13.2.22

שיעור 1:

# מבוא

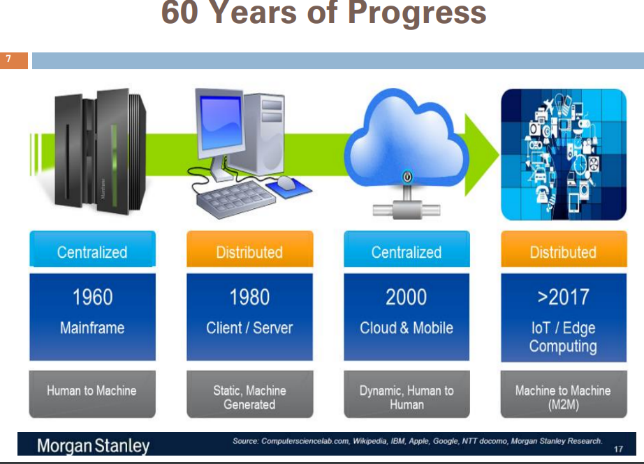
תורת ההגנה בסייבר (תוהג) -מהווה המלצה לכלל הארגונים שפועלים במשק כדי שידעו מה לעשות ולהיערך ליום שבו יקרה משהו.

בקורס הזה הולכים על הגדרות לפי ה NIST

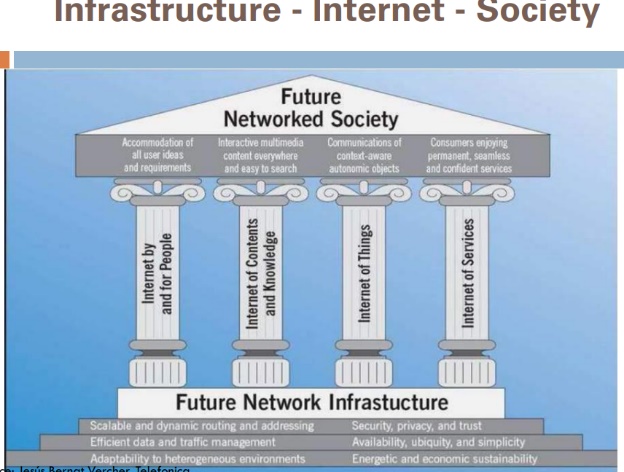
המילה סייבר הגיעה מהמילה היוונית cybernetics למשול, להוביל, לכוון.

התחיל כתורה שמדברת על נושא של קשר בין אנשים למכונות. מדבר על הנושא של איך מתכננים ומיישמים מערכות על מנת שהתפקוד ש ל המערכות יהיה יותר יעיל.

המרחב הקיברנטי – cyberspace, ברגע שיש מכשיר שיש לו קשר לאינטרנט אותו מכשיר מהווה חלק מהמרחב הקיברנטי. כל העולם שבו יש אינסוף מכשירים והתקנים שמחוברים ביחד ומתקשרים דרך האינטרנט דרך רשתות פרטיות וציבוריות. העולם של המרחב הקיברנטי הוא של איומים וסיכונים. כל דבר שמחובר לאינטרנט ושיש לו כתובת IP.



ההתפתחות כספירלה, התחילה \_\_\_ והופכת להיות מבוזרת, כיום מבוזרת



יישומים ראשונים במחשב הראשון – חיפוש ותקשורת.

האינטרנט נולד על שני עמודי התווך כאמצעי תקשורת וכאמצעי תוכן.

אינטרנט הוא מקור של מידע

# היבטים כלכליים במרחב הקיברנטי

בעקבות הקורונה הזמן שלנו במרחב הקיברנטי גדל ולכן נעשינו פחות רגישים והמודעות שלנו ירדה בעקבות העייפות והתחילו יותר מקרים של חשיפה.

# מפות איומים

3 סוגי איומים לפי Checkpoint: Malware, Phishing, Exploit

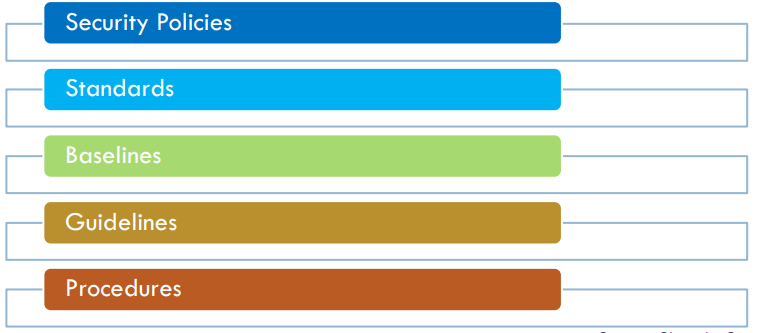
# מדיניות:

פרוצדורות או פרוטוקולים.

מדיניות היא דרך הפעולה או שיטה שמיועדת להשיג מטרה מסוימת. ניתן לראות מדיניות כסוג של תחום הפעילות שבו עוסקים בכוחות הפועלים בחברה או מדינה על מנת

מדיניות היא מה הוא סט ההגדרות, חוקים, מצב רצוי שאנחנו רוצים שיהיה מבחינת האיומים כסכנות של סייבר שיש סביבנו, שנדע להתפעל בעולם האיומים שסביבנו.

מדיניות נבנית על ידי סט הירככי של כלים ונהלים שנקראים Security Policies, Standards, Baselines, Guidelines, Procedures. הם מיועדים כל אחד לחוד וכולם ביחד לעזור לנו כארגונים לתכנן, להגדיר את היעדים וליישם את מדיניות הסייבר בארגון.



# Security Policies

המסמך ברמה האסטרטגית הכי גבוהה שמטרתו להגדיר את התכולות, את הטווח של אבטחה שנדרש לארגון. בין היתר מתאר את המטרות והפרקטיקות שארגון צריך להטמיע על מנת לשמור על ההמשכיות העסקית של הארגון ולכן כחלק מהגדרת ה Security Policies אנחנו מדברים על הגדרת מי אחראי על מה, איך יעבדו התהליכים ומהו תאבון הסיכון (מהי אותה רמת הסיכון המקובלת עלינו שאנחנו כארגון מוכנים לחיות איתה).

## 3 סוגים של Security Policies**:**

1. **organizational security policy** – מדבר בדרכ על מה רלוונטי בארגון שלי, לדוגמה אם הארגון שלנו הוא שייך לאחד משווקים רגלוטורים(שיש רגולטר= ממשלה)
2. **issue-specific security policy** – בכל אחד מהארגונים יש מחלקות שונות וכל אחת עוסקת בתחום פעילות שונה. לדוגמה ביה"ח/חברה עסקית, יש מישהו שנותן שירות, יש מי שמפתח/מנתח ויש מי שעובד במדור שכר. מטבע הדברים הדרישות של אבטחה לכל אחד מהיחידות האלה יהיו שונות.
3. **system-specific security policy** – סביר להניח שבכל אחד מהארגונים האלה יש מכל מיני מערכות, לדוגמה מערכות SaaS, בסיסי נתונים, רשתות, מדפסות, ציודי קצה**.** פוליסי זה עוסק באותם סוגי הציודים שלרוב קיימים בארגונים על מנת להגדיר מה נכון, מה מותר ומה לא נכון לעשות עם הציוד והמערכות שיש.

מזווית אחרת אפשר לראות כקטגוריות של Security Policies**:**

1. **Regulatory** – כל סט הפוליסי שמוכתובת ע"י הרגולטר, אם יש רגולטר הפוליסי הארגוני כנראה יהיה מהסוג של הרגולטר. אם אין רגולטר אז אין לארגון עניין בסוג הזה
2. **Advisory –** קטגוריה של הפוליסי שרעיון הוא שאומנם אי אפשר להכריח את העובדים להתנהל כמו שאנחנו רוצים שהם יתנהלו אז נותנים " המלצות חמות" = איך אנחנו רוצים שהעובדים שלנו יעבדו והתנהלו בהקשר של אבטחה**.** הארגון לא יכול להכריח את העובד אלא הוא ממליץ אבל הוא ממליץ את זה גם מצד מה יקרה במידה והעובד לא יעשה את שמה שמוגדר לו.
3. **Informative** – לתת לא בעלי העניין של האגון הצהרת כוונות, מה הראיה של הארגון מבחינת הפרטיות, מה המדיניות של הארגון מבחינת שמירת המידע שלו**.**

# Security Standards

דרישות להתנהלות מוגדרת היטב עבור תוכנה, חומרה, טכנולוגיות או בקרות אבטחה.

