

# קורס סייבר לתעשייה



# מטרות הקורס

- ✓ הקניית ידע בנושאי סייבר עם דגש על סייבר בתעשייה, בדגש נוסף על תעשיית החומרים המסוכנים
- ✓ תמיכה בדרישות הרגולציה בסייבר במפעלי חומרים מסוכנים המקבלים היתר רעלים מהמשרד להגנ"ס
- ✓ חשיפת אוכלוסיות נוספות במפעל (מעבר לאנשי IT, CISO) לאיומי הסייבר וסקירת פתרונות הגנה שונים
- ✓ מעבר והסבר על מדריך הסייבר של המשרד להגנת הסביבה גירסא 1.3
- ✓ חשיפת משתתפי הקורס לחברות סייבר שיכולות לסייע בפעילות





המשרד להגנת הסביבה



המשרד להגנת הסביבה



המשרד להגנת הסביבה



الوزارة لحماية البيئة  
Israel Ministry of the Environmental Protection

מדינת ישראל  
המשרד להגנת הסביבה

**יוסי שביט (MBA, CISM)**

ראש יחידת הסייבר בתעשייה

טל': 074-7675850  
נייד: 058-6662242  
E-mail: yosish@sviva.gov.il

רח' בנק ישראל 7, גנרי 2  
ירושלים 9195021  
www.sviva.gov.il

# קצת על עצמי

יוסי שביט – נשוי +3 מתגורר בהר אדר

## השכלה:

- מהנדס מכונות Bsc. הטכניון חיפה
- תואר שני MBA מינהל עסקים או"פ
- תואר CISM מטעם ארגון ISACA העולמי

## נסיון מקצועי מעל 25 שנה בתחומי הסייבר:

- עבודת HANDS ON ברכיבי אבטחת מידע וסייבר
- כתיבת מתודולוגיות
- מרצה באקדמיה
- נסיון תעשייתי – סייבר במערכות ICS



# נושאי הלימוד בקורס

- 1 מפגש : מבוא כללי + מבוא לחומרים מסוכנים
- 1 מפגש 2: מושגי יסוד בהגנת סייבר – חלק 1
- 2 מפגש 3: מושגי יסוד בהגנת סייבר – חלק 2
- 3 מפגש 4: מושגי יסוד בהגנת סייבר – חלק 3
- 5 מפגש : מבוא להאקינג
- 6 מפגש : שרשרת התקיפה
- 7 מפגש : סייבר במערכות תעשייתיות
- 8 מפגש : ניהול סיכונים במפעלי תעשייתי המחזיק חומרים מסוכנים
- 9 מפגש : מעבר משלים על מדריך הסייבר 1.3 וקובץ החישובים, השלמות, שאלות ותשובות, סיכום ומבחן סיום
- 10 מפגש : מפגש ספקים מטעם התאחדות התעשיינים

**קבלת תעודה סיום מותנה במעבר המבחן בציון 60 לפחות.**

# מפגש 1 - מבוא + מבוא לחומרים מסוכנים



- הסבר על הרגולציה בסייבר לתעשיית החומרים המסוכנים
- הצגת אירועי סייבר בתעשייה



# החלטות ממשלה 2443, 2444 מ-15.2.2015



1. החלטת ממשלה 2443 בנושא – קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר – **הקמת יה"ב**

2. החלטת ממשלה 2444 בנושא קידום ההיערכות הלאומית להגנת הסייבר – **הקמת מערך הסייבר הלאומי**

<http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2443.aspx>

**על בסיס שתי ההחלטות, יחוקק במדינת ישראל חוק הסייבר.**

# תהליכי עבודה במשק – על פי החלטות הממשלה



# רגולציה: הוספת תנאי סייבר בהיתר הרעלים

החלטות ממשלה 2443, 2444 מיום 15.2.2015

”... הכוונה והנחיה מקצועית בתחום הגנת הסייבר בהתאם **לסמכויות הרגולציה** המופעלות על ידי המשרד הממשלתי או במסגרתו....”

