



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

הקדמה

החלטת ממשלה מספר 2444 : "ההגנה על תפקודו התקין והבטוח של מרחב הסייבר מהווה יעד ביטחוני לאומי חיוני ואינטרס ממלכתי חיוני לביטחונה הלאומי של מדינת ישראל , לפעול לשיפור החוסן ההגנתי בסייבר, **לבנות ולחזק את החוסן של כלל המשק בסייבר**".

בעת האחרונה אנו הולכים ומטמיעים את העובדה ששיבושים במפעלים ובארגונים כתוצאה ממתקפת סייבר, פגיעתם עלולה להיות חמורה כמו מפגיעת מלחמה, נזקי טבע וכיו"ב. אנו רואים במרחב הסייבר איום נוסף ולא פחות חמור משאר האיומים ועלינו להיערך כמיטב יכולתנו לצמצם את הסיכונים, כדי שהחקלאות ומפעליה ימשיכו לספק מזון לאוכלוסייה .

מטרת המסמך להתוות מדיניות ומסגרת תומכת המסייעת לארגונים במגזר החקלאי לניהול כלל ההיבטים הנוגעים לאבטחת המידע וההגנה בסייבר במסגרת המפעל שלהם.

מדיניות אבטחת המידע מהווה את הבסיס הארגוני לבניית תכנית העבודה השנתית, למענה ארגוני, להקצאת אמצעים ומשאבים כלכליים ולהחלטות ההנהלה תוך וויסות תהליכי קבלת ההחלטות במסגרת אחריות מוגדרת.

המדיניות המוצגת במסמך, נבנתה על מדיניות הגנת הסייבר, במערך הסייבר הלאומי ועל ההבנה כי הפעילות התקינה של הארגון מושפעת ותלויה ברמת שלמות המידע, סודיותו, אמינותו, עדכניותו, זמינותו ושרידותו.

האחריות למדיניות אבטחת המידע מוטלת בראש ובראשונה על הנהלת הארגון אשר צריכה לאשר את המדיניות אחת לשנה ולהקצות את המשאבים הנדרשים לטובת מימושה.

המסמך הוכן על ידי היחידה המגזרית עבור משרד החקלאות.

תודה מיוחדת לאבי עזר, שרון נימרובסקי, ואביב סרור על הכנת המסמך

חיים אנג'וני

מנהל אגף בכיר ניהול משברים חירום וסייבר



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

תוכן עניינים

2	הקדמה
3	תוכן עניינים
4	1. רקע
4	2. הגדרות
4	3. אחריות מנהלים
5	4. הסיכונים הכלליים העומדים בפני גופים חקלאיים
6	5. הסיכונים בניהול רשתות OT
7	6. צמצום סיכונים והגנה במערכות ICS ובקרים תעשייתיים
8	7. תקנים מוכרים בנושא ניהול אבטחת מידע
9	8. תהליך ניהול סיכונים
9	9. ניהול, בקרה ודיווח לאירועי אבטחת מידע
10	10. בקרת גישה
11	11. ניהול אירועים ודיווח
12	12. הגנת פיסיית וסביבתית
12	13. הערכת פגיעות של מתקנים קריטיים
12	14. אבטחת מידע בשרשרת האספקה



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

1. רקע

המדיניות תהיה מובלת ע"י ממונה אבטחת המידע והיא נוגעת לכלל העובדים בחברה ומחייבת אותם.

מדיניות אבטחת המידע הנשענת על תורת ההגנה של מערך הסייבר הלאומי ומתבססת על תהליך ניהול והערכה של סיכוני סייבר. במסגרת תהליך זה נדרש לזהות את יעדי ההגנה, להגדיר מה הן הבקורות הנדרשות על-מנת להגן עליהם ולבנות תכנית עבודה מתאימה.

