לשכת המהנדסים
האדריכלים והאקדמאים
במקצועות הטכנולוגיים
בישראל

# בטיחות והגנת סייבר עבור מערכות בקרה תעשייתיות


אורי שמאי
ניהול אבטחת מידע וסייבר

אורי שמאי - מנהל ויועץ אבטחת מידע , מתמחה בבדיקות ויעוץ אבטחה , סקרי סיכונים

בשעות הפנאי תמצאו אותי מול גאגטים למינהם,בית חכם / מולטימדיה

CISSP CISM CEH OSCP CCSK CCSA MCSE CNE

ISO27001 Certified Internal Auditor

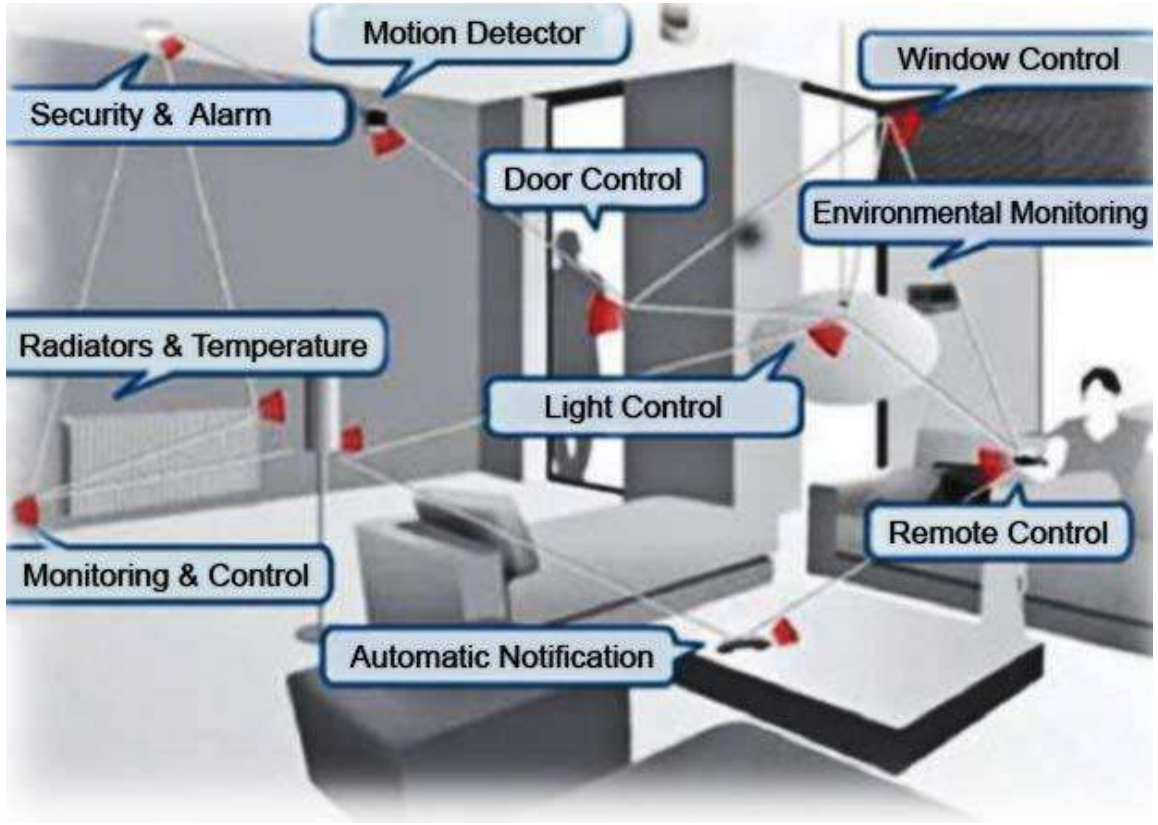
CISO@URISHAMAY.COM
0529594267
https://www.urishamay.com/

**CISO בחברת גדות כימקלים ו WIC מטעם חברת IPV SECURITY**
**ראש תחום אבטחת מידע במכללת גו'ן ברייס – מדייאטק חיפה.**
**מאמן סייבר – צוות לבן – חברת CyberGym**
**מרצה במכללות ובארגונים שונים בתחומי IT ואבטחת מידע .**

052-9594267
ciso@urishamy.com
www.urishamay.com

# IOT


SMART HOME


Motion Detector
Window Control
Security & Alarm
Door Control
Environmental Monitoring
Radiators & Temperature
Light Control
Remote Control
Monitoring & Control
Automatic Notification

