תוכן העניינים

1. הקדמה

1.1 ביום 15.02.2015 התקבלה החלטת ממשלה מספר 2443 (להלן: החלטת הממשלה), שכותרתה "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר". החלטה זו התקבלה בהמשך להחלטת ממשלה מספר 3611 מיום 07.08.2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי".

1.2 באותו מועד (15.02.2015), התקבלה החלטת ממשלה נוספת שמספרה 2444, בעניין "קידום ההיערכות הלאומית להגנת הסייבר", ולפיה תגובש מדיניות כוללת בתחום הגנת הסייבר ותוקם רשות לאומית להגנת הסייבר במסגרת מערך הסייבר הלאומי במשרד ראש הממשלה.

1.3 החלטות אלו נועדו לקדם אסדרה לאומית בנושא הגנת הסייבר, להעלאת החוסן הלאומי במרחב הסייבר במדינת ישראל.

1.4 בעקבות החלטת הממשלה, הכוונה והנחיה מקצועית בתחום הגנת הסייבר במשק הישראלי ישתלבו במערך הרגולציה הממשלתי. משמעותה של קביעה זו היא כי הגנה מפני מתקפות סייבר, העלולות לפגוע בסביבה או בבריאות הציבור ובחיי אדם, תתבצע באמצעות כלי הרגולציה העומדים לרשות הרגולטור.

1.5 כדי לקבוע הוראות בתחום ההגנה מפני מתקפות סייבר, הוקמה באגף חירום וסייבר של המשרד להגנת הסביבה יחידת סייבר בתעשייה. היחידה פועלת בהנחיה מקצועית של מערך הסייבר הלאומי.

1.6 יחידת הסייבר בתעשייה עוסקת בהנחיה, בפיקוח ובאכיפה של הגנת הסייבר בעסקים המחזיקים חומרים מסוכנים ובעסקים המקבלים היתר רישוי עסקים מהמשרד להגנת הסביבה. תפקיד היחידה הוא להגדיר את המדיניות המגזרית ואת דרישות האסדרה, ולהעניק ליווי מקצועי שוטף ומענה לפניות מקצועיות, בהתאם למאפייני העסקים המפוקחים על ידה.

1.7 היחידה עוסקת גם בהגנת סייבר בתחומים נוספים, אשר עלולים לגרום למפגע סביבתי רב היקף שלא באמצעות היתר הרעלים.

1.8 מסמך זה הוא מדריך עזר להגנה על לולים מבוקרים ואינו מהווה מסמך רגולטורי או מסמך מחייב. הוא נועד לסייע לבעלי לולים מבוקרים להגביר את רמת החוסן בסייבר בלול המבוקר.

1.9 המדריך נכתב לאחר סיורי שטח בכמה לולים מבוקרים, בתיאום עם אגף סביבה חקלאית של המשרד להגנת הסביבה ובתיאום עם האגף לניהול משברים במשרד החקלאות, ובעקבות פגישות עבודה עם חברות הבקרה המספקות את הבקרים ללולים, ובכללן סיור במעבדת הפיתוח של אחת מהן. בנוסף בוצע פיילוט סקר סיכונים ברוח מדריך זה וכן התקיימה הדרכת מודעות אבטחת מידע והגנת סייבר בלולים מבוקרים לעשרות לולנים.

לשאלות בנושא מדריך זה אפשר לפנות בדואר אלקטרוני לכתובת:

cyber_industry@sviva.gov.il

גלעד בן ארי,

ראש אגף חירום וסייבר
המשרד להגנת הסביבה

יוסי שביט,

ראש יחידת הסייבר בתעשייה
המשרד להגנת הסביבה

2. הגדרות

מונח	הסבר
אבטחה פיזית	האמצעים הפיזיים הנדרשים להגנה על ציוד המחשוב, לגישה למידע של העסק ולשרידות המערכות הממוחשבות המכילות את מאגרי המידע והרכיבים הממוחשבים התעשייתיים.
איום	מפגע פוטנציאלי אשר עלול לפגוע במערכות ממוחשבות של עסק במכוון או באקראי.
איום פנימי	איום מצד גורם פנימי "מתוך הארגון" שפעילותו עלולה לגרום לאירוע בלול המבוקר בשגגה או בזדון.
אירוע סייבר	התרחשות אשר מעידה על פגיעה אפשרית במערכת מחשוב עקב פגיעה מכוונת או פגיעה בשוגג, ושיכולה לגרום לאירוע חמור.
בעל הלול המבוקר	הבעלים בפועל / הנהלת העסק / אחראי על הלול מטעם הבעלים.
בקר	מחשב שאחראי על תהליך ייצור או תהליך אחר כחלק ממערכת בקרה תעשייתית.
בקרות	אמצעים שעל העסק ליישם על מנת להגן על עצמו מפני אירוע סייבר.
בקרה מפצה	בקרה שנועדה לפצות על העדר היכולת לממש את הבקרה המומלצת, ונותנת מענה הולם לסוגיית הפער בהגנת הסייבר.
דיודה חד כיוונית	Unidirectional Security Gateway. רכיב המאפשר מעבר פיזי של מידע רק בכיוון אחד.
הזדהות	תהליך המספק זיהוי מאומת של אדם או מחשב, באמצעות מידע ייחודי חד ערכי לאדם או למחשב, רכיב הזדהות פיזי או תכונה שלו.
הזדהות חכמה / הזדהות חזקה (MFA , 2FA)	שיטת הזדהות המבוססת על שילוב של לפחות שניים ממאפייני האימות שלהלן: משהו שהמשתמש יודע, כגון: סיסמה. משהו שיש למשתמש, כגון: רכיב פיזי כמו טוקן או מחולל סיסמאות חד פעמי או כרטיס חכם. מאפיין ביולוגי של המשתמש, כגון: טביעת אצבע, טביעת רשתית עין.
התרחיש החמור ביותר (WCS)	התרחיש שבו מתרחשת התוצאה בעלת פוטנציאל הנזק הגדול ביותר בלול.
מתקפת פישינג (מתקפת "דיוג")	ניסיון להחדרת קוד זדוני לעמדת מחשב של המשתמש ע"י פתיחת מייל זדוני והורדת קובץ זדוני, או לחיצה על קישור זדוני המוביל להורדת קוד זדוני.
לול מבוקר	לול שיש בו מדדים כגון: קביעת טמפרטורה, תאורה, אוורור, פינוי פסולת והזנת העופות, המבוצעים ע"י מערכות ממוחשבות.
מידע	נתון הנוגע ו/או קשור לפעילותן, תפעולן או תפקודן של מערכות מחשוב בעסקים ונמצא על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, מצעי מידע פיזיים וכן מידע המועבר בעל-פה.

מונח	הסבר
ממונה הגנת סייבר	גורם בעסק אשר יהיה מופקד על יישום ההנחיות במסמך זה למזעור סיכוני סייבר בעסק.
מערכות מחשוב בקרה תעשייתיות, מערכות ממוחשבות ICS - (Industrial Control System)	מונח כללי הכולל כמה סוגים של מערכות בקרה המשמשות בייצור תעשייתי. המערכות יכולות להיות מורכבות מהרכיבים האלה: יחידות חיישנים ויחידות שליטה מקומית: IED (sensors, actuators and electronic devices) יחידות בקרים מתוכנתים: RTU (Remote Terminal Unit) PLC (Programmable Logic Controllers) תקשורת בין האתרים למרכז הבקרה: WAN (Wide Area Network Communication) מרכז בקרה של כל התהליך: SCADA (Supervisory Control and Data Acquisition) מערכות בקרה מבוזרות: DCS (Distributed Control Systems) מחשבים לממשק אדם-מכונה: HMI (Human Machine Interface)
משאבים	בסיסי נתונים, קבצים, מערכות, תוכניות או אמצעים אחרים אשר כניסה אליהם מאפשרת גישה למידע ולמערכות ממוחשבות שברשות העסק.
מתקפת סייבר	פעולה התקפית של חדירה למרחב הקיברנטי של היעד, המסכנת תהליך הכולל מערכות, תשתיות ושירותים שנתמכים על ידם.
סודיות המידע (Confidentiality)	מידע שבעליו קבע שאין לחשוף אותו לגורמים שלא מאושרים לכך.
סיווג	מדד המגדיר את רמת רגישות המידע והמערכות התומכות.
סייבר, מרחב סייבר, המרחב הקיברנטי או ה-Cyber Space	מרחב מטפורי של מערכות מחשב ורשתות מחשב שנאגרים בהן נתונים אלקטרוניים ומתנהלת תקשורת מקוונת ואינטראקטיבית, ללא תלות במיקום הגיאוגרפי של המשתמשים.

מונח	הסבר
סנסור (חיישן)	רכיב במערכת בקרה תעשייתית אשר נותן חיווי אל הבקר על מצב מערכת הבקרה.
ענן (Cloud)	רשת בתוך עולם המרשתת שמחוץ לרשת הארגון.
קוד זדוני (Malware)	פיסת קוד שמטרתה לגרום נזק למשאב המחשוב שאליה הוחדרה.
רשת מתח נמוך	רשת תקשורת מבוססת TCP/IP ייעודית, שנועדה להגן ולפקח על ביטחון המתקן. המערכת יכולה להיות מורכבת מהרכיבים האלה: מצלמות אבטחה IP ומצלמות תרמיות (קבועות/PTZ/LPR) מערכות VMS ואנליטיקה מערכות גילוי פריצה מערכות בקרת כניסה מערכת גדר חכמה מערכות רדאר מערכות שו"ב IIOT (Industrial IOT)
תהליך מסוכן טכנולוגית	רכיב, תוכנה או חומרה המאגדים בתוכם מידע ו/או שירות בעבור העסק שעלול להיות נתון למתקפת סייבר.
Application List	רשימת תוכנות מורשות.
DAF	Database Firewall L – חומת אש לבסיסי נתונים.
Device Control	ניהול התקנים – בד"כ מדובר בסגירת התקנים לא נדרשים או התקנים המהווים פרצת אבטחה.
HMI	Human-Machine Interface – מחשב + תוכנה ייעודית המנהלים את התהליך המבוקר.
MITM	מתקפת Man in The Middle – "האיש באמצע".
ON PREMISE	תוכנה מקומית המותקנת ופועלת במחשבים באתר של המחזיק ולא באתר מרוחק כמו חוות שרתים או ענן.
RO	Read Only – מצב קריאה בלבד.
RW	Read / Write – מצב קריאה וכתיבה.
WAF	Web Application Firewall – חומת אש אפליקטיבית.