2. הגדרות

- א. אבטחת מידע- כלל האמצעים הטכנולוגיים והארגוניים הננקטים לשמירה על מידע של חברה או ארגון מחשיפה לגורמים בלתי מורשים.
- ב. הגנת סייבר- כלל הפעולות שתכליתן להגן על נכסי הסייבר של ארגון מפני תקיפת סייבר, מתוך פרספקטיבה של הגנת הארגון ו/או התהליך ו/או המערכת, המתבססים על מערכות התקשוב שלהן.
- ג. המרחב הקיברנטי (להלן: "סייבר")- המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה.
- ד. אירוע סייבר- התרחשות אשר מעידה על פגיעה אפשרית בפעילותה התקינה של מערכת תקשוב (נכס סייבר) שקיים יסוד להניח, כי היא נובעת מפעילות מכוונת במרחב הסייבר.
- ה. הערכת סיכונים- תהליך בו קובעים את רמת הסיכון הקיימת בגורמי סיכון ואיומים שונים שאותרו, על סמך ההסתברות וחומרת הפגיעה.
- ו. מערכת מידע- תוכנה או אוסף של תוכנות המאפשרות לנהל מידע בצורה ממוחשבת.
- ז. סיכון סייבר- פוטנציאל לנזק שנובע מהתרחשות אירוע סייבר, בהתחשב ברמת סבירותו וחומרת השלכותיו.
- ח. סקר סיכונים- שיטה לזיהוי גורמי סיכון אפשריים, סיכונים קיימים, או מפגעים, להערכתם ויצירת בקורות למזעורם.
- ט. מבדק חדירה- מתקפה מתוכננת ומבוקרת על מערכת ממוחשבת שנעשית על ידי בודק במטרה למצוא חולשות אבטחה, פוטנציאל הגישה לחולשות אלו, השימושיות שניתן להפיק מהגישה אליהן ואל המידע שהן מאחסנות.

3. אחריות מנהלים

אנו רואים במנכ"ל ומנהלי המפעלים החקלאיים בשרשרת האספקה שותפים ובעלי אחריות משמעותית בתהליך ניהול סיכוני הסייבר במגזר החקלאות, במסגרת תפקידם הם נדרשים לוודא מינוי ממונה הגנת סייבר אירגוני בעל אחריות ניהולית בכל הקשור ליישום הגנת הסייבר בארגון. הנ"ל יפעל ליישום מדיניות הגנת הסייבר בארגון ויבצע פיקוח ובקרה בנושאים אלו.



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

תפקידו של ממונה אבטחת מידע והגנת סייבר דורש היכרות עם המיפוי הטכנולוגי והעסקי של החברה, שיאפשרו לו לפעול לסגירת פרצות אבטחת מידע ולצמצום סיכוני סייבר ותרמישים של אירוע סייבר דוגמת: ריגול תעשייתי, דליפת מידע, פגיעה בפרטיות לקוחות ועובדים, דליפת סודות מסחריים, וירוס כופר ועוד.

בתחום אחריותו של ממונה אבטחת המידע במפעל יושבת בקרה על מחלקת אבטחת מידע, ביצוע הדרכות, ביצוע מבדקי חדירה פנימיים, חיצוניים ואפליקטיביים, סיוע בעמידה בתקנות, התאמת מערכות ניטור ובקרה, הטעמת כלי אבטחת מידע לאיתור הדלפות, בדיקות ריגול וליפת מידע במערכות ממוחשבות וסלולר, הטמעת מדיניות ונהלי אבטחת מידע וביצוע סקרי אבטחת מידע תקופתיים. באחריות הממונה כלל הנושאים הבאים :

- 1.1. התווית אסטרטגית הגנת סייבר כוללת ואישורה בהנהלת הארגון.
- 1.2. גיבוש מדיניות הגנת הסייבר ארגונית.
- 1.3. אישור מסגרת לניהול סיכוני הסייבר ומדיניות הגנת הסייבר של הארגון.
- 1.4. דיווח על אירועי סייבר משמעותיים.
- 1.5. וידוא קיומה של וועדת היגוי להגנת הסייבר בעלת תפקידים וסמכויות מוגדרות.

למידע נוסף אודות המשך הפעילות והנהגת תורת ההגנה בסייבר ניתן לפנות לקישור –

https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations

4. הסיכונים הכלליים העומדים בפני גופים חקלאיים

תרחישי אבטחת המידע הטמונים בתחזוקת רשתות הינם יצירתיים ודורשים להיכנס לראש של תוקף באשר הוא ומטרותיו :

א. שיבוש פעילות

בדומה לעולם ה-IT, הגורמים המניעים את היריב עשויים להיות מורכבים מהרצון לייצר שיבוש או סיכול של מערכות ICS או פגיעה בתהליך נקודתי לטובת עיכוב או מניעה מטעמי תחרות, מלחמה, יריבות מדינתית ועוד.