אפשר לראות בהם מסמכים טקטיים שמגדירם לנו או שלבים או שיטות שאומרות לעזור לנו להשיג את אותן המטרות שהגדרנו במסגרת הפוליסי.

# Security Baseline

מדבר על מצב הסטטוס של חברה שהוא מבחינת עולם התוכן שלנו מהווה רמת האבטחה המינימלית שאם המכשיר או מערכת או שילוב שלהם לא עומד בדרישות המינימליות של ה Security Baseline**.**

אנחנו צריכים להוציא אותם במיידי מכלל השימוש של הארגון ולכן בדר"כ שמגדירים Security Baseline מסתכלים עליו כשמשוהו שנגזר מתוך ההגדרות של התקנים המקובלים בתעשייה או על ידי הרגולטר**.**

# Security Guideline

ההמלצות הפרקטיות על איך אנחנו צריכים ליישם את הסטנדרטים וה baselines שלנו, ממש מדריך מקצועי, אמור להיות גם מספיק גמיש על מנת לאפשר לאנשי המקצוע ליישם את הדרישות. הם בד"רכ מדברים על מתודולוגיות על הדרך המומלצת ליישום אבל לא מכריחים

# Security Procedures

הרמה הכי תכלסית שמדברת על איך תכלס מיישמים את אותן הבקרות הספציפיות

20.2.22

שיעור 2:

# מה זה אבטחה?

להגן על נכס כלשהו, הגנה,

אבטחה זה קודם כל התחושה, להיות חופשי מהסכנה (בטחון).

אבטחת מידע – בכל אחד מהארגונים צריכים להיות שכבות ההגנה שלמעשה יאפשרו לארגונים להימצאות במצב של חופשיים מהסכנה.

השכבות של אבטחת מידע:

1. הגנה פיזית – גדרות, כלבי שמירה, מנעולים, כספות...
2. הגנה על האנשים
3. אבטחה על הפעילות, תפקוד של הארגונים
4. אבטחת תקשורת
5. אבטחת רשתות
6. אבטחת מידע – הגנה על הCIA

# מונחים:

Information security – אבטחת מידע

Cybersecurity – הגנת הסייבר

The National Cyber Security Authority (NCSA) – מערך הסייבר הלואמי

Cyber Defence Methodology – תורת ההגנה בסייבר

CERT - Computer Emergency Response Center (**119**) - המרכז המבצעי לניהול אירועי סייבר

National Institute of Standards and Technology (NIST) מכון התקנים האמריקאי

119 – מוקד חירום של מערך הסייבר הלאומי, נותן שירות לארגונים בעיקר

# מה זה אבטחת מידע?

הרעיון של אבטחת מידע זה הגנה על כל מידע ומערכות מידע משימוש, השמדה, שיבוש, גישה בלתי מורשת או גורמים בלתי מורשים.

סודיות, שלמות, וזמינות ((Availability, Integrity, Confidentiality של המידע ללא תלות בסוג המידע או בצורת האחסון - פיזית או אלקטרונית.

אבטחת מידע information security זה יותר רחב מהCIA כאשר מדברים על אבטחת מידע בניגוד לאבטחת סייבר ((cybersecurity אנחנו רוצם לשמור על הCIA של הנתונים והמערכות ללא קשר בצורת הנתונים (אנלוגי או דיגיטלי) מידע אנלוגי – קבצים, קלסרים, מידע שכתוב על דפים, דיגיטלי – מסמכים במחשב.

הסיפור של אבטחת מידע התחיל במלחמת העולם השנייה – מכונת האנגימה (מכונת קידוד שקידדה את המידע שהחליפו בין צוללות למטה). מדען בשם טיורינג החליט שהוא רוצה לפתח את התקשורת הזאת והוא המציא מכונה בשם מכונת טיורינג, גנבו מכונית אניגמה ופיצחו איך היא עובדת (קשור לאבטחה פיזית כי היו צריכים את המכונה עצמה).

# למה קיים אבטחת מידע?

1. אחת מהמטרות העיקריות של אבטחת מידע היא קודם כל לאפשר לארגונים לתפקד
2. להגן על הנכסים שקיימים בארגונים
3. להגן על הנכס הכי גדול של הארגונים = מידע (DATA)

# מרכיבים של אבטחת מידע:

חומרה, תוכנה, מידע (ליצור\לעבד), רשת, אנשים ותהליכים

כאשר מדברים על אבטחת מידע אנחנו צריכים לדעת להגן על כל אחד מהמרכיבים של תחום מערכות המידע.

כיוון שמערכות המידע קיימות על מנת לקבל מידע, לעבד אותו, להוציא אותו (פלט) ולאחסן אותו.

# מחזור החיים של מידע:

המידע לא רק מקבל תהליכים הוא גם נמצא בתנועה. צריך לשמור על המידע ב3 המצבים שלו :

Process, transit, in storage (data at rest)

## חומרה

טכנולוגיה פיזית בעולם הפיזי, שעוסקת באחסון, העברה ועיבוד של מידע (0 ו-1) ולכן אפשר לראות בחומרה סוג של שער יציאה וכניסה למערכת. לכן כל פעם שנדבר על חומרה נדבר על הגנה פיזית של הנכסים.

## תוכנה

הנושא הכי קשה כי הוא מגוון, משתנה בקצב מהיר ובגלל זה יש הרבה פעמים אי התאמה בין מערכות חומרה שחיות שנים לבין עולם התוכנה שמשתנה ברזולוציה יומית.

## רשתות

הכל התחיל ממחשבי הmain frame ורצו להתחיל לקשר את מרכזי המחשוב האלה של המוסדות האקדמיים. ברגע שאתה חלק מהמרחב הקיברנטי אתה חשוף לבעיות והיתרונות.

## מידע

משהו שמיוצר או שמעובר או שנשמר ואנחנו במסגרת אבטחת המידע צריכים לדאוג ולהקפיד על הגנת המידע בכל המחזור חיים שלו. ולהגן על המשאבים והאפליקציות שעוסקים במידע החל משלב הייצור, תהליך ואחסון.

## אנשים

שום מערכת\ תוכנה לא יכולה למנוע מבן אדם לעשות טעות.

הסיפור של החומה הסינית – היא כמעט ולא ניתנת לחדירה, נתנו שוחד לשומר על השער כדי להיכנס לחומה ולכן אנשים הם החוליה הכי חלשה בעסק.

## תהליכים

התהליכים אותם guideline, procedures הם נכסים ארגוניים שעליהם אנחנו צריכים להגן, תהליכים הם סוג של מידע.

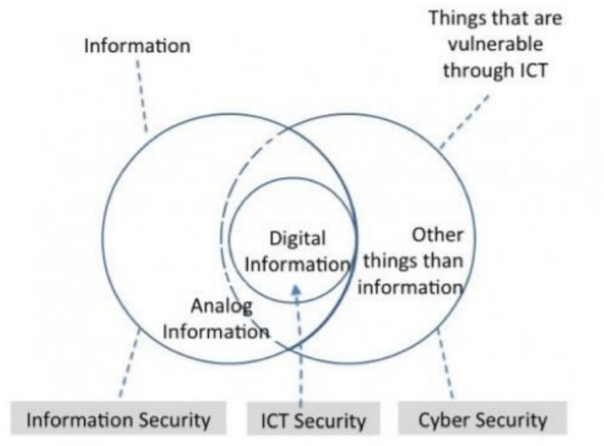
## הגנת סייבר – Cybersecurity

פרקטיקה יומיומית של הגנה על מחשבים, שרתים, טלפונים ניידים, רשתות, מידע ומערכות אלקטרוניות מהתקפות זדוניות. כאשר אנחנו מדברים על הגנת סייבר אנחנו צריכים להגן על כל מה שמחובר או שמהווה חלק מהמרחב הקיברנטי ממתקפות זדוניות.