3. מטרת המסמך

להדריך עסקים המחזיקים בלולים מבוקרים ולסייע להם להגביר את החוסן בסייבר בלול מבוקר.

המדריך נותן כלים להפחתת ההסתברות לפגיעה בבריאות הציבור ובסביבה, בעקבות אירוע סייבר או פגיעה מסוג אחר בתהליכים טכנולוגיים או במערכות ממוחשבות המנהלות/מבקרות לולים מבוקרים. אירוע סייבר עלול לגרום לתמותה המונית של עופות בלול ולהיות מפגע תברואתי רחב היקף, לפגוע בהמשכיות העסקית של העסק ובהמשכיות התפקודית של המדינה.

מסמך זה קובע הנחיות הנוגעות לביצוע פעילות הגנה בסייבר ללולים מבוקרים, ונבנה על בסיס ידע מקצועי של יחידת הסייבר בתעשייה, של המשרד להגנת הסביבה, בתחומי מערכות בקרה תעשייתיות (ICS), ביקור בלולים מבוקרים, ופגישות עם חברות הבקרה העוסקות בפיתוח התקנה והטמעה של בקרים מתוכנתים בלולים מבוקרים.

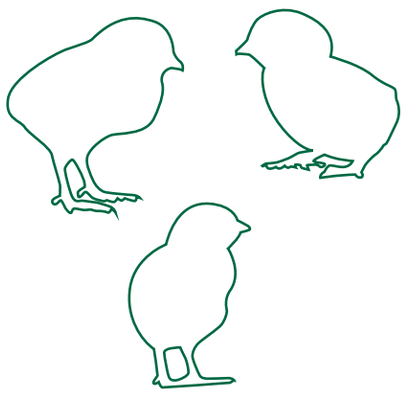
4. רקע – הגנת סייבר בתחום מערכות מבוקרות תעשייתיות

4.1 כשל במערכות ממוחשבות המבקרות/מנהלות לולים ממוחשבים בעקבות אירוע סייבר, עלול לגרום לפגיעה חמורה בלול ואף למוות של חלק ניכר מהלול או של כל הלול, ובעקבותיו לפגיעה בבריאות הציבור ובסביבה.

4.2 להלן דוגמאות לאירועים שעלולים להתרחש בלול עקב אירוע סייבר:

- הפסקת פעילות אוורור בתוך הלול המבוקר.
- שיבוש / שינוי ערכי חימום / קירור בלול המבוקר.
- שיבוש / פגיעה בתהליך ההזנה והשתייה בלול המבוקר.
- שיבוש / פגיעה בפינוי פסולת מהלול המבוקר.
- שיבוש מערכת ההתראה המתריעה על אחד מהאירועים שלעיל.

4.3 שיתוף מידע בין בעלי לולים מבוקרים ודיווח על אירועים ליחידת הסייבר בתעשייה במשרד להגנת הסביבה, ובכלל זה ל-CERT הלאומי, יסייעו לגילוי מוקדם של התרחשות פוטנציאלית של אירוע סייבר. בכל אחד מהשלבים המוקדמים יוכל בעל הלול המבוקר לזהות את פוטנציאל התקיפה ולמזער את הסיכון לגרימת נזק פוטנציאלי.



5. משטח חשיפת הלול המבוקר לאיומי סייבר

5.1 האיום החיצוני – גישה מרשת האינטרנט אל רשת הלול על מנת לבצע פעילות זדונית בדרכים האלה:

5.1.1 החדרת מייל פישינג המכיל קוד זדוני לרשת ה-IT, שימצא את דרכו לרשת המכילה את בקרי הלול ומשם ישבש את פעולת הבקר/ים.

5.1.2 הורדת קובץ נגוע ממחשב כלשהוא ברשת ה-IT של הלול. הקובץ הנגוע ימצא את דרכו לרשת המכילה את בקרי הלול ומשם ישבש את פעולת הבקר/ים.

5.1.3 גלישה מאחד ממחשבי הלול לאתר זדוני אשר נפל קורבן לפריצה וע"י כך קבלת קוד זדוני אל התחנה הגולשת. הקוד יגיע לרשת המכילה את בקרי הלול ומשם ישבש את פעולת הבקר/ים.

5.2 האיום הפנימי – גישה מרשת הלול

5.2.1 עובד בלול אשר יש לו גישה למערכות המחשוב של הלול, עשוי לטעות בתום לב עקב חוסר מודעות ולגשר בין רשת הלול לרשת האינטרנט. לדוגמה: חיבור מכשיר סלולרי לעמדת HMI וגלישה ממנה.

5.2.2 עובד בלול מבצע פעילות זדונית מכוונת עקב מרמור / אי שביעות רצון / הודעת פיטורין וכיוצא באלה. לדוגמה: שתילת קוד זדוני באמצעות התקן חיצוני, גישור בין רשת ה-IT לרשת הבקרים וכדומה.

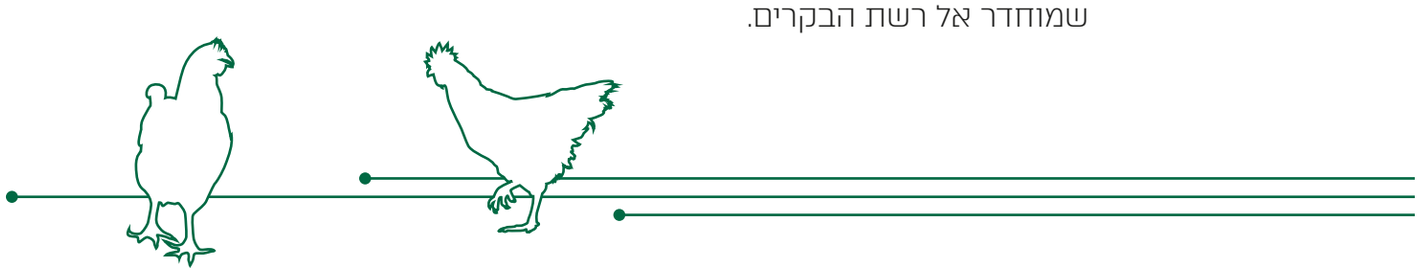
5.3 שרשרת האספקה – תמיכה במערכות הלול

5.3.1 טכנאי / תומך מאתר מרוחק אשר במסגרת תפקידו מבצע פעילות מחשובית ברשת הלול, מבצע גישה לא מאובטחת אל תוך רשת הלול אשר עלולה להיות מנוצלת ע"י תוקף פוטנציאלי.

5.3.2 טכנאי / תומך מאתר מרוחק אשר במסגרת תפקידו מבצע פעילות מחשובית ברשת הלול, מבצע גישה אל תוך רשת הלול באמצעות מחשב אשר מכיל קוד זדוני. הקוד ימצא את דרכו לרשת המכילה את בקרי הלול וישבש את פעולת הבקר/ים.

5.3.3 טכנאי / תומך בתוך האתר של הלול מבצע גישה לא מאובטחת במחשב שמכיל קוד זדוני שמוחדר אל רשת הבקרים.

5.3.4 טכנאי / תומך בתוך האתר מכניס DOK שלא הולבן לצורך פעילותו וכך מכניס קוד זדוני שמוחדר אל רשת הבקרים.



5.3.5 טכנאי / תומך בתוך האתר אשר מבצע פעילות בארון התקשורת וזו גורמת לגישור בין רשת ה-IT המחוברת לאינטרנט לרשת הבקרים.

5.3.6 טכנאי / תומך בתוך האתר או מאתר מרוחק אשר שינה הגדרות כלשהן במערכות המחשוב או במערכות אבטחת המידע (כגון חומת האש) והן גרמו לפריצה לרשת הבקרים של הלול.

5.4 ספק מערכת הבקרה הממוחשבת - על בעל הלול לדרוש מספק מערכת הבקרה הממוחשבת של הבקרים, כי ניהול המערכת המרכזית (אם הלול המבוקר של בעל הלול נמצא במערכת זו) תהיה מאובטחת לפחות על פי הסטנדרטים האלה:

5.4.1 הזדהות חכמה למערכות שהספק מנהל לפחות ב-2 פקטורים (2FA).

5.4.2 הגנה על הפורטל המרכזי של ספק / תומך מערכת הבקרה הממוחשבת באמצעות WAF (Web Application Firewall) או כל אמצעי אחר המהווה בקרה מפצה.

5.4.3 הגנה על בסיס הנתונים המרכזי של ספק / תומך מערכת הבקרה הממוחשבת באמצעות DAF (Database Firewall) או כל אמצעי אחר המהווה בקרה מפצה.

5.4.4 ביטול / אבטחת פורטים פתוחים אל המערכת המרכזית המנהלת את הבקרים הממוחשבים בלולים השונים (כגון: FTP, RDP, SSH וכדומה).

5.4.5 אי שימוש בתוכנות השתלטות המבוססות WEB (כגון TeamViewer, Anydesk ודומיהן), המאפשרות לתוקף פוטנציאלי לנצל את התווך האינטרנטי בהתקפת MITM (Man in The Middle) לתקיפת הלול המבוקר.

5.4.6 הספק יבצע בדיקת חדירות (Pen Test) על מערכותיו אחת לחצי שנה, כדי לוודא שאי אפשר לגשת אל בקרי הלול המבוקר ולבצע בהם פעילות זדונית, ויתקן את הליקויים שיימצאו בעקבותיה מהר ככל האפשר.

5.4.7 אבטחה לפי הסטנדרטים הנ"ל תתבצע גם אם מערכות הניהול בתצורת On Premise (באתר הלקוח) וגם אם הן בענן (אם הן בענן, יש לדרוש מספק הענן את האבטחות הנ"ל).

