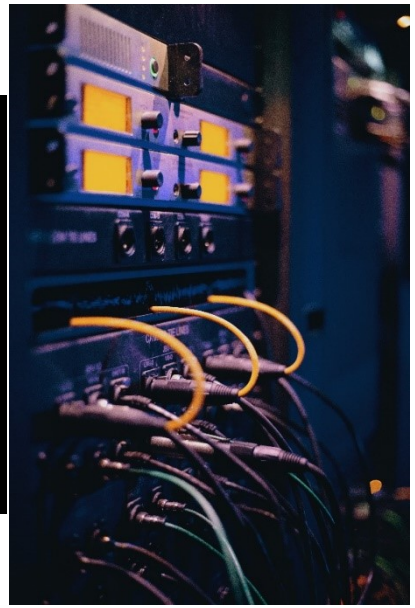
קורס סייבר לתעשייה מחזור 2
פברואר 2021



Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

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 , ואנשי סייבר) 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 העלאת החוסן בסייבר במפעלים (סקרים, הטמעת בקרות)

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

קצת על עצמי

יוסי שביט – נשוי +3 מתגורר בהר אדר

<u>השכלה:</u>

- מהנדס מכונות Bsc. הטכניון חיפה
- לימוד מדעי המחשב – אוניברסיטת מרילנד ארה"ב
- תואר שני MBA מינהל עסקים או"פ
- תואר CISM מטעם ארגון ISACA העולמי

<u>נסיון מקצועי מעל 25 שנה בתחומי הסייבר:</u>

- עבודת HANDS ON ברכיבי אבטחת מידע וסייבר בעולמות ה-IT
- כתיבת מתודולוגיות
- כתיבת רגולציה
- מרצה באקדמיה בקורסי סייבר במסלול תואר I במערכות מידע
- נסיון תעשייתי – סייבר במערכות ICS

מדינת ישראל
המשרד להגנת הסביבה

יוסי שביט (MBA, CISO, CISM)
ראש יחידת הסייבר בתעשייה

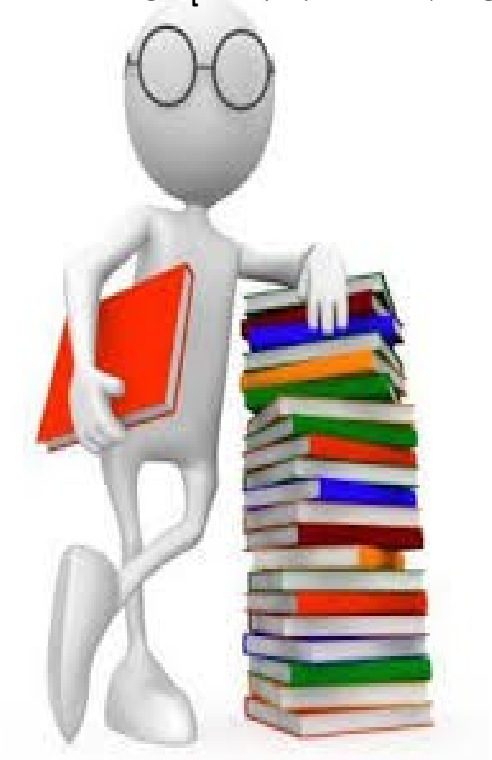
רח' בנק ישראל 7, גנרי 2
ירושלים 9195021
www.sviva.gov.il

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

נושאי הלימוד בקורס

- **מפגש 1:** <u>חלק ראשון</u> – הסבר על הרגולציה בסייבר לתעשיית החומרים המסוכנים, הצגת אירועי סייבר בתעשייה ובמערכות ICS

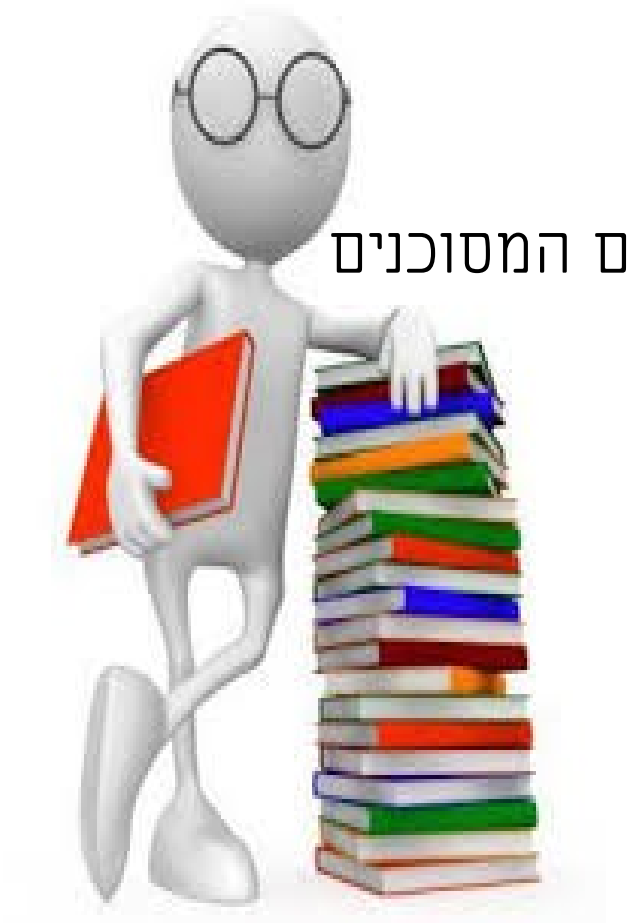
  <u>חלק שני</u> – מבוא לחומרים מסוכנים – קבוצות חומרים מסוכנים, סווג חומרים מסוכנים, גיליון בטיחות, שילוט החומרים המסוכנים, קודי חירום, סיכונים סביבתיים ממתקני תעשייה ותשתית
- **מפגש 2:** זיהוי ומיפוי תהליכים מסוכנים, סיווג תהליכים מסוכנים, רשימת תרחישים לניתוח (תרחישי WCS) חברת אתוס – אדריכלות תכנון וסביבה בע"מ
- **מפגש 3:** מושגי יסוד בהגנת סייבר – חלק 1
- **מפגש 4:** מושגי יסוד בהגנת סייבר – חלק 2
- **מפגש 5:** מושגי יסוד בהגנת סייבר – חלק 3
- **מפגש 6:** מבוא להאקינג + שרשרת התקיפה
- **מפגש 7:** סייבר במערכות תעשייתיות
- **מפגש 8:** ניהול סיכונים במפעלי תעשייתי המחזיק חומרים מסוכנים
- **מפגש 9:** מעבר משלים על מדריך הסייבר 1.3 וקובץ החישובים, השלמות, שאלות ותשובות, סיכום ומבחן סיום
- **מפגש 10:** מפגש ספקים מטעם התאחדות התעשיינים



