Fahn Kanne
Grant Thornton
An instinct for growth™

המשרד להגנת הסביבה

הנחיות המשרד להגנת הסביבה

יחידת הגנה על מידע וסייבר בתעשייה

יוני 2019

רקע – חומרים מסוכנים והיתר רעלים

על פי חוק החומרים המסוכנים, לא יעסוק אדם ברעלים אלא אם כן יש בידו היתר רעלים מאת הממונה על ידי השר להגנת הסביבה. היתר הרעלים ניתן לאחר בדיקת אנשי המקצוע, כולל ביקור במפעל, בחינת הסיכונים וההערכות למניעתם, וכן קביעת דרישות ותנאים לטיפול בהם, בשגרה ובחירום. רעל הוא כל חומר מן החומרים המפורטים בתוספת השנייה לחוק, בין בצורתו הפשוטה ובין מעורב או ממוזג בחומרים אחרים.

כתנאי לחידוש היתר: מפעלים רגישים יחויבו בתוכנית הגנת סייבר
המשרד להגנת הסביבה שלח הנחיות לכ-60 מפעלים חיוניים ברחבי ישראל בדרישה להציג תוכנית הגנה מקיפה בתחום הסייבר. על המפעלים למנות מנהל בתחום הסייבר בתוך שנה, ולהשלים את צעדי התוכנית בתוך שלוש שנים.
ההנחיה תקפה ל-60 **מפעלים המסווגים ברמה A , המסוכנת ביותר, אך תורחב למפעלים מסוג B ו- C החל ב-2021.**

להלן דוגמאות לאירועים סביבתיים שעלולים להתרחש עקב אירוע סייבר

שפך תעשייה למקור מים זורם / למערכת ניקוז

אירוע חומ"ס – פליטת גזים

שפך של חומר מסוכן נוזל ללא שריפה, סיכון לזיהום קרקע ומי תהום

פיזור של חומרים מסוכנים, מוצקים ללא שריפה

שריפת חומ"ס בשלושה מצבי הצבירה

פיצוץ חומ"ס

מתקפת סייבר יכולה להתבצע באחד או יותר מהרבדים האלה

- **רובד פיזי** - גישה פיזית לרכיבי התקשוב התעשייתיים: מחשבים, נתבים, מתגים, בקרים תעשייתיים, מערות ורכיבי שטח, כגון וסתי לחץ, טמפרטורה, זרימה וכדומה

- **רובד לוגי** - גישה לוגית למערכות מידע (IT) או מערכות תהליכים (OT)

- **רובד אנושי** - משתמשים במערכות מידע ובמערכות ממוחשבות, משתמשים ברשת רצפת הייצור (מהנדסים, עובדי ייצור) וכן עובדים בשרשרת אספקה בעלי גישה לעסק, שיכולים לגרום למערכות נזק בזדון

להלן דוגמאות להתקפות סייבר

- שימוש בפגמים בתוכנה / בחומרה / בתצורת המערכת הממוחשבת או במערכת שמגינה עליה
- השתלת תוכנה זדונית במערכת ממוחשבת
- פריצת מערכת ממוחשבת דרך האינטרנט
- פריצה באמצעות שירותים של מיקור חוץ
- ניצול חולשות בשרשרת אספקה
- השבתת מערכות המחשוב של עסק

תקיפות סייבר בעולם

בשנת 2010 הייתה מתקפת סייבר במתחם הגרעין ב**איראן**. מתקפה זו גרמה לשיבוש תשתיות קריטיות על ידי שינוי של מהירות הצנטריפוגות במתחם, ועקב כך השתבש תהליך הייצור של האורניום המועשר. אין ספק כי זאת הייתה מתקפה מאורגנת מטעם מדינה אחת או כמה מדינות.

בשנת 2015 דווח על תקלות ברשת החשמל בחלק ממערב **אוקראינה** לאחר ששובשה פעולתן של 27 תחנות חלוקה ושלוש תחנות כוח. התקלה גרמה לקריסה של אספקת החשמל, ובתים רבים נותקו מהרשת. מהתחקיר שנעשה בסיוע של מדינות אירופיות, עלה שלא הייתה זאת הפסקת חשמל שגרתית, אלא תקלה שנגרמה ממתקפת סייבר.