200 million Whatsapp messages


2000 hours of video uploaded YouTube

1 billion email’s

15 million Facebook posts

15 million Google searches

220000 photos uploaded to Instagram

2 millions tweet on Twitter


20000  'Things' Added To IoT


Opportunity
Just Ahead


Vulnerability
Just Ahead


# הוירוס הראשון

## מה קורה ביום ממוצע במרחב הסייבר של ארגון

**בכל 24 שניות** מחשב המשרת מחשבים אחרים ניגש לאתר זדוני

**בכל 34 שניות** מורדת תוכנה זדונית (מאלוור) לא ידועה

**בכל 1 דקה** רובוט (תוכנה המדמה משתמש בשיחת ועידה באינטרנט) יוצר קשר עם מרכז הבקרה והשליטה שלו

**בכל 5 דקות** נעשה שימוש באפליקציה בעלת סיכון גבוה

**בכל 6 דקות** מורדת תוכנה זדונית (מאלוור) ידועה

**בכל 36 דקות** מידע רגיש יוצא מחוץ לארגון

מקור: צ'ק פוינט

# סוגי ההאקרים

## מדינה

**המניעים**
- השגת יתרון כלכלי, פוליטי ו/או צבאי

**המטרות**
- מסחר בסמוית
- מידע עסקי רגיש
- טכנולוגיות מתקדמות
- תשתיות קריטיות

**ההשפעה**
- אובדן יתרון תחרותי
- פגיעה בתפקוד חשוב קריטיות

## פשע מאורגן

**המניעים**
- רווח כלכלי מיידי
- איסוף מידע לצורך השגת רווח כלכלי בעתיד

**המטרות**
- מערכות פיננסיות/תשלומים
- מידע אישי, פיננסי, רפואי

**ההשפעה**
- קנסות רגולטוריים כבדים
- תביעות של צרכנים ובעלי מניות
- אובדן אמון הצרכן

## אקטיביסט

**המניעים**
- השפעה פוליטית ו/או שינוי חברתי
- הפגלת לחץ על עסק לשנות את מדיניותו

**המטרות**
- סודות מסחריים
- מידע עסקי רגיש
- מידע שקשור למנהלים, עובדים, לקוחות ושותפים עסקיים

**ההשפעה**
- פגיעה בפעילות העסקית, במוניטין ובמוניטין
- אובדן אמון הצרכן

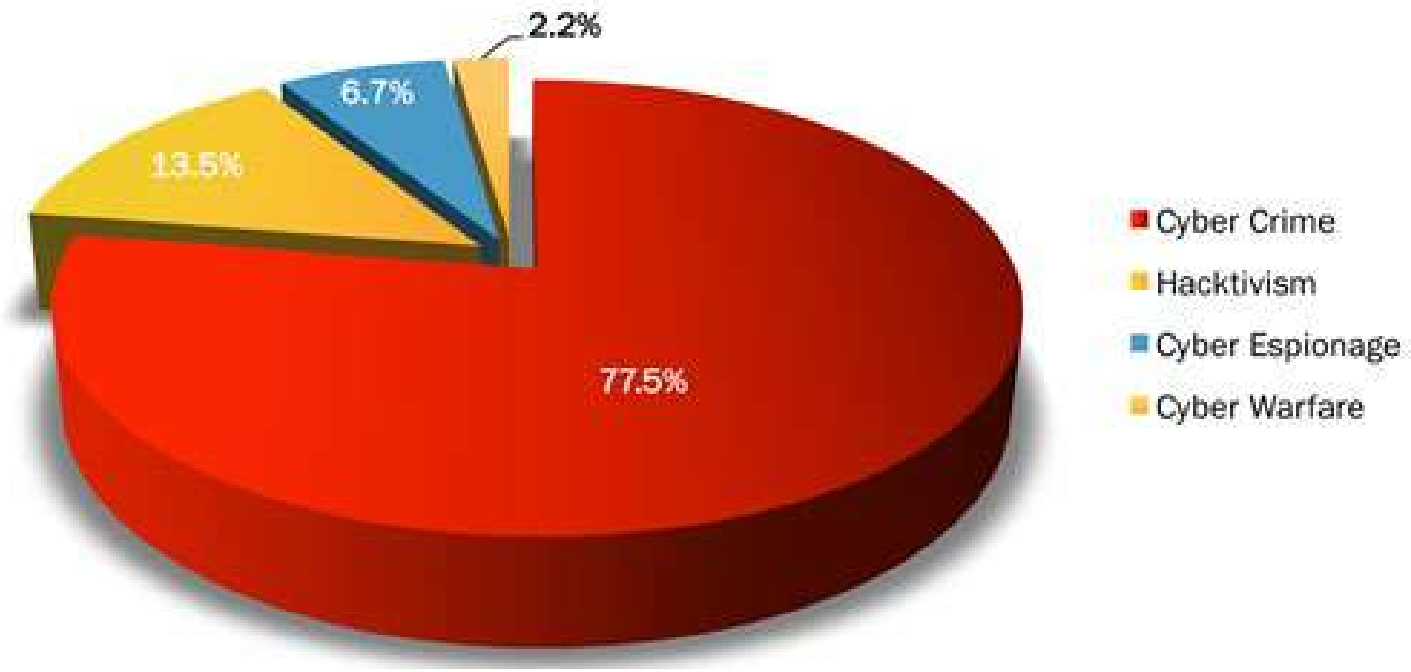
## בעלי עניין

**המניעים**
- יתרון אישי
- רווח כספי
- נקמה מקצועית
- פטריוטיות

**המטרות**
- סביבות, עסקאות, אסטרטגיות שוק, סודות מסחריים, קניין רוחני, מדיה, פעילות עסקית, מידע אישי

**ההשפעה**
- חשיפת סודות מסחריים
- פגיעה בפעילות, במוניטין ובמוניטין
- פגיעה בביטחון הלאומי

# איומי הסייבר




LIVE CYBER THREAT MAP
17,636,160 ATTACKS ON THIS DAY
Canada
VA, United States
Turkey
https://threatmap.checkpoint.com/

# מתקפות סייבר – מהנעשה בעולם

Italian energy giant Enel hit by Windows NetWalker ransomwar

German giant Dussmann Group has become the latest company to fall victim to a ransomware data breach attack, after hackers began posting stolen files to the dark web.

The facilities management multinational, which employs over 66,000 staff worldwide and makes billions of euros in sales annually, appears to have been struck by the Nefilim variant.

The group behind the ransomware began posting over 16,000 files to its dark web site as proof of its efforts, according to @ransomleaks. A screenshot shows the first part of the upload dated Monday with links to the archive, and reveals some personal contact details of the company's executives.

## עשרות ארגונים בישראל תחת מתקפת כופרה

עשרות משרדי עורכי דין ואדריכלים נמצאים כעת תחת מתקפת כופרה, ככל הנראה מהגדולות שידעה ישראל עד כה. מערך הסייבר כופרה, אך מומחים מעריכים כי

Australi NetWall

own after

Software AG.

## REvil Ransomware Hits Jack Daniel's Manufacturer

**Attackers who targeted US spirits manufacturer Brown-Forman reportedly stole a terabyte of confidential data.**

2020.03.27

## ESSILOR: TARGET OF A CYBER ATTACK

Saturday 21 March 2020, Essilor was the target of a cyber , which has temporarily disrupted access to some servers and personal computers.

ditmillion-dollar ransom

after suffering cyberattack

*A reported $10 million was demanded in ransom after the attackers took Xavier services offline*

פוחד, מפני שאתה לא אמור להיות מסוגל לתקוף מרחוק מכוניות"

**תגיות:** קרייזלר, רכב, מתקפת סייבר, סייבר, ג'יפ צ'רוקי

סוכנויות הידיעות

יום חמישי, 23 ביולי 2015, 12:07

3 תגובות


מחשב ראספברי פאי, כמה דקות עבודה – וה-Tesla Model X הנוצצת עברה לשליטה של חוקר אבטחת המידע. המידע התפרסם עכשיו, לאחר שטסלה שחררה עדכון אבטחה

הפורצים - שחדרו לחברת מצלמות אבטחה בעמק הסיליקון - טוענים כי יש להם גישה לשידורים ישירים ממרפאות לבריאות האישה והקלטות ראיונות של שוטרים עם עבריינים ■ הסיבות למעשיהם: "אנטי-קפיטליזם, קמצוץ אנרכיזם - וגם זה כיף מדי כדי לוותר על זה"

1 שמרו קריאת זן

**בלומברג**
ויליאם טורטון
פורסם ב-10.03.21

קבוצת האקרים טוענת כי פרצה ל-150 אלף מצלמות אבטחה, הממוקמות בבתי כלא, תחנות משטרה, בתי ספר, חברות ובתי חולים. הנתונים מאוחסנים בשרתים של חברת מצלמות האבטחה ורקדה (Verkada), היושבת בעמק הסיליקון.

לדברי הקבוצה, בידיהם גישה לשידור החי ממצלמות האבטחה של טסלה

# Ransomware attack at German hospital leads to death of patient

By Lawrence Abrams

September 17, 2020 11:41 AM 3

הידען > מתקפת סייבר חדשה עלולה לגרום למדענים לייצר נגיף ללא ידיעתם

# מתקפת סייבר חדשה עלולה לגרום למדענים לייצר נגיף ללא ידיעתם

אוניברסיטת בן גוריון | דצמבר 21, 2020 | תגובה אחת

**חוקרי סייבר מאוניברסיטת בן-גוריון בנגב מתריעים בפני ...**
**להם לייצר רעלים מסוכנים במעבדותיהם**


EXPERT VOICES OP-ED & INSIGHTS

Home > News

## Hackers Could Kill More People Than a Nuclear Weapon

By Jeremy Straub - North Dakota State University August 27, 2019

Digital attacks can hit many targets at once.

# האקרים פרצו לקזינו - דרך האקווריום

**מכשיר שאמור לשמור על הדגים שלא ימותו שמר קצת פחות על בטחונם של המהמרים הכבדים בקזינו**

יאיר מור | NEXTER | פורסם 17/04/18 12:57

# האקרים פרצו למחשבי קזינו דרך תרמוסטט חכם באקווריום שלו

כנס שנערך בלונדון חשף שתי תקריות סייבר חמורות: בראשונה נגנב מידע על מהמרים כבדים דרך וסת החום של האקווריום, ובשניה נפרצו מערכות בנק דרך מצלמות האבטחה שלו

שירות כלכליסט 16.04.18 21:58

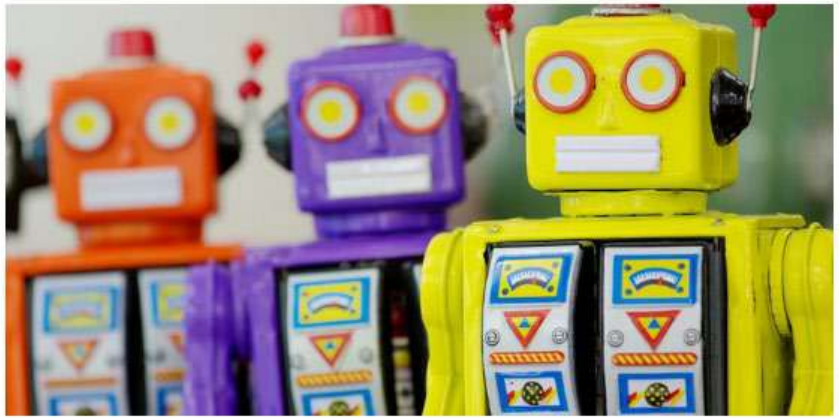
**תגיות:** אינטרנט הדברים | האקרים | קזינו | פריצה לקזינו | סייבר

האקרים הצליחו לפרוץ למערכות קזינו ולהשיג מידע על מהמרים בולטים דרך - האקווריום שלו. התרמוסטט במיכל היה מחובר לרשת של הקזינו, כדי לאפשר שליטה אוטומטית; התוקפים הצליחו להגיע דרכו למסדי נתונים שונים ולמשוך מידע רגיש על הלקוחות.



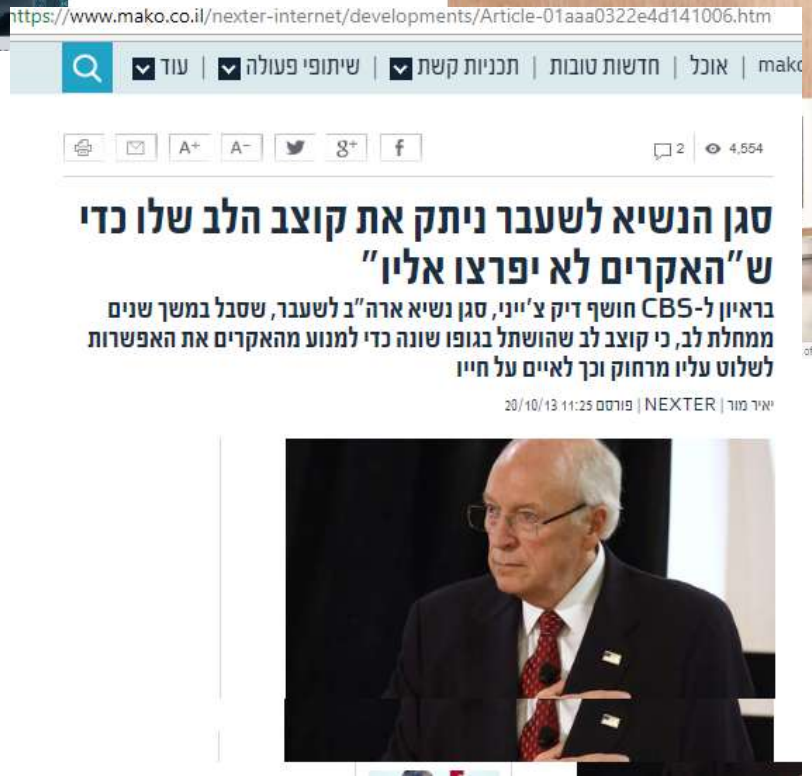
## Connected Children's Toys aren't Cybersafe: R
## Several Serious Vulnerabilities

December 12, 2019 | Malware and Vulnerabilities



- Almost every day a number of devices are reported to have vulnerabilities. Today it is children's connected toys.
- Several security flaws including lack of authentication for device pairing were found in toys sold this holiday shopping season.

uter-internet-security-news Group and a consumer group 'Which?' together tested the

קורונה בעולם

## מתקפת סייבר על רוסיה ואוקראינה, טיסות עוכבו

מקור המתקפה עדיין אינו ידוע
צילום: shutterstock

כלי תקשורת ברוסיה הושבתו, בנמל התעופה באודסה דחו טיסות וברכבת התחתית של קייב התקשו לשלם במכונות האוטומטיות. מי אחראי להפצת הווירוס BadRabbit?

סוכנויות הידיעות פורסם: 20:35 , 24.10.17

שתף בפייסבוק
הדפסה
שלח כתבה
תגובה לכתבה

מתקפת סייבר באמצעות תוכנה זדונית המכונה BadRabbit פגעה היום (ג') באוקראינה וברוסיה. היא גרמה לדחיית טיסות בנמל התעופה בעיר אודסה שבאוקראינה ושיבשה את עבודתם של כמה כלי תקשורת ברוסיה, בכלל זה סוכנות הידיעות המפורסמת "אינטרפקס".

נראה שמדובר באחת ממתקפות הסייבר הגדולות ביותר מאז מתקפת NotPetya ביוני – מתקפה שאוקראינה הייתה הראשונה שנפגעה בה, אך אחריה נפגעו מדינות רבות נוספות.

מרחבי הרשת
Sponsored Links by Taboola


# ה"ב: תורים ארוכים לתחנות דלק בעקבות מתקפת סייבר על
# ור נפט

ת המתקפה שהתחילה ביום שישי האחרון, ותחנות דלק רבות בחוף המזרחי ובדרום ארה"ב הולכת ומידלדלת.
רת האנרגיה מנסה להרגיע את הרוחות, ומפצירה באמריקנים לא לאגור דלק מיותר לחינם

קוגוסובסקי | 12/05/2021

שיתוף

# האיומים מתוחכמים יותר..


## האם האקרים יכולים לפרוץ לקוצבי לב ומשאבות תרופות?

מחקרים חדשים מראים שתעשיית המכשור הרפואי לא מצליחה להתמודד עם בעיות סייבר - ושרק אחוזים בודדים מהיצרניות מבצעות סקרי אבטחה קבועים. ואולם, המצב בישראל טוב מבשאר העולם והסבירות לפריצה נמוכה

רפאל קאהאן 28.05.17 13:07

דיגיטל digital

## ילד בן 11 פרץ לדובון צעצוע בכנס סייבר

הילד והדובון
צילום: מתוך טוויטר

רובן פול, תלמיד כיתה ו' מאוסטין שבטקסס, והדובון "בוב" היממו את מאות המומחים בתחום אבטחת הסייבר במהלך כינוס בהולנד. וזה לא היה הדבר היחיד שהוא פרץ

Recommend 27

ynet פורסם: 18.05.17 , 07:27

ילד אמריקני בן 11 הדהים השבוע קהל של מומחי אבטחת מידע כשהצליח לפרוץ למכשירי הבלוטות' שלהם ולבסוף לערוך מניפולציות בדובון רובוטי - וכך הוכיח למעשה שצעצועים חכמים ומקושרים "יכולים להפוך לכלי נשק" תחת הידיים הלא נכונות.

שתף בפייסבוק

הדפסה

## מומחים: התקפת הסייבר נעשתה דרך מוצרי בית חכם

אילוסטרציה
צילום: Shutterstock

יום אחרי המתקפה שהשביתה את האתרים הגדולים בעולם, מעריכים חוקרי אבטחה כי ההאקרים הצליחו לחדור לשרתי חברת Dyn דרך מכשירים מקבוצת הבית החכם - מצלמות רשת, ראוטרים וסטרימרים. בין הנפגעים: טוויטר, נטפליקס ופייפאל

גיא לוי פורסם: 22.10.16 , 08:43

שתף בפייסבוק

## הרכב החכם יזדקק להגנה חכמה מפני מתקפות סייבר

מאת אבי בליזובסקי חמישי, 23 יולי 2015 00:44

לא צריך להיות נביא כדי לנחש מה יוכל האקר לעשות אם ישתלט על מכונית. הוא יוכל למשל לדרוש מהנהג כופר כדי שיוכל בכלל להפעיל את המכונית, שלא לדבר על דברים יותר חמורים שבהם מכונית יכולה לשמש ככלי נשק.

חברת ארגוס (ARGUS) פיתחה מערכת שתגן על הרכב המקושר. עופר בן נון, יזם ומנכ"ל ארגוס תיאר את הבעיה והפתרונות לה במפגש

# INFORMATION TECHNOLOGY (IT) VS. OPERATIONAL TECHNOLOGY (OT)

## IT

Data and the flow
of digital information

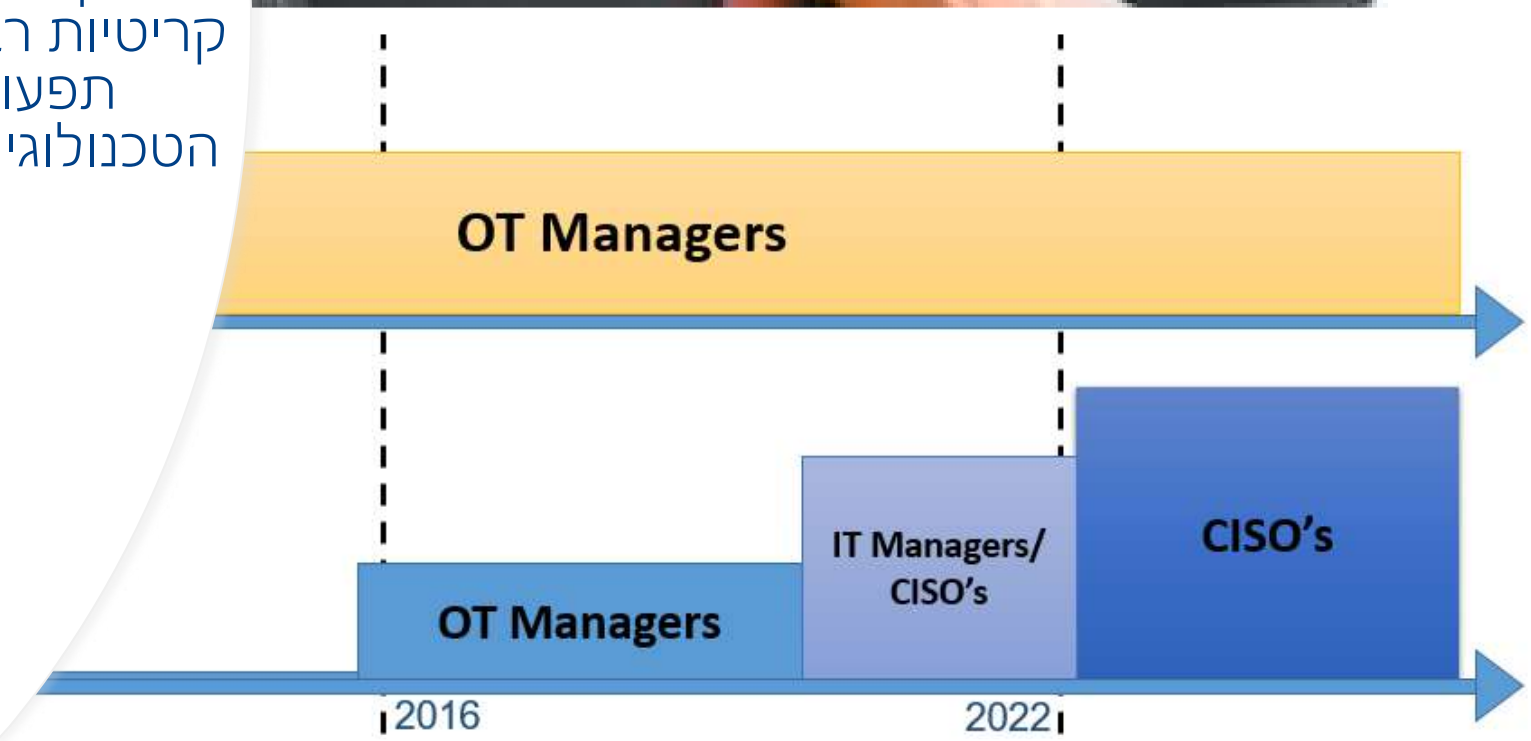
## OT

Operation of physical processes
and the machinery used
to carry them out

Coolfire

מערכות אלו נמצאות במגוון מגזרים עתירי נכסים ,
ומבצעות מגוון רחב של משימות ,החל בניטור תשתיות
ועד לשליטה ברובוטים בקומת ייצור .שירותי חירום ,
מתקני התפלת מים ,תחנות כוח ,בתי זיקוק ותשתיות
קריטיות רבות אחרות מסתמכות על פתרונות טכנולוגיים
תפעוליים לפעול כראוי ולעמוד בביקוש .סביבת
הטכנולוגיה התפעולית מורכבת בעיקר ממערכות בקרה
תעשייתיות

ICS – Industrial Control Systems .



| | |
|---|---|
| ICS | Industrial control system |

שם כללי לסוגים שונים של מערכות שליטה ובקרה תעשייתיות

| | |
|---|---|
| SCADA | Supervisory control and data acquisition |

מערכת בקרה ופיקוח מרכזית בתעשייה ותשתיות, לרוב שולטת ברכיבים רבים ובמספר אתרים

| | |
|---|---|
| PLC | Programmable logic controller |

בקר תעשייתי שמחובר לחיישנים ומציג מהם נתונים

# APT – STUXNET

מה שסייע להשגת מודיעין על המחשבים היו תמונות מביקור של נשיא איראן דאז ,מחמוד אחמדינג'אד ,במתקן בנתנז .בתמונות נראים בבירור המחשבים ,התצורות שלהם והחיבורים האחוריים שלהם . לימים נקודות הכניסה והיציאה האלה שימשו להחדרת הוירוס...

# APT – STUXNET

Figure 5: Operators in front of the SCADA displays of the Cascade Protection System, placed right

Figure 9: President Ahmadinejad holding a carbon fiber centrifuge rotor during his 2008 press tour at Natanz. This rotor is for the next-generation IR-2 centrifuge. Rotors used in the


The above picture shows another view of the PFEP's control room, with MIT graduate and thenpresident of the Iranian Atomic Energy Organization Ali Akbar Salehi at the keyboard,


**Pressure controller & readout**


# ארה"ב: איראנים חדרו למחשבי סכר בניו-יורק

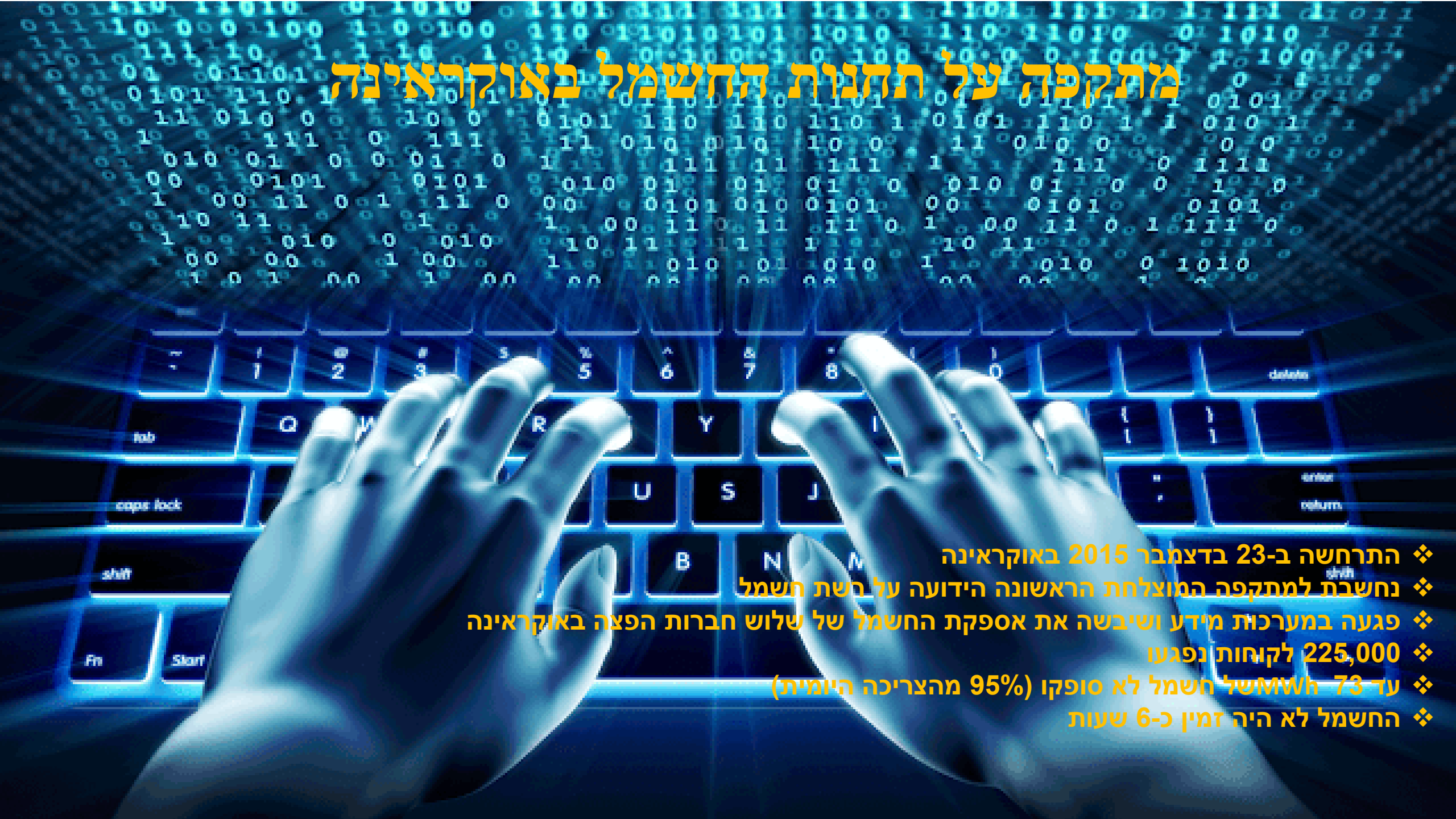
**ה"וול סטריט ז'ורנל" חשף כי ב-2013 הצליחו האקרים מהרפובליקה האסלאמית לפצח את מערכות ההגנה של תשתיות אזרחיות אמריקאיות, וציין כי הדבר מעיד על החולשה בתחום**

רויטרס | 21/12/2015 16:45

**תגיות:** האקרים, איראן, ארה"ב,סכר

פצחנים (האקרים) איראנים פרצו למערכות השליטה של סכר ליד העיר ניו-יורק ב-2013, בחדירה שהעלתה את החשש מפרצות אבטחה בתשתיות של ארה"ב – כך דיווח הבוקר (יום ב') ה"וול סטריט ז'ורנל", שציטט לשם כך בכירים אמריקאים בעבר ובהווה.

# מתקפה על תחנות החשמל באוקראינה



- התרחשה ב-23 בדצמבר 2015 באוקראינה
- נחשבת למתקפה המוצלחת הראשונה הידועה על רשת חשמל
- פגעה במערכות מידע ושיבשה את אספקת החשמל של שלוש חברות הפצה באוקראינה
- 225,000 לקוחות נפגעו
- עד 73 MWh של חשמל לא סופקו (95% מהצריכה היומית)
- החשמל לא היה זמין כ-6 שעות

# דוח אבטחת SCADA: עליית מדרגה במתקפות

פוטנציאל הנזק במתקפת סייבר על מערכות בקרה תעשייתיות גדול לעין ערוך בהשוואה למתקפה על מערכות IT. סקירת מספר מקרי תקיפה בשנה החולפת מלמד כי התוקפים כיום מראים התעניינות רבה יותר בהתקפות ממוקדות – בין אם בצורה ישירה או עקיפה – על מערכות בקרה תעשייתיות. לכן, זהו זמן טוב להעריך היכן אנחנו עומדים ביחס להגנה על המערכות הללו

רוחנה ניגאם, חוקרת אבטחה במעבדות FortiGuard, פורטינט 10.11.16 09:04

**תגיות:** פורטינט SCADA FortiGuard התקפות סייבר פישינג סייבר אבטחת מידע

מערכות בקרה תעשייתיות (Industrial Control Systems), הידועות גם בכינוי מערכות SCADA, הן מערכות ממוחשבות אשר מבקרות ומפקחות על תהליכים פיזיים כמו הולכת חשמל, שינוע של גז ושמן דרך הצינורות, אספקת מים, הפעלת רמזורים ומערכות אחרות המשמשות כבסיס של החברה המודרנית.