קבלת תעודה סיום משתתף
קבלת תעודה סיום משתתף ועבר מבחן מסכם

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

מפגש 1 – מבוא + מבוא לחומרים מסוכנים



- הסבר כללי ממעוף הציפור על הרגולציה בסייבר לתעשיית החומרים המסוכנים
  לא לדאוג: בהמשך הקורס תהיה העמקה
- הצגת אירועי סייבר בתעשייה

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

החלטות ממשלה 2443, 2444 מ-15.2.2015

1. החלטת ממשלה 2443 בנושא – קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר – **הקמת יה"ב (יחידת הגנה בסייבר של משרדי הממשלה)**

2. החלטת ממשלה 2444 בנושא קידום ההיערכות הלאומית להגנת הסייבר – **הקמת מערך הסייבר הלאומי – אחריות הגנה בסייבר על כל המשק הישראלי.**

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

על בסיס שתי ההחלטות, יחוקק במדינת ישראל חוק הסייבר.

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

תהליכי עבודה במשק – על פי החלטות הממשלה

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

פעילות יחידת הסייבר

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

הקמת "מרכז הגנה ארצי לתעשייה"

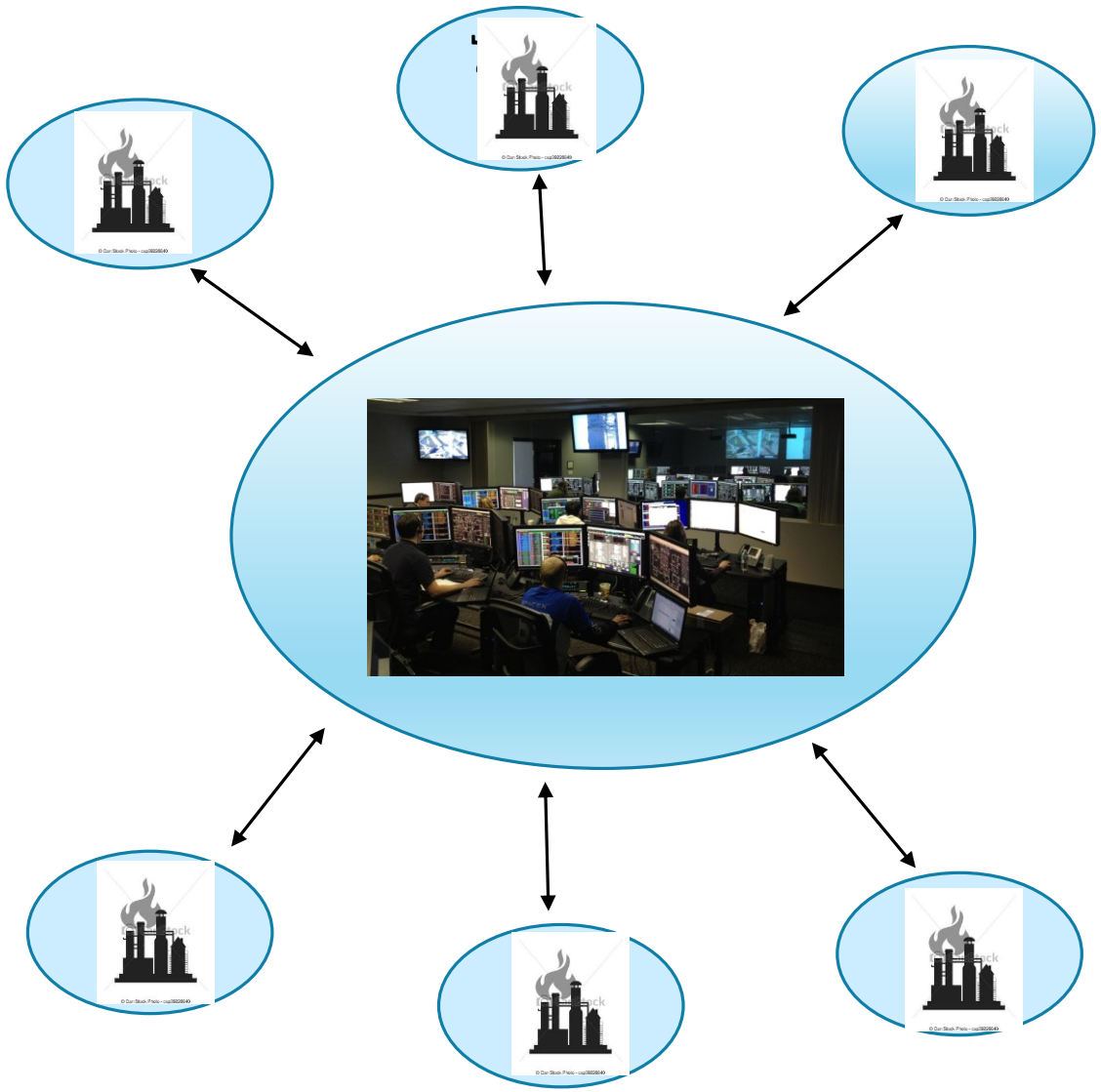
החל מדצמבר 2020 מרכז הגנה ארצי לתעשיה מופעל במתחם הסייבר בבאר שבע תחת ה-CERT הלאומי במערך הסייבר הלאומי