בשנת 2018 אותרה השתלטות על משאבי מחשוב בתאגיד מים **ישראלי**. ההשתלטות נועדה לכרות מטבע ביטקוין, אך באותה מידה הפצחנים שפרצו לתאגיד, יכלו לגרום נזק לבריאות הציבור, לסביבה ולתאגיד עצמו.

בשנת 2019 מתקפת סייבר על ענקית אלומיניום גורמת לשיבושים בפעילותה באירופה ובארה"ב, נורסק הידרו הנורווגית נפלה קורבן לתוכנת כופרה חלק ממפעלי החברה הושבתו ובמתקנים אחרים עברו להפעלה ידנית בחברה מעריכים כי מקור המתקפה הוא בארה"ב, הידרו ציינה כי בכוונתה לשחזר את המערכות בעזרת נתוני גיבוי.

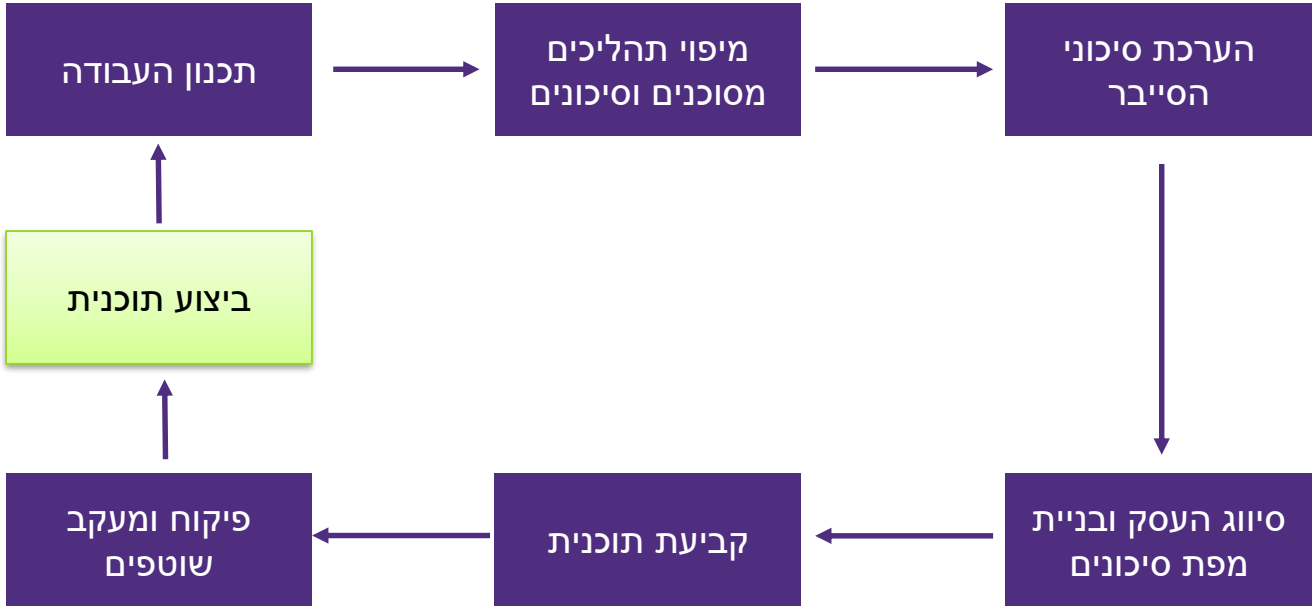
דירוג חומ"ס:

ע"פ תקנות החומרים המסוכנים (אמות מידה לקביעת תוקף היתרים), תשס"ג-2003 , סיווג הדרגות יקבע על פי:

- סוגי וכמויות רעלים,
- סוגי עסקים ופעילות
- כמות החומרים המסוכנים

רמת סיווג	A	B	C
דוגמא לסיווג	כלור גז מעל 1 טון- דרגה A בית זיקוק ותעשיה פטרוכימית- דרגה A (בכל כמות) נוזלים דליקים מעל 200 טון- דרגה A	כלור גז עד 1 טון- דרגה B נוזלים דליקים בין 30 ל- 200 טון- דרגה B	מפעל טקסטיל- דרגה C (בכל כמות) נוזלים דליקים עד 30 טון- דרגה C
תאריך להחלת ההיתר	2019-2020	החל משנת 2021	החל משנת 2021

מתודולוגיה



טיפים לדירקטור

- קיום סקר פערים ותוכנית עבודה להתגוננות מול התקפות סייבר
- וודא שתוכנית הגנה למתקפות סייבר מובאת בפני הדירקטוריון
- וודא לקבל דיווח תקופתי אודות מימוש תכנית הגנה מהתקפות סייבר
- קיום נוהל דיווח מיידי למשרד להגנת הסביבה בגין אירועי סייבר רלוונטיים
- קיום בחינה תקופתית לאפקטיביות הבקרות כנגד מתקפות סייבר

תודה על ההקשבה!

