



אסדרת הגנת סייבר בהיתרי רעלים



יעקב דולמצקי

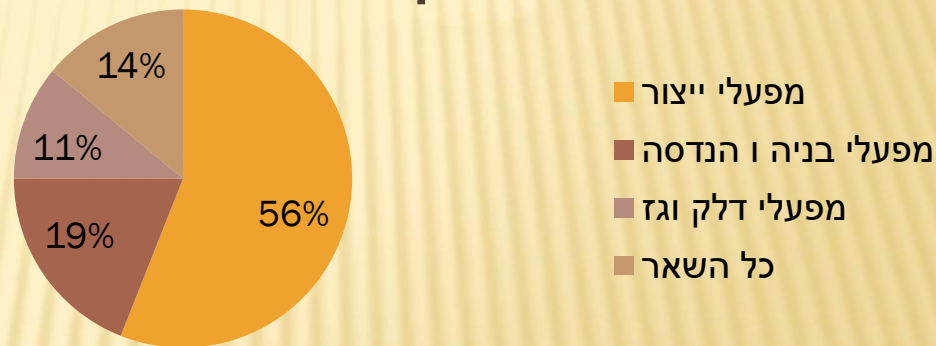
מנהל יחידת הגנה על מידע וסייבר בתעשייה

המשרד להגנת הסביבה



מדגם הנתונים לסקר

הסקר כלל 21 מדינות ברחבי העולם
359 מפעלים בסקטורים הבאים:



שליש מהמפעלים גדולים (מעל 5000 עובדים)
כשני שלישי מהמפעלים בגודל בינוני עד גדול (1000 עד 5000 עובדים)
ה-14% המכילים את "כל השאר" כללו: ממשלה, סקטורים ציבוריים, בתי חולים.



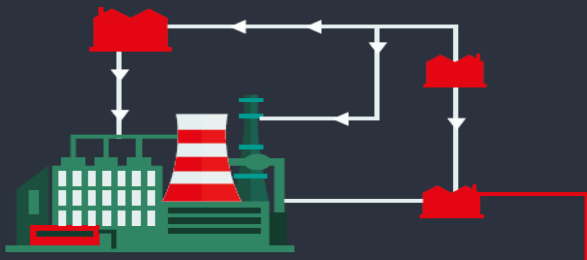
נתוני 2017 בתעשייה



54% ממפעלי תעשייה חוו לפחות התקפת סייבר אחת ב-12 חודשים האחרונים



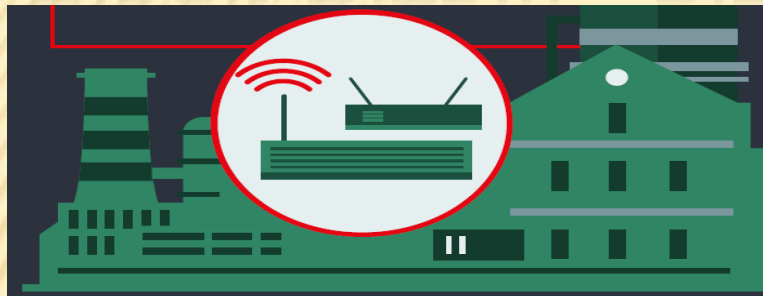
74% מהנשאלים מאמינים כי התקפת סייבר במערכות הבקרה שלהם היא רק עניין של זמן



