה על מידע וסייבר בתעשייה (להלן: היחידה). היחידה תפעל בהנחיה מקצועית של הרשות הלאומית להגנת הסייבר.
- 1.6. היחידה עוסקת בפיתוח שיטות הכוונה והנחיה בהיבטי הגנת הסייבר, לרבות הגדרת המדיניות המגזרית ודרישות האסדרה, ומעניקה ליווי מקצועי שוטף ומענה לפניית מקצועיות, בהתאם למאפייני העסקים שהפעילות מכוונת אליהם (להלן – המגזר).



1.7. ההוראות במסמך זה נועדו לסייע ביישום החובה (הנקבעת בהיתרי רעלים) לקבוע הגנות שונות בתחום הסייבר. וביתר פירוט – מסמך זה כולל הוראות לביצוע מיפוי סיכונים, הערכות הסיכונים ויישום ההגנות הנדרשות.

1.8. יודגש כי המסמך משמש מדריך בסיס לקביעת הוראות לשם צמצום פוטנציאל הפגיעה בסביבה או בבריאות הציבור. לממונה חומרים מסוכנים סמכות להורות, באמצעות היתר הרעלים, על הוראות שונות מאלה הקבועות במסמך זה.

1.9. יודגש כי מסמך זה מהווה מדריך בסיס לקביעת הוראות לשם צמצום פוטנציאל הפגיעה בסביבה או בבריאות הציבור. לממונה חומרים מסוכנים סמכות להורות, באמצעות היתר הרעלים, על הוראות שונות מאלה הקבועות במסמך זה. התאמות פרטניות או שינויים ייעשו בתיאום עם הממונה על חומרים מסוכנים במחוז, ובתיאום עם אגף חירום במשרד להגנת הסביבה.

לשאלות בתחום העיסוק של מדריך זה ניתן לפנות אל כתובת דוא"ל:

cyber_industry@sviva.gov.il

יעקב דולמצקי,

גלעד בן ארי

מנהל יחידת הגנה על מידע וסייבר בתעשייה

ראש אגף חירום



תוכן העניינים

1.	1. הקדמה
4.	2. הגדרות ומושגים
8.	3. מטרת המסמך
8.	4. רקע – סביבה וסייבר
10.	5. רקע – הגנה על מידע וסייבר
15.	6. הסבר התהליך
17.	7. תכנון העבודה
17.	8. מיפוי תהליכים מסוכנים וסיכונים
18.	9. הערכת סיכוני הסייבר
21.	10. ניהול סיכונים
21.	11. מיפוי בקורות נדרשות
22.	12. השוואה בין מצב נוכחי לבקורות נדרשות ומיפוי פערים
22.	13. בניית תוכנית עבודה על בסיס מיפוי הפערים
23.	14. יישום תוכנית העבודה והודעה על גמר ביצוע
23.	15. פיקוח ומעקב שוטפים
23.	16. ביצוע מחודש של הערכת סיכונים וניהולם
23.	17. אישורים
24.	18. שינויים בנוהל
26.	נספחים
26.	א. נספח א' - מבט בעיני התוקף (Cyber Kill Chain)
27.	ב. נספח ב' - מיפוי תהליכים מסוכנים
27.	ג. נספח ג' - טבלה לקביעת מידת הנזק העלול להיגרם מאירוע סייבר אצל בעל היתר רעלים
31.	ד. נספח ד' - טבלה לקביעת מידת החשיפה של ארגון המחזיק חומ"ס
35.	ה. נספח ה' - רשימת בקורות והגנות נדרשות
94.	ו. נספח ו' - תחזוקה מרחוק – חיווי ובקרה



2. הגדרות ומושגים

- 2.1. **אירוע חומרים מסוכנים** - התרחשות בלתי מבוקרת או תאונה, שמעורב בה חומר מסוכן, הגורמת או העלולה לגרום סיכון לאדם ולסביבה, לרבות שפך, דליפה, פיזור, פיצוץ, התאיידות, דליקה.
- 2.2. **אירוע סייבר** - מתקפת סייבר היוצרת חשש או משפיעה הלכה למעשה השפעה שלילית (שיבוש או מחיקה של מידע הנשמר בהתקן תקשובי ו/או שיבוש או הפרעה או שיתוק של תפקודו התקין של התקן תקשובי אחד או יותר, עפ"י הגדרת הגורם האחראי לו) על תהליך ארגוני ובכלל זה תעשייתי/פיזי המתבסס על ההתקן ו/או על מערכת מידע ומערכות ממוחשבות.
- 2.3. **אבטחה פיזית** - האמצעים הפיזיים הנדרשים להגנה על ציוד המחשוב, לגישה למידע של הארגון ולשרידות המערכות הממוחשבות המכילות את מאגרי המידע.
- 2.4. **איום** - מפגע פוטנציאלי אשר עלול לפגוע בנכסים/במערכות ממוחשבות של ארגון במכוון או באקראי.
- 2.5. **המשרד** - המשרד להגנת הסביבה
- 2.6. **הזדהות** - תהליך המספק זיהוי מאומת של אדם או מחשב, באמצעות מידע ייחודי חד ערכי - לאדם או למחשב, רכיב הזדהות פיזי או תכונה שלו.
- 2.7. **הזדהות חזקה** - שיטת הזדהות המבוססת על שילוב של כמה מאפייני אימות:
- (1) משהו שאתה יודע: סיסמה
 - (2) משהו שיש לך: רכיב פיזי כגון טוקן או מחולל סיסמאות חד-פעמי
 - (3) מאפיין פיזי (משהו שאתה): טביעת אצבע, טביעת קשתית עין, צורת כף יד.
- 2.8. **זמינות המידע** - Availability - וידוא שלמשתמשים המורשים יש גישה למידע ולנכסים הקשורים בו, לפי הצורך. תפקוד המערכת באופן שוטף, ללא הפרעות או הפסקות זיהוי.



2.9. **חומר מסוכן (חומ"ס)** - רעל או כימיקל מזיק כפי שמפורט בחוק החומרים המסוכנים, התשנ"ג-1993 (במסמך זה – חוק החומרים המסוכנים).

2.10. **מידע** - כל נתון הנוגע ו/או הקשור לפעילותם, תפעולם או תפקודם של ארגונים, לרבות מידע הנוגע לצנעת הפרט ומידע ארגוני רגיש, הנמצא על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, מצעי מידע פיזיים וכן מידע המועבר בעל-פה.

2.11. **מתקפת סייבר** - פעולה התקפית הננקטת על ידי אדם, ארגון זר או מדינה על מנת לחדור למרחב הקיברנטי של היעד במטרה לגנוב ממנו מידע, לרוב בעזרת שימוש ברוגלה ובסוס טרויאני. מטרה נוספת היא לשבש את הפעילות במרחב הקיברנטי ולהסב לו נזק או למערכות אחרות המסתמכות עליו (כולל פגיעה בחומרה), לרוב באמצעות נזקה או קוד עיון.

2.12. **משאבים** – בסיסי נתונים, קבצים, מערכות, תוכניות, או אמצעים אחרים אשר כניסה אליהם מאפשרת גישה למידע ולמערכות ממוחשבות שברשות הארגון.

2.13. **מערכות מחשוב, מערכות ממוחשבות (ICS - Industrial Control System)** - מונח כללי המקיף כמה סוגים של מערכות בקרה המשמשים בייצור תעשייתי. מערכות אלה יכולות להיות מורכבות מהרכיבים האלה:

- 1) יחידות חיישנים ויחידות שליטה מקומית (sensors, actuators and intelligent electronic devices – IED)
- 2) יחידות בקרים מתוכנתים (programmable logic controllers) (PLC, remote terminal units - RTU)
- 3) תקשורת בין האתרים למרכז הבקרה (wide area communication network - WAN)
- 4) מרכז בקרה של כל התהליך (supervisory control and data acquisition - SCADA)
- 5) מחשבים לממשק אדם-מכונה (human machine interface- HMI)
- 6) מערכת ניהולית לשמירה על המידע (IMS- information management system)
- 7) מערכות בקרה מבחורות (distributed control systems - DCS)





2.14. **סייבר, מרחב סייבר, המרחב הקיברנטי או הסייברספייס** - ביטוי

בשפה האנגלית, אשר תרגומו לעברית הוא "סביבת רשת". מדובר במרחב מטפורי של מערכות מחשב ורשתות מחשב שנאגרים בו נתונים אלקטרוניים ומתבצעת תקשורת מקוונת ואינטראקטיבית ללא תלות במיקום הגיאוגרפי של המשתמשים בו.

2.15. **סיווג** - מדד המגדיר את רמת רגישות המידע והמערכות התומכות.

2.16. **סודיות המידע – Confidentiality** - הוא מידע שנקבע על ידי בעליו

שאין לגלותו לציבור, משום שחשיפתו עלולה לפגוע בארגון שהמידע בבעלותו. מקובל גם בארגונים ממלכתיים ועסקיים, ביחס למידע המהווה סוד מסחרי או שיש להגן עליו מסיבות אחרות, כגון חוקים ותקנות (למשל לשם הגנת הפרטיות).

2.17. **רשות** - הרשות הלאומית להגנת הסייבר.

2.18. **תורת ההגנה** – תורת ההגנה בסייבר לארגון של הרשות הלאומית להגנת הסייבר.



פרק א' – מטרה ורקע

3. מטרת המסמך

- 3.1. צמצום הסיכון לפגיעה בבריאות הציבור או בסביבה, באמצעות קביעת הוראות לעניין צמצום או מניעה של סיכון להתרחשות אירוע סייבר, אשר תגרום לאירוע חומרים מסוכנים, וכל זאת באמצעות:
- 3.2. הגדרת הוראות מקצועיות לעמידה בתנאי היתר רעלים בתחום ההגנה על מידע וסייבר, אשר ניתן לבעל היתר רעלים על ידי ממונה לפי חוק החומרים המסוכנים.
- 3.3. מזעור סיכוני פגיעה בפעילות הסדירה של מערכות מחשוב המפעילות ומבקורות תהליכי תפעול וייצור שאחראים לתפעול חומ"ס.
- 3.4. קביעת מסגרת לתהליכים המרכזיים בנושאי הגנת הסייבר, תוך יצירת תשתית לנהלים ולהוראות עבודה.
- 3.5. פישוט תהליך ההגנה על מידע ועל סייבר לכל הארגונים העוסקים בחומרים מסוכנים ללא קשר לגודלם, לסיכוני הסייבר שהם חשופים אליהם או לרמת היישום של אמצעי ההגנה שהם נוקטים.
- 3.6. סיוע לבעלי היתרי רעלים להפחית את סיכוני הסייבר שבארגון.

4. רקע – סביבה וסייבר

- 4.1. הגנה על מידע וסייבר בתחום חומרים מסוכנים
 - 4.1.1. כשל מערכות הייצור/שינוע/אחסון של בעל היתר הרעלים עלול לגרום לאירוע חומרים מסוכנים, ובעקבותיו לפגיעה בבריאות הציבור ובסביבה. מערכות אלו בדרך כלל מתופעלות ומבוקרות על ידי מחשב, ולכן הכשל יכול לנבוע מפעילות לא תקינה של המערכת ממוחשבת. מכאן שאירוע סייבר הגורם לכשל במערכת הממוחשבת עלול לגרום לאירוע חומרים מסוכנים.
 - 4.1.2. להלן כמה דוגמאות לאירועים סביבתיים שעלולים לקרות עקב אירוע סייבר:
 - שפך של חומר מסוכן נחל ללא שריפה, סיכון לזיהום קרקע ומי תהום.

- פיזור של חומרים מסוכנים מוצקים ללא שריפה.
- שריפת חומ"ס בשלושת מצבי הצבירה.
- אירוע חומ"ס – פליטת גזים.
- פיצוץ חומ"ס.
- שפך תעשייה למקור מים זורם/מערכת ניקוז.
- שפך תעשייה לשטח פתוח.
- שפך תעשייה למערכת הביוב (מאגרי מים/קולחין).

4.1.3. שיתוף מידע בין ארגונים ודיווח על אירועים ליחידת הגנה על מידע וסייבר בתעשייה במשרד להגנת הסביבה ובכלל זה ל-CERT הלאומי, יסייעו לגילוי מוקדם של התרחשות פוטנציאלית של אירוע סייבר. בכל אחד מהשלבים המוקדמים יוכל בעל היתר הרעלים לזהות את פוטנציאל התקיפה ולמזער את הנזק הפוטנציאלי.



5. רקע – הגנה על מידע וסייבר

5.1. מהי הגנה על מידע וסייבר?

5.1.1. הגנה על מידע וסייבר היא הגנה על מידע במרחב הקיברנטי מפני זליגת מידע מתוך המרחב או מפני תקיפות סייבר המכוונות לגנוב מידע, לשבש אותו או לפגוע בו. הגנת סייבר כוללת לעתים איסוף מודיעין על יריבים פוטנציאליים, שימוש בכלי ניטור לפיקוח על הפעילות בנכס ואיתור חולשות ארגוניות, אבטחתיות וקבצים מזיקים. כמו כן התחום כולל פעילות שתכליתה זיהוי מקור התקיפה וייעודה. חקירות מסוג זה יכולות להתבצע באמצעות פעילות אקטיבית ושימוש בכלים מחוץ למרחב שעליו מגינים.

5.2. כיצד מבוצעת ההתקפה בפועל?

5.2.1. על-מנת ליישם אבטחת סייבר יש להכיר היטב את המרחב הקיברנטי. אין להסתפק רק בהכרת סביבת ההגנה ונדרשת היכרות מעמיקה עם סביבת ההתקפה, עם הטכנולוגיות והטכניקות ועם הלך הרוח הכלכלי והפוליטי. יש להבין את שיטות הפצחות (Hacking) ומשמעותן, ואת כל השלבים בתהליך ההתקפה: החל בשלב איסוף המידע (חקירה ומודיעין), ריכוז כלי ההתקפה, החדירה, וכלה בשלב ה"ניקיון" שלאחר ההתקפה (House Keeping). מבחינה טכנולוגית, עולם התקיפה מורכב מסביבת המערכת (התקשורת, מסדי הנתונים, המכשירים הניידים, היישומים הרגילים והאינטרנט), מהתקפת הגורם האנושי (Social Engineering), ולבסוף - ממערכות מיוחדות במינן (משולבות).

להרחבה בנושא שלבי תקיפה טיפוסית ראו נספח א' שעניינו "מבט בעיני התוקף".

5.3. דוגמאות לתקיפות הסייבר:

- בשנת 2000 הייתה התקפת סייבר במערכת הביוב באוסטרליה, וגרמה להצפה של 1,000,000 קוב מי ביוב בשמורות הטבע באזור ולנזק סביבתי כבד.
- בשנת 2010 הייתה מתקפת סייבר במתחם הגרעין באיראן. מתקפה זו גרמה לשיבוש תשתיות קריטיות על ידי שינוי מהירות הצנטריפוגות במתחם, ועקב כך השתבש תהליך הייצור של האורניום המועשר. אין



ספק כי זאת הייתה מתקפה מאורגנת מטעם מדינה אחת או כמה מדינות.

(3) בסוף שנת 2015 דווח על תקלות ברשת החשמל בחלק ממערב אוקראינה. זאת לאחר ששובשה פעולתן של 27 תחנות חלוקה ושלוש תחנות כוח, מה שגרם לקריסה של אספקת החשמל ובתים רבים נותקו מהרשת. מהתחקיר שנעשה בסיוע של מדינות אירופיות, עלה שזאת לא הייתה הפסקת חשמל שגרתית, אלא התקלה נגרמה ממתקפת סייבר.

5.3.1. אירועי סייבר שהתרחשו בתעשייה העולמית בשנים האחרונות הוכיחו שוב ושוב שהאיומים והנזק הנגרם מהם גדלים במהירות. מוכנות בעל היתר רעלים לאירוע סייבר היא צעד חשוב וחיוני בניתוח סיכונים ובהתמודדות עם תרחישי האיום, אשר עלולים לגרום לפגיעה בסביבה או בבריאות הציבור.

5.3.2. במתקפת סייבר גורמים זדוניים מנצלים חולשות של נכס מידע מסוים לצורך ביצוע המתקפה. חשוב לדעת, שרוב המתקפות על מערכות מידע וסייבר הן משולבות ויכולות להתבצע בשלושה רבדים בד בבד:

(1) **רובד פיזי** - גישה פיזית לרכיבי התקשוב: מחשבים, נתבים, מתגים, בקרים תעשייתיים וכו'.

(2) **רובד לוגי** - גישה לוגית למערכות IT או למערכות ICS ממוחשבות.

(3) **רובד אנושי** - משתמשי מערכות מידע ומערכות ממוחשבות שיכולים לגרום להן נזק בזדון או בשוגג.

5.3.3. על מנת להיות מוכן לאירוע סייבר, בעל היתר הרעלים צריך להכיר את נכסי המידע שבארגונו ואת מערכות הבקרה, ולהבין את הנזק הפוטנציאלי שעלול להיגרם ממתקפות סייבר.

5.3.4. אנשי מקצוע בארגון יכולים להסתייע בחברה המייעצת בנושא הגנה על מידע וסיכול איומי סייבר, על מנת להכיר את מערכות ההגנה על מידע וסייבר, ולדעת לתכנן ולתפעל אותן כהלכה. עליהם להכיר שיטות תקיפה אפשריות, מקורות איום, יריבים אפשריים ויכולותיהם, וכן לתת פתרונות לאיומי סייבר.



5.3.5. בעל היתר הרעלים צריך לפתח את שיטות ההגנה על מנת לצמצם סיכון לאירוע חומרים מסוכנים, ולהציע דרכי התמודדות בזמן האירוע לפי סוגו.

5.4. יריבים פוטנציאליים

5.4.1. בהתאם למיפוי איומי סייבר בתחום עיסוק בחומרים מסוכנים, יחידת הגנה על מידע וסייבר בתעשייה במשרד להגנה"ס מגדירה את הסוגים ליריבי סייבר:

- מדינות עימות או מדינות בעלות אינטרסים שונים;
- גורמי פח"ע וג'יהאד עולמי;
- גורמים אנרכיסטיים ("אנונימוס", תנועות אנטי גלובליזציה וכו');
 - פשע מאורגן ישראלי ובין-לאומי;
 - קבוצות מאורגנות של האקרים;
 - גורם מסחרי מתחרה;
 - גורם פנימי בארגון (עובד, ספק שירות, שותף עסקי) הפועל בזדון או בשגגה;
- גורם בשרשרת האספקה;
- גופים בעלי אינטרסים ובעלי יכולות – אנשי תקשורת, חוקרים פרטיים;
- אדם אקראי או גורם אחר בעל יכולת זדונית;

5.5. דרכי פעולה של יריבים

5.5.1. הנחת העבודה היא שהיריב יכול להיות בעל ידע מעמיק במבנה המערכת, וייתכן שהוא משתמש מורשה במערכת הממוחשבת.

5.5.2. להלן דוגמאות לדרכי פעולה של יריבים:

- שימוש בפגמים בתוכנה/בחומרה/בתצורת המערכת הממוחשבת או במערכת שמגינה עליה.
- השתלת תוכנה זדונית למערכת ממוחשבת
- פריצת מערכת ממוחשבת דרך האינטרנט
- פריצה באמצעות שירותי מיקור חוץ
- ניצול חולשות בשרשרת אספקה



- השבתת מערכות המחשוב של עסק
- הצפנת מידע ודרישת כופר
- מתקפות סייבר על ספקי שירותי התקשורת/המחשוב או שיבוש הממשק עם המערכת הממוחשבת - ICS
- מתקפה על כמה מערכות בעסק אחד או בעסקים שונים בו זמנית.
- שימוש בעובד פנימי בעסק להשגת המטרה ללא ידיעתו (שימוש בהנדסה חברתית)
- שיתוף פעולה עם עובד פנימי בעסק לצורך מתקפת סייבר או מתקפה על ידי עובד פנימי
- גישה פיזית לתחנות/בקרים/שרתים/ציוד תקשורת של גורם מורשה/לא מורשה

5.6. כשלים במערכות ממוחשבות - ICS

5.6.1. כשלים בתוכנה או בחומרה עקב אירועי סייבר, אירועים סביבתיים, הזדקנות או נסיבות אחרות, עלולים לגרום לתקלות במערכות ICS ולמימוש תרחיש סביבתי או פגיעה בבריאות הציבור או בחיי אדם. דוגמאות לכשלים מערכתיים:

- כשל טכנולוגי במערכות מידע וציוד (IT)
- כשל תהליכי
- כשל במערכות שמירה ועיבוד נתונים (DATA)
- כשל בתקשורת נתונים
- כשל בהצגת נתונים (Data Output)
- כשל בבקרים
- כשל בחיישנים
- כשל סביבתי, לדוגמה: שינויים בטמפרטורה/לחות
- כשל באספקת חשמל
- כשל בתוכנה
- כשל במערכת הפעלה

5.7. אסונות טבע וסביבה



5.7.1. אסונות טבע וסביבה יכולים לגרום נזק לתשתיות קריטיות של הארגון. בעל היתר הרעלים צריך להיערך לאירועים מסוג זה ולמזער את השפעת האירוע ואת הנזקים האפשריים. אסונות טבע יכולים להיות מאופיינים גם מבחינת החומרה ו/או משך הזמן שלהם. דוגמאות לאסונות טבע וסביבה:

- אסון טבע או אסון טכנוגני (עקב פעילות אדם)
- שריפה
- הצפה/צונאמי
- רוחות סוערות/טורנדו/הוריקן
- רעידת אדמה
- פיצוץ
- אירוע טבעי חריג (למשל: כתמי שמש)
- קריסת תקשורת/מערכת חשמל



פרק ב' – תהליך

6. הסבר התהליך

6.1. שלבי העבודה ודרישות כלליות

6.1.1. מסמך זה קובע דרישות והנחיות הנוגעות לביצוע סקרים, סיווגים,

תכנון וביצוע של הוראות לעניין הגנה על מידע או על תהליכים מפני מתקפת סייבר, לבעל היתר רעלים, ביחס לתהליכים מוסדרים.

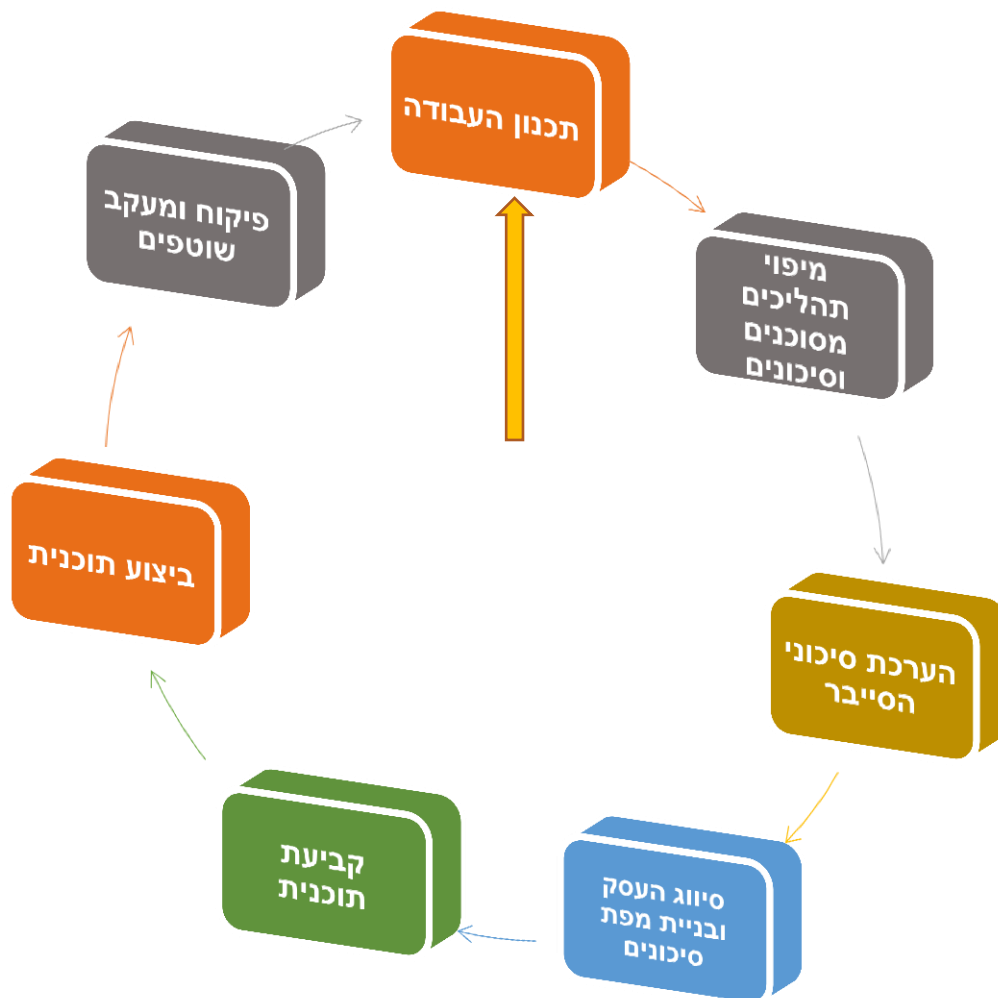
6.1.2. כל שלבי התהליך כפי שיפורטו להלן (ובכלל זה הבדיקות,

החישובים, התכנון והביצוע) ייעשו בהתאם לתורת ההגנה לארגון, אשר נכתבה על ידי הרשות הלאומית להגנת הסייבר.¹ התהליך כפוף להנחיות מפורטות במסמך זה ולתקנים ישראליים רלוונטיים עדכניים, החלים על מבני תעשייה, אשר פגיעה בהם עלולה לסכן אוכלוסייה רחבה ואת הסביבה כולה. כמו כן הוא מבוסס על מדריך המכון הלאומי לתקנים וטכנולוגיה של ארה"ב, בעניין אבטחת מערכות בקרה ממוחשבות בתעשייה, תוך התאמה לדרישות הייחודיות הנוגעות לאסדרה של פעילות מפעלי חומרים מסוכנים.

6.1.3. יודגש כי במקרה של סתירה או אי התאמה בין הוראות אלה

למסמכים אחרים, לרבות תורת ההגנה ומדריך המכון הלאומי לתקנים וטכנולוגיה של ארה"ב, הוראות מסמך זה גוברות, ויש לבצען.

6.2. שלבי יישום ההנחיות



תרשים זה מציג תהליכי פעולה מחזוריים. אם לא היה שינוי בתהליכים בארגון ולא נוסף תהליך חדש, אין צורך לבצע מיפוי תהליכים מסוכנים חדש, וניתן להשתמש במיפוי תהליכים שכבר בוצע.



7. תכנון העבודה

- 7.1. הפעילות להגנה על מידע וסייבר צריכה להיות חלק בלתי נפרד מהתרבות הארגונית. המחויבות של בעל היתר הרעלים ושל הנהלת הארגון ליישום דרישות הגנה על מידע וסייבר צריכה להיות חלק מהתרבות הארגונית. על בעל היתר הרעלים להתוות מדיניות ונהלים לניהול סיכונים במערכות ממוחשבות שפגיעה בהן עלולה לגרום לאירוע חומרים מסוכנים. יש להקצות משאבים, למנות בעלי תפקיד לניהול אירועי הגנה על מידע וסייבר, לקבל ייעוץ חיצוני, ולהתוות מדיניות פתוחה וגלויה של שיתוף מידע פנים ארגוני בין העובדים להנהלה בנוגע לסיכונים.
- 7.2. לפיכך, לשם יישום הוראות הגנת מידע וסייבר לבעל היתר רעלים, יש להקפיד על גיוס העובדים הרלוונטיים, לקבל ייעוץ מקצועי רלוונטי, להקצות משאבים לנושא (כוח אדם, תקציב, זמן), ולהיערך לתחילת ביצוע ההוראות שבמסמך זה.
- 7.3. השלב הראשון בביצוע ההוראות המסמך הוא תכנון מוקדם של העבודה על כל שלביה, תוך הקצאת המשאבים הנדרשים ליישומה, והכול בהתאם ללוחות הזמנים שנקבעו.

8. מיפוי תהליכים מסוכנים וסיכונים

- 8.1. כאמור, מטרת מסמך זה היא למנוע אירוע חומרים מסוכנים. לפיכך על העסק לזהות תהליכים המתרחשים בו ומעריכים חומרים מסוכנים. פגיעה בתהליכים אלה עלולה לגרום לאירוע חומרים מסוכנים, ולכן מיפוי התהליכים הוא חיוני.
- 8.2. השלב השני ביישום התהליך הוא אפוא מיפוי תהליכים בארגון שעלולים לגרום לאירוע חומרים מסוכנים ולפגוע בבריאות הציבור או בסביבה.
- 8.3. בעזרת מידע זה יקבל העסק החלטות לגבי היקף המשאבים, הנכסים והמערכות הנוגעים לתהליכים מסוכנים שבהם נדרש ליישם ולהטמיע מערכות ובקורות להגנה על מידע וסייבר.