חנן טויזר
שותף, מנהל מח' ייעוץ וביקורת מערכות מידע
פאהן קנה ניהול בקרה בע"מ
Hanan.Twizer@il.gt.com

Grant Thornton
An instinct for growth™

מיפוי, הערכת סיכונים וסיווג מערכות

עם קבלת תנאים אלה ולא יאוחר מתשעה חודשים ממועד קבלתם יבחן בעל היתר הרעלים את כלל התהליכים המסוכנים בשטח המפעל, ויסווגם לתהליכים מסכני בריאות הציבור או סביבה כתוצאה מאירוע הסייבר האפשרי. להלן השלבים:

מיפוי תהליכים העוסקים בחומרים מסוכנים

↓

מיפוי מערכות ממוחשבות העוסקות בחומ"ס

↓

הערכת סיכונים

↓

סיווג המערכות

תוכנית מניעת סיכונים מאירועי חומרים מסוכנים בעת אירוע סייבר

- במידה ובעל היתר הרעלים מצא בתום תהליך הסיווג קיום תהליכים מסכנים בשטח המפעל, יכין תכנית למניעת הסיכון לבריאות הציבור ולסביבה עקב אירוע הסייבר.

- תכנית זו תכלול, לפי הצורך, הוראות שונות לרבות הוראות לעניין שינוי של תהליכי הגנה על מערכות ממוחשבות המטפלות בחומרים המסוכנים בהם עוסק העסק, אמצעי הפחתת סיכון פסיביים או אקטיביים לפי מסמך ההנחיות.

- עם סיום הכנת התכנית ולא יאוחר משניים עשר חודשים ממועד קבלת תנאים אלה יגיש בעל היתר הרעלים לממונה הודעה על סיום תהליך המיפוי והסיווג, ועל השלמת תהליך בניית תכנית למניעת סיכונים מאירועי חומרים מסוכנים בעת אירוע סייבר.

תיעוד, רישום ,שמירת מסמכים, בקרה ושיפור מתמיד

בעל היתר רעלים יאשר מסמך מדיניות הגנה על מידע וסייבר שגיבש ממונה ההגנה ויעשה רישום ושמירה של מסמכים. התיעוד והרישום יישמרו בעסק למשך תקופה שלא תפחת משש שנים מיום סיום ההטמעה והיישום של תכנית השיפור.

בעל היתר רעלים ישמור את כל המסמכים המנויים במסמך ההנחיות במשך 7 שנים, ובכל שלב, ולפי דרישת הממונה, ימסור בעל היתר הרעלים לממונה כל אחד מהמסמכים.

בעל היתר הרעלים יבצע מחדש את סקר סיכונים במערכות ממחושבות באופן מחזורי בהתאם לסעיף 16 למסמך ההנחיות.