6. שלבי התהליך להעלאת החוסן בלולים מבוקרים

6.1 מיפוי

6.1.1 מיפוי המערכות הממוחשבות המחוברות ישירות ללול הממוחשב - כל מחשב, שרת, עמדת HMI, בקר, סנסור או כל רכיב אחר המעורב בתהליך המבוקר שמחובר ללול המבוקר, ימופה ויירשם בטבלת המיפוי כפי שמופיעה בנספח א' למדריך זה. המיפוי יעודכן אם יש תוספת / גריעה של ציוד.

6.1.2 מיפוי המערכות הממוחשבות שאין להם חיבור ישיר ללול הממוחשב - כל מחשב, שרת, רכיב אבטחת מידע או רכיב ממוחשב כלשהו ברשת הלול שאינו מחובר ישירות לרשת הבקר בלול המבוקר, ימופה ויירשם בטבלת "מערכות ממוחשבות תומכות" המופיעה בנספח ב' למדריך זה. המיפוי יעודכן אם יש תוספת / גריעה של ציוד.

6.2 הגנות סייבר בשכבות השונות

6.2.1 הגנה ברכיבי המערכות הממוחשבות המחוברות ישירות ללול הממוחשב.

6.2.2 הגנה על מחשבי ממשקי אדם-מכונה (Human Machine Interface) HMI למערכת הבקרה.

6.2.2.0.1 יש לוודא שיש עדכוני אבטחת מידע במערכת ההפעלה המכילה בתוכה את תוכנת ה-HMI. לפני כל עדכון יש לוודא תאימות של העדכון מול יצרן ה-HMI.

6.2.2.0.2 יש לבדוק הימצאות תוכנת אנטי-וירוס עדכנית, ולבצע עדכונים שוטפים לתוכנה זו. במידת האפשר יש להוסיף לתוכנת האנטי-וירוס מודולים נוספים להגנה, כגון רכיב Sand Box , רכיבי Device Control, רכיבי Application List ויכולות נוספות.

6.2.2.0.3 בדיקת העדר תוכנות שליטה מרחוק המבוססות WEB על עמדת HMI (כגון: "TeamViewer", וכל תוכנת השתלטות המבוססת גישה דרך רשת האינטרנט כגון: "LogMeIn").

6.2.2.0.4 בדיקת עדכוני תוכנה שוטפים לתוכנת ה-HMI המותקנת על העמדה, בתיאום עם ספק תוכנת ה-HMI.

6.2.2.0.5 בדיקת ביצוע Log Off של מערכת ההפעלה של עמדת ה-HMI לאחר פרק זמן של 5 דקות ללא עבודה.

6.2.2.0.6 הקמת מערכת הרשאות לאנשים המשתמשים במערכת ה-HMI: הרשאות לצפייה בלבד (RO) והרשאות חזקות יותר לקריאה / כתיבה (RW) לאנשים מורשים. הרשאות RW יינתנו במשורה רק למי שבאמת נדרש להרשאות כאלה בעבודתו.

6.2.2.0.7 יש לוודא כי שינוי של ערכים קריטיים ע"י משתמש בעל הרשאות RW, ידרוש הזנת סיסמה לאישור השינוי.

6.2.2.1 הגנה על הבקרים

6.2.2.1.1 יש לוודא הימצאות תוכנה עדכנית לבקרים – מול ספק הבקר. אם נדרש עדכון, יש לוודא את בדיקת העדכון בסביבת ניסוי או אצל הספק טרם הטמעתו בסביבה המבוקרת.

6.2.2.1.2 יש לוודא הימצאות עדכוני חומרה מול ספק הבקר. יש לוודא בדיקת העדכון בסביבת ניסוי או אצל הספק טרם ביצוע בסביבה המבוקרת.

6.2.2.1.3 אם הבקר מגיע ללא משתמש וסיסמה, יש ליצור שם משתמש וסיסמה ייחודיים אל הבקר לגישת מורשים בלבד.

6.2.2.1.4 אם הבקר מגיע עם משתמש וסיסמה כברירת מחדל של היצרן, יש לשנותם וליצור משתמש וסיסמה ייחודיים לגישת מורשים בלבד.

6.2.2.1.5 יש לוודא שבקוד שנכתב והותקן בבקר הוגדרו ערכי קיצון לפרמטרים קריטיים שלא יהיה ניתן לחרוג מהסף שלהם בשום מצב, גם אם נעשה ניסיון שינוי בעמדת ה-HMI (לדוגמה: מידת הטמפרטורה בלול).

6.2.2.1.6 יש לגבות את קונפיגורציית הבקר בכל יום, ואחת לחודש לבדוק אפשרות של שחזור הקונפיגורציה.

6.2.2.2 הגנה על רשת הלול

6.2.2.2.1 יש לוודא שרשת הלול מבודדת מרשתות אחרות באמצעות הפרדה לוגית (חומת אש) או פיזית (הפרדת כבילה, או יישום דיודה חד כיוונית - Unidirectional Security Gateway).

6.2.2.2.2 יש לוודא איסוף לוגים הקשורים לרשת הבקרים של הלול המבוקר.

6.2.2.2.3 יש לשים לב ללוגים המכילים מידע על תקשורת מרשת ה-IT אל רשת הבקרים של הלול המבוקר.

6.2.2.2.4 מומלץ ליישם כלי איסוף, ניתוח והצגה של הלוגים החשובים המתקבלים ומקשרים בין גורמים חיצוניים (רשת ה-IT, רשת האינטרנט) לרשת הבקרה של הלול המבוקר.

6.2.2.3 הגנה פיזית / בקרת גישה

6.2.2.3.1 יש לוודא כי הגישה הפיזית לבקרים מוגבלת למורשים בלבד. אם נדרש גורם חיצוני לטיפול בבקרים, יש ללוות אותו ליווי צמוד בכל מהלך הפעילות שלו מול הבקרים.

6.2.2.3.2 יש לוודא כי הגישה לארון התקשורת של רשת הבקרים מוגבלת למורשים בלבד. אם נדרש גורם חיצוני לטיפול בבקרים, יש ללוות אותו ליווי צמוד בכל מהלך הפעילות שלו מול הבקרים.

6.2.2.4 האיום הפנימי

6.2.2.4.1 יש לוודא כי העובדים המטפלים במערכות המחשוב מודעים לסיכונים המוצגים במדריך זה.

6.2.2.4.2 יש להעביר הדרכת מודעות עובדים לפחות אחת לחודש. אפשר להיעזר בלומדות מוכנות המפורסמות באתר מערך הסייבר הלאומי.

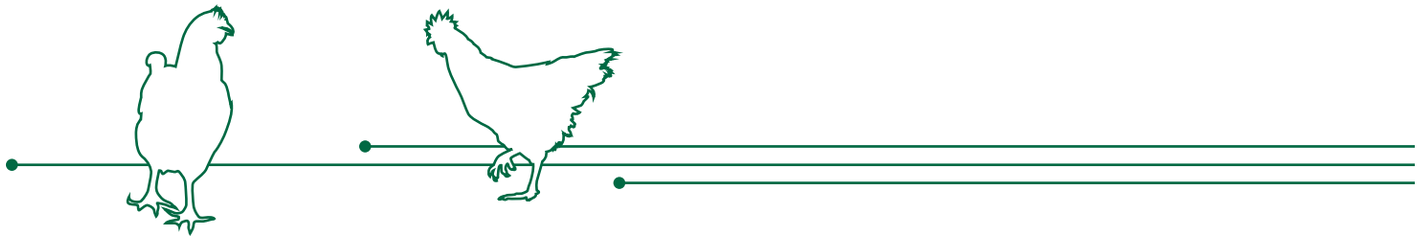
6.2.2.4.3 יש להיות ערים למצב של "עובד ממורמר" אשר מהווה "איום פנימי" ועלול לפגוע במערכות המחשוב ולשבש את פעילות הבקרים בלול המבוקר.

6.2.2.4.4 יש ללוות ליווי צמוד פעילות של ספקים חיצוניים המגיעים פיזית לאתר, לצורך פעילות הקשורה במערכות המחשוב והבקרה של הלול.

6.2.2.5 האיום מכיוון שרשרת האספקה

6.2.2.5.1 יש לוודא שכל חיבור מרחוק לרשת המבוקרת של הלול יבוצע על פי הכללים שלהלן:

- אישור גורם מורשה בתוך הלול להתחברות.
- ההתחברות תתבצע בתווך מוצפן.
- ההתחברות תתבצע ע"י הזדהות לשרת הזדהות ברשת הלול, ולא באמצעות תוכנות Web דוגמת TeamViewer.



- הזדהות למערכות הבקרה של הלול תהיה חד-חד ערכית (באמצעות הזדהות חכמה).
- יש לוודא רישום לוגים המכילים מידע על המערכת שאליה נדרש החיבור: שעת כניסה למערכת, שעת יציאה מהמערכת ושעת סיום התחברות מרוחקת. כמו כן, נדרש לשמור את הלוגים של כל פעילות ההתחברות מרחוק, ואם אפשרי גם לבצע הקלטת כל הפעילות.
- על הספק / הגורם המתחבר להצהיר בדבר עדכוני אבטחה של מערכת ההפעלה והימצאות אנטי-וירוס מעודכן במחשב שממנו הוא מתחבר אל הלול על פי נספח ה' במדריך זה.
- על הספק לעדכן את הגורם המורשה בלול על סיום הפעילות וניתוק התקשורת.

6.2.3 הגנות נוספות למערכות שאינן מחוברות ישירות לרשת הלול

6.2.3.1 הגנות נוספות לרשת הבקרים של הלול המבוקר וגם לרשתות תומכות נוספות במתחם הלול ייושמו לפי נספח ג' למדריך זה.

6.2.4 דרישות מספק הבקר לגבי תפעול הבקר

6.2.4.1 קבלת הנחיות לשינוי משתמש וסיסמה ראשוניים לבקר האחראי על פעילות שוטפת תקינה של הלול.

6.2.4.2 קבלת הנחיות / המלצות על הקשחות נוספות שאפשר לבצע בבקר המטפל בלול המבוקר.