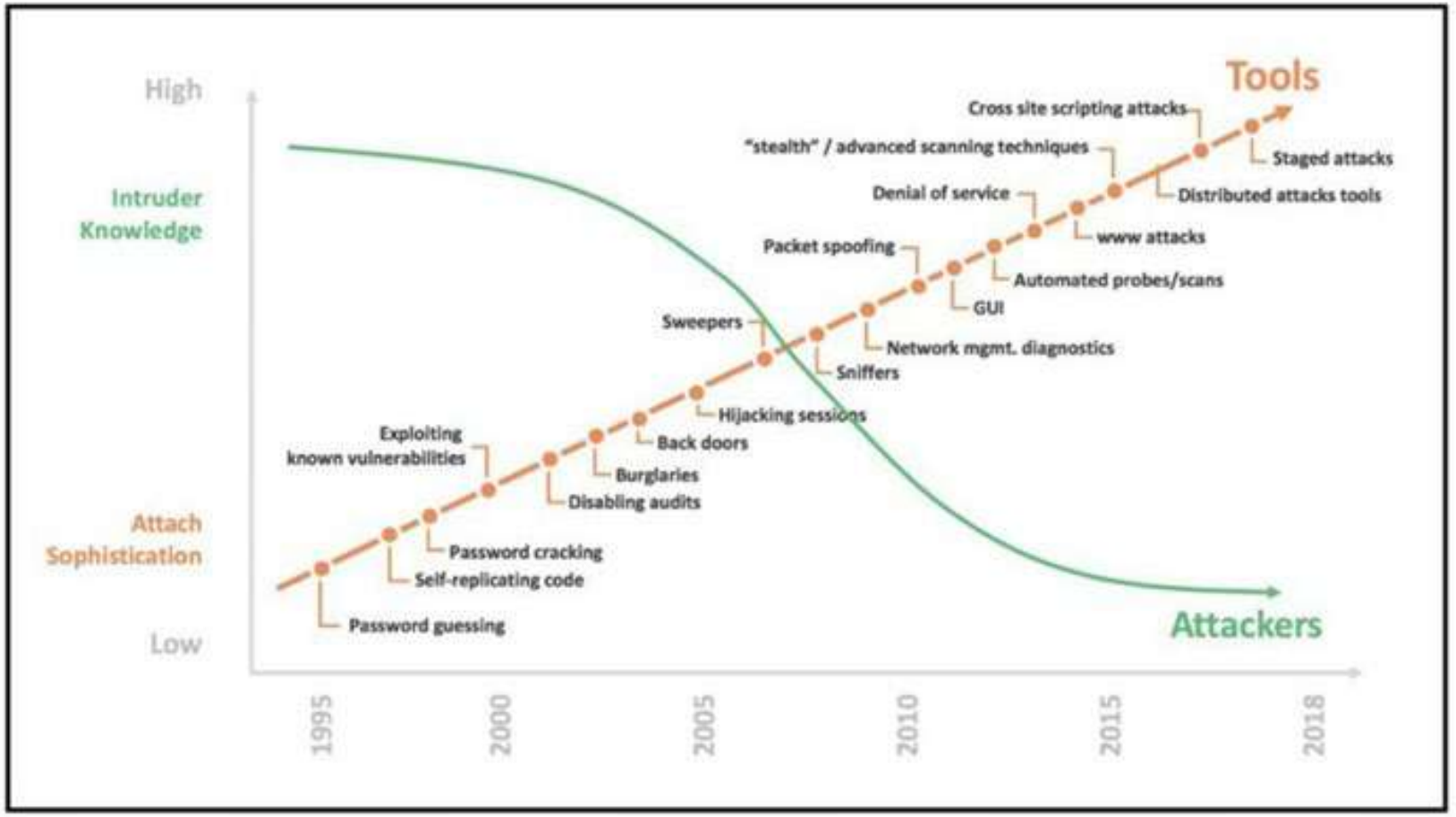
בשנים האחרונות נמצאות מערכות הבקרה הללו – שבהן תלויות מרבית התשתיות הקריטיות ותעשיית הייצור שלנו – נתונות תחת התקפות סייבר מתוחכמות באופן תדיר.


## השפעת אירוע סייבר על יעדים תפעוליים ועסקיים

התממשות סיכון סייבר בסביבת OT עלולה לפגוע באחד או יותר מהיעדים התפעוליים והעסקיים של הארגון:

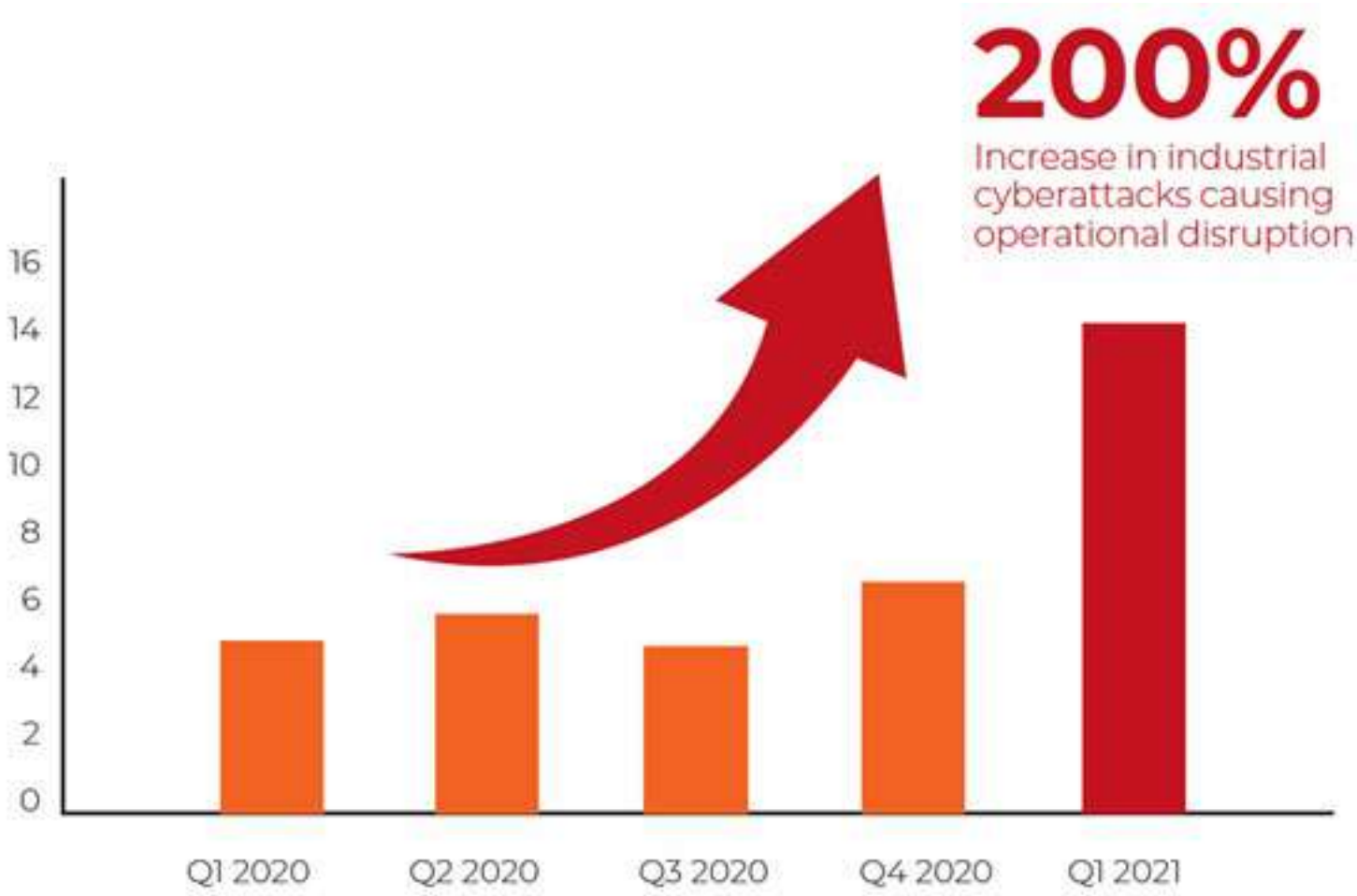
- **בטיחות עובדים** – לדוגמה, כתוצאה מניצול ערוץ גישה ושליטה מרחוק לטובת שיבוש הגדרות בבקר תעשייתי המוביל לפיצוץ דוד קיטור.
- **הגנת הסביבה** – לדוגמה, שיבוש תפקוד של חיישנים, אשר גורמת הזרמת שפכים עודפת או תהליך כימי בלתי מבוקר הגורם להתפשטות גז רעיל .
- **איכות המוצר** – לדוגמה, שינוי בלתי מורשה בנתוני הייצור עלול לקצר את אורך חיי המדף של מוצר מזון.
- **יעדי ייצור** – נדרש לנהל את סיכוני הסייבר שעלולים לפגוע באופן שלילי ביעדי הייצור. כך למשל השבתת קו ייצור לפרק זמן משמעותי כתוצאה מחדירת נוזקת כופר (Ransomware) עלולה להוביל לפגיעה ביעדי הייצור ובהתחייבויות הארגון מול לקוחותיו.
- **סודות מסחריים** – לדוגמה, דליפת מסמך המתאר את תהליך הייצור הייחודי. ככלל, בשונה מסביבת IT, המיקוד בסביבת OT הוא בשמירה על תקינות התהליך התפעולי והגנה על חיי אדם.