8.4. מיפוי מערכות טכנולוגיות חיוניות לתהליכים מסוכנים

- 8.4.1. יש לבצע מיפוי מדויק של כלל המערכות והתשתיות הטכנולוגיות החיוניות לתהליכים מסוכנים. המיפוי יתייחס בין היתר למערכות מידע ארגוניות, מערכות ממוחשבות בתעשייה, מאגרי מידע,



יישומים (אפליקציות), מערכות מתח נמוך ונכסים טכנולוגיים אחרים. בין אלה: מערכות הפעלה, חומרות, מולטימדיה, רשתות תקשורת, ציוד, תשתיות, בעלי תפקידים שעובדים עם המערכות הללו וכדומה.

8.4.2. על הארגון להכין מפת סטטוס שתכלול את הנכסים הטכנולוגיים שיש בארגון בהקשר של תהליכים מסוכנים.

8.4.3. מיפוי תהליכים מסוכנים ביחס לחומרים המסוכנים שבהם עוסק העסק, יצוין על גבי הטבלה המפורטת בנספח ב' למסמך זה.

8.4.4. הפעילות לפי מסמך זה תימשך רק ביחס לתהליכים שיש סכנה שיפגעו בסביבה או בבריאות הציבור, בהתאם לממצאי המיפוי.

9. הערכת סיכוני הסייבר

9.1. ניהול הסיכונים מושתת על הערכת סיכונים המשקפת את מידת פגיעותן של מערכות ממוחשבות, הערכת האיומים, השלכותיהם ומידת ההיתכנות שלהם.

9.2. הערכת סיכונים תתבצע ברובה בהתאם לתורת ההגנה בסייבר לארגון של הרשות הלאומית להגנת הסייבר, עם **התאמות ייחודיות** לתחום החומרים המסוכנים ומערכות בקרה תעשייתיות. הפרטים ורמת התחכום של הערכת הסיכונים בארגון יתאימו לגודלו ולפעילותו העסקית.

9.3. הערכת סיכונים תתבסס על עקרון "מבט בעיני התוקף" - היות שמאחורי המתקפה עומד תוקף אנושי, הדרך לפתרון מיטבי לאבטחת סייבר מחייבת הבנה עמוקה של דרכי פעולתו של התוקף, זיהוין ומניעתן. להרחבה בנושא זה ניתן לעיין במסמך "הסתכלות בעיני התוקף" (או הגנה מוכוונת מודיעין) מאת משרד ראש הממשלה (המרכז הלאומי להתמודדות עם איומי סייבר) (ראו נספח א').

9.4. הסיכונים מבוססים על האיומים הרלוונטיים לרכיבי כל מערכת, בהתאם לניתוח הסיכונים שנעשה בארגון.



9.5. הערכת הסיכונים

9.5.1. הערכת סיכונים מתחילה בבדיקת **רמת הנזק** שעלול להיגרם לסביבה או לבריאות הציבור, אם יהיה אירוע סייבר בארגון. מידת הנזק תנותח לפי הטבלה המופיעה בנספח ג' למסמך זה, ביחס לכל תהליך שנכלל במיפוי תהליכים מוסדרים וביחס לכל מערכת ממוחשבת הנוגעת לכל אחד מהתהליכים.

9.5.2. מידת הנזק תוערך בטווחים שבין 1 ל-4, לפי השיטה המוצגת בטבלה שבנספח ד' במסמך זה.

9.5.3. יש לשים לב כי הציון שנקבע בשלב זה הוא לפי הערכת הנזק **המקסימלית**.

9.5.4. לאחר שנקבעה רמת הנזק הצפויה במקרה של אירוע סייבר בעסק, ביחס לכל תהליך מוסדר וביחס לכל מערכת ממוחשבת שנעשה בה שימוש בתהליכים מוסדרים, **יש לקבוע את רמת החשיפה של המערכות הממוחשבות שנעשה בהן שימוש בתהליכים מוסדרים בעסק**.

9.5.5. לאחר שנקבעה רמת הנזק הצפויה במקרה של אירוע סייבר בעסק, ביחס לכל תהליך מוסדר וביחס לכל מערכת ממוחשבת בה נעשה שימוש בתהליכים מוסדרים, יש לקבוע את **רמת החשיפה של המערכות הממוחשבות בהן נעשה שימוש בתהליכים מוסדרים בעסק. קביעה זו מתבצעת בהתאם לשיטה המוצגת בטבלה המופיעה בנספח ד למסמך**.

9.5.6. ניתוח רמת החשיפה, באמצעות הטבלה בנספח ד', יהיה ביחס לכל תהליך מוסדר וביחס לכל מערכת ממוחשבת שנעשה בה שימוש בתהליך מוסדר.

9.6. קביעת הערכת הסיכון וסיווג המערכות בעסק

9.6.1. הערכת הסיכון תהיה מבוססת על שקלול מידת הנזק הצפויה עם הסיכוי שהנזק יתרחש, בהתאם לנוסחה להלן:

הערכת הסיכון של מערכת ממוחשבת שנעשה בה שימוש במסגרת הליך מוסדר = $(P) + 3*(I)$

(I) = מידת הנזק הצפויה (לפי תוצאות
הניתוח בהתאם לנספח ג').
(P) = הסיכוי שהנזק יתרחש (הממוצע
המתקבל מהחישוב בהתאם לנספח ד'); ;

9.6.2. יישום הנוסחה המפורטת לעיל יכול לייצר למערכת ממוחשבת ניקוד של 4-16.

9.6.3. כל אחת מהמערכות הממוחשבות תסווג בעסק (המעורבות בהליכים מוסדרים) תסווג לאחת מ-4 קבוצות, לפי הערכת הסיכון שלה, כמפורט להלן:

1. : פוטנציאל נמוך (ניקוד 4-7);
2. : פוטנציאל בינוני (ניקוד 8-11);
3. : פוטנציאל גבוה (ניקוד 12-14);
4. : פוטנציאל גבוה מאוד (ניקוד 15-16).

ובהתאם לטבלה:

1	2	3	4	הסתברות (P) עוצמה (I)
7	10	13	16	4
6	9	12	15	3
5	8	11	14	2
4	7	10	13	1



10. ניהול סיכונים

- 10.1. רמת ניהול הסיכונים של כל מערכת ממוחשבת בעסק ורמת ההגנות הנדרשת ביחס אליה, תיקבע על פי הציון שקיבלה המערכת.
- 10.2. מכל אלה ייגזרו דרכי הטיפול בממצאים, החלופות, דחיפות יישום ההמלצות והקצאת המשאבים.
- 10.3. לאחר מכן נדרש העסק לפעול באופן המפורט להלן (ראו הרחבה ופירוט בפרקים הבאים):
- 10.3.1. מיפוי בקורות נדרשות;
- 10.3.2. השוואה בין מצב נוכחי לבקורות נדרשות, ומיפוי פערים;
- 10.3.3. על בסיס מיפוי הפערים תיבנה תוכנית עבודה להשלמת הפערים;
- 10.3.4. אישור התוכנית והקצאת משאבים (תקציב, כ"א);
- 10.3.5. יישום התוכנית;
- 10.3.6. הודעה על גמר ביצוע.

11. מיפוי בקורות נדרשות

- 11.1. בהתאם לסיווג המערכות לפי קבוצה (1-4) כאמור בפרק 9 במסמך זה, נדרש העסק לעשות את הבקורות המתאימות לכל מערכת ממוחשבת, לפי הטבלה בנספח ה', המפרטת את רשימת הבקורות הנדרשות לפי סיווג המערכת. בעבור כל מערכת יש לממש את סך כל הבקורות שהערך שלהן קטן מציון המערכת או שווה לו. כך למשל, למערכת שציונה 3 נדרש ליישם את הבקורות שערך 1, 2 ו-3.
- 11.2. יש לשים לב כי הטבלה שבנספח ה' האמור כוללת לצד פירוט הבקורות הנדרשות גם הסברים והמלצות ל בעל העסק.
- 11.3. הגדרה זו מסייעת להתאים את הבקורות הנדרשות ליישום ביעד ההגנה, אל מול פוטנציאל הנזק.



12. השוואה בין מצב נוכחי לבקורות נדרשות ומיפוי פערים

12.1. אל מול רשימת בקורות ההגנה המפורטות בנספח ה, יש לבדוק מה מיושם כיום ביחס לכל אחת מהמערכות, ומה נדרש לבצע. בסיום תהליך זה, העסק יקבל רשימת פערים - "רצוי מול מצוי".

12.2. יש להקפיד כי בעסק נעשית בדיקה פרטנית לגבי כל מערכת ממוחשבת שנעשה בה שימוש במסגרת הליך מוסדר, לעניין ביצוע הבקורות הנדרשות לגבי אותה מערכת.

12.3. רשימת הפערים המתקבלת היא הבסיס לבניית תוכנית העבודה של העסק.

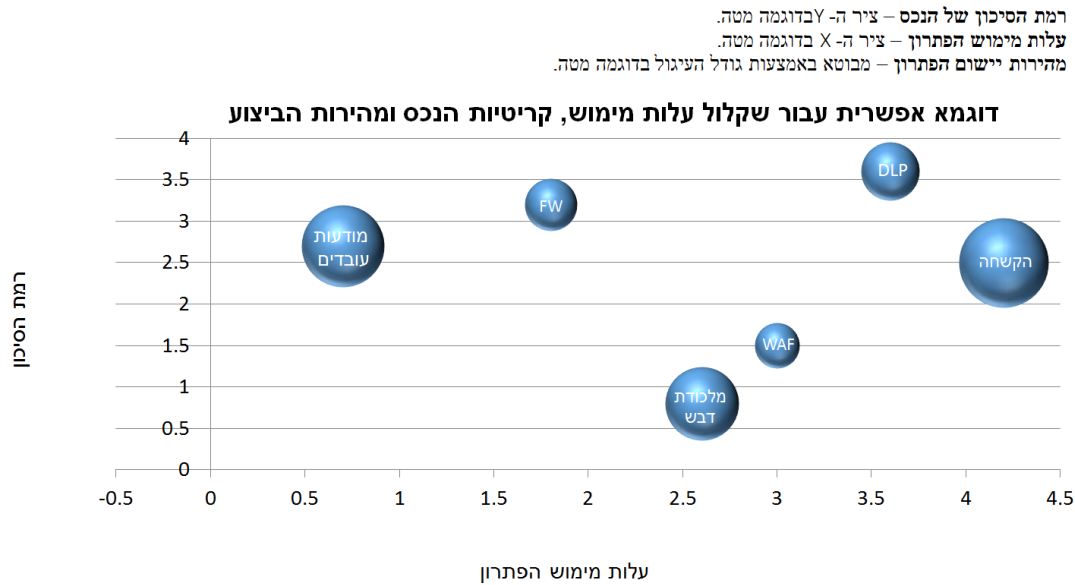
12.4. דוגמה לטבלת השוואה בין מצב נוכחי ובין בקורות נדרשות :

מקרה	מערכת קירור באמוניה	מערכת ייצור חומרים
12.6 אין לחבר התקנים שאינם בקרי סביבת ייצור לרשת בקרי הייצור	קיים, אין צורך בפעולה נוספת	יש פער, נדרש לממש

13. בניית תוכנית עבודה על בסיס מיפוי הפערים

13.1. באחריות העסק לגבש תוכנית ליישום ההמלצות, תוך ציון הגורמים האחראים, לוחות הזמנים ודרכי הטיפול. העסק יקצה לצורך היישום משאבי תקציב, כוח אדם וזמן .

13.2. סדר העדיפויות של יישום הבקורות החסרות לעסק במסגרת תוכנית העבודה ייקבע על-ידי שקלול רמת הסיכון של הנכס, בעלות הפתרון ובמורכבות המימוש, לפי השרטוט המוצג להלן:



14. יישום תוכנית העבודה והודעה על גמר ביצוע

14.1. תוכנית העבודה תיושם על פי המועדים ואבני הדרך שנקבעו בה, ובהתאם להוראות הממונה.

15. פיקוח ומעקב שוטפים

15.1. העסק יקבע שיטה ויקצה משאבים נדרשים לפיקוח, בקרה ומעקב שוטפים על המערכות הממוחשבות ששימוש בהן מהווה סיכון לאירוע חומרים מסוכנים.

16. ביצוע מחודש של הערכת סיכונים וניהולם

16.1. תהליך העבודה המפורט במסמך זה יבוצע מחדש במקרים האלה:
16.2. מדי שלוש שנים, ממועד התחלת תהליך המיפוי והערכת הסיכונים הראשוניים;
16.3. בעת התקנת מערכת ממוחשבת חדשה שבה נעשה שימוש בהליך מוסדר;
16.4. בשל שינוי מהותי במערכת ממוחשבת שבה נעשה שימוש בהליך מוסדר.

17. אישורים



מהדורה	שם	תפקיד	סימוכין	תאריך
0.1	גלעד בן ארי	מנהל חירום, המשרד להגנ"ס		
0.1	שולי נזר	סמנכ"לית בכירה – אשכול תעשיות, המשרד להגנ"ס		
0.1	ישראל דנציגר	מנכ"ל המשרד להגנ"ס		

18. שינויים בנוהל

מהדורה	תאריך	אחראי	מאשר	מהות השינוי
0.1				טיוטה ראשונית





נספחים

א. נספח א' - מבט בעיני התוקף (Cyber Kill Chain)

גילוי מתקפת סייבר בכל אחד מהשלבים המוקדמים יאפשר לבעל היתר הרעלים לזהות את פוטנציאל התקיפה ולמזער את הנזק המרבי. בשנת 2011 פרסמה החברה האמריקנית לוקהיד מרטין מאמר אשר סוקר את התהליך של יריב מתקדם בעת תקיפה בסייבר אל יעדיו. סקירה זו נחשבת לאבן דרך משמעותית בחשיבה על הגנה בסייבר, ועודדה ארגונים וגופי הגנה רבים לתכנן את הגנתם לפי צעדי היריב ולהשיג מודיעין מתאים על כל שלב. מודל זה מתאר 7 שלבי תקיפה מרכזיים שתוקף מבצע בשלבי התקיפה:



גילוי תקיפת סייבר בכל אחד מהשלבים המוקדמים יאפשר לבעל היתר הרעלים לזהות את פוטנציאל התקיפה ולהפחית ואף למזער את הנזק המרבי.



ב. נספח ב'- מיפוי תהליכים מסוכנים

מס'	שם החומר	מס' CAS	מס' בהיתר רעלים	כמות מאושרת בהיתר רעלים	האם נכלל בתהליך שמופעל באופן דיגיטלי/מחשובי?	הסבר על התהליך המסוכן (שלבי התהליך, מטרותיו, אופן הביצוע)	פירוט מערכות מחשב/תהליך דיגיטלי המעורבים בתהליך המסוכן	פוטנציאל פגיעה בבריאות הציבור או בסביבה
-----	----------	---------	-----------------	-------------------------	--	---	--	---

ג. נספח ג'- טבלה לקביעת מידת הנזק העלול להיגרם מאירוע סייבר אצל בעל היתר רעלים

יש לקבוע את מידת הנזק העלול להיגרם מאירוע סייבר לכל אחת ממערכות המחשוב המעורבות בתהליך מסוכן, לפי אחת משלוש קטגוריות:

1. פגיעה בסודיות הנתונים – לדוגמה, תקיפת סייבר לצורך הדלפת נתונים ממערכות ממוחשבות של העסק הארגון החוצה אל האינטרנט.
2. פגיעה באמינות הנתונים - לדוגמה, תקיפת סייבר המשנה את נתוני אחסון החומרים המסוכנים בעסק, או משנה תנאים בראקטור.
3. פגיעה בזמינות הנתונים – לדוגמה, תקיפת סייבר הגורמת לכך שהמידע אינו זמין לחברה או ללקוחותיה (למשל בעת נפילת מערכת ממוחשבת העוסקת בתהליך מסוכן או נעילת קבצים/כופרה).

יש לענות על השאלות המפורטות בטבלה מטה ולתת ציון מ-1 עד 4 על פי הנזק שייגרם בעקבות אירוע סייבר. זאת לכל מערכת מחשוב שנעשה בה שימוש במסגרת הליך חומרים מסוכנים.

מידת הנזק הצפויה לגבי כל מערכת תיקבע על פי הציון הגבוה שהתקבל מבין כלל הציונים שניתנו, בהתאם לנוסחה: $I = \text{Max}(1-3)$.

קריטריון הקבילות שקבע המשרד מתייחס לנקודות קצה לחומרים רעילים, דליקים ופציצים. נקודת הקצה (endpoint) לחומרים רעילים מבוססת על המערכת האמריקנית (Protective Action Criteria) PAC - מערכת ערכי הסיכון לחומרים רעילים הנחלקת לשלוש רמות:



- **PAC1** = הריכוז באוויר שגורם תסמינים חולפים והפיכים לאדם לא ממוגן הבא עימו במגע במשך שעה.
- **PAC2** = הריכוז באוויר שגורם תסמינים חמורים, בלתי הפיכים או פגיעה ביכולת המילוט לאדם לא ממוגן הבא עימו במגע במשך שעה.
- **PAC3** = הריכוז באוויר שגורם סכנת מוות לאדם לא ממוגן הבא עימו במגע במשך שעה.

חשוב: מערכת PAC אינה מתייחסת לחומרים פציצים ודליקים.

תרחיש הייחוס ינותח באמצעות תוכנת ALOHA, אלא אם כן הוגדרה דרך חישוב חלופית כמצוין בפרק ההנחיה המקצועית. התוכנה מבוססת על מודל המחשב את המרחק בין מקום פריצה אפשרי של החומר המסוכן לסביבה ובין הנקודה המרוחקת ביותר שעדיין יש בה סכנה ניכרת לשלום הציבור.

שיטת חישוב מידת הנזק מתייחסת לפגיעה בבריאות הציבור או בחיי אדם של כל אדם במרחק הפגיעה עקב אירוע חומרים מסוכנים.

שאלה	1	2	3	4
	הנזק מוערך כאחד או יותר מהקריטריונים להלן:			
מהי מידת הנזק לבריאות ציבור או לסביבה שעלולה להיגרם עקב חשיפת מידע קשיח או ממוחשב שנמצא בבעלות העסק?.	1. פוטנציאל לדליפת חומרים רעילים ללא פגיעה משמעותית בבריאות הציבור 2. פגיעה בסביבה שהיא הפיכה בזמן קצר	1. פוטנציאל פגיעה בבריאות הציבור ב-PAC 1 2. פוטנציאל לשרפה/פיצוץ חומרים מסוכנים ללא פגיעה בבריאות הציבור. 3. פוטנציאל לפגיעה לטווח ארוך בשטח של 500 מ"ר עד 5000 מ"ר של שמורת טבע / מינים מוגנים	1. פוטנציאל פגיעה בבריאות הציבור ב-PAC 2 או 3 2. פוטנציאל פגיעה בבריאות הציבור עקב שרפה/פיצוץ של חומרים מסוכנים. 3. פוטנציאל לפגיעה בבריאות הציבור עקב שינויים בתהליך ייצור שלא צוינו בסעיפים 1 ו-2 4. פוטנציאל לפגיעה	העסק מוגדר תשתית מחשוב קריטית בהתאם לחוק הסדרת הביטחון בגופים ציבוריים
מהי מידת הנזק				



שאלה	1	2	3	4
שייגרם לבריאות הציבור או לסביבה בעקבות שיבוש המידע ברכיב התעשייתי או בתהליך OT או שיבוש התהליך שהרכיב התעשייתי הוא חלק בלתי נפרד ממנו ?		בחקיקה. 4. פוטנציאל לפגיעה לטווח ארוך בשטח 1,000 מ"ר עד 10,000 מ"ר של שטחים מכל סוג לרבות שטחים חקלאיים. 5. פוטנציאל לפגיעה במי תהום / אקוויפר בשטח 100 מ"ר עד 1,000 מ"ר. 6. פוטנציאל לפגיעה בנהר/אגם/מי ים בשטח 100 מ"ר עד 1,000 מ"ר	בבריאות הציבור עקב שינוי מיקום או תנאי אחזקה של חומרים מסוכנים 5. פוטנציאל לפגיעה לטווח ארוך בשטח של 5,000 מ"ר ויותר של שמורת טבע / מינים מוגנים בחקיקה. 6. פוטנציאל לפגיעה לטווח ארוך בשטח 10,000 מ"ר ויותר של שטחים מכל סוג לרבות שטחים חקלאיים. 7. פוטנציאל לפגיעה במי תהום / אקוויפר בשטח 1,000 מ"ר ויותר. 8. פוטנציאל לפגיעה בנהר/אגם/מי ים בשטח 1,000 מ"ר ויותר.	
מהי מידת הנזק שעלול להיגרם לבריאות הציבור או לאיכות הסביבה בעקבות השבתת הרכיב התעשייתי או תהליך ממוחשב?				

סיכום:

שם הבודק	תפקיד	חתימה	תאריך	ציון רמת חשיפה





ד. נספח ד' - טבלה לקביעת מידת החשיפה של ארגון המחזיק חומ"ס

בטבלה זו יש לענות על כל 42 השאלות שבעמודת "פרמטר נבדק", ע"י מתן ציון מ-1 עד 4. לאחר מתן ציונים לכל השאלות יש לחשב את מידת החשיפה על ידי סיכום כל הציונים וחישוב ממוצע לכל הטבלה. התוצאה המתקבלת היא מידת החשיפה – P.

יש לבצע את הניתוח שלפי טבלה זו ביחס לכל תהליך המצוין במיפוי התהליכים המוסדרים, וביחס לכל מערכת ממוחשבת הנוגעת לכל אחד מתהליכים אלה.

מידת חשיפה				פרמטר נבדק
4	3	2	1	
יותר מ-50	50-10	10-5	עד 5	1. מספר העובדים החשופים למערכות אדם - מכונה (HMI)
יותר מ-50	50-25	25-10	עד 10	2. מספר העובדים החשופים למערכות הבקרה התעשייתיות (ICS)
יותר מ-50	50-25	25-10	עד 10	3. מספר העובדים החשופים לרכיבים בשטח המשפיעים על חומרים מסוכנים (ברזים, וסתים, שסתומים וכדומה)
נגישות לגורמים נוספים	ספקים חיצוניים מזדמנים	ספקים חיצוניים קבועים	רק עובדים פנימיים	4. אחריות הטיפול במערכות אדם - מכונה (HMI)
נגישות לגורמים נוספים	ספקים חיצוניים מזדמנים	ספקים חיצוניים קבועים	רק עובדים פנימיים	5. אחריות הטיפול במערכות הבקרה התעשייתיות (ICS)
נגישות לגורמים נוספים	ספקים חיצוניים מזדמנים	ספקים חיצוניים קבועים	רק עובדים פנימיים	6. אחריות הטיפול ברכיבים בשטח שמשפיעים על חומרים מסוכנים (ברזים, וסתים, שסתומים וכדומה)
יותר מ-10	10-5	5-2	1	7. מספר עמדות אדם – מכונה (HMI) במפעל
יותר מ-50	50-10	10-5	עד 5	8. מספר מערכות הבקרה התעשייתיות (ICS) במפעל
יותר מ-100	100-50	50-20	עד 20	9. מספר הרכיבים בשטח שמשפיעים על חומרים מסוכנים (ברזים, וסתים, שסתומים וכדומה) שיש במפעל



מידת חשיפה				פרמטר נבדק
4	3	2	1	
יש ללא אמצעי בקרה	יש באמצעות חומת אש בלבד	יש באמצעות חומת אש ודיודה חד כיוונית	אין	10. תקשורת בין רשת מנהלית לרשת תפעולית
כן	כן, אך עם בקרת חומת אש וסינון תוכן או רכיבי אבטחה נוספים	יש חיבור, אבל הוא בדרך כלל מנותק. מופעל לצורך תמיכה מרחוק	לא	11. האם מאופשרת גישה לאינטרנט מסביבת הבקרים התעשייתיים?
לא	כן במידה חלקית מאוד	כן במידה רבה	כן בצורה מלאה	12. האם יש חציצה בתוך רשת מערכות הבקרה התעשייתיות בין הרכיבים (מערכות אדם- מכונה, שרתי ניהול, רכיבי סקאדה וכדומה)?
לא מתבצע	מתבצע באופן מועט	מתבצע באופן רחב	מתבצע באופן מלא וקבוע	13. עדכון קושחה אם יש במערכות (ממשקי אדם מכונה, רכיבי בקרה, רכיבי שטח כגון ברזים, וסתים, שסתומים וכדומה)
לא מתבצע	מתבצע באופן מועט	מתבצע באופן רחב	מתבצע באופן מלא וקבוע	14. עדכון תוכנה אם יש במערכות (ממשקי אדם מכונה, רכיבי בקרה, רכיבי שטח כגון ברזים, וסתים, שסתומים וכדומה)
נגישות לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	15. אבטחה פיזית למערכות אדם - מכונה (HMI)
נגישות לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	16. אבטחה פיזית למערכות הבקרה התעשייתיות (ICS)
נגישות לגורמים נוספים	נגישות לספקים חיצוניים מזדמנים	נגישות לספקים חיצוניים קבועים	נגישות לגורמים מורשים בלבד	17. אבטחה פיזית לרכיבים בשטח שמשפיעים על חומרים מסוכנים (ברזים, וסתים, שסתומים וכדומה)
1	2	3	4	18. אמצעי מיגון ואבטחה פיזית במתקן כולו מתוך הארבעה האלה : מצלמות, מערכת



מידת חשיפה				פרמטר נבדק
4	3	2	1	
				אזעקה, גישה ביומטריה, מאבטחים
אין	1	2	3 ויותר	19. הגנות לוגיות למערכות אדם - מכונה (HMI)
אין	1	2	3 ויותר	20. הגנות לוגיות למערכות הבקרה התעשייתיות (ICS)
אין	1	2	3 ויותר	21. הגנות לוגיות (במידה וקיימות) לרכיבים בשטח שמשפיעים על חומרים מסוכנים (ברזים, וסתים, שסתומים וכדומה)
לא מתבצע כלל	מתבצע לעיתים רחוקות	מתבצע לעיתים קרובות	מתבצע באופן סדיר וקבוע	22. קמפיין מודעות עובדים לאבטחת מידע
לא	הוראות בע"פ בלבד	תהליך חלקי	כן	23. האם מתנהל תהליך מסודר בקליטת עובד לעניין גישה למערכות מחשוב תעשייתיות?
לא	הוראות בע"פ בלבד	תהליך חלקי	כן	24. האם מתנהל תהליך מסודר בעזיבת עובד הכולל גריעת הרשאות/מחיקת משתמש?
לא	הוראות בע"פ בלבד	תהליך חלקי	כן	25. האם מתנהל תהליך לניוד עובד מתפקיד לתפקיד בתוך הארגון לעניין גישה למערכות מחשוב תעשייתיות?
יש שימוש ביותר מ- 10 רכיבים	יש שימוש ב-4 עד 10 רכיבים	יש שימוש ברכיב 1 עד 3	אין שימוש ברכיב IOT	26. שימוש ברכיב IOT בארגון
אין	באופן מצומצם מאוד	חלקית	כן	27. האם יש מדיניות ארגונית כתובה לצורך ניהול, בקרה והגנה על סביבת בקרים תעשייתיים?
לא קיים	באופן מצומצם מאוד	חלקית	כן	28. האם יש מיפוי תהליכים מסוכנים?
יש ללא תקשורת מוצפנת וגם ללא הזדהות חכמה	יש כאשר התקשורת לא מוצפנת או ההזדהות לא חכמה	יש עם תקשורת מוצפנת והזדהות חכמה	לא	29. האם יש שימוש בטכנולוגית סלולר לצורך התחברות לעמדות HMI או רכיבים אחרים במערך



מידת חשיפה				פרמטר נבדק
4	3	2	1	
				ה-ICS?
משאירים את ערכי המחדל ברירת המחדל	משנים רק את שם המשתמש	משנים רק את ססמת ברירת המחדל	משנים את שם המשתמש ואת ססמת ברירת המחדל	30. טיפול בהרשאות גישה של ברירת מחדל (משתמש וססמה דיפולטיביים) במערכות
ישנה ולא מוגנת כלל	ישנה ומוגנת עם הצפנה חלשה	ישנה ומוגנת עם הצפנה חזקה	לא	31. האם ישנה רשת WIRELESS ברצפת הייצור?
לא נעשים כלל	נעשים לעיתים רחוקות	נעשים לעיתים קרובות	נעשים באופן שוטף	32. האם נעשים רישום ובקרה של מצאי הרכיבים במפעל העלולים להשפיע על אירוע חומרים מסוכנים?
יש ללא תקשורת מוצפנת וללא הזדהות חכמה	יש כאשר התקשורת לא מוצפנת או ההזדהות לא חכמה	יש עם תקשורת מוצפנת והזדהות חכמה	אין	33. אפשרות גישה מרחוק למערכות אדם - מכונה (HMI)
יש ללא תקשורת מוצפנת וללא הזדהות חכמה	יש כאשר התקשורת לא מוצפנת או ההזדהות לא חכמה	יש עם תקשורת מוצפנת והזדהות חכמה	אין	34. אפשרות גישה מרחוק למערכות הבקרה התעשייתיות (ICS)
יש באופן מלא	יש במידה רבה	יש במידה מועטה	אין	35. שימוש במחשוב ענן
לא מבוצעים כלל	מבוצעים לעיתים רחוקות	מבוצעים לעיתים קרובות	מבוצעים בשוטף	36. ביצוע מבדקי חדירות
אין	יש בחלק קטן מהרכיבים הקריטיים	יש ברוב הרכיבים הקריטיים	יש באופן מלא	37. יתירות לרכיבים קריטיים
התקן USB מאופשר חופשי	התקן USB מופעל עם הרשאות למורשים בלבד	התקן USB מופעל עם יכולת הלבנה	התקן USB מושבת	38. שימוש במדיה נתיקה במערכות אדם - מכונה (HMI)
מועבר באופן חופשי	מועבר אך רק למורשים	מועבר באמצעות הלבנה	לא	39. אם יש מדיה נתיקה - האם מועבר חומר בין הרשתות השונות?
לא	מוטמעת חלקית	מוטמעת ברובה	כן	40. האם מוטמעת מערכת לאיסוף וניטור לוגים?