ב. השגת רווח כספי

תוקף עלול לבצע את פעילותו במטרה לקבל תשלום עבור סיום ההתקפה, תיקון הנזק, שחרור כופרה ועוד. בשונה מעולם ה-IT, מרבית התקיפות לא יהיו במטרה להשיג מידע. נקודה זו משמעותית וחשובה שכן היא תשפיע על סוג ועוצמת הסיכונים וכן על מאמצי ההגנה אשר ננקוט במטרה להגן על נכסיו.

ג. האיום הפנימי

עובד לא מרוצה עלול לנקום על היעדר קידום, חברה מתחרה המעוניינת ביתרון, ארגון פשיעה המעוניין בהכנסה נוספת או כפי שדווח בשנים 2015-2016, יריבה מדינתית כדוגמת רוסיה אשר תקפה את אוקראינה ויצרה לראשונה הפסקת חשמל למעל 200,000 לקוחות במדינה.



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

5. הסיכונים בניהול רשתות OT

OT - Technology Operation - הינו התחום בו עולם הנכסים החיים בו הם בקרים מתוכנתים, עמדות מהנדס ותפעול, שרתי SCADA אשר למעשה משפיעים על עולמות אבטחת המידע לא פחות מרשתות IT.

אמינות מערכות SCADA בתשתית המודרנית שלנו עשויה להיות חיונית לביטחון ולבריאות הציבור במפעלים העוסקים בשרשרת ערך, הפקת מזון ועבודה עם בעלי חיים. לפיכך, התקפות על מערכות אלו עשויות להיות קריטיות.

תקיפות כאלו כבר התרחשו בעבר, לדוגמא התקיפה שבוצעה על מערכת בקרת שפכים של המועצה של מארצ'י שייר בקווינס לנד, אוסטרליה. זמן קצר לאחר שהקבלן התקין מערכת SCADA בינואר 2000, רכיבי המערכת החלו לפעול באופן לא יציב. משאבות פעלו שלא צורך ומערכות ההתרעה לא פעלו באופן תקין. שפכים הציפו פארק סמוך וזיהמו תעלת ניקוז פתוחה של מי התהום. במערכת ה-SCADA כווננו שסתומי ביוב על פתיחה כאשר הפעולה המתוכננת הייתה אמורה לשמור אותם סגורים. בתחילה זה נראה כבאג במערכת אך מעקב אחר יומני המערכת גילה כי התקלות היו תוצאה של התקפות סייבר. החוקרים דיווחו על 46 מקרים נפרדים של התערבות חיצונית זדונית לפני שהאשם זוהה. ההתקפות בוצעו על ידי עובד ממורמר לשעבר של החברה אשר התקין את מערכת SCADA, תוך תקווה שישכרו את שרותיו כדי להגן על המערכת הפגועה.

הדרכים לביצוע התקפות מסוג זה הם רבות ומגוונות:

- א. סנסור/רכיב מפעיל
 - פגיעה פיזית כמו חבלה ברכיב עצמו.
 - שיבוש או פגיעה בתעבורה כתלות בסוג התעבורה מהרכיב (רדיו, סלולאר, קווי וכדומה).
- ב. בקר
 - פגיעה פיזית כמו חבלה ברכיב עצמו.
 - שינוי הלוגיקה הצרובה בבקר.
 - פגיעה בעדכוני תוכנה הניתנים להורדה לבקר.
- ג. שרתי SCADA
 - שיבוש או פגיעה בנתונים ותהליכים תפעוליים.
 - שיבוש המידע אשר יוצג לבעלי עניין בתהליך התפעולי.
 - פגיעה בגיבוי תהליכים או במידע תפעולי.
- ד. עמדת HMI
 - גישה בלתי מורשית בשל היעדר מדיניות אבטחת מידע (סיסמאות, פרופיל משתמש וכדומה).
 - גישה למידע מסווג.
- ה. עמדת מהנדס
 - גישה בלתי מורשית בשל היעדר מדיניות אבטחת מידע (סיסמאות, פרופיל משתמש וכדומה).



