דוח הערכת השפעות רגולציה

משרד הגנת הסביבה

הוספת תנאים להיתר רעלים בנושא הגנה על מידע וסייבר

דצמבר 2019

עורכים:

גלעד בן ארי, ראש אגף חירום וסייבר

יוסי שביט, מנהל יחידת הסייבר בתעשייה

גורם מאשר:

אוהד קרני, מנהל תחום מדיניות רגולציה

תוכן

חלק א – כללי

א. רקע

1. בשנות ה-90, החלו בעולם לצוף בעיות בהגנת סייבר במערכות תעשייתיות. אלו קיבלו משקל ותשומת לב משמעותית יותר בסוף העשור הראשון של שנות האלפיים, כאשר התברר פוטנציאל ניצול חולשות בהגנת הסייבר על ידי ארגוני טרור ופשע, על ידי מדינות עוינות, מתחרים עסקיים דרך שרשרת האספקה, או אף גורמים פנימיים בתוך העסק. בעוד שבעולם קיים מזה שנים דגש באבטחת מידע במערכות בנקאיות-פיננסיות, במגזר ממשלתי ובתחום המידע הביטחוני וכן בתחום ההגנה על פרטיות, הסקטור התעשייתי מהווה עדיין "בטן הרכה" להתקפות סייבר, כיוון שחלק לא מבוטל מהמערכות התעשייתיות הוקמו הרבה לפני שצצו איומי הסייבר הנוכחיים ובשל אופי הפעילות עלול לסכן את הציבור במקרה של התקפות סייבר.

2. חשוב להבהיר כי התקפת סייבר על מתקן תעשייתי יכולה לגרום להשבתתו ולנזק כלכלי ועל כן הגנה מפני התקפות סייבר היא אינטרס ישיר ומשמעותי של בעל המפעל לצורך הגנה על השקעותיו ועל ההמשכיות העסקית. במקרים בהם מדובר במתקן המחזיק בחומרים מסוכנים עלול להיגרם נזק סביבתי משמעותי עקיף. התקפת סייבר מכוונת על מתקן תעשייתי המחזיק בחומרים מסוכנים אשר מעורב בהם תהליך מחשובי (בפרט, בכמויות גדולות ומסוגים מסוכנים במיוחד), עלולה לגרום ליצירת אירוע חומרים מסוכנים כדוגמת פיצוץ, דליקה או שחרור של חומר רעיל. התקפה כזו יכולה להתבצע, למשל, על ידי השתלטות על הבקר האחראי על התהליך, שינוי ערכי לחץ, טמפרטורה וזרימה, כמו גם השבתת מערכות הגנה כולל השבתת מערכות גלאים, ומערכות התראה על פריצת חומ"ס. "אירוע חומרים מסוכנים משמעותי" לפי ההגדרה בדירקטיבת SEVESO עלול לגרום, לצד נזק סביבתי וכלכלי, גם פגיעה בנפש.[1]

3. במהלך שנים רבות, נושא הגנת הסייבר במערכות בקרה תעשייתיות (ICS[2]) לא קיבל התייחסות מיוחדת. מדינת ישראל החלה לטפל בנושא בתחילת שנות ה- 2000, לאחר חקיקתו של חוק הסדרת הביטחון בגופים ציבוריים, תשנ"ח–1998. החוק מתייחס בין היתר לצורך להגן על מערכות בקרה תעשייתיות במפעלים המוגדרים כמערכות ממוחשבות חיוניות. בין הגופים המנויים בתוספות לחוק מפורטים בין היתר מפעלי חברת החשמל, כי"ל, בז"ן, קצא"א, נמלים. כמות מצומצמת של כמה עשרות מפעלים מקבלים לפי החוק הנחיה בתחום הגנת הסייבר ממערך הסייבר הלאומי. זאת ועוד, אגף חירום ביטחון מידע וסייבר במשרד האנרגיה והמים, עוסק בהכוונה ובקרה של תחום האבטחה של כל מתקני התשתית הפרטיים אשר בתחום האחריות של משרד האנרגיה והמים ובכלל זה האבטחת הפיזית והחמושה, אבטחת מידע, תשתית מחשוב קריטית (תמ"ק) והרציפות התפקודית, בתאום מול מערך הסייבר הלאומי.

4. ישנם כ- 70 מפעלי חומרים מסוכנים המוסדרים כיום ברגולציה שצוינה לעיל. מתוכם, 30 מפעלים המסווגים כמפעלי SEVESO רף עליון (upper tier). ישנם 35 מפעלים נוספים בישראל בסיווג זה שאינם

---

[1] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC

[2] ICS – "מערכות בקרה תעשייתיות" - מונח כללי הכולל מספר סוגים של מערכות בקרה ושליטה בשימוש בענפי התעשייה ובתשתיות קריטיות

מוסדרים על פי חוק הסדרת הביטחון או על ידי משרד האנרגיה. 40 המפעלים הנוספים המוסדרים ברגולציה הקיימת מסווגים כמפעלי SEVESO רף תחתון (lower tier) מתוך כ- 500 מפעלים בסיווג זה בישראל. לאור זאת, כיום לא ניתן בישראל מענה שלם לסיכוני סייבר הקיימים במערכות בקרה תעשייתיות, בהן יש שימוש בחומרים מסוכנים שעלולים לגרום לאירוע חומרים מסוכנים משמעותי.

5. ייתכן אם כן שאירוע סייבר במערכות כאלה יגרום לאירוע סביבתי ואף לפגיעה משמעותית בבריאות הציבור. לאור כל זאת, ב-15 לפברואר 2015 התקבלה החלטת הממשלה מספר 2443 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (להלן – החלטת הממשלה). ההחלטה כוללת בין היתר את הקמתן של יחידות להכוונה מקצועית מגזרית בתחום הגנת הסייבר במשרדי הממשלה, שמטרתן לספק הכוונה והנחיה מקצועית בתחום הגנת הסייבר.

6. על פי החלטת הממשלה הוטל על מערך הסייבר הלאומי לסווג את הרגולטורים השונים בממשלה על פי סמכויותיהם והמגזר שבו הם פועלים ובהתאמה לקבוע את כוח האדם וגודל היחידה להכוונה מקצועית מגזרית הדרוש להם. לאור זאת ובהתאם להחלטת הממשלה, ביום 17 בספטמבר 2015, ראש מערך הסייבר הלאומי הנחה את המשרד להגנת הסביבה לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו המשרד פועל ולהקים יחידה להכוונה מקצועית מגזרית בתחום הגנת הסייבר. ברקע הדברים נזכיר כי בחודש יוני 2018 פרסם מערך הסייבר הלאומי את תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018 (להלן: תזכיר החוק). סעיף 46 לתזכיר החוק, מגדיר פגיעה משמעותית בסביבה כאינטרס חיוני לבחינה בהגנה מתקיפת סייבר. בהתאם להחלטת הממשלה, על המשרד לפעול במסגרת הסמכויות הרגולטוריות הנתונות לו להסדרת הנושא.

7. יצוין כי לעניין מפעלים אשר כפופים להנחיית מערך הסייבר או רגולטורים אחרים, ונדרשים ליישם מערך בקרות מלא וכוללני, ייתכן כי האסדרה הייעודית של המשרד בהיבטי החומרים המסוכנים לא תייצר בפועל דרישות נוספות, ולכאורה היה ניתן לראותה ככפילות בלבד. יחד עם זאת, מערך הסייבר – הן לגבי מפעלי תמ"ק והן לגבי קביעת רגולטור מוביל – לא קבע בשלב זה כי יהיה גורם אחד האחראי לכלל היבטי האסדרה בהגנת הסייבר, כולל היבט החומרים המסוכנים. על כן, לא ניתן להניח כי האסדרה תתבצע ללא תנאים ייעודיים שייקבעו על ידי המשרד. במהלך אוקטובר 2019 סוכם עם אגף תמ"ק במערך הסייבר כי יבוצע פיילוט במספר מפעלים על מנת להעריך אם ביכולתו של האגף לתת מענה שלם להיבטי החומרים המסוכנים במסגרת האסדרה המבוצעת על ידיו. בהתאם לתוצאות הפיילוט תתקבל החלטה בדבר הליכי האסדרה של המשרד.

ב. זיהוי הבעיה וסיבותיה

1. תקיפת סייבר במתקנים מסוגים שונים המוסדרים והמורשים על ידי המשרד להגנת הסביבה, עלולה לגרום לאירוע סביבתי שיביא לנזק חמור לסביבה ואף לפגיעה בחיי אדם. זאת, בפרט כאשר תקיפת הסייבר היא במתקנים העושים שימוש בחומרים מסוכנים, הטעונים היתר רעלים, לפי חוק החומרים המסוכנים, התשנ"ג-1993. למידע נוסף על היקף התקפות סייבר על מערכות תעשייתיות בעולם ועל הפגיעות של מפעלים בעולם לתקיפות סייבר ראו את ממצאי הסקירה הבין לאומית המובאת בפרק הבא.