מידת חשיפה				פרמטר נבדק
4	3	2	1	
משתמשים גנריים בלבד	משתמשים גנריים ברובם	משתמשים אישיים ברובם	משתמשים אישיים בלבד	41. הגישה לממשקי אדם - מכונה (HMI) מאפשרת אך ורק באמצעות משתמשים אישיים לכל מפעיל?
סיסמה ללא מדיניות	סיסמה כפופה למדיניות	הזדהות חכמה ללא ביומטרי	הזדהות חכמה כולל ביומטרי	42. הזדהות עם ממשקי אדם - מכונה (HMI)

סיכום:

שם הבודק	תפקיד	חתימה	תאריך	ציון מידת חשיפה

ה. נספח ה' - רשימת בקורות והגנות נדרשות

מבוא

דרישות ההגנה מעסק מכונות בשפה המקצועית – בקורות. לטובת הגנה על העסק בתחום הסייבר, בעל היתר הרעלים נדרש לממש בקורות בתחומים שונים. בקורות אלו כוללות תהליכים, נהלים, מערכות הגנה וטכנולוגיות, אשר העסק מיישם במטרה להפחית את הסיכון להתממשות אירוע במרחב הסייבר.

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

לטובת בניית תורת הגנה פרופורציונלית, הבקורות במסמך זה סווגו לרמות שנעות בציר של 1-4, כאשר בקורות מרמה 1 הן הבקורות הבסיסיות ביותר, אשר נדרשות מכל עסק ולכל נכס ואילו בקורות מרמה 4 הן כאלו אשר נדרשות עבור יעד הגנה שפוטנציאל הנזק שלו הינו 4.

פירוט רשימת הבקורות

Identify					
1. אחריות בעל העסק/הנהלת העסק: 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 בעל העסק או של הנהלת העסק, מדיניות ההגנה בסייבר של ההנהלה ונוהלי ההגנה בסייבר הארגוניים. כמו כל תוכנית הגנה, הגנה בסייבר אינה הרמטית, וההנהלה נדרשת להחליט על רמת הסיכון שהיא מוכנה לקחת בהתחשב בעלויות המימוש של הבקורות 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.					
שם הפרק	1.1	בקה נדרשת	הסבר	המלצות	סיווג העסק
אחריות בעל העסק/הנהלת העסק	1.1	בעל העסק יאשר את מדיניות אבטחת המידע והגנת הסייבר הארגונית אחת לשלוש שנים, ויקצה משאבים נדרשים לטובת מימושה. מדיניות זו צריכה לשקף טיפול בסיכוני הסייבר בהקשר המסמך הנוכחי, ואופן הטמעתה בארגון, מההנהלה ומטה.		מומלץ למנות בקרב חברי הנהלת העסק, עובד אשר יהיה מוקד ידע (ברמה הניהולית) בנושא. היבטי הממשל התאגידי הכוללים תהליכי איתור וניהול סיכונים כחלק מהתהליכים העסקיים הם חשובים מאוד להתמודדות סדורה עם איומי הסייבר. לטובת עמידה בדרישה זו, חשוב לוודא, כי מפת הסיכונים מוצגת להנהלת העסק בשפה העסקית לצד המענה הקיים כיום בארגון והפערים הנדרשים לטובת צמצום הפער והגעה לרמת סיכון מקובלת. להשלמה ומעבר למחויבות הישירה לפי מסמך זה,	2
2. בקרה, ביקורת ותאימות: כל בעל עסק נדרש להגן על נכסי הסייבר שלו, כמפורט במסמך זה, על מנת למנוע או לצמצם סיכוי להתרחשות אירועי חמרים מסוכנים בשל מתקפת סייבר. על העסק לבנות מנגנוני בקרה על-מנת לוודא באופן שוטף, כי הוא עומד בדרישות מסמך זה.					
שם הפרק	2.1	בקה נדרשת	הסבר	המלצות	סיווג העסק
בקה, ביקורת ותאימות	2.1	בדיקה אוטומטית של רמת ההגנה של הארגון.	יש להשתמש בכלים ממוכנים, אשר מדמים את פעילות התוקף באופן אוטומטי.	מאחר שביצוע מבדקי חדירה הוא פעולה אשר מצריכה על-פי רוב מעורבות אנושית, היכולת לכסות מערכות רבות ובזמן אמת הינה מוגבלת. לטובת מתן מענה על מגבלות הזמן והידע, קיימים כמה מוצרים, המאפשרים למנהל ההגנה לקבל חיווי באמצעות כלים שמדמים "משחק מלחמה", התוקף את הארגון בשיטות שונות במטרה לזהות וקטורי תקיפה וחולשות לטיפול.	4



Protect

4. בקרת גישה:

גורמים רבים נדרשים לגשת למידע הארגוני לצורך תפקודם התקין – הן גורמים אנושיים (העובדים בעסק, לקוחותיו, ספקיו) והן גורמים טכנולוגיים (אפליקציות). הללו נדרשים לגישה למערכות ולסוגי מידע שונים. במטרה למנוע ניצול לרעה של גישות אלו, על העסק 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, להוסיףם, 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.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
בקרת גישה	4.1	יש לפתח, לתעד וליישם מדיניות בקרת גישה.	מדיניות בקרת הגישה נועדה לוודא, כי רק גורמים מורשים יכולים לגשת למידע ולמערכות הארגון, לצפות ולבצע שינויים, וכל זאת בהתאם להגדרות תפקידיהם ובכפוף לפיקוח.	2
בקרת גישה	4.2	יש להגדיר חשבונות משתמשים אשר תומכים בפונקציות העסקיות של הארגון. 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
בקרת גישה	4.3	יש לסקור את רשימת המשתמשים מעת לעת, ולא פחות מתקופה של 12 חודשים, ולעדכן אותה אם חל שינוי בכח האדם בעסק.	תהליך סקירת משתמשים תקופתי ותיעדודו בנוהל בקרת גישה ארגוני, ביצוע מעקב שוטף באמצעות מערך ממוכן או ידני, שיבוצע 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, אם עובד שינה תפקיד בארגון, במקרים רבים הוא "גורר" עמו את ההרשאות הקודמות. סקירה של מנהל המערכת מהצד העסקי	2



	עשויה להציף מקרים כאלו.			
3	במידת האפשר, יש להגדיר חשבונות זמניים עם הקצבת זמן לכל מערכת המתממשת ל Active Directory או למערך ניהול זהויות (IDM). חשבונות שצריך להאריכם נדרשים לאישור מיוחד.		יש לנטרל/להסיר חשבונות זמניים באופן אוטומטי מעת לעת, ולא פחות מתקופה של 3 חודשים.	4.4 בקרת גישה
3	מומלץ להוציא דו"חות תקופתיים לגבי פעילות Login של משתמשים במערכות המתממשת ל Active Directory וכן חשבונות אשר ננעלו לפני תקופה ארוכה (כפי שמוגדר בנוהל בקרת גישה). יש להסיר חשבונות שנמצאו.		יש לנטרל/להסיר חשבונות לא פעילים באופן אוטומטי מעת לעת, ולא פחות מתקופה של 3 חודשים.	4.5 בקרת גישה
3	ניתן ליישם באמצעות הניטור (SIEM), אשר יתממשק למערכי ניהול ההרשאות בארגון - Active Directory, IDM, שרתים, מערכות אפליקטיביות וכן ציודי תקשורת ואבטחת מידע.		יש לתעד ביומן רישום אוטומטי (רישום Log) כל יצירה, שינוי, אפשר, ניטרול והסרה של חשבון	4.6 בקרת גישה
3	ניתן ליישם באמצעות מערכת SIEM לניטור משתמשים בקבוצות רגישות. איסוף המידע ייעשה ממקורות, כגון Active Directory, ציודי תקשורת ואבטחת מידע (חומת-אש וכו'). יודגש כי מדובר בניטור לתכלית אבטחתית, תוך יישום תובנות מקובלות בתחום הגנת הסייבר.	דוגמאות לשימוש חריג: התחברות למערכת בימים מסוימים ובשעות מסוימות, התחברות מכתובות שאינן תואמות לתבניות השימוש הרגיל.	יש לנטר פעילות חריגה במערכות המידע בהתאם לסטנדרטים מקובלים, לצורך איתור שימוש לרעה בידי גורם זדוני. במקרה של חשש שימוש חריג ולדווח על שימוש חריג לבעלי התפקידים המתאימים.	4.7 בקרת גישה
4	ניתן להגדיר מגבלת כניסה בהגדרת משתמש בתוך חשבון ה- Active Directory, כך שהמגבלה לא תאפשר התחברות בשעות שאינן שעות פעילות.	דוגמאות לתנאי חסימת כניסה: סופ"ש, שעות הלילה.	יש להגדיר ולאכוף תנאים לחסימת שימוש בחשבונות, בהתאם לשעות פעילות העסק, ובהתאם לשעות העבודה של סוגי העובדים השונים.	4.8 בקרת גישה
1	המשתמשים ינוהלו בצורה מרכזית באמצעות מרכזי ארגוני, כגון Directory, Active Directory, OpenLDAP ועוד. מערך ההרשאות ימופה לפרופיל המשתמש.	בקרת הגישה יכולה להיעשות ברמה אישית (identity-based), ברמת תפקיד (role-based), ומטרתה לשלוט בגישה של ישויות (משתמשים, או תהליכי מחשב) לאובייקטים (קבצים, רשומות, מכשירים ועוד).	יש להגדיר ולאכוף הרשאות גישה לוגיות למערכת ולמידע בהתאם למדיניות בקרת הגישה.	4.9 בקרת גישה



2	הרשאות משתמשים יינתנו בהתאם לתפקיד העובד. יוגדר פרופיל בסיסי, שיינתן למשתמש והרשאות נוספות יינתנו בהתאם לצורך ובאישור ממונה ישיר - אם קיימת מערכת IDM ניתן למפות פרופיל בסיסי וכן פרופילים אפליקטיביים. לאחר טיוב התהליך יינתנו ההרשאות בהתאם לתפקיד.	הארגון יגדיר רמת הרשאות מינימלית לכל תפקיד וכן רמת הרשאות מינימלית למשתמש בסיס (ללא תפקיד מוגדר) שנדרשת עבורו גישה למערכות הארגון.	יש להגביל את הרשאות המשתמשים למינימום ההכרחי הדרוש לביצוע תפקידם.	4.10	בקרת גישה
3	יש לבצע מיפוי הרשאות, התומך במערך של הפרדת סמכויות וליישמו 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'.	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 המנהל את בקרת הגישה אינו מנהל גם את פונקציות הביקורת על בקרת הגישה.	יש להגדיר בעלי תפקידים, לבצע הפרדה בין תחומי אחריות (Separation of duties) ולהביא אותה לידי ביטוי במתן הרשאות למערכת.	4.11	בקרת גישה
4	ניתן לממש בקרה זו באמצעות הגדרת גישה ברכיב חומת-האש, כי התחברות אל נכסים רגישים תותר אך ורק מרכיב הקישור, הכולל את הבדיקות והמדיניות הארגונית המחמירה (כגון מניעת יכולת ביצוע "העתק/הדבק", מניעת יכולת הורדת קבצים, נעילת CLI וכו').	לטובת החלת מדיניות אחידה "מוקשחת" אל משאבים רגישים, יש לוודא, כי הגישה אליהם תתבצע אך ורק לאחר מעבר דרך רכיב התיווך (כגון שרת פרוקסי או טרמינל).	הגישה אל מערכות ויישומים רגישים תתבצע אך ורק דרך רכיב תיווך ייעודי מוקשח (טרמינל).	4.12	בקרת גישה
3	במערכות ניהול תוכן (CMS) יש לתת הרשאות עריכה ולאפשר הרשאות פרסום רק למנהלי התוכן.	הארגון יגדיר משתמשים אשר תפקידם דורש יכולת פרסום מידע במקורות פומביים ויתעד כחלק מנוהלי הארגון את התפקידים הנ"ל.	יש להגדיר מי הם העובדים אשר מורשים לפרסם מידע במערכת נגישה ציבורית (כמו אתר אינטרנט), וליישם הרשאה זו כחלק מתהליך מתן ההרשאות.	4.13	בקרת גישה
2	ניתן להגביל את מספר הניסיונות הכושלים להתחברות בתוך ה-Group Policy וה- Domain Policy.	מטרת הבקרה היא להתמודד עם הסיכון של התקפות מניעת שירות. יש ליישם את הבקרה הן ברמת החיבור למערכת ההפעלה והן ברמת חיבור לאפליקציות ספציפיות.	יש להגביל התחברות משתמש למערכת לאחר 5 ניסיונות התחברות כושלים באמצעות נעילת האפשרות לביצוע התחברות במשך פרק זמן מוגדר, או עד לשחרור על-ידי מנהל מערכת.	4.14	בקרת גישה



3	ניתן להגביל מספר התחברויות בו זמנית בתוך מדיניות ה-Remote Logon Policy ב-Group Policy.	מטרת הבקרה הינה לזהות התחברות משני מקומות שונים באמצעות אותם פרטי הזדהות. תרחיש כזה עלול להוות אינדיקציה לשימוש לא מורשה בחשבון המשתמש.	יש להגביל את מספר החיבורים המותרים בו-זמנית של משתמש בודד.	4.15	בקרת גישה
3	ניתן לממש באמצעות הגדרת שומר מסך. במידת האפשר יש לוודא, כי מערכות בפיתוח עצמי וכן מערכות מוצרי מדף יכללו מנגנון של Session time out.	בקרה זו מיועדת להביא לכך שמערכת ממוחשבת אשר לא נעשה בה שימוש לפרק זמן מסויים ועקב כך היא נכנסה "למצב שינה", או שנותקה התקשורת לשרת המרכזי, אזי חידוש העבודה במערכת יחייב הקלדה חוזרת של שם משתמש וסיסמא. 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).	יש לנעול חיבורים כתוצאה מאי-פעילות זמנית ולא לאפשר את המשכיות החיבור עד להזדהות ואימות חוזר של המשתמש. כחלק מביצוע נעילת החיבור יש להסתיר מידע שהוצג על המסך טרם הנעילה.	4.16	בקרת גישה
2	ניתן לממש גישה מאובטחת לארגון באמצעות מערכות כגון VPN או SSH, אשר עומדות בקנה אחד עם המדיניות הארגונית להתחברות מרחוק למשאבי הארגון.		נדרשת מדיניות העוסקת בחיבורים מרחוק, אשר מגדירה את מגבלות השימוש בהתחברות מרחוק למשאבי הארגון. כן נדרש שימוש במערכות המספקות גישה מרוחקת מאובטחת למשאבי הארגון.	4.17	בקרת גישה
2	ניתן להשתמש בחיבור מוצפן כגון SSH או VPN בהתחברות אל תוך הארגון.	גישה מרחוק למערכות מידע ארגוניות מוגדרת כביצוע חיבור על-ידי משתמשים או תהליכי מחשב מתוך רשתות חיצוניות. ארגונים נוהגים להטמיע רשתות וירטואליות מוצפנות (VPN) על-מנת להגביר את סודיות החיבור ואת שלמותו.	יש לממש מנגנונים להצפנת התווך לצורך הגנה על סודיות התחברויות מרחוק ושלמותן.	4.18	בקרת גישה
3	ניתן לממש את מערכות הגישה מרחוק למערכות הניטור, כגון ה-SIEM, ולוודא שאכן נרשמים אירועים על התחברות. יש לשים דגש מיוחד על התחברות מרחוק של ספקים חיצוניים לתוך הארגון לצורך תחזוקה ותמיכה ולנטר את פעילותם בצורה אפקטיבית (כגון באמצעות כלי ניטור והקלטת מסכים).	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.	יש לנטר התחברויות מרחוק.	4.19	בקרת גישה



3		הקטנת מספר נקודות בקרת הגישה מצמצמת את משטח התקיפה.	יש לנתב את כל ההתחברויות מרחוק דרך לא יותר מנקודת בקרת גישה מנוהלות (managed network) access control (points); הממונה רשאי, לפי בקשת בעל העסק, לאשר הוספת נקודות בקרה.	4.20	בקרת גישה
3	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).	פקודות רגישות הן, למשל, אתחול שרת או ביטול טרנזקציה. יש לוודא, כי אי אפשר להריץ פקודות אלו במסגרת התחברות רגילה למערכת.	גישה למערכות רגישות מרחוק תתבצע רק באמצעות זיהוי חזק	4.21	בקרת גישה
4	יש למנוע Administrator Login בעת התחברות מרחוק למערכות (ניתן לבצע גם בלינוקס על-ידי ביטול PermitRootLogin).	הארגון לא יאפשר גישה ישירה מרחוק לממשקי ניהול, אלא בצורה מאובטחת בלבד, לאחר אימות והתחברות לרשת ניהול.	יש לאסור התחברות מרחוק למערכת לצורך ניהול, וכן להגביל גישה למערכת מרשתות שאינן מנוהלות על-ידי העסק.	4.22	בקרת גישה
2	הגישה אל הרשת האלחוטית תותר אך ורק לאחר הזדהות אל מול ה-Point Access.	מטרת הבקרה הינה למנוע שימוש לא לגיטימי ולא מזוהה ברשת האלחוטית.	יש להגן על חיבור למערכת מרשת אלחוטית באמצעות אימות משתמשים/מכשירים, שימוש בהצפנה והגדרת הגבלות שימוש. העסק יאפשר חיבור לרשת אלחוטית רק עבור מכשירים המנוהלים/מאומתים על-ידו וכן רק עבור משתמשים מזוהים.	4.23	בקרת גישה
4	ניתן לבצע מיפוי של טווחי קליטה באמצעות סקירה מרחבית וכן ציוד ייעודי (Radio) בתיאום עם ספק המערכת האלחוטית. כמו כן ניתן לבצע עצמאית באמצעות Radio Analyzer וסריקה סביב שטח המבנה.	העסק יסקור את אותות השידור של הרשתות האלחוטיות ויוודא, כי האות אינו חורג מטווח שהוגדר מראש.	יש לכייל את עוצמת השידור של האות האלחוטי על-מנת להפחית את הסיכוי שאותות ייקלטו מחוץ למתקן העסק.	4.24	בקרת גישה
2			גישה למערכות ממוחשבות בעסק תתאפשר רק עבור ציוד מחשב, המחובר באמצעות חיבור קווי לרשת הארגונית.	4.25	בקרת גישה



2	יש לכתוב מדיניות מכשירים ניידים, המגדירה את גבולות השימוש במכשירים ניידים (כגון טלפונים סלולריים וטאבלטים) - מה ניתן לשמור או לגשת אליו בארגון באמצעות המכשיר הנייד.	על המדיניות להתייחס הן למכשירים המסופקים ומנוהלים על-ידי העסק וכן למכשירים אישיים של עובדי בעסק או אורחים.	העסק יגדיר מדיניות יישום בקורות אבטחת מידע על מכשירים ניידים הניגשים למערכות הארגון.	4.26	בקרת גישה
3	ניתן ליישם באמצעות Policy, אשר יופץ למכשירים הניידים באמצעות Mobile Device Management ונתמך ברוב מכשירי אנדרואיד ואפל.	העסק יצפין את שטח הדיסק של המכשירים הניידים המתחברים למערכותיו.	יש להטמיע הצפנה מלאה של המידע המאוחסן על מכשירים ניידים על-מנת להגן על סודיות המידע ושלמותו.	4.27	בקרת גישה
4	ניתן ליישם באמצעות זיהוי הדפדפן במכשיר הנייד, או, לחלופין, לא לאפשר חשיפה של מערכות רגישות לרשתות הנגישות למכשירים ניידים (גם לא מאחורי סגמנט ה-VPN, או, לחלופין, לחבר את המכשירים הניידים לסגמנט VPN שונה משאר המחשבים).	העסק יחסום ויאכוף באמצעות בקורות טכנולוגיות גישה למערכות ארגוניות רגישות באמצעות מכשירים ניידים.	יש לאסור על התחברות למערכת ממוחשבת באמצעות מכשירים ניידים.	4.28	בקרת גישה
2	לכל משתמש מערכת יהיה שם משתמש ייחודי (אשר ימופה לאדם מסוים). עבור משתמשים גנריים יצוין מי בעל המשתמש הגנרי ומשתמשים אפליקטיביים יהיו בבעלות מנהל המערכת.	הארגון יאמת באופן חד-ערכי משתמש המתחבר למערכות הארגון.	יש לזהות ולאמת באופן ייחודי את משתמשי המערכת.	4.29	בקרת גישה
2	לדוגמה, ניתן לממש באמצעות כרטיסים מגנטיים, טביעות אצבעות או מנגנונים אחרים, הנתמכים על-ידי Active Directory.	העסק יישם הזדהות מקומית בכמה אמצעי זיהוי (שניים או יותר) לחשבונות רגישים.	יש לממש הזדהות חזקה עבור התחברות חשבונית בעלי הרשאות יתר דרך הרשת.	4.30	בקרת גישה
3	ניתן לממש באמצעות כרטיסים מגנטיים, טביעות אצבעות או מנגנונים אחרים, הנתמכים על-ידי Active Directory.	העסק יישם הזדהות בכמה אמצעי זיהוי (שניים או יותר) לחשבונות רגישים בהתחברות מקומית.	יש לממש הזדהות חזקה עבור התחברות לוקאלית של חשבונות בעלי הרשאות יתר.	4.31	בקרת גישה
4	ניתן לממש באמצעות מנגנונים, כגון כרטיס חכם או סיסמה חד-פעמית.	העסק יישם מנגנון הזדהות חסין האזנה (כגון מנגנון זיהוי, אשר מנפיק הזדהות חד-פעמית) עבור כלל החשבונות.	יש לממש מנגנון אימות שהוא replay-resistant עבור התחברות של כל חשבון (בדגש על מנגנון אימות בעל אמצעי הצפנה).	4.32	בקרת גישה
2	ניתן לממש באמצעות מנגנונים, כגון כרטיס חכם או סיסמה חד-פעמית בגישה מרחוק למערכות כגון VPN.	העסק יישם הזדהות מרוחקת בכמה אמצעי זיהוי (שניים או יותר) למערכות הארגון.	יש לממש הזדהות חזקה לצורך התחברות מרחוק למערכת.	4.33	בקרת גישה



3	ניתן לממש באמצעות תעודות דיגיטליות, המונפקות למחשבי קצה ולמחשבים ניידים.	העסק יזהה באופן חד-ערכי מכשירים המתחברים לרשת הארגונית.	יש לזהות ולאמת באופן ייחודי מכשירים שמתבצעת מהם התחברות.	4.34	בקרת גישה
2	ניתן לממש באמצעות מערכת לניהול OTP במידה שנדרש אמצעי זיהוי חזק יותר מזה הקיים במערכת.	יש לנהל מאגר של אמצעי הזדהות והנפקתם. כמו כן, ניתן לבצע ביטול אמצעי הזדהות באמצעות מערכת מרכזית.	יש לנהל אמצעי הזדהות למערכת, לרבות: בחירת אמצעי זיהוי של עובד או בעל תפקיד, השמתם וחסימתם לאחר פרק זמן של חוסר שימוש.	4.35	בקרת גישה
2	ניתן לממש באמצעות נוהל ומערכת הזדהות.	יש לבצע הערכה של הבקורות וכתביבת נוהל, המתאר שימוש באמצעי מסוג מסוים במערכת מסיווג גבוה או מרמת סיכון גבוהה.	יש לנהל אמצעי אימות למערכת, לרבות: בחירת אמצעי אימות, וידוא עמידה בתנאי האבטחה הנדרשים, הגדרת תהליך הפצתם, הגדרת הגבלות שימוש.	4.36	בקרת גישה
2	ניתן לממש באמצעות Domain Policy ו- Group Policy Policy.	על אכיפת המדיניות לכלול לכל הפחות: הגדרת מורכבות מינימלית, שונות מסיסמאות קודמות, זמן תפוגה מוגדר, דרישה להגדרת סיסמה חדשה לאחר התחברות ראשונית.	על העסק ליישם אכיפה של מדיניות סיסמאות באמצעים טכנולוגיים.	4.37	בקרת גישה
2	ניתן לממש באמצעות מנגנונים מובנים במערכות ההפעלה. כמו כן ניתן לממש בדפי Web באמצעות הגדרת השדה כ- Password.		יש לוודא כי הנתונים ממערכת המידע לאורך תהליך האימות לא יספקו מידע שעלול לגרום נזק אם יתגלה או אם יבוצע בו שימוש על-ידי גורמים לא מורשים. יש להסוות את שדות האימות באמצעות הסתרת הסיסמה.	4.38	בקרת גישה
2	ניתן לממש באמצעות מנגנונים, כגון כרטיס חכם או סיסמה חד-פעמית.	המטרה היא כי פרטי ההזדהות לא יהיו חשופים (Clear text). פרטי זיהוי חשופים ניתנים לגניבה אם יועברו בתווך תקשורת שאינו מוצפן, לדוגמה במקרה של מתקפת MIDM.	יש ליישם מנגנון אימות מוצפן.	4.39	בקרת גישה

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 – סיווג, אחסון, נידוד וכד'.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
הגנה על המידע	בקרה נדרשת	הסבר	המלצות	
5.1	יש למנוע העברת מידע לא מורשית או לא מכוונת דרך משאבי מערכת משותפים.	על הארגון למנוע את העברתו של מידע באופן לא מורשה באמצעות תיקיות משותפות, דואר אלקטרוני, מדיה נתיקה וכו'.	יש להגביל את השימוש בתיקיות משותפות לצורך העברת מידע, בייחוד כאשר יש הרשאות גם לגורמים שאינם מורשים. ניתן לעשות שימוש במערכת DLP על-מנת	1



	למנוע העברת מידע השמור בתיקיות משותפות.				
2	ניתן ליישום בעזרת כמה טכנולוגיות, אשר כל אחת מהן עשויה למנוע תרחיש מסוים: 1. מערכת למניעת דלף מידע; 2. מערכת מאובטחת להעברת מידע, כגון מייל מאובטח/מוצפן, כספת אלקטרונית וכו'.	על הארגון ליישם מנגנונים להגנה על מידע בעת תנועה בין מערכות הארגון ובשליחתו אל גורמים מחוץ לארגון בהתאם למדיניות הגנת המידע הארגונית.	יש לממש מנגנוני הגנה על-מנת למנוע דלף מידע בעת העברת מידע לגורמים פנימיים או חיצוניים.	5.4	הגנה על המידע
3	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 הגבלה וניטור של גישה לקבצים רגישים (כפי שמורחב בפרקי בקרת גישה וניטור).	על הארגון ליישם מנגנונים להגנה על מידע בעת שמירתו במערכי האחסון הארגוניים, 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 שהוגדר כמידע רגיש בניגוד למדיניות שנקבעה עבור מידע זה.	יש ליישם מנגנוני הגנה לניטור ומניעה של גישה, שימוש או הוצאת מידע, אשר הוגדר רגיש על-ידי הארגון, אל גורמים שאינם מורשים בתוך הארגון ומחוצה לו.	5.5	הגנה על המידע
3	רצוי לחסום באופן קבוע עזרי מחשב שלא נעשה בהם שימוש במטרה לצמצם סיכון זה.	יש למנוע/לחסום/לנטרל הפעלה מרחוק של מצלמות, מיקרופונים וכו'.	יש למנוע הפעלה מרחוק של עזרי מחשב (מצלמות רשת, מיקרופונים, רמקולים, אוזניות וכל אביזר שעשוי להיות מחובר למחשב) ולספק אינדיקציה מפורשת לכך, שעזרי המחשב פעילים פיזית מול המשתמש.	5.6	הגנה על המידע

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. בקורות הגנת תחנות עבודה ושרתים כוללות מס' שכבות הגנה - הקשחת שירותים (White/Black List), מניעת יצירת פרוצדורות אבטחה בידי משתמשים הן בזדון והן בשוגג ועוד.