# עליה בפיתוח כלי תקיפה כנגד OT




איור 9: התפתחות כלי התקיפה לסביבות ה-ICS בשנים האחרונות[9]

# עליה בכמות התקיפות ה"מוצלחות"



# פוליטי-מדיני politics



# 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"**


אחד מהמתקנים שהותקפו
צילום: רועי עידן

ynet פורסם: 01.06.20 , 03:29




# דיווח: ישראל ביצעה מתקפת סייבר נגד נמל איראני

**גורמי מודיעין אמרו ל"וושינגטון פוסט" כי ישראל עומדת מאחורי מתקפה ששיבשה את פעילות הנמל למשך כמה ימים. נכתב כי ייתכן שמדובר בתגובה על מתקפת סייבר נגד מתקני המים בישראל, שעליה פורסם לראשונה ב-ynet**

ynet פורסם: 19.05.20 , 03:58

ה"וושינגטון פוסט" דיווח הלילה (בין שני לשלישי) כי ישראל ביצעה מתקפת סייבר נגד המחשבים בנמל שהיד רג'אי שבדרום איראן. המתקפה גרמה לשיבושים קשים בפעילות הנמל למשך כמה ימים. בדיווח נכתב כי ייתכן שמדובר בתגובה על מתקפת סייבר נרחבת נגד מתקנים של תאגידי מים וביוב בישראל בחודש שעבר. על החשד למתקפה זו פורסם לראשונה ב-ynet.
ישראל סירבה להגיב על הדיווח.

בארץ national



# חברת החשמל: כ-20 אלף מתקפות סייבר כל יום

**יו"ר חברת החשמל רון-טל חשף במהלך ועידת הסייבר השנתית כי ביום נתון חווה החברה עד 20,000 ניסיונות לחדור לרשת המחשבים שלה. חלק מזערי מהניסיונות מגיע מכיוון איראן. "תקיפת סייבר מסוכנת יותר מתקיפה נקודתית של טילים"**

שירי הדר פורסם: 04.09.12 , 19:31

**"ביום נתון יש בין 10,000 ל-20,000 ניסיונות לחדור לרשת המחשבים של חברת החשמל "** - כך חשף היום (ג') יו"ר דירקטוריון חברת החשמל, אלוף (מיל') יפתח רון-טל בוועידת הסייבר השנתית שנערכה במכון למחקרי ביטחון לאומי. רון-טל ציין בדבריו כי "מלחמת סייבר היא מלחמה אחת ארוכה ולעומת תקיפה טקטית נקודתית של טילים למשל, תקיפת סייבר הרבה יותר מסוכנת וקשה יותר להתאושש ממנה".

• בחירות בארה"ב 2012 - לכל הכתבות של CNN ו-ynet

יו"ר חברת החשמל הסביר ל-ynet בהתייחסו לנתונים שהציג בוועידה כי "זיהינו ניסיונות חדירה לרשת באמצעות הכנסת וירוס או שליחת אימיילים לא ברורה או הכנסת סיסמאות וכדומה. אנחנו יכולים לדעת די בקלות את מדינות המקור שיכולות להיות גם מדינות מתווכות, אבל לא בהכרח יודעים את המיקום המדויק".

רון-טל הוסיף כי "חמש המדינות שמהן מגיעים ניסיונות החדירה הגדולים ביותר הן ארה"ב, סין, רוסיה, דרום קוריאה וישראל. מאיראן יש מספר ניסיונות חדירה קטנים מאוד באופן יחסי והם נעים בין 100 ל-200 בשבוע".



"לא יודעים את המיקום המדויק". רון-טל


פריצה למערכות שליטה של בריכת שחייה. צילום: BigStock

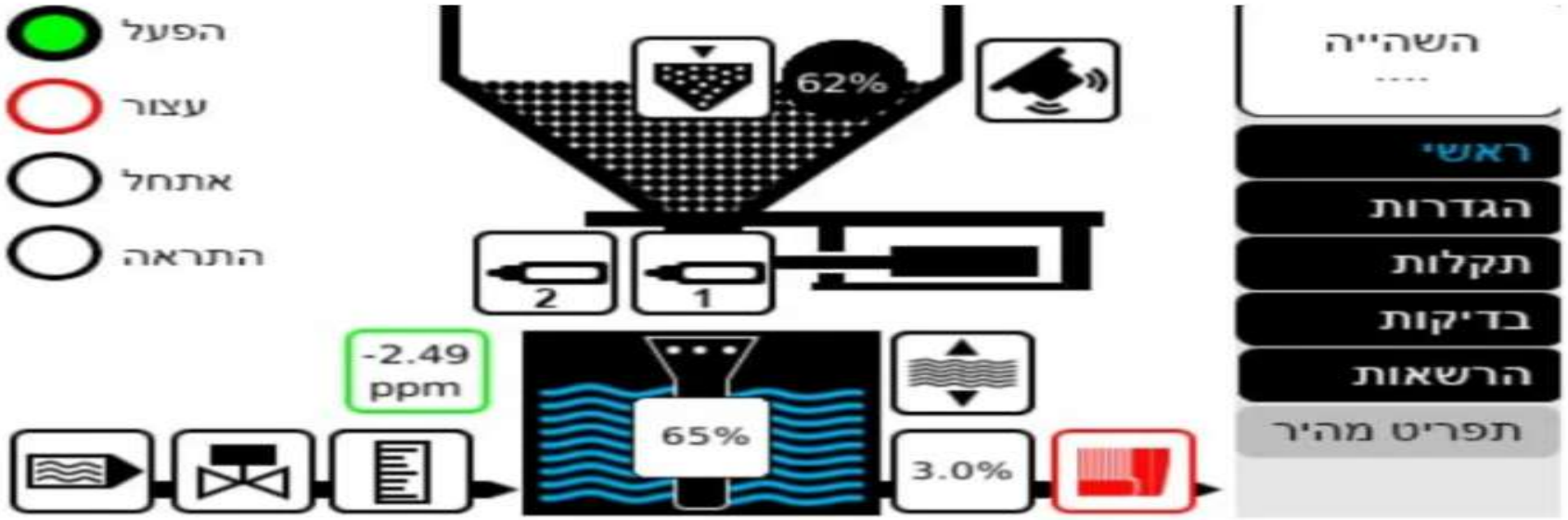
חדשות

# האקרים פרו פלסטינים תקפו בסייבר מערכות בקרה של בריכות השחייה בבית מלון בישראל

מבחינה טכנית, לקבוצת התוקפים הייתה היכולת לשנות את מינוני הכימיקלים בבריכות השחייה, אבל הקבוצה הודיע, כי למרות השנאה למדינה, היא לא מתכוונת לסכן חיי אכן חיי אדם בשלב זה ● לא ידוע על נזק ממשי שנגרם