כל הזכויות שמורות - המשרד להגנת הסביבה ©

חוק החומרים המסוכנים, התשנ"ג-1993<sup>1</sup>

- הגדרות  
(תיקונים:  
התשנ"ז, התשס"ה,  
התשע"ג)
1. בחוק זה -  
"חומר מסוכן" - רעל או כימיקל מזיק;  
"אירוע חומרים מסוכנים" - התרחשות בלתי מבוקרת או תאונה, שמעורב בה חומר מסוכן, הגורמת או העלולה לגרום סיכון לאדם ולסביבה, לרבות שפך, דליפה, פיזור, פיצוץ, התאיידות, דליקה;  
"גוף הצלה" - (נמחקה);  
"כימיקל מזיק" - כל חומר מן החמרים המפורטים בתוספת הראשונה, בין דיאורגני או אורגני, או ממוצא דיאורגני אחרים.



# תוספת תנאים בהיתר – חוק חומרים מסוכנים

<p>2. כל מקום למכירת חומרים מסוכנים טעון רישוי לפי חוק רישוי עסקים, התשכ"ח-1968.</p>	<p>חובת רישוי</p>
<p>3. (א) לא יעסוק אדם ברעלים אלא אם כן יש בידו היתר רעלים מאת הממונה; הוראה זו לא תחול על רוקח מורשה העוסק ברעלים רפואיים לצרכי המואה בבית מרקחת או בעסק שעיקר עיסוקו סמי מרפא או רעלים רפואיים או על עסק המוכר תכשירים בלא מרשם, מהגדרתם בפקודת הרוקחים, אף אם המכירה נעשית שלא בבית מרקחת.</p> <p>(ב) בהיתר רעלים יפורטו מסחרו של בעל ההיתר, הרעלים שהוא ראוי לסחור בהם ומטרת השימוש בהם, אין בהיתר כדי להחיר סחר או יבוא של סם מסוכן כמשמעותו בפקודת הסמים המסוכנים (נוסח חדש), התשל"ג-1973.</p> <p>(ג) היתר רעלים יינתן רק למבקש שידוע כאדם הגון ולאחר שהוכיח להגנת דעתו של נתן ההיתר שהוא יודע קרוא וכתוב והוא מודע היטב לתכונות המסוכנות של אותם רעלים.</p> <p>(ד) תוקפו של היתר רעלים יהיה לשנה אחת, לשנתיים, לשלוש או לתקופה הפחותה משנה או העולה על שלוש שנים, בהתאם לאמות מידה, ובכללן סוג המטרה, חומרי הרעל, וכו'.  <b>(ה) הממונה ראוי להתנות את מתן היתר הרעלים בתנאים מיוחדים שיש לקיימם לפני מתן ההיתר, כן ראוי הוא לקבוע בהיתר תנאים מיוחדים, ורשאי הוא, בכל עת, להוסיף או לגרוע מהם, הכל על מנת להגן על הסביבה או על בריאות הציבור.</b></p> <p>(ו) הממונה ראוי לנסח כללי ענייני רעלים, מהטעמים המנויים בסעיף קטן (ה), לא יבטל הממונה היתר רעלים אלא לאחר שנתן לבעל ההיתר הזדמנות להשמיע את טענותיו.</p>	<p>היתר רעלים (חוק רעלים, התשל"ג, התשכ"ח)</p>
<p>4. לא ימסור המכס רעלים המוכנסים לישראל אלא לאחד מאלה בלבד -          (1) לבעל היתר רעלים;          (2) למי שיש לו הרשאה בכתב מאת הממונה.</p>	<p>רעלים מיוחדים</p>
<p>5. (א) בעל היתר רעלים ינהל מנקסי רעלים לפי הטופס שבתוספת השלישית ובהם יירשמו כל קניה ומכירה של רעלים.          (ב) בנקסי הקניות יפורטו תאריכה של כל קניה, החמרים שנקנו, כמותם וכן שמו של האדם שממנו נלקחו.          (ג) בנקסי המכירות יפורטו תאריכה של כל מכירה, תיאורו של הרעל שנמסר וכמותו, השימוש לו הוא מיועד ושמו ומענו של הקונה.</p>	<p>מנקה רעלים</p>



חוק חומרים מסוכנים

3. (ה) הממונה רשאי להתנות את מתן היתר הרעלים בתנאים מיוחדים שיש לקיימם לפני מתן ההיתר, **כן רשאי הוא לקבוע בהיתר תנאים מיוחדים ורשאי הוא בכל עת להוסיף או לגרוע מהם, הכל על מנת להגן על הסביבה או על בריאות הציבור**



**לעיסוק ברעלים** כמפורט בתוספת הראשונה לבקשה להיתר רעלים מיום 03/03/2020 המאושרת והחתומה בידי הממונה, המצורפת להיתר זה והמהווה חלק בלתי נפרד ממנו (להלן - הבקשה).