סיווג העסק	טור ג'	טור ב'	טור א'		
	המלצות	הסבר	בקרה נדרשת		שם הפרק
2	ניתן לממש בקרה זו באמצעות הגבלת חשבונות משתמש להתקנה/שינוי של תוכנות בעמדות הקצה וכן באמצעות שימוש בכלי Application control.	מטרת הבקרה הינה לוודא, כי תוכנות מותקנות על עמדות הקצה ועל השרתים רק באישור ולאחר בחינה של הצורך והסיכון הכרוכים בשימוש בתוכנה.	יש להגדיר מדיניות לשליטה, אכיפה וניטור של התקנת תוכנות על מחשבי הארגון	6.1	הגנה על תחנות עבודה ושרתים
3	ניתן לממש באמצעות הגדרת חוקים רלוונטיים במערכת ה-SIEM באמצעות השוואת דו"חות תקופתיים (קונפיגורציה	שינוי בתצורת מערכת (קונפיגורציה) עלול להוריד את רמת ההגנה על הנכס. כך, לדוגמה, שינוי של הגדרת אורך	יש להגדיר ולהטמיע אמצעי אבטחה על-מנת לאתר ולהתריע על שינויים לא מורשים בהגדרות תצורה.	6.2	הגנת תחנות עבודה ושרתים



	נוכחית מול קודמת), באמצעות כלי ניטור ובקרה/שוי"ב ייעודיים המספקים חיזוי על שינוי קונפיגורציה וכו'. מומלץ לאמץ כלי - CCM Continuity Control Monitoring על-מנת לקבל את החיזוי בזמן אמת.	סיסמה או של הרשאה להתקנת תוכנות שלא בהתאם למדיניות הארגון חושף אותו לסיכון.			
1	ארגון ברמה 1 יכול לבצע זאת באמצעות דרישה חוזית מספק התוכנה/שירות לקבלת מוצרים מוקשחים בהתאם לפרקטיקות מקובלות. ארגונים ברמה 2 ומעלה נדרשים לבצע בדיקת אפקטיביות המוצר/שירות בהתאם לרמת ההקשחה הנדרשת. ארגונים ברמה 3 נדרשים לבצע בדיקה של אפקטיביות ההקשחה. ניתן להתבסס בכתיבת נוהלי ההקשחה על פרקטיקות מקובלות, כגון NIST, פרסומי ה-CERT הלאומי ו-CIS, או על שירותי מומחה, אשר יכין נוהלי הקשחה לפי הטכנולוגיה הרלוונטית.		יש להגדיר את תצורת המערכת כך שתספק את הפונקציונלית המינימלית הנדרשת (תוך חסימת פונקציות, פורטים ופרוטוקולים שאינם נדרשים), על בסיס פרקטיקות מקובלות, כך שיכללו, לכל הפחות: 1. הפחתה של שטח התקיפה של המערכת על-ידי חסימת פורטים שאינם 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.	6.3	הגנה על תחנות עבודה ושרתים
2	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 (Protection Endpoint) תומכים ביכולות הני"ל.		הארגון יגדיר רשימת תוכנות האסורות לשימוש (Black List). יש למנוע הרצה של תוכנות לפי הגדרת הארגון (Black List).	6.4	הגנה על תחנות עבודה ושרתים
3	ניתן להגדיר רשימת תוכנות המותרות לשימוש באמצעות ה- Active Directory, או באמצעות כלי ניהול תצורה. חלק מכלי ההגנה על תחנות קצה ושרתים (Protection Endpoint) תומכים	הארגון יגדיר את רשימת התוכנות המותרות לשימוש ויחסום התקנה ושימוש בכל שאר התוכנות באמצעות מערכת ניהול התצורה הארגונית, או באמצעות כלי צד ג' ויחסום התקנה	הארגון יגדיר את רשימת התוכנות המותרות לשימוש ויחסום התקנה ושימוש בכל שאר התוכנות באמצעות מערכת ניהול התצורה הארגונית, או	6.5	הגנה על תחנות עבודה ושרתים



	ביכולות הנ"ל.	של תוכנות אלו.	באמצעות כלי צד ג' ויחסום התקנה של תוכנות אלו.		
3	ניתן להגדיר ראש תחום או בעל תפקיד, אשר יהווה "סמכות מאשרת" לחריגה מהמדיניות לטובת צורכי החריגה, שיבחן את הצורך התפעולי והעסקי להחרגה וימליץ על בקרה מפצה.	לעתים, מסיבות עסקיות ו/או תפעוליות אי אפשר להחיל את רמת ההגנה על כל הנכסים באותה הצורה. במקרים אלו הארגון נדרש ליישם תהליך, אשר ידרוש אישור מיוחד להחרגת שרת או מערכת מסוימת מדרישות אבטחת המידע בעקבות צורך כלשהו, ובתוך כך יהיה הארגון אחראי לספק בקרה מפצה במקום ההחרגה.	הארגון ינהל מעקב אחר שרתים ומערכות אשר הוחרגו (והחרגתם אושרה) מיישום תצורה מוקשחת.	6.6	הגנה על תחנות עבודה ושרתים
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.					
שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק	
מניעת קוד זדוני	7.1	הארגון יפעיל כלים ומערכות בנקודות התקשורת החיצונית שלו. כלים אלה יסרקו ויזהו קוד עוין. הכלים יופעלו על תקשורת עם גורמים חיצוניים, דואר אלקטרוני ושרותי גלישה.	מטרת בקרה זו הינה לזהות קוד עוין טרם כניסתו לארגון עוד ברמת ה-GW.	ניתן ליישם באמצעות שימוש בשרתי Proxy, במערכות UTM ובכלים ייעודיים לפרוטוקולי תקשורת שונים, כגון דואר אלקטרוני.	2
מניעת קוד זדוני	7.2	הארגון יגדיר נהלים לטיפול בתחנות, בשרתים או ברשתות הנגועים בקוד זדוני.	מטרת הבקרה הינה לוודא, כי הארגון ערוך להתמודדות באירועים של חדירת קוד עוין.	דוגמאות לנהלים: נוהל זיהוי והסרה של נזקה, נוהל התקנת מערכת הפעלה מחדש, נוהלי זיהוי מגמות והסקת מסקנות במקרה של התפשטות והדבקה מסיבית בארגון.	2
מניעת קוד זדוני	7.3	יש להטמיע כלים לזיהוי ולמניעה של 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 ייושמו גם ברמת תחנות העבודה.	ניתן להשתמש בכל כלי לזיהוי ומניעה של קוד עוין (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 הרמה של יכולת הזיהוי והטיפול 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



4	ניתן לממש באמצעות פתרונות לזיהוי אנומליות ברמת מערכת ההפעלה.	הארגון יפעיל מנגנונים במערכת ההפעלה, המקשים על קוד עיון את הגישה לזיכרון או לפונקציות מערכת ההפעלה.	יש להפעיל בקורות מתקדמות למניעת קוד זדוני במערכות הפעלה של שרתים ותחנות קצה.	7.5	מניעת קוד זדוני
3	דוגמאות לכלים אלו: Honeypots, טכנולוגיות Anti-Bot, רכיבי IDS ועוד.	הארגון יפעיל כלים שיוטמעו ברשת הארגון ומטרתם לזהות ולהתריע על נזקות המתפשטות ברשת.	יש להטמיע כלי לזיהוי נזקות ברמת הרשת.	7.6	מניעת קוד זדוני
2	מרבית המערכות למניעת קוד זדוני מאפשרות שימוש בכלי ניהול בעלי ממשק ניהול מרכזי.	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.	הארגון ינהל באמצעות מערכות מרכזיות את כלי מניעת הקוד הזדוני בארגון. כלי הניהול המרכזיים יאפשרו דיווח מרכזי על זיהוי אירועים חשודים ואירועי מערכת (בעיות עדכון, הגנה לא-פעילה, הסרת רכיב וכו').	7.7	מניעת קוד זדוני
3	ניתן להשתמש בכלים המנתחים היוריסטיקות (Heuristics), התנהגות משתמש או מערכת (behavioral).	מטרת בקרה זו הינה לאתר פעילויות חורגות מהנורמה. הצפנה של קבצים רבים, מסמכים המנסים לגשת לקובצי רגיסטרי וכו' הם אירועים לדוגמה, אשר אמורים "להדליק נורה אדומה" בארגון.	הארגון יפעיל אמצעים לזיהוי ומניעה, המתבססים על זיהוי התנהגות חורגת מהתנהגות מקובלת וסבירה, נוסף על שימוש בכלים מבוססי חתימות אלקטרוניות.	7.8	מניעת קוד זדוני
1	ניתן להשתמש בשרתי עדכון, המוטמעים בתוך הארגון כחלק משרתי הניהול של מערכות אלו, או, לחלופין, להשתמש בשרתי היצרן אם אין שרת עדכונים מרכזי ברשת הארגון (תקף גם לגבי שירותי ענן).	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.	יש להפעיל עדכון אוטומטי של כלל המערכות לזיהוי ולמניעת הקוד הזדוני בארגון.	7.9	מניעת קוד זדוני

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, תוכי תקשורת 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).

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
הצפנה	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, נוהלי הקשחה וכן נוהלי החלפת מפתחות.	הקשחה ושמירה על שרתי Root Ca, שמירה באמצעות HSM, הפצת מפתחות הצפנה לעובדים ולמערכות, תפעול מערך PKI.	1



3	לדוגמה: מערך שחזור הצפנת דיסקים של מחשבים ניידים באמצעות כלי היצרן של מערכת הצפנת הדיסק, ותהליכי שחזור מנוהלים.	הארגון יטמיע מערך שחזור נתונים מוצפנים באמצעות יישום תהליכים מנוהלים וכלים מתאימים.	יש לוודא את זמינות המידע גם במקרה של אובדן מפתחות הצפנה.	8.3	הצפנה
2	שימוש בתעודות SSL מאושרות ועדכניות בדפדפן.	הארגון יממש מערכי הצפנת נתונים למידע רגיש המוצג למשתמש באמצעות דפדפן, אפליקציית מובייל או מערכות אחרות, המנגישות מידע באמצעות רשתות ציבוריות, כגון רשת האינטרנט.	יש לממש מנגנוני הצפנה למידע רגיש, המועבר בין מערכות הארגון לממשקי משתמש קצה על-גבי תווך תקשורת ציבורי.	8.4	הצפנה
4	ניתן ליישם באמצעות שימוש בפרוטוקולים כגון HTTPS, SSH, SSL ועוד.	הארגון יממש תעבורה מוצפנת בממשקים בין שרתים ושירותים המעבירים מידע רגיש וכן יעדיף שימוש בפרוטוקולים המצפינים תעבורה.	יש לממש מנגנוני הצפנה למידע רגיש המועבר בין מערכות בתוך הארגון.	8.5	הצפנה
2	ניתן ליישם באמצעות שימוש בפרוטוקולים כגון HTTPS, SSH, SSL, SFTP ועוד.	הארגון יממש תקשורת מוצפנת אל מול ספקים ומערכות מחוץ לארגון.	יש לממש מנגנוני הצפנה למידע רגיש, המועבר בין הארגון לממשקים חיצוניים, לספקים, למערכות חיצוניות.	8.6	הצפנה
2	במכשירים סלולריים ובטאבלטים ניתן להשתמש במערך הצפנת הדיסק של היצרנים. במערכות הפעלה אחרות ניתן להשתמש בכלים של הספקים, המאפשרים הצפנת דיסק.	הארגון יממש הצפנה של דיסקים קשיחים של התקנים ניידים ושל התקני מדיה ניידים.	יש לממש מנגנוני הצפנה על מדיה של התקנים ניידים (מחשבים ניידים, מכשירים סלולריים, טאבלטים ועוד).	8.7	הצפנה
2	לדוגמה: לא להשתמש בשיטות הצפנה מיושנות, כגון SHA1, SSLv1, SSLv2, או מפתחות הצפנה קטנים מ-128 Bit ועוד.	הארגון לא ישתמש במנגנוני הצפנה בעלי חולשות ופגיעויות ידועות ויתאים את חוזק ההצפנה, לרבות את גודלי מפתחות ההצפנה, למתאר האיום.	יש להשתמש במנגנוני הצפנה, המתבססים על אלגוריתמים מוכרים של הצפנה, ובגודלי מפתח המתאימים למתאר האיום.	8.8	הצפנה
2	ניתן לממש באמצעות מערך שרתי CRL מסודר ומעודכן, שימוש בתעודות חיצוניות של שירותים מאושרים (Trusted CA).	הארגון ינהל מערך הנפקה של תעודות דיגיטליות ומערך של ביטול תעודות (CRL). כמו כן, ישתמש בתעודות חיצוניות, שהונפקו על-ידי מקורות מהימנים בלבד (Trusted CA).	יש לנהל מערך להנפקה ולביטול תעודות דיגיטליות ולהשתמש בתעודות דיגיטליות ממקור מהימן בלבד.	8.9	הצפנה
2		הארגון יוודא, כי התעודות הדיגיטליות אשר בשימוש קבוע יחודשו לפני מועד תפוגתן.	יש להגדיר תהליך לחידוש תעודות דיגיטליות טרם מועד תפוגתן. אם התעודות מוחלפות - התעודות הישנות מופצות לשרתי ביטול התעודות (CRL).	8.10	הצפנה



2		הארגון יגדיר את אורך החיים של מפתחות הצפנה רגישים וידאג להחליפם בזמן. כמו כן יש ליישם תהליך להחלפה של מפתחות ההצפנה באפליקציות רגישות.	יש לבצע החלפה יזומה של מפתחות הצפנה רגישים מעת לעת לפי הצורך, ולא פחות מתקופה של 6 חודשים ממועד ההחלפה הקודם.	8.11	הצפנה
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, והשבתה 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 לבקורות שנועדו להגן על חיבור הרשתות הארגוניות בינן לבין עצמן, על צומתי התקשורת הארגוניות וכמובן בינן לבין האינטרנט.					
סיווג העסק	טור ג'	טור ב'	טור א'		
	המלצות	הסבר	בקרה נדרשת		שם הפרק
2	כתיבת מסמך מדיניות או שילוב כפרק במדיניות אבטחת המידע הארגונית.	על הארגון לכתוב וליישם מדיניות אבטחת רשת. המדיניות צריכה לכלול התייחסות לנושאים, כגון ערוצי הגישה לרשת האינטרנט הציבורי ותצורת ההגנה עליהם. בנוסף, יש להתייחס להיבטי ההגנה בתווך התקשורת הפנים-ארגוני והחוץ-ארגוני.	יש לכתוב וליישם מדיניות הגנה על רשתות תקשורת, לבקר ולעדכן אותה תקופתית.	9.1	אבטחת רשת
3	ניתן לממש באמצעות דף התחברות (login) נפרד עבור משתמשים ועבור מנהלי המערכת, רשת תקשורת נפרדת, המשמשת להתחברות לממשקי ניהול ציוד, הגבלת כתובת IP מורשית לגישה לממשק הניהול וכו'.	ממשקי ניהול יופרדו מממשקי משתמש אחרים במטרה לצמצם את החשיפה לגישה לא מורשית לממשקי הניהול.	יש להפריד בין פונקציונליות משתמש לשירותי הניהול של הרשת.	9.2	אבטחת רשת
1	ניתן ליישם את הבקרה באמצעות כלים, כגון מערכות חומת-אש (באמצעות מודול IPS), מערכות לזיהוי חדירות (IPS), חומת-אש אפליקטיביות (WAF) וכן הגבלות על כמויות נפח התעבורה לכיוון מערכות מסוימות, או הגבלת כמות שאילתות מבוצעות למערכות.	יש להגן מפני התקפות מניעת שירות (DOS) מסוגים שונים, כדוגמת העמסה על משאבי מחשב עד לקריסתם, העמסת רוחב פס התקשורת, העמסת אתר אינטרנט עד לקריסתו ועוד.	הארגון יפעיל אמצעים טכנולוגיים על-מנת להגן על שירותיו מפני התקפות מניעת שירות.	9.3	אבטחת רשת
2	הבקרה ניתנת ליישום באמצעות חומת-האש והגדרה, הקובעת כי חיבורי רשת מקבלים Timeout לאחר תקופה קצובה של חוסר פעילות.	הארגון יחיל מגבלות על אורך חיי החיבור וכן ינטר וינתק חיבורי תקשורת ללא תשדורת.	יש לנתק חיבור רשת המקושר ל-session בעת סיומו, או לאחר פרק זמן מוגדר של חוסר פעילות.	9.4	אבטחת רשת



2	ניתן ליישם באמצעות הפרדת רשת ה-VOIP לרשת נפרדת מהרשת הרגילה, הגבלת חיבוריות ציוד שאינו טלפוניה לרשת באמצעים כגון NAC, הזדהות של הציוד אל מול שרתי ה-VOIP וכן שימוש בהצפנה והזדהות באמצעות SSL.	הארגון יגדיר מתי וכיצד מותר/אסור לבצע שימוש בשירותי VOIP (המוטמעים במערכות הארגון או כשירות חיצוני) וכן יפעיל אמצעי אבטחת מידע על-מנת לאכוף הגדרות אלו.	יש להגדיר הנחיות לשימוש בטכנולוגית טלפונית IP (VOIP) וכן לנטר ולבקר את השימוש בה. יודגש כי הכוונה היא לשימוש בתשתית זו לפגיעה במערכות המידע של הארגון ולא לניטור תוכן השיחה.	9.5	אבטחת רשת
1	יוגדרו שרתי DNS פנימיים, אשר יספקו מענה לשרתי הארגון. אפשר גם להגדיר שרתי DNS ייעודיים לאזורים מאובטחים יותר של הרשת. שרתי הארגון יוגדרו כך, שהפנייה לשירותי DNS תבוצע אך ורק לשרתים אלו.	הארגון יאפשר קבלת שירותי תרגום כתובות (DNS) אך ורק משרת פנימי מאובטח, זאת במטרה למנוע ניתובי תקשורת שגויים (במזיד או בשוגג) אל יעדים עוינים.	יש לוודא, כי שירותי תרגום כתובות (DNS) מסופק על-ידי שרת מהימן (פנים-ארגוני וכן חוץ-ארגוני).	9.6	אבטחת רשת
1	ניתן ליישם באמצעות שימוש בהרחבות DNSSEC של שירותי ה-DNS.	הארגון יוודא, כי התשובות המוחזרות משרת תרגום הכתובות לא ניתנות לשינוי באמצעות מנגנונים כגון חיתום התשובות הנשלחות על-ידי תעודה דיגיטלית.	יש לוודא כי התשובות המתקבלות משרת תרגום הכתובות אמינות ולא שונו במהלך התשדורת.	9.7	אבטחת רשת
2	ניתן להשתמש בתעודות SSL המזהות את השירות ובאמצעות שרת CA פנימי מאובטח, אשר מנפיק תעודות לשירותים השונים בארגון. השירות נתמך בתשתית ה-Active Directory וכן שירותי Kerberos של מיקרוסופט. את בקרת ניהול השיחה (Session) ניתן ליישם באמצעות שימוש בבקרת Session ברמת השרת (כדוגמת IIS או Apache), או ברמת הרשת באמצעות Load Balancer.		יש להגן על אמינות התקשורת ברמת session, כך ששני קצות ה-session יהיו בטוחים בנכונות זהות הצד השני (הגנה מפני session, MITM, hijacking וכו'). הארגון יפעיל בקרות אמינות באמצעים טכנולוגיים, כדוגמת תעודות דיגיטליות, בעת יצירת חיבורי תקשורת בין השירותים והמערכות השונים.	9.8	אבטחת רשת
2	ניתן לממש באמצעות יישום חומות-אש, המבדילות בין רשת הארגון ובין רשתות חיצוניות.		יש לשלוט בתעבורת הרשת היוצאת/נכנסת לארגון, כך שהתעבורה אל תוך הארגון ומחוצה לו תתאפשר אך ורק בהתאם למדיניות שהוגדרה (גישה בפרוטוקולים מותרים, SERVICE מאושרים, ממקורות/אל יעדים מאושרים וכו').	9.9	אבטחת רשת
3	ניתן להפריד את הרשתות באמצעות חומות-אש ארגונית בין הסביבות, הגדרת סביבות כגון אזור חיץ (DMZ) לטובת שירותים המוחזנים לרשת		יש לנטר ולשלוט בצומתי תקשורת מרכזיים בתוך רשת הארגון. הארגון יחלק את הרשת שלו לתת-רשתות לפי רמת	9.10	אבטחת רשת



	האינטרנט, רשתות ניהול אשר יחוברו מאחורי חिבור מאובטח, רשתות אשר יכילו שירותים רגישים ומערכות רגישות.		הסיכון / סיווג המידע במערכות		
	שימוש בשרת מסופים (Terminal Server) לצורך התחברות למערכת.	הארגון יצמצם ויאחד ערוצי תקשורת כדי להבטיח שליטה טובה על החיבורים למערכת.	יש להגביל את מספר ערוצי התקשורת החיצוניים למערכת.		
1	הגדרת "חוק אפס" בחומות האש, החוסם את כל התעבורה שלא אפשרה באופן מפורש. יש לוודא, כי הניתובים מוגדרים כך, שכל התעבורה תנותב דרך חומות-האש.	הארגון יגדיר את חוקי הסינון של תעבורת הרשת באופן החוסם בבירור מחדל כל תעבורה שלא הוגדרה במפורש כמותרת.	יש לחסום כברירת מחדל כל תעבורת רשת ולאפשר ידנית כל תעבורה רצויה על-ידי כלל חריגה.	9.12	אבטחת רשת
2	ניתן להגדיר את תחנות העבודה עם מדיניות (Policy) הקובעת, כי רק כרטיס רשת אחד יהיה פעיל בכל עת, ברמת השרתים, יוגדרו חיבורים אך ורק לרכוזות של הארגון, מאחורי חומת-אש, תוך כדי ביטול כרטיסי רשת נוספים (שלא מחוברים לרשת נדרשת בהגדרה, כגון רשת אחסון), כדוגמת כרטיסי רשת קווים ואלחוטיים.		יש למנוע ממכשירים ליצור תקשורות מקומיות על המערכת במקביל לתקשורת דרך חיבור חיצוני, כדי למנוע מצב שבו המחשב משמש גשר אשר מקשר את העולם החיצוני לתוך הרשת הפנימית של הארגון.	9.13	אבטחת רשת
3	ניתן ליישם באמצעות שרת מתווך (Proxy) המחובר לעולם ושהגלישה מבוצעת דרכו בלבד. השרת המתווך יוגדר עם אפשרות להגביל את החיבורים לאתרים לא מורשים ולקטגוריות לא מורשות. כמו כן, שרתים יוגדרו כך, שתאפשר גישה לאינטרנט לטובת עדכונים בלבד דרך השרת המתווך (אם אי אפשר להשתמש בשרת עדכונים ייעודי של יצרן המערכת).		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 ליצור תווך, אשר ימנע תקשורת ישירה החושפת את משאבי הארגון אל רשת האינטרנט, וכן במטרה לאפשר יישום בקורות והגנות מרוכזות על ערוצי התקשורת אל מול רשת האינטרנט.	9.14	אבטחת רשת
2	ניתן ליישם באמצעות מערכות NAC.	חיבור ציוד לא מורשה לרשת הארגון חושף את משאבי הארגון לפגיעה בסודיות ובשלמות משאבי המחשוב והמידע ובזמינותם.	יש ליישם מנגנונים למניעת חיבור פיזי לא מורשה לרשת הארגון.	9.15	אבטחת רשת
3	לדוגמה: סינון תעבורה שאינה עומדת בסטנדרטים בחומות-האש, יישום Firewalls XML.	יש ליישם מנגנונים אלו על-מנת להתגונן מפני שימוש זדוני בפרוטוקולים שאינם מאובטחים/מורשים. כמו כן, יש לוודא, כי חבילות התקשורת	יש ליישם מנגנונים המסננים תקשורת שאינה תואמת את מבנה הפרוטוקול/המידע המצופה.	9.16	אבטחת רשת



		מגיעות בתצורה הנכונה וכי לא עברו שינוי לפני הגעתן ליעד.			
2	מרבית ציודי אבטחת המידע מאפשרים הגדרה כך שניתנת יתירות לכיוון ציוד משני (חומת-אש משנית לטובת יתירות, נתיב תקשורת מאובטח אחר ועוד), ובמידה שאין יתירות, יעביר הכשל את המערכת למצב Fail- Close.		יש לוודא, כי במקרה של כשל תפעולי של אחד ממכשירי הגנת הגבולות (חומת-אש וכו') - רמת אבטחת המערכת לא תיפגע. יש להגדיר את ציוד אבטחת המידע כך שיחסום תקשורת בעת כשל.	9.17	אבטחת רשת
2	ניתן להשתמש בכלים, כגון חומת-אש (Firewall), כלי VPN המאפשרים התחברות מאובטחת לרשתות ניהול, Access Control ברמת הנתבים, שרתים מתווכים (Proxy).		יש להשתמש במנגנוני הגנת גבולות כדי להפריד בין רכיבי מערכת התומכים במשימות או בשירותים עסקיים, שהוגדרו על-ידי הארגון ככאלה שדורשים הפרדה. העסק יגדיר, כי הפרדת הרשתות לאזורים מאובטחים תבוצע באמצעות ציוד אבטחת מידע ייעודי.	9.18	אבטחת רשת
1	ניתן ליישם באמצעות ניהול כתובות מרוכז על ממשק הניהול המרכזי של חומת- האש, או באמצעות רישום ידני (מנוהל ומבוקר) של כתובות הרשת השונות.		יש להשתמש בכתובות רשת נפרדות (תת-רשת שונה) כדי להתחבר למערכות באזורי אבטחה שונים. העסק יגדיר, כי לכל תת-רשת יהיה טווח כתובות נפרד, אשר יפורסם לחומת-האש ולנתבים.	9.19	אבטחת רשת
2	לדוגמה: הצפנת תעבורה היוצאת אל מחוץ לארגון, הצפנת קווי תקשורת על- גבי תווך ציבורי.		יש ליישם מנגנונים לשמירה על שלמות תעבורת רשת על-גבי תווך ציבורי ועל סודיותה.	9.20	אבטחת רשת
3	המלצות הקשחה ניתן למצוא בתקנים מקובלים, כגון SANS, DISA ובאתר הרשמי של היצרן.		יש להגדיר, לתעד וליישם מדיניות הקשחה לציודי תקשורת, אשר מספקת מענה לדרישות אבטחת המידע של הארגון. הארגון יגדיר דרישות הקשחה למערכות התקשורת בארגון, בדגש על מה הן דרישות הבסיס, תדירות העדכונים ורמת הסיווג, ואז יתעד את הדרישות במסגרת- על, שתהווה בסיס לכתיבת נוהלי ההקשחה. מסמכי Baseline וכן	9.21	אבטחת רשת



			התייחסות לדרישות הקשחה במסמכי המדיניות. כמו כן, יש להגדיר מי אחראי על יישום ההקשחות בפועל ואיך מתבצעת הבדיקה השוטפת של הבקורות. 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 היצרן.		
3	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 באמצעות ממשק הניהול של כל רכיב בנפרד.		יש להטמיע מנגנונים לניהול מרוכז, ליישום ולאימות הגדרות התצורה של ציודי התקשורת.	9.22	אבטחת רשת
2	ניתן ליישום ישיר בממשק הניהול של המערכת. ניתן ליישם תהליך אישורים לפתיחה/הסרה של חוקים, כמו גם את יצירת החוקים והסרתם בפועל במערכת באמצעות מערכות לניהול שינויים אוטומטיים.	הארגון יגדיר את תצורת ניהול המדיניות של מערכת חומת-האש, אשר תכלול התייחסות לתהליך הוספה/הסרה של חוקי ניתוב במערכת, כולל תהליך אישור להוספה/הסרה של חוקים. כמו כן, יש להגדיר את אופן התיעוד והפירוט לגבי כל חוק אשר נפתח בחומת-האש לצורך ניהולו התקין.	מנגנון (מקומי או מרכזי) לניהול מדיניות חומת-אש.	9.23	אבטחת רשת
3	ניתן ליישום באופן ממוכן באמצעות מערכות ממוכנות לניהול השינויים, או, לחלופין, לבצע תהליך ידני של בחינת החוקים וההגדרות.		טיוב של חוקי חומת-האש. הארגון יבצע תהליך של בדיקת החוקים של מערכת חומת-האש וטיובם, לצורך שמירה על כשירות המערכת וכן לצורך וידוא כי לא קיימים חוקים, העלולים לחשוף את הארגון לסיכונים שלא לצורך.	9.24	אבטחת רשת
2			סריקת רשת תקופתית – מעת לעת ולא יאוחר מ - 18 חודשים ממועד הסריקה הקודמת.	9.25	אבטחת רשת