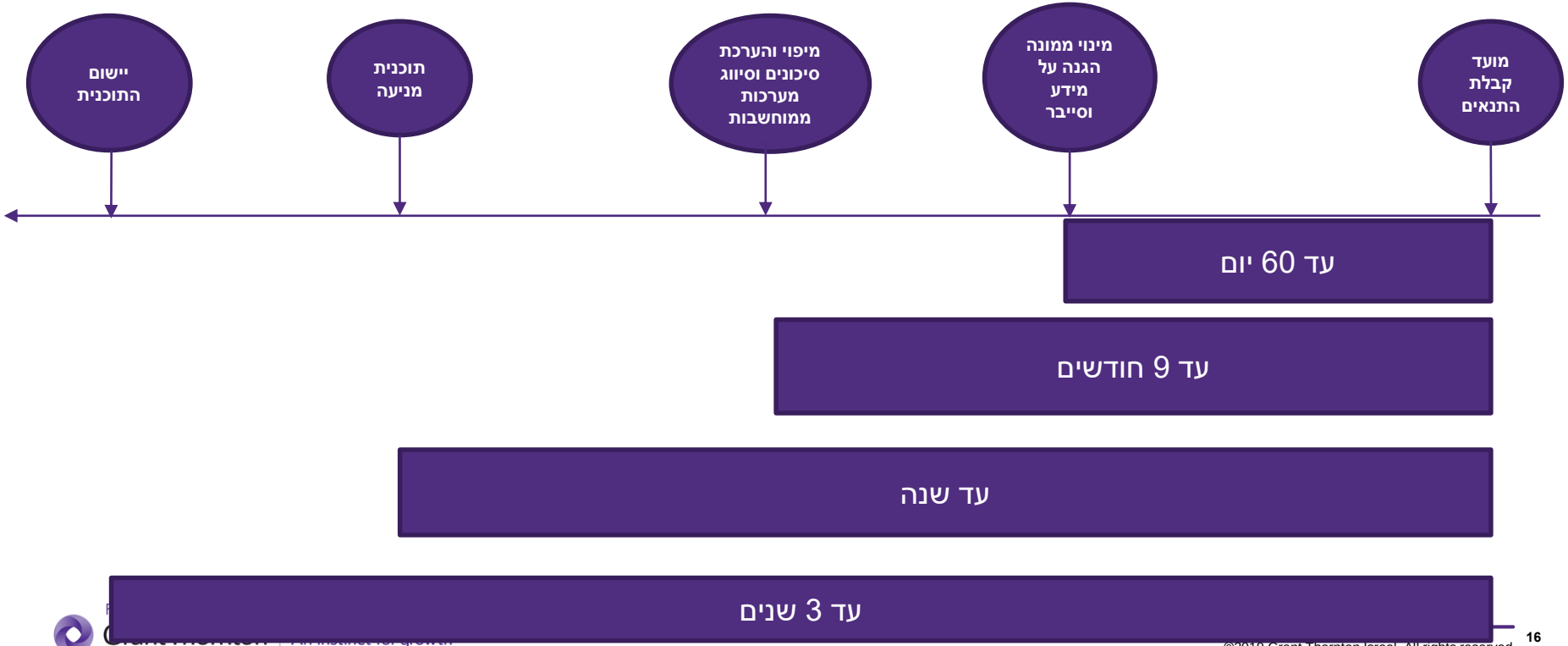
ניהול אירוע סייבר, הסקת מסקנות ודיווח למשרד להגנת הסביבה

לאחר סיום טיפול באירוע סייבר, על בעל היתר הרעלים להכין דו"ח אירוע סייבר. בנוסף, על בעל היתר הרעלים לזהות את הגורם לאירוע ולקבוע דרכי טיפול על מנת לזהות את הפרצות והליקויים אשר אפשרו את התפתחותו, במטרה למנוע הישנות מקרה דומה בעתיד ולייצר דרכי עבודה יעילות יותר.

הנדון: דוח אירוע

פירוט האירוע
שם האירוע:
תאריך האירוע:
שעת האירוע:
מיקום האירוע:
סוג האירוע:
גורם מדווח:
תקציר האירוע:
השפעת האירוע
מסקנות:
הפעולות הנדרשות לצורך הפקת לקחים:
רושם הדוח:

תנאים להיתר רעלים-ציר זמן

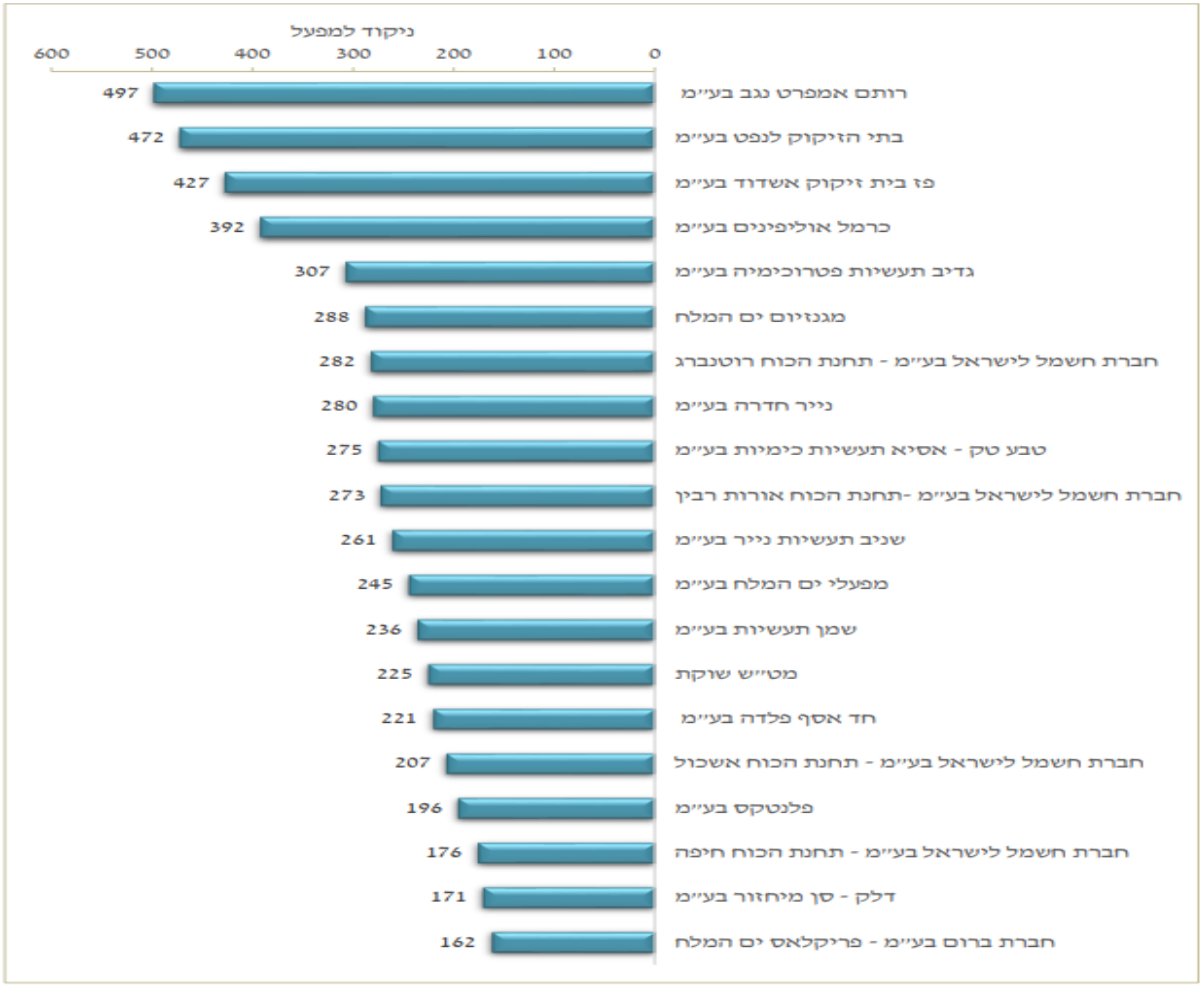


סדר העדיפויות של יישום הבקרות החסרות לעסק במסגרת תוכנית העבודה ייקבע על ידי שקלול רמת הסיכון של הנכס, עלות הפתרון ומורכבות המימוש

שלבי עבודה

1. מינוי ממונה הגנה על מידע וסייבר
2. מיפוי מערכות טכנולוגיות חיוניות למניעת תהליכים מסוכנים
3. מיפוי תהליכים מוסדרים לרבות סיווג תהליכים מסוכנים
4. הערכה של סיכוני הסייבר
5. ניהול סיכונים
6. מיפוי בקרות נדרשות
7. מיפוי פערים
8. בניית תוכנית עבודה
9. הטמעה ויישום התכנית
10. תיעוד, רישום ושמירת מסמכים
11. פיקוח ומעקב שוטפים
12. שיפור מתמיד- ביצוע סקר סיכונים באופן מחזורי
13. ניהול אירוע סייבר לרבות לעניין הדיווח
14. חירום- תוכנית היערכות לחירום בקרות אירוע סייבר

מדד ההשפעה הסביבתית - 20 המפעלים שקיבלו את הניקוד השלילי הגבוה במדד



מיפוי תהליכים מוסדרים וסיכונים: