**1,000 מפעלים יידרשו ליישם דרישות סייבר להיתר רעלים**

דרישות סייבר להיתר רעלים יורחבו מ-200 מפעלי סווסו ל- 1,000 מפעלים בעלי היתר רעלים בסיווג רמת סיכון גבוהה ובינונית. דרישה לביצוע סקר סיכונים שבהתאם לתוצאותיו יש להטמיע הגנות ובקרות סייבר בעלות שיכולה להגיע ליותר ממיליון ₪

בימים האחרונים פורסמה טיוטה של עדכון גרסה להוראות לעמידה בתנאים של היתר רעלים בתחום ההגנה על סייבר בתעשייה. מדובר בגרסה 2.0 של [מדריך שפורסם בתחילת שנת 2020](https://infospot.co.il/n/Cyber_Guide_Guidelines_businesses_with_permit_toxins) ועתיד להחליפו לאחר סבב הערות הציבור.

השינוי העיקרי הוא דרישה חדשה מכ- 1,000 מפעלים העוסקים בחומרים מסוכנים ובעלי היתר רעלים בסיווג רמת סיכון A (סיכון גדול) ו-B (סיכון בינוני) לבצע סקר סיכונים בהיבט של הגנת סייבר.

ככל שהסקר יצביע על סיכון גדול יותר לסביבה ולציבור, המפעל יידרש ליישם דרישות מקיפות ומעמיקות יותר כמתואר במדריך. עלות היישום יכולה להגיע ליותר ממיליון ₪. ענף משנעי החומ"ס יטופל בנפרד מהמדריך החדש.

נכון להיום התנאים להיתר רעלים להגנת סייבר מיושמים בצורה מדורגת על כ- 200 מפעלי סווסו SEVESO – קבוצת מפעלים שעוסקים בחומ"ס בעלי הסיכון הרב ביותר על פי דירקטיבת סווסו האירופאית. עד כה כ- 70 מפעלי סווסו נדרשו לנושא. מפעלי סווסו הם בפועל תת-קבוצה מבין המפעלים ברמת סיכון A לפי הסיווג של חוק חומ"ס.

כלומר, כעת רוצים להרחיב את דרישות הסייבר להיתר רעלים מכ- 200 מפעלי סווסו, ל- 1,000 המפעלים בעלי היתר רעלים ברמת סיכון A ו- B.

*טיוטת ההנחיות החדשה מפורסמת להערות הציבור עד לתאריך 31.12.2021.*

**

**כתבות רלוונטיות:**

1. [עדכונים בתנאים הנוספים להיתר רעלים: סיכוני סייבר](https://infospot.co.il/n/Poison_permit), 15/09/2020
2. [עדכון מדריך הגנת סייבר לעמידה בתנאי היתר רעלים](https://infospot.co.il/n/Cyber_defense_hazmat), 11/08/2020
3. [מדריך סייבר הנחיות לעסקים בעלי היתר רעלים](https://infospot.co.il/n/Cyber_Guide_Guidelines_businesses_with_permit_toxins), 15/1/2020
4. [טיוטה מעודכנת של הוראות לבעלי היתר רעלים להגנת סייבר](https://infospot.co.il/n/An_updated_draft_of_a_toxicology_permit_for_protection_from_cyber_attack), 01/1/2019
5. [מענק ממשלתי בהיקף 10 מיליון ₪ להגנה ממתקפות סייבר](https://infospot.co.il/n/NIS_10_million_in_assistance_to_protect_against_cyber_attacks), 17/9/2018
6. למידע נוסף על [היתר רעלים](https://infospot.co.il/scp/%D7%94%D7%99%D7%AA%D7%A8_%D7%A8%D7%A2%D7%9C%D7%99%D7%9D) | infospot

**רקע: התגברות איומי סייבר**

על רקע התעצמות פגיעות הסייבר ברחבי העולם, המשרד להגנת הסביבה גיבש הוראות להגנת סייבר למפעלים העוסקים בחומרים מסוכנים, במטרה לצמצום ולמנוע מתקפת סייבר שתגרום לאירוע חומ"ס.

כבר בשנת 2017 [המשרד להגנ"ס הודיע על כוונתו לגבש תנאים להיתר רעלים להגנת סייבר](https://infospot.co.il/n/Plants_with_poison_permits_are_required_to_protect_against_cyber_attacks) וטיוטות ראשונות אכן פורסמו להערות ציבור בשנים 2018-2019. כאשר במקביל החל פיילוט ליישום התנאים על 9 מפעלים. [בשנת 2020 פורסמה גרסה סופית של המדריך להגנת סייבר](https://infospot.co.il/n/Cyber_Guide_Guidelines_businesses_with_permit_toxins) והמשרד להגנ"ס החל לדרוש ממפעלים המוגדרים בעלי רמת סיכון גבוהה לפי דירקטיבת סווסו האירופאית (SEVESO), ליישם את דרישות הגנת הסייבר.

לפי הנתונים שהמשרד פרסם, נכון ללפני חודשיים, כ- 70 מפעלים מוסדרים בתנאי הגנת הסייבר להיתר רעלים, כולם מפעלי סווסו, כמחציתם סווסו עליון והיתר סווסו תחתון (חלוקה לפי רמת סיכון).

**החלופות: להחיל את המדיניות על כולם או לפי רמת סיכון**

כאשר המשרד להגנת הסביבה בחן על מי להחיל את ההוראות להגנת סייבר, עלו לדיון 3 חלופות:

1. **המשך הסדרת מפעלי SEVSO בלבד:** כיום דרישות הסייבר מיושמות (באופן מדורג) רק על 200 מתקני SEVESO המחזיקים חומרים מסוכנים בכמויות ובסוגים המוגדרים בדירקטיבת סבסו האירופאית. מדובר במפעלים המסוכנים ביותר מבחינת הפוטנציאל לאירוע חומרים מסוכנים שיש לו השפעות משמעותיות על הציבור והסביבה. בפועל, הם מהווים חלק מהמפעלים בסיווג רמת סיכון גבוהה A לפי היתר הרעלים.
2. **הסדרת כל הגורמים שחייבים בהיתר רעלים:**לפי הצעה זו, הרגולציה תוטל על כ-4,200 מפעלים ואתרים בעלי היתר רעלים בכל רמות הסיכון, כולל יותר מ- 3,000 בסיכון נמוך C.
3. **הסדרת מפעלים בעלי היתר רעלים ברמת סיכון A ו-B בלבד:**להרחיב לכ 1,000 מפעלים בסיווג רמת סיכון גבוהה A (בהם 200 מפעלי SEVESO) ורמת סיכון בינונית B.

בסוף, החלופה שנבחרה היא האחרונה: החלת הרגולציה רק על מפעלי A ו-B (וכן מפעלי סבסו).

**כיצד תיושם המדיניות החדשה בעניין הגנת סייבר?**

שאלה נוספת שהתקיים סביבה דיון היא כיצד ליישם את הרגולציה על קבוצת המפעלים החדשה? בכל מקרה יישומה יתבטא בכך שהמפעלים יידרשו לערוך בקרה למזעור ההיתכנות של אירוע חומ"ס שנובע מפרצת אבטחה טכנולוגית ובזיהוי נקודות תורפה במערכות הממוחשבות של הארגון. אך גם לביצוע בקרות יש רמות שונות והועלו גם כאן לדיון 3 אפשרויות:

* **בקרות אחידות:** כל המפעלים אשר עליהם תחול המדיניות יידרשו לעמוד באותו סט של דרישות ליישום.
* **בקרות מבוססות על סקר סיכונים:**זו האפשרות שנבחרה. מפעלים אשר תחול עליהם המדיניות יידרשו לבצע סקר סיכונים שיעריך פרטנית את רמת הפגיעות שלהם לאירוע סייבר ואת תוצאותיו. הבקרות הנדרשות מהמפעל ייקבעו בהתאם לממצאי סקר הסיכונים. כך תיבחר הבקרה הנדרשת מתוך 4 אפשרויות אבטחת סייבר – מהמחמירה והיקרה ביותר (בקרה 4) למקלה ולזולה ביותר (בקרה 1). כמו כן, יינתן משקל משמעותי יותר לסיכון לפגיעה בבריאות הציבור מאשר לפגיעה שהיא סביבתית בלבד.
* **הגדרת דרישות ברמה סקטוריאלית:**לפי הצעה זו, המפעלים יחולקו לסקטורים שונים בעלי מאפיינים דומים וכל סקטור יקבל דרישות הגנת סייבר אחידות המתאימות לו ללא צורך בסקר סיכונים פרטני.