# רבדים של הגנת סייבר

1. אבטחת רשתות
2. אבטחת מידע
3. אבטחת אפליקציות
4. אבטחת אופרציה
5. המשכיות עסקית והתאוששות מאסון

כל מה שהוא חלק מהמרחב הקיברנטי הוא חשוף וזאת בעיה

ICT – information and communication technology

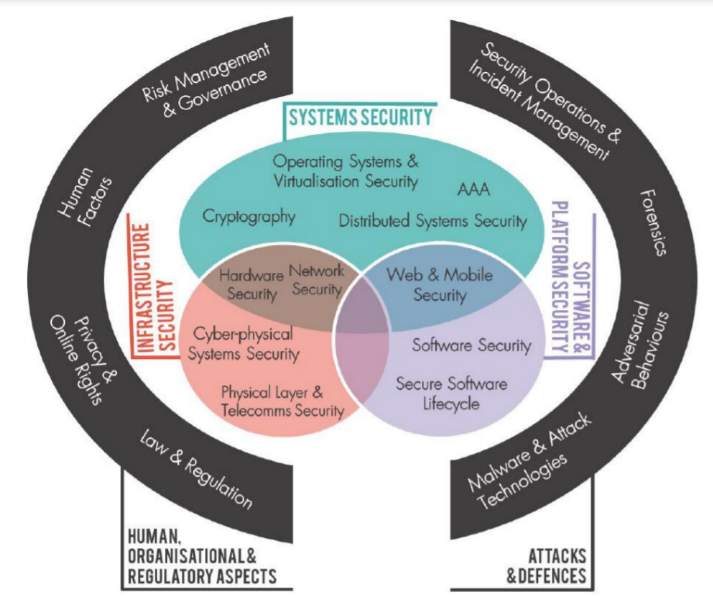
Information security אבטחת מידע – אבטחה על מערכות ללא תלות בסוג המידע. אבטחת מידע אנלוגי ואבטחת מידע דיגיטלי.

ICT – כל הטכנולוגיות שעוסקות ביצירת המידע והעברת המידע הספרתי=דיגיטלי. האזור המשותף בין אבטחת מידע לאבטחת סייבר המשותף המידע הדיגיטלי.

Cyber security - עוסק בכל מה שפגיע בתוך המערכות ICT. לא רק מידע דיגיטלי אלא הגנה פיזית וכו'.

27.2.22

שיעור 3:



**Security Management Concepts and Principles** - (SMCP) define the basic parameters needed for a secure environment.

SMCP define the goals and objectives for policy designers and system implementers to achieve a secure solution.

כל העולם של מטרות ויעדים שצריכים להיות מיושמים בארגונים על מנת שהארגונים שלנו יהיו מוגנים.

The primary goals and objectives of security are contained within the **CIA** Triad.

The CIA Triad is the name given to the three primary security principles: Confidentiality, Integrity, and Availability.

The importance of each principle is specific to organization and depends on the organization’s security goals, requirements and on the extent to which its security might be threatened.

**Security controls** must address one or more of CIA principles. Security controls are typically evaluated on whether or not they address these core information security tenets

בעברית יש מילה אחת והיא בקרה ובאנגלית יש לפחות 3 מונחים שהם משלימים אחד את השני – controls, save guard, countermeasures. יש responsive defense ו proactive defense

**Vulnerabilities** and **risks** are also evaluated based on the threat they pose against one or more of the CIA Triad principles.

## Confidentiality

גורם בלתי מורשה לא יגיע למידע שהוא לא רשאי אליו. כל המידע, אובייקטים ומשאבים לא חשופים למישהו שהוא לא מורשה לחשיפה הזאת.

מידע חייב להיות מוגן בכל שלושת השלבים שלו. מידע בתהליך, מידע באחסון (storge\rest) ומידע בהעברה ( transit).

הגורם הראשי להפרה של סודיות המידע הוא הגורם האנושי.

חלק מהשגרה של הארגון זה: בקרת גישה, אימות, הצפנה, תעבורה, סיווג מידע...

## Integrity

כל המרחב של הגנת סייבר לא רק מידע, מדברים גם על אובייקטים וגם על משאבים בנוסף למידע. אנחנו צריכים לוודא שכל מה שנגיש דרך מרחב הסייבר (אובייקטים, משאבים, מידע) אף אחד לא נגע\ שינה ממצבם המקורי.

יש הרבה מונחים משלימים : unauthorized access – ברגע שיש גישה למידע שלנו או למערכות הארגוניות ( (exposureאי אפשר לדבר על שלמות כי אי אפשר לדעת מה השתנה, כי עד שלא עושים חקירה פורנזית לא יכולים לדעת האם המידע נפגע.

## Availability

זמינות לא רק של מידע אלא גם של שאר ההיבטים. אנחנו רוצים להבטיח זמינות של מידע למשתמשים אך זה האתגר של אחראי אבטחת מידע. צריך לדעת לשמור על איזון בין הקשחה של המערכות לבין הזמינות למשתמשים.

זמינות תלויה גם בשלמות וסודיות אבל אין את אותה התלות כמו בין שלמות לסודיות. אך ורק אם יש חשש שאחד משני עקרונות הזמינות והשלמות נפגע אי אפשר לדבר על זמינות.

חוץ מהCIA יש עוד עקרונות שנגזרים מפוליסי, privacy, identification, authentication, authorization, accountability, and auditing.

# מושגים:

Threat (איום) **–** כל נסיבות או אירועים עם **פוטנציאל** לגרום נזק למידע או מערכות מידע דרך גישה, שינוי, שיבוש או השמדה של המערכות האלה כתוצאה מפעילות בלתי מורשית. פוטנציאל יכול להגיע מהנסיבות או מהאירועים.

הרחבה: כל נסיבות או אירועים עם פוטנציאל שיכול לפגוע בארגון, בנכסים של הארגון, אנשי הארגון או מדינות.

ההרחבה היא שמדברים גם על האנשים שעובדים בארגון..

Vulnerability (פגיעות) **–** פגם או חולשה בנהלים, בעיצוב, במימוש או בבקרות בכל המרחב של הסייבר. שיכולים להיות מנוצלים בזדון או בשוגג כתוצאה מהפריצה או אי עמידה בדרישות של מדיניות הסייבר בארגון.

הרחבה: מדבר על החולשות במערכות מידע, נהלים, בקרות פנימיות או יישומים שיכולים להיות מנוצלים או יוזמים על ידי משהו שנקרא מקור איום (threat source)

הרחבה נוספת: יש אבחנה בין בשוגג לבין בזדון.

דוגמאות לפגיעות: הגדרה שגויה בקונפיגורציה של אתרים (פיירוול, חומת הגנה), חלוקת הרשת, הגנות על הרשת, יישומי צד שלישי, רכיבים לא מזוהים, ניצול לרעה של חשבון המשתמש.

Risk (סיכון) **–** תמיד מדברים על שני היבטים: מה ההסתברות שמשהו יקרה ומה הנזק שלו.   
סיכון זה מדידה, משהו שמורכב משני דברים בסיסים:

1. Impact (נזק) – מה יקרה לנכס\מערכת\ארגון אם וכאשר האירוע יתרחש (נמדדים ב1-4).
2. Likelihood (סבירות) – מדד שמההתחלה הוא לא כמותי (בניגוד להסתברות 1-10), מודדים בסבירות נמוכה\בינונית\גבוהה. הסתברות נעה בין 0-10, סבירות נעה בתחום רחב יותר (1-4)

הרחבה: סיכון מוגדר ככל הסיכונים שעלולים להתרחש כתוצאה מהאיבוד או פגיעה בCIA של מערכות מידע וכתוצאה מכך כולל שינוי השמדה וכו' של כלל הנכסים הארגונים, אנשים, מערכות או מדינות.

Attack (התקפה) **–** מימוש האיום שמשפיע על הCIA. מבחינת תקן אחר זה כל ניסיון לקבל גישה בלתי מורשת למידע, מערכות, משאבים וכו' במטרה לפגוע בCIA. או שניתן להגדיר את ההתקפה ככל סוג של פעילות זדונית.

דוגמה: Stuxnet.

סוגי התקפות: Malware (malicious software), Network security attacks, Social Engineering וכו'.

Malware (תוכנה זדונית) -תוכנה שמההתחלה פותחה במטרה לגרם נזק, לשבש, להרוס או לקבל גישה בלתי מורשית למערכות).

סוגים של malware: Viruses ,Worms, Spyware ,Trojans, Ransomware.

מקור ההגעה של malware : אתרים נגועים, מיילים, אתרי שיתוף קבצים וכו'

**שיעורי בית:**

**באתר של הקורס case studies מסמך של target לקרוא אותו לשיעור הבא**

6.3.22

שיעור 4:

Virus **–** תהליך ההדבקה, בדרך כלל הם מגיעים מהעולם החיצון (הורדה של קבצים, מיילים, לינקים... כל דבר שמהפעולה הזאת אנחנו מפעילים משהו) המאפיין של וירוס הוא שצריך פעולה **אקטיבית** בניגוד לתולעת. הוירוס רדום עד שהמשתמש לא מפעיל את התוכנה שלו.

Worm **–** יודעת **להתפשט** בתוך הרשת הארגונית, היא לא צריכה פעולה של משתמש כדי לטייל.

Spyware **–** היא לומדת מה אנחנו עושים (הקלדה, העתקה...), המטרה שלה היא ללמוד ולאסוף כמה שיותר מידע על המשתמש. לדוגמה תוכנה שמעתיקה את כל מה שהמשתמש מקליד. דוגמה : keylogger.

Trojan **–** תוכנה זדונית כלשהי במסווה של תוכנה חוקיתולגיטימית. דוגמה ב Case studies דוגמה של asus.

Ransomware **–** כופרה, תוכנה זדונית שמטרתה לדרוש כופר מהקורבן. היא מונעת מהקורבן גישה למידע או כלל מערכות המידע שנוגעות לו. הדרך היחידה להתמודד עם כופרה היא גיבוי.

## דוגמאות להתקפות:

**Botnet –** רשת של בוטים,ברגע שמישהו משתלט על מחשב\ רשת מחשבים אפשר לעשות פעולה איתם. רשת של בוטים שבדר"כ משתמשים בהם כדי ליצור מתקפות בעיקר DDoS.

**פישניג, DoS , DDoS**

# תמונה שמכילה שולחן התיאור נוצר באופן אוטומטיסוגי תוקפים:

שלושה סוגים עיקריים:

Cyber criminal– פושעי סייבר, המניע העיקרי זה כסף

Hacktivist – המניע העיקרי זה האידיאולוגיה שלהם, הם "לוחמי צדק"

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיInsiders **–** אנשים שנמצאים בתוך הארגון ובכלל סיבה כלשהי (לדוגמה כסף, אמונה, נקמה וכו') הופכים להיות cyber criminals.

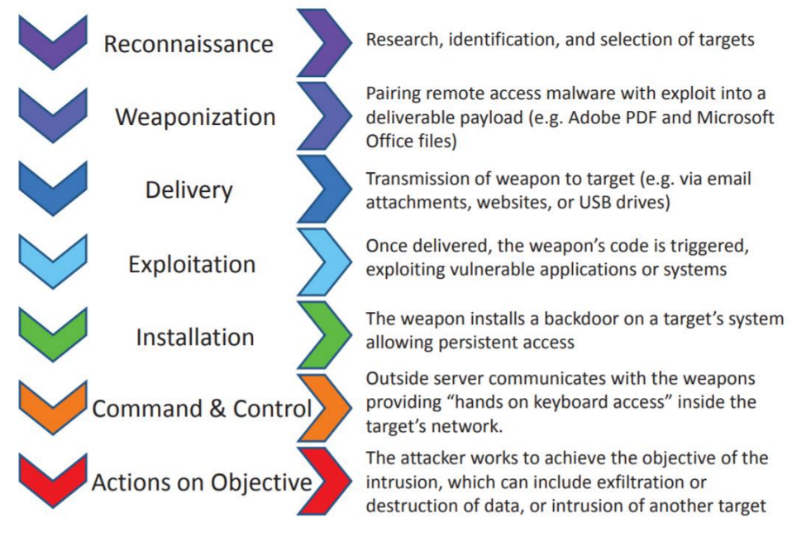
# סוגי Cybercrimes:

כל פעולה זדונית שמטרתה לחשוף, להטריד, לשבש או למנוע את הגישה   
למידע או מערכות מידע ארגוני.

המקרה של target – פרטים של כ110 מיליון תושבי ארה"ב נגנבו (1\3 מתושבי ארה"ב). הגיעו לtarget דרך שרשרת האספקה (ספק צד שלישי). חברת פאזיו הייתה קבלן שנתן שירותי מיזוג אוויר לחברת טארגט ולהם הייתה גישה למערכת תשלומים של החברה וההאקרים הגיעו לחברת פאזיו דרך פישינג ככל הנראה. דרך פאזיו הגיעו לPOS (המכשיר סליקה) של טארגט.  
  
היו מספר כשלים:

1. הנוזקה שהושתלה היא נוזקה שהייתה מוכרת כבר לפני שנתיים.
2. המערכת התריעה ואנשי הSOC התעלמו מההתראה פעמיים, פעם אחת על זה שהנוזקה נמצאת בטרמינל ופעם שנייה כאשר היא עברה בFTP.

# Cyber Kill Chain



Cyber kill chain \* זה מודל שבדר"כ רוב ההתקפות יהיו לפי המודל הזה, הוא מפרט לנו 7 שלבים

1. **Reconnaissance** – איסוף מודיעין.   
   \* הגילוי שחברת fazio עובדת עם target.

איסוף המודיעין יכול להיות גלוי ונסתר, אין לנו דרך להתגונן מאיסוף מודיעין נסתר.

סריקת פורטים – ניתן לגלות אם אוספים עלינו מידע אם אנחנו מגלים שמפורט מסוים שולחים אלינו יותר מידי פינגים.

1. **Weaponization** - בחירת הנשק, מטרתו לגלות את ה vulnerability בארגון

\* יצירת הפישניג

3. **Delivery** – דרך אספקת הנשק

4. **Exploitation** – ניצול חולשות ארגונית

\* סיסמה דיפלוטית באחת ממערכות הארגון,

5. **Installation** – התקנת תוכנות שמאפשרות לנו להגיע לC&C, התקנת ה backdoor

\* הורדה של המידע שנאסף, העברת המידע בשרת הFTP

6. **Command & Control –** סט הפעילויות של התקנות תוכנות הזדוניות

7. **Actions on objectives** – מה שעושים עם המידע.

לטענת חברת לוקהיד מרטין ניתן לעשות משהו בכל אחד מהשלבים של kill chain

והם פרסמו את D- layers of control, הם הגדירו את 5 שלבי ההגנה\בקרות שיכולים לעזור לארגונים לגלות, לזהות ולהתמודד עם ההתקפות.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

D layers of defense

אומר בעצם מה ניתן לעשות בכל אחד מהשלבים אם לא הצלחנו לעצור בשלב הקודם.

1. Detect – המטרה היא לעזור לנו לגלות את איסוך המודיעין על הארגון
2. Deny – מסתכל על שלב של עצירת ההתקפה ע"י כך שנמנע את חשיפת המידע לגורמים הלא מורשים
3. Disrupt – שלב שבו ניתן לשנות או לעצור את זרימת\ זליגת המידע
4. Degrade – אם לא הצלחנו לשנות או לעצור את זליגת המידע אנחנו מנסים להוריד את היעילות של ההתקפה, לצמצם את הנזקים.
5. תמונה שמכילה שולחן

   התיאור נוצר באופן אוטומטיDeceive – להתעמת עם התוקף תוך כדי ההתקפה. שלב נדיר כי זה אומר שצריך לגלות את ההתקפה בזמן אמת.

13.3.22

שיעור 5:

# The Unified Kill Chain

פרויקט שמומן ע"י ממשלת ארה"ב שהמסגרת הזאת עוזרת לנו להבין, ללמוד את מה בעצם עושה התוקף (הפעילויות) בכל אחד מהשלבים כי יש ריבוי סוגי המתקפות. הפרויקט הזה נועד לעזור לצד המתגונן עם proactive defense.

# The Cybersecurity Framework (by NIST)

תורת ההגנה של מערך הסייבר מבוססת עלThe Cybersecurity Framework , שפורסם בשנת 2018 והוא מהווה מסמך מסגרת הכי מקיף והכי שימושי עבור ארגונים על מנת לתת מענה מה ואיך צריכים לעשות ארגונים בכל אחד מהשלבים של מחזור החיים של הגנת סייבר. החל מהשלב של הגדרת המטרות, יעדים ואסטרטגיה ארגונית להגנה דרך השלבים של פיתוח יישום, והטמעת הכלים להורדת הסיכונים ומניעה עד כמה שניתן את הנזק שעלול לקרות כתוצאה מהתקפה. כולל שלבים של זיהוי ההתקפה, טיפול בהתקפה וחזרה לשגרה.

ה framework מסתכל על הארגון במסגרת מערכת הecosystem , לכל ארגון יש למעשה ספקים ולקוחות ויש גם ספקים של ציוד ולפעמים גם כל ארגון בעצמו פועל כספק טכנולוגיה עבור הארגונים האחרים. הארגון אינו פועל לבד וכל אחד בשרשרת ה ecosystem גם בהיבט הטכנולוגי וגם בהיבט העסקי של הארגון מהווה מקור איום פוטנציאלי ולפעמים גם ממשי.