**עסקד מסווג לסיווג A.**

**בתנאים מיוחדים** כמפורט בתוספת השנייה המצורפת להיתר זה והמהווה חלק בלתי נפרד ממנו.

**מודגש בזה כי :**

1. היתר זה ניתן אך ורק לסוגי העיסוק, זהות העוסק, מיקום העיסוק, שם הבעלים/מנהל, שם אחראי הרעלים וסוגי וכמויות הרעלים שפורטו בו. יש להודיע מיד לממונה על כל שינוי בנתונים האמורים, לשם בדיקת הצורך לשנות את ההיתר, לבטלו או להחליפו.
2. עיסוק ברעלים ללא היתר רעלים ובכלל זה עיסוק שלא לפי הנתונים להם ניתן ההיתר או בניגוד לתנאיו **מהווה עבירה פלילית** שהעונש המרבי עליה הוא מאסר עד שלוש שנים או קנס **מ- 404,000 ש"ח עד 808,000 ש"ח למנהל ועד 1,616,000 ש"ח** לתאגיד או עסק, כמפורט בחוק.

\_\_\_\_\_  
\_\_\_\_\_  
**תאריך**

**חתימת הממונה וחותמת**

כל האמור בלשון זכר אמור גם בלשון נקבה.

# היתר רעלים

עבור :

מר ישראל ישראלי  
חברת ישראל

ישראלי 1, הרצליה

שלום רב,

הנדון : היתר רעלים

מצי"ב היתר רעלים שמספרו 123456.

לאחר סיווג עסקד בקטגוריה A תוקף ההיתר

הוא ל 1 שנים.

מיום 03/03/2020 עד ליום 02/03/2021.

הנך מתבקש להתחיל בהליך חידוש ההיתר הבא

3 חודשים לפני מועד פקיעת היתר זה.

בכבוד רב

הממונה

# הנחיות סייבר ל 4262 מפעלים המקבלים היתר רעלים



- מפעלי ייצור חומרים מסוכנים
- תאגידי מים
- מתקני התפלה
- חברת החשמל הישראלית
- נתיבי גז לישראל
- בתי חולים (חומרים לעיקור ציוד רפואי)
- נמלים
- שדה תעופה
- התעשייה הפרמצבטית
- תעשיית הדשנים
- יקבים
- בריכות שחיה
- מכבסות חכמות
- בתי דפוס

# דרישות רגולטוריות להגנה בסייבר

מה מפיק המפעל:

העלאת החוסן בסייבר



שמירה על רציפות עסקית



גופי תמ"ק  
שמירה על רציפות תפקודית

מנדט המשרד להגנת הסביבה:

בריאות הציבור



הגנה על הסביבה





# גופי תמ"ק – תשתיות מידע קריטיות

תמ"ק = תשתית מדינה קריטית

"גופים הנדרשים לעמוד ברגולציית סייבר של מערך הסייבר הלאומי על פי התוספת החמישית בחוק להסדרת הביטחון בגופים ציבוריים התשנ"ח 1998"

רגולטור בסייבר:

מערך הסייבר הלאומי – אגף תמ"ק  
 חוק להסדרת הביטחון בגופים  
 ציבוריים התשנ"ח 1998  
 התוספת החמישית

מטרה:

רציפות תפקודית למשק

רגולטור בסייבר:

המשרד להגנת הסביבה  
 החלטת ממשלה 2443  
 חוק חומרים מסוכנים התשנ"ג 1993

מטרה:

בריאות הציבור הגנת  
 הסביבה





# גופי תמ"ק

מתווה עבודה משותף : המשרד להגנת הסביבה – מערך הסייבר הלאומי

אכיפה	פיקוח	הנחיה
על פי סמכות	משותף	תוספת תנאים ספציפיים

## המטרה

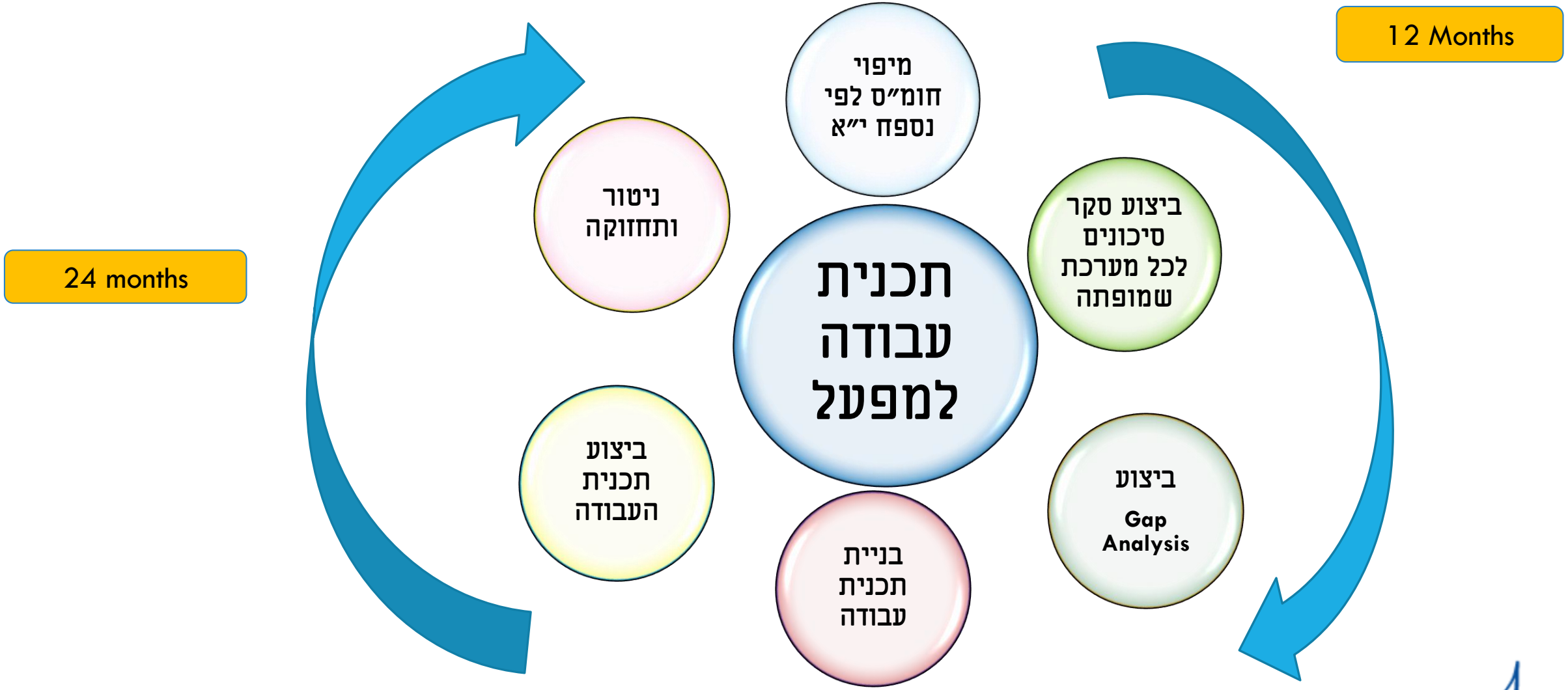
קיום רגולציה משלימה



מניעת כפל רגולציה



# תכנית עבודה למפעל



# אימוץ דירקטיבת III SEVESO

## נספח י"א – כמויות סף לחומרים מסוכנים

טבלת החומרים המסוכנים הנכללים בביצוע סקר סיכוני סייבר

סך עליון כמות השווה או העולה על (טון)	סך תחתון כמות השווה או העולה על (טון)	מספר CAS \ משפטי סיכון (H) (הערה 0)	חומר
			עם תכונות סיכון לבריאות (H), מקטגוריות הסיכון הבאות:
20	5	H300, H310, H330	H1 ACUTE TOXIC - Category 1, all exposure routes
200	50	H300, H310, H330, H331	H2 ACUTE TOXIC - Category 2, all exposure routes - Category 3, inhalation exposure route (7 הערה)
200	50	H370	H3 STOT SPECIFIC TARGET ORGAN TOXICITY – SINGLE EXPOSURE STOT SE Category 1
			עם תכונות סיכון פיזיקאליות (P), מקטגוריות הסיכון הבאות:
50	10	H200, H201, H202, H203, H205	P1a EXPLOSIVES (8 הערה) - Unstable explosives or - Explosives, Division 1.1, 1.2, 1.3, 1.5 or 1.6, or - Substances or mixtures having explosive properties and do not belong to the hazard classes Organic peroxides or Self-reactive substances and mixtures, Type C, D, E or F or organic peroxides, Type C, D, E, or F
200	50	H204	P1b EXPLOSIVES (8 הערה) Explosives, Division 1.4
50	10	H220, H221	P2 FLAMMABLE GASES

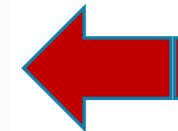
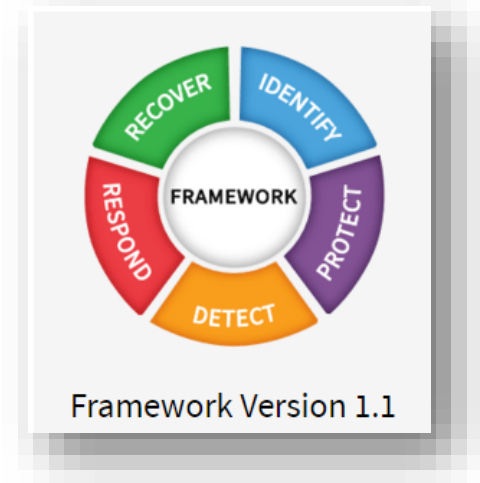
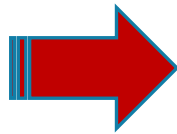
הרגולציה תחול תחילה על מפעלי סבסו תחתון קריטריון כניסה לרשימת סבסו על פי נתוני טבלאות שיפורסמו במדריך הסייבר 1.3 – נספח י"א



<sup>10</sup> הטבלה מבוססת על טבלת כמויות סף לחומרים מסוכנים הקיימת במדריך ניהול הסיכונים של אגף חומ"ס

# מדריך הסייבר לתעשייה גירסא 1.3

עבודת שטח מסיבית  
סקרי סיכונים במפעלים



[https://www.gov.il/he/departments/publications/reports/cyber\\_industry\\_toxins\\_permit](https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit)

**יתורגם לאנגלית לבקשת ארגון ה-OECD**

# גיליון החישובים

- ❖ חישוב רמת הנזק - I
- ❖ חישוב רמת החשיפה - P
- ❖ חישוב רמת הסיכון R =
- ❖ רשימת בקורות לרמת סיכון 1
- ❖ רשימת בקורות לרמת סיכון 2
- ❖ רשימת בקורות לרמת סיכון 3
- ❖ רשימת בקורות לרמת סיכון 4