6.2.4.3 קבלת הנחיות / המלצות על אופן הגיבויים ובדיקת שחזורים לבקר המטפל בלול המבוקר.

6.2.4.4 קבלת הנחיות / המלצות על גישה מאובטחת של אנשי הלול אל הבקר המטפל בלול המבוקר.

7. בניית תוכנית עבודה לסגירת פערי ההגנה הנדרשים

7.1 באחריות בעל הלול המבוקר לגבש תוכנית עבודה ליישום הבקרות הנדרשות, בציון הגורמים האחראים, לוחות הזמנים ודרכי הטיפול. בעל הלול יקצה את המשאבים הנדרשים ובכללם תקציב, כוח אדם וזמן הנדרשים ליישום הבקרות הנדרשות.

7.2 סדר העדיפויות של יישום הבקרות החסרות בלול במסגרת תוכנית העבודה, ייקבע באמצעות שקלול עלות הפתרון של יישום הבקרות, מורכבות המימוש, מהירות יישום הבקרות, ושיקול דעתו של בעל הלול.

8. יישום בקרות מומלצות

8.1 הבקרות המומלצות ליישום כתובות בנספח ג' למדריך זה ומסווגות לפי רמות: מרמה 1 ועד רמה 4. ככל שהבקרה ברמה גבוהה יותר, קשה יותר ליישמה, אך ההגנה על העסק מפני תקיפת סייבר טובה יותר.

8.2 מומלץ לקרוא בעיון בקרות אלה וליישמן לפי רמות הבקרה: תחילה בקרות מרמה 1, ולאחר מכן בקרות מרמה 2. במצב זה הלול המבוקר יהיה במצב מוגנות בסיסי.

8.3 אם העסק מעוניין להעלות את החוסן מפני תקיפה סייבר לרמה גבוהה יותר, יש ליישם גם בקרות מרמה 3. מומלץ ליישם בקרות מרמה 4 אם קיים סיכון ממשי לחיי אדם עקב אירוע סייבר שיגרור אחריו אחד מהתרחישים שלהלן: פיזור רעלים, אפקט קרינה בעקבות שריפה, אפקט לחץ עקב פיצוץ.

חבילת הבקרות בהתאם לפוטנציאל הסיכון	סה"כ כמות הבקרות הכוללת לחבילה זו
1	38
2	59
3	81
4	89

9. פעילות שוטפת לשמירה על החוסן מפני מתקפת סייבר

9.1 בדיקת שחזור מגיבוי – אחת לשבוע שחזור מדגמי במערכות: מחשבי HMI, שרתים, בקרים וכל מערכת ממוחשבת קריטית לפעילות השוטפת של הלול המבוקר.

9.2 בדיקת מערכת הפעלה – בשוטף. בדיקה שוטפת של עדכוני מערכת ההפעלה.

9.3 בדיקת עדכוני אנטי וירוס – בשוטף. בדיקה שוטפת של עדכוני אנטי וירוס.

9.4 בדיקת חדירות למערכת מרחוק – אחת לחצי שנה.

9.5 ביצוע הכשרה / הדרכת מודעות עובדים - אחת לחודש.

9.6 תחזוקת נוהלי אבטחת מידע וסייבר – אחת לרבעון.

10. אירוע סייבר

10.1 אם יש חשד לאירוע סייבר יש לנקוט אחת מהפעילויות האלה:

10.1.1 להתקשר בכל שעות היממה למרכז המבצעי לניהול אירועי סייבר של מערך הסייבר הלאומי בטלפון מספר 119 ולדווח על אירוע סייבר.

10.1.2 לפנות למרכז המבצעי לניהול אירועי סייבר באמצעות דואר אלקטרוני: team@cyber.gov.il.

10.1.3 לפנות למרכז ההגנה בסייבר של המשרד להגנת הסביבה בדואר אלקטרוני: socsviva@cyber.gov.il, בטלפון: 072-3990844.

10.1.4 לפנות למוקד החירום של המשרד להגנת הסביבה בטל: 073-2733200 או: 6911*.

10.1.5 לאחר סיום האירוע יש למלא דוח אירוע סייבר לפי נספח ד' במדריך זה, ולשלוח ליחידת סייבר בתעשייה של המשרד להגנת הסביבה בקובץ מוגן סיסמה ל: cyber_industry@sviva.gov.il.

11. מחויבות הנהלה ומינוי ממונה הגנת סייבר

11.1 פעילות ההגנה בסייבר אמורה להיות חלק בלתי נפרד מהתרבות הארגונית של העסק, ומבוססת על המחויבות של בעל הלול והנהלת העסק ליישם את דרישות מסמך זה.

11.2 השלב החשוב בביצוע הוראות מדריך זה הוא תכנון מוקפד של ההנחיות, בצד הקצאת המשאבים הנדרשים ליישומן ובהתאם ללוחות הזמנים שנקבעו.

11.3 על הבעלים של הלול להכין מסמך המפרט את מחויבות הנהלת הלול להגנת סייבר על הלול המבוקר, כולל מחויבות להקצאת המשאבים הנדרשים להעלאת החוסן מפני תקיפת סייבר בלול המבוקר.

11.4 על הבעלים של הלול למנות ממונה הגנת סייבר מטעמו. הממונה יהיה איש קשר בכל הקשור להגנת סייבר בלול ויהיה אחראי על יישום ההנחיות הכלולות במדריך זה, כמו גם על יישום התראות והנחיות שיועברו אליו בהמשך. יצוין כי ממונה הגנת הסייבר אינו חייב להיות אדם בעל הכשרה בסייבר או במערכות IT או בקרה. יש למלא את נספח ו' – מינוי ממונה הגנת סייבר שבמדריך זה.

12. לוח זמנים

12.1 מומלץ להתחיל פעילות מייד עם קבלת מדריך זה.

12.2 מינוי ממונה הגנת סייבר על הלול המבוקר - שבוע מיום קבלת המדריך.

12.3 הכנת מסמך מחויבות הנהלת הלול המבוקר להגנת סייבר – חודש מיום קבלת המדריך.

12.4 מיפוי מערכות המחשוב והבקרים המטפלים בלול המבוקר, כולל הכנת מסמך מפורט - 3 חודשים מיום קבלת המדריך.

12.5 יישום הבקרות הנדרשות - 12 חודשים מיום קבלת המדריך.

12.6 ניטור ובקרה של פערים חדשים עקב הוספת מערכות מחשוב, בקרים, לולים מבוקרים נוספים וכדומה – אחת לשנה.

13. נספחים

נספח א' - מיפוי המערכות הממוחשבות המחוברות ישירות ללול הממוחשב

טבלאות מערכות ממוחשבות קריטיות לפעילות הלול המבוקר

1. מיפוי בקרים

יצרן	דגם	גרסת חומרה	גרסת תוכנה	תפקיד הבקר	כתובת IP	מועד עדכון אחרון (תוכנה או חומרה)

2. מיפוי עמדות HMI

מערכת הפעלה	שם תוכנת HMI	גרסת תוכנת HMI	תפקיד HMI	כתובת IP	מועד עדכון אחרון (תוכנה או חומרה)

3. מיפוי מערכות קריטיות נוספות לתפעול הלול (סנסורים, רכיבי שטח, גלאים המחוברים לרשת המחשוב)

רכיב	דגם	גרסת חומרה	כתובת IP	מועד עדכון אחרון (תוכנה או חומרה)

נספח ב' - מיפוי המערכות הממוחשבות שאין להן חיבור ישיר ללול הממוחשב

טבלת מערכות ממוחשבות תומכות בפעילות הלול המבוקר

רכיב	דגם	מערכת הפעלה	תפקיד	כתובת IP	מועד עדכון אחרון (תוכנה או חומרה)

נספח ג' - רשימת בקרות

1. מבוא

כדי להפחית את הסיכון לאירוע סייבר, בעל העסק נדרש ליישם בקרות בתחומים שונים הקשורים לסייבר. בקרות אלו כוללות תהליכים, נהלים, מערכות הגנה, טכנולוגיות ועוד.
בקרות אלו מאוגדות על פי הנושאים: בקרות להגנה על שרתים ותחנות קצה, בקרות על ניהול משתמשים, בקרות ניטור, נהלים ועוד.

2. פירוט רשימת הבקרות

ישנן ארבע רמות של בקרות, מרמה 1 עד רמה 4. מומלץ ליישמן לפי הסדר, בקרות מרמה 1 תחילה, לאחר מכן רמת בקרה 2, ואם העסק מעוניין להעלות את רמת החוסן שלו לאירוע סייבר עד לרמה המרבית, יש ליישם גם בקרות מרמה 3 ו-4.

3. בחירת בקרות ליישום

כפי שכבר נכתב במדריך זה, בעל הלול יישם בקרות ברמה 1 ו-2 לפחות, על מנת לקבל מיגון בסיסי, ובשלב מתקדם יותר ועל פי שיקול בעל הלול המבוקר, כדי להגביר עוד יותר את החוסן - מומלץ ליישם בקרות ברמה 3. בקרות ברמה 4 מיועדות למקרים שיש סיכון ממשי לחיי אדם, ומומלץ ליישמן רק במקרים אלה.