המטרה: פעילות פרו-אקטיבית לניטור מידע על נסיונות תקיפת סייבר או חולשות של מפעלים מסוכנים

CERT: Cyber Emergency Response Team

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

הקמת מק"מ תעשייתי (מרכז קיברנטי מגזרי)



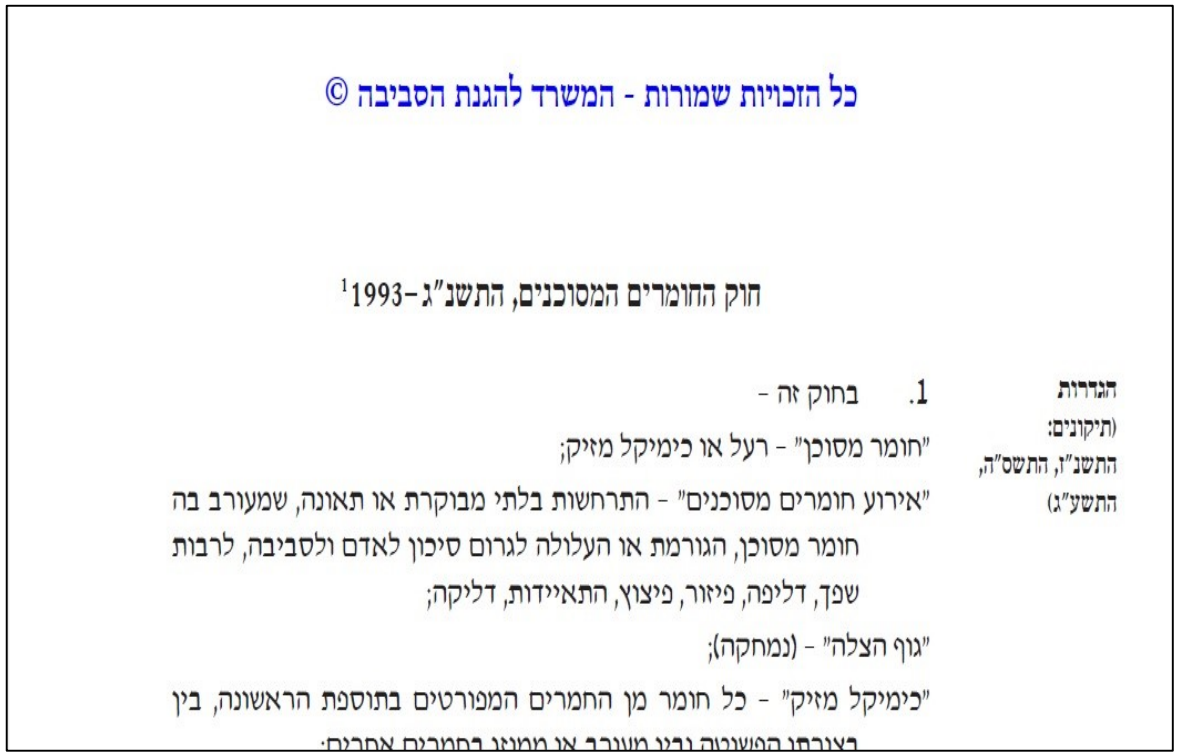
- שיתוף ידע ומידע בין מפעלים, כולל מודיעיני ועל מתקפות קיימות למניעת התפשטות מתקפה
- שיתוף ניסיון ותובנות להתמודדות עם אירוע קיים
- בניית מאגר ידע מקצועי של טיפול באירועים מורכבים באמצעות העמדת מומחי תוכן לעולם התוכן של המגזר
- רתימת גופים להעלאת רמת החוסן באמצעות הצפת סיכונים ואיומים קונקרטיים אשר המרכז יזהה אל מול גופים שונים במגזר
- בניית תמונת מצב מגזרית למקבלי החלטות בשגרה

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

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[1]

הגדרות (תיקונים: התשנ"ז, התשס"ח, 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;

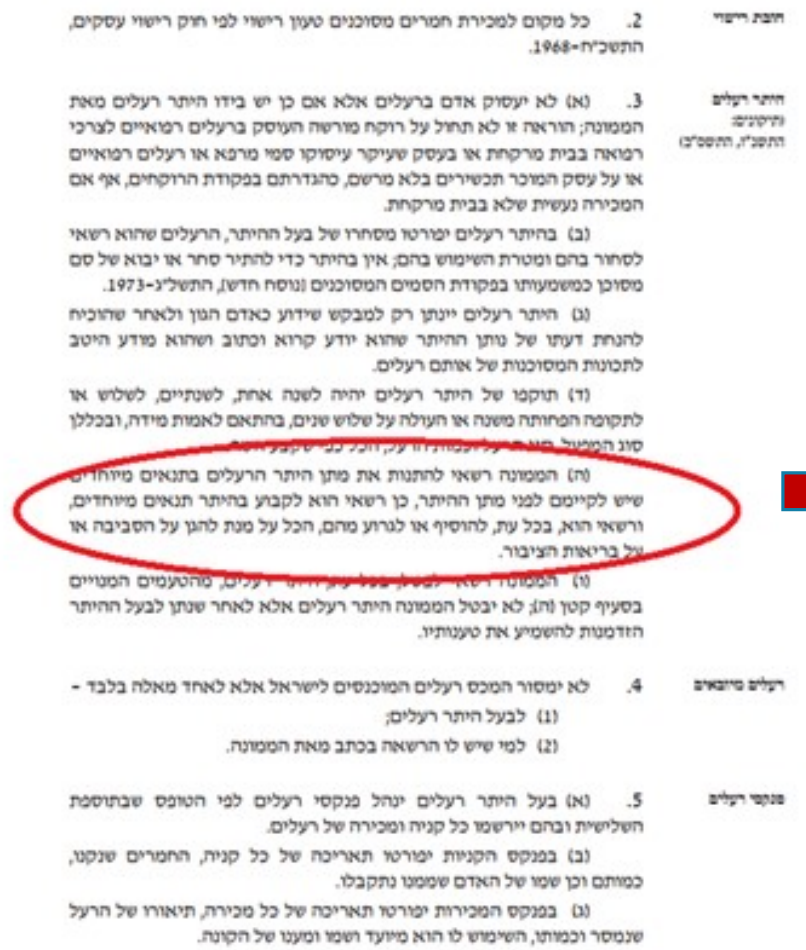
"גוף הצלה" - (נמחקה);

"כימיקל מזיק" - כל חומר מן החמרים המפורטים בתוספת הראשונה, בין בצורתו המקורית בין מעורב או ממוזג בחמרים אחרים;

חוק החומרים המסוכנים התשנ"ג 1993

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

תוספת תנאים בהיתר – חוק חומרים מסוכנים



חובת רישוי

2. כל מקום למכירת חמרים מסוכנים טעון רישוי לפי חוק רישוי עסקים, התשכ"ח-1968.

היתר רעלים

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 רפואה בבית מרקחת או בעסק שעיקר עיסוקו שמי מרפא או רעלים רפואיים או על עסק המוכר תכשירים בלא מרשם, כהגדרתם בפקודת הרוקחים, אף אם המכירה נעשית שלא בבית מרקחת.

(ב) בהיתר רעלים יפורטו מסחרו של בעל ההיתר, הרעלים שהוא רשאי לסחור בהם ומטרת השימוש בהם; אין בהיתר כדי להתיר סחר או יבוא של סם מסוכן כמשמעותו בפקודת הסמים המסוכנים [נוסח חדש], התשל"ג-1973.

(ג) היתר רעלים יינתן רק למבקש שידוע כאדם הנוח ולאחר שהוכיח להנחת דעתו של נותן ההיתר שהוא יודע קרוא וכתוב ושהוא מודע היטב לתכונות המסוכנות של אותם רעלים.

(ד) תוקפו של היתר רעלים יהיה לשנה אחת, לשנתיים, לשלוש או לתקופה הפחותה משנה או העולה על שלוש שנים, בהתאם לאמות מידה, ובכללן סוג הפעיל [illegible]

(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.

(ו) הממונה רשאי [illegible] רעלים, מהטעמים המנויים בסעיף קטן (ה); לא יבטל הממונה היתר רעלים אלא לאחר שנתן לבעל ההיתר הזדמנות להשמיע את טענותיו.

רעלים מיובאים

4. לא ימסור המכס רעלים המוכנסים לישראל אלא לאחד מאלה בלבד -

(1) לבעל היתר רעלים;

(2) למי שיש לו הרשאה בכתב מאת הממונה.

מנקסי רעלים

5. (א) בעל היתר רעלים ינהל מנקסי רעלים לפי הטופס שבתוספת השלישית ובהם יירשמו כל קניה ומכירה של רעלים.

(ב) במנקס הקניות יפורטו תאריכה של כל קניה, החמרים שנקנו, כמותם וכן שמו של האדם שממנו נתקבלו.

(ג) במנקס המכירות יפורטו תאריכה של כל מכירה, תיאורו של הרעל שנמסר וכמותו, השימוש לו הוא מיועד ושמו ומענו של הקונה.

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

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

היתר רעלים

עבור:
מר ישראל ישראלי
חברת ישראל

ישראלי 1, הרצליה

שלום רב,

הנדון: היתר רעלים

מצ"ב היתר רעלים שמספרו 123456.

לאחר סיווג עסקך 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

המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

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).

<u>עסקך מסווג לסיווג A</u>.

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.

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

התאחדות התעשיינים בישראל

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

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

דרישות רגולטוריות להגנה בסייבר

מנדט המשרד להגנת הסביבה :

בריאות הציבור

הגנה על הסביבה

מה מפיק המפעל:

העלאת החוסן בסייבר

שמירה על רציפות עסקית

גופי תמ"ק
שמירה על רציפות תפקודית

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

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

רגולטור בסייבר:
מערך הסייבר הלאומי – אגף תמ"ק
חוק להסדרת הבטחון בגופים
ציבוריים התשנ"ח 1998
התוספת החמישית

מטרה:
בריאות הציבור הגנת
הסביבה

מטרה:
רציפות תפקודית למשק

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

גופי תמ"ק

מתווה עבודה משותף : המשרד להגנת הסביבה – מערך הסייבר הלאומי

הנחיה	פיקוח	אכיפה
תוספת תנאים ספציפיים	משותף	על פי סמכות

המטרה

מניעת כפל רגולציה

קיום רגולציה משלימה

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

גופי מלמ"ב – תעשיות בטחוניות

הממונה על הביטחון במשרד הביטחון

על פי המתווה שסוכם בשלב הראשון:

1. הוקצה איש קשר במלמ"ב לצורך אסדרת פעילות הסייבר בגופים משותפים
2. מלמ"ב יעביר ליחידת הסייבר רשימה של גופים מונחים שלו בסייבר, אנו נבצע סינון על פי היתר רעלים.
3. תבוצע פעילות משותפת של איתור 2-3 גופים בשרשרת האספקה של מלמ"ב אשר מקבלים היתר רעלים מהמשרד
4. יבוצע מיפוי משותף של הממשקים באותם גופים
5. העברת מדריך הסייבר לתעשייה אל מלמ"ב על מנת שיוכלו להשוות למול התקינה שלהם ולהבין חפיפות והבדלים.

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

פעילויות נוספות מתוכננות לזמן המיידי

נמלים – חיפה, אשדוד, אילת

לולים– לולים ממוחשבים

משאיות חומ"ס – מיפוי הסיכונים הקיימים ברכב מקושר ורכב אוטונומי

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

אימוץ דירקטיבת SEVESO III

נספח י"א – כמויות סף לחומרים מסוכנים

טבלת החומרים המסוכנים הנכללים בביצוע סקר סיכוני סייבר

	חומר	מספר CAS \ משפטי סיכון (H) (הערה 0)	סף תחתון כמות השווה או העולה על (טון)	סף עליון כמות השווה או העולה על (טון)
	עם תכונות סיכון לבריאות (H), מקטגוריות הסיכון הבאות:			
	H1 ACUTE TOXIC - Category 1, all exposure routes	H300, H310, H330	5	20
	H2 ACUTE TOXIC - Category 2, all exposure routes - Category 3, inhalation exposure route (הערה 7)	H300, H310, H330 H331	50	200
	H3 STOT SPECIFIC TARGET ORGAN TOXICITY – SINGLE EXPOSURE STOT SE Category 1	H370	50	200
	עם תכונות סיכון פיזיקאליות (P), מקטגוריות הסיכון הבאות:			
	P1a EXPLOSIVES (הערה 8) - 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	H200, H201, H202, H203, H205	10	50
	P1b EXPLOSIVES (הערה 8) Explosives, Division 1.4	H204	50	200
	P2 FLAMMABLE GASES	H220, H221	10	50

[10] הטבלה מבוססת על טבלת כמויות סף לחומרים מסוכנים הקיימת במדריך ניהול הסיכונים של אגף חומ"ס

הרגולציה תחול תחילה על מפעלי סבסו תחתון

קריטריון כניסה לרשימת סבסו על פי נתוני טבלאות שיפורסמו במדריך הסייבר 1.3 – נספח י"א

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

תנאים לכניסה לרגולציה בסייבר 2021

עמידה בכמויות סף של דירקטיבת SEVESO

עמידה ב"תהליך מסוכן"

התהליך המסוכן מחובר למערכות בקרה ומיחשוב

מבוסס על חוק
חומרים
מסוכנים 1993

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

רגולציה בסייבר שנת 2020

רגולציה בסייבר החלה בפועל מ-8.6.2020

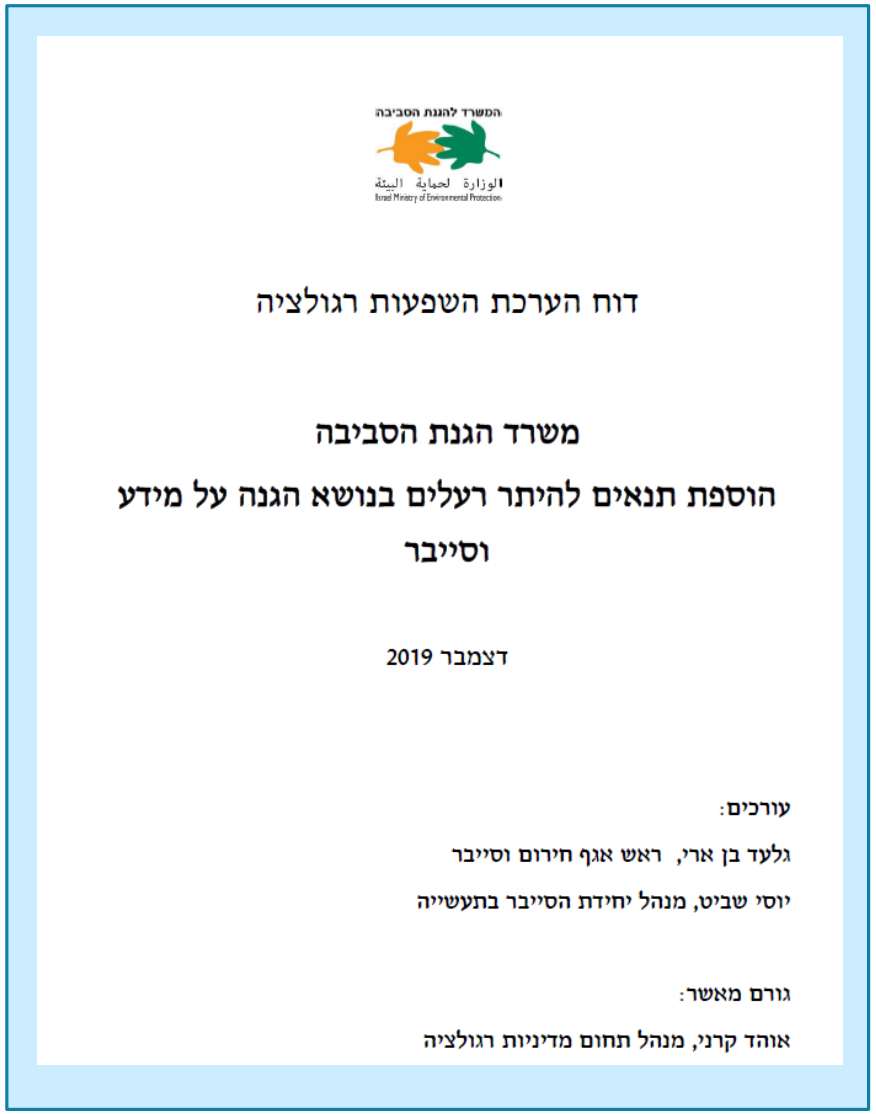
- 21 מפעלי סבסו תחתון – תוספת תנאי סייבר בהיתר רעלים
- 7 מפעלי סבסו עליון – רגולציה משולבת: ניהול סיכונים (חומ"ס) , סייבר, רע"ד

תכנית ל-2021

- 40 מפעלי סבסו תחתון
- מפעלי אמוניה – ממתין לאישור משרדי
- משאיות חומ"ס – ממתין לאישור משרדי ותיאום עם משרד התחבורה
- לולים מבוקרים בתיאום עם משרד החקלאות
- 25 מפעלי סבסו עליון

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

דו"ח RIA



המשרד להגנת הסביבה

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

RIA = Regulatory Impact Assessment

- ✓ הגורם היוזם
- ✓ החלופות האפשריות
- ✓ רגולטורים משיקים
- ✓ מגבלות ביישום
- ✓ מיפוי בעלי ענין
- ✓ שיח עם בעלי עניין
- ✓ סקירה בינלאומית
- ✓ הערות הציבור

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

מדריך הסייבר לתעשייה גירסא 1.3

NIST CSF
1.1

עבודת שטח מסיבית
סקרי סיכונים במפעלים

Framework Version 1.1

https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

תורגם לאנגלית לבקשת ארגון ה-OECD

https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

גיליון החישובים

- חישוב רמת הנזק – I
- חישוב רמת החשיפה – P
- חישוב רמת הסיכון = R
- רשימת בקרות לרמת סיכון 1
- רשימת בקרות לרמת סיכון 2
- שימת בקרות לרמת סיכון 3
- רשימת בקרות לרמת סיכון 4

המשרד להגנת הסביבה

סייבר בתעשייה

המשרד להגנת הסביבה

الوزارة لحماية البيئة

Israel Ministry of Environmental Protection

מדריך סייבר לעמידה בתנאים של היתר רעלים בתחום הסייבר בתעשייה

הנחיות לחישוב רמת סיכון

הערכת הסיכון מבוססת על שקלול רמת הנזק הצפויה לנוכח הסיכוי שהנזק יתרחש.

יש לחשב תחילה את רמת הנזק ואת רמת החשיפה ולאחר מכן תחושב רמת הסיכון לפי הנוסחה:
סיכון = I*3+P (הסיכון שווה לרמת החשיפה ועוד 3 פעמים רמת הנזק).

בגיליונות "חישוב רמת הנזק" ו"חישוב רמת החשיפה" יש להשיב על השאלות ע"י הזנת מספר.
בתחתית הגיליון יחושבו הרמות באופן אוטומטי.

לאחר חישוב רמת הנזק וההשפעה, יש להיכנס לגיליון "חישוב רמת הסיכון" ולצפות ברמת הסיכון שהתקבלה (חושבה אוטומטית לפי המספרים שהוזנו), בהתאם לתשובותיכם. יש להטמיע את הבקרות הדרושות על פי ערך הסיכון המתקבל (בין 4 ל-16).

קובץ זה מכיל 7 גיליונות נוספים:

1. חישוב רמת הנזק - I
2. חישוב רמת החשיפה - P
3. חישוב רמת הסיכון = R
4. רשימת בקרות לרמת סיכון 1
5. רשימת בקרות לרמת סיכון 2
6. שימת בקרות לרמת סיכון 3
7. רשימת בקרות לרמת סיכון 4

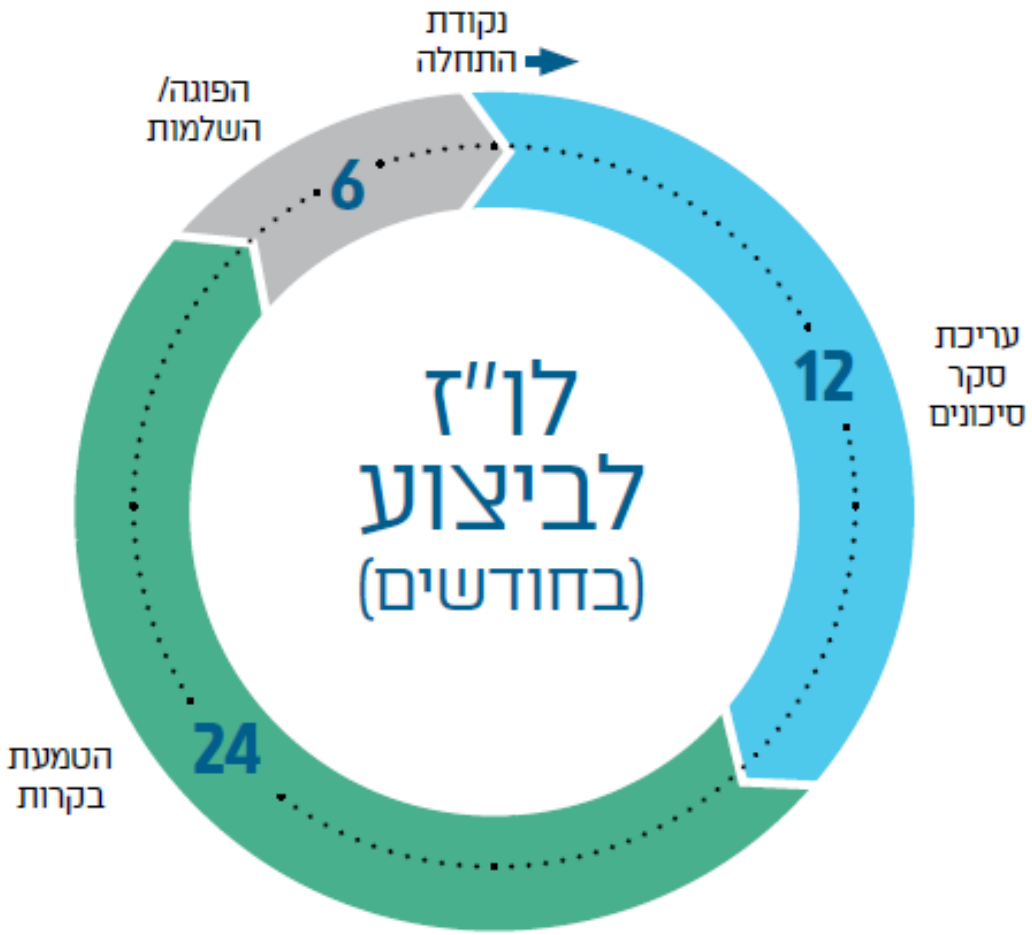
לשאלות ומידע נוסף ניתן ליצור קשר עם יחידת הסייבר בתעשייה במייל:
cyber_industry@sviva.gov.il

https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

התאחדות התעשיינים בישראל

לו"ז לביצוע



1. החלת תנאים נוספים בהיתר
2. פעילות סקר סיכונים
3. הטמעת בקרות
4. חצי שנה הפוגה
5. פיקוח ואכיפה

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

פעולות ראשונות עם קבלת תנאי סייבר בהיתר הרעלים

מינוי ממונה הגנת סייבר במפעל

מסמך מדיניות המגדיר מחויבות ההנהלה לפעילות סייבר

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

פעולות המשך לאחר קבלת תנאי סייבר בהיתר הרעלים

סקר סיכוני סייבר

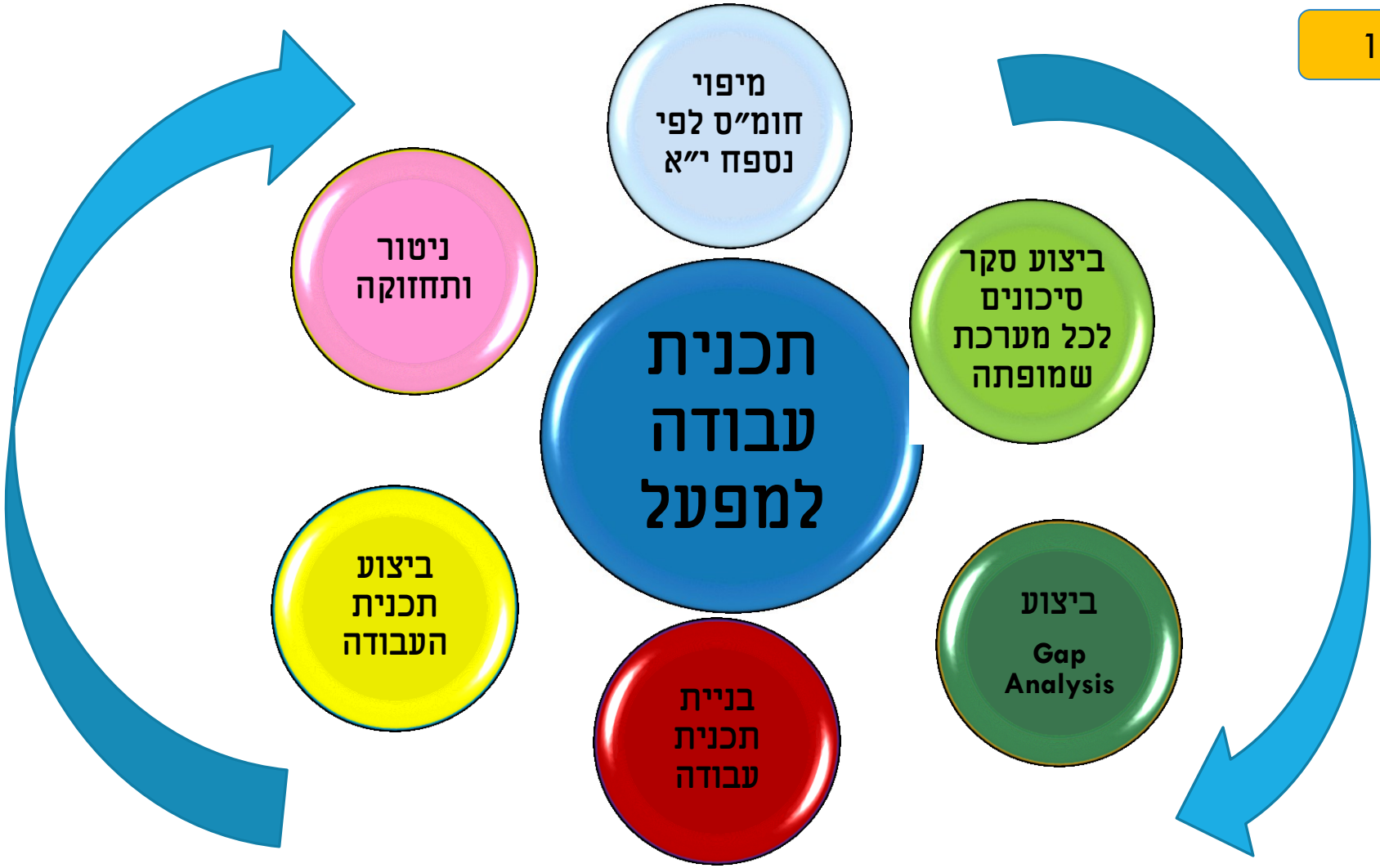
הטמעת בקרות סייבר להעלאת החוסן

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

תכנית עבודה למפעל

12 Months

24 months



Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

איך לעזאזל לבצע סקר סיכונים???

המשך יבוא.....

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

אירועי סייבר בתעשייה על ציר הזמן

אירועי סייבר בתעשייה על ציר הזמן

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

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 HMI ו SCADA. **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

share

| 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

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

אירועי סייבר בתעשייה בישראל

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/

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

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

2020

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

אירועי סייבר בתעשייה בישראל – כלור

המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

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

גורם מערבי אמר ל"פיננשל 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)

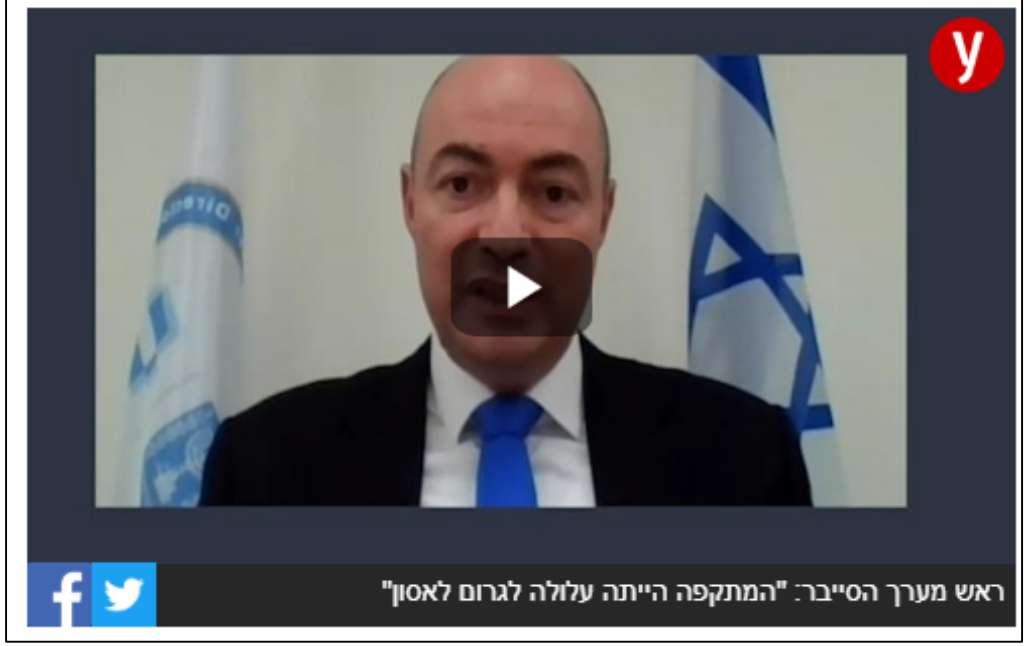
גורם מודיעין מערבי חשף אמש (יום א') בפני העיתון הבריטי "פיננשל טיימס" פרטים חדשים על מתקפת הסייבר על מתקני המים בישראל, שיוחסה לאיראן ונחשפה לראשונה ב-ynet. על פי הגורם, מטרת התקיפה הייתה העלאת רמת הכלור שבמים המוזרמים לבתי האזרחים בישראל.

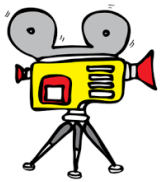
ארבעה גורמים ישראליים ואותו גורם מערבי סיפרו לעיתון כי האיראנים פרצו לתוכנות שמפעילות את משאבות המים בישראל לאחר שעברו בשרתים אמריקניים ואירופיים כדי להסתיר את מקור הקוד. לדברי הגורם המערבי, מתקפת הסייבר שמיוחסת לאיראן עלולה הייתה להוביל להשבתת המשאבות לאחר גילוי החריגה הכימית, דבר שעלול היה להותיר אלפי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

הוא ציין כי "במקרה הגרוע יותר, מאות אנשים היו בסיכון לחלות". עוד אמר כי מתקפת הסייבר הייתה מתוחכמת 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, "כקורבן 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".



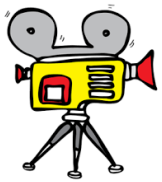


Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

התאחדות התעשיינים בישראל

אירועי סייבר בתעשייה בישראל – כלור

ראש המכון למחקרי ביטחון לאומי



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: 18:33 , 01.06.20

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

מתקפת סייבר השביתה חלק מקווי הייצור של טאואר

6 ספטמבר, 2020

מערכות המידע של החברה זיהו חדירה לשרתי הארגון. בצעד מניעתי השביתה החברה חלק מקווי הייצור. עדיין לא ברור מתי תשוב הפעילות לסדרה ומהו הנזק שנגרם לחברה. גם קבלניות הייצור X-Fab ו-TSMC הותקפו בעבר

קבלנית ייצור השבבים טאואר סמיקונדקטור (Tower) דיווחה הבוקר (א') על "אירוע סייבר", שחייב את החברה לבצע השבתת ייצור בחלק ממתקניה בעולם. טאואר מסרה כי מערכות אבטחת המידע זיהו עדות לחדירה במערכות מסוימות, וכצעד מניעתי השביתה החברה חלק מהשרתים ועצרה באופן יזום את הפעילות של חלק מקווי הייצור.

במקביל, יידעה החברה את רשויות החוק ופועלת בשיתוף מומחי סייבר לפתרון הבעיה כדי שניתן יהיה להפעיל מחדש את המערכות המושבתות. בטאואר עדיין לא יודעים להעריך מתי יחזרו קווי הייצור לפעילות ומה היקף הנזק שנגרם לחברה בעקבות התקרית.
לטאואר יש 6 מפעלי ייצור בישראל, ארצות הברית ויפן. שני המפעלים בישראל מתמחים בייצור רכיבים דיסקרטיים ואנלוגיים כמו

מאז הארוע,
הותקפו מספר מפעלים המכילים
חומרים מסוכנים

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Yosi Shavit MBA, CISM Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il