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

- גישה למידע מסווג.
- הרכשה של גישות מרוחקות לעמדה (חיבורי VPN או חיבורים מרוחקים אחרים).

6. צמצום סיכונים והגנה במערכות ICS ובקרים תעשייתיים

מערכות ICS ורשתות OT בכלל, הינן מערכות מורכבות רב שכבתיות לכן דרוש לתת מענה לפערים ובקורות מפצות לתרחישי התקיפה ולהתאימן לרגולציה ולתקנים במשרד החקלאות. הסיכונים הטמונים במערכות מסוג זה הינם הגדולים ביותר והמוחשיים ביותר במגזר החקלאות. חלוקת המענה תתבצע באופן הבא:

- זיהוי – יש לבצע סקרי סיכונים מקיף בארגון במטרה למפות את הנכסים ולקבוע נהלים ומדיניות בארגון.
- הגנה – יש לממש טכנולוגיות הגנה, בקורות גישה והכשרות מתאימות.
- ניטור (Detection) – יש לממש טכנולוגיות המזהות אנומליות בתהליכים הקיימים באותה במערכות. נוסף על כך את המתואר יש ליישם לטיפול המשיך דוגמת צוותי SOC ומערכות SIEM.
- תגובה – יש לייצר תכנית להתמודדות עם אירועים ותקיפות (IR) אשר תומכות בתהליך העסקי.
- התאוששות – יש לייצר תוכניות המשכיות עסקית (DRP/BCP) לאחר אירוע או תקיפה.

את מערכות ה ICS ניתן לפרק לפי שכבה, כאשר כל אחת מאלו דורשת התייחסות והגנה רלוונטית:

שכבה 0 - סנסורים

יש לוודא הגנה פיזית על הסנסורים כדי למנוע טיפול זדוני בסנסור אשר יאפשר שליחה או קבלת מידע שגוי למערכת. כמו כן, יש לוודא כי התקשורת, בין אם קווית, אלחוטית או גלי רדיו מוגנת ככל הניתן ולא ניתן לבצע גישה לתווך.

שכבה 1 - בקרים

- יש לבצע עדכון לבקרים על פי הוראות היצרן, במידה והעדכון אינו משפיע על התהליך העסקי.
- יש לייצר בקרת גישה לבקר.
- יש להגביל את סוג הפקודות הניתנות למימוש בבקר.
- יש לנטר את התקשורת בין הבקר לבין עמדת המפעיל באופן רציף.
- עבודה עם Whitelist לתהליכים מורשים בתוך המערכת.
- יש לבצע הפרדת רשתות בין רשת הבקרה לרשתות אחרות.

שכבה 2 – RTU/LOCAL HMI



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

את שכבה זו יש לאבטח בעזרת מעגל מצלמות ולבצע בקרה פיזית לאזורים אלו. נוסף על כך, יש לוודא בקרת גישה לוגית ולממש מערך הרשאות לאמצעים אלו.

שכבה 3 – HMI/Engineering Station

- יש למנוע חיבור התקנים חיצוניים למחשבים.
 - יש לייצר בקרת גישה הכוללת סיסמה מוקשחת וביטול משתמש Admin מקומי.
 - יש לממש מדיניות שמירת לוגים לטווח זמן מוגדר אחורה.
 - יש לבטל כל תקשורת אלחוטית באם קיימת במערכות.
 - המחשב חייב להיות מנותק מרשת האינטרנט.
 - התקנת רכיב EDR אשר יוכל לנטר ולמנוע איומים.
 - במקרים של שירות תמיכה מרחוק, יש להכתיב נוהל מסודר לאופן החיבור:
 - חיבור Head-Hook.
 - הקלטת הסשן של החיבור.
 - דיווח על כל התנתקות.
 - חיבור מחשב ייעודי מוקשח אשר יועד לטובת כך בלבד.
 - קיום בקרת גישה עם Two Factor Authentication למחשב היעד.
- להרחבה ניתן לפנות למסמך:

<https://www.industry.org.il/files/cyber/%D7%A1%D7%99%D7%99%D7%91%D7%A80501.pdf>

7. תקנים מוכרים בנושא ניהול אבטחת מידע

א. תורת ההגנה בסייבר לארגונים (מערך הסייבר הלאומי)

מערך הסייבר הלאומי גיבש מסמך למען הארגונים במשק הישראלי אשר מסתמכת על תקינה בין לאומית בנושאי הגנה בסייבר. המסמך מדגיש עקרונות להגנה על המידע, מתייחס למחשוב ענן, רכש תוכנות ועוד.