רשימת הבקרות

4. רשימת הבקרות בטבלה להלן:

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות בפרק זה
1	מיפוי מערכות מחשוב ובקרת הלול המבוקר **1.1** בעל העסק ימפה את המערכות הממוחשבות המנהלות / מבקרות את הלול המבוקר.	**1.1** המיפוי יכלול: רשימת המחשבים - בציון תפקידם והמערכות המותקנות עליהם לצורך תפקידם; עמדות HMI/ אוטומציה ייעודיות/ משולבות מכונה - בציון דגם וגרסת תוכנה; בקרים ומרכזות גלאים - בציון דגם, גרסת קושחה/תוכנה וסוג התקשורת Ethernet) Wi-Fi טלפון, אחר); רכיבי IoT/IIoT וגלאים בציון דגם, מקום וסוג התקשורת אליהם; רכיבי הרשת (מתגים, נתבים, נקודות גישה אלחוטיות, חומת אש) בציון דגם וחיבורם לרשתות אחרות/ אינטרנט.		1	**1.1** האם מופו מערכות המחשוב והבקרה.	1

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
1	בדיקת חדירות (Penetration Test) **1.6** אחת לשנתיים יש לעשות בדיקת חדירות בעזרת מומחה אבטחת מידע, אשר תכלול לפחות: **א.** בדיקת עמידות מערכות המחשוב ובקרת הלולים להתקפה מחוץ לעסק. **ב.** בדיקת עמידות מערכות המחשוב ובקרת הלול להתקפה מרשת ה-IT בעסק. **ג.** בדיקת עמידות מערכות המחשוב ובקרת הלול לתוקף בעל גישה פיזית לעמדות תפעול ולארונות התקשורת והבקרים.			4	1.6 דוח הבדיקה	1

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
4	בקרת גישה בסיסית 4.1 עמדות המחשוב יהיו מוגנות בשם וסיסמה אישיים, ויינעלו אוטומטית אחרי 10 דקות של חוסר שימוש או על פי החלטת העסק, ולא יותר מ-30 דקות. 4.2 משתמשי מערכות המחשוב יופרדו לפחות לשתי רמות הרשאות ברמת מערכת ההפעלה - "משתמש" (וביחס אליהם ייאכפו הרשאות מינימליות להפעלת מערכות על פי תפקידם, גישה מינימלית לקבצים ומשאבים ברשת, אי יכולת להתקין תוכנה) ו"מנהל" בעל הרשאות רחבות יותר לשיקול העסק. 4.3 לעמדות הפעלה (HMI/ אוטומציה ייעודיות/משולבות מכונה) יוגדרו הרשאות גישה אפליקטיביות למשתמשים מורשים. ההרשאות יהיו ברמת צפייה, ברמת הפעלת תהליכים מוגדרים, וברמת ביצוע שינויים במערכת ובתהליכים. 4.4 יוגדרו בעלי תפקיד המורשים לבצע שינויי הגדרות ופעולות תחזוקה לבקרים, חיישנים ורכיבי SCADA. יזוהו שמית המורשים לעשות זאת מרחוק (באמצעות אפליקציה, חיבור רשת, טלפוניה וכו'). 4.5 יוגדרו בעלי תפקיד הרשאים לבצע שינויים והגדרות ברשתות העסק. 4.6 לכל עמדת HMI, תחנת עבודה ומחשב המשמש לתכנות בקרים, תוגדר תצורת התוכנות הדרושות ותיאסר התקנת תוכנות אחרות.	מדיניות בקרת הגישה נועדה לוודא כי רק גורמים מורשים יכולים לגשת למחשוב ובקרת הלול, לצפות ולעשות שינויים, וכל זאת בהתאם להגדרות תפקידיהם וכפוף לפיקוח.		1	4.1-3 הדגמה מוצלחת של הזדהות, הרשאות שונות על עמדות אקראיות. 4.4-5 הצגת רשימת בעלי התפקידים. 4.6 בדיקת תוכנות המותקנות על עמדות אקראיות.	6

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
4	בקרת גישה מתקדמת 4.7 יש לסקור את רשימת המשתמשים מורשי הגישה למערכות מחשוב ובקרת הלול, לפחות בתדירות רבעונית ולעדכן אותה אם חל שינוי בכוח האדם ובעלי התפקידים המורשים בעסק. 4.8 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. 4.9 תוגדר ותיאכף מדיניות העוסקת בהתחברות לרשת התפעולית מרחוק, אשר מגדירה את מגבלות השימוש בהתחברות מרחוק למערכות מחשוב ואוטומציה של הלול המבוקר. כל חיבור מרחוק יהיה מוצפן מקצה לקצה ומזוהה אישית בהזדהות חזקה (2FA). 4.10 תיאסר ותיחסם גישה למערכות מחשוב ובקרת הלול המבוקר מרשתות אלחוטיות של העסק, ותותר רק ממחשבי העסק המחוברים בחיבור חוטי לרשת. 4.11 תוגדר ותיאכף מדיניות סיסמאות נאותה, הכוללת אורך, מורכבות וזמן תפוגה. 4.12 תוגדר מדיניות אישור מחשבים ניידים המשמשים לקונפיגורציה מקומית של בקרים ומערכות אוטומציה. 4.13 שינויים קריטיים בעמדות HMI דוגמת שינויי הזנה, טמפרטורות, ניקוי ואוורור ידרשו הקפצת חלון להזדהות נוספת. לא ייעשו שינויים קריטיים על פי הוראה שניתנה בדואר אלקטרוני / הודעת טקסט / שיחת טלפון / שיחת וידאו.	4.11 מומלץ 8 תווים לפחות, מורכבות של 3 מתוך 4 (אותיות גדולות, קטנות, מספרים ותווים מיוחדים). 4.12 למשל מחשב נייד ללא חיבור לאינטרנט שלא יוצא מתחומי העסק ולצורך תכנות הבקר בלבד. או מחשב של טכנאי חיצוני מוכר שנבדק בדיקת נוזקות. 4.13 יש לתוקפים יכולת זיוף דואר אלקטרוני, הודעות טקסט, התחזות בטלפון ואף בשיחת וידאו.	4.10 ניתן ליישום באמצעות מערכת לחיבור חד-כיווני לסיגנלים החשמליים ישירות מהסנסורים והמפעילים (level 0) בתצורה מנותקת לחלוטין מרשת הלול ולא מושפעת ממנה. 4.13 ניתן לממש בקרה מפצה לפי שיקול העסק להקפצת חלון הדורש הזדהות נוספת. על הבקרה המפצה לוודא שלא ייעשה שינוי מהותי אשר עלול לגרום לאירוע סייבר בלול המבוקר ע"י גורם בלתי מורשה.	2	4.7 הצגת רשימה מעודכנת. 4.8 בדיקה על עמדה אקראית. 4.9 הדגמת אופן חיבור מרחוק. 4.10 בדיקה באמצעות מחשב ברשת האלחוטית. 4.11 הדגמת שינוי סיסמה. 4.12 הצגת המדיניות. 4.13 הדגמת התהליך של הקפצת חלון.	7

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
4	בקרת גישה מחמירה 4.14 מדיניות החיבור מרחוק תוגבל רק למשתמשים שהזדהו בהזדהות חזקה (2FA) ומחשבם נבדק וזוהה כבטוח (סרוק ונקי מקוד זדוני ובעל עדכוני אבטחת מידע במערכת ההפעלה כמו גם אנטי וירוס מעודכן). 4.15 משתמש המנסה לבצע פעולה אסורה (הכנסת DOK, התקנת תוכנה) יינעל מייד והתראה תצא למנהל המערכת. 4.16 משתמש בעל הרשאות יתר (מנהל מחשוב, יכולת שינויי תצורה במערכות הייצור) יידרש להזדהות חזקה ויוגבל, אם המערכת מאפשרת זאת, לעבודה בעמדה אחת בלבד בו-זמנית. 4.17 תיאסר ותיחסם כליל אפשרות השתלטות ישירה על מערכות מחשוב של הלול המבוקר העובדות במוד אינטרנטי (Remote Desktop, TeamViewer, Remote Assist, AnyDesk וכו'). 4.18 תיאסר ותיחסם גישה ישירה לרכיבי חומרה (בקרים, חיישנים וכו') מחוץ לעסק. 4.19 יש לנטר ולבצע רישום של כל פעילות שנעשית מרחוק. 4.20 יש לתעד ביומן רישום אוטומטי (רישום Log) של כל יצירה, שינוי, אפשור, נעילה והסרה של חשבון.		4.16 תתאפשר בקרה מפצה אשר עונה על הצורך האבטחתי. 4.17 תתאפשר בקרה מפצה הולמת אשר מונעת את אפשרות הגישה של גורם בלתי מורשה למערכות המחשוב המנהלות / מבקרות את הלול.	3	4.14 הדגמת התהליך. 4.15 הדגמת התהליך. 4.16 הדגמת התהליך. 4.17 בדיקת הגדרות במחשבים וברשת (FW/SWITCH) 4.18 הדגמת התהליך. 4.19 הצגת התיעוד.	7

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
4	בקרת גישה מרבית 4.21 לא תינתן גישה למערכות מחשוב ואוטומציה המטפלות בלול המבוקר ע"י מחשבים אשר הגיעו מחוץ לעסק או עזבו את תחומו. 4.22 לא יתאפשר חיבור מרחוק כלשהו אל רשת הלול המבוקר, למעט צפייה בלבד (קבלת סטטוס) בחיבור חד-כיווני מאובטח. 4.23 יש להגדיר ולאכוף תנאים לחסימת שימוש בחשבונות, בהתאם לשעות פעילות העסק, ובהתאם לשעות העבודה של סוגי העובדים.	4.21 כגון: מחשבים ניידים של טכנאים, אפליקציות SCADA לטלפונים חכמים על מכשירי העובדים. דוגמאות לתנאי חסימת כניסה: סופי שבוע, שעות הלילה.	4.22 ניתן ליישום באמצעות מערכת לחיבור חד-כיווני לסיגנלים החשמליים ישירות מהחיישנים והמפעילים (level 0) בתצורה מנותקת לחלוטין מרשת הלול ולא מושפעת ממנה.	4	4.20 בדיקת התיעוד. 4.21 הצגת הפתרון החד-כיווני. 4.22 הצגת אופן המימוש.	3
6	הקשחת תחנות עבודה, HMI ושרתים 6.1 יש להגדיר את תצורת המערכת כך שתספק את הפונקציונליות המינימלית הנדרשת (תוך הסרת אפליקציות, חסימת פונקציות, פורטים ופרוטוקולים שאינם נדרשים), על בסיס פרקטיקות מקובלות, כך שיכללו לכל הפחות: א. חסימת פורטים שאינם נחוצים; ב. הסרת אפליקציות, תוכנות מ"ה ושירותים לא נחוצים; ג. הסרת חשבונות אורח/ברירת מחדל ומנהל מקומי; ד. מנגנון קבלת עדכוני מערכת הפעלה; ה. חסימת הכנסת התקני אחסון ומדיה; ו. חסימת התקנת תוכנה וחומרה על-ידי משתמשים לא מורשים;	6.1 ד. כגון WSUS או הבאה ידנית של עדכונים ע"ג מדיה. 6.1 ה. כגון DOK, CD/DVD, מכשיר סלולרי, מצלמה וכדומה.	6.1 ניתן להתבסס על פרקטיקות מקובלות, כגון NIST, פרסומי ה-CERT הלאומי וכדומה, או על שירותי מומחה, אשר יכין נוהלי הקשחה לפי הטכנולוגיה הרלוונטית.	1	6.1 הצגת אופן ההקשחה שנעשתה לכל סוג של מערכת מחשוב.	1