H	G	F	E	D	C	B	A
 <p>המשרד להגנת הסביבה</p>							 <p>الوزارة لحماية البيئة Israel Ministry of Environmental Protection</p>
<h2>מדריך סייבר לעמידה בתנאים של היתר רעלים בתחום הסייבר בתעשייה</h2>							
<h3>הנחיות לחישוב רמת סיכון</h3>							
<p>הערכת הסיכון מבוססת על שקלול רמת הנזק הצפויה לנוכח הסיכוי שהנזק יתרחש.</p> <p>יש לחשב תחילה את רמת הנזק ואת רמת החשיפה ולאחר מכן תחושב רמת הסיכון לפי הנוסחה:  <math>P+3 \cdot I =</math> (סיכון שווה לרמת החשיפה ועוד 3 פעמים רמת הנזק).</p> <p>בגיליונות "חישוב רמת הנזק" ו"חישוב רמת החשיפה" יש להשיב על השאלות ע"י הזנת מספר. בתחתית הגיליון יחושבו הרמות באופן אוטומטי.</p> <p>לאחר חישוב רמת הנזק והחשיפה, יש להיכנס לגיליון "חישוב רמת הסיכון" ולצפות ברמת הסיכון שהתקבלה (חושבה אוטומטית לפי המספרים שהוזנו), בהתאם לתשובותיכם. יש להטמיע את הבקורות הדרושות על פי ערך הסיכון המתקבל (בין 4 ל-16).</p>							
<p>קובץ זה מכיל 7 גיליונות נוספים:</p> <p>1. חישוב רמת הנזק - I</p> <p>2. חישוב רמת החשיפה - P</p> <p>3. חישוב רמת הסיכון R =</p> <p>4. רשימת בקורות לרמת סיכון 1</p> <p>5. רשימת בקורות לרמת סיכון 2</p> <p>6. רשימת בקורות לרמת סיכון 3</p> <p>7. רשימת בקורות לרמת סיכון 4</p>							
<p>לשאלות ומידע נוסף ניתן ליצור קשר עם יחידת הסייבר בתעשייה במייל:  <a href="mailto:cyber_industry@sviva.gov.il">cyber_industry@sviva.gov.il</a></p>							

[https://www.gov.il/he/departments/publications/reports/cyber\\_industrytoxinspermit](https://www.gov.il/he/departments/publications/reports/cyber_industrytoxinspermit)



# לו"ז לביצוע



1. החלת תנאים נוספים בהיתר

2. פעילות סקר סיכונים

3. הטמעת בקורות

4. חצי שנה הפוגה

5. פיקוח ואכיפה

# פעולות ראשונות עם קבלת תנאי סייבר בהיתר הרעלים



מינוי ממונה הגנת סייבר במפעל

מסמך מדיניות המגדיר מחויבות  
ההנהלה לפעילות סייבר



# איך לעזאזל לבצע סקר סיכונים???



המשך יבוא.....

# אירועי סייבר בתעשייה על ציר הזמן



אוסטרליה- הזרמת  
 מליון קו"ב שפכים ע"י  
 עובד ממורמר ויטק בודן



התקפת סייבר על בקר **Siemens S7**  
 בכור האיראני באמצעות וירוס  
**Stuxnet** המכיל כ-15,000  
 שורות קוד!!



חברת הנפט ARAMCO בסעודיה  
 ווירוס בשם Shamoon הדביק ופגע כאמור  
 בכ-30 אלף תחנות עבודה ובכאלפיים  
 שרתים. הווירוס מחק קבצים כמו מסמכים,  
 גיליונות אלקטרוניים, ודואר אלקטרוני,  
 ובמקומם הוצגה תמונה של דגל ארה"ב  
 עולה באש. התקפות נוספות 2016, 2018



מפעל היתוך פלדה שני בגודלו  
 בגרמניה מושבת עקב תקיפת מייל  
 של אחד העובדים (פישינג)

2000

2010

2012

2014

# אירועי סייבר בתעשייה על ציר הזמן



דצמבר 2015 אספקת חשמל  
בשטח גדול כולל שטח הבירה.  
שיטת הפעולה: מאקרו בקבצי  
אקסל שנשתלו דרך פשינג  
ממוקד במייל.



מרץ 2016 - דווח על התקפה  
על סכר ניו - יורק. גורמים  
איראנים תוקפים מערכת ICS  
בסכר ריי-ברוק בניו יורק.  
התקיפה בוצעה תוך שימוש  
במודם סולרי עוד ב- 2013  
ודווחה 3 שנים אחר כך



נסיון איראני גרימת נזק  
למערכת ייצור הפקת  
נפט ARAMCO בערב  
הסעודית במטרה לגרום  
לאירוע סביבתי ופגיעה  
בציבור



ענקית האלומיניום Norsk  
Hydro - נורבגיה קטאר  
וברזיל. פגיעה מנוזקת  
כופר צפון קוריאנית  
שפגעה קשה במערכות  
המחשוב - שהשביתה  
מערכות ייצור. עלייה  
במחירי האלומיניום בעולם



29 אוקטובר,  
2 כורים בהודו  
בהספק של 1000  
מגה וואט הושבתו  
עקב תקיפת סייבר  
ע"י גורם צפון  
קוריאני.

2015

2016

2018

2019

2019



# אירועי סייבר בתעשייה בישראל



11.2.2018

## נוזקה לכריית מטבעות וירטואלים הותקנה במפעל תשתית קריטית

עמי רוחקס דומבה חברת ישראלית מצאה תוכנה זדונית מותקנת במתקן תשתית קריטית לאספקת מים שמטרתה כריית מטבעות וירטואלים.

החברה גילתה התקפה זו כחלק משגרת ניטור מתמשך של רשת OT של לקוח שירות מים. החברה מדווחת כי בהתקפה זו הותקפו מספר שרתים ברשת OT כדי לכרות מטבע מסוג Monero כותבים בדיווח של החברה.

התקפות תוכנה זדונית לכריית מטבעות וירטואלים צורכות משאבי CPU ורוחב פס מהרשת, וגורמות לזמני תגובה גדולים מצד כלים המשמשים לפקח על שינויים פיזיים ברשת ה OT כגון שרתי SCADA ו HMI. **עובדה זו מפחיתה את השליטה של מפעיל התשתית הקריטית על פעילותו ומאטה את זמני התגובה.**



חדשות בארץ

צה"ל מנע ניסיון איראני לפגוע במערך ההתרעה של פיקוד העורף

חטיבת ההגנה בסייבר של צה"ל סיכלה בשנה שעברה כ- 130 מתקפות סייבר, שברובן הופעלו מאיראן

07.02.19 | ב' אדר א' התשע"ט | גבי שניידר

פעילות הסייבר התוקפנית של איראן מנוהלת על ידי משמרות המהפכה האיראניים, וזוכה למימון נכבד המוערך ביותר **ממיליארד דולר לשנה**. האיראנים מפעילים לשם כך עשרות קבוצות, והמעקב אחרי אחת מהן הוא שהוביל לחשיפת המתקפה על פיקוד העורף ולנטרולה.

2018

2019

# אירועי סייבר בתעשייה בישראל



**חשד למתקפת סייבר חריגה על שורת מתקני מים בישראל.**  
<https://www.ynet.co.il/articles/0,7340,L-5720969,00.html>

ל- ynet נודע כי בסוף השבוע הותקפו לפי החשד מתקנים מצפון עד דרום, במטרה להשתלט על מערכות תפעול ולשבש פעילות משאבות. התאגידים התבקשו לשנות סיסמאות, אך "לא אירע נזק תפעולי". רשות המים: "הנושא מטופל"

אחיה ראב"ד פורסם: 15:15 , 26.04.20



## חדשות מתפרצות

<https://www.maariv.co.il/breaking-news/Article-764070>

דיווח בפוקס ניוז: "איראן ביצעה מתקפת סייבר נגד תשתיות המים של ישראל בחודש שעבר"

מקורות מסרו לפוקס ניוז כי איראן השתמשה בשרתים אמריקאים על מנת לבצע מתקפת סייבר נגד תשתיות מים בישראל בחודש שעבר.

סוכנויות הידיעות 14:08 07/05/2020



**מערך הסייבר מזהיר: האקרים פרו-איראנים יפתחו במתקפה נגד ישראל.**

מאת יוסי הטוני 13 במאי 2020, 13:29  
 ההאקרים ינצלו את התקופה שסביב יום ירושלים - האיראני והישראלי - וצפויים לתקוף את ישראל בסייבר לדברי המערך, "ההישענות המוגברת על טכנולוגיה בעקבות משבר הקורונה יצרה משטח תקיפה רחב, שעלול להיות מנוצל על ידם"

<https://www.pc.co.il/news/315672/>

2020

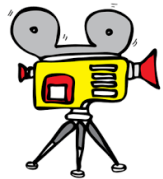


# אירועי סייבר בתעשייה בישראל - כלור

הוא ציין כי "במקרה הגרוע יותר, מאות אנשים היו בסיכון לחלות". עוד אמר כי מתקפת הסייבר הייתה מתוכנמת יותר ממה שחשבו תחילה בישראל. "זה היה קרוב להצליח, ולא ברור בוודאות שזה לא הצליח".