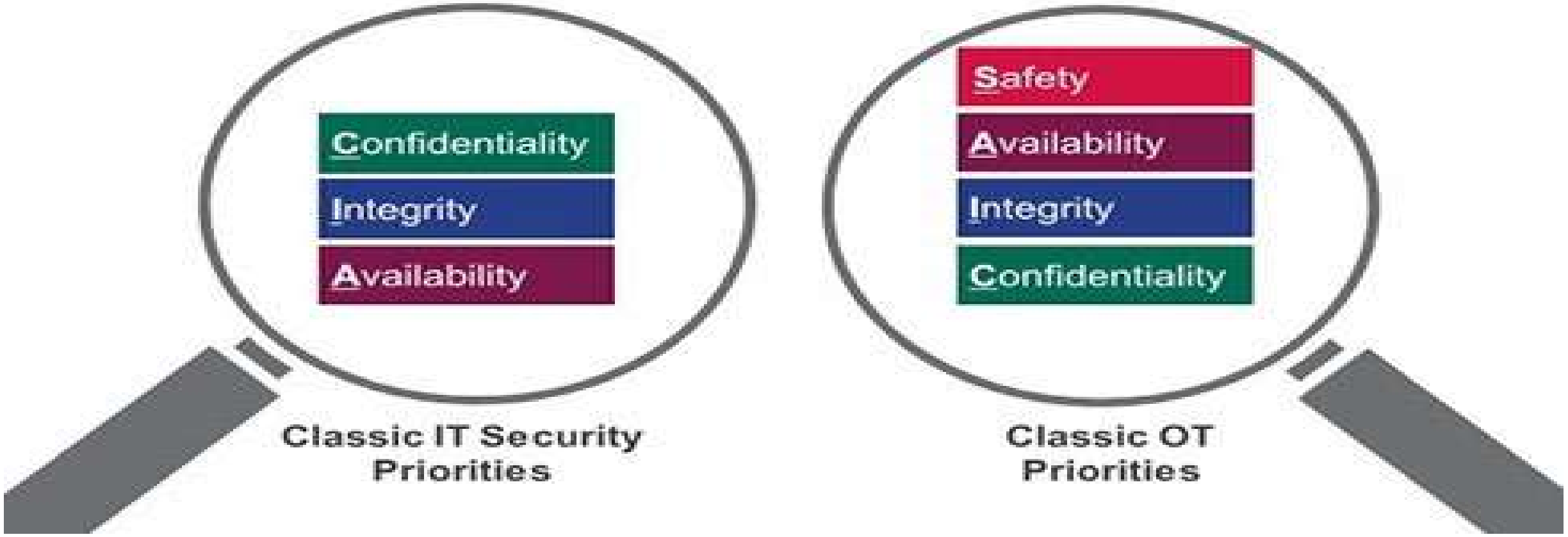

אחרי הביוב באור עקיבא: האקרים שוב פרצו לעשרות בקרים תעשייתיים בישראל
מומחי סייבר אישרו את דבר הפריצה ומזהירים: בקרים תעשייתיים רבים בישראל השולטים במערכות מים ותשתיות לא שודרגו - אין להם אמצעי אבטחה, הגישה פרוצה
שמרו
קריאת זן
כשתעשו מינוי, תבינו
מינוי לאתר הארץ החל מ-4.90 ש"ח בחודש הראשון
לרכישה
62%
השהייה
ראשי
הפעל
עצור
אתחל

ובארץ, האקרים שוב פרצו לעשרות בקרים תעשייתים. קבוצת GhostSec פרסמה השבוע צילומי מסך של ממשק מערכת בעברית לצד סרטון המציג כיצד הם מצליחים לעצור את פעולתו של בקר תעשייתי מתוצרת חברת Berghof Automation.



# מי אחראי ומה ניתן לעשות?

# אבטחת מידע


Confidentiality
Integrity
Availability
Classic IT Security Priorities
Safety
Availability
Integrity
Confidentiality
Classic OT Priorities

# המטרה שלנו:


רציפות תפעולית
שמירה על חיי אדם
שמירה על איכות הסביבה
שמירה על סודות מסחריים
בקרת איכות תוצר


airgap
airgap
airgap
airgap
ICS

# The 10 Operational Technology Security Controls

# מדיניות ואחריות

## מדיניות ממשל סיכוני סייבר

- סטטוס כללי על הגנת הסייבר בארגון והגנת סייבר ב- OT?
- האם מונה בארגון גורם האחראי על הגנת הסייבר של תחום ה-OT ?
- למי כפוף ארגונית, אחראי הגנת הסייבר של תחום ה- OT: לגורם מהתחום התפעולי, לגורם מתחום העסקי או לגורם מתחום הגנת הסייבר?
- האם הוגדרו תחומי סמכותו ואחריותו של האחראי על תחום הגנת הסייבר באופן שיבטיח יישום, אכיפה וניטור אפקטיביים של בקרות הגנת סייבר בסביבת ה-OT ?
- האם הוקנו לגורם האחראי על תחום הגנת הסייבר המיומנות הנדרשת לניהול ויישום הגנת סייבר בסביבת ה- OT?
- האם הוקצו לגורם האחראי על תחום הגנת הסייבר המשאבים והכלים הנדרשים לשם מילוי תפקידו?
- האם גובשו מדיניות ונהלים לתחום הגנת סייבר בסביבת ה-OT?

- האם הארגון מבצע בדיקות חוסן יזומות?
- האם המשאבים המוקצים להפחתת סיכוני סייבר בסביבת OT עונים על צרכי הארגון?
- מהו סטטוס תוכנית העבודה ביחס לסיכונים שזוהו והאם מטופלים בהתאם ללוחות הזמנים שנקבעו?

# מוקדי סיכון סייבר אופיינים לרשת OT

- האם קיימת הפרדה בין מערכות תפעול למערכות מנהלתיות וקישור לאינטרנט ?
- האם קיים מיפוי עדכני של הממשקים בין רשת ה- IT לבין רשת ה- OT?
- האם קיימים מדיניות ונהלים המנחים על אופן אבטחת ממשקים בין רשת ה- IT לבין רשת ה- OT?
- האם הגישה מרחוק לרשת ה- OT מתבצעת באופן מאובטח דרך רכיב גישה מרכזי?
- האם קיים מיפוי עדכני של מערכות ורכיבים בסביבת רשת ה- OT?
- האם הארגון עושה שימוש בתקשורת אלחוטית העושה שימוש בטכנולוגית תקשורת לא מאובטחת לרבות ברכיבי IIoT?

# ניטור ומענה לאירועי סייבר

- כיצד ובאילו כלים מנטר הארגון אירועי סייבר בסביבת ה-OT?
- כיצד נערך הארגון להתמודדות ותגובה לאירועי סייבר בסביבת ה-OT?
- האם הוגדרו קריטריונים ומנגנון דיווח מידי להנהלה ולדירקטוריון, בעקבות התרחשות אירוע קיצון?
- האם גובש תהליך לתחקור, להפקת לקחים וליישומם, בעקבות התרחשות אירועי סייבר בסביבת ה- OT?

# סיכום
# דרכי התמודדות

- ניטור שוטף
- זיהוי כפול – מורכב (נעילה , החלפת סיסמאות וכו' - בקרת גישה והגבלה)
- הפרדת רשתות
- זהירות בחיבור לענן
- גישה מרחוק מאובטחת
- מדיניות ארגונית – נאכפת
- חסימת נתיקים
- עדכונים לבקרים ולמכונות
- מודעות ואחריות (הנהלה ועובדים)
- גיבויים
- הקשחה
- בדיקות חוסן
- מוכנות

# צמצום סיכוני סייבר עבור מערכות בקרה תעשייתיות (ICS)

הרחבה מקצועית

סייבר ישראל
מערך הסייבר הלאומי

# ניהול סיכוני סייבר בסביבת OT

מדריך לדירקטוריון

# שאלות ?

אורי שמאי

ניהול אבטחת מידע וסייבר


תודה רבה
אורי שמאי
052-9594267
ciso@urishamy.com