את המסמך ניתן למצוא בקישור –

https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations

ב. תקן ISO

תקן ISO 27001 הינו תקן בינלאומי לניהול אבטחת מידע, אשר מתווה כללים ברורים והנחיות מפורטות ליישום מוצלח של תהליכי אבטחת המידע בארגון. תקן ISO 27001 מספק ראייה רחבה על כלל הסיכונים הקיימים בארגון על היבטיו הטכניים, הפיזיים והארגוניים.

מידע נוסף אודות התקן ניתן למצוא בקישור –



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

https://www.gov.il/BlobFolder/legalinfo/regulation/he/%D7%AA%D7%A7%D7%A0%D7%99%D7%9D%20%D7%95%D7%A8%D7%92%D7%95%D7%9C%D7%A6%D7%99%D7%94_0.pdf

ג. המלצות NIST

NIST פועל תחת המשרד למסחר והוא מאגד בתוכו מספר גופי משנה וועדות לתקינה והסדרת השימוש בטכנולוגיות ומדע. NIST שואב חלק מההנחיות והסמכויות שלו מחוק בשם 2002 Act Management Security Information Federal או בקיצור, FISMA אשר ממנה על קידום נושאי ניהול אבטחת מידע במוסדות פדראליים והגנה על מידע פדראלי רגיש.

מידע נוסף אודות התקן ניתן למצוא בקישור –

https://www.gov.il/BlobFolder/legalinfo/regulation/he/%D7%AA%D7%A7%D7%A0%D7%99%D7%9D%20%D7%95%D7%A8%D7%92%D7%95%D7%9C%D7%A6%D7%99%D7%94_0.pdf

8. תהליך ניהול סיכונים

בתהליך ניהול סיכונים יש לפעול מהבנה כי זהו תהליך מתמשך, כאשר הסיכונים משתנים באופן תדיר. הגנה מוחלטת אינה קיימת ולכל מערכת יש פגיעות וחשיפה לאיומים. מצופה מכל גוף חקלאי שיבצע ניהול סיכונים מסודר הכולל בתוכו התייחסות לכל הסיכונים האפשריים בנושא אבטחת המידע – השבתת מערכות, פגיעה בנתונים וכו'. הסיכונים הינם שונים מנקודת מבט של אבטחת מידע, להלן הקטגוריות העיקריות:

- נזק פיזי - שריפה, שיטפון, ונדליזם, מחסור בחשמל, אסונות טבע.
- שגיאת אנוש - ניצול לרעה של סמכויות עובדים לצורך עדכון/שיבוש/שינוי מידע ותהליכים עסקיים.
- תקלות חומרה - שרתים, מערכון אחסון, מערכות אבטחת מידע וציוד תקשורת.
- שימוש זדוני בנתונים - מתן גישה למידע סודי, הונאה, ריגול, גניבה.
- אובדן נתונים - השחתה במזיד או בשוגג של מידע.
- שגיאות יישום וטעויות חישוב / אספקה.

מידע נוסף ניתן לקרוא במסמך תורת ההגנה בסייבר של מערך הסייבר הלאומי.

9. ניהול, בקרה ודיווח לאירועי אבטחת מידע

מצופה כי בכל מפעל ינוהלו כלל הנושאים המפורטים מטה לפי תורת ההגנה של מערך הסייבר הלאומי בקישור הנ"ל:

https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations

רשימת הנושאים מפורטת בעמוד הבא.