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
7	מניעת קוד זדוני בסיסית 7.1 יש להטמיע כלים לזיהוי ולמניעה של קוד זדוני על תחנות עבודה ושרתים בעסק. כלים אלו יופעלו במתכונת התראה / הגנה אקטיבית (לשיקול העסק) וכן יבוצעו סריקות תקופתיות. 7.2 העסק יגדיר נהלים לטיפול בתחנות, ברשתות או בשרתים הנגועים בקוד זדוני. 7.3 יש לקבוע מנגנון קבלה והעברה של עדכונים לכלים (מסעיף 7.1) בתדירות דו-שבועית לפחות.	7.1 מאחר שחלק מהפוגענים עשויים לחדור את מנגנוני האבטחה, יש לוודא כי בקרות לטיפול בקוד זדוני ייושמו בכל השרתים ובתחנות העבודה. 7.3 בדומה לעדכוני מערכת הפעלה יש להציג פתרון עדכונים לכלי.	7.1 אפשר להשתמש בכל כלי לזיהוי ומניעה של קוד עוין (כגון אנטי-וירוס) מיצרן מוכר.	1	7.1 הצגת הכלי המותקן. 7.2 הצגת הנוהל. 7.3 הצגת מנגנון העדכון.	3
7	מניעת קוד זדוני מתקדמת 7.4 יש להטמיע כלי לזיהוי וחסימת נוזקות ברמת הרשת. 7.5 העסק יפעיל אמצעים לזיהוי ומניעה IDS/IPS, המתבססים על זיהוי התנהגות החורגת מהתנהגות מקובלת וסבירה (זיהוי אנומליה ברשת והתנהגות עמדה/משתמש). 7.6 העסק ינהל באמצעות מערכת בקרה מרכזית (SIEM) את כלל כלי מניעת הקוד הזדוני ואבטחת המידע בעסק.	7.4 ניתן למימוש באמצעות חומת אש בעלת סינון תוכן ומערכות IDS רשתיות.	7.5 אפשר להשתמש בבקרה מפצה אחרת שתיתן מענה לצורך. 7.5 ניתן ליישום באמצעות הטמעה של מערכת לזיהוי אנומליות תהליכיות בסביבת הסיגנלים החשמליים. 7.5 ניתן להפעיל ב-IPS את רכיב ה-IDS בלבד, כל עוד יש מענה אנושי שיחליף את המענה האוטומטי של חסימה, והוא יפעיל שיקול דעת ויחליט מה לחסום.	3	7.4 הצגת הכלים ואופן הטמעתם.	3

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
9	אבטחת רשת בסיסית 9.1 יש לתעד במסמכים את תיאור הרשתות המשמשות את מערכות המחשוב והאוטומציה של הלול המבוקר, ההפרדות, המגבלות וההגנות שיושמו בהן. 9.2 תוגבל הגישה מרשתות אחרות בעסק (IT, Wi-Fi) לרשתות המשמשות את מערכות המחשוב והאוטומציה של הלול המבוקר באמצעות ניהול הרשאות. 9.3 יש ליישם מנגנונים למניעת חיבור לא מורשה לרשתות המשמשות את מערכות המחשוב והאוטומציה של הלול המבוקר. 9.4 הרשתות המשמשות את מערכות המחשוב והאוטומציה של הלול המבוקר ינותקו מרשת האינטרנט, למעט אפשרות חיבור ייעודי מוצפן (VPN). 9.5 יש למנוע גישורים בין רשתות שונות באמצעות כבלים וחיבורים שונים כגון חיבורים סריאליים (RS-232 וכדומה), המשמשים לשליטה ובקרה על ציוד. מחשבים המשמשים להגדרת ציוד מקרוב ינותקו מהאינטרנט. 9.6 יש לוודא כי לכל מרכיבי הרשת (מתגים, נתבים, חומת אש, נקודות גישה) יש סיסמאות ניהול מורכבות וייחודיות השונות מסיסמת ברירת מחדל של היצרן, והשמורות אך ורק אצל בעלי התפקידים המוסמכים לעשות שינויים בהגדרות הרשת.	9.3 יש לוודא כיבוי כל הפורטים שאינם בשימוש במתגים, והפעלתם בהגדרה ידנית או מנגנוני NAC.	מומלץ לבצע הפרדת רשתות פיזית או באמצעות חומת אש.	1	9.1 הצגת תיעוד הרשתות. 9.2-6 הצגת ההגבלות שיושמו.	6

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
9	אבטחת רשת מתקדמת 9.7 ברכיבי החומרה התומכים בחיבור אלחוטי יש לכבות או להסיר את יכולת החיבור האלחוטי. 9.8 תימנע גישה ישירה מחוץ לרשת המקומית לרכיבי חומרה. גישה מחוץ לרשת המקומית תוגבל אך ורק לעמדות ניהול הדורשות הזדהות. 9.9 יש ליישם סינון תקשורת ברמה פרטנית ברשתות המשמשות את מערכות המחשוב והאוטומציה של הלול המבוקר ולהגדיר בדיוק את הפורטים ונתיבי התקשורת המותרים. 9.10 יש לבצע סריקת רשתות תקופתית המאזינה לתקשורת ברשתות המחשוב והאוטומציה של הלול המבוקר, לזהות את כל האלמנטים המשתתפים בתקשורת וסוגי התקשורת שהם יוזמים ומקבלים, להסיר אלמנטים לא מזוהים, לנתח חריגות בתקשורת ולתקן בהתאמה את מנגנוני ההפרדה. תדירות הביצוע תהיה אחת ל-18 חודשים לפחות.			3	9.7-8 הצגת הפעולות שנעשו. 9.9 הצגת יישום הסינון. 9.10 הצגת תוצאות הסריקה האחרונה.	4
9	אבטחת רשת מרבית 9.11 הרשתות המשמשות את מערכות המחשוב והאוטומציה של הלול המבוקר יהיו סגורות, חוטיות ונפרדות לחלוטין (מתגים וכבילה נפרדת) מרשתות אחרות של העסק. 9.12 החיבור היחיד שיותר החוצה הוא הוצאת נתוני בקרה/סטטוס/לוגים באופן חד-כיווני לרשת אחרת, באמצעות פתרון מאושר להעברת מידע באופן חד-כיווני. 9.13 יש ליישם מנגנונים בתוך הרשתות, שמסננים תקשורת שאינה תואמת את מבנה הפרוטוקול/ המידע המצופה.			4	9.11 הצגת הרשת הנפרדת. 9.12 הצגת הפתרון החד-כיווני. 9.13 יש להציג את פתרון הסינון.	3

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
10	הפרדת סביבת מערכות המחשוב והאוטומציה ברשת הלול המבוקר 10.1 יש להגדיר תהליך אישור להעברת נתונים, סקריפטים ותוכנה שהתקבלה מסביבה אחרת בעסק או מחוצה לו אל סביבה זו. 10.2 יש לבצע עדכוני תוכנה וקושחה ישירות מיצרן הציוד או התוכנה באופן מאומת. 10.3 יש לאסור הכנסת סקריפטים או קונפיגורציות לאוטומציית ייצור/HMI או לקונפיגורציות בקרים שמקורם אינו ידוע או אינו מאומת.	10.2. אימות התוכנה והקושחה באמצעות checksum או קבלת מדיה ישירות מנציג החברה.		1	10.1-3 הצגת התהליכים להעברת עדכוני קושחה ותוכנה ובדיקתם.	3
11	שימוש במשאבי ענן ציבורי בעבור מערכות המחשוב והאוטומציה ברשת הלול המבוקר. 11.1 יש להגדיר מספר מצומצם של בעלי תפקידים בעלי גישה לממשק הניהול של שירות הענן. 11.2 חיבור לממשק הניהול של שירות הענן יהיה מאובטח בהזדהות חזקה. 11.3 יש לוודא כי גם השרתים/המכונות המופעלים בענן עונים לכל הדרישות המתאימות לרמת הבקרה הנדרשת בהתאם לפוטנציאל הסיכון (לרבות הקשחה, הגבלת תקשורת, כלים למניעת קוד זדוני, שימוש בהרשאות מינימליות למשתמשים וכו').	11. כל הבקרות במסמך זה תקפות גם לשימוש במחשוב ענן ציבורי. על העסק המעלה נתונים לענן לוודא חלוקת אחריות ברורה לאבטחת המידע בין ספק הענן ללקוח.		1	11.1-2 יש להציג את בעלי התפקידים ואת אופן ההזדהות. 11.3 הצגת סוגי המכונות בשימוש וההגנות שיושמו.	3

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
11	חיבור חד-כיווני 11.4 מערכות מחשוב ובקרת הלול יוגבלו רק לייצוא נתונים לענן בחיבור חד-כיווני, באמצעות פתרון מאושר להעברת מידע באופן חד-כיווני.		11.4 ניתן ליישום באמצעות מערכת לחיבור חד-כיווני לסיגנלים החשמליים ישירות מהסנסורים והמפעילים (level 0) בתצורה מנותקת לחלוטין מהרשת המפעלית ולא מושפעת ממנה.	4	11.4 הצגת הפתרון החד-כיווני.	1
12	הגדרת כללי שימוש ותחזוקה 12.1 יוגדרו בעסק בעלי תפקידים המורשים לגשת לבקרים (לתחזוקה מקרוב) ולעמדות ניהול/HMI וכן כללים לביצוע שינויי קונפיגורציה, זיהוי והתמודדות עם כשלים בבקרים (אישורים נדרשים, פיקוח, סדר עצירת/הפעלת מערכות). 12.2 עדכוני קושחה, שינויי קונפיגורציה וכדומה ייבדקו מראש בסביבת מעבדה בטרם העברתם לסביבת ייצור.	12. המטרה - למנוע אירוע שיגרום נזק ללול המבוקר עקב טעות אנוש, כשל בבקר או שינוי קונפיגורציה שגוי.		1	12.1 הצגת הנהלים. 12.2 הצגת תהליך הבדיקה.	2

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
12	מעקב תצורה וגיבוי 12.3 העסק ינהל רישום של הבקרים הנוגעים ללול המבוקר ויכלול לפחות: יצרן, דגם, גרסת קושחה, גרסת קונפיגורציה, מיקום קובץ קונפיגורציה לגיבוי, מיקום גרסת קושחה לגיבוי. 12.4 יש לגבות קושחות וקונפיגורציות של בקרים, סקריפטים, תצורות/Image תחנות עבודה/HMI ותהליכי ייצור במערכת מאובטחת/ נפרדת, המרוחקת פיזית (50 קילומטרים לפחות) מהאזור שממנו נלקח הגיבוי. 12.5 העסק צריך להיות בעל יכולת לשחזר בקר מגיבוי, או לשחזר תחנת עבודה/HMI בתוך יום עבודה מזיהוי תקלה או פעולה חריגה. לחלופין -השבתת התהליך המבוקר עד לסיום השחזור. 12.6 על העסק להיות בקשר רציף עם יצרני הבקרים והמערכות שברשותו ולקבל עדכונים על סוגיות אבטחת מידע וגרסאות תוכנה וקושחה עדכניות.	12.5 היכולת יכולה להיות עצמאית או באמצעות מיקור חוץ.	12.4 רצוי גם בעותקים על מדיה נתיקה (דיסק, DOK) שיישמרו באתר במרחק של לפחות 50 ק"מ מהאזור שממנו נלקח הגיבוי.	2	12.3 הצגת הרישום. 12.4-6 הצגת הגיבויים, יכולת השחזור, עדכונים מהיצרן.	4

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
12	אבטחה מתקדמת 12.7 יש לבצע הקשחה של הבקרים על פי הוראות היצרן, ולהשתמש בכל יכולות אבטחת המידע של הבקר הנוגעות להזדהות, צמצום והגנת התקשורת אליו ומניעת שינויים לא רצויים. יש לבצע בדיקה של ההקשחה בסביבת מעבדה לפני העברה לסביבת ייצור. 12.8 יש לוודא כי לכל בקר יש סיסמת ניהול מורכבת וייחודית, ולא סיסמת ברירת מחדל של היצרן. הסיסמה תהיה שמורה אך ורק אצל בעלי התפקידים המוסמכים לעשות שינויים בבקרים. 12.9 גישה לתחנות עבודה/HMI תדרוש הזדהות חזקה. 12.10 מערכת ההפעלה של תחנת עבודה/HMI ללא שימוש תינעל לאחר 10 דקות או לשיקול המפעל, אך לא יותר מ-30 דקות, למעט תחנות שהוגדרו לצפייה בלבד. 12.11 ניסיון לחולל שינוי מהותי בתהליך, דוגמת שינוי ספים לערכים קריטיים בלול , ידרוש הזנה נוספת של סיסמה או ביצוע הזדהות חזקה בטרם השלמתו.	12.7 ליצרנים שונים הנחיות הקשחה שונות בהתאם ליכולות הציוד, לרבות סגירת פורטים, הפסקת תמיכה בפרוטוקולים לא מוצפנים, דרישת הזדהות לפני ביצוע שינוי קונפיגורציה, יכולת שחזור אוטומטית של קונפיגורציה קודמת ועוד.		3	12.7 הצגת ההקשחות. 12.8-10 סקירת ההגנה המתקדמת. 12.11 הצגת יישום ההפרדה.	5

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
12	אבטחה מרבית 12.12 מערכות המחשוב יחויבו לרוץ על מערכת הפעלה עדכנית נתמכת, המקבלת עדכוני אבטחה רציפים. 12.13 שינויי תהליך ידרשו אישור בהזדהות חזקה של מנהל בכיר. 12.14 הבקרים יופרדו לרשתות שונות בהתאם לתפקידם/ לתהליך שהם משתתפים בו. תחנות העבודה/HMI יחוברו לרשת נפרדת מהבקרים. תקשורת בין הרשתות תנוהל באמצעות חומת אש.	12.12 גרסאות נתמכות של חלונות, לינוקס וכו'. 12.14 אפשר לבצע על בקרים חלופיים כבדיקה לפני העלאה לייצור או על בקרי ייצור בתקופות השבתה / הדממה של מערכות הייצור.	12.13 ניתן להשתמש במגוון אמצעים, כגון ביומטריה, כרטיסים חכמים, OTP ועוד.	4		3

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
12	הגנה והפרדה של מערכות בטיחות, גילוי ואבטחה 12.15 יש לוודא כי רשת הגלאים בעסק תבודד ברשת נפרדת ללא אפשרות גישה ממנה אל מערכות מחשוב ובקרת הלול. 12.16 עמדת בקר הגלאים תהיה נעולה בארון תקשורת על מנת לוודא שלא יבוצעו שינויים בלתי- מבוקרים. 12.17 אם בבקר הגלאים יש יכולת לנעילת מצב תכנות הבקר, עליו להיות במצב נעול בזמן שגרה. 12.18 אם בקר הגלאים מחובר בחיבור רשת/טלפוניה למוקד שמירה/תמיכה, יש לוודא כי נמנעת היכולת לבצע שינויי הגדרות/השבתה מרחוק. 12.19 גדרות חשמליות, מערכות בקרת גישה, מערכות מתח נמוך - יש להפרידן רשתית ללא אפשרות גישה מהן אל מערכות מחשוב ובקרת הלול המבוקר. 12.20 מצלמות אבטחה - יש למנוע גישה פיזית אל מצלמות האבטחה, ולהפרידן רשתית ללא אפשרות גישה מהן אל מערכות מחשוב ובקרת הלול המבוקר.	12.15 אם רשת הגלאים היא חלק מרשת הייצור, פריצה לרשת זאת תאפשר גישה לרשת רצפת הייצור. 12.16 אם עמדת הבקר גלויה, יש חשיפה לשינוי ערכי סף בגלאים. 12.17 בבקרים ישנם מצבי תכנות ומצבי עבודה. אין להשאיר את הבקר במצב פתוח לתכנות בזמן עבודה שגרתית. 12.18 במידת הצורך יתאפשר שינוי הגדרות רק לזמן קצוב למתן תמיכה מרחוק וייחסם שוב. 12.19-20 במצלמות ובמערכות מתח נמוך אחרות שהגישה הפיזית אליהן חופשית, יש אפשרות להכניס מדיה נתיקה או להתערב בצורה אחרת, ודרכם להחדיר קוד זדוני.	12.15 ניתן ליישם באמצעות חומת אש או בידוד פיזי או פריסת גלאים במגע יבש. 12.17 ניתן ליישם באמצעות נעילה פיזית או לוגית כפי שנתמכת על ידי הבקר. 12.19-20 ניתן ליישם באמצעות חומת אש או הפרדה פיזית. 12.20 מומלץ במידת האפשר להציב את המצלמות גבוה, ולהימנע מחיבור אלחוטי.	1		6

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
15	מדיות בשימוש בקרים ועמדות תפעול/HMI 15.1 על מנת להעביר גרסאות תוכנה וקושחה, קונפיגורציות, סקריפטים וכו' יש להשתמש במדיה ייעודית של העסק, השמורה לשימוש זה בלבד במקום בטוח. 15.2 מדיות המשמשות לגיבוי גרסאות קושחה, קונפיגורציות בקרים וסקריפטים יאוחסנו במקומות בטוחים ונעולים. 15.3 יש לסרוק נוזקות במדיה שבה מועבר המידע לפני כל העברה.	15.1 מדיה שיש לה שימושים אחרים חשופה יותר להידבקות בנוזקה. 15.2 סריקת נוזקות במדיה במחשב / עמדת הלבנה שאינן קשורות למחשוב ובקרה של הלול המבוקר.		1		3
18	מודעות ואכיפה 18.1 יש להפיץ בקרב העובדים והשומרים הנחיות מתאימות - עובדים ואורחים שאינם קשורים למערכות הבקרה והמחשוב המחוברות ללול המבוקר, לא אמורים להיות בסביבתן. עובד לא מורשה שיימצא למשל בסמיכות לארונות בקרים או גלאים, מחבר אלמנטים לרשת על דעת עצמו, או מנסה לגשת לעמדות תפעול/HMI - יטופל בחומרה. העסק יכתוב ויפיץ נוהל ברוח הדברים. 18.2 יש לנעול ארונות תקשורת וארונות בקרים ולוודא את הימצאות המפתח במקום דיסקרטי.			1	18.1 הצגת פעילות ההסברה שנעשתה בקרב העובדים והשומרים. 18.2 בדיקת נעילה.	2

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
18	אבטחה מתקדמת 18.3 יש להציב מצלמות אבטחה לתיעוד הגישה לארונות תקשורת, ארונות בקרים ותחנות עבודה/HMI. 18.4 יש להתקין מערכת אזעקה שתתריע על ניסיון לגשת לארונות תקשורת, ארונות בקרים ותחנות עבודה שלא בשעות העבודה. 18.5 יש להפיץ בקרב העובדים והשומרים הנחיות מתאימות - טכנאים חיצוניים ומבקרים יידרשו להפקיד אצל גורם מוסמך בעסק כל מדיה (מגנטית, אופטית), טלפון סלולרי ואמצעי מחשוב שברשותם לפני גישה או קרבה פיזית למערכות מחשוב ובקרה של הלול המבוקר.		18.3 ניתן ליישם באמצעות הצבת מצלמות מול עמדות HMI או מצלמות בעלות עדשה נעה, אשר סורקות גם את אזור עמדות ה-HMI ופנלים לוקליים. 18.4 אם ישנה התנגדות פנימית בעסק להצבת מצלמות מסיבות של שמירת הפרטיות, התנגדות ועדי עובדים וכדומה, יש ליישם בקרה מפצה אחרת אשר מהווה מענה חלופי והולם לבקרה זו. 18.5 מומלץ להחיל את הנוהל גם על עובדים, למעט מדיות ייעודיות המשמשות לעבודה בלבד.	3	18.3-4 הצגת אמצעי האבטחה. 18.5 הצגת פעילות ההסברה שנעשתה בקרב העובדים והשומרים.	3