The Cybersecurity Framework מאחד בתוכו הרבה מאוד תקנים כמו ISO ועוד שנכתבו ספציפית להגנה בסייבר. היתרון שלו הוא שהוא נותן מסגרת מקיפה, במקום להבין תקן תקן, המסגרת הזאת נותנת לנו את מהסדרת שמכילה את כלל הפעילויות שהארגון צריך לבצע בכל אחד מהשלבים של הגנת סייבר.

התהליך הזה הוא תהליך מחזורי שמתבצע ב3 רמות ארגוניות:

1. Senior Executive Level – אחראים על קביעת המדיניות, להגדיר את האסטרטגיה בכל הקשור לעולם הסייבר. כחלק מהאסטרטגיה בשכבה הזאת מתקבלות החלטות של מהי רמת הסיכון המקובלת של הארגון (עם איזה סיכונים הוא מוכן לחיות ועם איזה לא).
2. Business Process Level – המנהלים של דרג הביניים באחריותם להביא לידיעת הדרג הבכיר שמקבל החלטות את כלל הנכסים הארגוניים או תהליכים עסקיים שעליהם חל איום סייבר. ארגונים צריכים להערך ולהגן עליהם. לאחר הבאת המידע להנהלה הבכירה, לאחר שנקבעת מדיניותו נקבעים התקציבים, אחריותם גם לנהל את הפרויקטים והתקציבים שקשורים ביישום, בפיתוח והטמעה של בקרות ההגנה.
3. Implementation Operations Level – האנשים שעסוקים תכלס בפיתוח והטמעה של הכלים והבקרות.

נוסף על כך, The Cybersecurity Framework מורכב משלושה core, profiles ו implementation tiers

**Core** – כלל הפעילויות, התוצאות וגם נותן רפרנס לכל הבקרות האפשריות בכל אחד מהשלבים של מחזור החיים, גם לפי משפחות הבקרות (בהמשך).

**Profiles** – ההגדרות שעוזרות לארגון לקחת ולסווג\ לחלק את כלל הנכסים או תהליכים עסקיים לקבוצות ולהגדיר דרישות עבור על אחד מהקבוצות האלה מבחינת ההתמודדת והפעילויות מה נדרש לעשות עבור כל אחד מהקבוצות האלה והדרישות שלהן בהתאם.

**implementation tiers** (שכבות היישום) – הדרך של הארגון לקבוע סט של מדדים שיעזרו לעשות הערכה לטובת\יעילות היישום של אותו core לפי אותם הprofiles.

ה Cybersecurity Frameworkמדבר איתנו על חמשת המשפחות של ההגנות



identify - לזהות\להגדיר נכסים, מדיניות ותהליכים עסקים,

protect- להגן על הנכסים (כל מה שזיהינו ב identify)

detect – לגלות אירועים

Respond – תגובה

Recover – התאוששות

Cybersecurity Framework לוקח את כל ההגנות ומחלק אותם לקטגוריות, קטגוריות משנה ומחלק אותם לתקינה. ולכן זה היתרון שלו שהוא מאחד הכל תחת מקום אחד במקום מספר תקנים.

## המבנה של Cybersecurity Framework

**Functions** (פונקציות) – חמשת המשפחות

**Categories** (קטגוריות) – הנושאים הספציפיים מהעולם של ההגנה על הנכנסים או תהליכים עסקיים

**Subcategories** (קטגוריות משנה) – התוצרים\ תוצאות שרוצים להגיע אליהם כתוצאה מהפעילויות שיושמו ע"י הבקרות.

**Informative References** (הפניות) – ההפניות לתקנים, איפה כל בקרה מופיעה בתקן הבינלאומי.

יותר ויותר מדינות מקבלות את ה Cybersecurity Framework כבסיס לתורת ההגנה שלהם.

# מערך הסייבר הלאומי

הגנה על ארגון מפני איומי סייבר דורשת ידע והשקעות טכנולוגיות, ארגוניות, ותהליכיות.

מערך הסייבר הלאומי הוקם על-מנת לעצב, ליישם ולהטמיע תורה לאומית להגנת הסייבר.

תורת ההגנה בסייבר לארגון (ת"ה) פותחה ע"י מערך הסייבר הלאומי לטובת הציבור ומהווה המלצה לכלל הארגונים במשק הישראלי.

# מטרות תורת ההגנה

**\* להסתכל במצגת \***

מטרת ת"ה היא להציג בפני המשק הישראלי שיטה סדורה **לניהול סיכוני הסייבר בארגון**.

המטרה היא להיות מסוגלים לטפל בכל מחזור החיים של הסייבר בארגון. החל מזיהוי והגדרה של פוטנציאל הסיכון, הבנת הבקרות מה ואיך ניתן לעשות, קביעת האסטרטגיה\ מדיניות למענה ומימוש של דרך המענה שנקבעה.

ת"ה מציגה מספר שיטות לביצוע הערכת וניהול סיכונים, לפי חלוקה לארגונים:

* בעלי פוטנציאל נזק קטן יחסית (עד ל 5 מיליון שקל(
* בעלי פוטנציאל נזק גדול יותר

# עקרונות תורת ההגנה

העיקרון הראשי של ת"ה הינו "**הגנה מפני איומים רלוונטיים"**

איומים רלוונטיים = לפי התעשיה המסוימת שאנחנו שייכים אליה ולפי היסטורית האירועים בכלל ובמדינת ישראל בפרט..

## תתי עקרונות:

* אחריות ההנהלה
* הגנה מתוך ראיית היריב
* הגנה בהתאם לפוטנציאל הנזק
* הגנה מבוססת עומק יישום
* הגנה מבוסס ידע וניסיון ישראלי

## אחריות ההנהלה

כל מה שקורה או יקרה בארגון, הנהלת הארגון היא תמיד האחראי גם בפן המשפטי וגם בפן החוקתי.

## הגנה מתוך ראיית היריב

תורת ההגנה מכירה ומעודדת את קבלת הפרספקטיבה של פעילות התוקף, איך הם פועלים.

## הגנה בהתאם לפוטנציאל הנזק

תוה"ג נותנת לנו רשימה של בקרות ואנחנו בתור ארגון צריכים את פוטנציאל הנזק. סוגי הסיכונים, חישוב הסיכונים ומה עושים עם כל אחד מהסיכונים.

## הגנה מבוססת עומק יישום

תוה"ג 2.0 בניגוד ל cyber security framework מגדירה רמות שונות של יישום הבקרות.

## הגנה מבוסס ידע וניסיון ישראלי

ההתאמות והשינויים למשק הישראלי.

# מבנה תורת ההגנה

מחולק לשני חלקים\מסלולים ועוד חלק של נספחים. תוה"ג מחלקת את כלל הארגונים במשק הישראלי ל2 קטגוריות.

כלל המשקים הישראלים עם פוטנציאל נזק קטן מ5 מיליון ₪ .

כלל המשקים הישראלים עם פוטנציאל נזק גדול מ5 מיליון ₪

פוטנציאל הנזק הוא שקלול של כלל העלויות הקשורות לפוטנציאל הנזק במישרין ובעקיפין.

לאחר שתוה"ג מלמדת אותנו להחליט לאיזה מהמסלולים שייך הארגון היא מגדירה 2 תהליכים שונים עבור כל קטגוריה.

## סיווג הארגונים

סיווג הארגונים מורכב ממספר שלבים:

1. האם אירוע סייבר בארגונך יגרום לנזק של יותר מ5 מיליון?

במידה ולא מקרב להחלטה שאולי מדובר בקטגוריה א

1. האם הארגון מספק שירות ליותר מאלף ארגונים?

במידה ולא מקרב להחלטה שאולי מדובר בקטגוריה א

1. האם יש בארגון יותר מ200 עובדים?

במידה ולא מקרב להחלטה שאולי מדובר בקטגוריה א

1. האם מחזור הכספי של גבוה מ200 מיליון שקל?

במידה ולא מקרב להחלטה שאולי מדובר בקטגוריה א

1. האם הארגון שייך למגזר הIT?

גם אם ענינו על הכל שלא עדיין יתכן שאנחנו לא מקטגוריה א כי יש עוד שאלה שמדברת על האם הארגון הוא ספק של שירותים ומוצרים לארגון מקטגוריה ב?