2. בתחום מתקפות סייבר על תעשייה, קיים מידע רב המפורסם לציבור. אחד ממקורות המידע המשמעותיים בתחום הוא ניתוח שנתי שעורך מכון המחקר SANS. בדוח המכון שעניינו Securing Industrial Control Systems משנת 2017, מתואר מיפוי המצב בתעשיה בארצות הברית ובעולם בתחום ההגנה על מערכות בקרה תעשייתיות. בסקר נשאלה השאלה הבאה: "האם מערכת הבקרה שלכם נפגעה על ידי קוד זדוני או נפרצה במהלך 12 החודשים האחרונים?". לשאלה זאת התקבלו תשובות הבאות:
   - 12.1% מהנשאלים ענו "כן"
   - 18.8% מהנשאלים ענו "לא ואנחנו בטוחים שלא הייתה פריצה למערכת בקרה"
   - 40.3% מהנשאלים ענו "אנחנו לא יודעים"
   - 24.8% מהנשאלים ענו "לא ניתן לענות בשל מדיניות החברה"
   - 0.7% מהנשאלים ענו "יש לנו חשש שהותקפנו, אבל אנחנו לא בטוחים"
   - 3.4% מהנשאלים ענו "אנחנו לא יודעים, האם הותקפנו ואין לנו חשש שהותקפנו"
3. בהתאם לסקר, לארבעה מתוך כל עשרה עסקים שיש בהם מערכת בקרה תעשייתית ICS, אין כלים שמאפשרים לנטר את המערכות. מחסור זה בכלים הוא אחד מהמכשולים העיקריים שלא מאפשרים להגן באופן יעיל על מערכת בקרה תעשייתית ICS. במצב זה העסקים פועלים למעשה באופן עיוור ואינם מסוגלים לקבל החלטות מושכלות בצורה הולמת לגבי אילו בקרות יש ליישם, או כיצד לקבוע סדר עדיפויות של תכניות אבטחה והוצאות.
4. תקיפת סייבר במתקנים יכולה להביא לשינויים תהליכיים והפעלת מערכות בשונה מהאופן המתוכנן (למשל על ידי פתיחה של ברזים מרחוק). כמו כן הפגיעה יכולה לבוא לידי ביטוי בהשבתה של מערכות זיהוי אירוע סביבתי ופגיעה במערכות ההגנה הנועדות למנוע את חומרת האירועים. המשרד להגנת הסביבה ערך בחינה ראשונית בדבר מעגלי סיכון אפשריים לפגיעה בסביבה או בציבור בעקבות אירועי סייבר. מבחינה זו עולה כי סיכונים מתקיפות סייבר רלוונטיים למתקנים מסוגים שונים הכפופים לרגולציה של המשרד ואלו עלולים לגרום לנזק כמעט בכל תחום סביבתי (אוויר, קרקעות שפכים וכד'). תקיפות סייבר, כאשר מכוונות למתקנים מסויימים, עלולים לגרום לאירועים סביבתיים ואירועי חומרים מסוכנים משמעותיים.
5. הנזק הסביבתי או היקף הפגיעה עלול להשתנות בהתאם לסוג המתקן וסוג ההתקפה. יובהר כי לתפיסת המשרד, על אף מעגלי הסיכון הנרחבים, לא ניתן לייחס לכולם את אותה רמת חומרה. המפעלים בעלי פוטנציאל הסיכון הגדול ביותר הם מתקני SEVESO, כפי שהוזכר לעיל, וכן מפעלים אשר נדרשים לעמוד במדיניות ניהול סיכונים שאף היא מבוססת על הדירקטיבה. בקבוצות המפעלים האלו, הסיכון בפגיעה במתקן בעקבות אירוע סייבר הוא חמור ביותר, שכן מדובר במתקנים שאירוע חומרים מסוכנים בהם עלול להביא ליצירת אירוע סביבתי רב נפגעים או פגיעה משמעותית בסביבה. למעשה, לתפיסת המשרד, באופן גס ניתן לחלק את מעגלי הסיכון לשניים, לפי סדר חומרה יורד:

- מתקנים שתקיפת סייבר בהם עלולה להביא לאירוע סביבתי שיגרום ל**פגיעה בנפש** (לדוגמא מפעלי חומרים מסוכנים ובפרט מפעלי SEVESO ומפעלים הנדרשים לניהול סיכונים);
- מתקנים שתקיפת סייבר בהם עלולה להביא ל**אירוע סביבתי** שאינו גורם לפגיעה בנפש (לדוגמה מתקנים לטיפול בשפכים).

6. כפי שיורחב בהמשך מסמך זה, בין היתר בפרק ניתוח החלופות, המשרד להגנת הסביבה רואה את הצורך בראש ובראשונה לטפל בתחום הגנת הסייבר במפעלים מהם הסיכון לסביבה ולחיי אדם הוא הגדול ביותר.

ג. סקירה בינלאומית

1. יחידת הסייבר במשרד להגנת הסביבה ערכה סקירת ספרות בין לאומית, בנושא הגנת סייבר בתעשייה. הסקירה מובאת בהרחבה בנספח א' למסמך זה. מהסקירה ניתן ללמוד על היקף הבעיה בתחום התקפות וההגנות בתחום הסייבר על מתקני תעשייה, על הפגיעויות של מערכות וכן על הנזקים בתחום בעקבות התקפות שצלחו. מהסקירה עולה כי כי תקיפות סייבר הן דבר נפוץ בתעשייה בעולם (12% מהעסקים שנשאלו לפי אחד המקורות המובא בסקירה). עוד עולה שעסקים רבים (19%) כלל אינם בטוחים האם היו פריצות למערכת הבקרה שלהם.

2. בסקירה מוצגים מספר אירועי סייבר חשובים שהתרחשו בעולם בשנים האחרונות, כמו כן, ניתן ללמוד מהסקירה על רגולציות בעולם בתחום הגנת הסייבר. במדינות שונות בעולם קיימים גופים שונים העוסקים בהגנת הסייבר במערכות בקרה תעשייתיות, אך כיום הרגולציה עוסקת במערכות אשר מוגדרות כמערכות תשתית קריטית ואינה מסדירה מפעלים העוסקים בחומרים מסוכנים ככאלה.

3. הגישות של יישום מדיניות סייבר, עם זאת, משתנות בין מדינות, אם כי במרבית המדינות ישנו שימוש בסקר סיכונים. ישנן מדינות הנוקטות ביישום גמיש כגון בריטניה וארה"ב בהן הוגדרו רשימת בקרות כלליות וכל גוף מורשה עורך את ההתאמות הנדרשות ובוחר את הפתרונות שיתנו את המענה המתאים. רשימת בקרות היא רשימה של אמצעים טכנולוגיים, פיזיים, מינהליים וארגוניים המשמשים למיגון ואבטחה של המערכות הממוחשבות הקיימות בארגון. רשימה כזו יכולה לכלול הפרדה בין רשתות ממוחשבות מינהלתית ותפעולית, כתיבת נהלי עבודה לאבטחת מידע, יישום מוצרים טכנולוגיים לאבטחת מידע ועוד.

ד. רגולציה ורגולטורים משיקים

1. **מערך הסייבר הלאומי** - בשנת 2016 הועברה האחריות למערכות ממוחשבות חיוניות משב"כ לרשות הלאומית להגנת הסייבר (כיום מערך הסייבר הלאומי), בהתאם להחלטות הממשלה בנושא. המערך אחראי להנחייה של חלק ניכר מהמפעלים המפוקחים על המשרד במסגרת חוק החומרים המסוכנים, וכן אחראי להנחייה מקצועית של המשרד וכלל הרגולטורים בהיבטי הגנת הסייבר.

2. **משרד הביטחון** אחראי על אבטחת מידע בגופים המוגדרים בתוספת הראשונה לחוק להסדרת הביטחון בגופים ציבוריים. חלק מגופים אלה הם מפעלים המחזיקים בהיתר רעלים.

3. **משרד האנרגיה והמים** מבצע הכוונה ובקרה של תחום אבטחה של כל מתקני התשתית הפרטיים אשר בתחום אחריותו, ובכלל זה כל התחומים הקשורים לאבטחת הפיזית והחמושה, אבטחת מידע, תמ"ק והרציפות התפקודית, בתאום מול מערך הסייבר הלאומי. בשנת 2019 סוכם כי תבוצע פעילות משותפת עם משרד האנרגיה לצורך תיאום העבודה בתחום הגנת סייבר למיתקנים המפוקחים על ידי שני המשרדים.

4. **משרד הבריאות** מבצע הכוונה ובקרה של תחום אבטחת מידע במגזר הבריאות. למשרד הבריאות אין מומחיות בהגנה על מערכות בקרה תעשייתיות שיש בהן חומרים מסוכנים. בשנים 2017 ו- 2018 התקיים שיתוף פעולה מקצועי בין יחידות הסייבר של שני המשרדים, במסגרתו הציג המשרד את עמדתו המקצועית בהיבטי חומרים מסוכנים לגורמי משרד הבריאות.

5. **משרד התחבורה** מבצע הכוונה ובקרה של תחום אבטחת מידע בגופים המפוקחים על ידו. בשנת 2017 התקיימו פגישות עבודה עם משרד התחבורה. בתיאום בין המשרדים מתוכנן שיתוף פעולה מקצועי במטרה לבחון היבטי חומרים מסוכנים בגופי התחבורה.

6. **משרד הכלכלה** – על פי המידע שהוצג למשרד, משרד הכלכלה מתעתד להנחות - על בסיס וולונטרי -כ- 300 מפעלים שפעילותם מוגדרת פעילות חיונית למשק בשעת חירום, מכוח חוק שירות עבודה בשעת חירום, תשכ"ז-1967. חלק מהמפעלים כפופים לרגולציה של המשרד. יש לוודא במסגרת תיאום מקצועי את היקף החפיפה בפעילות. **רשות המים** מבצעת הכוונה ובקרה של תחום אבטחת מידע למיתקני משק המים והביוב, שחלקם מוסדרים גם בהיתרי רעלים של המשרד. מתוכנן תיאום מקצועי.

ה. פערים ביישום החלטת הממשלה

בהתאם להחלטת הממשלה מספר 2443, קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר: "במגזרים שבהם יותר ממשרד ממשלתי אחד האחראי להפעלת סמכויות רגולציה ביחס לגופים או לפעילויות, להטיל על ראש המטה לקבוע את המשרד המוביל לעניין פעילות זו." מערך הסייבר הלאומי כגוף המתכלל את הפעילות אחראי על הסדרת הנושא מול הרגולטורים השונים, אך עד כה לא קבע משרדים מובילים, כך שהמשרד נדרש להסדיר את תחום הסייבר בגופים המפוקחים על ידו גם במקרים בהם קיימים רגולטורים נוספים.

ו. מגבלות המשרד להגנת הסביבה ביישום הגנת סייבר בגופים מפוקחים

1. **העדר הקצאת משאבים מספקת** - יישום המטלות בהתאם להחלטת הממשלה כרוך בהקצאת משאבי כוח אדם ותקציב, בין היתר בשל הצורך להקצות כוח אדם ייעודי לנושא ולהכשירו כראוי. למשרד לא הוקצו תקנים למטרה זו, וכן לא ניתן תקציב מעבר לשלוש השנים הראשונות.
2. **כוח האדם העוסק בנושא במשרד מבוסס על יועצים חיצוניים בלבד, שלא ניתן להסמיכם בסמכויות הנדרשות**.

ז. מיפוי בעלי העניין

- בעלי העניין העיקריים העשויים להיות מושפעים מהרגולציה בתחום הסייבר הם **גורמי תעשייה** החשופים לסיכוני סייבר העלולים לגרום לאירועי חומרים מסוכנים. דרישות בתחום הגנת הסייבר יחולו בראש ובראשונה עליהם, לרבות ההשקעות הכרוכות בצמצום הסיכונים והטמעת בקרות שונות.
- בעלי עניין נוספים חשובים הם **הרגולטורים** אשר מופקדים על הסקטורים התעשייתיים, וקובעים להם תנאים ודרישות בתחום הגנת הסייבר בהיבטים שאינם סביבתיים.
- במידה רבה, **הציבור הרחב** הוא בעל עניין במובן זה שהמדיניות נועדה להגן עליו. עם זאת, יישום המדיניות לא צפוי להתבטא בהשפעה ישירה על הציבור.

ח. תכליות ויעדים

בהתאם להחלטת הממשלה מטרת האסדרה בתחום הסייבר היא העלאה שיטתית ורציפה של רמת ההגנה במרחב הסייבר במדינת ישראל. החלטה זו כפופה כיום גם להחלטת הממשלה מספר 2118 שעניינה הפחתת הנטל הרגולטורי. בהתאם, מטרת האסדרה המוצעת של המשרד להגנת הסביבה היא העלאה שיטתית ורציפה של רמת ההגנה במרחב הסייבר בהיבטים של הפחתה ומניעה של סיכונים סביבתיים וסיכונים לבריאות הציבור ולחיי אדם, בדגש על סיכוני הסייבר במפעלי תעשייה העלולים לגרום לאירועי חומרים מסוכנים

מטרת המשרד להטמיע את הדרישות באופן יעיל ומהיר, בעלות כספית נמוכה ככל האפשר, תוך צמצום הנטל הרגולטורי ככל שניתן.

יצוין כי מסמך זה מניח שלאחר תקופת יישום ראשונה של מספר שנים ברגולציה בתחום, יהיה צורך לשקול עדכון המדיניות נוכח התפתחויות טכנולוגיות אפשריות, ושינויים נוספים.

בהתאם להחלטת הממשלה, האסדרה תשאף להשגת היעדים הבאים:

א. האסדרה תאמץ, ככל האפשר, רעיונות, תכניות ופעילויות מוצלחות שנעשו בעולם תוך התאמתם למציאות הישראלית.

ב. האסדרה תסתמך, במידה רבה, על תקינה בינלאומית.

ג. האסדרה תקיים שותפות והתעדכנות בתהליכי פיתוח רגולציה בעולם.

ד. האסדרה תהיה מידתית.

ה. האסדרה תאפשר, במקרים מסוימים, מרחב גמישות לארגונים על מנת לממש ייעודם.

ו. האסדרה תמנף ותסתייע בגורמים הקיימים הפועלים בתחום אבטחת המידע והגנת הסייבר.

ז. האסדרה תגדיר רמות שונות של הגנה ותיצור מנגנונים להתאמה והלימה ביניהן.

ח. האסדרה תאפשר ותציע נגישות לכלים ולמתודות לשימוש ארגוני.

חלק ב – ניסוח חלופות

1. במסגרת בחינת החלופות ליישום הגנת סייבר למפעלים ואתרים הטעונים רישוי במשרד, עלו שתי סוגיות מהותיות –

- **בחירת המפעלים והאתרים אשר עליהם תחול הרגולציה** - בהתאם לאמור לעיל בעניין מעגלי הסיכון כמפורט בפרק זיהוי הבעיה וסיבותיה, המשרד להגנת הסביבה נדרש להחליט על אילו מעגלי סיכון יש להחיל את המדיניות ובאילו לוחות זמנים;
- **בחירת אופן יישום הגנות הסייבר על המפעלים והאתרים** – כפי שעלה בין היתר בסקירת הספרות שערך המשרד, ישנן גישות שונות לקביעת היקף הדרישות שיחולו על מפעלים ואתרים לצורך הגנת סייבר. החלופות העיקריות בהקשר זה הן דרישת יישום של בקרות על מפעלים באופן אחיד (אותן בקרות לכולם); דרישת בקרות באופן אחיד בהתאם לסקטורים תעשייתיים שונים; או קביעת הבקרות הנדרשות באופן פרטני בהתבסס על ממצאים של עריכת סקר סיכונים. לכל אפשרות ישנם יתרונות וחסרונות שיש לשקול. להלן יוצג בהרחבה תיאור של החלופות ולאחר מכן יובא הדיון בחלופות.

2. יש לציין כי מעבר לשתי הסוגיות המובאות לעיל, המשרד דן בכמה סוגיות נקודתיות נוספות הנוגעות לאופן יישום המדיניות, כדוגמת לוחות זמנים, שילוב עם רגולציות נוספות, ביצוע פיקוח ואכיפה וכד׳. אלו יוצגו גם כן במסגרת ניתוח החלופות.
3. יצוין כי לפי החלטת הממשלה המשרד נדרש להטמיע דרישות להגנת הסייבר בגופים המפוקחים ועל כן המשך המצב הקיים לפיו לא ניתנות דרישות אלה אינו בגדר חלופה אפשרית ולכן לא נותחה חלופה זו.

תיאור החלופות

I – רשימת מפעלים ואתרים עליהם תחול המדיניות (מעגלי סיכון)

1. חלופת ראשונה – כלל המפעלים והאתרים שבאחריות המשרד להגנת הסביבה

בהתאם להחלטת הממשלה, על המשרד להגנת הסביבה להכווין ולהנחות מקצועית בתחום הגנת הסייבר בהתאם לסמכויות הרגולציה המופעלות על ידו. המשרד להגנת הסביבה הוא רגולטור של גופים שונים שלגביהם תיתכן רלוונטיות לדרישות הגנת הסייבר ובעיקר לפי חוק החומרים המסוכנים, התשנ״ג-1993 (להלן – חוק החומרים המסוכנים). עם זאת, הרגולציה של המשרד מתייחסת גם לגופים וגורמים נוספים שעלולים לסכן את הסביבה בהתרחש התקפת סייבר, שאינם עוסקים בחומרים מסוכנים..

לפי חלופה זו, המשרד יידרש לבחון באופן פרטני את כל הרגולציות הסביבתיות הרלוונטיות ולבנות אסטרטגיה לאופן יישום הרגולציה לכלל העסקים והאתרים סביבתיים תוך איפיון רמת הסיכון על פי פרמטרים מורכבים שונים. על פניו, יש להתמקד בעסקים בהם רמת הסיכון הינה הגבוהה ביותר, וזאת בין היתר משיקולי יעילות תהליכית, כלכלית והקלת העומס הרגולטורי.

2. חלופה שנייה - גורמים מפוקחים לפי חוק החומרים המסוכנים

העוסקים בחומרים מסוכנים הם קבוצה מוגדרת מתוך סך כל הגופים המפוקחים על ידי המשרד ומתודולוגיות האסדרה החלות עליהם כוללת באופן אינהרנטי הערכת סיכון לציבור ולסביבה. בחלופה זו תחול הרגולציה על כלל העסקים הטעונים היתר רעלים של המשרד להגנת הסביבה בהתאם לחוק החומרים המסוכנים, כלומר, כ-4,200 מפעלים ואתרים. תת חלופה של חלופה זו היא החלת הדרישות לפי רמות הדירוג של העסקים הטעונים

היתר כפי שהן מוגדרות בתקנות החומרים המסוכנים (אמות מידה לקביעת תוקף היתרים), תשס"ג-2003 (דרגות A, B ו- C).

3. חלופה שלישית - מפעלים בעלי רמת סיכון גבוהה – מפעלי SEVESO

משמעות חלופה זו הינה צמצום הרגולציה למפעלי חומרים מסוכנים שזוהו במסגרת הרגולציה הקיימת של רישוי חומרים מסוכנים כמפעלים בעלי פוטנציאל הסיכון הגבוה ביותר. דהיינו, מפעלים המחזיקים בחומרים מסוכנים מהסוגים והכמויות המוגדרים בספים של דירקטיבת סווסו האירופאית ובמדיניות ניהול סיכונים של המשרד להגנת הסביבה. זאת, בראש ובראשונה לאור הסיכון האקוטי והחמור ממתקנים אלו בדגש על רצפטורים ציבוריים. המשמעות של חלופה זו היא יישום רגולציה בתחום הגנת הסייבר על רשימה סגורה של כמה מאות מפעלים.

II – אופן יישום המדיניות (בחירת בקרות)

הבקרות הנדרשות להגנת הסייבר נובעות מחיבור של מערכת ממוחשבת לטיפול בחומרים מסוכנים, שפגיעה בה עלולה לגרום לאירוע חומרים מסוכנים. מאחר שכיום כלל הגורמים העסקיים הפעילים בארץ מפעילים מערכות שיש בהן רכיבים ממוחשבים המחוברים למערכת תקשורת, הבקרות הנדרשות להגנת הסייבר ממוקדות בזיהוי נקודות התורפה לתקיפת סייבר או לתקלה, ויישום בקרות למזעור הייתכנות לאירוע והסיכונים הנובעים ממנו. יצוין כי תחום הסייבר הוא תחום דינמי ביותר מבחינה טכנולוגית ועל כן ישנו צורך לעדכן את הבקרות מדי מספר שנים, על מנת לשמור על רמת הגנה מספיקה.

1. חלופה ראשונה - בקרות אחידות

על פי חלופה זו, כל המפעלים אשר עליהם תחול המדיניות יידרשו לעמוד באותו סט של דרישות ליישום. בחלופה זו הבקרות הנדרשות ידועות מראש, כאשר לא תעשה הבחנה בין המפעלים בכל הנוגע לבקרות הנדרשות מהם. חלופה זו תואמת את גישת מערך הסייבר לעניין מפעלי תשתית מדינה קריטית (להלן 'מפעלי תמ"ק').

2. חלופה שנייה - בקרות מבוססות על סקר סיכונים

לפי חלופה זו, מפעלים אשר תחול עליהם המדיניות יידרשו לבצע סקר סיכונים אשר יעריך באופן פרטני את רמת הפגיעות לאירוע סייבר ואת רמת הנזק לסביבה ולבריאות הציבור, העלול להתרחש בעקבות אירוע סייבר. הבקרות הנדרשות מהמפעל ייקבעו בהתאם לממצאי סקר הסיכונים כאמור, באופן הבא: ייקבעו ארבעה סטים של דרישות בתחום הגנת הסייבר, ברמות אבטחה שונות בהתאם לרמת הסיכון וזאת ברוח תורת ההגנה של מערך הסייבר.

המפעלים יידרשו להעריך את הסיכון הצפוי מהם בעת אירוע סייבר באמצעות השלמת הנתונים מביצוע סקר סיכונים במסגרת הדרישה הכללית לניהול סיכונים. סקר הסיכונים כולל בחינת טווחי סיכון באירוע חומרים מסוכנים כגון פיצוץ, שריפה או שחרור חומר רעיל. ככל שהסיכון לפגיעה בבריאות הציבור או הסביבה גדול יותר, והיקף החשיפה לאירוע סייבר גדול יותר, המפעל יידרש לפעול לפי סט תנאים מקיף ומעמיק יותר. בחלופה זו יושם משקל משמעותי יותר לפגיעה בבריאות הציבור מאשר לפגיעה שהיא סביבתית בלבד.

יש להעיר כי בחלופה זו, מפעל שמיישם רמת ההגנה המירבית (חבילת בקרות מס' 4), לא נדרש לבצע סקר סיכונים בהיבט הסייבר.

חלק ג – השוואה בין חלופות ותעדוף

סיכום יתרונות וחסרונות של החלופות והשוואה ביניהן:

I – רשימת מפעלים ואתרים עליהם תחול המדיניות (מעגלי סיכון)

חלופה ראשונה – כלל המפעלים והאתרים שבאחריות המשרד להגנת הסביבה

1. החלופה הראשונה עוסקת במתן דרישות רגולטוריות לכלל העסקים העומדים תחת רגולציה של המשרד להגנת הסביבה. לפיה, המשרד יידרש לבחון באופן פרטני את כל הרגולציות הסביבתיות הרלוונטיות (כ-40 חוקים ותקנות) ולבנות אסטרטגיה לאופן יישום הרגולציה לכלל העוסקים תוך איפיון רמת הסיכון על פי פרמטרים מורכבים שונים. .

2. במסגרת חלופה זו המשרד יידרש לבחון באמצעות אילו חוקים ותקנות הוא יוכל לקבוע תנאים בתחום הגנת הסייבר (היתרים רעלים, תנאים סביבתיים ברישיון העסק, היתר פליטה, היתר הזרמה לים ועוד), ולהחיל את דרישותיו בתחום הסייבר.

3. היתרון בשיטה זו הוא שיינתן מיגון מירבי לסיכוני סייבר לכל העסקים המפוקחים תחת הרגולציה של המשרד להגנת הסביבה. החיסרון המובהק שבחלופה זו הוא קושי בתעדוף ואיפיון העסקים על פי רמת הסיכון, תוך פגיעה ביעילות הרגולציה לגבי העסקים בעלי רמות סיכון גבוהות מובהקות. בנוסף, מדובר בפוטנציאל להשתת נטל רגולטורי משמעותי על מספר גדול של עסקים פוטנציאליים ובנוסף אין אפשרות מעשית מבחינת משאבי המשרד להגנת הסביבה לתת מענה לכלל העסקים בחלופה זו.

חלופה שנייה – החלת המדיניות על כל המפעלים המחזיקים בהיתר רעלים

1. חלופה זו עוסקת ביישום המדיניות על העוסקים בחומרים מסוכנים, בכמויות ובסוגי חומרים העולים על הספים הנדרשים לפי תקנות החומרים המסוכנים (סיווג ופטור), תשנ"ו-1996 ומחזיקים בהיתרי רעלים.

2. חלופה זו כוללת גם עוסקים בחומרים מסוכנים שהסיכון הצפוי מהם לציבור ולסביבה בעת אירוע הוא קטן יחסית. מדובר בכמות גדולה של למעלה מ-4,200 עסקים. תת חלופה של חלופה זו היא מיקוד הרגולציה לפי סקטורים הקבועים בתקנות החומרים המסוכנים (אמות מידה לקביעת תוקף היתרים), תשס"ג-2003 (עסקי A ו- B). מדובר בכ- 900 עסקים בעלי מגוון רחב של פעילויות.

3. היתרון בחלופה זו הוא הסתמכות על קטגוריות סיכון קיימות אשר מעוגנות בחקיקה ועל כן משקפות רמה גבוהה יחסית של שקיפות וודאות לגבי תחולת הרגולציה. החסרון בחלופה זו הוא שאיפיון הסיכון נעשה בצורה כללית ורחבה יותר מזו המקובלת בסטנדרטים המקצועיים המקובלים כיום באירופה.

חלופה שלישית – מפעלים בעלי רמת סיכון גבוהה – מפעלי SEVESO

1. על פי חלופה זו, הרגולציה תחול על קבוצה של כ- 500 מפעלים, המחזיקים חומרים מסוכנים בכמויות ובסוגים המוגדרים בדירקטיבת סווסו האירופאית כמפעלים המסוכנים ביותר מבחינת

הפוטנציאל לאירוע חומרים מסוכנים שיש לו השפעות משמעותיות על הציבור והסביבה. מדובר במפעלים המחזיקים בהיתרי רעלים מכוח חוק החומרים המסוכנים.

2. חסרון החלופה הוא באפשרות כי מפעלים שקיים בהם סיכון משמעותי לאירוע חומרים מסוכנים שייגרם מתקיפת סייבר, ואשר עלול להביא לסיכון משמעותי לציבור ולסביבה - לא יוסדרו ויפוקחו בהיבט זה. כך למשל, מפעלים המחזיקים באמוניה אינם כלולים בחלופה זו, על אף היות האמוניה חומר גזי רעיל שעלול לסכן חיי אדם בהתרחש אירוע. יחד עם זאת, יתרונה הברור של החלופה טמון בכך שהיא מתמקדתבמפעלים מהם הסיכון לבריאות הציבור ולסביבה הוא המשמעותי ביותר. למעשה מדובר במפעלים שבעת אירוע סייבר בהם, עלול להיווצר סיכון חמור ביותר לסביבה ולבריאות הציבור, שכן במפעלים אלו מוחזקים חומרים שטווחי הסיכון מהם גדולים ביותר ועלולים להגיע למספר קילומטרים. כמו כן, מדובר באיפיון הסיכון על פי סטנדרט בינלאומי מקובל וברמת שקיפות גבוהה לעוסקים בתחום.

3. זאת ועוד, חלופה זו עולה בקנה אחד עם המדיניות הכללית לאסדרת תחום החומרים המסוכנים במשרד, כך שהיא משקפת גישה עקבית לטיוב הרגולציה והתאמתה לסטנדרטים הבינלאומיים. יצוין כי בחלופה זו תשתלב הרגולציה בהיבטי הסייבר עם היבטים של ניהול סיכונים בשגרה ובשיפור עמידות המפעלים לרעידות אדמה, באופן שיצמצם את הנטל הרגולטורי ויחסוך כפילויות בסקירת הסיכונים במפעל, ויאפשר התאמת לוחות זמנים.

II – אופן יישום המדיניות (בחירת בקרות)

1. מטרת הרגולציה היא לצמצם את הסיכון לאירועי חומרים מסוכנים משמעותיים כתוצאה מתקיפות סייבר. יש לציין, כי כלל התעשייה הישראלית חשופה למגוון סיכונים עסקיים בהיבטי הסייבר, אשר עלולים לפגוע במידע העסקי, הפרטי והמסחרי השמור בגופים אלה. עם זאת, הרגולציה של המשרד אינה עוסקת בסיכונים שאינם סביבתיים. על כן, המפעלים שיהיו כפופים לרגולציה יידרשו על ידי המשרד לקיים בקרות רק על תהליכים תעשייתיים ממוחשבים המערבים חומרים מסוכנים ובמידה שהם עלולים לסכן את הציבור והסביבה. מפעלים שיהיו מעוניינים בכך או יידרשו לכך על ידי רגולטורים אחרים, יוכלו לשלב את הבקרות הנדרשות בהיבטים הסביבתיים עם בקרות בהיבטים נוספים. לדוגמה, מפעל שרוכש מוצר אבטחת מידע כלשהו, לדוגמה אנטי-וירוס, יוכל להשתמש באותו מוצר הן לבקרות בהיבטים הנדרשים על ידי המשרד והן למטרות נוספות.

2. על כן, למרות שמערך הסייבר מצביע על 323 בקרות ביישום מכסימלי של הגנת סייבר למפעלי תמ״ק, רק כ-90 בקרות נדרשות במסגרת הרגולציה הסביבתית. עם זאת יצוין כי תחום זה הוא תחום דינמי ומתפתח בקצב מהיר הן בהיבט הסיכונים והן בהיבט הבקרות, ועל כן מספר זה ותוכן הבקרות צפויים להשתנות בעתיד, על מנת לשמור על רמת ההגנה הנדרשת. עדכון הבקרות ייעשה מעת לעת על בסיס אותם עקרונות שצוינו לעיל, על פי ההנחיה המקצועית של מערך הסייבר, ולאחר בחינת הערות הציבור בנושא.

3. להלן מובא ניתוח החלופות של אופן יישום המדיניות. חלופות אלו ניתנות ליישום עבור כל חלופה כמפורט בחלק הקודם. עם זאת, הניתוח הכלכלי בפרק זה מבוצע על פי החלופה של קבוצת

המפעלים בעלי רמת סיכון גבוהה – מפעלי SEVESO (החלופה הנבחרת כפי שיפורט וינומק בהמשך). החישוב הכלכלי מבוצע תוך הנחה כי מדובר בכ- 500 מפעלים.

1. בקרות אחידות

על פי חלופה זו, כל המפעלים והאתרים עליהם תחול המדיניות יקבלו את אותן הדרישות ליישום בקרות. היתרון בחלופה זו נובע מכך שמדובר בחלופה שהיא פשוטה וברורה ליישום. גישה זו נבחרה על ידי מערך הסייבר למפעלי תמ"ק. בחלופה זו לא יידרש ביצוע של הערכת סיכונים כלל. יחד עם זאת, חסרון חלופה זו הוא כי מפעלים יידרשו לבצע סדרת בקרות מלאה ומחמירה, מבלי להתייחס למידת הפגיעות שלהם לאירוע סייבר ולא לפוטנציאל הסיכון שלהם על הסביבה והציבור. לפי חלופה זו מפעל שאינו צפוי להיות בעל סיכון גדול ואשר נמצא רחוק מאוכלוסיה יידרש באותן השקעות כמו מפעל אשר הסיכון ממנו משמעותי ואשר נמצא סמוך לאוכלוסיה. למעשה, החסרון הבולט בחלופה זו הוא שיישומה יביא לכדי כך שיהיו מפעלים אשר יידרשו בדרישות העלולות להיות מוגזמות ביחס לסיכון הנובע מהם.

2. **בקרות מבוססות על סקר סיכונים**

בחלופה זו, ייקבעו ארבע רמות של דרישות בתחום הגנת סייבר, וברמות עלויות צפויות שונות. המפעלים יידרשו להעריך את הסיכון הצפוי מהם בעת אירוע סייבר, באמצעות ביצוע סקר סיכונים הכולל הרצה של מודלים ובחינת טווחי הסיכון כחלק מסקר ניהול הסיכונים הכולל של המפעל.ככל שהסקר יצביע על סיכון גדול יותר לסביבה ולציבור, המפעל יידרש לפעול לפי סט דרישות מקיף ומעמיק יותר.ככל שהפגיעה הצפויה בציבור קטנה יותר, סט הדרישות יהיה מופחת.

חסרון חלופה זו הוא בכך שהמפעלים יידרשו בביצוע מטלה נוספת - השלמת סקר הסיכונים בהיבטי הגנת הסייבר. על מנת להקל על המפעלים, המשרד הכין מדריך מפורט להנחיית אופן ביצוע הסקר במפעלים, ואף מקדם בשיתוף התאחדות התעשיינים ומערך הסייבר קיום הכשרה ייעודית למפעלים.

היתרון המרכזי בחלופה זו הוא התאמה מיטבית של הבקרות לרמת הסיכון מכל מתקן, ובין היתר, צמצום הנטל שיוטל על התעשייה למינימום הנדרשבנוסף, באמצעות יצירת מדרג הכולל ארבע רמות, אופן יישום המדיניות צפוי להיות ברור ופשוט באופן יחסי. יתרון נוסף של שיטה זו הוא שילוב של סקר הסיכונים הנדרש ממילא לאותם מפעלים, באופן שימנע כפילות ויאפשר ניצול מכסימלי של הממצאים שנאספו בתהליך. יצוין כי תהליך העדכון של סקר הסיכונים הכללי לנושאי חומרים מסוכנים צפוי, על פי מדיניות המשרד, מדי 7 שנים. תדירות זו אינה מספיקה על מנת לתת מענה לקצב המהיר של השינויים בתחום הגנת הסייבר, ועל כן בחלופה זו יידרש עדכון של הסקר בהיבטי הגנת הסייבר באמצע התקופה, על מנת לשמר את רמת ההגנה.

כפי שיפורט להלן, עלות ביצוע סקר סיכונים לצורך הגנת הסייבר צפוייה להיות פחותה באופן משמעותי מהעלות של יישום הבקרות ברמה המחמירה ביותר. יחד עם זאת יובהר כי מפעל הנדרש או מעוניין ליישם את רמת

3. <u>עלויות למשרד</u>

היחידה המשרדית מבוססת על העסקת כוח אדם חיצוני, באופן המגביל את אפשרויות הפיקוח והאכיפה על ידי גורמי המשרד. בהעדר כוח אדם פנימי, להלן עלויות המשרד לצורך הנחיה ובקרה:

- יחידת סייבר מגזרית המונה כ-5 אנשים: מנהל יחידה ועוד 4 אנשי סייבר. עלות ממוצעת לאיש צוות[3] 260 ₪ , עלות ממוצעת למנהל יחידה 304 ₪ לשעת עבודה .
- עלות שנתית עבור אדם אחד מבוסס על 2040 שעות בשנה: 530,400
- עלות שנתית מנהל היחידה מבוסס על 2040 שעות בשנה : 620,160
- עלות שנתית עבור כל היחידה: 2,741,720

א. החלופה הנבחרת:

החלופה הנבחרת היא לפי החלת הרגולציה על כ- 550 מפעלים באמצעות ביצוע סקר סיכונים פרטני. היתרון בחלופה זו הוא התאמה מיטבית של רמת הבקרות לרמת הסיכון, תוך צמצום הנטל שיוטל על התעשייה. באמצעות יצירת מדרג הכולל ארבע מדרגות בלבד, אופן יישום המדיניות צפוי להיות ברור וכזה שנותן ודאות בתעשייה לגבי היקף הדרישות הצפויות ממנה.

יתרון נוסף של שיטה זו הוא פוטנציאל הסינכרון וההתאמה של הרגולציה בתחום הסייבר למדיניות ניהול סיכונים של חומרים מסוכנים בכלל. לאחר תקופת היישום הראשונה, ניתן יהיה לשלב את סקר הסיכונים של הרגולציות לסקר יחיד.

אופן ותקופת היערכות

1. כפי שפורט לעיל, החלופה הנבחרת היא יישום הרגולציה בשילוב עם מדיניות ניהול הסיכונים למפעלי החומרים המסוכנים בכלל ההיבטים באופן המאפשר סינכרון בין השתיים.
2. בתקופת ההיערכות הראשונה קיים קושי יישומי בשילוב מלא של הרגולציה מאחר שמדיניות ניהול הסיכונים נמצאת בבחינה ובכל מקרה תופעל בהדרגה, כאשר בשנה הראשונה להפעלתה צפויים להכלל בה רק מפעלים בודדים. דחיית היישום עד להשלמת המדיניות הכוללת אינה מתחייבת, ועלולה להביא לעיכוב שאינו מוצדק ביישום הרגולציה דווקא בהיבטים טכנולוגיים שבהם קצב השינויים הוא מהיר.
3. יש להבהיר כי אין כוונה להחיל על כלל האוכלוסיה המונה כ- 550 מפעלים את הרגולציה באותו מועד, אלא לפרוש את קביעת הרגולציה לאורך חמש שנים. העיקרון המנחה יהיה סינכרון מיטבי ככל האפשר, כך שמפעל לא יידרש לבצע ניהול סיכונים בפרק זמן של פחות מ- 3 שנים בהיבטים שונים. בשנה הראשונה ייקבעו תנאים לכ- 20 מפעלים, ובשנים הבאות לכ-150 עד 200 מפעלים בשנה. במסגרת החלוקה יהיה תמהיל של מפעלים מהסיכון הגבוה והסיכון הנמוך.
4. נזכיר כי משך התקופה ליישום התנאים יהיה 3.5 שנים, באופן שיאפשר סינכרון טוב יותר של ניהול הסיכונים בתקופות היישום בהמשך.

[3] על פי תעריפי חשכ"ל משרת מתודולוג אבטחת מידע 6.5.ב, 6.5.ג

חלק ה – שיח עם בעלי עניין, עם מומחים ועם יחידים וקבוצות מהציבור

א. תיאור תהליך השיח מול בעלי העניין וסוגיות שעלו ממנו

1. במהלך השנים 2016-2017, במסגרת ניסוח מסמך תנאים בהיתר הרעלים לנושא העלאת החוסן כנגד תקיפות סייבר במפעלי חומרים מסוכנים, נפגשו אנשי יחידת הסייבר בתעשייה עם נציגים במשרדי הממשלה שונים על מנת להבין את תפקידם כרגולטורים ולהתייעץ עמם לגבי מדיניות פרק הרגולציה. התייעצות מקיפה ומעמיקה יותר בוצעה עם משרדים שזוהו כרלוונטיים יותר לרגולציית הגנת הסייבר, כגון משרד התשתיות הלאומיות, האנרגיה והמים, רשות המים, משרד הבריאות, משרד התחבורה, משרד הכלכלה, אגף תמ"ק במערך הסייבר הלאומי (משרד ראש הממשלה).
2. במהלך הפגישות הובחנו תהליכים בתחום הגנה על מידע וסייבר שנמצאים בתחומי אחריות של משרדי הממשלה השונים שיש בהם מעורבות רגולטורית של מספר משרדי הממשלה. בהתייעצות עם מערך הסייבר התקבלה ההחלטה, שהנחיה של המשרד להגנת הסביבה בתחום הגנת הסייבר תבוסס על תורת ההגנה לארגון של מערך הסייבר, הדבר שיאפשר לפתח שיטת עבודה אחידה בהנחיה של גופים שונים בתחום הסייבר.
3. במקביל, נפגשו אנשי היחידה עם עסקים שונים במשק שעושים שימוש בחומרים מסוכנים. לרוב, נערכו הפגישות עם אנשי המקצוע בתחומים הבאים: ייצור, בטיחות, ביטחון, הסייבר והחירום. לעיתים רבות בפגישות השתתפו מנהלים בעמדות שונות בעסק. יחידת הסייבר בתעשייה ערכה תשעה סקרי סיכונים בעסקים שונים שעוסקים בחומרים מסוכנים במגזרים שונים נציגי התאחדות התעשיינים, יחד עם נציגי יחידת הסייבר בתעשייה, השתתפו בסיורים משותפים במספר מפעלים.
4. כחלק מהתהליך, נפגשו אנשי היחידה גם עם מומחים בתחום הסייבר, מחברות ייעוץ בתחומים חומרים מסוכנים והגנת הסייבר, חברות למוצרי ושירותי סייבר וחברות לשירותי IT . הדגשים המרכזיים בפגישות אלה היו ההיבטים הייחודיים לסייבר בתעשיה מהפן הסביבתי, ומתן הסבר לגבי הרגולציה העתידית.
5. במהלך השנים 2017 – 2019 התקיימו כ- 4 כנסים בהתאחדות התעשיינים בשיתוף המשרד להגנת הסביבה בנושא הגנת סייבר בתעשייה בכנסים האלה הוצגו סיכונים הנובעים משימוש לא מאובטח במערכות בקרה תעשייתיות, עקרונות החלטת הממשלה מספר 2443, פתרונות המצעים שעומדים על הפרק במדינת ישראל ובמשרד להגנת הסביבה.
6. בסך הכל השתתפו בהליך ההיוועצות לא פחות מ-5 משרדי ממשלה ורשויות סטטוטוריות, 10 חברות ייעוץ, כ-30 חברות פרטיות במשק וגופי ההתעדה המובילים בישראל.
7. לאחר הפצת טיוטת המדריך, התאחדות התעשיינים, חברות ועסקים שונים הגישו למשרד להגנת הסביבה הערות למסמך ההוראות לעמידה בתנאים של היתר רעלים בתחום ההגנה על מידע וסייבר. כל ההערות נבדקו לעומק על ידי אנשי מקצוע והלשכה המשפטית במשרד להגנת הסביבה. בתאריך 27.12.2018 פורסם מסמך ההוראות לעמידה בתנאים של היתר רעלים בתחום ההגנה על סייבר בתעשייה פעם נוספת להערות הציבור. פירוט הערות הציבור והתייחסות אליהן מצוי בנספח.

ב. פיילוט בתעשייה

1. על מנת להבין את התועלות והשלכות רגולציה בנושא הגנת הסייבר בישראל, בהתייחס לאירועי סייבר במערכות בקרה תעשייתיות אשר עלולים לגרום לאירוע חומרים מסוכנים, יחידת סייבר בתעשייה פנתה למספר עסקים במשק בהצעה לקיים פיילוט לביצוע סקרי סיכונים וולונטריים. מטרות הפניות היו:

- להעריך את המצב הקיים במשק בנושא הגנה על מערכות בקרה ממוחשבות העוסקות בחומרים מסוכנים
- לקבל אינדיקציה לגבי רמת החוסן של מפעלים תעשייתיים לתקיפת סייבר
- תיקוף המתודולוגיה לביצוע סקר סיכונים שפותחה במשרד להגנ״ס

2. תשעה עסקים קיבלו את הצעת המשרד להגנת הסביבה והצטרפו לפיילוט, בהם עסקים קטנים, בינוניים וגדולים, שמספר העובדים בהם בין 4 ליותר מ- 1000 עובדים. שבעה מהם מחזיקים בהיתר רעלים ברמה A ונדרשים לחדש את היתר הרעלים פעם בשנה לפי תקנות החומרים המסוכנים (אמות מידה לקביעת תוקף היתרים), התשס״ג-2003, אחד ברמה B ואחד ברמה C. בכל אחד מעסקים אלה נבדקה מערכת אחת שזוהתה כמערכת הקריטית ביותר מבחינת סיכון לאירוע חומרים מסוכנים עקב תקיפת סייבר.

3. הסקרים כללו התייחסות להגנת הסייבר על מערכות בטיחות שקשורות לתהליכים שנבדקו. בכל סקרי הסיכונים נבדקה ההגנה גם במערך ה-IT של המפעל, כמו גם מערכות תומכות ברצפת הייצור כגון מערכת ניהול מחסן חומרים מסוכנים, מערכות אספקה, ומערכות ERP. מביצוע הפיילוט עלו הממצאים הבאים:

- בחמישה עסקים מתוך תשעה קיימות מערכות בקרה תעשייתיות ממוחשבות, בהן קיים פוטנציאל שאירוע סייבר עלול להביא לאירוע חומרים מסוכנים שיגרום לנזק בלתי הפיך ואפילו למוות לבני אדם ברצפטורים ציבוריים הנמצאים במרחקים הקרובים לעסקים האלה.
- בארבעה עסקים מתוך תשעה קיימות מערכות בקרה תעשייתיות ממוחשבות, בהן קיים פוטנציאל שאירוע סייבר יביא לאירוע חומרים מסוכנים שיגרום לפגיעה סביבתית קשה.
- בחלק גדול מן העסקים קיימת מודעות נמוכה מאוד בנושא הגנה על סייבר בתעשייה.
- בחלק גדול מהעסקים קיימות בעיות הגנת הסייבר בשרשרת האספקה. בחלק מהמקרים זוהתה אפשרות של השתלטות לא מבוקרת על מערכות הבקרה הממוחשבות על ידי ספקים בארץ ובחו״ל.
- בחלק מן המקרים מדובר על מערכות ישנות שקיימות במפעלים עשרות שנים. חלק מהן הותקנו ומעולם לא שודרגו כך שלא הוטמעו בהן עדכוני אבטחה.
- ברוב העסקים קיימים פתרונות שאינם מספקים מענה הולם לאיומי סייבר. יחידת הסייבר בתעשייה גיבשה המלצות לשיפור המצב הקיים במפעלים בהתאם לטיוטת המדריך שגובש במשרד. במסמך זה נלקחו בחשבון רמת הסיכון של המערכת, מורכבותה והצרכים העסקיים. יש לציין, כי הדגש ניתן על ניצול מקסימלי של יכולות האמצעים ומערכות ההגנה שכבר קיימים בעסקים, שינוי הגדרות קונפיגורציה, הפעלת מערכות הגנה לא פעילות, כתיבת נהלי עבודה ונהלי אבטחת מידע. הכל בשאיפה לתת הגנה מיטבית תוך חסכון וניצול יעיל של המשאבים הקיימים.
- בשלב מאוחר יותר, לאחר כתיבת טיוטת המדריך, יחידת הסייבר בתעשיה ואגף חומ״ס הכינו טיוטת מדריך מאוחד לניהול סיכונים וזאת על מנת לצמצם את הטיפול בנושא סקר הסיכונים.

ג. תוצרי השיח

בהמשך לשיח שנערך כאמור, הוכנו גרסאות עדכניות למסמך ההוראות לעמידה בתנאים של היתר רעלים בתחום ההגנה על סייבר בתעשייה. מסמכים אלו לקחו בחשבון את ממצאי השיח שנערך, עם בעלי העניין השונים (בפרט עם התעשייה) ואת ממצאי הפיילוט כמתואר בחלק הבא במסמך.

אחת ההערות המהותיות שעלתה עם פרסומה של המדיניות, לצד פרסום של מדיניות מקבילה בתחום ניהול סיכונים מחומרים מסוכנים בשגרה, הוא על כפל הרגולציה בתחום. לאור זאת, כיום המשרד להגנת הסביבה פועל ליצירת מדיניות אחידה לניהול סיכונים שתכלול היבטי סייבר לצד ניהול סיכונים בשגרה, הכל במדריך אחד מאוחד. וזאת על מנת להקל על הנטל הרגולטורי לתעשייה ובכדי למנוע כפילויות. כמו כן, המשרד פועל מול מערך הסייבר לצמצום כפילויות מול רגולטורים אחרים.

1. שיטת חישוב של אימפקט

בהתאם לתוצאות השיח, שונתה שיטת חישוב של אימפקט שמאפשרת למפעל לבצע את ההערכה בשיטות מוכרות של חישובי פיזור רעלים, וחישוב נזקים כתוצאה מדליקה ופיצוץ

2. שינוים בשיטת חישוב של רמת החשיפה.

נעשו שינויים בחישוב של רמת החשיפה על ידי פישוט של שאלונים. השאלון המקורי התבסס על 42 שאלות, במהלך ביצוע פיילוט סקרי סיכונים בעסקים טוייב השאלון ל- 36 שאלות.

3. שינוי בלוחות הזמנים

שונו לוחות זמנים לצורך יישום הדרישות הרגולטוריות. לוח הזמנים שונה למחזורים של 3.5 שנים על מנת להסתנכרן עם ניהול סיכונים של אגף חומרים מסוכנים במשרד.

4. הצמדות לתורת ההגנה בסייבר לארגון של מערך הסייבר

שיטת העבודה ואופן בחירת בקרות נדרשות הוצמדו לדרישות המפורטות בתורת ההגנה בסייבר לארגון של מערך הסייבר הלאומי. מתוך תורת ההגנה של מערך הסייבר נגזרו בקרות הקשורות למערכות המחשוב המחוברות לחומ״ס כך שמספר הבקרות ירד מכ-321 בקרות ל-94 בקרות.

5. שילוב פעילות ניהול סיכוני סייבר עם ניהול סיכוני חומ״ס

המשרד להגנת הסביבה יזם פעילות של שילוב סקרי הסיכונים בתחום החומ״ס והסייבר כולל איחוד של מדריכי החומ״ס והסייבר וזאת על מנת להקל על המפעלים שעליהם תחול הרגולציה.

נספח א' - סקירה בינלאומית

להלן עיקרי סקירה בינלאומית לגבי רגולציה בסייבר מבוססת על מזכר 180 "רגולציה במרחבי הסייבר" בהוצאת המכון למחקרי בטחון לאומי באוניברסיטת תל אביב –מאוגוסט 2018 מאת גבי סיבוני ועידו סיון -סבילה.

<u>גרמניה</u>

1. בגרמניה, משרד הפנים הוא הרשות המרכזית בתחום הרגולציה של הגנת הסייבר על כל רבדיה הכוללים: טכנולוגיה, מודיעין, פשיעת סייבר ותשתיות קריטיות. המשרד הפדרלי לאבטחת מידע הוקם ב- 1991 והיה אחראי מתחילת דרכו על עיצוב ומימוש הגנת הסייבר בגרמניה, תוך קידום תחומי המניעה, הגילוי והתגובה לאירועים. כיום הוא אחראי על מימוש אסטרטגיות הסייבר של גרמניה ונושא באחריות להגנת הסייבר בכל המגזרים: המדינתי, העיסקי והאזרחי.

2. בגרמניה הוקם מרכז תגובה ייעודי לאירועי סייבר מדינתיים (Cyber AZ) המשתף פעולה עם משרדי המודיעין וביטחון הפנים ועם המשטרה בגרמניה. ב-2005 הציגה המדינה את התוכנית הלאומית להגנה על תשתיות מערכות מידע, המיועדת למוסדות המדינה והן עבור התעשייה. בנוסף, הממשלה דאז יצאה בתוכנית ייעודית לשיתוף פעולה בין התעשייה ובין המדינה בכל הקשור לתשתיות קריטיות. התוכנית טיפלה בנושאים הקשורים הן להגנה פיזית והן להגנת סייבר בתשתיות אלו. בנוסף לכך, התוכנית התוותה סימולציות לניהול אירועי סייבר בתשתיות קריטיות, קידמה פעולות הכשרה והדרכה בתחום זה, פרסמה מחקרים והגדירה אלו תשתיות קריטיות אמורות לעמוד בדרישות להגנת מערכות המידע שלהן.

3. המגזרים שהוגדרו בתוכנית זו כתשתית קריטית הם: אנרגיה, תקשורת ותשתיות מידע, תחבורה, בריאות, מים, מזון, פיננסים וביטוח, תקשורת המונים, מדיה ותרבות. החזקת חומ"ס וסיכון לאירועי חומ"ס לא היוותה קריטריון להכללה בסקטורים הללו.

4. ב-2007 פרסמה הממשלה הפדרלית תוכנית ליישום ההגנה על תשתיות קריטיות בגרמניה (KRITIS). התוכנית עסקה בניהול משברים ובתגובה לאירועים, כמו גם ברציפות התפקודית של תשתיות אלו. ספציפית, התוכנית הציגה את עקרונות מערכת היחסים ושיתופי הפעולה בין הממשל ובין מפעילים פרטיים של תשתיות קריטיות וסקרה את האופן בו יש להגיב לאירועי סייבר.

5. ב-2015 חוקק חוק בטחון המידע (IT Security Act) המהווה את התשתית החוקית הנוכחית להגנת מערכות המידע של מפעילי תשתיות הסייבר בגרמניה. החוק קובע כי המפעילים הפרטיים צריכים להגן לא רק על האתרים שלהם, אלא גם על מערכות הקצה האחורי (backend). ב-2016 נכנסה לתוקפה הרגולציה של KRITIS המפרטת את הקריטריונים על פיהם מפעילים פרטיים יוגדרו ככפופים לרגולציה של תשתיות קריטיות. רגולציה

זו מאפשרת למשרד הפדרלי לאבטחת מידע להטיל קנסות על מפעילי תשתיות קריטיות שאינם עומדים בתקינה הנדרשת עד לסכום מרבי של 100,000 אירו.

6. נכון להיום אין בגרמניה אסדרה לגבי מפעלים העוסקים בחומרים מסוכנים שאינם מוגדרים כתשתית קריטית. לפי מידע שהתקבל מרגולטור המטפל במפעלי חומרים מסוכנים, באופן עקרוני החקיקה הגרמנית דורשת מהמפעיל לנקוט אמצעים לאבטחה של מיתקני החומרים המסוכנים שהם תחת הרגולציה של סווסו. עוד נמסר כי החל מסוף 2018 החלה עבודה משותפת עם רשות הסייבר הלאומית BSI במיתקני סווסו במתכונת של פיקוח משותף. כמו כן נמצאת בהכנה טיוטה של מדריך מקצועי לגבי אבטחת סייבר על ידי הנציבות לבטיחות במפעלים.

<u>בריטניה</u>

1. ב־1999 בריטניה הקימה את National Infrastructure Security Coordination Centre (NISCC) שמטרתו הייתה למזער איומים על תשתיות קריטיות ולהגן עליהן מפני מתקפות אלקטרוניות. הבריטי להקים מרכז הגנת סייבר ייעודי המאחד את NISCC ומרכז נוסף בשם National Security Advice Centre (NSAC) שהיה יחידה של סוכנות מודיעין הפנים הבריטית. מטרתו של המרכז החדש הייתה להבטיח את חסינות התשתיות הלאומיות במדינה ולהגן עליהן מפני איומי סייבר.