כאמור, החלופה שנבחרה היא שרמת הבקרות שהמפעל יידרש להן תהיה בהתאם לרמת הסיכון הפרטנית שלו, כפי שיעלה מסקר סיכונים. היתרון בחלופה זו הוא  התאמה של רמת הבקרות לרמת הסיכון, תוך צמצום הנטל שיוטל על התעשייה. באמצעות יצירת מדרג הכולל 4 מדרגות, אופן יישום המדיניות צפוי להיות ברור וכזה שנותן ודאות בתעשייה לגבי היקף הדרישות הצפויות ממנה.

יצוין כי תהליך העדכון של סקר הסיכונים הכללי לנושאי חומרים מסוכנים צפוי מדי 7 שנים לפי המדיניות של המשרד להגנ"ס. אך מאחר שתדירות זו אינה מספיקה כדי לתת מענה לקצב המהיר של השינויים בתחום הגנת הסייבר, יידרש עדכון של הסקר בהיבטי הגנת הסייבר כל 3.5 שנים.

כדי להקל על המפעלים בביצוע המשימה החדשה של התייחסות לסייבר בסקר הסיכונים, המשרד להגנ"ס הכין מדריך מפורט לאופן ביצוע הסקר בתחום הסייבר. כמו כן, הוא מקדם הכשרה ייעודית למפעלים בנושא.

**כמה יעלה למפעלים ליישם את המדיניות?**

עלות הטמעת המדיניות צפויה להשתנות ממפעל למפעל, בהתאם לרמת הבקרה (האבטחה) שיידרש לה והמצב של הגנת הסייבר במפעל כיום. נתוני הפיילוט שהתקיים על 9 מפעלים מלמד על סדר הגודל של העלויות:

* מפעל/מתקן אמוניה בגודל בינוני במצב מוכנות גבוהה, שילם כ- 20,000 ₪ באופן חד פעמי ו-18 אלף ₪ מדי שנה עבור מערכת מסוימת.
* מפעל ייצור חומר מסוכן בגודל בינוני במצב מוכנות לא טובה שילם 800 אלף ₪ עבור הטמעת הגנות סייבר של כוח אדם ורישיונות.
* מתקן התפלה שמפעיל מתקן תוספת חומ"ס למי שתייה (כלור) שילם עלות שנתית של 20 אלף ₪ ל-3 שנים.
* מתקן רפואי לעיקור ציוד רפואי לא נדרש להטמעה נוספת מאחר שכבר קיימת מערכת עיקור סגורה שלא חשופה לפגיעות סייבר. במקרה זה לא תהיה עלות לבית החולים או הארגון המפעיל את המתקן.
* מפעל בינוני ברמת מוכנות נמוכה בענף הציוד לתעשיית המזון שילם 14 אלף ₪ כדי לעמוד בדרישות.
* מפעל ייצור חומרים מסוכנים בגודל בינוני ברמת מוכנות נמוכה שילם כ- 530 אלף $.

חישוב העלויות הנ"ל לא לוקח בחשבון זמן ניהול ועלויות כוח אדם פנימי במפעל שעוסקים בנושא.

**שינויים נוספים בשיטות חישוב הסיכון**

בנוסף לכל המתואר לעיל, נעשו מספר שינויים נוספים:

* שונתה שיטת חישוב של אימפקט שמאפשרת למפעל לבצע את ההערכה בשיטות מוכרות של חישובי פיזור רעלים, וחישוב נזקים כתוצאה מדליקה ופיצוץ.
* נעשו שינויים בחישוב של רמת החשיפה על ידי פישוט של שאלונים. (36 שאלות במקום 42).
* 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-324 בקרות ל-92 בקרות.