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
19	עובדים בעלי גישה למערכות מחשוב ואוטומציה המטפלות בלול המבוקר 19.1 יש להחתים את העובדים על הצהרת התחייבות להקפיד על דרישות אבטחת המידע של העסק, והצהרת סודיות לגבי מערכות המחשוב והבקרה של הלול המבוקר. 19.2 יש להשעות גישה לעובדים אשר יש לגביהם חשש (ממורמרים, לא יציבים, לא ממלאים הנחיות). 19.3 יש לבטל הרשאות גישה ולחסום חשבונות משתמש בעת סיום העסקה. 19.4 יש להנחות עובדים שלא לקבל הנחיות לביצוע פעולות במערכות המחשוב והבקרה של הלול המבוקר על פי הוראה שניתנה בדואר אלקטרוני / הודעת טקסט / שיחת טלפון / שיחת וידאו.	19.1 חשיפת מידע על אודות מערכות המחשוב והבקרה של הלול המבוקר עלולה לאפשר לתוקף לתכנן ולבצע מתקפת סייבר שתגרום נזק משמעותי ללול המבוקר. 19.4 יש לתוקפים יכולת זיוף דואר אלקטרוני, הודעות טקסט, התחזות בטלפון ואף בשיחת וידאו.		2	19.1-4 הצגת הפעילות שנעשתה בקרב העובדים.	4

סעיף	בקרה נדרשת	פירוט	המלצות / הערות	רמה	בדיקה	מס' הבקרות
24	זיהוי וניהול אירועי סייבר למערכות מחשוב ואוטומציה המטפלות בלול המבוקר 24.1 על העסק להכין תוכנית תגובה לאירוע סייבר במערכות ממוחשבות של הלול המבוקר. התכנית תתורגל אחת לשנה לפחות. 24.2 אם אומת חשד לאירוע סייבר במערכות ממוחשבות של הלול המבוקר, יש לעדכן את מוקד מערך הסייבר הלאומי ואת יחידת הסייבר בתעשייה במשרד להגנת הסביבה.	24.1 התוכנית תכלול בירור ההתנהגות החשודה מול אנשי המקצוע בעסק ומחוצה לו, יידוע הנהלה, סמכות קבלת החלטה לניתוק רכיב/השבתת מערכת/ניתוק תקשורת עד לבירור העניין, בדיקות תקינות שיש לבצע ברכיבים אחרים ועוד. 24.2 מוקד הסייבר הלאומי בטל' 119 (24/7) ובמייל: team@cyber.gov.il יחידת הסייבר בתעשייה במייל: cyber_industry@sviva.gov.il	24.1 ניתן להפנות לנהלים קיימים להשבתת מערכת והחלפת רכיב מקולקל.	1	24.1 הצגת התוכנית והנהלים. 24.2 הצגת היסטוריית האירועים שהתגלו ודווחו.	2
25	תיקון וחזרה לפעילות לאחר אירוע סייבר 25.1 יש לכתוב במסמך מדיניות אבטחת המידע את תהליך ההתאוששות מאירועים - התוכנית תתחשב בתרחישי האסון למיניהם בלול המבוקר (למשל לכמה זמן אפשר להשבית בבטחה בקר מסוים או מערכת HMI). 25.2 יש לוודא חזרה לשגרה על פי נוהל חזרה לשגרה. 25.3 יש לכתוב ולשלוח ליחידת הסייבר בתעשייה בתוך 60 יום מגילוי האירוע מסמך תחקיר, המסכם את מהות האירוע, את הכשלים שאפשרו אותו ואת הלקחים שהופקו.		25.1 אפשר להפנות לנהלים להשבתת מערכת והחלפת רכיב מקולקל.	2	25.1 הצגת הנהלים הצגת החלפים והגיבויים לצורך ההתאוששות.	3
						89

נספח ד' – דוח אירוע סייבר בלול

שם העסק:.....

1. פרטי איש קשר המדווח על האירוע:	
שם:	
תפקיד:	
טלפון:	
כתובת דואר אלקטרוני:	

2. תיאור האירוע
תקציר האירוע:

3. פרטים על האירוע	
תאריך ושעה שבה התגלה האירוע:	
סטטוס הטיפול באירוע	☐ לא טופל
	☐ תחילת טיפול - לא הסתיים
	☐ הטיפול הסתיים
מיקום פיזי של האירוע	
מערכות שהושפעו מהאירוע	
האם גורמים נוספים שמחוץ לעסק הושפעו מהאירוע (אם כן פרט)?	

4. מידת הנזק / פוטנציאל הנזק (סמנו כל מה שנכון):
☐ פגיעה במערכת מחשוב המנהלת/מבקרת לול מבוקר ☐ פגיעה במערכת מחשוב תומכת בבקרת הלול הממוחשב ☐ לא ידועה מידת הנזק בשלב זה
תיאור מילולי קצר של הפגיעה:

5. אנשים שעודכנו באירוע

רשימת האנשים שעודכנו באירוע:

שם	תפקיד	טלפון

6. מה הצעדים שננקטו עד כה (מלאו כל מה שנכון)?

☐ לא ננקט שום צעד בשלב זה
☐ המערכת נותקה מרשת הבקרה של הלול
☐ נעשתה סריקה של המערכת לגילוי וירוסים
☐ הלוגים של המערכות נשמרו לצורך תחקור
☐ נעשה שחזור מגיבוי
☐ נעשתה פעולה אחרת (תארו מה נעשה)

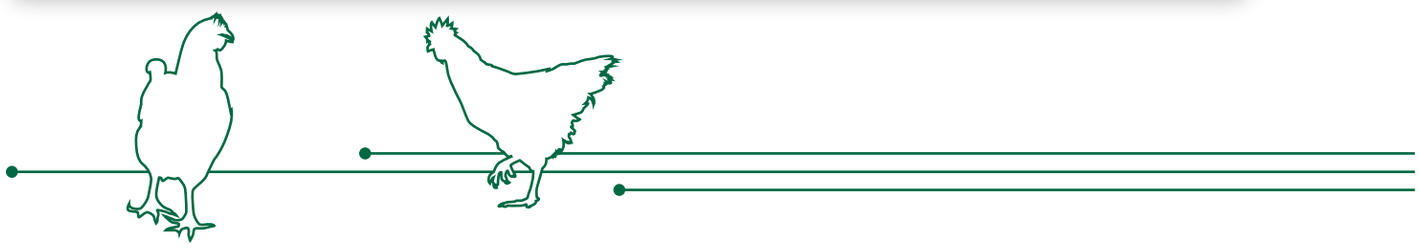
תיאור מילולי קצר של הצעדים שננקטו:

7. נתונים נוספים / מידע נוסף שלדעתכם חשוב לציין ולא נמצאים בטופס דוח אירוע

8. לקחים ומסקנות למניעת הישנות אירוע מסוג זה:

פעולות לביצוע	אחראי	לו"ז

שם מלא:	ת"ז:	חתימה:



נספח ה' - טופס הצהרת ספק המתחבר אל הלול מרחוק בדבר מחשב מעודכן ונקי מנוזקות

אני החתום/מה מטה_____, מס' זהות_____, מצהיר/ה בזה לאמור:

1. המחשב שממנו אני מבצע/ת התחברות מרחוק אל משק _____ הוא:

א. מחשב בעל מערכת הפעלה בתוקף, נתמכת ומעודכנת בכל עדכוני האבטחה באופן שוטף.

ב. מחשב המכיל אנטי-וירוס בתוקף ומעודכן בעדכונים שוטפים.

2. המחשב שממנו אני מתחבר/ת אל משק _____
נסרק ונבדק לגילוי נוזקות ונמצא נקי.

3. מטרת התחברותי מרחוק אל משק _____ היא לצרכים האלה:

_____

_____

_____

_____

_____

4. משך הזמן המוערך להתחברות הוא _____

5. בסיום ההתחברות אני מתחייב/ת להודיע לבעל המשק על סיום התחברותי ולוודא ניתוק החיבור.

חתימה וחותמת: _____

נספח ו' - מינוי ממונה הגנת סייבר

תאריך:_____

אל:_____, מס' ת"ז_____

כתובת מייל:_____ מספר טלפון:_____

הנדון: כתב מינוי ממונה הגנה בסייבר

תפקיד ממונה הגנת סייבר יכלול:

1. גיבוש מדיניות הגנת סייבר בהתאם לתהליך הטמעת בקרות ארגוני ובהתאם להנחיות במדריך הסייבר להגנה על לולים מבוקרים.
2. בניית תוכנית עבודה להגנת סייבר על פי המדיניות.
3. בקרה ומעקב אחר ביצוע תוכנית העבודה להעלאת חוסן הלול בפני תקיפת סייבר.
4. פעילות בהיבטי הגנת סייבר בהתאם למסמך ההנחיות ועדכוני האבטחה השוטפים של יחידת הסייבר בתעשייה, המשרד להגנת הסביבה.

בברכה,

_____	_____	_____
שם מלא	(תפקיד)	(חתימה וחותמת)

14. ניהול גרסאות המסמך

גרסה	כתב	אישר	מהות השינוי	תאריך
0.9	יוסי שביט ראש יחידת הסייבר בתעשייה	גלעד בן ארי ראש אגף חירום וסייבר	מסמך מקורי	29.12.2020
0.91	יוסי שביט ראש יחידת הסייבר בתעשייה	גלעד בן ארי ראש אגף חירום וסייבר	הוספת נספח ד'	26.1.2021
1.0	יוסי שביט ראש יחידת הסייבר בתעשייה	גלעד בן ארי ראש אגף חירום וסייבר	1. הוספת נספח ו' 2. תיקונים ועידכונים	12.9.2021