55% מודים כי לשרשרת האספקה ישנה גישה חופשית לרשת הבקרה של



סייבר במפעלים - עובדות נוספות



81% מהמפעלים משתמשים באינטרנט
אלחוטי ברשת הבקרה התעשייתית

שלהם



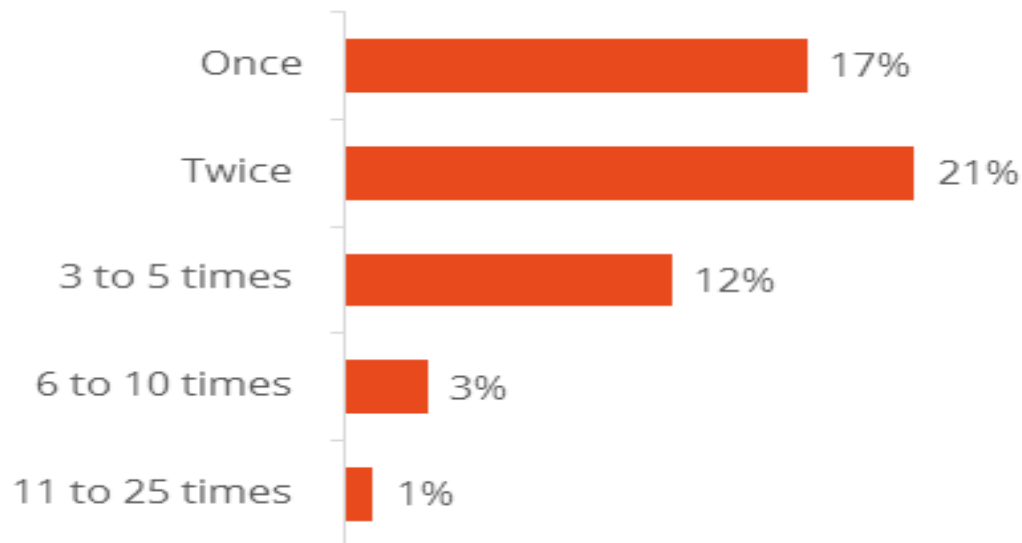
50% מהנשאלים הצהירו כי
קשה מאד לגייס אנשי סייבר
בעלי כישורים מתאימים



60% מהמפעלים אשר לא מאפשרים גישה
לשרשרת האספקה לרשת הבקרה התעשייתית
לא חווים אירועי אבטחת מידע ברשת זו.



54% ממפעלי תעשייה חוו לפחות התקפת סייבר אחת ב-
12 חודשים האחרונים





ציר זמן - אירועים במערכות תעשייתיות

1992

אירוע חומ"ס
בחברת
Chevron

2000

אירוע
סביבתי ב-
Maroochy
Shire
(Vitek
Boden)

2003

הווירוס
Slammer
השבתת
פעילות של
הכור ב-Ohio

2010

הווירוס
Stuxnet
משבית את
המפעל
בנתנז, אירן

2016

מתקפת
סייבר נגד
תשתית
החשמל
באוקראינה

2017

וירוסים
WANNACRY
PETYA ו
השביתו
תעשיות
רבות בעולם



האקרים. עם מי התמודדנו בעבר?



Kevin Poulsen

ידוע בכינוי Dark Dante
פרץ רשתות טלפוניות בארה"ב
נעצר אתרי גניבת מידע
ממסדי נתונים מסווגים



Jonathan Joseph James

הצליח לפרוץ רשת NASA
נשפט כאשר היה בגיל בן 16

אהוד טננבאום שכונה האנלייזר - פרץ למחשבים של נאס"א, הפנטגון, הכנסת, והצבא. הוסגר לארה"ב אחרי גניבה של 10 מיליון דולר.



Ryan Cleary

מקבוצת פצחנים שחורים LulzSec





והיום אנחנו מתמודדים ...





סייבר טרוק: יעדים

- חשמל
- מים
- תעשייה, לרבות תעשייה כימית ופרמצבטית
- גופי תקשורת
- תחבורה
- בתי חולים ומוסדות רפואיים
- מוסדות ממשלתיים
- מוסדות פיננסיים





ואם אין מסגרת אבטחת מידע?



אולי זה לא נורא?



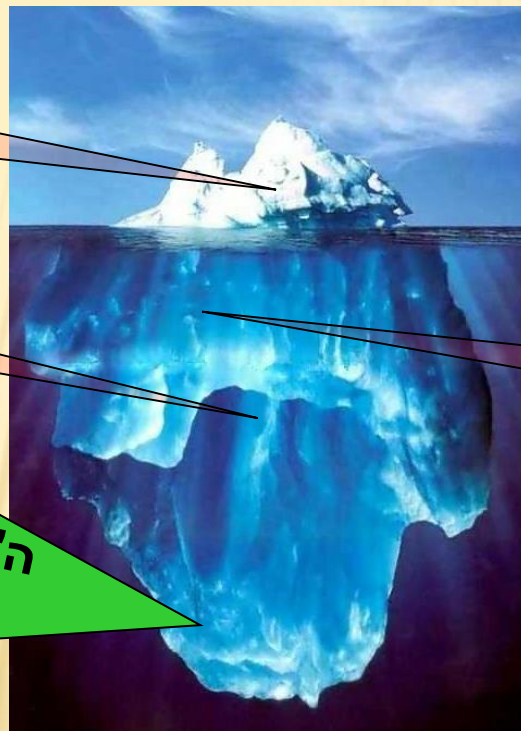
אפקט הקרחון

"אין ברירה, חייבים
לטפל"

"אין מה לטפל במה שלא
קיים..."