2. החוק הבריטי העיקרי העוסק בתשתיות קריטיות הוא ה-Civil Contingencies Act המעניק סמכות רחבה למדינה במגזרים מרכזיים כגון תקשורת, תחבורה ותשתיות מים וחשמל. סמכות זו כוללת מתן רשיונות והקפאת היתרי פעולה למגזר העסקי כאשר מתעוררים איומים על הביטחון הלאומי כתוצאה מהיעדר הגנה על תשתיות קריטיות. עם זאת הגישה הבסיסית כלפי המגזר הפרטי בבריטניה היא ברובה גישה של שיתוף פעולה וולונטרי.

3. ב־2017 הקימה בריטניה מערך ארגוני חדש להתמודדות עם אתגר הסייבר The National Cyber Security Center (NCSC) שאמור לטפל בכל המגזרים הפועלים במרחב הסייבר, תוך מתן עדיפות למגזרים לאומיים־ביטחוניים בעלי חשיבות אסטרטגית וכלכלית לבריטניה. בריטניה הגדירה 13 מגזרים כקריטיים: כימיקלים, המגזר האזרחי־גרעיני, תקשורת, ביטחון, תשתיות חירום, אנרגיה, פיננסים, מזון, שירותים ממשלתיים, בריאות, חלל, תחבורה, תשתיות מים. מטרותיו המוגדרות של המערך המוסדי החדש העוסק בהגנת סייבר הן איסוף ושיתוף מידע, פיתוח יכולות במרחב הסייבר, מתן תגובה לאירועי סייבר ותמיכה בתשתיות קריטיות.

4. במהסקירה עולה כי גם בבריטניה נכון להיום אין אסדרה רגולטורית של הגנת הסייבר במפעלי חומרים מסוכנים, אלא אם הם מוגדרים כתשתית קריטית.

<u>ארה"ב</u>

1. במסגרת רגולציה מדינתית להגנת סייבר בארצות הברית הוקם בדצמבר 2015 ערוץ סיוע בין הממשל הפדרלי ליישויות ממשלתיות, וביניהן המדינות בארצות הברית. ערוץ זה התבסס על החוק לשיתוף מידע על איומי סייבר (CISA) הנותן בין השאר למדינות השונות ממשק כמעט אוטומטי לשיתוף מידע על אירועי אבטחה ברשתות הממשלתיות. הממשל הפדרלי מסנכרן מידע זה עם מקורות מידע נוספים על מנת להזהיר את המדינות ברחבי ארצות הברית מבעוד מועד. החוק חל גם על תאגידים בשוק הפרטי האמריקאי ונותן תמריצים לשיתוף מידע.

2. בארה״ב ישנה חקיקת סייבר שונה בין מדינות שונות. יחד עם זאת, באופן כללי חוקים אלה ממוקדים בהיבטי הגנת מידע ולא בהיבטים של סיכוני חומרים מסוכנים. בסקירה שנערכה לא נמצא כי קיימת רגולציה בארה״ב העוסקת בהגנת סייבר במפעלי חומרים מסוכנים ככאלה נכון להיום.

תקנים וסטנדרטים ישראליים ובינלאומיים.

תקנים של הגנת הסייבר שפותחו בעולם מייצגים טכניקות שפותחו על ידי גורמים מקצועיים שקובעים סדר פעולות שנדרש על מנת להגן על מערכות ממוחשבות של ארגון או עסק. התקנים מתייחסים להגנה על רשתות, התקנים, תוכנות, תהליכים, מידע, יישומים, שירותים ומערכות שניתן לחבר ישירות או בעקיפין לרשתות, היבטי אבטחה בנושא מעטפת כוח אדם. המטרה העיקרית של שימוש בתקנים היא לצמצם את הסיכונים, על ידי מניעה או הפחתה של התקפות סייבר ומזעור הנזקים האפשריים. תקני אבטחת מידע כוללים אוסף של כלים שונים כולל: מדיניות, נהלים, אמצעי אבטחה, הנחיות, שיטות ניהול סיכונים, שיטות עבודה מומלצות, טכנולוגיות, הגברת מודעות וביצוע הדרכות בנושא הגנה על מידע וסייבר.

תקנים בעולם הגנה על מידע וסייבר במערכות בקרה תעשייתיות הנפוצים:

- **תורת הגנה בסייבר לארגון -** מערך הגנת הסייבר הלאומי גיבש והפיץ טיוטה להתייחסות באפריל 2017. התורה נכתבה למען הארגונים במשק הישראלי, היא אמנם נסמכת במקורותיה על תקינה בינלאומית בנושא הגנה בסייבר, אך היא מהווה גיבוש של תפיסה המושתת ברובה על ניסיון וידע ישראלי ובראיית צרכי ומאפייני הארגונים במשק הישראלי. התורה הופצה בגרסתה הראשונה 1.0 ביולי 2017. מסמך ההוראות לעמידה בתנאים של היתר רעלים בתחום ההגנה על מידע וסייבר של המשרד להגנת הסביבה מתבסס על שיטות ההגנה ועל רשימת הבקרות שנקבעו בתורת ההגנה בסייבר לארגון.

המכון הלאומי לתקנים וטכנולוגיה האמריקאי (NIST – National Institute of Standards and Technology) פיתח סדרה של סטנדרטים בעולם אבטחת מידע והגנה על סייבר ביניהם:

- **NIST Cybersecurity Framework (NIST CSF)** - מסגרת הגנת הסייבר של NIST המספקת מדיניות בסיסית פשוטה וקלה להבנה. מימוש המדיניות מאפשר לארגונים להיות פרואקטיביים בהגנת הסייבר, להיערך לאירוע סייבר בצורה יעילה תוך שימוש בניהול סיכונים, לשפר את יכולתם למנוע, לזהות ולהגיב להתקפות סייבר. תורה ההגנה בסייבר לארגון של מערך הסייבר הלאומי מבוסס על NIST CSF. לכן המסגרת הזאת מהווה בסיס גם למסמך ההוראות לעמידה בתנאים של היתר רעלים בתחום ההגנה על מידע וסייבר של המשרד להגנת הסביבה.
- NIST Special Publication 800-53 - עוסק בבקרות הגנה על מידע ופרטיות בארגונים ומערכות מידע,
- NIST Special Publication 800-30 - עוסק בניהול סיכונים
- NIST Special Publication 800-82R2 ו -עוסק בהגנה על מערכות אוטומציה ובקרה תעשייתיות.

- **מכון התקנים הישראלי** אימץ חלק ממשפחת תקני 27000 של ארגון ISO (International Standardization for Organization) ארגון התקינה הבינ״ל ו- IEC (Commission technical-)

(Electro International הנציבות הבינלאומית לאלקטרו-טכניקה, ארגון תקינה בתחום החשמל והאלקטרוניקה.

- **תקן -IEC 62443** - תקן זה מביא הערכה נוכחית של כלים שונים באבטחת סייבר, של אמצעי להפחתה (mitigation) של האיום ושל טכנולוגיות שניתן להחיל אותן ביעילות על מערכות מודרניות אלקטרוניות המבוססות על מערכות אוטומציה ובקרה תעשייתיות (IACS) שמווסתות ומנטרות תעשיות ותשתיות קריטיות רבות. התקן מתאר מספר קטגוריות של טכנולוגיות אבטחת סייבר ממוקדות- מערכות בקרה, את סוגי המוצרים הזמינים בקטגוריות אלה, את היתרונות והחסרונות של השימוש במוצרים אלה בסביבות מערכות אוטומציה ובקרה תעשייתיות אוטומטיות, בכל הנוגע לאיומים הצפויים ולפגיעויות הסייבר הידועות, והחשוב מכול, את ההמלצות ואת ההנחיות הראשוניות לשימוש במוצרים אלה של טכנולוגיית אבטחת סייבר. המושג של אבטחת סייבר למערכות אוטומציה ובקרה תעשייתיות (IACS) כפי שחל בתקן זה הוא במובן הרחב ביותר, שמקיף את כל סוגי הרכיבים, המפעלים, מתקנים והמערכות בתעשיות ובתשתיות הקריטיות. מערכות אוטומציה ובקרה תעשייתיות כוללות, בין היתר הולכת חשמל וחלוקתו, רשתות חלוקת גז ומים, תפעול הפקת נפט וגז וצנרת להולכת גז ונוזלים.
- משפחת התקנים ISO 27000 העוסקת בניהול אבטחת המידע בארגון ומהווים מסגרת לבנית תכנית הגנה ושיטות עבודה מומלצות להגנה על המידע, קיימים לפחות 45 תקנים בתתי-תחומים תחת נושא זה. התקנים ברובם בתשלום. תקנים מובילים במשפחה הינם :

- ISO 27001 - המגדיר את עקרונות הקמת ניהול ותחזוקה של מערכת אבטחת מידע המתאימה לארגון
- ISO 27002 - מתכונת מומלצת למילוי דרישות תקן ISO 27001.
- ISO 27010 - טכנולוגיית המידע – טכניקות אבטחה – ניהול אבטחת מידע לתקשורת בין-מגזרית ולתקשורת בין-ארגונית
- ISO 27014 - טכנולוגיית המידע – טכניקות אבטחה – ניהול אבטחת מידע
- ISO 27032 - טכנולוגיית המידע – טכניקות אבטחה – קווים מנחים לאבטחת סייבר