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 ובקורות 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.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
הפרדת סביבות	10.2	יש להגדיר סביבות נפרדות לפיתוח, לבדיקות ולייצור.	הארגון יגדיר ויתחם את הסביבות שיש צורך להפריד ביניהן במטרה למנוע זליגת אירועי סייבר בין הסביבות במקרה של פגיעה באחת מהן.	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 רמה כסביבת הייצור.	מאחר שלסביבות הנמוכות יותר נגישים מפתחים ואנשי אבטחת איכות באופן פחות מבוקר, קיים חשש כי נתונים רגישים ידלפו החוצה. נוסף על כך, רמת האבטחה בסביבות אלה על-פי רוב נמוכה מרמת האבטחה בסביבת הייצור. לטובת צמצום החשיפה בשל גישת המפתחים וגורמים נוספים אל סביבות הבדיקות והאינטגרציה, יש למנוע העברת נתונים רגישים לסביבות אלו.	2
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 לא מורשית במקרה של פריצת חשבון המשתמש או ניצול הרשאות לרעה.	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 לעתים כחלק מתהליכי פיתוח ובדיקות. במטרה למנוע ניצול לרעה של תהליכים אלו, נדרש ליישם תהליך העברת נתונים מבוקר, המחייב קבלת אישורים מתאימים טרם ביצועו.	2



3	ניתן ליישם במסגרת "ועדת עלייה לייצור", המרכזת שינויים בסביבת הייצור ואישור טרם ביצוע המעבר.	יש ליישם תהליך העברת רכיבי תוכנה לסביבת הייצור, שמטרתו לוודא השלמת תהליכי בדיקות וקבלת האישורים המתאימים טרם ביצוע המעבר.	יש להגדיר תהליך מבוקר של העברת רכיבי תוכנה מסביבות הפיתוח והבדיקות לסביבת הייצור.	10.6	הפרדת סביבות
2		סביבות ייצור נוטות להיות מנוהלות בקפידה ובעלות בקורות ואמצעי הגנה נרחבים, בעוד סביבות פיתוח ובדיקות נוטות להיות בעלות ניהול רופף יותר ומכילות פחות בקורות ואמצעי הגנה. כדי 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.	יש להפריד בין סביבות המיישמות רמת אבטחה שונה באופן הלוקח בחשבון את רמת האיום הנשקפת לסביבה ה"מוגנת יותר" מהסביבה ה"מוגנת פחות".	10.7	הפרדת סביבות
3		הפרדה מלאה בין סביבות דורשת יישום רשתות פיזיות נפרדות ותשתיות משותפות דורש יישום מנגנוני הפרדה מספקים, המותאמים לרמת האיום ולאופי הסיכונים הנשקף לסביבה הטכנולוגית.	יש ליישם את ההפרדה בין הסביבות ברשת התקשורת, במערכות האחסון, בווירטואליזציה, בתהליכי ההזדהות ובניהול מפתחות ההצפנה.	10.8	הפרדת סביבות
3	ניתן ליישם באמצעות טכנולוגיות סינון מתקדמות, המאפשרות מסנני תוכן וחוקי סינון מתקדמים.	הפרדה מלאה בין סביבות דורשת יישום רשתות פיזיות נפרדות ותשתיות משותפות דורש יישום מנגנוני הפרדה מספקים, המותאמים לרמת האיום ולאופי הסיכונים הנשקף לסביבה הטכנולוגית.	יש ליישם בממשקי תקשורת והעברת נתונים בין סביבות מנגנוני סינון דו-כיווניים, המונעים מעבר קוד עין, תקיפת חולשות, ניצול ממשקים אפליקטיביים והוצאה לא מבוקרת של מידע.	10.9	הפרדת סביבות

11. מחשוב ענן ציבורי:

ארגונים רבים נסמכים בקצב הולך וגדל על שירותי ענן לצורך עיבוד מידע ואחסון. 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 בקורות ההגנה בהתאם – הן ברמת הארגון והן ברמת הספק. הארגון נדרש לוודא, כי ספק שירותי הענן מתחייב לעמוד בתקנים וברגולציה הנדרשים מהארגון, לקיים את בקורות ההגנה בסייבר המתאימות לערכיות המידע ולהגדיר תהליכי בקרה ופיקוח מתאימים. תוכנית 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.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
	בקרה נדרשת	הסבר	המלצות	



1	במקרה של שירותים מסוג תשתיות PaaS או IaaS, אחריות חלוקה הינה גם לניהול המשתמשים, לניטור השימוש על-ידי המשתמשים, לניהול הנתונים ולאבטחתם, 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 כחלק מהשירות, באמצעות כלים הקיימים בארגון, או באמצעות ספקים חיצוניים, המספקים שירותי אבטחת ענן.	בעת השימוש בשירותי ענן ציבוריים יש חלוקת אחריות להגנת הסייבר בין הנושאים שבאחריות הספק ובין נושאים הנשארים באחריות חלוקה. חלוקת אחריות זו תלויה באופי השירות ובמודל המימוש. על הארגון להבין מה הם הנושאים הנמצאים באחריותו וליישם את ההשלכות של אחריות זו.	יש להבין את חלוקת האחריות לאבטחת השירות בין ספק השירות ובין הארגון וליישם את בקרות ההגנה בהתאם.	11.1	מחשוב ענן ציבורי
2	מדיניות בנושא שימוש בשירותי ענן עוסקת, בדרך כלל, בנושאים הבאים: מה הם השירותים המותרים לשימוש בארגון, מה הן הדרישות הספציפיות של הארגון, נושאים שיש לכלול בהתקשרות עם ספקים, ניהול סיכונים 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).	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.	יש לכתוב וליישם מדיניות שימוש והגנה על שירותי ענן ציבוריים, לבקר ולעדכן אותה תקופתית.	11.2	מחשוב ענן ציבורי
2	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 הפעילים 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 חומת-אש, filtering וכו'). במקרים רבים תוכנות לניהול שכר, לשיתוף מסמכים, לבניית טפסים וסקרים ועוד נמצאות בענן והארגון אינו "מודע" לכך (Shadow IT).	ארגונים שונים כפופים להנחיות רגולטוריות, המתייחסות לשימוש בשירותי ענן, כגון הגנת פרטיות, רגולציה מגזרית או חבות חוזית לצדדים שלישיים. חובות אלה מכתיבות לעתים כללים נוקשים לשימוש בשירותי ענן.	יש לוודא כי ספק שירותי הענן מתחייב לעמידה בתקנים וברגולציה הנדרשת, בהתאם לחובות הארגון ולתקנים שסוכמו עם הספק.	11.3	מחשוב ענן ציבורי
2	לדוגמה: משלוח שאלונים	יישום הגנת סייבר	יש להגדיר וליישם	11.4	מחשוב ענן



	ציבורי		תהליכי פיקוח ובקרה תקופתיים על עמידת הספק בהתחייבויותיו.	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.	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 בדרישות שהוגדרו בהסכם ההתקשרות ומימושן. חריגות של הספק מההסכם יאושרו על-ידי מנהל הגנת הסייבר בארגון. כך, לדוגמה, במקרה של דרישה עקרונית במדיניות הארגון לעמידה ב-SLA מסוים, או למדיניות סיסמאות שספק התוכנה אינו יכול לבצעה, נדרש הליך פורמלי, שבו הספק מסביר מדוע הוא אינו יכול לעמוד בדרישה זו והאם יש צפי לסגירת פער זה. נתונים אלו יועברו אל מנהל ההגנה בסייבר בארגון לאישור ולהגדרת בקורות מפצות להפחתת הסיכון.
3	מחשוב ענן ציבורי	11.5	יש לבצע בדיקות אבטחת מידע בלתי-תלויות של ממשקים אל שירותי הענן, החשופים לרשת האינטרנט.	בדיקה של שירותי הענן על-ידי הארגון - על ידי צד ג' שנשכר לשם כך, או על-ידי גורם אובייקטיבי אחר - מאפשרת לזהות חשיפות אבטחת מידע ולטפל בהן מבלי להסתמך על הספק באופן בלעדי.	בין הבדיקות הרלוונטיות אפשר 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.
1	מחשוב ענן ציבורי	11.6	יש לוודא כי לא מועברים לשירותי הענן נתונים שעל-פי הרגולציה והמחויבויות של הארגון אסור להעבירם.	יש נתונים אשר הארגון מנוע מלהעבירם לאחסון או לעיבוד בשירותי ענן ציבוריים בשל שיקולים של רגולציה או התחייבות לצדדים שלישיים. טרם העברת נתונים לענן יש לוודא, כי נתונים מסוג זה לא נשמרים או מועברים לשירות הענן.	לדוגמה: בדיקה של שדות הנתונים אשר הארגון מתכוון להעביר לשירותי הענן טרם קבלת ההחלטה בנושא. ניתן גם לבצע על-ידי מחיקה או החלפה של נתונים מסוג זה ברשומות המועברות לשירותי ענן. התייעצות עם גורם משפטי מוסמך בעת ביצוע בחינה והערכה של רגישות הנתונים והאפשרות להעברתם לאחסון בשירות ענן.
2	מחשוב ענן ציבורי	11.7	על תוכנית ההמשכיות העסקית של הארגון להביא בחשבון מצבים של שלילת יכולת הגישה לשירותי הענן.	שירותי הענן הם חיצוניים לארגון, ובדרך כלל התקשורת אליהם היא באמצעות תשתיות ציבוריות, כגון רשת האינטרנט. יש להביא בחשבון, במסגרת תוכנית ההמשכיות העסקית, מצבים שבהם אין גישה	לדוגמה: שיטות חלופיות למתן שירות ללקוחות במקרים של נתק משירות הענן, קובצי נתונים מעודכנים בארגון, המכילים את המידע הנמצא בשירותי הענן.



		לשירותי הענן - אם בשל תקלה אצל הספק, או בשל כשל בתשתיות המאפשרות גישה אל הספק.			
2	לדוגמה: הזדהות חזקה לממשקי ניהול, הגבלת גישה לממשקים רגישים לכתובות אינטרנט מסויימות	לשירותי הענן יש בדרך כלל כמה 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.	יש להגדיר וליישם מנגנונים לבקרת גישה, המתאימים לממשקי הגישה לשירותי הענן, בהתאם לאיומים ולחשיפות הרלוונטיים לכל ממשק.	11.8	מחשוב ענן ציבורי
3	לדוגמה: הצהרה של הספק כי הוא מיישם תהליכי פיתוח מאובטח, הצגה של תוצאות בדיקות אבטחת המידע התקופתיות המבוצעות במערכות הספק.	אזורי החשיפה העיקריים של שירותי "תוכנה כשירות" (SaaS) בענן הם ממשקי משתמש וממשקים אפליקטיביים. על-מנת לצמצם חשיפות מסוג זה, על ספק שירותי הענן ליישם תהליכי פיתוח מאובטח ולשלב בדיקות אבטחה מתאימות בשלבי הפיתוח והתחזוקה. על הארגון לוודא, כי הספק מיישם באופן נאות תהליכים אלו.	יש לוודא, כי ספק שירותי הענן מיישם תהליכים של פיתוח מאובטח ומשלב בדיקות אבטחת מידע בשלבי הפיתוח והתחזוקה.	11.9	מחשוב ענן ציבורי
2	ניתן ליישם באמצעות עיגון הנושא בהסכם ההתקשרות עם הספק ודיווח תקופתי מצד הספק על מספר האירועים שהתרחשו וניתוחם.	יש אזורים בתחום הגנת הסייבר המצויים תחת אחריותו של ספק שירותי הענן. על הארגון לוודא, כי הספק מבצע ניטור של אזורים אלה ומדווח לארגון (לקוח השירות) על חשדות לאירועי סייבר, על-מנת שהארגון יוכל לנקוט את צעדי ההגנה מצדו: הכלה והתאוששות.	יש לוודא, כי ספק שירותי הענן מיישם מנגנוני ניטור לאבטחת מידע ומדווח לארגון על אירועים חריגים.	11.10	מחשוב ענן ציבורי
3	ניתן ליישם באמצעות קבלת פיד אירועים ממערכות הספק למערכות הניטור של הארגון, או על-ידי גישה לממשקי ניטור של הספק עצמו.	על-מנת לקבל תמונה שלמה של אירועי סייבר ואירועים חשודים, על הארגון לנטר את הפעילות בשירותי הענן. ניטור זה יכול להתבצע באמצעות המערכות של ספק שירותי הענן או על-ידי חיבור מערכות הניטור של הארגון לרשומות לוג, המופקות ממערכות הספק של שירותי הענן.	יש לקיים מנגנון לניטור אבטחת מידע במטרה לזהות אירועי סייבר בשירותי הענן.	11.11	מחשוב ענן ציבורי



2	ניתן ליישם באמצעות עיגון הנושא בהסכם ההתקשרות 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.	יש להגדיר וליישם מנגנון, המאפשר המשכיות תפקודית ומחיקה מלאה של הנתונים שנשמרו אצל ספק שירותי הענן במקרה של הפסקת הסכם השירות עם הספק.	11.12	מחשוב ענן ציבורי
---	--	---	---	-------	---------------------

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.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
בקרים תעשייתיים	12.1	יש לכתוב, לנהל ולבקר מדיניות ארגונית להגנה על סביבות בקרים תעשייתיים.	המלצות	2
בקרים תעשייתיים	12.2	יוגדרו כללי שימוש נאות בצידוד בסביבת הייצור ויוצב שילוט המסביר כללים אלו.	הסבר	1
בקרים תעשייתיים	12.3	יש להגדיר את התהליכים הרגישים שקיימות בהם סביבות בקרה תעשייתיות לפי מידת רגישותם.	הארגון ימפה את התהליכים שקיימות בהם סביבות בקרה ויגדיר את התהליכים העיקריים לעסק המעריבים בקרות אלו, על-מנת להבין את רמת הפגיעה העסקית והרגולטורית שעלול לנבוע מכל סביבה כזו.	2
בקרים תעשייתיים	12.4	יש להפריד את רשתות הבקרה ממערכות אחרות ומרשתות חיצוניות.	הארגון יבודד את רשתות הבקרה מרשתות משתמש או שרתים לרשתות נפרדות באופן המגביל גישה ישירה בין הרשתות	1



	מידע אל מחוץ לארגון.				
2		יש ליישם הפרדה נאותה בין רשת הבקרים האופרטיביים ובין מערכת הניהול של הבקרים.	יש להפריד בין מערכת הניהול של בקרי ציוד תעשייתי ובין הרכיבים האופרטיביים של המערכת.	12.5	בקרים תעשייתיים
1	במידה שנדרש לחבר ציוד שונה לצורך ממשקים למערכות הייצור, יש לחברו בסגמנט רשת נפרד מאחורי חומת-האש.	הארגון לא יתקין ברשת הבקרים ציוד שאינו חלק ממערך רשת הבקרים התעשייתיים. ציוד אשר נדרש לחברו יחובר לאזור רשת נפרד, ותקשורת תאפשר באופן פרטני.	אין לחבר התקנים שאינם בקרי סביבת ייצור לרשת בקרי הייצור.	12.6	בקרים תעשייתיים
2	ניתן ליישם באמצעות מערך VPN לשרת ניהול ומשתמשים ייעודיים לכל ספק (בעדיפות למשתמש לכל עובד של הספק), אשר יינעלו בשוטף ויפתחו אך ורק במידת הצורך.	הארגון יטמיע מערך תקשורת מאובטח לגישת ספקים ויבקר את גישת הספק לארגון באמצעות מתן הרשאה מראש לכל התחברות ספק לרשת הבקרה.	גישת ספקי תמיכה לרשת הייצור תאופשר בהרשאה מראש וכן באמצעות תקשורת מאובטחת ומזוהה, המאפשרת רישום של פעולות הספק.	12.7	בקרים תעשייתיים
2	ניתן להגביל את רשתות הבקרה בחומת-האש ולא לאפשר תקשורת ישירה לאינטרנט מרשתות אלו. עדכונים יאופשרו מרשת חיץ באופן פרטני ולאחר מעבר דרך ציוד כגון PROXY.		לא תאופשר גישה ישירה לאינטרנט מסביבת הבקרים התעשייתיים וכן מסביבת ממשקי אדם-מכונה.	12.8	בקרים תעשייתיים
2	ניתן להתבסס על מסמכי הקשחה של יצרני מערכת ההפעלה והאפליקציות ולכבות שירותים, לחסום פורטים, להגביל גישה אפליקטיבית לפונקציות מסוימות ועוד.	הארגון יבטל ו/או יגביל שירותים לא נחוצים על כלל המערכות בסביבת הבקרה, בין אם ברמת מערכת ההפעלה, ברמת התקשורת וברמת האפליקציה.	יוגבלו שירותים לא נחוצים בסביבת הייצור ובמערכות תומכות, כגון ממשקי אדם-מכונה וחיישנים חכמים.	12.9	בקרים תעשייתיים
2	בכל מקרה שבו ניתן להשתמש בגרסאות מאובטחות של פרוטוקולים אלה יש להשתמש בגרסאות אלו (HTTPS, SFTP), (SNMPv3 ועוד).	יש להשתמש בפרוטוקולים המאפשרים אימות המקור והיעד והצפנה של התווך בציוד תומך.	יש להשתמש בתקשורת אמינה בין ציודי הקצה לבקרים התעשייתיים במידת האפשר.	12.10	בקרים תעשייתיים
4	יש להגדיר כלים להעברת תקשורת חד-כיוונית בין חיישנים ומערכות בסביבות רגישות.		יוגדר מערך תקשורת חד-כיווני ממערכות ייצור לציוד החישה.	12.11	בקרים תעשייתיים
1	יש להעדיף שלא להשתמש בכל ברשתות אלחוטיות ברשת הבקרה, אך אם הדבר נדרש לצורך עסקי - תוקם רשת זו בנפרד, כשגם ניהולה יהיה בנפרד והיא לא תוצמד ל-VLAN כלשהו של הרשת הפנימית.	הארגון יטמיע רשת אלחוטית ייעודית נפרדת מהרשת האלחוטית הארגונית שתשמש אך ורק לטובת תקשורת ברשת הבקרה. רשת זו לא תנותב לרשת הארגונית, ולהיפך.	רשתות אלחוטיות בסביבת הייצור יופרדו מרשתות אלחוטיות ארגוניות.	12.12	בקרים תעשייתיים



1	יש להשתמש ב WPA-2 PSK, ובמידת האפשר מומלץ להשתמש בגרסה מבוססת תעודות דיגיטליות לרשתות אלחוטיות אלו.		תקשורת אלחוטית בסביבת הייצור תוגבל באמצעות פרוטוקולים מאובטחים.	12.13	בקרים תעשייתיים
2	מומלץ לחבר את הרשת האלחוטית לשרת Radius ייעודי, אשר יאמת משתמשים ברשת זו ויאפשר את ניהולם.	הארגון יגדיר משתמש נפרד לכל אדם ולכל ציוד ברשת האלחוטית.	יוגדר משתמש נפרד לכל לקוח קצה ברשת אלחוטית בסביבת הייצור.	12.14	בקרים תעשייתיים
3		הארגון יגדיר משתמש אישי לכל אדם העובד מול ממשק אדם-מכונה. אם העמדה הינה שיתופית, ניתן להשתמש בהזדהות כרטיסים חכמים.	הגישה לממשקי אדם-מכונה תאופשר באמצעות משתמשים אישיים לכל מפעיל.	12.15	בקרים תעשייתיים
4	ניתן להשתמש במגוון אמצעים, כגון ביומטריה, כרטיסים חכמים, OTP ועוד.	הארגון יגדיר הזדהות חזקה בגישה לממשק אדם-מכונה.	הגישה לממשקי אדם-מכונה תאופשר באמצעות הזדהות חזקה.	12.16	בקרים תעשייתיים
2	ניתן להשתמש במגוון אמצעים, כגון כלים להקלטת מסכים ופעילויות משתמש, רישום לוגים של אפליקציה וכד'.	הארגון יגדיר מערכות הקלטת פעילות/רישום לוגים על שרתי הניהול של סביבת הבקרה.	יותקנו מערכות ניטור ורישום פעילות על שרתי ניהול.	12.17	בקרים תעשייתיים
3	ניתן ליישם באמצעות כלי IPS רשתי, כלי HIPS וכלים דומים, כגון Honeypots.		יותקנו כלי עזר, כגון כלי זיהוי חדירות בסביבת רשתות הניהול של סביבת הייצור.	12.18	בקרים תעשייתיים
3	ניתן ליישם באמצעות מגוון כלי File Integrity Checking, כולל כלים כמו Verifier של מייקרוסופט או מקביליו, שמסופקים כחלק מחבילות ההגנה על תחנות קצה.		יותקנו כלי וידוא חתימות קבצים (Integrity Checking) לסריקת הקבצים המועברים לסביבת הניהול או המותקנים בסביבת הניהול.	12.19	בקרים תעשייתיים
1	ניתן ליישם באמצעות כלי anti-malware ייעודיים, בהתאם לסוג המערכת.		יותקנו כלים ייעודיים כנגד נזקות בממשקי אדם-מכונה.	12.20	בקרים תעשייתיים
2	ניתן ליישם באמצעות הקמת סביבה נמוכה (לפחות חלקית), הפניית התקשורת לסביבה זו בזמן חלון תחזוקה על סביבת הייצור ובדיקת התהליך.	הארגון יוודא התקנה של עדכונים בסביבת בדיקות ויריצם לאורך זמן לצורך בדיקת היציבות של המערכת והתהליך.	עדכוני תוכנה של היצרן יותקנו על סביבות נמוכות (סביבות בדיקה) טרם התקנתם בסביבת הייצור.	12.21	בקרים תעשייתיים
1		הארגון יטמיע בתוך פרק זמן סביר עדכוני מערכת הפעלה ואפליקציה כפי שנתקבלו מיצרן המערכת וידרוש מהספק עדכוני אבטחה לליקויים חמורים המתפרסמים.	יותקנו עדכוני מערכת הפעלה הנתמכים על-ידי הספק בסביבת הייצור.	12.22	בקרים תעשייתיים
3	ניתן להשתמש בכלים כגון Bit9, נועלים את תצורת המערכת.	הארגון יטמיע כלים, הנועלים את תצורת המערכת לתצורה "נקייה" במידה שאין אפשרות לעדכן את	כלי "נעילת תצורה" יותקנו על מערכות "סוף מחזור חיים" (End Of Life), ובהם מערכות הפעלה	12.23	בקרים תעשייתיים



מיושנות.	הציווד.		
12.24	תוגבל היכולת לחיבור 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
12.25	העברת קבצים ממדיה נתיקה למערכות הייצור תבוצע לאחר "הלבנת" הקבצים המועברים.	הארגון יטמיע מערך "הלבנת" קבצים ובדיקתם לעומק באמצעות כמה כלים טרם העברתם לסביבת הבקרים.	3
12.26	יתקיים מערך יתירות לרכיבים קריטיים בסביבת הייצור.	הארגון יטמיע מערכת יתירות של שרתים וחיישנים קריטיים לסביבות הבקרה לצורך המשכיות התהליך.	2
12.27	תוגבל גישה פיזית לפי צורך עסקי בלבד לסביבת הבקרים התעשייתיים וכן לציוד התקשורת בסביבה זו.	הארגון יגביל גישה פיזית לארונות תקשורת, לרכיבים ולעמדות ניהול של סביבת הבקרים.	2
12.28	תוגבל גישה לוגית לפי צורך עסקי בלבד לסביבת הבקרים התעשייתיים וכן לציוד התקשורת בסביבה זו.	הארגון יגביל גישה משתמשים ארגוניים שאין להם נגיעה עסקית למערך הבקרה וימנע גישתם לציוד ולרשתות אלו.	2
12.29	תוגבל במידת האפשר גישה לוגית (פונקציונלית) למערכות הייצור, ובכללן ממשקי הבקרה, ממשקי הדגימה וממשקי אדם-מכונה.	גישה למערכות הניהול תוגבל לפי פרופיל משתמש. בקר מערכת לא ישנה הגדרות ופרמטרים של מערכת. שינוי פרמטרים יבוצע על-ידי משתמש ניהולי.	3
12.30	יש לבצע בדיקות אבטחת מידע בסביבות הייצור ובממשקי הניהול, ובכללן מבדקי חדירה.	הארגון יגדיר מתווה בדיקות כולל למגוון הרכיבים ברשת הבקרה, בדגש על בדיקות אבטחת מידע מקיפות לכלל הרכיבים, על-מנת לשמור על רציפות התהליך העסקי.	2
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.	2

**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.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
אבטחת טלפונים סלולריים	13.1	יש להגדיר מדיניות שימוש בטלפונים ניידים ולעדכנה באופן תקופתי.	על הארגון להגדיר מדיניות שימוש בטלפונים ניידים לצורכי הארגון, לרבות גישה ליישומים ארגוניים ושמירה של נתונים רגישים של הארגון מכשיר 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.	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 וכד'.	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 לא מוכרות או מסוכנות וכד'.	3
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.	2
אבטחת טלפונים סלולריים	13.5	יש ליישם כלי הגנה ייעודיים, המזהים וחוסמים גישה לא 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.	3



2	ניתן ליישם באמצעות שימוש בפרוטוקולי הצפנה מקובלים ובאמצעות יישומים (אפליקציות) המבצעים הצפנה בעת הגישה לרשת הארגון.	תקשורת נתונים, הנכנסת ויוצאת מטלפונים ניידים, עושה שימוש ברשתות ציבוריות ולא מאובטחות. על-מנת להגן על המידע מחשיפה - יש להצפינו.	יש ליישם הצפנה של נתונים רגישים בתקשורת הנכנסת והיוצאת ממכשירים ניידים.	13.6	אבטחת טלפונים סלולריים
3		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.	יש ליישם אמצעי בקרת גישה לחיבור של מכשירים ניידים לרשת הארגון.	13.7	אבטחת טלפונים סלולריים
2		אכיפת תצורה מאובטחת של טלפונים ניידים ושליטה מרחוק בנתונים רגישים הנשמרים על מכשירים ניידים מתאפשרת באמצעות מערכת ניהול מרכזית ורכיבי ניהול, המיושמים על המכשירים.	יש ליישם מערכת ניהול מרכזית, המנהלת את תצורת המכשירים הניידים ומאפשרת מחיקה מרוחקת של נתונים מהמכשיר.	13.8	אבטחת טלפונים סלולריים
3		על-מנת לזהות אירועי תקיפה של מכשירים ניידים ולאפשר הכלתם ותגובה מתאימה, יש ליישם מערכת ניטור מרכזית, המקבלת התרעות מרכיבים המיושמים על המכשירים הניידים.	יש ליישם מערכת ניטור אבטחת מידע מרכזית, המקבלת התרעות על אירועים חריגים במכשירים הניידים ומאפשרת הכלה ותגובה לאירועים.	13.9	אבטחת טלפונים סלולריים
4		מכשירים ניידים עושים שימוש ברשתות ציבוריות ולא מאובטחות - על הארגון להגדיר כללי התנהגות וזהירות בעת ביצוע שיחות טלפון רגישות.	יש לקבוע מדיניות להגנה או להגבלה של שיחות המבוצעות באמצעות טלפונים ניידים.	13.10	אבטחת טלפונים סלולריים

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.