"איזה מזל שלא קרה
דבר... אפשר
להמשיך..."

ה"גישה הפרואקטיבית"
פועלת כאן





שורש הבעיה...

היעדר מסגרת ניהול להגנה על מידע וסייבר

בת היענה

מתנערים מהאחריות



סוכריות M&M

קשה מבחוץ, רך מבפנים



כיבוי שריפות

באים לעבודה,
ומטפלים בשוטף





נזקים אפשריים

הרגולציה של המשרד להגנת הסביבה

האינטרס של בעלי העסקים ליישם את הרגולציה



- סיכון מעשי לחיי האדם או לבריאות הציבור
- נזקים משמעותיים לסביבה
- פגיעה בביטחון המדינה
- פגיעה בהמשכיות עסקית/תפקודית
- פגיעה בתפוקה מרבית
- פגיעה באיכות הייצור
- גרימת נזק כספי
- אובדן בטיחות
- אובדן אמינות
- אובדן זמן
- ריגול עסקי - פגיעה בתחרותיות
- אובדן מידע חיוני
- נזק תדמיתי - אובדן או נטישת לקוחות
- עלויות שיקום



2 החלטות ממשלה בנושא הגנת הסייבר

- החלטת ממשלה 2443 בנושא קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר

- החלטת ממשלה 2444 בנושא קידום ההיערכות הלאומית להגנת הסייבר



על בסיס שתי ההחלטות, יחוקק במדינת ישראל חוק הסייבר.



החלטת הממשלה: הכוונה והנחיה מקצועית בתחום הגנת הסייבר בהתאם לסמכויות הרגולציה המופעלות על ידי המשרד הממשלתי או במסגרתו.

כל הזכויות שמורות - המשרד להגנת הסביבה ©

חוק החומרים מסוכנים, התשנ"ג-1993¹

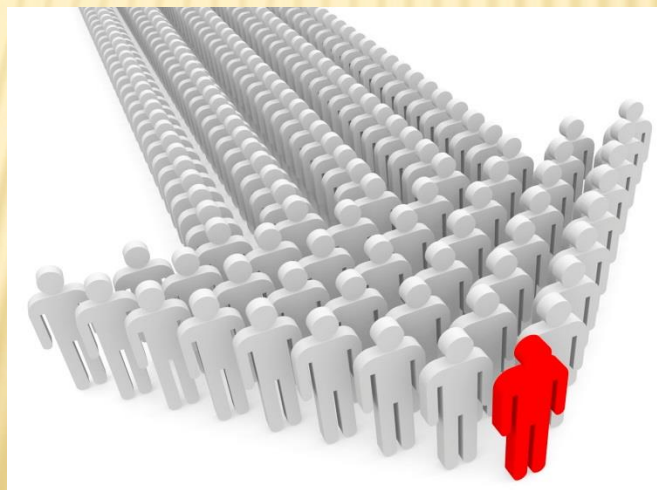
<p>1. בחוק זה - "חומר מסוכן" - רעל או כימיקל מזיק; "אירוע חומרים מסוכנים" - התרחשות בלתי מבוקרת או תאונה, שמעורב בה חומר מסוכן, הגורמת או העלולה לגרום סיכון לאדם ולסביבה, לרבות שפך, דליפה, פיזור, פיצוץ, התאיידות, דליקה; "גוף הצלה" - (נמחקה); "כימיקל מזיק" - כל חומר מן החמרים המפורטים בתוספת הראשונה,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

בצורתו הפשוטה ובעיניו מפורטת או ממוינת בחמרים אחרים:



כפיפות

- א. היחידה פועלת בכפיפות למשרד להגנת הסביבה. ✘
- ב. היחידה פועלת בהנחיה מקצועית של הרשות הלאומית להגנת הסביבה. ✘





מטרת היחידה

הפחתה ומניעה של סיכונים סביבתיים וסיכונים לבריאות הציבור ולחיי אדם, באמצעות צמצום סיכוני סייבר במערכות ממוחשבות התומכות בתהליכים העוסקים בחומרים מסוכנים.





יישום דרישות בהיתר הרעלים

2018 הוספת דרישות הגנה בסייבר ל-60 מפעלים





מי יקבל את התוספת בתנאים להיתר הרעלים?

- × שנת 2018 - המפעלים המסווגים ברמה A בהתאם למדיניות מרחקי הפרדה של המשרד להגנ"ס
- × שנות 2019-2020 - שאר המפעלים המסווגים ברמה A
- × החל מהשנה 2021 מפעלי חומ"ס המסווגים ברמות B ו C




היתר רעלים - איר זה יעבוד?

המחוקק
המשרד להגנת הסביבה
אגף חירום
יחידת הגנה על
פרדס וסייבר
במקסימה

המשרד להגנת הסביבה
الوزارة لحماية البيئة
Israel Ministry of Environmental Protection

הוראות לעמידה בתנאי היתר רעלים בתחום ההגנה על מידע
וסייבר גרסה 0.9



2017

ניתן לשלוח את הערותיכם לטיוטת
המסמך עד 31.03.2018 לכתובת
בדואר אלקטרוני:
cyber_industry@sviva.gov.il



איר זה יעבוד?





הצהרת מחויבות הנהלה

- ✘ בעל הארגון / דירקטוריון / הנהלת הארגון יגבש הצהרת מחויבות של הנהלת הארגון בנושא הגנה על סייבר
- ✘ ההצהרה תכלול מחויבות הנהלה בנושאים הבאים:
 - ✘ מינוי ממונה הגנה על מידע וסייבר
 - ✘ ביצוע סקרי סיכונים בתחום הסייבר בארגון
 - ✘ הקצאת תקציב ייעודי להגנת הסייבר בהתאם לסיכוני הסייבר הקיימים בארגון
- ✘ בהמשך תגובש מדיניות הגנה על מידע וסייבר על בסיס ההצהרה



מיפוי סטאטוס הגנת סייבר בארגון

- ✘ כל ארגון יגיש מיפוי מצב קיים בתחום הגנה על מידע וסייבר
- ✘ המיפוי ייבנה בפורמט שהוגדר על ידי יחידת הגנה על מידע וסייבר בתעשייה, משרד להגנ"ס בשיתוף עם הרשות הלאומית להגנת סייבר
- ✘ בשלב זה למיפוי תהיה משמעות אינפורמטיבית בלבד ללא השפעה על מתן היתר הרעלים



מיפוי תהליכים מסוכנים

#	שם החומר	מס' בהיתר רעלים	כמות מאושרת בהיתר רעלים	האם נכלל בתהליך שמופעל באופן דיגיטלי/ מחשובי ?	הסבר על התהליך המסוכן (שלבי התהליך, מטרותיו, אופן הביצוע)	פירוט מערכות מחשב/ת הליך דיגיטלי המעורבים בתהליך המסוכן	פוטנציאל פגיעה בבריאות הציבור ובסביבה
1	אמוניה	1	20 טון	כן	תהליך קירור באמוניה	מערכת קירור באמוניה של חברת SIEMENS	1. שחרור אמוניה עקב השבתת המערכת הממוחשבת 2. דליפת אמוניה עקב פתיחת ברזים 3. דליפת אמוניה עקב פיצוץ צנרת
2	גפ"מ	2	8 טון	לא	תהליך ייצור של מוצרי חלב	אין	אין



שאלה	1	2	3	4
הנזק מוערך כאחד או יותר מהקריטריונים להלן:				
מהי מידת הנזק לבריאות ציבור או לסביבה שעלולה להיגרם עקב חשיפת מידע קשה או ממוחשב שנמצא בבעלות העסק? .?	1. פוטנציאל לדליפת חומרים רעילים ללא פגיעה משמעותית בבריאות הציבור 2. פגיעה בסביבה שהיא הפיכה בזמן קצר	1. פוטנציאל פגיעה בבריאות הציבור - PAC 1 2. פוטנציאל לשרפה/פיצוץ חומרים מסוכנים ללא פגיעה בבריאות הציבור. 3. פוטנציאל לפגיעה לטוח ארוך בשטח של 500 מ"ר עד 5000 מ"ר של שמורת טבע / מינים מוגנים בחקיקה. 4. פוטנציאל לפגיעה לטוח	1. פוטנציאל פגיעה בבריאות הציבור - PAC 2 או PAC 3 2. פוטנציאל פגיעה בבריאות הציבור עקב שרפה/פיצוץ של חומרים מסוכנים. 3. פוטנציאל לפגיעה בבריאות הציבור עקב שינויים בתהליך ייצור שלא צוינו בסעיפים 1 ו-2 4. פוטנציאל לפגיעה בבריאות הציבור עקב שינוי מיקום או תנאי אחזקה של חומרים	העסק מוגדר תשתית מחשוב קריטית בהתאם לחוק הסדרת הביטחון בגופים ציבוריים
מהי מידת הנזק				
שייכים				

ציון הערכיות לכל נכס הינו הציון הגבוה ביותר שהתקבל לשלוש השאלות (1-3) $Impact = MAX$. ציון זה גם מכונה העוצמה של הסיכון (מסומן באות א) . הציון מגדיר את פוטנציאל הנזק המקסימלי לארגון מנכס זה.



רמת החשיפה

4	3	2	1	רמת חשיפה <
				פרמטר נבדק v
מעל 50	10-50	5-10	עד 5	1. מספר עובדים החשופים למערכות אדם - מכונה (HMI)
מעל 50	25-50	10-25	עד 10	2. מספר עובדים החשופים למערכות הבקרה התעשייתיות (ICS)
מעל 50	25-50	10-25	עד 10	3. מספר עובדים החשופים לרכיבים בשטח המשפיעים על חומרים מסוכנים (ברזים, וסתיים, שסתומים וכדומה)
נגישות גם לגורמים נוספים	ספקים חיצוניים מזדמנים	ספקים חיצוניים קבועים	רק עובדים פנימיים	4. אחריות הטיפול במערכות אדם - מכונה (HMI)



רמת החשיפה - P (Probability)

ציון החשיפה לכל נכס הינו הציון הממוצע שהתקבל לעשר השאלות
 $P = \text{Average (1-42)}$



דוגמה לביצוע הערכת סיכון

אחר מענה על השאלון הנ"ל עבור כלל הנכסים של הארגון, מתקבלת רשימה כזו:

1	2	3	4	הסתברות(P)/עוצמה (I)
7	10 מערכת ג'	13	16 מערכת א'	4
6	9	12	15	3
5 מערכת ה	8	11 מערכת ב' מערכת ד'	14	2
4	7	10	13	1

$$\text{Risk} = 3I + P$$

שאלה: באיזה מערכת נטפל תחילה??



GAP ANALYSIS

מערכת ייצור חומרים	מערכת קירור באמוניה	בקרה
נדרש לממש	קיים	12.6 אין לחבר התקנים שאינם בקרי סביבת ייצור לרשת בקרי הייצור
יצרן המערכת מתנגת לשינוי בתקשורת נתונים. שינוי מסוג זה יפגע בתפקוד המערכת	קיים	12.10 יש להשתמש בתקשורת אמינה בין ציודי הקצה לבקרים התעשייתיים במידת האפשר
הספק הוחתם על הצהרה	מדובר בספק מחו"ל אשר אין באפשרותנו להחתימו. נבחן את הדרישות אל מול ההסכם הגנרי עמו	6.2 : יש להשתמש בכלים חוזיים ומשפטיים בעת רכישת מערכת מידע או שירות מספקים



שקלול רמת הסיכון של הנכס, עלות הפתרון ומורכבות המימוש

המשאבים בארגון מצומצמים - במה לטפל קודם???
 סדר העדיפויות של יישום הבקורות בתוכנית העבודה ייקבע על-ידי שקלול:

- ✓ רמת הסיכון של הנכס
- ✓ עלות מימוש הפתרון
- ✓ מהירות יישום הפתרון (מבוטא באמצעות גודל העיגול)





תוכנית עבודה ליישום הדרישות המפורטות בהיתר הרעלים

- ✘ כל ארגון יגבש תוכנית עבודה ליישום הדרישות המפורטות בהיתר הרעלים
- ✘ התוכנית תאושר על ידי הנהלת הארגון
- ✘ יישום התוכנית יהיה באחריות הארגון
- ✘ התוכנית תוגש למשרד להגנ"ס בצורה הצהרתית
- ✘ יחידת הגנה על מידע וסייבר בתעשייה, המשרד להגנ"ס תהיה רשאית לבדוק את יישום התוכנית על ידי הארגון



שאלות?