אם הוא ספק, הארגון יצטרך לעבוד לפי כל הנהלים של ארגון מקטגוריה ב אך הוא עדיין לא מוגדר כקטגוריה א.

תמונה שמכילה טקסט, כרטיס ביקור

התיאור נוצר באופן אוטומטיתמונה שמכילה טקסט, כרטיס ביקור

התיאור נוצר באופן אוטומטילאחר מכן יש שאלון על מנת לקבוע האם הוא שייך לקטגוריה א

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

רק אחרי שנענה על כל השאלות האלה נוכל לקבל החלטה מושכלת לאיזה קטגוריה משתייך הארגון.

אחרי שסיווגנו את הקטגוריה של הארגון תוה"ג מחלקת למסלולים:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

בונוס לעלות על אירוע סייבר ולעשות עליו שקף או למצוא סרטון ולדבר עליו 5 דק.

20.3.22

שיעור 6:

דוגמה לשאלה במבחן לאיזה קטגוריה שייכת עירייה? בעירייה אנחנו לא צריכים לעבור את תהליך הסיווג, ארגונים ציבוריים או ארגונים שעובדים תחת דרישות רגולטוריות או ארגונים גדולים ברור מאליו שיהיו תחת קטגוריה ב. יש מוטיבציה מאוד גבוהה לתקוף אותם ולכן מההתחלה הם בקטגוריה הזו.

# תהליכי התכנון עבור ארגונים מקטגוריה א

תוה"ג מגברת על 5 שלבים בתהליך התכנון שמות השלבים הם גם לקטגוריה א וגם לב אבל תוכן השלבים שונה.

1. **שלב תיחום הפעילות** – מטרת השלב היא להבין מה יעדי ההגנה מפני איומי סייבר. (נכסי הארגון, מערכות מידע של הארגון, פטנטים, **תהליכים ארגונים**).

תוה"ג 2.0 מלמדת אותנו להתייחס לארגונים בראיה של תהליכים מעבר לנכסים בלבד.

תהליכים חשובים יותר מנכסים כי בכל אחד מתהליכים יכולים להיות מעורבים מספר ציודים.

בסוף שלב זה, לארגון תהיה רשימה של נכסים ותהליכי עבודה.

1. **שלב הערכת הסיכונים** – יוצאים מנק' הנחה שארגון מקטגוריה א לא יוכל לבצע הגנות בעצמו ולכן הוא מומלץ לאמץ דרישות הגנה רוחביות. 25 בקרות שמחולקות לעשר קטגוריות והן מוגדרות כבקרות אפקטיביות במיוחד שמערך הסייבר כבר בחן והן אמורות לתת מענה לרוב האיומים לארגונים הקטנים. תוה"ג אומרת שאם הארגון הוא מקטגוריה א צריך להכיר את 10 הקטגוריות ולאחר מכן לראות את הרשימה של הבקרות ששייכות לקטגוריות האלה ולמצוא MSSP - צד שלישי,manage security **ser** provider – שרותי צד שלישי שנותנים שירותי אבטחת מידע וסייבר ושהם יתנו תמיכה.

* באג בתוה"ג יש 25 בקרות שמחולקות ל10 קטגוריות הגנה בניגוד ל cyber security framework שבנוי מ5 קטגוריות. יש קטגוריות ותת קטגוריות. יש רק 5 משפחות של ה cyber security framework שהן הבסיס .

תוה"ג קוראת לבקרות האלה בקרות בעלות אפקטיביות גבוהה במיוחד והיא ממליצה באופן גורף לכלל הארגונים מקטגוריה א לשקול את הדרך להטמעה של כל 25 הבקרות הללו.

1. **שלב קביעת אסטרטגיה לטיפול** – לאחר בחינת סטטוס יישום הבקרות יש להחליט מהו המענה הנדרש לסיכונים שנובעים מהפערים בהטמעת בקרות אלו. יש לבחון את הסיכונים מול יעדי ההגנה (נכסים ותהליכים ארגונים) שהוגדרו בשלב 1. אם אנחנו ארגון קטן ויש לנו את ה baseline במקרה שלנו הוא יהיה אותן 25 בקרות שתוה"ג אומרת לנו כדרישות ההגנה ולאחר מכן אנחנו צריכים להסתכל על שלל הבקרות לעומת ה baseline שיש לנו בארגון ולבנות לנו תוכנית עבודה. למעשה שלב זה הוא בחינה של סטטוס יישום הבקרות מתוך 25 הבקרות ואנחנו צריכים להבין היכן אנחנו נמצאים עבור כל אחד מהבקרות בארגון כדי להגיע לשלב הבא של בניית תוכנית העבודה.
2. שלב בניית תוכנית העבודה **–** אנחנו לוקחים את כלל הסיכונים ולעשות לבדיקה איפה אנחנו לעומת הדרישות.

* אם יש לנו נכסים ארגונים שלא עומדים ב baseline אם אנחנו לא מסוגלים לשפר אותו אנחנו מוציאים אותו מכלל שימוש. שלב 4 מיועד לזה שנוציא את כל מה שלא שייך לbaseline ולאחר מכן נבנה תוכנית עבודה שתעזור לנו לקחת את הbaseline שלנו ולהביא אותו לרמת המוכנות עבור 25 הבקרות.

1. **ביקורת ובקרה רציפה** – בקרה מתמדת, עדכונים לפי מפת האיומים... תהליך סדרתי שעושים אותו לפחות פעם בשנה.

* 4 השלבים הראשונים מסכמים את ליבת התהליך עבור ארגון מקטגוריה א.

# תהליכי התכנון עבור ארגונים מקטגוריה ב

שמות השלבים דומים לשמות של השלבים בקטגוריה א אך מעבר לכך כל אחד מהשלבים הללו מתחלק לתתי שלבים וכל אחד מהם מורכב בפני עצמו.

מגדרים שלב 0 בקטגוריה הזו.

**אסטרטגיה הארגונית לניהול הסיכונים –** שלב שהוא לפני כל 5 השלבים. המטרה שלו היא לבחון או להגדיר ממשל תאגידי, להבין האם יש מדיניות בארגון ובמידה ואין להגדיר אותה לפי צורך. יש לבחון את המטרות, הגדרת ההיררכיה, בעלי התפקידים, שגרות ההגנה והליכי הבקרה המבוצעים. איך להגדיר מנא"מ (מערכת לניהול אבטחת מידע) ומה המערכת ההיררכית שתעזור לנו להתנהל בכל עולם אבטחת המידע והסייבר.

בשלב הזה יש הגדרה מי האחראי על כל תהליכי הערכת סיכונים, מה המשאבים שלו, האם יש בארגון מיפוי תהליכים רגישים ובמידה וכן מי אחראי על זה, האם ניתן להשתמש בתהליכים הקיימים לטובת התהלכים של הערכת הסיכונים, באיזו תדירות נעשה הערכת סיכונים ומה המדיניות שלנו בהקשר הזה.. כל אלה חלק מהממשל התאגידי. לפני הכניסה ל5 השלבים של תכנון אנחנו צריכים להבין מי אחראי על מה ואיך אנחנו מקבלים החלטות.

1. **שלב תיחום הפעילות** – על מה יש להגן. הבנת הסביבה שבה פועל הארגון, הגדרת ג"ג ותחומי אחריות.
   1. **הגדרת מרחב הסמכויות וגבולות האחראיות –** יש להגדיר חלוקת בסמכות ואחריות עם בעלי עניין פנימיים, כגון קב"ט, מנהל תפעול, מנהל מערכות מידע, מנהל סיכונים, יועמ"ש, מנכ"ל וכו'. אם הארגון הוא ארגון גדול (או קטן כי הוא מספק שירותים לארגון מקטגוריה א) וצורך שירותי MSSP. סביר להניח שיש לארגון משאבים פנימיים או שייתכן והוא נעזר בMSSP כחלק מאבטחת המידע שלו, כאשר בארגון יש פעילות עם MSSP צריך להגדיר את גבולות הגזרה והאחריות בין הMSSP לבין כלל הסמכויות בארגון.
   2. **הגדרת אסטרטגיה ארגונית להגנה בסייבר** – חזון הארגון, יעדים, מאפייני השוק העסקי, המתחרים וכיצד משלב נושא הגנת הסייבר. איך הסביבה העסקית של הארגון והאסטרטגיה הארגונית משפיעה לחיוב או לשלילה על כל ההיבטים של הגנת מידע וסייבר.
   3. **תיחום סקר הסיכונים** – מתחילים לדבר על מה יש לנו בארגון מבחינת הכלים, נהלים, מערכות. היבטי אבטחה פיזית, תהליכים עסקיים, עם איזה ציודים עובדים ומה הסוג שלהם, מה שרשרת האספקה? האם הארגון מפוזר על מספר מדינות ומנסים להבין את הסביבה העסקית של הארגון.