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

1. הגנה מפני נזקות
2. ניהול עדכונים
3. מדיניות סיסמאות
4. בקרת חוקים ורגולציה
5. מדיניות הצפנה
6. מדיניות גיבויים
7. גיבוי ושחזור נתונים
8. מודעות
9. הגנת סייבר פרואקטיבית
10. גלישה לאינטרנט
11. הגנה באפיק המייל
12. מודעות עובדים ומשאבי אנוש
13. הכנסה והוצאה של מידע מתוך הארגון
14. עדכוני אבטחה
15. הפרדת רשתות
16. VLAN
17. Firewall
18. מעבר חד - כיווני
19. ניטור וגיבוי

10. בקרת גישה

- אנו ממליצים לכלל המפעלים והארגונים החקלאים לעבוד על פי העקרונות המנחים הבאים תוך העמקה בהמלצות הכתובות במסמכים המצורפים.
- א. הגישה לכלל מערכות המידע של מחייבת אימות של זהות מבקש הגישה. על כל המערכות לדרוש אימות מספיק (לדוג' סיסמה, Token, אישור). עבור מערכות עם רמת סיכון גבוהה או חשבונות עם הרשאות גבוהות, יש להשתמש באימות דו שלבי.
- ב. יש לשלוט על הגישה למקורות המידע של המפעלים על ידי ארגוני צד ג'. כאשר יש צורך עסקי בגישה של גורם צד שלישי, על מחלקת ה-IT של המפעל לבצע הערכת השלכות אבטחת מידע. יש להסכים ולהגדיר בקורות באמצעות חוזה עם הצד השלישי. על מחלקת ה-IT לבדוק את החוזים וההסכמים החתומים והנחתמים בהסתכלות אבטחתית.



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

- הגישה לרשת של המפעלים תהיה מוגבלת רק על פי צורך בגישה. רק משתמשים מורשים
- יורשו לגשת לרשת. הגישה תוגבל לשירותי הרשת המאושרים בלבד.
- ד. הגישה תוענק רק למשתמשים שיש להם חשבון פעיל ברשת או באמצעות ספריות משתמשים מבוקרות על ידי מחלקת ה-IT.
- ה. הגישה לאפליקציות של המפעלים תוגבל רק על פי צורך. הגישה תוגבל ליישומים המאושרים בלבד ובמידת האפשר לפונקציות ספציפיות בתוך אותם יישומים. הגישה תוענק רק למשתמשים שיש להם חשבון פעיל ברשת.
- ו. על מערכות מסדי נתונים להגביל את הגישה למשאבי המידע למשתמשים מורשים בלבד בהתאם לדרישות העסקיות. הגישה חייבת להיות מוגבלת לתצוגות ספציפיות ובמידת האפשר לפונקציות ספציפיות (קריאה, שינוי, מחיקה..).
- ז. יש לשלוט על הגישה מרחוק למשאבי המידע והרשתות של גילת באמצעות מנגנוני הגישה מרחוק של המפעל. על הגישה למשאבי המידע מרשתות ציבוריות להיות חייבים לעבור בקורות אימות והצפנה, כמו גם מעבר דרך מוצר Firewall.
- ח. כלל העובדים, הקבלנים או אנשים עם גישה מרחוק לרשתות חייבים להבטיח שהמערכת או שיטת הגישה המשמשת תואמת את דרישות האבטחה והשימוש המקובל ברשתות, במערכות ובמידע או בנתונים שאליהם ניתן להגיע.

ניתן למצוא מידע נוסף אודות הזדהות חזקה במסמך מטעם מערך הסייבר –

<https://www.gov.il/he/departments/news/mfadocs>

11. ניהול אירועים ודיווח

שמירה על יכולת אספקת השירותים והמוצרים אותם יחתור משרד החקלאות לספק לתושבי המדינה כמו גם יכולת עבודה שוטפת במערכות המידע האחרות של המשרד מתבססת (בין השאר) על השגה של ושמירה על רמה נאותה של אבטחת מידע. אחד מהמרכיבים העלולים לחבל ברמת אבטחת המידע הנן התרחשויות שונות המוגדרות כאירועים חריגים/אירועי אבטחת מידע. על כל הגורמים להם זכויות גישה למערכות טכנולוגיות המידע ולמערכות הפו"ב להכיר את הסוגים השונים של האירועים החריגים/אירועי אבטחת המידע, לדווח עליהם במועד מוקדם ככל האפשר לגורם מוסמך במשרד כפי שייקבע בנוהל זה או בהוראות רשמיות אחרות של המשרד מעת לעת, ולפעול בהתאם להנחיות שיקבלו מגורם זה על מנת לאפשר צמצום ממדי הנזק ככל הניתן. בה בעת מוטלת אחריות על גורמי אבטחת המידע במשרד להכין את עצמם לתגובה מושכלת וממוקדת עבור כל אחד מסוגי האירועים הצפויים. ישנה חשיבות מרבית להעברת מידע על אירוע חריג/אירוע אבטחת מידע גם באם המידע הקיים בידי המדווח הנו חלקי בלבד!