מנגד, גורם במשטר האיראני דחה בפני העיתון את ההאשמות. "איראן לא יכולה להרשות לעצמה לנסות להרעיל אזרחים ישראלים. ואם איראן עשתה זאת, איפה התגובה ההולמת הישראלית?", תהה. "החשד שלנו הוא שהישראלים רוצים עוד כסף מהאמריקנים והם המציאו את כל הסיפור. אבל האמריקנים לא טיפשים".

גם עלי רזה מיר-יוספי, דוברו של שגריר איראן באו"ם, ציין כי פעולות הסייבר של איראן הן "הגנתיות לחלוטין". לדבריו, "נקורבן של לוחמת סייבר וחבלות סייבר אחרות, אנחנו יודעים היטב כמה הפעולות יכולות להיות הרסניות. אנחנו מטרה קבועה של כוחות זדוניים ונמשיך להתגונן בפני כל מתקפה".



## מתקפת הסייבר על מתקני המים: "איראן ניסתה להעלות את רמת הכלור"

גורם מערבי אמר ל"פייננשל טיימס" כי במתקפת הסייבר שמיוחסת לאיראן ונחשפה לראשונה ב-ynet, נרשם ניסיון להעלות את רמת הכלור במים שמוזרמים לאזרחים: "מאות היו בסיכון לחלות, אלפים עלולים היו להישאר בלי מים". באיראן הכחישו מעורבות: "ישראל רוצה עוד כסף מארה"ב".



ynet פורסם: 01.06.20, 03:29



(צילום: רועי עידן)

גורם מודיעין מערבי חשף אמש (יום א') בפני העיתון הבריטי "פייננשל טיימס" פרטים חדשים על מתקפת הסייבר על מתקני המים בישראל, שיוחסה לאיראן ונחשפה לראשונה ב-ynet. על פי הגורם, מטרת התקיפה הייתה העלאת רמת הכלור שבמים המוזרמים לבתי האזרחים בישראל.

ארבעה גורמים ישראליים ואותו גורם מערבי סיפרו לעיתון כי האיראנים פרצו לתוכנות שמפעילות את משאבות המים בישראל לאחר שעברו בשרתים אמריקניים ואירופיים כדי להסתיר את מקור הקוד. לדברי הגורם המערבי, מתקפת הסייבר שמיוחסת לאיראן עלולה הייתה להוביל להשבתת המשאבות לאחר גילוי החריגה הכימית, דבר שעלול היה להותיר אלפי אזרחים ללא מים בברזים בזמן גל החום האחרון שפקד את המדינה.

# אירועי סייבר בתעשייה בישראל - כלור

## ידלין על המתקפה האיראנית: "תקיפת סייבר ברמה גבוהה שעוד לא ראינו כמותה"

ראש אגף המודיעין לשעבר התייחס באולפן ynet לדיווח על הניסיון להגביר את רמת הכלור במי הברזים בישראל: "זו יכולת לצאת מהממד הקיברנטי ולפגוע במערכות פיזיות". עם זאת הוא הרגיע: "לישראל יש מערכת הגנה טובה על התשתיות"



אלכסנדרה לוקש וניר (שוקו) כהן | פורסם: 01.06.20, 18:33

ראש המכון למחקרי ביטחון לאומי

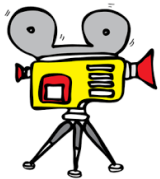
שידור חי / אלוף (במיל") עמוס ידלין | ראש המכון למחקרי ביטחון לאומי

**"איראן ניסתה להעלות את רמת הכלור"**

לפי הגורם המודיעיני: מתקפת הסייבר יועדה לפגוע באורחי ישראל דרך מתקני מים

10:05 | מעדות, בתי קפה וספרקים | הערכה בארה"ב: כ-4,100 נעצרו מאז תחילת ההפגנות | החחית: עלייה קלה בסמפרטורות | הקורונה במקסיקו: 151 חולי

אולפן ynet: ראיון עם אלוף במיל" ידלין (צילום: אלי סגל)





# סאלות ותשובות