סיווג העסק	טור ג'	טור ב'	טור א'		
	המלצות	הסבר	בקרה נדרשת		שם הפרק
2	פרק ניהול שינויים בתוך מדיניות אבטחת המידע הארגונית ונהלים תומכים.		יש לכתוב וליישם מדיניות לניהול תצורה, לבקר ולעדכן אותה תקופתית.	14.4	ניהול שינויים
2	ניתן ליישם באמצעות הכנת תיק מערכת.	הארגון יתעד את תצורת מערכת המידע בעת הקמתה, כולל תיעוד הרכיבים, תיעוד התקשורת, תיעוד הגדרות המערכת וכן	יש לקבוע, לתעד ולעדכן בעת הצורך את התצורה הבסיסית הנדרשת של מערכת המידע.	14.2	ניהול שינויים



		נוהל התקנתה.			
2	ניתן ליישם באמצעות תהליך תיעוד שינויים.	הארגון יתעד את השינויים במערכות המידע בעת שינוי תצורה משמעותי, או אחת לתקופה (הקודם מביניהם).	יש לסקור את התצורה הקיימת של מערכות המידע על בסיס תקופתי, כאשר מתרחשים אירועים שהוגדו על-ידי הארגון וכחלק אינטגרלי בתהליכי התקנה ועדכון גרסה.	14.3	ניהול שינויים
3	ניתן ליישם באמצעות מגוון כלים לגיבוי תצורה, כגון BackBox, גיבוי באמצעות כלי אוטומציה, כגון Chef ו-Puppet ועוד.	הארגון יישם מערך של גיבוי ושחזור תצורה של מערכת המידע ורכיביה.	יש ליישם מנגנונים אוטומטיים על-מנת לשמור על עדכניות, התצורה הבסיסית של מערכת המידע על שלמותה ועל מוכנות ההגדרות.	14.4	ניהול שינויים
2	ניתן ליישם באמצעות גיבוי המערכת באופן מלא לפני השינוי ובאמצעות שדרוג מדורג של רכיבים (סביבת בדיקות/סביבת DR ועוד).	הארגון יוודא, כי קיימים כלים ושיטות לחזרה לאחור עבור שינויים שלא צלחו.	יש לשמור גרסאות קודמות של תצורת המערכת לצורך תמיכה בחזרה לאחור (Rollback).	14.5	ניהול שינויים
2	ניתן ליישם באמצעות קיום ישיבות ניהול שינויים שבועיות ואשרור השינויים תוך הסבר על מהות השינוי.	הארגון ינהל תהליך של אשרור השינויים לפני החלתם.	יש לקבוע אילו שינויים במערכת מוגדרים כשינויי תצורה, לתעד בקשות לשינויי תצורה ואת הסטטוס שלהן (אושרו ובוצעו/נדחו) ולשמור אותן למשך פרק זמן שיוגדר.	14.6	ניהול שינויים
4	ניתן ליישם באמצעות כלים, כגון Remedy.	הארגון יתפעל מערכת מידע, אשר תרכז את תהליך ניהול השינויים בכלל ואת תהליך אשרור השינויים בפרט.	יש ליישם מנגנון אוטומטי לתיעוד בקשות לשינויי תצורה, להתראה לסמכות המאשרת ולאיסור ביצוע שינויים עד שיתקבלו כל האישורים הנדרשים.	14.7	ניהול שינויים
2	ניתן ליישם באמצעות שאלון משלים לבקשת ניהול השינויים, שמפורטים בו הסיכונים בעת ביצוע השינוי.	הארגון ינהל תהליך של הערכת הסיכון כחלק מתהליך ניהול השינויים הארגוני. כחלק משלבי הגשת בקשת השינויים יתועדו ההשפעות הפוטנציאליות על זמינות המערכת ואמינותה.	יש לנתח שינויים במערכת המידע על-מנת לקבוע השפעות אבטחה פוטנציאליות לפני הטמעת השינוי (עקב חולשות, חוסר תאימות, כוונת זדון וכו').	14.8	ניהול שינויים
2	ניתן ליישם באמצעות קיום סביבת בדיקות הדומה בגרסתה לסביבת הייצור.	הארגון יבדוק את השינויים בסביבת בדיקות נפרדת לפני יישום השינויים בסביבת הייצור.	יש לנתח שינויי תצורה במערכת המידע בסביבת בדיקות נפרדת לפני יישום בסביבת הייצור.	14.9	ניהול שינויים
3	יש לבצע באמצעות סקירה של הבקורות הנדרשות ובמידת הצורך אף באמצעות מבדקים, כגון סקר בקורות ומבדקי	הארגון יבדוק את כל המערכת ורכיביה בהתייחס להיבטי אבטחת המידע, ובכללם: אימות, הרשאות, הצפנה,	לאחר ביצוע שינוי תצורה במערכת המידע, יש לבדוק את פונקציות האבטחה על-מנת לוודא כי הן	14.10	ניהול שינויים



	פועלות כהלכה.	הקשחה וכל פונקציונליות אטח מידע אחרת הקיימת במערכת.	חדירה.	
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 גרסאות המדיה).				
שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
אבטחת מדיה	15.1	יש לכתוב וליישם מדיניות הגנה על מדיה (מגנטית, נתיקה, אופטית, מכנית), לבקר ולעדכן אותה באופן שוטף אחת לתקופה.	הארגון יכתוב ויישם מדיניות שימוש והגנה על מדיה, הכוללת התייחסות לאופן השימוש במדיה, אחסונה ואופן השמדת המידע האגור במדיה ואו השמדת המדיה עצמה בסוף השימוש (או סוף חיי המדיה).	2
אבטחת מדיה	15.2	יש לתייג את המדיה בהתאם לרמת הסיווג של המידע האגור בה וכן לציין את אופן הטיפול במדיה בהתייחס להיבטי אבטחת מידע והגבלות על הפצתה.	הארגון יגדיר נהלים ותהליכי תיוג של המדיה וכן יתייג את המדיה עצמה בהתאם לרמת הסיווג של המידע האגור בה.	2
אבטחת מדיה	15.3	יש לאחסן מדיה באופן מאובטח.	הארגון יגדיר את אופן האבטחה של אחסון המדיה, לרבות התייחסות לסוגים שונים של מדיה (מגנטית/אופטית/נתיקה).	2
			ניתן לממש באמצעות תהליכים, כגון הגנה פיזית על אזורי האחסון 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	ניתן לבצע השחרה של מדיה באמצעות תהליך ידני (כגון מחיקה פרטנית של המידע הרגיש, כמו נתוני כרטיסי אשראי או פרטים מזהים של לקוחות וכו'), או באמצעים טכנולוגיים (במקרים שבהם ההשחרה מבצעת מחיקה שיטתית של תבניות ידועות מראש). השמדת מדיה יכולה להתבצע באמצעות גריסה/מגנוט/איפוס על-ידי כתיבה מרובה למדיה.	הארגון יגדיר נהלים ותהליכים להשחרת (השחרה = מחיקת כל מידע רגיש מהרכיב טרם הוצאתו מרשות הארגון או ייעודו לשימוש אחר) והשמדת מדיה וכן ינהל מעקב שוטף אחר ביצוע תהליכי השחרת המדיה והשמדתה. מטרת הבקרה הינה לוודא, כי מידע רגיש לא יוצא מהארגון ללא בקרה.	יש להגדיר תהליכי השחרה ו/או השמדת מדיה.	15.4	אבטחת מדיה
2	ניתן לממש באמצעות עמדות הלבנה ייעודיות, אשר יסרקו את המידע במדיה לפני חיבורה למערכות הארגון.	הארגון יגדיר תהליך של הלבנת המדיה (הלבנה = סריקה וניקוי מאימי קוד עיון) לפני הכנסתה למערכות הארגון.	בעת חיבור מדיה נתיקה אל רשת הארגון יש לבצע פעולות ניקוי כדי לוודא, שהמדיה אינה מכילה נזקות או גורמים זדוניים אחרים.	15.5	אבטחת מדיה
2	ניתן למימוש באמצעות הקשחת תחנות העבודה בהתאם לסוג המערכת/העמדה או הרשאות של בעל התפקיד, כך שלא כל עובד יוכל לחבר התקן זיכרון (כגון Disk On Key) למחשב. ניתן לממש הגדרה, שלפיה כל מידע המוצא מתוך העמדה למדיה נתיקה יעבור וידוא יציאה אל התקן/תיקיה מוצפנת.	הארגון יגדיר ויישם טכנולוגיות ושיטות להגבלת שימוש במדיה. זאת במטרה לצמצם איומי דלף מידע או איומי חדירת קוד עיון לרשת הארגון באמצעות מדיה נתיקה.	יש להגדיר וליישם הגבלות שימוש במדיה תוך שימוש באמצעי אבטחה.	15.6	אבטחת מדיה
3	ניתן לממש באמצעות כלים, כגון הצפנת מדיה נתיקה, הצפנת קלטות גיבוי בעת הגיבוי וכו'.	הארגון יחיל אמצעי הצפנה על מדיה המיועדת להיות מועברת אל מחוץ לארגון, או כזו המצויה באופן שוטף בשימוש מחוץ לארגון (כגון מדיה נתיקה).	יש לממש מנגנוני הצפנה להגנה על מדיה דיגיטלית במהלך העברתה אל מחוץ למתקני הארגון.	15.7	אבטחת מדיה
3	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.	הארגון יגדיר תהליך לבדיקת ציוד ותהליכי הלבנה והשמדה של מדיה, אשר יכללו בדיקה של אפקטיביות התהליכים והטכנולוגיות המיושמות.	יש לבדוק את הציוד להלבנה ולהשמדה של המדיה באופן תקופתי, על-מנת לוודא את אפקטיביות הטכנולוגיה.	15.8	אבטחת מדיה

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 נהלי עבודה מול הספק וכו'.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
	בקרה נדרשת	הסבר	המלצות	



2	לצורך המיפוי ניתן להיעזר גם באיסוף מידע מודיעין סייבר על-אודות הספק, במטרה להתחשב במידע זה במכלול השיקולים וקבלת ההחלטות על-אודות ניהול הסיכון. כמו כן, יש להתחשב במנגנונים, בבקורות ובתהליכים הקיימים בחצרות הספק ובהשפעתם על התהליך העסקי (או התהליכים העסקיים) שהמערכת/השירות תומכים בהם (לדוגמה: בקורות אוטומציה והקמת שרתים ווירטואליים בפלטפורמת הספק בענן ואופן ההקשחה שלהם עלולים להשפיע על הארגון עצמו אם הסביבות לא מוקשחות ו/או ספק שירותי הענן אינו מאובטח/נמצא במדינה עוינת ועוד).	הארגון ימפה ויזהה את האיומים והסיכונים הנובעים משימוש במערכת/שירות הספק על האספקטים הטכנולוגיים והתהליכיים הגלומים בהם, וימפה את הסיכונים כחלק מתהליך ניהול הסיכונים והאיומים הארגוני.	יש להתגונן מפני איומים של שרשרת האספקה על המערכת כחלק מאסטרטגיית "הגנה לרוחב" (Defense in Breadth).	16.1	שרשרת אספקה ומיקור-חוץ
2			באחריות בעל העסק להכין מסמך מדיניות לעניין עמידה בדרישות מסמך זה במקרים של מיקור חוץ לעניין רכישת מוצרים או שירותים רלבנטיים	16.2	שרשרת אספקה ומיקור-חוץ
3	בקורות כאלו יכולות להיות הפרדת סביבות, הפרדת ממשקים, סנטיזציה של הפלט המגיע ממערכות הספק, הפרדת התקשורת באמצעות שרת מתווך (Proxy) ועוד.	הארגון ישתמש בבקורות הקיימות אצלו, או בבקורות ייעודיות אחרות, על-מנת למזער את הנזק ממערכות/שירותי הספק.	במקרים שבהם יש חיבור לרשת הספק, יש ליישם בקורות מונעות, שתפקידן למזער נזק המגיע מתשתיות הספק.	16.4	שרשרת אספקה ומיקור-חוץ
4	ניתן לבדוק את המערכת הן באמצעות כלים לניהול פגיעויות והן באמצעות ביצוע סקרי סיכונים ומבדקי חדירה לפתרון הספק, תוך כדי וידוא שאין ממצאים חמורים אשר ישפיעו על הארגון ועל תהליכיו.	הארגון יבדוק את המערכת/השירות באמצעות כלים פנימיים וכן יערוך מבדקי חדירה טרם עליית המערכת/השירות לשלב הייצור.	יש לבצע בדיקת מערכת/שירות בהיבטי אבטחת מידע לפני היישום בארגון.	16.5	שרשרת אספקה ומיקור-חוץ
3	יש להוסיף את המערכת/שירות לרשימת המערכות הקריטיות בארגון ולהפעיל אמצעי ניטור ובקרה על המערכת/השירות כדי לוודא שאין פגיעה ברציפותו.	הארגון יגדיר מערכת מסוימת כקריטית אם פגיעה בה או ברכיביה משפיעה על תהליך עסקי קריטי.	יש להגדיר את רמת הקריטיות של המערכת/שירות בהתייחס לתהליכים העסקיים המסתמכים עליה.	16.6	שרשרת אספקה ומיקור-חוץ
3		הארגון יגדיר את רמת המהימנות הנדרשת מן המערכת (בהיבטי אמינות, זמינות וסודיות המידע) כפועל יוצא מן התהליך העסקי המונע על-ידי המערכת.	יש להגדיר את רמת המהימנות (Trustworthiness) של המערכת/השירות הנדרשת מן הספק. במידה שהמערכת קשורה בתהליכים	16.7	שרשרת אספקה ומיקור-חוץ



קריטיים בארגון או במידע רגיש, ניתן להגדיר, כי נדרשת רמת מהימנות גבוהה מן המערכת, כך שלאחר מכן יידרש הספק ליישם או לוודא קיום בקורות שרידות, הצפנה ועוד על המערכת וסביבתה, על-מנת לוודא כי אין פגיעה בתהליך העסקי ו/או במידע השמור, המעובד ומועבר באמצעות השירות בהיבטים של אמינותו, זמינותו וסודיותו.

17. אבטחה ברכש ופיתוח:

במסגרת תהליכי רכש ופיתוח, הארגון מכניס מרכיבי סייבר לתוככי 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 הבקורות להקטין את הסיכוי כי הרכש או התוכנה/המערכת המפותחת יחדירו סיכוני סייבר לארגון. הבקורות 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'.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
אבטחה ברכש ופיתוח	17.1	מטרת הבקרה הינה לוודא, כי כלל מערכות הארגון יעמדו ברף ההגנה שהגדיר הארגון הן עבור מערכות המפותחות באופן עצמאי והן מערכות הנרכשות 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, גישה מפתחים לייצור וכו'.	2
אבטחה ברכש ופיתוח	17.3	מטרת הבקרה הינה לוודא, כי היבטי ההגנה שולבו עוד משלב הייזום והתכנון, עבור בפיתוח ועד ההעברה 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 הייזום כך שהארגון יהיה ערוך להטמיע בקורות 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 שהן כוללות סיכונים פרטניים שחלקם מכוסים במסמך זה. לטובת העמקה ניתן לבחון את ההמלצות של תקנים ייעודיים לאבטחת ענן, כגון ISO 27017, תקן CSA וכו'.	3



2	ניתן להגדיר דרישות אבטחת מידע בשלב הייזום, בשלב התכנון (בשלב ה-POC), בשלב הביצוע (שלב הרכש), הפיתוח וההטמעה) ובשלב המסירה (בדיקות אבטחת מידע ומבדקים לפני עלייה ליצור). יש להגדיר בשלבים הללו אחריות להנחיה ואחריות לבקרה כי התהליך והדרישות מתקיימים. שיקולי האבטחה בפרויקט יכללו גם היבטים שאינם טכנולוגיים, או שאינם נוגעים ישירות לפיתוח ולמסירה, כגון שמירת מידע אצל הספק בתום הפיתוח, מידור בחצרות הספק, נוהלי גישה מרחוק, SLA, התחייבות לתמיכה במוצר לפרק זמן מוגדר, אופן העברת קבצים ומידע של לקוחות אל הספק וכו'. יש להיעזר בבקורות הכלולות בפרק מיקור-חוץ במסמך זה.	הארגון ימסד תהליך מסודר של פיתוח מאובטח, המגדיר את שלבי ההטמעה של אבטחת מידע בכל שלב בתהליך הפיתוח ויוודא כי גורמי המפתח, האחראים לשלבים שונים בתהליך הפיתוח, מקבלים אחריות לתפקידם בנושא אבטחת המערכת המפותחת והינם בעלי הידע הנדרש לכך.	הגנת סייבר כחלק ממחזור חיי הפיתוח - יש לקחת בחשבון שיקולי אבטחה בכל שלב במחזור חיי פיתוח המערכת ולהגדיר בעלי תפקידים בהיבטי אבטחה בכל שלב.	17.4	אבטחה ברכש ופיתוח
3	מומלץ לקבל את מסמכי האפיון הפונקציונלי, מסמכי האפיון המפורט ואפיון-העל (FD), (HLD, DD/LLD), הכוללים את תיעוד הבקורות כחלק ממכלול התיעוד המלא של מנגנוני המערכת. תיעוד זה יכלול, לדוגמה, את סוג ההצפנה, את אופן וידוא בדיקת הקלט, את 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').	הארגון ידרוש תיעוד מלא של בקורות אבטחת המידע המוטמעות במערכת על-מנת לוודא עמידה בדרישות אבטחת המידע ולצרכי תהליך ניהול הסיכונים והאיומים הארגוני	יש לדרוש ממפתחי המערכת לספק תיאור פונקציונלי של בקורות האבטחה שיושמו במערכת, ומידע אודות עיצוב ומימוש הבקורות	17.6	אבטחה ברכש ופיתוח
2	עקרונות הארכיטקטורה המאובטחת יכולים להיגזר מבקורות המובאות בפרקים של מסמך זה, מסטנדרטים מקובלים ועוד.	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 הספק	ארכיטקטורה מאובטחת - יש להטמיע עקרונות ארכיטקטורה מאובטחת במסגרת האפיון, העיצוב, הפיתוח, המימוש ושינוי מערכת המידע.	17.7	אבטחה ברכש ופיתוח



		החיצוני.			
3	ספק התוכנה יעביר תיעוד על אופן מימוש עקרונות פיתוח מאובטח בפועל. התיעוד יפרט את הכלים בהם נעשה שימוש, המתודה איתה עובדים, סוגי הבקורות שיש לספק על רמת ההגנה של המערכת ועוד.	הארגון יטמיע מתודולוגיית פיתוח מאובטח ויודא הטמעה של מתודולוגיה לפיתוח מאובטח אצל ספקי מערכות ושירותים המבצעים תהליכי פיתוח.	פיתוח מאובטח - יש לדרוש ממפתחי המערכת שימוש בכלים ושיטות לפיתוח מאובטח כחלק אינטגרלי מתהליך הפיתוח.	17.8	אבטחה ברכש ופיתוח
2	כחלק מתיעוד תצורת קנפוג המערכת יש לכלול - מדריך התקנה, הגדרות להקשחת התשתיות והאפליקציה, פריסה מומלצת וכד'. 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 שסוגיית ניהול שינויים בתצורת המערכות הינו נושא אשר קשה לפיקוח ומעקב באופן ידני, נכסים ברמה 3 יכללו מנגנון מפצה לבחינה אוטומטית של שינוי תצורה (חוקים בתוך ה-SIEM, מערכת ניהול תצורה מרכזית, Continuity control monitoring).	מדריך ההתקנה ותפעול המערכת יספקו את המידע הנדרש לטובת התקנת המערכת בתצורה (קונפיגורציה) בטוחה.	הפעלה בטוחה - יש להחזיק מדריך לניהול מערכת המידע, הכולל את אופן הגדרת התצורה הטובה ביותר עבור היבטי האבטחה.	17.9	אבטחה ברכש ופיתוח
1	ניתן להגדיר את הדרישות הרגולטוריות של הארגון כחלק ממסך דרישות אבטחת מידע סטנדרטי, המיועד לספקי שירות חיצוניים.	הארגון יודא, כי ספקי השירות עומדים בדרישות הציות (Compliance) הארגוניות וכן בדרישות הרגולטוריות החלות במדינות שבהן פועל הארגון.	אבטחת שרשרת אספקה - יש לדרוש מספקי שירותים לציות לדרישות האבטחה הארגוניות, לרגולציות, לסטנדרטים ולהנחיות.	17.10	אבטחה ברכש ופיתוח
2	במקרים שבהם מתקבל שירות מספק חיצוני, ניתן להסתמך על מבדקים אשר בוצעו על-ידי או עבור הספק.	הארגון יודא, כי בוצעו בדיקות אבטחת מידע בטרם העלאה לאוויר של מערכת או שירות חדש, או בעת ביצוע עדכונים למערכת.	יש לבצע בדיקות אבטחת מידע ולטפל בחשיפות שנתגלו בהן טרם הטמעת מערכות ושירותים. בדיקות אלו יכללו, לכל הפחות, בדיקת פונקציונליות האבטחה (מימוש הדרישות) ובדיקת חשיפות אבטחה.	17.11	אבטחה ברכש ופיתוח
2	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 תוכנית העבודה	מטרתו של תיעוד תהליך הטיפול בחשיפות הינו לוודא שלמות ואפקטיביות הטיפול.	יש לתעד את התהליך לטיפול בליקויים ובחשיפות אבטחת המידע שנתגלו במהלך הבדיקות.	17.12	אבטחה ברכש ופיתוח



	התקופתית של מנהל הגנת הסייבר ויוצגו להנהלה אחת לתקופה.				
3	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 ייעשה הן לפני רכישת המערכת והן בעת ביצוע שינויים בסביבת המערכת.	הארגון יבחן מערכות ברמה 3 באמצעות כלים אוטומטיים, המהווים תחליף לסקירת קוד ידני (Code review).	יש לבצע ניתוח קוד סטטי (Static Code Analysis) כחלק ממבדקי אבטחת מידע למערכת/שירות חדש.	17.13	אבטחה ברכש ופיתוח
3	ביצוע סקר סיכונים למערכת בסיום הפיתוח ולפני כניסה לייצור.	מטרת התיקוף של הערכת הסיכונים היא לוודא את התאמת תמונת הסיכונים שבוצעה בעת תכנון המערכת למערכת כפי שפותחה.	יש לבצע תיקוף של הערכת הסיכונים והחשיפות של המערכת לאחר השלמת פיתוחה.	17.14	אבטחה ברכש ופיתוח
3	ביצוע PT באמצעות אנשי הארגון עלול ליצור 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 המכסות את התיחום של המערכת וכי גורם זה ינגיש את התוצרים לארגון (כתיבת הדו"ח המסכם של הבדיקה). הבדיקות יתבצעו בסביבה קרובה ככל האפשר לסביבת הייצור.	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.	יש לבצע את בדיקות אבטחת המידע של המערכת על-ידי גורם חיצוני בלתי-תלוי.	17.15	אבטחה ברכש ופיתוח
3	בדיקות אלו יכולות להתבצע באמצעות הפעלת כלי תקיפה אוטומטיים או באמצעות גורם אנושי. בדיקות אלו יכולות לכלול ניסיונות להשיג גישה לא מורשית, להחדיר קוד עוין לבסיס הנתונים ולממש תקיפות ידועות, כגון CSRF, XSS, SQLI וכו'.	מטרת הבקרה הינה לבחון את אפקטיביות הבקורות וההגנות בפועל. הדבר מבוצע באמצעות ניסיונות לאתגר ולחדור למערכת/תשתית.	יש לבצע מבדקי חדירה למערכת/שירות.	17.16	אבטחה ברכש ופיתוח
3	בשלב המסירה יש לוודא אל מול רשימת הדרישות המוגדרות בתכנון המפורט, כי הן אכן הוטמעו, וכן יש לתעד את מהות הבדיקה ואת תוצאותיה.	יש לנהל רשימת תיוג של דרישות ההגנה שהוגדרו למערכת ולוודא, כי כל הדרישות אכן מומשו על-ידי אנשי הארגון והספק.	יש לוודא כי בדיקות המערכת כוללות אימות, כי בקורות אבטחת המידע שהוגדרו אכן מיושמות בהתאם לאפיון המקורי.	17.17	אבטחה ברכש ופיתוח



3	בדיקות הקוד הדינמיות יבוצעו באמצעות כלי מדף ייעודיים קיימים, או באמצעים כגון Fuzzing, וכן בדיקות אוטומטיות של כלי סריקה בעת ריצה. הדו"חות או הממצאים יבדקו אחת לתקופה על- ידי הארגון באופן מדגמי כדי לוודא, כי אכן מבוצעים תיקונים בהתאם.	יש לדרוש מהספק ניתוח קוד דינמי (Dynamic Code) (Analysis) כחלק ממבדקי אבטחת מידע למערכת/שירות חדש.	17.18	אבטחה ברכש ופיתוח
4	מנגנונים למניעת שיבוש יכולים להיות מיושמים באמצעות חתימת קבצים, הצפנה, יצירת העתקים ועוד.	הארגון יוודא, כי גוף הפיתוח (פנימי או חיצוני) מימש במערכת יכולת למניעת שיבוש קבצים.	17.19	אבטחה ברכש ופיתוח
3	דוגמאות למנגנונים מסוג זה הם: בדיקת רכיבי חומרה, בדיקה ואימות של קובצי תוכנה נכנסים וכד'. 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.	מטרתם של מנגנונים אלה הינם למנוע הכנסה של רכיבי חומרה או תוכנה מזויפים לארגון, בין אם במתכוון או באמצעות הטעיה של גורם בשרשרת האספקה.	17.20	אבטחה ברכש ופיתוח
2	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 התייחסות של סקר מבדק החדירה, כי נושא בדיקות הקלט מכוסה בצורה מקיפה (OWASP יכול להוות נקודת ייחוס טובה) וכן בהתאם למדיניות הארגון בנושא.	מערכות מפותחות יישמו מנגנונים שמטרתם לוודא סינון של קלטים לא צפויים, כגון קלט באורך/פורמט לא צפוי, העלולים להוביל לתוצאה בלתי-צפויה ולפגיעה בחיסיון, בשלמות או בזמינות המערכת בהתאם לרמת ערכיותה.	17.21	אבטחה ברכש ופיתוח
2	ניתן לבצע על-ידי הטמעה של מנגנון ניהול שגיאות, המציג שגיאה סטנדרטית בקרנות שגיאה.	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 אינו	17.22	אבטחה ברכש ופיתוח



		חושף מידע רגיש של המערכת, כגון שמות טבלאות או משתמשים בבסיס הנתונים, שפת כתיבת המערכת, גרסאות של תוכנות וכו'.			
3	ניתן לבצע על-ידי שימוש בספריות תוכנה סטנדרטיות, המסננות תוצאות בהתאם לאופי הפלט הצפוי. כמו כן ניתן לממש באמצעות מערכות לאיתור אנומליות, המבוססות על התנהגות המערכת/משתמש/מערכת הפעלה וכו'.	מערכות מפותחות יישמו מנגנונים שמטרתם לוודא סינון של תוצאות (פלט) לא צפויות, העלולות להיגרם מהתקפה על המערכת ולחשוף מידע רגיש מתוכה.	יש לוודא, כי מערכות נרכשות/מפותחות מיישמות מנגנוני אימות פלט.	17.23	אבטחה ברכש ופיתוח
2	ניתן לבצע על-ידי ניהול נכון של session, מחיקת חיבור בתום פעילות משתמש, אקראיות של מזהי חיבור (Tokens) וכד'.	מערכות מפותחות יישמו מנגנונים, שמטרתם לוודא מניעה של מתקפות על מנגנון ניהול חיבור, כגון חטיפת חיבור (session hijacking) או man-in-the-middle.	יש לוודא, כי מערכות נרכשות/מפותחות מיישמות מנגנוני מהימנות Session.	17.24	אבטחה ברכש ופיתוח

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 בצידוד וכן יתרע 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.

סיווג העסק	טור ג'	טור ב'	טור א'		
	המלצות	הסבר	בקרה נדרשת		שם הפרק
2		מטרת הבקרה הינה להגדיר את ראיית הארגון בנושאים כגון נעילת משרדים בסוף יום, מצלמות אבטחה, כניסת אורחים וכניסת עובדים חיצוניים למתחמי החברה ולאזורים רגישים, הגנה נאותה על חדרי השרתים וחדרי הבקרה וכו'.	יש לכתוב וליישם מדיניות הגנה פיזית וסביבתית, לבקר ולעדכן אותה תקופתית.	18.1	הגנה פיזית וסביבתית
2		יש לכתוב נוהלי בקרת גישה פיזית למתקן הארגון, לרבות: 1. נוהל גישה פיזית; 2. נוהל אורחים במתחם הארגון; 3. נוהל גישה לחדר מחשב/חדר תקשורת.	יש לכתוב וליישם נהלים, אשר יסייעו בהטמעת מדיניות הגנה פיזית וסביבתית ובקורות רלוונטיות.	18.2	הגנה פיזית וסביבתית
2	הנפקת תעודת עובד/מבקר לצורך זיהוי.	יש לתחזק את רשימת מורשי הגישה למתקני החברה ועל הארגון להחזיק רשימה עדכנית.	יש להגדיר ולתחזק רשימת מורשי גישה למתקן שבו נמצא הנכס, לנפק אמצעי הזדהות לצורך גישה למתקן, לסקור את הרשימה תקופתית ולהסיר ממנה אנשים	18.3	הגנה פיזית וסביבתית



			כאשר הרשאת הגישה אינה נדרשת עוד.		
2	דלת + קורא כרטיסים, מנעול, קורא ביומטרי, שומר, קודן וכו'.	יש ליישם בקרת גישה פיזית בכל הכניסות/יציאות ממתקני הארגון.	יש לאכוף בקרת גישה פיזית בנקודות כניסה/יציאה למתקן.	18.4	הגנה פיזית וסביבתית
3	רישום כלל הכניסות והיציאות במסד נתונים/לוגים או רישום ידני באמצעות שומר.	יש לתעד ולשמור את הרישומים (לוגים) של כלל הכניסות והיציאות של כלל המבקרים.	יש לשמור לוגים של גישה פיזית למתקן.	18.5	הגנה פיזית וסביבתית
2	1. יש להגדיר הרשאות גישה (פיזית ולוגית) מתאימות עבור הגורמים המורשים. 2. יש לתעד באמצעות רישום לוגים או רישום נוכחות בעת הגישה לחדרי מחשב. במידה ואי אפשר למכן את תיעוד הגישה לארונות התקשורת וחדרי השרתים, יש לבחון הגנה פיזית עליהם באמצעות מנעול, אשר ימנע מגורמים לא מורשים להתחבר אל ציוד זה.	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 ועל-פי נוהלי הארגון.	יש לבקר, לתעד לאבטח ולאכוף בקרת גישה פיזית לאזורי ריכוזי תקשורת/מחשוב (חדרי שרתים/ארונות תקשורת).	18.6	הגנה פיזית וסביבתית
3	ניתן ליישם בכמה תצורות: 1. על-ידי מערכת בקרת הדפסה, הדורשת 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 הממוקמים באזורים ציבוריים/מרווי משתמשים יהיו "נקיים" וכי מידע אישי לא יהיה נגיש למי שאינו אמור להיות חשוף אליו.	מטרת הבקרה הינה לוודא, כי המידע מגיע לבעלי המקוריים. בקרה זו חשובה בפרט במקומות שבהם יש מידע פרטי, כגון פקסים, הכוללים מידע רפואי או ביטוחי, הדפסה של פרטים אישיים של עובדים וכו'. במקרים אלו, חשוב לוודא כי המידע נחשף אך ורק למי שאמור להיחשף אליו.	יש לשלוט בגישה פיזית למכשירי פלט של המערכת על-מנת למנוע מגורמים לא מורשים להשיג את הפלט (לדוגמה, מדפסות ופקסים)	18.7	הגנה פיזית וסביבתית
3	יש לנטר את כלל הגישות הפיזיות לאזורים רגישים, כגון חדרי שרתים, ארונות תקשורת וכו', באמצעות רישום של הנכנסים והיוצאים.	מטרת הבקרה הינה למנוע גישה מגורמים לא מורשים אל אזורים רגישים. גישה כזו יכולה לאפשר לגורמים עוינים לבצע 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	יש לנטר את הגישה הפיזית למתקן שבו נמצא הנכס על-מנת לגלות ולהגיב לאירועי אבטחה, ולסקור את הלוגים על בסיס תקופתי.	18.8	הגנה פיזית וסביבתית



		הוא מורשה לבצע זאת.			
3	ניתן לעשות שימוש במערכת אזעקה ו/או במוקד ביטחון לצורך ניטור והתרעה מפני גישה לא מורשית למתקן.	יש לעשות שימוש באמצעי ניטור והתרעה לצורך זיהוי גישות שאינן מורשות בשעות ובזמנים שאינם מוגדרים עימי ושעות עבודה מקובלות לצורך זיהוי גישות לא מורשות.	יש לנטר ולהתריע על כל גישה פיזית לנכס שלא בשעות העבודה המקובלות או בימים שאינם ימי עבודה.	18.9	הגנה פיזית וסביבתית
3	ניתן ליישם באמצעות שימוש בכונן מהארגון (קב"ט), מוקד ביטחון חיצוני/חברת שמירה וכו'.		יש להגדיר ולקיים מערך תגובה עבור גישות לא מורשות למתקן הארגון בעת זיהוי.	18.10	הגנה פיזית וסביבתית
4		יש להתקין מצלמות אבטחה במעגל סגור לצורך ניטור שוטף של כלל הכניסות/הפתחים למתקני הארגון, ולנטרם באופן שוטף ורצוף על-ידי איש ביטחון.	יש להטמיע מצלמות וידיאו למעקב אחר גישה פיזית לנכס ולשמור את ההקלטות לפרק זמן שיוגדר.	18.11	הגנה פיזית וסביבתית
2	רישום ביומן מבקרים/תיעוד כלל המבקרים במערכת ייעודית לזימון אורחים למתקני הארגון.	יש לתעד ולתחזק את רשימת האורחים למתקני הארגון.	יש לתעד רשימת אורחים למתקן.	18.12	הגנה פיזית וסביבתית
2	יש לסמן כל כבל בקצותיו על-מנת שעובדי הארגון יוכלו לזהות בקלות לאיזה שרת/מערכת הוא שייך ולמנוע ניתוק בשוגג.	יש להקפיד על סלילה נכונה ותיוג נכון של כלל כבלי החשמל בחדרי השרתים ובארונות התקשורת.	יש לשמור על ציוד החשמל וכבלי החשמל של המערכת מפני נזק.	18.13	הגנה פיזית וסביבתית
2	ניתן ליישם מערך UPS's לצורך אבטחת הורדה מסודרת של המערכות בעת מצב שבו אין זרם חשמל קבוע.		על הארגון להיות בעל יכולת לספק חשמל לטווח קצר באופן שאינו ניתן לשיבוש על-מנת לאפשר כיבוי מסודר של המערכת או העברתה לספק כוח חלופי.	18.14	הגנה פיזית וסביבתית
3	ניתן להשתמש בגנרטור לצורך יישום הבקרה.		על הארגון להיות בעל יכולת לספק חשמל למשך זמן ממושך באופן שאינו ניתן לשיבוש	18.15	הגנה פיזית וסביבתית
1			יש ליישם ולתחזק תאורת חירום אוטומטית, שתופעל באירוע של הפסקה או שיבוש באספקת החשמל, ותכלול יציאות חירום ונתיבי פינוי במתקן.	18.16	הגנה פיזית וסביבתית



1			יש ליישם ולתחזק אמצעים/מערכות לזיהוי וכיבוי אש עבור מערכת המידע, אשר נתמכים במקור אנרגיה עצמאית.	18.17	הגנה פיזית וסביבתית
2	בקרה זו רלוונטית בעיקר בחדרי שרתים.		יש לשמור ולנטר רמות טמפרטורה ולחות מקובלות במתקן שבו נמצא הנכס.	18.18	הגנה פיזית וסביבתית
2			יש להגן על הנכס מפני נזק כתוצאה מדליפת מים באמצעות האופציה ל-master shutoff או שסתומי בידוד.	18.19	הגנה פיזית וסביבתית
2	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 זיכרון שחולקו). הרישום והמעקב יהיו תקופתיים ויכללו למי ניתנה החומרה, לכמה זמן, לאיזו מטרה ותאריך החזרה משוער.		יש לאשר, לנטר ולשלוט ברכיבי מערכת המוכנסים ומוצאים מהמתקן.	18.20	הגנה פיזית וסביבתית
2	רמת האבטחה הפיזית באתר חלופי, כגון אתר ה-DR, תהיה ברמה מקובלת והולמת את המידע המאוחסן שם. מימוש הבקרה תהיה באמצעות תמיכת הנושא בנוהל ובחווה ההתקשרות מול האתר שאליו פורסים בחירום, וכן באמצעות ביקורת תקופתית של הנושא.		יש ליישם בקרות אבטחה באתרי העבודה החלופיים (כגון אתר DR) ולהעריך את מידת האפקטיביות שלהן.	18.21	הגנה פיזית וסביבתית
3		במידת האפשר, יש למקם את המערכות (חדרי השרתים/תקשורת) במיקום מוגן ככל האפשר במרכז המבנה ולא בצמוד לקירות חיצוניים או בקירוב למקורות מים (כולל צינורות).	יש למקם את רכיבי המערכת במתקן שבו פוטנציאל הנזק כתוצאה ממפגע יהיה מינימלי, והאפשרות לגישה לא מורשית תהיה מינימלית.	18.22	הגנה פיזית וסביבתית

**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 להיות 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.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
משאבי אנוש ומודעות עובדים	19.1	על הארגון לקבוע מדיניות המסדירה את הסיכונים הקשורים לגורם האנושי, ועליה לכלול לפחות: מיפוי התפקידים הרגישים מבחינה בטיחותית או אבטחתית, קריטריונים לבדיקת התאמה ואי התאמה של עובדים לתפקידים אלה, אופן המיון ולתפקידים אלה, הדרכות הכשרות לעמידה בדרישות אלה	המלצות	2
משאבי אנוש ומודעות עובדים	19.3	יש להחתים את העובדים על הצהרה לגבי מחויבות להקפיד על דרישות הסייבר של הארגון.	העובד חותם על הצהרות, כי הוא מודע לכך שמערכות הארגון מכילות מידע חסוי ואין להוציאו או לניידו ללא אישור מפורש בהתאם לנוהלי הארגון.	2
משאבי אנוש ומודעות עובדים	19.4	יש להחתים את העובדים על הצהרה לגבי מחויבות לשמירה על סודות הארגון לאחר סיום ההעסקה.	העובד חותם על הצהרה, כי לא ימסור מידע רגיש של הארגון לגורמים שאינם מורשים, וכי לא לקח עמו מסמכים או אמצעי אוגר מידע המכיל מידע עסקי של הארגון.	2
משאבי אנוש ומודעות עובדים	19.5	יש להגדיר דרישות אבטחה לספקים ולגורמי צד ג'.	הארגון יגדיר דרישות אבטחת מידע כחלק ממדיניות ההתקשרות עם ספקים. הדרישות יכללו הגבלות לגבי שיתוף מידע, הסכמי סודיות, הכרה של נוהלי אבטחת המידע בארגון,	2



		הדרכות לספקים ועוד.			
1	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 המתעד את נוהלי השימוש, או באמצעות לומדות הניתנות לעובדים חדשים, וכן באמצעות כלים מיכוניים, כגון Appliction & control URL filtering.	הארגון יגדיר נוהלי התנהגות בהתייחס למערכות המידע ופיצם לכלל העובדים.	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.	19.6	משאבי אנוש ומודעות עובדים
2	נוהלי שימוש ברשתות חברתיות יכולים לכלול התייחסות לאופן שבו הארגון מצפה מעובדיו לייצג את הארגון במדיה זו, למידע שמותר/אסור לחשוף בעת השימוש במדיה ולכללי זהירות בעת גישה לרשתות חברתיות ממערכות הארגון.	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.	יש להגדיר נהלים והגבלות, המתייחסים לשימוש ברשתות החברתיות.	19.7	משאבי אנוש ומודעות עובדים
3			ארגון יקבע נוהל המסדיר אמצעים סבירים לוודא עמידה של עובדיו בדרישות הבטחון	19.8	משאבי אנוש ומודעות עובדים
1	יישום תהליך עדכון ההרשאות יכול להתבצע באופן ידני, על-ידי העברת הודעה מתאימה לגורם המנהל את ההרשאות במערכות המידע או באופן אוטומטי - במקומות שבהם יש ממשקים ממוכנים לניהול ההרשאות, המשולבים במערכות משאבי האנוש (כגון מערך ניהול זהויות ממוכן). בעת מעבר תפקיד, יש עדיפות להסרה מלאה של ההרשאות הישנות והגדרת ההרשאות הנדרשות לתפקיד החדש, על-מנת שלא תיוותרנה הרשאות עודפות כתוצאה מתפקיד קודם.	יש להגדיר תהליכים של עדכון על ניווד העובד ושל עדכון ההרשאות בהתאם לתפקיד החדש (הסרת ההרשאות המיותרות והקמת ההרשאות הנדרשות לתפקיד החדש).	יש לבחון ולעדכן את הרשאות הגישה של עובד בעת ניווד עובד מתפקיד לתפקיד.	19.9	משאבי אנוש ומודעות עובדים



2	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 שבהם יש 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.	יש להגדיר תהליכים של עדכון על עזיבת צפויה של עובד, ושל טיפול בחסימת הרשאותיו וחשבון המשתמש.	יש לבטל הרשאות גישה ולחסום חשבונות משתמש בעת סיום העסקה.	19.10	משאבי אנוש ומודעות עובדים
---	---	--	---	-------	---------------------------

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 (Fishing), 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.

סיווג העסק	טור ג'	טור ב'	טור א'		
	המלצות	הסבר	בקרה נדרשת		שם הפרק
2	ניתן ליישם באמצעות כתיבת מדיניות הדרכות, הכוללת את הגדרת הסמכויות לביצוע ומעקב אחר קיום ההדרכות והתכנים המועברים. מדיניות זו תגדיר את אוכלוסיות היעד השונות (עובדים חדשים, בעלי תפקידי מפתח, עובדים שהעסקתם הסתיימה), התייחסות לספקים ולגורמים חיצוניים, הגורם המעביר את ההדרכות, אופן הפיקוח והבקרה (החתמה על הצהרה/מבחן וכו'), הישגים נדרשים, תדירות ההדרכות ונושאים חיוניים אשר חייבים להיכלל בהדרכות.	הארגון יגדיר מדיניות הדרכות בנושאי מודעות אבטחת המידע ויפרט בה מה הוא פרק הזמן שבו יש לרענן את ההדרכות, מי יודרך ובאילו תחומים וכיצד יש לבצע מעקב אחר ביצוע ההדרכות.	יש לפתח, לתעד וליישם מדיניות הדרכות מודעות בנושא אבטחת מידע. ולקיים הדרכת ריענון תקופתית אחת לשנה.	20.1	הדרכות
2	ניתן ליישם באמצעות לומדה פנימית ו/או לומדה חיצונית, שתותאם לצורכי הארגון (בהתייחס למדיניות הארגון).	הארגון יקיים הדרכה בסיסית, אשר תתייחס לשימוש נאות במידע, כללי אבטחת מידע בארגון, איומים פנימיים וחיצוניים, הכוללים את הסימנים המזהים לאיומים.	יש לבצע הדרכה בסיסית לעובדים בנושא אבטחת מידע	20.2	הדרכות



3	ניתן ליישם באמצעות לומדה פנימית ו/או לומדה חיצונית, שתותאם לצורכי הארגון ובהתאם להגדרות התפקיד (בהתייחס למדיניות הארגון).	הארגון יקיים הדרכות ראשוניות ותקופתיות, אשר יכללו (בהתאם לתפקיד): בקורות אבטחה סביבתיות ותפעולן במידת הצורך, בקורות אבטחה פיזית ותפעולן, תרגולים מעשיים לגבי התנהלות בעת קרות אירוע אבטחת מידע וסייבר, התנהגויות חשודות של מערכת וזיהוי התנהגות קוד זדוני.	יש לבצע הדרכה ייעודית בנושא אבטחת מידע לבעלי תפקידים ולנושאי משרה בעלי גישה למשאבים רגישים.	20.3	הדרכות
4	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.	יש לוודא כי בעלי התפקיד השונים מכירים את איומי ההתחזות והניסיונות לשיטוי מצד תוקפים פוטנציאליים	הארגון יעלה את המודעות לנושא ההנדסה החברתית בקרב העובדים.	20.4	הדרכות

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. הבקורות נועדו להגדיר את האירועים ולייצר תשתיות תיעוד וניטור אפקטיביות.

שם הפרק	טור א'	טור ב'	טור ג'	סיווג העסק
תיעוד וניטור	בקרה נדרשת	הסבר	המלצות	
21.1	יש לכתוב וליישם מדיניות תיעוד וניטור, לבקר ולעדכן אותה תקופתית.		מדיניות ארגונית בנושא ניטור ובקרה וכן נהלים תומכים, כגון נוהלי מוקד ניטור אבטחת מידע, נוהלי איסוף אירועים ועוד.	2
21.2	יש לקבוע אירועים שהמערכת תתעד (כלומר תרשום לוגים שלהם), 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 ייאספו ממערכות הארגון למערך ניטור אבטחת המידע וכן יגדיר רשימת חוקי ניטור, אשר ישתמשו באירועים אלו. יש להגדיר את פרק הזמן המינימלי לשמירת הנתונים, בייחוד במקרים שבהם יש דרישה רגולטורית, המגדירה את פרק הזמן האמור.	ניתן ליישם באמצעות אפיון וסקירה של אירועים נפוצים לאחר התרחשותם.	2



2	בחינה תקופתית של מנגנוני רישום הלוגים והתאמתם למערכות הארגון. במקרה של מערכת ניטור מרכזית, ניתן להפעיל מנגנונים אוטומטיים, המוודאים את פעילות מערכת רישום האירועים ואת תקינותה.	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 הארגון ולצרכיו.	יש לבחון באופן תקופתי את הגדרת האירועים המתועדים ואת אפקטיביות מערך הרישום.	21.3	תיעוד וניטור
1	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, המחברים למערכות הארגון ואוספים את רשומות האירועים ממערכות אלו למאגר מרכזי.	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 מערכות המעבדות מידע רגיש, כאלה המהוות חלק מהתשתית הקריטית של הארגון או מערכות המנהלות את תהליכי הליבה של הארגון.	יש להפעיל מנגנון המייצר רשומות בקרה על 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').	21.4	תיעוד וניטור
3	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.	יומן הפעילות (לוג) הבסיסי במערכות השונות אינו מכיל בהכרח את כל המידע הנדרש לטובת תחקור אירוע. לצורך קבלת מידע חיוני זה על הארגון להגדיר את הפעולות/מידע הרצויים לשמירה בקובצי הלוג. במערכות רגישות יש צורך בתיעוד מעמיק ומפורט של הפעולות שבוצעו, במטרה ליצור התרעות איכותיות	הארגון יגדיר מידע חיוני נוסף הנדרש לרישום בלוגים המתקבלים מהמערכות הארגוניות, לרבות מזהה ייחודי של הפעולה, פקודות ושאליות שבוצעו.	21.5	תיעוד וניטור
3	לדוגמה, יישום מערכת SIEM, המרכזת את מכלול תהליכי הניטור וההתרעה על אירועי אבטחת סייבר.	יש לאפיין ולהטמיע מערכת ניטור והתרעה מרכזית בארגון, המקבלת אירועים ממערכות הארגון השונות ומרכזת את תהליכי הניתוח, ההתרעה והטיפול באירועים חשודים.	הארגון יישם מערכת מרכזית לניטור והתרעה.	21.6	תיעוד וניטור
1	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.		מנגנוני הרישום יכללו, לכל הפחות, מידע אודות אופי הפעולה שבוצעה, חתימת זמן, מקור ויעד הפעולה, מזהה משתמש, מזהה תהליך, כישלון/הצלחה, שם קובץ מעורב.	21.7	תיעוד וניטור



	בדרך כלל, ניתן להפעיל מנגנוני רישום קיימים במערכות תשתית. במקרה של מערכות אפליקטיביות, יש לוודא כי המערכת מאפשרת רישום פעילויות.				
2	יש לבצע תכנון מקדים של דרישות אחסון הנתונים וכן לבצע תכנון קיבולת תקופתי.	הארגון יוודא כי שטח האחסון המוקצה לרשומות הלוג ולמערך הניטור עונה לצרכיו לאורך זמן, כפי שהוגדר.	יש להקצות שטח אחסון מספק עבור רשומות הבקרה.	21.8	תיעוד וניטור
2	הארגון יוודא כי מערך ניטור אבטחת המידע מנוטר ומתריע כאשר לא מתקבלים אירועים לאורך זמן ממערכת מידע המחוברת למערך הניטור. ניתן להגדיר כחוק והתראה כאשר לא מתקבלים אירועים ממקור מידע במרבית מערכות הניטור ואיסוף הלוגים (SIEM ו-Log Management).		יש לייצר מנגנון של קבלת התראה במקרים של הפסקת כתיבת נתונים ללוגים/ייצור לוגים.	21.9	תיעוד וניטור
2	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, בפלטים ממערכות שונות, במצלמות, בתשואול עובדים ועוד.	מטרת הבקרה הינה לוודא, כי הארגון הגדיר לעצמו את התרחישים שהוא רוצה לנטרם וכי הוא מסוגל לקבל מידע זה.	יש להגדיר פעילויות רגישות שהארגון מעוניין לנטרן.	21.10	תיעוד וניטור
2	ניתן להפיק דו"חות מרוכזים מכל מערכת ניטור אבטחת מידע, כגון SIEM.	הארגון יפיק דו"חות על אירועי אבטחת מידע וטרנדים וידווח על הממצאים להנהלה או לגורם המוגדר לכך.	יש לסקור ולנתח תקופתית את רשומות הבקרה ולדווח את הממצאים לבעלי תפקידים מתאימים שהוגדרו.	21.11	תיעוד וניטור
2	ניתן ליישם באמצעות דו"חות, שאילתות וחוקים המיושמים על מאגר נתוני הניטור, או במערכת ניטור ייעודית כגון SIEM.	על-מנת לאתר אירועים חשודים, יש להפיק התרעות ואינדיקציות מתוך נתוני הניטור הנאספים ממערכות הארגון. יש להתייחס	הארגון יישם מנגנונים אוטומטיים לזיהוי אירועים החשודים כאירועי סייבר, מתוך רשומות הניטור.	21.12	תיעוד וניטור



		לאירועים שהארגון הגדיר כחשודים, בהתאם למתאר האיומים הארגוני.			
3	לדוגמה, שילוב נתונים ממערכות סיסטם ותקשורת, שילוב מידע ממערכות תשתית ומערכות אפליקטיביות, שילוב נתונים ממערכות בקרת גישה פיזית, סריקת פגיעויות והזנות ממקורות מודיעין סייבר.	הארגון יישם "מנוע קורלציה", שמטרתו שילוב נתונים ממקורות מידע שונים (מערכות שונות) באופן שמאפשר זיהוי אירועים רוחביים ותקיפות מתקדמות על מערכות הארגון.	מערכת הניטור תרכז רשומות בקרה ממקורות מידע שונים על-מנת להשיג תמונת מצב ארגונית שלמה.	21.13	תיעוד וניטור
2	ניתן ליישם על-ידי הגבלת גישה למערכת אחסון רשומות הניטור והגבלת הגישה לשרתים עצמם.	הארגון יאבטח את שטח האחסון וכן יקשיח את מערך הניטור כך שלא ניתן יהיה לשנות רשומות לוג לאחר כתיבתן.	יש להגן על רשומות הבקרה מפני גישה לא מורשית, שינוי או מחיקה.	21.14	תיעוד וניטור
3	הארגון יגדיר גיבוי שוטף הן של הגדרות מערך הניטור (גיבוי החוקים) וקונפיגורציות מערכת הניטור) והן של הלוגים שנאספו.		יש לגבות את רשומות הבקרה על בסיס תקופתי ולשמור את הגיבוי בנפרד ממערך הניטור עצמו	21.15	תיעוד וניטור
3	מרבית מערכות ה-SIEM תומכות בפונקציונליות זו - יש לוודא את הפעלתה התקינה.	מערך הניטור יחתום באמצעות מנגנוני חתימות דיגיטליות ו-Hashing את קובצי הלוג שנאספו על-מנת לוודא שלא בוצעו שינויים בקבצים אלו.	יש להשתמש במנגנונים קריפטוגרפיים על-מנת להגן על שלמות הרשומות וכלי הבקרה.	21.16	תיעוד וניטור
4	ניתן להפיק דו"ח על אירועים מהקמת המערכת, לדוגמה, על-מנת לוודא כי אכן אירועים אלו קיימים במערכת הניטור.	הארגון יוודא מדי תקופה, כי ניתן לאחזר ו/או לחפש רשומות מתקופה אחסון ארוכה ככל האפשר.	יש לוודא שניתן לאחזר רשומות בקרה שנשמרו לטווח ארוך.	21.17	תיעוד וניטור
4	ניתן ליישם מנגנון הקלטה באמצעות הפעלת מערכת על תחנות המשתמשים, התקנה על שרתי טרמינל או שרתי אפליקציה.	יש להגדיר את מנגנון ההקלטה וכן את כללי השימוש במנגנון זה, לרבות המקרים שבהם יש להקליט, כללי זהירות בנושא פרטיות משתמשים בהקשר זה והרשאות הגישה למערכת ההקלטה.	יש ליישם מנגנון להקלטה ולמעקב של פעילות המשתמשים (User Session) במערכות המידע.	21.18	תיעוד וניטור
3	ניתן ליישם באמצעות הגדרת חוקים במערך ה-SIEM, אשר יתריעו על אירועי מתקפה ואירועי אבטחת מידע. כמו כן ניתן להפעיל צוות אנליטים (SOC), אשר ינתחו את האירועים.	מנגנוני ההתרעה יזהו ויתריעו על חשד להתקפה	יש ליישם מנגנונים, המזהים ומתריעים בזמן אמת מפני ניסיונות התקפה.	21.19	תיעוד וניטור
3	ניתן ליישם על-ידי ניתוח תעבורת חומת-האש הארגונית וה-IPS ולבצע קורלציה מול Feeds חיצוניים על-מנת לזהות תקשורת לשרתים חשודים.		יש לנטר תעבורת תקשורת יוצאת ונכנסת לזיהוי פעילות לא שגרתית או לא מורשית.	21.20	תיעוד וניטור



3	ניתן להשוות הן מול קבוצה של משתמשים רגישים בתוך ה-Active 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.	הארגון יאפיין פונקציות ארגוניות רגישות ויוודא כי חלים עליהן חוקי ניטור פרטניים בהתייחס לפעולות רגישות במערכות הארגון.	יש להטמיע אמצעי ניטור ספציפיים על פעילות משתמשים, המהווים רמת סיכון גבוהה (למשל, משתמשים בעלי רמת הרשאות גבוהה).	21.21	תיעוד וניטור
---	--	---	--	-------	--------------

22. סקרי הערכת בקורות אבטחה:

סקרי הערכת בקורות האבטחה נועדו לבחון את מימוש הבקורות בפועל על-פי תורת הגנה זו וכן לבחון את אפקטיביות ההגנה. רצוי לבחון את העמידה בבקורות הנדרשות על-ידי גורם עצמאי בארגון או גורם חיצוני. את העמידה באפקטיביות ניתן לבחון על-ידי מבדקי חדירות, בחינת פגיעויות, Red Teams וכד'. הבקורות נדרשות לבחון באופן תקופתי, כי מערכות הגנה הסייבר הקיימות בארגון אכן מוגדרות כראוי ומעודכנות בהתאם לשינויים שחלו בארגון ובאיומי הסייבר האפשריים.

סיווג העסק	טור ג'	טור ב'	טור א'		
	המלצות	הסבר	בקרה נדרשת		שם הפרק
2		הארגון יגדיר מדיניות בנושא ניהול חשיפות בארגון, הכוללת: זיהוי פגיעויות וחשיפות והערכתן, תיקון החשיפות והפגיעויות, אחריות לביצוע המשימות ומעקב שוטף.	מדיניות - יש לכתוב וליישם מדיניות לניהול פגיעויות וחשיפות אבטחת מידע, וכן לבקר ולעדכן אותה תקופתית.	22.1	סקרי הערכת בקורות אבטחה
2	תוכנית הערכת אבטחת מידע וניהול הפגיעויות תכלול מגוון נהלים ותהליכים, אשר נועדו לאפשר את 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 בתוכנית שימוש במערכות לסריקת פגיעויות, ביצוע של מבדקי חדירה המדמים משתמש ארגוני פנימי ו/או תוקף חיצוני, וכן מערכות לסקירת תצורה וכו'.	הארגון יכתוב תיק נהלים ותוכנית ליישום ותפעול של מערך ניהול הפגיעויות, בדגש על הטמעת מערכות לזיהוי, הפעלת כלים וסוקרים, הפעלת ספקי משנה ועובדים לטיפול בממצאים. כמו כן, יש לכלול בתוכנית ניהול הפגיעויות וחשיפות האבטחה אחת או יותר מהבדיקות הבאות: סריקת פגיעויות, בדיקת משתמש זדוני, הערכת איום פנימי ובדיקות ספציפיות אחרות שיוגדרו על-ידי הארגון.	נוהל - יש לכתוב תוכנית לניהול פגיעויות וחשיפות אבטחת מידע, הכוללת את תהליך ההערכה ותיקון הליקויים שנתגלו.	22.2	סקרי הערכת בקורות אבטחה
3	הארגונים הפיננסיים, לדוגמה, מנהלים תוכנית לביצוע מבדקי חדירה על כלל מערכות הארגון ברמה שנתית ואף רב-שנתית, כך שניתן לבצע מעקב שוטף אחר הממצאים ותיקונם.	הארגון יבצע מבדקי חדירה תשתיתיים ואפליקטיביים למערכות הארגון (בין אם הן פנימיות או חיצוניות אבל מנוהלות על-ידו) אחת לתקופה.	יש לבצע מבדקי חדירות למערכות על בסיס תקופתי.	22.3	סקרי הערכת בקורות אבטחה
4	ניתן לפעמים לבצע את המבדקים על-ידי צוות פנימי, אשר אינו כפוף למערכות המידע, אלא לגוף אבטחת המידע, כך שאינו אחראי לתיקון הליקויים עצמם.	הארגון יעסיק בודקי אבטחת מידע חיצוניים (לביצוע מבדקי חדירה).	יש למנות גורם עצמאי/בלתי-תלוי לביצוע מבדקי החדירות.	22.4	סקרי הערכת בקורות אבטחה



4	ניתן לבחון על-ידי בקרה זו את יכולת התגובה של צוותי הניטור, כמו גם את יכולת אנשי התשתיות ואבטחת המידע לחסום מתקפות שזוהו בזמן אמת.	הארגון יעסיק קבוצת בודקי אבטחת מידע חיצוניים, אשר ידמו ניסיונות פגיעה בנכסים על-מנת לבחון הן את הבקורות והן את יכולת התגובה של הארגון.	על הארגון להפעיל קבוצה עצמאית לביצוע מבדקי חדירה ולהפעיל תרגילי Red Team על-מנת לדמות ניסיונות של תוקפים לסכן את הנכס.	22.5	סקרי הערכת בקורות אבטחה
2	ניתן לממש באמצעות התקנה של כלי לסריקת פגיעויות (כגון Nessus, Qualis ועוד) ותזמון סריקות אחת לכמה שבועות, חודש, או כמה חודשים (ניתן גם להגדיר תזמון שונה לכל סביבה).		יש לבצע סריקת פגיעויות באופן שוטף ובהתאם לתהליך ניהול הפגיעויות הארגוני, באמצעות כלי ייעודי למטרה זו על מערכות המידע של הארגון (פנימיות וחיצוניות).	22.6	סקרי הערכת בקורות אבטחה
2	ניתן לוודא לפי תאריכי עדכון של הפגיעויות ולוודא שיש תקשורת לאתר העדכונים של ספק המערכת (או שקיים אתר מראה פנימי לעדכונים).	יש לוודא שכלי הסריקה הוא בעל יכולת עדכון שוטף, בעל רישיון בתוקף (על-מנת לקבל עדכונים לגבי פגיעויות חדשות) וכי אכן מתבצע עדכון של הפגיעויות שהכלי מסוגל לזהות.	יש לוודא כי כלי סריקת הפגיעויות מעודכן באופן שוטף ומכיל את הפגיעויות החדשות המתגלות ומדווחות.	22.7	סקרי הערכת בקורות אבטחה
4	לדוגמה, אם נמצאה פגיעות קריטית במערכת הפעלה של חלונות או בבסיס הנתונים של המערכת, ניתן לבצע סקירה של השרתים הלא מעודכנים אשר מריצים אותה גרסה באמצעות כלי כגון SCOM.	הארגון יגדיר תהליך תיקוף, שמתייחס לכל הפחות לחולשות ולפגיעויות קריטיות וגבוהות שזוהו ומוודא בדיקה באופן ידני או באופן ממוכן הימצאות של החולשות והפגיעויות במערכות נוספות.	על הארגון לתקף את החולשות והפגיעויות שזוהו על-ידי המערכת האוטומטית באמצעות תהליך פנימי, הכולל סקירה של הימצאות החולשות והפגיעויות שזוהו במערכות נוספות.	22.8	סקרי הערכת בקורות אבטחה
4	מרבית כלי סריקת הפגיעויות הקיימים בשוק מכילים מצב סריקה Credentialed Scan.	הארגון יגדיר משתמש מערכת לכלי סריקת הפגיעויות, שיאפשר התחברות למערכת עצמה וסריקה של התהליכים והעדכונים המותקנים עליה. המטרה היא לזהות גם חולשות בהגדרות ההקשחה של המערכת הנבדקת.	יש לבצע סריקות עם משתמש מערכת (Credentialed Scan) בכלי סריקת הפגיעויות.	22.9	סקרי הערכת בקורות אבטחה
4	ניתן לממש הן באמצעות כלי הסריקה עצמם והן על-ידי ממשק למערכות צד ג' (כדוגמת SIEM).	הארגון ינהל מעקב אוטומטי על מצב הפגיעויות שזוהו לאורך תקופה, על-מנת לזהות מערכות המהוות סיכון באופן חריג, או, לחלופין, מערכות שיישום הבקורות בהן אינו מספק.	יש לוודא כי קיים כלי אוטומטי, המשווה בין תוצאות סריקת הפגיעויות בעבר לתוצאות נוכחיות לטובת בקרה וניתוח מגמות.	22.10	סקרי הערכת בקורות אבטחה
4	ניתן לבצע על-ידי הקמת ממשק מכלי ה-Vulnerability Scanning Patch Management לממשק מרכזי, כגון ה-SIEM או מערכת Data Analytics/BI, על-מנת להפיק דו"ח מרכזי ואחיד של מצב הפגיעויות.	יש לוודא כי מגוון כלי סריקת הפגיעויות ו/או כלי הניטור מחוברים למערכת מרכזי על-מנת לקבל תמונת מצב אחידה על מצב הפגיעויות והבקורות.	יש לוודא, כי קיימת התאמה בין התוצאות של כלים שונים לניהול פגיעויות המוטמעים בארגון לצורך קבלת תמונת מצב שלמה על מגוון הפגיעויות במערכת.	22.11	סקרי הערכת בקורות אבטחה



3	ניתן לממש על-ידי הקמת ממשקים בין מערך ניהול החשיפות לבין מערכת הקריאות הארגונית, או, לחלופין, להשתמש במערכת ייעודית לצורך זה (כלי GRC).	הארגון יטמיע מערכת מרכזית לניהול החשיפות שזוהו ומאמצי התיקון.	יש להטמיע מנגנון אוטומטי לניהול מרוכז של תהליך תיקון הליקויים.	22.12	סקרי הערכת בקורות אבטחה
3	לדוגמה, חשיפות קריטיות יתוקנו באופן מיידי, חשיפות ברמה גבוהה בתווך של עד חודש, בינוני עד שלושה חודשים וכו'. בנוסף, יש לממש התראות SLA לקריאות הנפתחות ממערך ניהול הפגיעויות והוצאת דו"חות על חריגות מיעדים אלו.	הארגון יגדיר יעדי SLA לטיפול בחשיפות לפי רמת חומרתן. בנוסף, יש להגדיר התראות לגבי סטייה מלוחות הזמנים של תיקון החשיפות לפי המדדים והיעדים שהוגדרו (SLA).	יש לבקר את תהליך תיקון הפגיעויות ולהחיל יעדים בני מדידה לתיקון הפגיעויות לפי רמת חומרתן.	22.13	סקרי הערכת בקורות אבטחה

23. הגנת סייבר פרואקטיבית:

בקורות סייבר פרואקטיביות מאפשרות לארגון להתגונן מפני תקיפות באופן שמשנתנה עם השתנות התקיפה. במסגרת זו הארגון יאסוף מידע עדכני לגבי איומי הסייבר שלו ודרכי התמודדות מולם ומידע הנוגע לנוכחותו הדיגיטלית ויתרגם אותם לבקורות 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 בקורות המבוססות על ניתוח דפוסי התנהגות (מערכת ומשתמש) בסביבות רגישות.

סיווג העסק	טור ג'	טור ב'	טור א'		
	המלצות	הסבר	בקרה נדרשת		שם הפרק
3		תכנית הגנת סייבר פרואקטיבית תעסוק בזיהוי איומים חדשים, התאמת הבקורות לאיומים שזוהו, אחריות לאיסוף מידע מודיעיני ואחר, סקירת בקורות חדשות ועוד.	הארגון יגדיר תוכנית בנושא הגנת סייבר פרואקטיבית ויעדכן אותה תקופתית	23.1	הגנת סייבר פרואקטיבית
3	ניתן ללמוד ממידע המפורסם במקורות מידע מקצועיים גלויים, כגון metasploit, אתרי חברות אבטחה המפרסמות פגיעויות, חולשות וכו' וכן להתקשר עם חברות מתמחות, המספקות שירותי מודיעין מסוג זה.	הארגון ילמד ממקורות מידע פומביים לגבי איומי סייבר חדשים הנוגעים לעסקי הארגון ולטכנולוגיות המיושמות בו והשפעותיהם עליו.	הארגון יאסוף מידע עדכני לגבי איומי סייבר ודרכי התמודדות מולם.	23.2	הגנת סייבר פרואקטיבית
3	ניתן להשתמש בשירותים של חברות המתמחות בכך.	מטרתו של איסוף המידע היא לזהות מקרים של חשיפת מידע רגיש של הארגון ברשת האינטרנט, לרבות ב"רשת האפלה".	הארגון יאסוף מידע הנוגע לנוכחותו הדיגיטלית (פעילות עסקית, מידע על לקוחות, מידע לגבי משתמשים פנימיים).	23.3	הגנת סייבר פרואקטיבית
3	שינויים יכולים להיות בהגדרת רשתות, חומות-אש, מערכות וממשקים אפליקטיביים ועוד. יש לעדכן את נוהלי המערכות בהתאם לאחר עדכון ההגדרות.	הארגון ימפה את השינויים הנדרשים להגדרות מערכות אבטחת המידע וכן הבקורות התשתיות והאפליקטיביות של הארגון על-מנת להתמודד עם איומים חדשים.	הארגון יפרוט את המידע לגבי איומי הסייבר לבקורות יישומיות, או לטיוב בקורות קיימות.	23.4	הגנת סייבר פרואקטיבית



3	מערכות כגון Honeypots, שרתים וירטואליים ייעודיים מנוטרים, חתימת קבצים (כגון canary) ועוד. ניתן לממש במספר רב של דרכים, כגון הגדרת משתמשים פיקטיביים, אובייקטים בתוך ה-DC, שמטרתם למשוך את התוקף, הטמנת קבצים בעלי שמות ומאפיינים "חמידים", כגון "סיסמאות"/"משכורות"/"ח סוי וכו'.	הארגון יטמיע מערכות טכנולוגיות, שמטרתן לבלבל ולעכב תוקף פוטנציאלי, על-מנת לשפר את יכולות הזיהוי וההתמודדות עם האיומים.	הארגון יישם מערך "שיטוי והטעה" של תוקפים פוטנציאליים.	23.5	הגנת סייבר פרואקטיבית
3	מערכות מסוג זה יכולות להיות הן מערכות ברמת השרת (כגון Advanced Threat analytics) וכן ברמת הרשת (כגון McAfee STRM, NTBA, sourcefire 3d) ועוד.	הארגון יטמיע מערכות לזיהוי אנומליות הן ברמת השרת והן ברמת הרשת בסביבת שירותים ומידע רגיש.	הארגון יטמיע בקרות, המבוססות על ניתוח דפוסי התנהגות (מערכת ומשתמש) בסביבות רגישות.	23.6	הגנת סייבר פרואקטיבית

Respond

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.

סיווג העסק	טור ג'	טור ב'	טור א'		
	המלצות	הסבר	בקרה נדרשת		שם הפרק
2	בכתיבת מדיניות לטיפול באירועים יש להגדיר בעלי תפקידים וצוותי תגובה, רמות חומרה של אירועים וכן דרכי תקשורת עם רשויות במידת הצורך (משטרת ישראל, רמו"ט, הרשות הלאומית להגנת הסייבר, רגולטור ישר וכו'). התוכנית תגדיר מי מנהל את האירוע במידה שהוא מתרחש (ניתן להגדיר, כי במקרים שונים בעלי תפקיד שונים לוקחים את האחריות לניהול האירוע, כגון הבדל בין ניהול אירוע של בקשת כופר לשחרור מחשבים ארגוניים ובין איום לפרסום נתוני לקוחות רגישים החוצה). חשוב כי המדיניות תיכתב בשיתוף עם גורמי צד ג' שרלוונטיים לארגון, כגון רגולטור, ספקים, בדגש על מערכות הפועלות בענן, עובדי מיקור-חוץ וכו'.	הארגון יכתוב ויישם מדיניות תגובה לאירועי אבטחת מידע כחלק ממדיניות אבטחת המידע הארגונית ויבדוק וירענן את התכנית אחת לתקופה.	יש לכתוב וליישם מדיניות תגובה לאירועים, לבקר ולעדכן אותה תקופתית.	24.1	ניהול אירועים ודיווח



	מומלץ כי המדיניות תגדיר מתי פותחים חדר מצב, עבור אילו אירועים נדרש לערב את ההנהלה וכיצד, תדירות דיווח, פנייה ל-CERT הלאומי/רשות הגנת הסייבר, הכרזה על חזרה לשגרת עבודה וכו'.				
2	ניתן ליישום באמצעות מיפוי התהליכים הארגוניים והגופים בארגון שיהיו צוותי תגובה, בהתבססות על יכולותיהם, התממשקות עם הצוותים שמתחזקים את מערכות הניטור הארגוניות על-מנת לוודא שניתן לתרגל ולבדוק אירועים.	הארגון יכתוב תוכנית לזיהוי, לטיפול ולתגובה לאירועי סייבר ואבטחת מידע, הכוללת: מתווה למימוש יכולת תגובה לאירועי אבטחה, הסבר כיצד יכולות הארגון מתאימות לטיפול באירועים, מענה לדרישות הארגון בהתחשב במשימותיו ובגודלו, הגדרת תקריות הנדרשות בדיווח, אספקת אמצעי מדידה ליכולת הארגון להגיב לאירועים, הגדרת המשאבים ותמיכת ההנהלה הנדרשת לתחזוקה ולשיפור יכולת התגובה לאירועי אבטחה.	יש לפתח תוכנית לטיפול באירועי סייבר ואבטחת מידע.	24.2	ניהול אירועים ודיווח
2	ניתן ליישם באמצעות התכנית לטיפול באירועי אבטחת מידע, בדגש על גיוס אנשי מקצוע שיהיו את הבסיס למוקד זיהוי האירועים והתגובה, הכשרת הצוות לטיפול באירועים מסוגים שונים (כגון התפשטות וירוס, כופרה, התמודדות עם DDOS, התמודדות עם מידע שדלף אל מחוץ לארגון וכו'). ניתן לממש באמצעות שימוש בכלי חקירה או באמצעות התקשרות מול צוותי "ניהול אירועים" (ERT).	מטרת הבקרה הינה להביא את הארגון להחזיק בידע והכלים הנדרשים מארגון לטובת תחקור אירוע, הכללתו, ניהולו בצורה יעילה והתמודדות עם השלכותיו.	יש לפתח יכולת לטיפול באירועי סייבר ואבטחת מידע אשר כוללת הכנה, זיהוי וניתוח, בלימה והתאוששות.	24.3	ניהול אירועים ודיווח
3	ניתן לממש באמצעות חיבור מערכות השו"ב למערכות ניטור וזיהוי האירועים. כמו כן, ניתן להגדיר מראש שנוהלי התגובה ישולבו בתוך קריאות השו"ב. ניתן למימוש גם באמצעות מערכות תומכות החלטה, מערכות ניהול Work Follow או מערכת ניהול קריאות (Ticketing). מומלץ כי הכלים יסייעו לארגון לאתר אירועים אשר פתוחים זמן רב, אירועים	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 שאפשר בתהליך ניהול האירועים.	יש להטמיע מנגנונים ממוחשבים לתמיכה בתהליך הטיפול באירועים.	24.4	ניהול אירועים ודיווח



	חמורים אשר הטיפול בהם אינו "מתקדם" ומצבים הדורשים התערבות מיידית.				
2	ניתן לממש בצורה מרוכזת תחת מוקד ניטור אבטחת מידע (SOC), אשר יאסוף, יתעד וירכוז את המידע המתקבל.	הארגון ינהל דיווח מרוכז וכן ניהול אירועים מרוכז לטובת קבלת תמונה אחידה ומלאה לגבי אופי האירוע והערכת הסיכונים.	יש לתעד אירועי אבטחת מידע ואת תהליכי הטיפול באירוע, לרבות איסוף מידע, פעולות שבוצעו ומסקנות.	24.5	ניהול אירועים ודיווח
1	ניתן לממש גם באמצעות הדרכות, אשר יסבירו לעובדים מה הם אירועי אבטחת מידע וכיצד לדווח עליהם. מומלץ לפנות אל ה-CERT הלאומי לטובת קבלת סיוע לצורך תגובה והתאוששות.	הארגון יחיל נהלים המחייבים דיווח ואת אופן הדיווח לגבי אירוע המוגדר כאירוע סייבר.	יש להגדיר ערוצי דיווח עבור העובדים לצורך דיווח על חשד לאירועי אבטחה לגורמים הממונים.	24.6	ניהול אירועים ודיווח
3	הגורם יכול להיות פנימי, או, לחלופין, גורם חיצוני בעל ניסיון בזיהוי, בחקירה ובתגובה לאירועים. הגורם ינחה וייתדרך את הצוותים המתפעלים את האירועים ויהווה מקור ידע מניסיונו בנושאים של אירועי סייבר ואבטחת מידע ותגובה לאירועים מסוג זה.	הארגון יגדיר גורם מקצועי, שתפקידו להוות מקור ידע מקצועי לזיהוי וחקירה של אירועי אבטחת מידע.	יש להגדיר גורם, שתפקידו לספק ידע מקצועי, תמיכה וכן ליווי מקצועי בנושאי ניטור, זיהוי, חקירה ותגובה לאירועי אבטחת מידע.	24.7	ניהול אירועים ודיווח
2	ניתן לממש סעיף זה באמצעות כל מערכת לניהול מידע, או מערכת לניהול מסמכים, או בעותק מודפס.	הארגון ינגיש תיק נהלים, המכיל את נוהלי הזיהוי והתגובה לאירועי סייבר ואבטחת מידע.	יש להטמיע מנגנון, המנגיש מידע לגבי תגובה וטיפול באירועי סייבר ואבטחת מידע.	24.8	ניהול אירועים ודיווח
2	ניתן לבנות את תיק ההדרכות כך שיכילו את נוהלי התגובה, Best Practice וכן את הכללים שהארגון משתמש בהם על-מנת להנגיש את המידע הנ"ל בזמן אירוע אמת.	הארגון יבצע הדרכות בנושא זיהוי ותגובה לאירועי אבטחת מידע לכל הגורמים אשר אמונים על תפעול אירועים אלה. יש לרענן הדרכות אלו אחת לתקופה.	יש לבצע הדרכות לבעלי תפקידים רלוונטיים בנושא תגובה לאירועי אבטחה.	24.9	ניהול אירועים ודיווח
3	חלק מהסימולציות ניתן לבצע בתור "תרגול יבש", אשר ידמה אירוע מונחה, ותגובת הצוותים תימדד על-ידי בקר התרגיל, וחלק מהסימולציות ידמו אירועים בסביבות חיות עם אמצעים אמתיים, כגון שירות תרגול phishing.	הארגון ידמה תרחישים של אירוע אבטחת מידע על-מנת לבחון את מוכנותו ולהיערך בהתאם.	יש לשלב סימולציות לאירועים במסגרת ההדרכות על-מנת לשפר את אפקטיביות התגובה של הצוות במצבי משבר.	24.10	ניהול אירועים ודיווח
4	ניתן לדמות מקרים בסביבות סגורות (סביבת בדיקות) או במעבדות חיצוניות ייעודיות (כדוגמת מעבדת סייבר מקצועית).	הארגון ידמה התנהגות של אירוע אבטחת מידע, בדגש על שימוש בסביבות המדמות את הסביבה הארגונית.	יש ליישם מנגנונים אוטומטיים על-מנת לספק סביבת הדרכות מעמיקה ומציאותית יותר.	24.11	ניהול אירועים ודיווח
3	ניתן למדוד באמצעות הכנת תסריט האירוע ומדידה של כמות האירועים שזוהו וכן מדידת איכות התגובה (מזעור הנזקים לארגון, תקשורת בין גורמים, ריכוז	הארגון ידמה מתקפות אמיתיות, בין היתר באמצעות כלי תקיפה אוטומטיים, לטובת מדידת יכולת התגובה לאירועי אבטחת מידע.	יש לבדוק את יכולת התגובה לאירועים על בסיס תקופתי תוך שימוש במבדקים שיגדיר הארגון, ובכלל זאת באמצעות	24.12	ניהול אירועים ודיווח



	והפעלה, חזרה לשגרה). ניתן לשלב את זיהוי האירועים עם אמצעים, כגון מבדק חדירה אמתי המבוצע על הארגון. חלק מהבדיקה תהיה על-ידי שימוש בכלי תקיפה אמתיים.	הארגון יתעד ויפיק לקחים מתרגילים המבוצעים לצורך זיהוי ובקרה, ויפיק דו"ח תחקיר אירוע בסיום התרגיל.	סימולציה של אירוע אמת, על-מנת לקבוע אפקטיביות. יש לתעד את תוצאות הבדיקה התקופתית.		
Recover					
חזרה לשגרה: מטרתו של העסק לחזור לשגרה בהתרחש אירוע סייבר משמעותי אשר מביא לידי אירוע חומ"ס. על העסק לוודא יכולת שחזור מהיר של תשתיות המחשוב שנפגעו באירוע סייבר לרמה נאותה. על העסק להיערך מבחינת תשתיות חלופיות באם נדרשות (כולל זמינות ויתירות), לבדוק את תוכנית החזרה לשגרה באופן עתי ואף לתרגל אותה. הנושא של יתירות המערכות העוסקות בחומרים מסוכנים קריטי לתהליך החזרה לשגרה חשוב ונדרש לתרגל אותו באופן שוטף.					
2	העסק יכתוב ויישם מדיניות חזרה לשגרה. יש לעדכן מדיניות זו באופן תקופתי. מדיניות זו תגדיר כיצד העסק מתנהל בשוטף ובחירום במטרה להבטיח את החזרה לשגרה.	העסק יכתוב ויישם תוכנית חזרה לשגרה, הנגזרת מיעדי העסק.	העסק יכתוב ויישם מדיניות חזרה לשגרה בהיבטי הגנת סייבר. התוכנית תתחשב בתרחישי האסון השונים ובתהליכים הקריטיים למימוש יעדי העסק. העסק יגדיר אילו נכסים תומכים בפעילות של משימות ופונקציות עסקיות קריטיות (פיזיים ודיגיטליים). העסק יגדיר את פרק הזמן המקסימלי הנסבל להשבתה של שירותים חיוניים בטרם יתממש תרחיש לאירוע חומרים מסוכנים עקב פגיעה במערכת מחשוב. העסק יגדיר במסגרת תוכנית החזרה לשגרה את פרק הזמן שבו תהליכים חיוניים יחזרו לפעילות מרגע הפעלת התוכנית.	25.1	חזרה לשגרה
2	ניתן ליישם לאחר מיפוי השירותים והתהליכים הקריטיים וכן לאחר הגדרת יעדי ההתאוששות והשרידות לכל שירות. העסק בדרך כלל מבצע מדידה של הקיבולת הנדרשת באתר החלופי מבחינת רכיבי HMI, בקרים, יחידות קצה וצנרת.	העסק יוודא, כי המערכות והתשתיות המיועדות לחזרה לשגרה במצבי אסון תומכות בקיבולת הנחוצה להיקפים ולפרקי הזמן הנדרשים.	העסק יבצע תכנון קיבולת הנחוצה לפעילות למקרה אסון (לדוגמה, מערכות HMI מערכות בקרה ממוחשבות, ורכיבי קצה הניתנים לתכנות).	25.2	חזרה לשגרה
2	בתוך כך, יש להתייחס לתפקידים של העובדים במערך ההתאוששות, מקומות התכנסות זמניים, לוגיסטיקה והפעלה וכן יעדי ההתאוששות עצמם ברמת כל צוות וברמת	העסק יבצע הדרכות לעובדים בהתייחס לנוהלי החזרה לשגרה.	בעל העסק יבצע פעם בשנה לפחות הדרכה לעובדים בנושא חזרה לשגרה.	25.3	חזרה לשגרה



	העסק.				
2	ניתן ליישם באמצעות "תרגיל יבש", המכיל כמה תרחישים, ובכך לבדוק את מוכנות העובדים. מומלץ כי התרגול יכלול הן את היבטי ה-OT של תוכנית החזרה לשגרה של מערכות ה-ICS, כגון החלפת רכיבים שנפגעו והן צדדים משלימים, כגון עמידת ספקים חיצוניים ושירותים (בענן ומקומיים) בהנחיות תוכנית החזרה לשגרה. כמו כן, חשוב לוודא, כי העסק מבצע מהלכים של העלאת מודעות בחירום, כגון בחינת הנחיות והדחיפות בהעברת גרסאות לסביבת הייצור, הקפדה על ליווי אורחים, ניסיונות לשחזור קבצים, תרגול ניהול אירוע סייבר וקבלת החלטות של ההנהלה, כולל תחקור והפקת לקחים ועוד.	העסק יתכן ויבצע תרגילי מוכנות לשם בדיקה של אפקטיביות תוכנית החזרה לשגרה.	בעל העסק יבצע פעם בשנתיים לפחות תרגול של תוכנית החזרה לשגרה.	25.4	חזרה לשגרה
3	על-מנת לבצע סימולציה הקרובה למציאות ככל האפשר ("תרגיל רטוב"), יש להכין תסריטים של תרחישי אסון, להפעיל את התוכנית (במתכונת מצומצמת) בסביבת האמת (סביבת DR) ולבחון את תפקוד התוכנית.	העסק ישתמש בסימולציות והפעלת העובדים המעורבים ביישום התוכנית לבדיקת מערך ההתאוששות.	יש לבצע תרגול של תוכנית החזרה לשגרה באמצעות סימולציה של הפעלת התוכנית.	25.5	חזרה לשגרה
2	לדוגמה: תוכנית בדיקות, המבצעת הפעלה חלקית של מעבר לסביבת החירום באופן תקופתי או למערכות שונות, במטרה לוודא את תקינות תהליכי המעבר.	העסק יבקר ויתקן את תוכנית החזרה לשגרה באופן תקופתי.	בעל העסק יבדוק את תוכנית החזרה לשגרה ולתקן פערים שהתגלו.	25.6	חזרה לשגרה
3	ניתן לבצע על-ידי גיבוי תצורה בנקודת זמן (כגון טרם ביצוע שינויים) וכן על-ידי קביעת נקודת שחזור נתונים ומנגנון גלגול לאחור (Rollback).	יש לוודא מנגנונים, המאפשרים שחזור נתונים או תצורת מערכת למצב ידוע, כגון תצורה שהוקפאה במועד מסוים או מצב נתונים ממועד מסוים.	על העסק לוודא יכולת לשחזור רכיבי מערכת למצב מבצעי ידוע.	25.7	חזרה לשגרה
2	ניתן ליישם ע"י החזקת מלאי מינימלי או ביצוע הסכם חוזי עם ספק.	העסק יחזיק רכיבים קריטיים (ברזים, וסתים צנרת וכדומה) או שיחתום על הסכם אספקה מיידי של רכיבים אלה במקרה ונפגעו	העסק יוודא קיום רכיבים חליפיים למקרה שרכיבים נפגעו בהתקפת סייבר	25.8	חזרה לשגרה



2	ניתן לשמור את הקוד ופרטי הקונפיגורציה ברשת התפעולית של העסק, או בקבצי גיבוי.	העסק ישמור עותקים של הקונפיגורציה / התכנה הקיימים ברכיבים על מנת שיוכל לקנפג רכיבים חדשים במקרה ונפגעו המקוריים.	העסק יוודא שמירת הקונפיגורציה / קוד התכנה הקיימים ברכיבים התעשייתיים.	25.9	חזרה לשגרה
---	--	--	---	------	------------



ו. נספח ו'- תחזוקה מרחוק – חיווי ובקרה

המלצה לתיעוד הפעולות הבאות:

1. ניסיונות גישה לניהול.
2. שינוי/מחיקה של קבצי מערכת.
3. שינוי תצורה לרבות שינויים בהגדרות רכיבי אבטחה.
4. גישה/שינוי או ניסיונות שינוי בהגדרות החיווי.
5. גישה לקובץ סיסמאות.
6. תעבורה שנחסמה.
7. פעולות המבוצעות באמצעות חשבון בעל הרשאות ניהול.
8. פעולות ניהול בטווחי זמן שמחוץ לשעות הפעילות המוגדרות.
9. חיווי לגישה מקומית או מרוחקת.