לקבלת מידע מפורט אודות נוהל עבודה בחירום יש לפנות למסמך נוהל עבודה בחירום של מערך הסייבר:



היחידה המגזרית של משרד החקלאות במערך הסייבר – מדיניות אבטחת מידע

<https://www.gov.il/BlobFolder/news/cybercrisispreparedness/he/Management%20of%20crisis%20situations%20final.pdf>

12. הגנת פיסית וסביבתית

ניהול מערך האבטחה בכל ארגון, קטן כגדול הינו תחום בעל חשיבות עליונה בשל הסיכונים הרבים מחוץ ומבית. כשלים במערך זה יכולים להשפיע על התנהלותו השוטפת של ארגון ואף לאיים על קיומו. בניה של פתרון אפקטיבי לאבטחה פיזית, מצריך מיפוי יסודי של כלל אתרי הארגון, סימון של נקודות התורפה והצלבת המידע עם תהליכי העבודה היומיומיים. יעוץ בטחוני אפקטיבי משלב ידע מקצועי וניסיון רב שנים בהקמת מערכי אבטחה במגוון ארגונים מובילים. בשלב הראשון של ניהול אבטחה דרוש לערוך מבדק סיכונים שנועד לזהות פערים למול האיומים והכשלים שהחברה תקלע אליהם ע"פ תרחישי הייחוס שנקבעו. אופי הנושאים נבחנים בראייה מבצעית מעשית.

לאחר זיהוי הסיכונים, יבוצע ניתוח פערים שעלו בסקר, שעיקרו בחינה של מה נדרש / מה ניתן לבצע ובעיקר מה אינו מחויב לביצוע בשל נסיבות עלות-תועלת.

חשוב לזכור כי נהלי אבטחה בלבד, כולל הנחיות ביטחון נגד טרור - אינם מספיקים ויש צורך בייעוץ מקצועי בתחום האבטחה הפיזית, בראייה כוללת ונטולת השפעות. שירותי ייעוץ ביטחוני מסויעים גם בנושאים ודרכי עבודה כמו שימור שרשרת הייצור/ אספקה, חומרי גלם, תוצרת גמורה/ מידע רגיש ועוד.

13. הערכת פגיעות של מתקנים קריטיים

על המפעלים והארגונים החקלאיים לבצע הערכת איומים ופגיעות תקופתית של המתקנים הקריטיים ומתקנים בעלי סיכון גבוה כדי לזהות איומים הפועלים על במפעל, על המתקנים ועל הנכסים. מומלץ בחום לבצע הערכות בתדירות גבוהה בהיבט ניהול הסיכון.

אנו ממליצים להפריד מתקנים קריטיים ורגישים ממתקנים מנהלתיים.

14. אבטחת מידע בשרשרת האספקה

ניהול אבטחת שרשרת האספקה הינו תחום רחב ששורשיו במספר תחומים כולל ניהול שרשרת האספקה, סחר בינלאומי, ניהול איכות, ניהול סיכונים, יבוא ויצוא, חוקים ותקנות בינלאומיות וכמובן אבטחת מידע והגנת הסייבר. השחקנים הנוטלים חלק באבטחת שרשרת האספקה גם הם רבים ומעבר למפעלי השרשרת ובעליהן של כל תחנה בדרך חשובה מעורבותם של גורמי אבטחת מידע בתהליך.

אנו ממליצים לבצע ניהול יעיל של אבטחת שרשרת האספקה, בסיוע גוף המתמחה בנושא, הכולל סקרי סיכונים בגופי הספקים, אפיון הקשר מולם, אפיון ההשפעה העסקית ועוד, שיבטיח שיפור ברמת אבטחת שרשרת האספקה תוך מינימום הפרעה להתנהלות השוטפת של העבודה.