קורס סייבר לתעשייה מחזור 5
מאי 2023

Yosi Shavit MBA, CISO, CISM, CDPSE, CC 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
- הסמכות בינלאומיות CISM, CSPSE מטעם ארגון ISACA העולמי

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

- עבודת HANDS ON ברכיבי אבטחת מידע וסייבר
- פעילות סייבר במערכות בקרה תעשייתיות ורשתות OT
- כתיבת מתודולוגיות (מדריך סייבר לתעשייה גירסאות 1.3, 2.0)
- כתיבת רגולציה סייבר למפעלי חומרים מסוכנים
- מרצה באקדמיה בקורסי סייבר במסלול תואר I במערכות מידע
- מרצה בכנסים בארץ ובחו״ל
- מנטור בפרוייקט Cyber in Africa

Yosi Shavit MBA, CISO, CISM, CDPSE, CC 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 , וגירסא 2.0 שפורסמה בינואר 2022
- ✓ חשיפת משתתפי הקורס לחברות סייבר שיכולות לסייע בפעילות העלאת החוסן בסייבר במפעלים (סקרים, הטמעת בקרות)

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

נושאי הלימוד בקורס

- **מפגש 1:** הסבר על הרגולציה בסייבר לתעשיית החומרים המסוכנים, הצגת אירועי סייבר בתעשייה ובמערכות ICS
- **מפגש 2:** מבוא לחומרים מסוכנים - קבוצות חומרים מסוכנים, סווג חומרים מסוכנים, גיליון בטיחות,, קודי חירום ועוד
- **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 – סוגי האקרים, מתודולוגיות תקיפה, כלי האקינג על קצה המזלג
- **מפגש 7:** שרשרת התקיפה – הסבר על מתודולוגיית Cyber Kill Chain הכוללת מספר שלבים לתקיפה.
- **מפגש 8:** סייבר במערכות תעשייתיות – זו מול OT, הסבר על מערכות ICS (מערכות DCS מול מערכות SCADA)
- **מפגש 9:** ניהול סיכונים במפעל תעשייתי וסיכום קורס . מבחן מסכם.
- **מפגש 10:** מפגש ספקים מטעם התאחדות התעשיינים

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

קורס סייבר לתעשייה בשיתוף התאחדות התעשיינים

מחזור 1 - יולי 2020

מחזור 2 - פברואר 2021

מחזור 3 - נובמבר 2021

מחזור 4 - 1 ביוני 2022

מחזור 5 – 30 אפריל 2023

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

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

אוגוסט 2020 – ביירות

אמוניום ניטראט 2750 טון

- 170 הרוגים
- 6000 פצועים
- 300,000 ללא קורת גג
- נזק למרחק של עשרות ק"מ

מושל ביירות: נזקי הפיצוץ עלולים להגיע ל-15 מיליארד דולר

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

נמל עקבה – יוני 2022

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

פגיעה בחיי אדם

- פיצוץ
- קרינת חום
- פיזור רעלים

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

איך נראה מפעל תעשייתי?

יחידת הסייבר בתעשייה אחראית על:
הנחיית סייבר ל 4262 מפעלים המקבלים היתר רעלים

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

חומרים מסוכנים וסייבר

מערכות ייצור, שינוע ואחסון חומרים מסוכנים במקרים רבים מבוססות על מערכות מבוקרות מחשב

- **פריצה לבקר או למערכת HMI** (מערכת אדם-מכונה המנהלת את הבקר)
  - שינוי לחצים, טמפרטורות, ספיקות – גרימה לדליפת חומר מסוכן במכלים/ צנרת, או דליפת חומר בעיר / פציץ
  - שינוי ערכי PH– הזרמת חומר מסוכן לסביבה – גזים רעילים / זיהום מי תהום

- **פריצה למערכות ERP**
  - עלולות לשנות הרכבים של חומרים המגיעים לריאקטור ולגרום לריאקציות מסוכנות.
  - שינוי יעדי אחסון – החלפה בין חומרי תרופות לחומרי דשן למשל

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

תרחישים עקב אירוע סייבר במערכות בקרה תעשייתיות

1. פיזור רעלים – נמדד ביחידות PPM (כמות חלקיקי רעל במיליון חלקיקי אוויר)

2. אפקט קרינת חום משריפה – נמדד ביחידות של קרינת חום ביחידות של קילוואט למ״ר למשך 60 שניות.

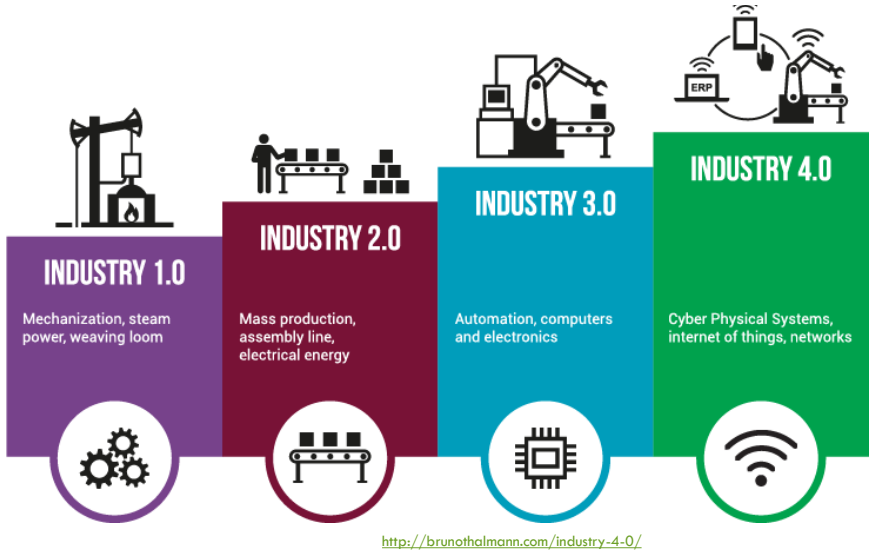
3. אפקט לחץ מפיצוץ – נמדד ביחידות של לחץ (PSI, BAR)

4. השבתת מערכות קריטיות – חשמל, מים, גאז, נמלים, בתי חולים, מוסדות ממשלה

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

המקור לסיכוני סייבר בעולם התעשייתי

- מפעלים תעשייתיים הוקמו לפני עשרות שנים לצורך ייצור, בזמן שלא חשבו על סייבר
- חיבור המחשוב היה בכבלים סריאליים ללא אינטרנט
- מפעלים היו רחוקים מרצפטורים ציבוריים – שהתקרבו למפעלים עם השנים
- החיים היו טובים בהיבט הסייבר אך לצורך התייעלות המפעלים הגיעו 2 מהפיכות חשובות



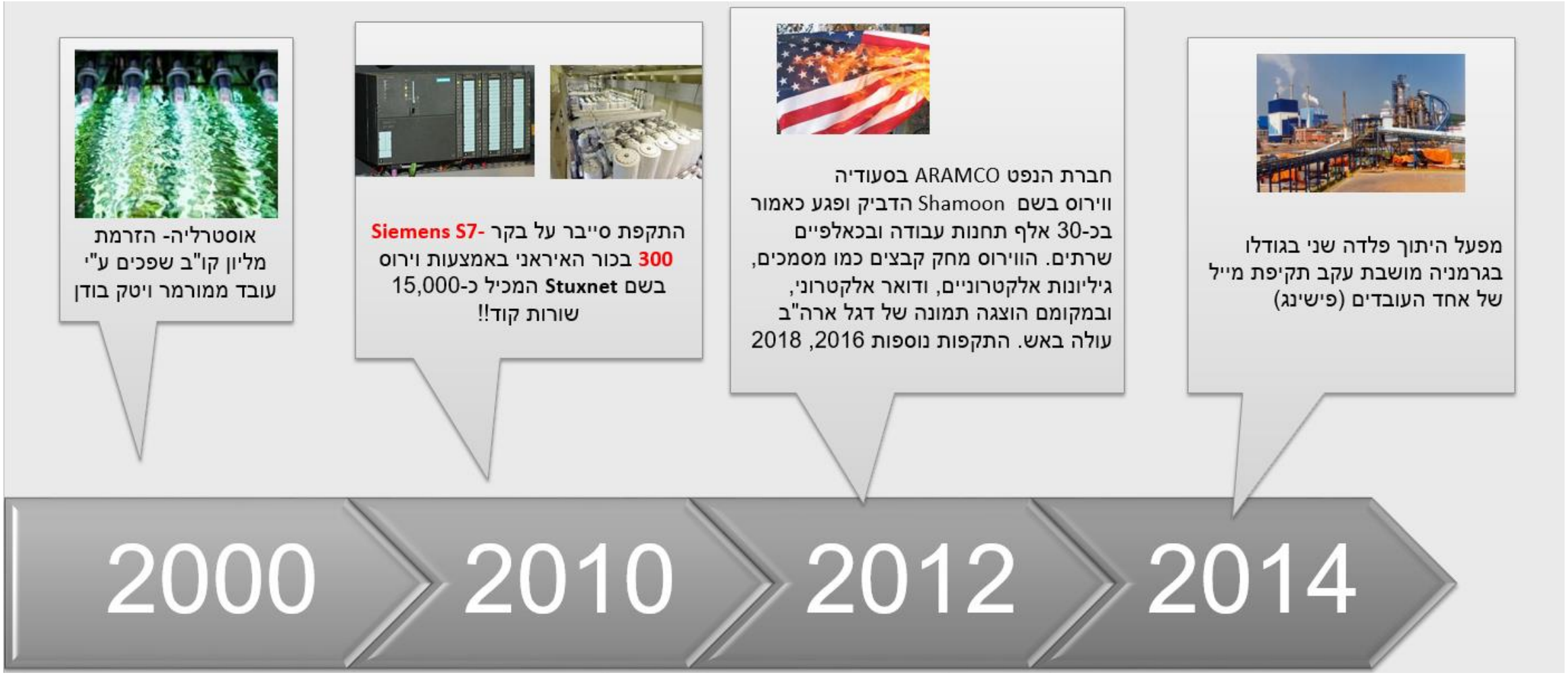
IIOT DEVICES
OPEN TO INTERNET

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

ואז..... הגענו לשנת 2000

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

אירועי סייבר בתעשייה על ציר הזמן



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

אירועי סייבר בתעשייה על ציר הזמן

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

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

2018 – נסיון איראני גרימת נזק למערכת ייצור הפקת נפט ARAMCO בערב הסעודית במטרה לגרום לאירוע סביבתי ופגיעה בציבור

2019 – ענקית האלומיניום Norsk Hydro – נורבגיה קטאר וברזיל. פגיעה מנוזקת כופר צפון קוריאנית שפגעה קשה במערכות המחשוב – שהשביתה מערכות ייצור. עלייה במחירי האלומיניום בעולם

2019 – 29 אוקטובר, 2 כורים בהודו בהספק של 1000 מגה וואט הושבתו עקב תקיפת סייבר ע"י גורם צפון קוריאני.

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

פברואר 2021 הרעלת מים בפלורידה

מה עשו? 100ppm ⟵ **11,100ppm**

איך עשו? השתלטות על ה - HMI דרך **TeamViewer**

ההאקר שפרץ הגדיל את כמות הסודה הקאוסטית (NaOH) למי השתיה

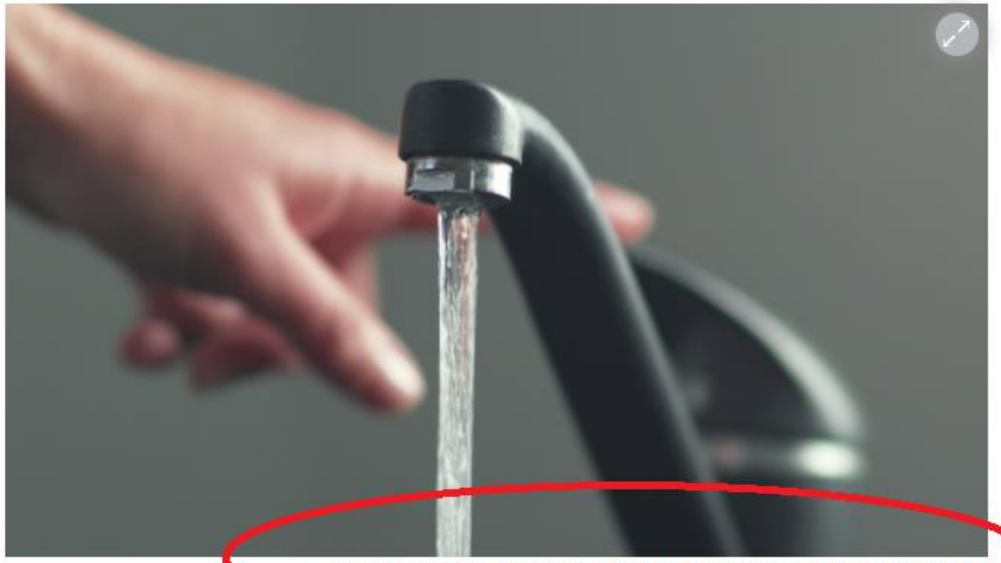
פי 100 מעל הערך הנדרש

האקרים ניסו להרעיל את המים בעיר בפלורידה

פחות משנה אחרי הפריצה למתקני המים בישראל, מתקפה דומה בארה"ב: האקרים השתלטו מרחוק על המחשב במתקן בעיר בת 15,000 תושבים, והעלו לגובה מסוכן את רמת הנתרן ההידרוקסידי במי השתייה. פקח הבחין בעכבר זז מעצמו וסיכל את הפריצה: "קריאת השכמה"

סוכנויות הידיעות פורסם: 12:03 , 09.02.21

האקרים הצליחו להשתלט על מערכת הניהול מרחוק של מתקן המספק מים לעיר בת 15,000 תושבים בפלורידה – וכמעט הצליחו להרעיל אותם. כך חשפו אמש (ב') הרשויות במחוז פינלס הסמוך לטמפה, תוך שהן מדגישות כי הניסיון הזה התגלה במהירות על ידי אחד הפקחים במתקן שנפרץ – וסוכל.

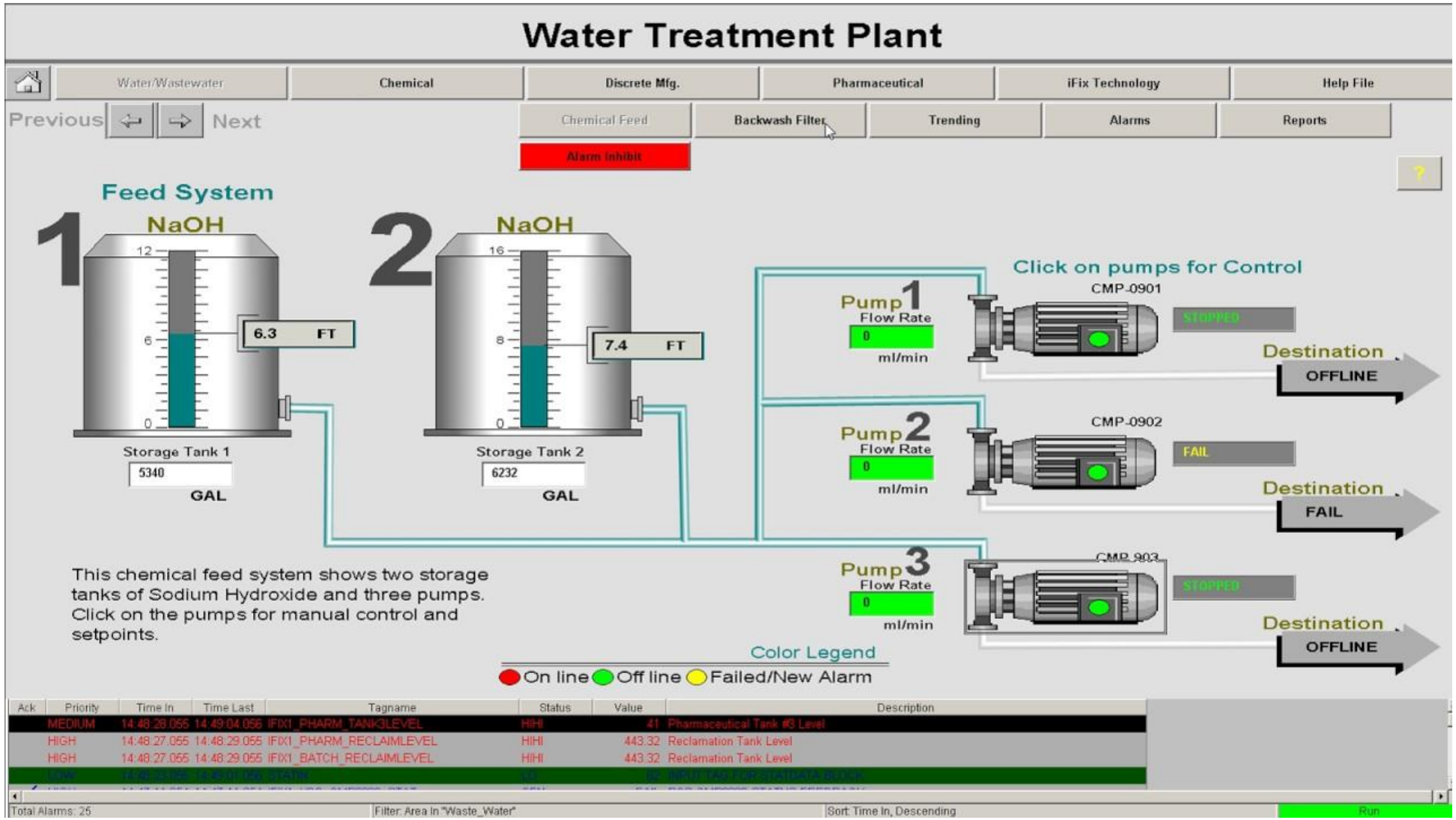


מ-100 חלקיקים למיליון ל-11,100. ההאקרים ניסו להרעיל, וכמעט הצליחו (צילום: shutterstock)

Holocaust 2nd Gen Rights
Open

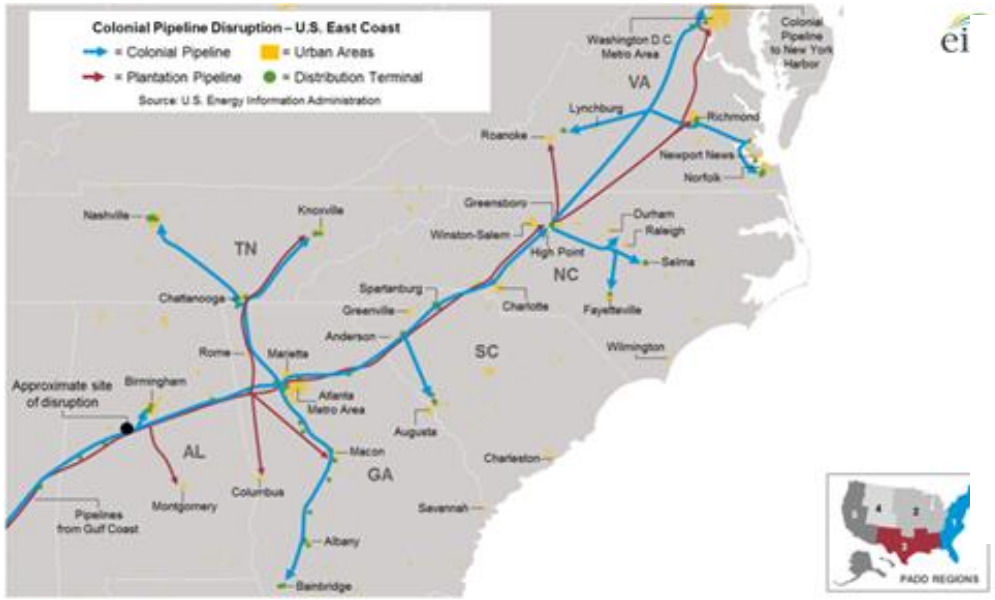
Yosi Shavit MBA, CISO, CISM, CDPSE, CC Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

מתקן טיפול במים מנקודת מבט של המפעיל



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

מאי 2021 – נעצרה אספקת דלק לחוף המזרחי



בעקבות מתקפת סייבר: חברת הולכת הדלקים הגדולה בארה"ב משותקת

חברת קולוניאל פייפליין עצרה את כל פעילותה לאחר שנפלה קורבן למתקפה. לחברה מערכת צינורות של קרוב ל-9,000 ק"מ שבהם היא מעבירה 45% מאספקת הדלק של החוף המזרחי של ארה"ב. קולוניאל פנתה לחברת אבטחת סייבר בבקשה לפתוח בחקירה

חדשות חוץ 15:20, 08.05.21

התקיפה במערכת החיוב (Billing) עצרה פעילות החברה לחלוטין

- האם בשל אי יכולת לחייב לקוחות?
- **האם בשל החשש מזליגת התקיפה למערכות התעשייתיות המכילות חומרים דליקים?**

דיווחים: קולוניאל פייפליין נאלצה לשלם כופר של 5 מיליון דולר להאקרים

הכופר שולם לכנופיית דארקסייד, שהשביתה את מחשביה של החברה המפעילה צינור דלק מרכזי בארצות הברית; למרות החזרת הפעילות, תחנות דלק במזרח המדינה ממשיכות לדווח על מחסור

חדשות חוץ 10:40, 15.05.21

תגיות: דארקסייד סייבר כופר קולוניאל פייפליין

קולוניאל פייפליין (Colonial Pipeline), המפעילה את אחד מצינורות הדלק המרכזיים בארצות הברית, שילמה לפי הדיווחים כופר של קרוב ל-5 מיליון דולר לכנופיית ההאקרים דארקסייד (DarkSide), לאחר שהמחשבים שלה הותקפו ופעולתה הושבתה.

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

אירועי סייבר בתעשייה בישראל – כלור

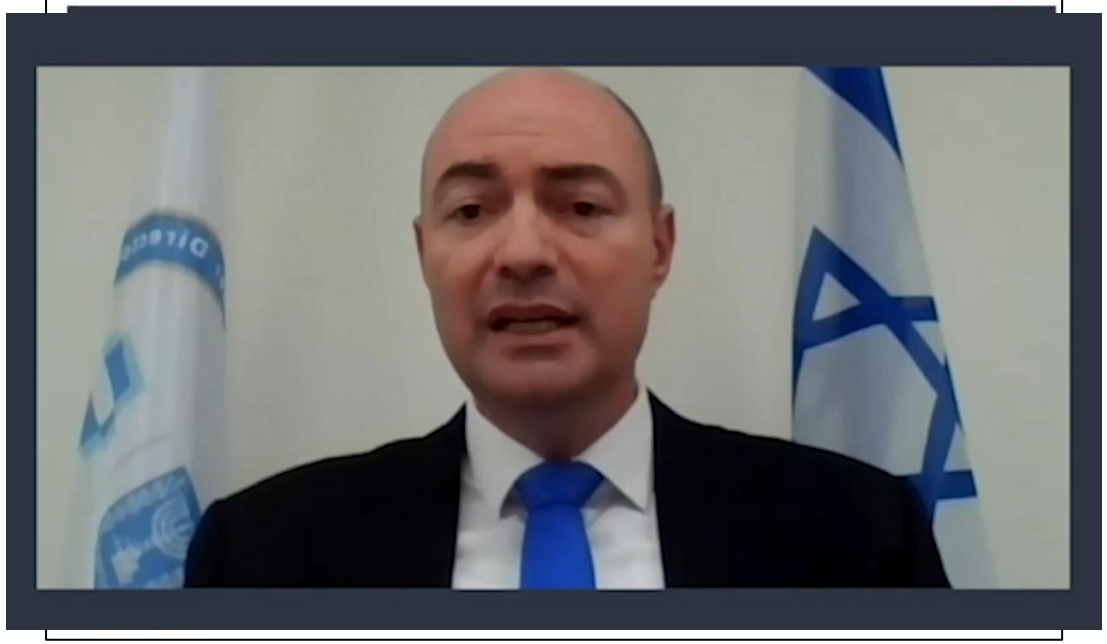
המשרד להגנת הסביבה

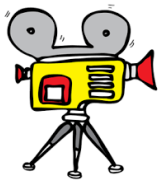
סייבר בתעשייה
המשרד להגנת הסביבה

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".





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.

התאחדות התעשיינים בישראל

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

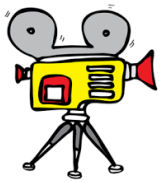
אירועי סייבר בתעשייה בישראל – כלור

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"

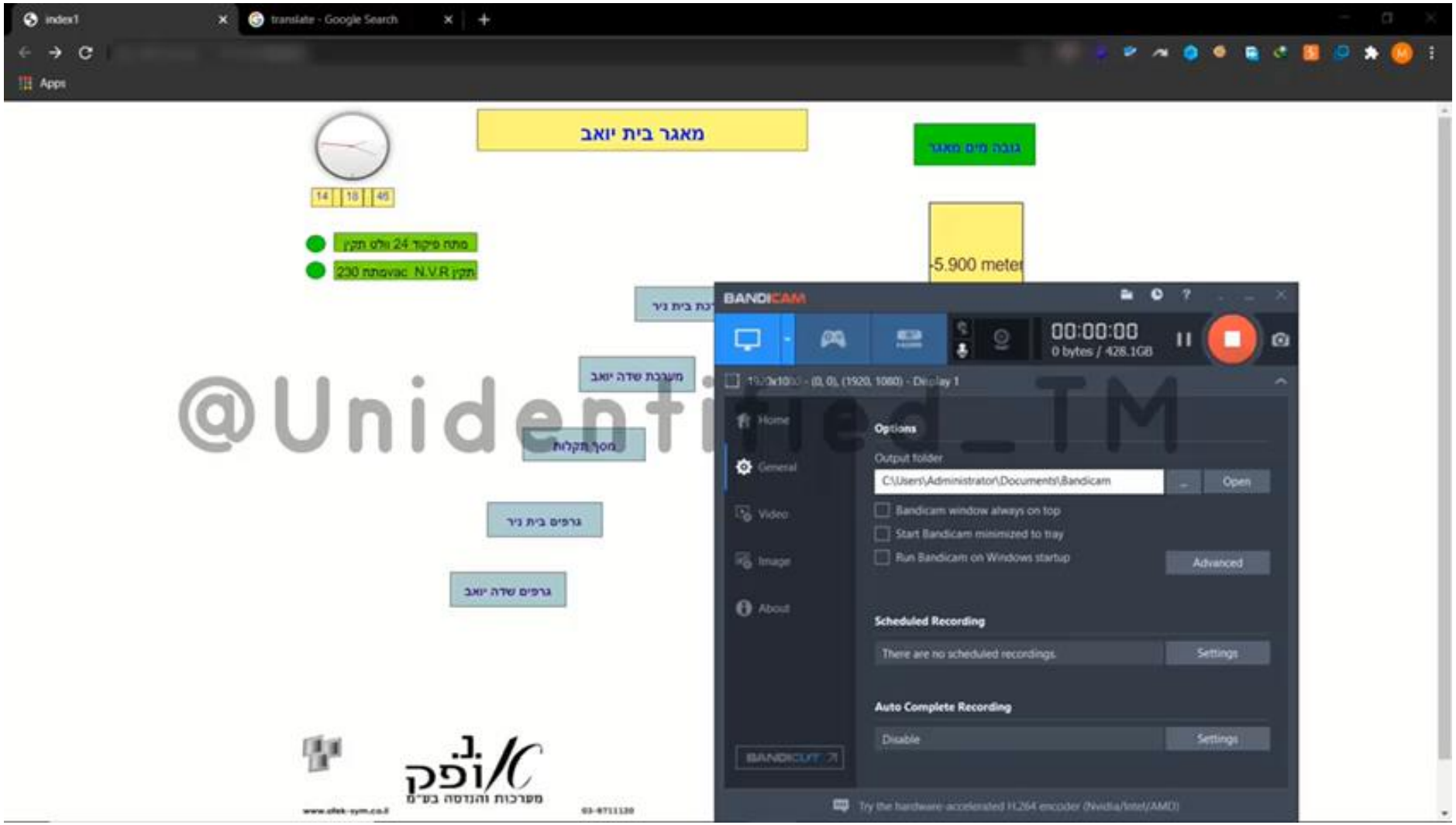
אלכסנדרה לוקש וניר (שוקו) כהן פורסם: 01.06.20 , 18:33

ראש המכון למחקרי ביטחון לאומי



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

תקיפת סייבר בעיני התוקף



@Unidentified_TM

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

ספטמבר 2020 – תקיפת מפעל טאואר סמיקונדקטור

במפעלי ייצור שבבים חומרים מסוכנים רבים בכללם גזים מאד רעילים

יצרנית השבבים הישראלית טאואר נמצאת עכשיו תחת מתקפת סייבר

אושרי אלקסלסי 06.09.2020 16 תגובות אבטחת מידע

Share

ציוץ

יצרנית השבבים הישראלית "זיהתה אירוע במערכות המידע והתקשורת שלה" וביצעה ניתוק יזום של המערכות כדי לבצע הערכת מצב. לא ברור כיצד המתקפה השפיעה על הייצור של החברה

יצרנית השבבים הישראלית טאואר (Tower Semiconductor) נמצאת תחת מתקפת סייבר המתמשכת החל מיום שישי. על פי הדיווחים ייתכן שמדובר במתקפה המבוססת על תוכנת כופר, בדומה לזו שתקפה את מערכות סאפיינס הישראלית בחודש יוני האחרון – והובילה על פי הדיווחים לתשלום של רבע מיליון דולר לתוקפים.

הווירוס שפגע בטאואר כבר תקף עיר שלמה באמריקה

בענף הסייבר מעריכים שהווירוס שפגע בחברה הוא RYUK, ששימש בעבר לתקיפת עיר במסצ'וסטס, תחנת הרדיו הגדולה בספרד וחברת ההייטק המקומית סאפיינס. לפי הערכות, חברות ישראליות נוספות נפלו קורבן למתקפת כופר שלו בסוף השבוע האחרון

מאיר אורבך 08.09.20 08:39

התאחדות התעשיינים בישראל

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

אוקטובר 2021 תקיפת בית החולים הלל יפה

המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

פריצת הסייבר לבית החולים: הלל יפה עדיין מושבת

מספר ימים לאחר מתקפת הסייבר יוצאת הדופן בבית החולים, מודיעים במשרד הבריאות כי התקלה עדיין לא תוקנה, אך לא נגרם נזק: "נמשכת העבודה במטרה להחזיר את מערכות המידע"

מתי ברנהרט, חדשות סרוגים
08:26 17.10.21 י"א בחשון תשפ

צילום RickP, ויקימדיה

במשרד הבריאות מודיעים כי בית החולים הלל יפה עדיין מושבת, לאחר שביום רביעי האחרון הותקף המקום באירוע סייבר מסוג כופרה, שפגע במערכות המחשוב של בית החולים.

"במהלך סוף השבוע זוהו על ידי מרכז הסייבר של משרד הבריאות עלייה בניסיונות למתקפות כנגד מספר בתי חולים וארגונים רפואיים", נמסר בהודעה משותפת של משרד הבריאות ומערך הסייבר הלאומי. "הערכות מוקדמת ותגובה מהירה של המרכז והצוותים בשטח בלמה את הניסיונות ולא נגרם נזק".

בבתי חולים קיימים החומרים המסוכנים הבאים:

- אתילן אוקסיד
- חמצן
- גפ"מ
- חומרים מסוכנים נוספים

https://cameochemicals.noaa.gov/

אתילן אוקסיד:

PACs (Protective Action Criteria)

Chemical	PAC-1	PAC-2	PAC-3	
Ethylene oxide; (Oxirane) (75-21-8)	5 ppm	45 ppm	200 ppm	LEL = 30000 ppm

(DOE, 2016)

NIOSH Pocket Guide
Ethylene oxide

NFPA 704

Diamond	Hazard	Value	Description
4 / 3 / 3	Health	3	Can cause serious or permanent injury.
	Flammability	4	Burns readily. Rapidly or completely vaporizes
	Instability	3	Capable of detonation or explosive decompositi
	Special		

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

התעשיינים בישראל

ינואר 2022 תקיפת קבוצת גולד בונד

מתקפת סייבר על קבוצת גולד בונד השביתה את פעילותה

הקבוצה שמחזיקה במספנות ישראל הודיעה לבורסה על השבתת רוב מערכת המחשוב שלה. ככל הנראה מדובר בתקיפה של קבוצת Hackers of Saviors הפועלת בשם המאבק הפלסטיני. גולד בונד: "פועלים בתיאום עם מערך הסייבר. צפויים שיבושים בפעילות הלוגיסטית בנמל"

רפאל קאהאן 14:49, 31.01.22

האזינו לכתבה 3 דקות

תגיות: גולד בונד | מספנות ישראל | מתקפת סייבר

קבוצת גולד בונד, העוסקת בהפעלת מסוף מטענים ומחסנים באשדוד, הודיעה היום לבורסה על תקיפת סייבר שהשביתה את מחשבי החברה וכתוצאה מכך גם חלק גדול מפעילותה. לפי הודעת החברה, שיבושים שהחלו בלילה זוהו ככל הנראה כחדירה של גורם זר למערכות שלה.

התאחדות התעשיינים בישראל

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

סקר מערך הסייבר הלאומי והלמ"ס

המדגם כלל כ-2,500 עסקים

- שניים מכל חמישה עסקים גדולים חווה תקיפת סייבר (42%)
- בקרב תעשיית טכנולוגיית עילית (47%)
- בענפי ההיי-טק, אחד מכל שלוש חברות דיווחו על תקיפה (37%)
- כ-15% מהעסקים הקטנים חוו מתקפת סייבר

חדשות

אחד מחמישה עסקים בישראל חווה תקיפת סייבר

תאריך פרסום: 21.07.2021

אחד מכל חמישה עסקים בישראל (18%) חווה תקיפת סייבר - כך עולה מסקר חדש של הלמ"ס ומערך הסייבר הלאומי

שתפו:

https://www.gov.il/he/departments/news/cyberweeknews

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

עלויות למשק- מקורס קודם

- צוות משא ומתן
- צוות תגובה ופורנזיקה
- ייעוץ משפטי
- נזק תדמיתי
- תביעות משפטיות הגנת פרטיות
- ניהול תקשורתי
- השבתת מערכות
- אובדן לקוחות
- תשלום כופרה !

מתקפות סייבר

סקר: עלות התאוששות ממתקפת כופר בישראל - כ-570 אלף דולר

עפ"י סקר שערכה חברת הסייבר סופוס, סכום תשלום הכופר הממוצע הוא 170 אלף דולר • רק 8% מהארגונים הצליחו לקבל חזרה את כל הנתונים שלהם לאחר ששילמו דמי כופר, ו-29% לא קיבלו בחזרה יותר מחצי מהנתונים • תשלום הכופר הגבוה ביותר בסקר - 3.2 מיליון דולר, והתשלום הנפוץ ביותר – 10,000 דולר

אורי ברקוביץ' 03.05.2021

מתקפת כופר / צילום: שאטרסטוק

https://www.globes.co.il/news/article.aspx?did=1001369619

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

עלויות למשק

המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

- תשלום כופרה
- צוות משא ומתן
- צוות תגובה ופורנזיקה
- ייעוץ משפטי
- נזק תדמיתי
- תביעות משפטיות הגנת פרטיות
- ניהול תקשורתי
- השבתת מערכות
- אובדן לקוחות

עלויות נזקי מתקפות הסייבר – לשיא של כל הזמנים

לפי יבמ, העלות הממוצעת של מתקפה היא 4.35 מיליון דולר - זינוק של 13% בשנתיים • משך מתקפות הכופר התקצר ב-94% בשלוש שנים

יוסי הטוני | 07:00 27/07/2022

מתקפות סייבר - כמה זה עולה לנו? צילום: BigStock

עלויות הנזק של מתקפות הסייבר הפכו יקרות מאי פעם: לפי דו"ח חדש של **יבמ**, העלות הממוצעת של מתקפה לארגון שעבר אותה עומדת על 4.35 מיליון דולר – נתון המשקף זינוק של כ-13% בשנתיים.

חוקרי הענק הכחול בחנו 550 חברות ברחבי העולם שחוו לפחות תקיפת סייבר אחת. לפי המחקר, הנזק של תקיפות הסייבר משפיע יותר מתמיד על הצרכנים של קורבנות התקיפה: כ-60% מהחברות שהותקפו העלו את מחירי הסחורות, המוצרים והשירותים שהן מספקות, ובכך נלגלו את העלויות הגבוהות של הנזק לצרכנים שלהן.

לפי המחקר, 83% מהחברות חוו יותר ממתקפת סייבר אחת במהלך חייהן. בנוסף, מתברר שלמתקפות יש השפעה ארוכה יותר משחשבו עד כה: כמעט מחצית מהעלויות של נזקי התקיפות נוצרו יותר משנה לאחר הפריצה.

https://www.pc.co.il/news/367970/

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

תקיפות סייבר מפעלי תעשייה בשנת 2022

עד כה ידוע על 6 תקיפות ברבעון ראשון של שנה זו :

- ❑ **מפעל באיזור הדרום – כשבועיים השבתה עדיין לא חזר לגמרי לפעילות**
- ❑ **מפעל באיזור המרכז – עדיין תחת ניהול האירוע**
- ❑ **מפעל בצפון – 2 אירועים שגרמו נזק כלכלי ותדמיתי**
- ❑ **מפעל גלובאלי גדול – 2 ארועים אחד בסניף בחו"ל ואחד בסניף בארץ – האירועים טופלו במהירה ונמנע נזק**

❑מי הבא בתור??!!!

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

קצת על הרגולציה בסייבר למפעלי חומרים מסוכנים

איך הכל התחיל?.....

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

פברואר 2015 החלטות ממשלה 2443, 2444

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, CISO, CISM, CDPSE, CC 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, CISO, CISM, CDPSE, CC Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

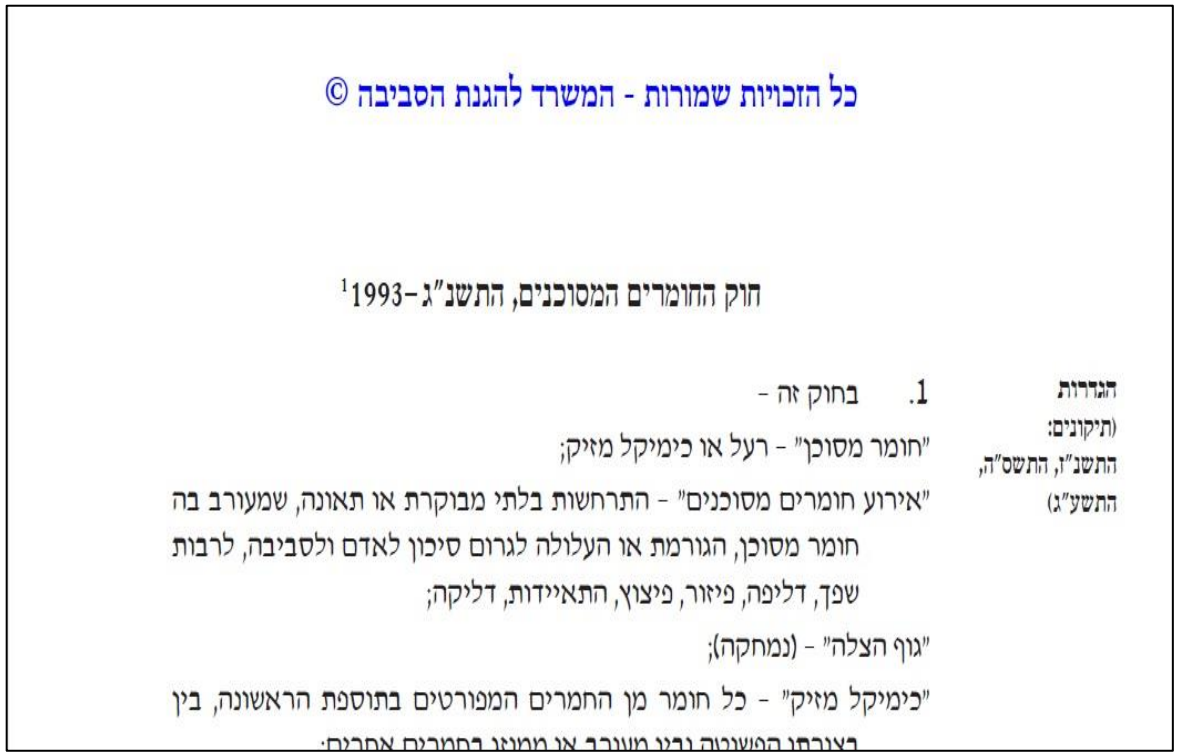
פעילות יחידת הסייבר

Yosi Shavit MBA, CISO, CISM, CDPSE, CC 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

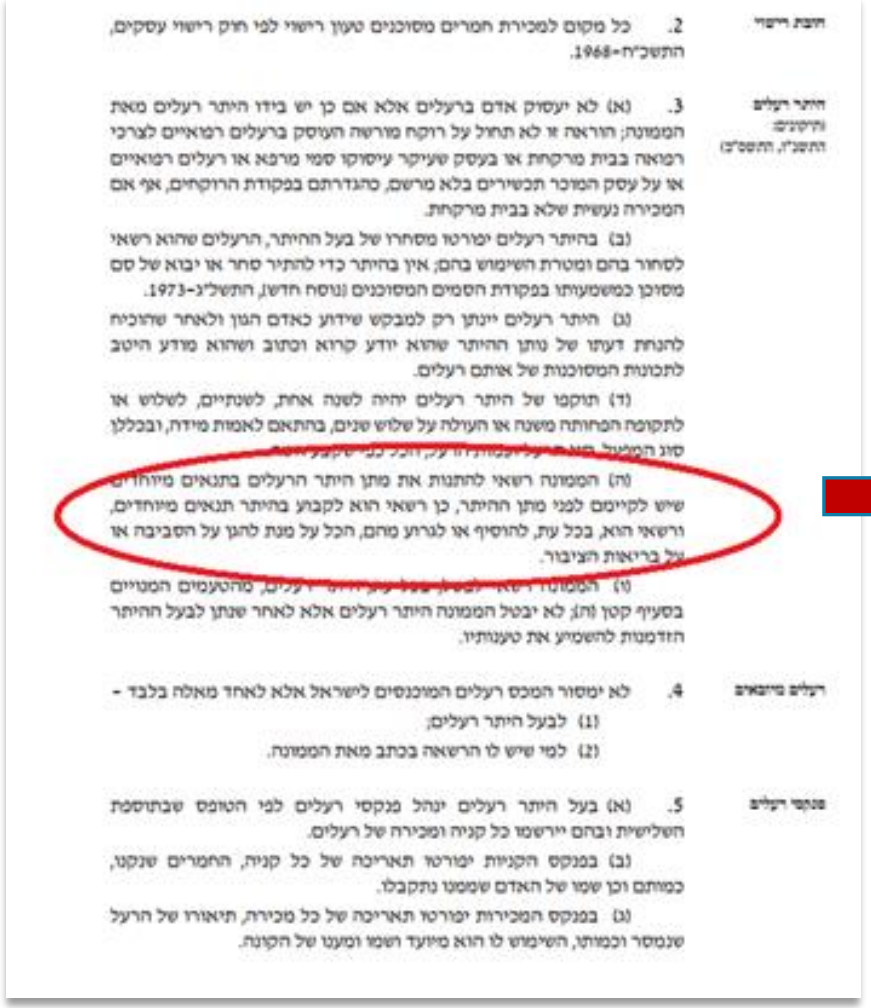
"... הכוונה והנחיה מקצועית בתחום הגנת הסייבר בהתאם **לסמכויות הרגולציה** המופעלות על ידי המשרד הממשלתי או במסגרתו....."



חוק החומרים המסוכנים התשנ"ג 1993

Yosi Shavit MBA, CISO, CISM, CDPSE, CC 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 חומרים 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 סמי 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 מספרו 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 הגון 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 המעגל [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, החומרים 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

23 אפריל, 2023 Yosi Shavit MBA, CISO, CISM, CDPSE, CC 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).

עסקך 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.

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

הנחיות סייבר ל 4262 מפעלים המקבלים היתר רעלים

- מפעלי ייצור חומרים מסוכנים
- תאגידי מים
- מתקני התפלה
- חברת החשמל הישראלית
- נתיבי גז לישראל
- בתי חולים
- נמלים
- שדה תעופה
- התעשייה הפרמצבטית
- מפעלי סמיקונדקטור
- תעשיות ביטחוניות
- תעשיית הדשנים
- יקבים
- בריכות שחיה
- מכבסות חכמות
- בתי דפוס

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

רגולציה על בסיס היתר רעלים

קבוצה	חידוש	כמות מפעלים
A	אחת לשנה	382
B	אחת לשנתיים	555
C	אחת ל-3 שנים	3325

מבוסס על חוק חומרים מסוכנים 1993

החל מיוני 2020
תוספת תנאי הגנה בסייבר

קביעת קבוצה ע"פ הקריטריונים הבאים:

- ✓ **כמות חומ"ס**
- ✓ **קירבה לרצפטור ציבורי**

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

תנאים לכניסה לרגולציה בסייבר 2020

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, CISO, CISM, CDPSE, CC Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

תנאים לכניסה לרגולציה בסייבר 2022

היתר רעלים ברמה A או B

מבוסס על חוק
חומרים
מסוכנים 1993

החומר המסוכן מנוהל / מבוקר ע"י מערכות בקרה ומיחשוב

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

רגולציה בסייבר החל מ- 8 ביוני 2020

סה"כ 168 מפעלים קיבלו רגולציית סייבר

שנת 2020

21 מפעלים סווסו תחתון

7 מפעלים סווסו עליון – רגולציה משולבת פיילוט

שנת 2021

32 מפעלי סבסו תחתון
25 מפעלי סבסו עליון – רגולציה משולבת
21 מפעלים לפיקוח משנה קודמת

שנת 2022

10 מפעלי סווסו תחתון

33 מפעלי סווסו עליון

40 מפעלי אמוניה

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

רגולציה בסייבר לשנים 2023 – 2033

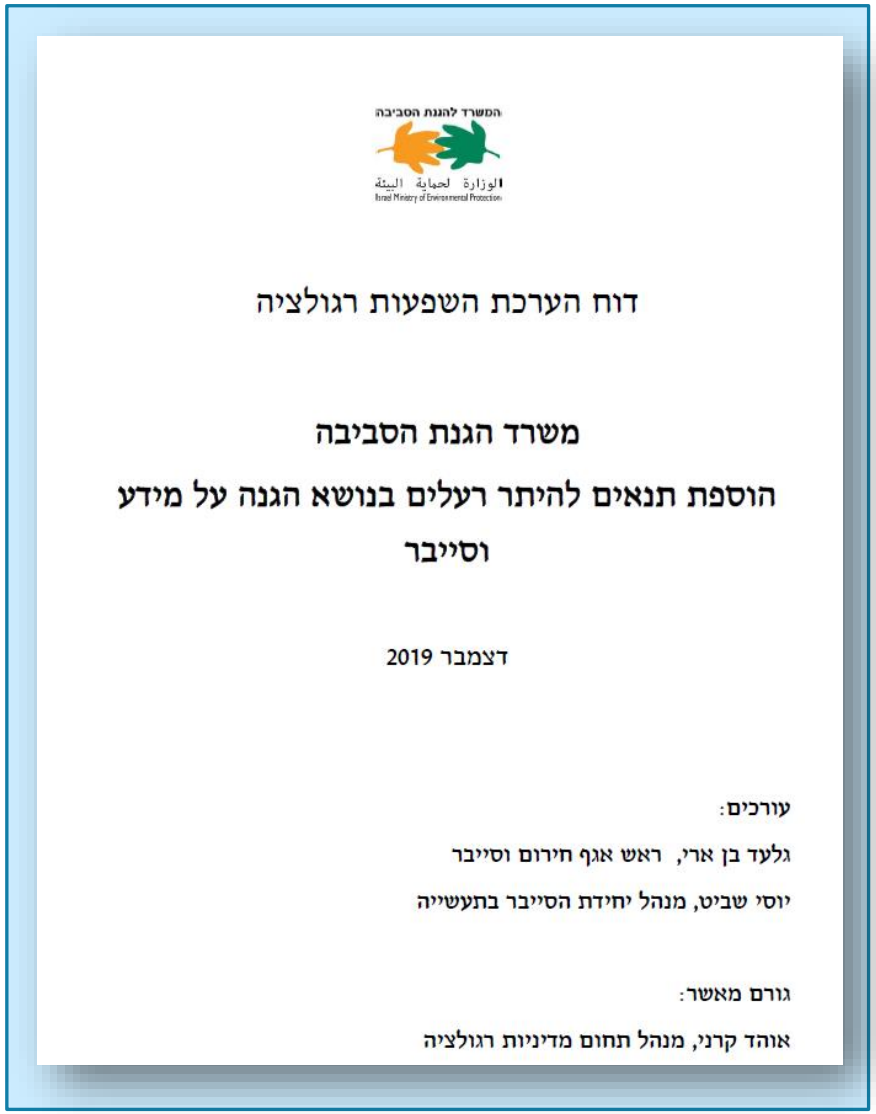
ינואר 2022 – אישור להחלת רגולציה ל-1000 מפעלים נוספים ברמות היתר A ו- B

תחזית תוספת תנאי סייבר
להגנת סייבר במפעלים
לאורך השנים 2022 – 2032

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

דו"ח RIA

RIA = Regulatory Impact Assessment



המשרד להגנת הסביבה
الوزارة لحماية البيئة
Israel Ministry of Environmental Protection

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

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

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

כלים לישום הרגולציה מדריך הסייבר לתעשייה גירסא 1.3

עבודת שטח מעמיקה
סקרי סיכונים במפעלים

NIST CSF
1.1

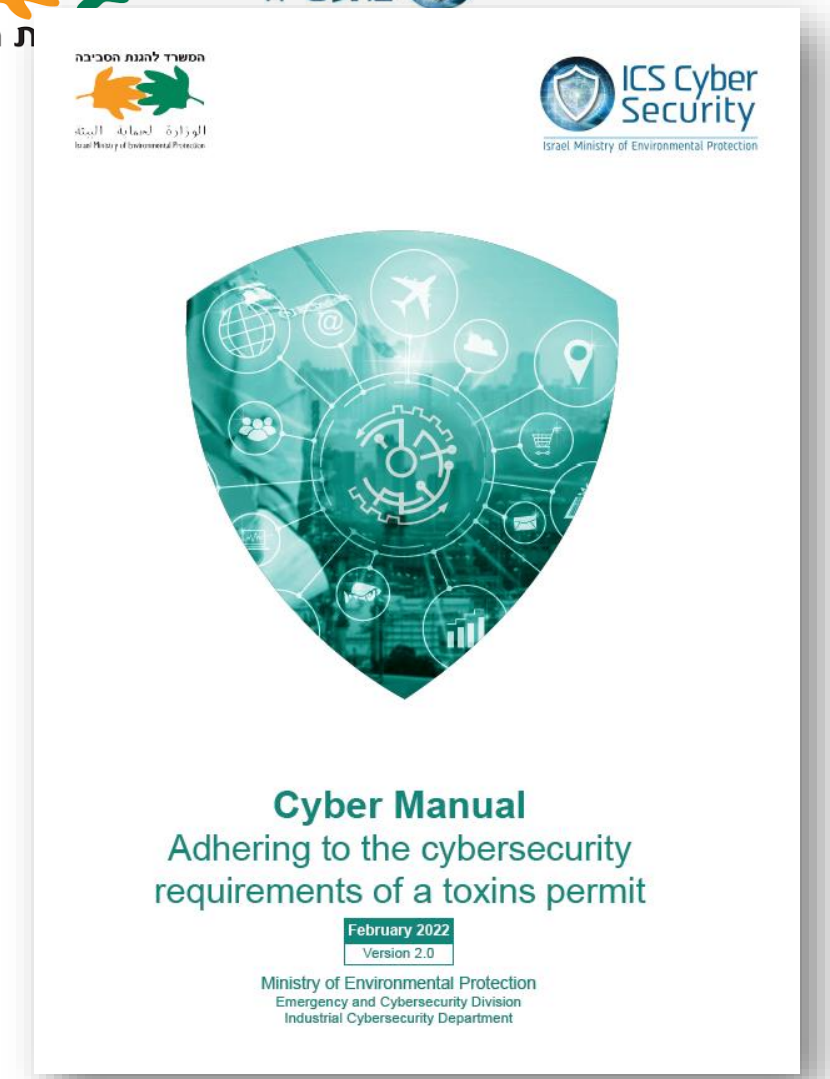
https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit

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

פעילות בינלאומית

תורגם לאנגלית לבקשת ארגון ה-OECD

המתודולוגיה הפכה לתקן מחייב למפעלים שמקבלים רגולציה
הוצג פיסית במדינות הבאות:



אירופה
כנס בנושא סייבר במערכות ICS בלונדון

אסיה
כנס בנושא סייבר במערכות ICS בסינגפור

אמירויות
כנס Cyber-Tech Global Dubai 2021 בדובאי

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

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

2022 – הרחבת רגולציה

המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

מדריך סייבר גירסא 2.0

רגולציה לכל מפעלי A , B
1000 מפעלים

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

מה עושים עם רגולטורים משיקים??

מערך הסייבר הלאומי – רגולטור של תמ"ק (תשתית מדינה קריטית)

משרד הבטחון מלמ"ב – רגולטור תעשיות ביטחוניות

משרד התחבורה – נמלים, שינוע

משרד האנרגיה – תחנות כוח פרטיות

רשות המים – מתקני התפלה, מט"שים

משרד הבריאות – בתי חולים

משרד החקלאות – לולים מבוקרים

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

גופי תמ"ק – מערך הסייבר הלאומי

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, CISO, CISM, CDPSE, CC Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

תכניות מרכזיות לשנת 2023

הגנת סייבר למשנעי חומ"ס

- סקירת חשיפות סייבר במשנעי חומ"ס
- סקירת פתרונות סייבר למשנעים
- פיתוח מתודה להגנת סייבר למשנעי חומ"ס
- כתיבת רגולציה להגנת סייבר במשנעי חומ"ס

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

תכניות מרכזיות לשנת 2023

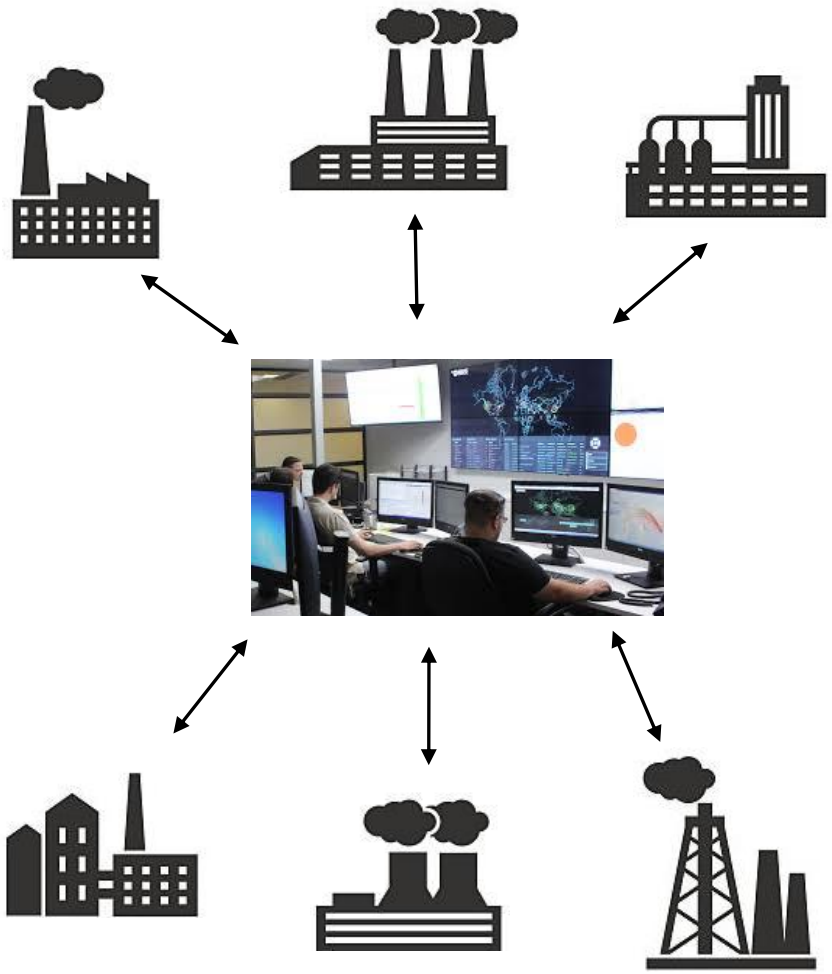
הרחבת פעילות הגנת סייבר בלולים מבוקרים

- פרסום מתודולוגיה שפותחה בקרב חוואים
- ביצוע מספר פיילוטים בלולים מבקרים
- הרצאות מודעות לחוואים בשיתוף משרד החקלאות

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

פעילות לא רגולטורית מול מפעלים

שנת 2023 הקמת מק"מ (מרכז קיברנטי מגזרי)



- שיתוף ידע ומידע בין מפעלים, מידע מודיעיני ומידע אודות מתקפות קיימות למניעת התפשטות מתקפה
- שיתוף ניסיון ותובנות להתמודדות עם אירוע קיים
- בניית מאגר ידע מקצועי של טיפול באירועים מורכבים
- 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, CISO, CISM, CDPSE, CC Information Security & Cyber Expert
Cellular: 058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

שאלות ותשובות