* בסוף שלב זה מסיימים עם מסמך שמתאר את הסביבה העסקית ותיחום הפעילות לביצוע סקר.

1. **הערכת הסיכון –** 
   1. **זיהוי הסיכון Risk Identification** – מורכב משני תתי שלבים:
      1. **מיפוי יעדי ההגנה** - על מה צריך להגן. מיפוי נכסים ותהליכים עסקיים. חלק מהציודים יכולים לשמש בעלי תפקידים שונים ולכן צריך להגן עליהם אחרת. לדוגמה: חשוב להגן גם על תהלכים עסקיים בכל ארגון מודרני יש מחשב אישי, בחברות גדולות מבצעים רכש של מחשבים ניידם באופן מרוכז. אותו מחשב פיזית יכול להגיע לשימוש ע"י איש תמיכת לקוחות, איש פיתוח ועובד מדור שכר. אם נלך לפי הנכסים נקבל את רשימת המחשבים אבל אופי העבדוה (תהליכים) שבהם מעורב העובד של התמיכה מול מחלקת שכר הוא אחר לגמרי ולכן יש חשיבות גדולה להבין תהליכים עסקיים מעבר לנכסים. ההגנה הבסיסית בכל המחשבים צריכה להיות זהה אבל לכל מחשב יש הגנה בהתאם לאופי התפקיד שבו עובדים.
      2. **שיוך סיכונים ו/או איומים ופגיעויות לתהליכים ונכסים** – צריך להבין איזה איומי סייבר רלוונטי עבור כל אחד מהתהליכים/ נכסים של הארגון. ניתן לעשות זאת על ידי הכרה של דרך הפעולה של התוקפים
   2. תמונה שמכילה שולחן

      התיאור נוצר באופן אוטומטי**ניתוח הסיכון Risk Analysis** – להשליםםםם

בנוסחה תמיד יהיו 2 אלמנטים impact ו- likelihood את הנזק שעלול להיגרם מחשבים לפי תשובות ל3 שאלות. בהתאם לCIA.

צריך לקחת את הערך המקסימלי שהתקבל כתשובה לשלושת השאלות הוא זה שמגדיר לנו את **עוצמת הנזק/ הסיכון** או **ציון הערכיות לתהליך/ נכס**, והוא בעצם מגדיר את פוטנציאל הנזק המקסימלי לארגון כתוצאה מפגיעה בתהליך/ נכס ספציפי.

חישוב מידת הסבירות (likelihood) – ניתן לחשב לפי היסטוריית אירועים שהייתה לחברות דומות, סקירת אירועי סייבר שהתרחשו בשנים האחרונות, מודיעים סייבר, קלות המימוש – עד כמה קל או קשה לממש מתקפה מסוימת, המוטיבציה לתקיפה וסוג המידע.

דוגמה – צריך להחליט איזה מהמדדים חשובים שלנו בד"Rכ יש 3 קטגוריות עיקריות – היסטוריית אירועים, מודיעים סייבר ומשטח תקיפה ( אבטחה פיזית, רמת ההרשאות, אפשרויות גישה מרחוק וכו'). לצורך חישוב הסבירות אנחנו יכולים לתת ערל בין 1 ל-4 ובסופו של דבר אם יש מספר תתי סעיפים אנחנו יכולים לחלק אותם בין 1ל-4 ולהציב אותם בנוסחה כלל שלושת ההיבטים צריכים להגיע בנוסחה לסכום של 1 מקסימום.

אחרי שיש לנו השפעה וסבירות אחנו יכולים להגיע לחישוב רמת הסיכון.

**"סיכון שורשי"** – הסיכון המקורי שמחושב כפונקציה של שני האלמנטים I וL (השפעה וסבירות) בתוה"ג כתוב שיש I\*L אבל בפועל זה , בגלל ש I נע בערכים בין 1 ל-4 וגם L נע בין 1 ל-4 אנחנו מקבלים טבלת חום. ככל שהסיכון השורשי גבוה יותר כך מצופה מאיתנו להתחיל לטפל בו כמה שיותר מהר דחוף כי הוא סיכון שורשי גבוה במיוחד.

* תמונה שמכילה שולחן

  התיאור נוצר באופן אוטומטיהרעיון הוא לקחת את כלל הסיכונים שזיהינו ברמת הארגון (גם הסיכונים לתהליכים וגם סיכונים לנכסים תוה"ג 2.0 מעודדת לעבוד לפי הערכת הסיכונים לתהליכים עסקיים בעדיפות גבוהה מאשר לנכסים).
* לאחר שעושים את החישובים מגיעים ל2 תובנות -   
  1. ברמה היחסית – איפה נמצאים הסיכונים שלנו ברמה נמוכה\בינונית\ גבוהה  
  2. נחשוב במה אנחנו נרצה לטפל קודם  
  זה ייתן לנו תמונה כללית כדי להבין איפה אנחנו נמצאים לפני שעשינו משהו.

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי**"סיכון שיורי" –** מסתכלים איזה בקרות קיימות לאותם הנכסים\ תהליכים שמיפינו, לכל אחת מהבקרות יש ערך מסוים ואנחנו יכולים להחליט באופן שרירותי שהיישום של בקרה מסוימת מוריד את רמת הסיכון לדוג' ב2 רמות. הסיכון עבור התהליך\נכס לאחר מיפוי של הבקרות הקיימות בארגון נקרא סיכון שיורי.  
סיכון שיורי = הסיכון שנשאר לאחר שקלול הבקרות.  
סיכון שיורי = סיכון שורשי – הבקרות.

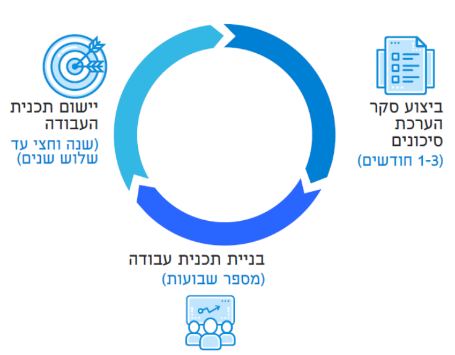
* 1. **אומדן הסיכון Risk Assessment** – אנחנו עושים הערכת הסיכונים שנותרו על מנת להיערך לשלב 3.1 ששם אנחנו מתחילים להפעיל אחת מ4 האסטרטגיות לטיפול בסיכון.  
     בשלב זה אנחנו מסתכלים על הסיכונים השיורים שלנו ואנחנו צריכים להסתכל על כלל התהליכים\ נכסים שאפיינו ועשינו להם הערכת סיכון על מנת להבין איך להתחיל לטפל בהם.  
     ניתן להשתמש בטבלה שהמטרה שלה למפות את הסיכונים על התהליכים ובכך להסתכל על כל הנתונים שאספנו, אנחנו מתסכלים על סבירות, עוצמת הנזק, סיכון שורשי, בקרות קיימות וסיכון שיורי.  
     אחרי שיש לנו רשימה מדורגת של הסיכונים אנחנו צריכים להסתכל על כלל הסיכונים.

**Risk Appetite (תאבון הסיכון) –** ההגדרה של אותה רמת הסיכון המקובלת על הארגון

**Target Risk** **(סיכון מטרה)** – כאשר רמת הסיכון השיורי גבוהה ״מתיאבון סיכון״ של הארגון, יש לבנות תוכנית הפחתה ((**Mitigation Plan** שמטרתה להפחית את הסיכון השיורי לרמת הסיכון הרצויה (סיכון המטרה). אומר שצריך לעשות משהו עם הנכסים\ תהליכים כי הרמת סיכון שלהם גבוהה ממה שהארגון מוכן לספוג (תאבון הסיכון) ואז צריך לעבוד לפי 4 האסטרטגיות.

1. **הטיפול בסיכון –** 
   1. **הגדרת אופן המענה –** השקעת תשומות להפחתת הסיכון צריכה להתבצע תוך שקלול של מספר פרמטרים: מבחן עלות-תועלת כלכלית לארגון, משך ההטמעה, רמת הסבירות להתממשות הסיכון, חובות משפטיות של הארגון מכוח התקשרות עם ספקים ו/או מכוח חוק ורגולציה, שיקולים מוסריים (דוגמת אחריות חברתית, פרמטרים נוספים שעליהם החליטה הנהלת הארגון. בשלב הזה הארגון יסווג כל אחת מהסיכונים תחת 4 האפשרויות:   
      **קבלת הסיכון Risk Acceptance –** מודעים לעובדה שקיים הסיכון ולמרות זאת אנחנו מחליטים לחיות איתו. יכול לקרות מהחלטות עסקיות או החלטות שנובעות מחוסר במשאבים (אנשים, תקציבים, זמן וכו'). החלטה לא טובה כי או שהארגון צריך להוריד את תאבון הסיכון שלו או שהוא מהמר מראש לחיות תחת איום מסוים כל הזמן. לאורך הזמן החלטה לא טובה.  **הפחתת הסיכון Risk Reduction** – בין הדרכים המומלצות אך לא תמיד אפשרית. צריכים לראות איך ומה ניתן לעשות מבחינת יישום והטמעת הגנות נוספות. חלק מההגנות יכולות להיות שהן בכלל יפחיתו את ההסתברות להתקפות מסוג מסוים (לדוג' צמצום משטח התקיפה).   
      **העברת הסיכון Risk Transfer** – במקרים שבהם יש לבצע את הפעילות, אך הארגון אינו מעוניין להחזיק במשאבי ההגנה הנדרשים, אפשר להעביר את הפעילות לצד ג'.   
      **דחיית הסיכון Risk Avoidance –** אנחנו מבינים שהסיכון הוא גבוה והנזק כתוצאה מהתרחשות האירוע יהיה כל כך משמעותי כך שאנחנו דוחים את הפעילות.
   2. **יישום והטמעה של בקרות הגנה –** כל הבקרות מסודרות לפי ה cyber security framework. צמצמו את כמות הבקרות אבל הכניסו לכל בקרה עומק יישום (הגדירו מספר רמות יישום לכל אחת מהבקרות), עכשיו מצופה מאנשים שעובדים עם זה בפועל איזה יישום בקרה מתאים\ לא מתאים. בנק הבקרות מיושם בניגוד לתקנים אחרים בטבלת האקסל, יותר מסורבל מבעבר.  
      \* למבחן צריך לדעת את השקפים אבל לא את הקובץ אקסל.  
      תוה"ג מעודדת עבודה עפ"י תהלכים עסקיים, היות ומבינים את האיום ברמה אסטרטגית על תהליך  
      לקחת את הקובץ לעבור על כל הבקרות ולזהות את ערך הנכס שלי (I) ולבחור את הבקרות הנכונות, אם הנכס 3 אז את כל הבקרות מ1 עד 3, אם הנכס הוא 2 אז מ1 עד 2.
2. רוב מוחלט של ההתקפות על ארגונים מתבצע לרוב על פי 3 ערוצים:  
   1. ממשקים חיצונים  
   2. תוכנות זדוניות  
   3. גלישה לאתרים נגועים

אם אנחנו מבינים שזה הרוב אנחנו צריכים להיערך בהתאם. כשאנחנו בונים תוכנית עבודה במקום ללכת לשיטה של ציות ולקחת את 120 הבקרות ולסמן על עיוור מה אנחנו צריכים ליישם, עדיף לחשוב בשיטה של תהליכים עסקיים.  
אם אנחנו מבינים את 3 הערוצים האלה ונדע לבנות להם מענה ראוי, אנחנו נדע לתת מענה יעיל ל2 ערוצי ההתקפה (אחד מהם הוא zero days ולכן לא ניתן לתת לו מענה).

1. **ביקורת ובקרה רציפה –**

חמשת השלבים צריכים לחזור על עצמם לפחות פעם בשנה או כפונקציית איומים או שנויים בסביבה החיצונית או קונפליקטים מדינים.  
אנחנו צריכים להבין שהארגון לא חי לבד ויש לו ספקים, לקוחות, עובד בענן וכו'. אחרי שהסתכלנו כפי פנים צריך להסתכל גם כלפי חוץ.

3.4.22

שיעור 8:

**בקרות:**

- **Identify**עוסקת בכל הנושא של הבנה והגדרה של הסיכונים. יש בה 2 קטגוריות עיקריות:

אחריות הנהלה (4), ניהול הסיכונים (3). בסוגריים כתוב את מספר הבקרות שיש בכל קטגוריה לפי התוה"ג.

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי

הבקרות כמו רמת הנזק (Impact) מחולקים ל4 רמות מ 1 (בסיסי) עד 4. אם יש הערך של הנכס הוא 2 צריך ליישם את בקרות 1 ו-2.

**Protect –** המשפחה הכי גדולה, עוסקת בפיתוח ויישום של ההגנות הדרושות על מנת לספק את התפעול של העסק. היא מכילה 13 מתוך 19 קטגוריות בתורת ההגנה

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטיתמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

במשפחה הזאת מופיעות גם בקרות גם ברמה 4 והן הכי קשות ומסובכות ליישום.

במשפחה הזאת יש בקרה של מיסוך גלי RF.

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי**Detect -** 2 קטגוריות הגנת סייבר פרואקטיבית ומערך ניטור מרכזי

* למבחן צריך לדעת לאיזה משפחה משתייכות הבקרות לפי היגיון.

אין צורך לזכור את הבקרות בע"פ.

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי**Respond & Recover**

כל צבע זאת משפחה שונה.

1. **Identify** – עוסקת בכלל הנהלים והאחריות, Policies, Standards, Baselines, Guidelines, and Procedures.
2. **Protect** – עוסקת בין היתר בפיתוח ויישום של הבקרות.
   1. **Access Control** - הפעילות הכי בסיסית וחיונית בכל ארגון. 2 מונחי יסוד שיש להכיר:
      1. **Subject** – מדברים על יישות שמקבלת מידע (משתמשים – אנושי, מערכות – לא אנושי), משתמשים, תוכנה, תהליכים, תוכנות, מחשבים, מסדי נתונים וכו'.
      2. **Object –** מי שמספק את המידע או את הגישה למידע. יכול להיות אובייקט לא אנושי (תוכנה, מסדי נתונים, מחשבים...) המטרה שלהם לאחסן ולספק מידע.

הקונספט של בקרת גישה עוסק בכלל הפעילויות הקשורות בזיהוי וניטור של גישה או מניעת הגישה למשאבים ארגונים. וכאשר אנחנו מדברים על כל התהליכים ובכל מה שכלול באישור או מניעת הגישה אנחנו מטבע הדברים מדברים על כל מה שכרוך בתוכן הזה של בקרה. בקרה יכולה להיות תהליכים, נהלים, תוכנה, חומרה או שילוב האלמנטים שמיועדים לתת או למנוע את הגישה, לנטר ולרשום את הניסיונות לגישה וכמובן לנטר ולבקר את האישורים מבחינת הגישה ושימוש באובייקט.  
בתהליך הזה מוערבים 2 צדדים Subject ו object.

בקרת גישה היא נדרשת כתנאי הכרחי על מנת שאנחנו נדע שאנחנו מסוגלים לשמור על סודיות, שלמות וזמינות (CIA) של המשאבים הארגוניים שלנו.

**סוגי בקרת גישה:**

1. Preventative(מונעת) – מטרתה למנוע גישה בלתי מורשית או לא רצויה. דוגמאות כוללות בקרות מעולם פיזי, דיגיטלי, נהלים**.**
2. Detective(מגלה) – מטרתה לגלות את הפעילות הבלתי מורשית או לא רצויה. דוגמאות שמכילות עולמות תוכן פיזיים, דיגיטליים ונהלים.
3. Corrective(מתקנת) – מטרתה לתקן עד כמה שאפשר מהרגע שמזהים חריגה בגישה. לדוגמה מערכות שמסוגלות להוריד חלק מהמערכות בזמן אמת.
4. Deterrent(מרתיעה) – הרעיון הוא איך אנחנו מסוגלים להרתיע כדי לא להגיע למצב שצריך להגן על משהו. דוגמאות מעולמות התוכן הפיזיים, הנהלים וקצת עולם דיגיטלי.
5. Recovery (משחזרת\ להתאושש) – להחזיר את המצב שיהיו לנו בקרות גישה אם מישהו פרץ את כל הבקרות. דוגמאות שחזור של ACLM
6. Compensation(מפצה\ עוזר) – איך ניתן לעזור במעקף על ביצוע או חוסר פגיעה שעוסקות ב access control. הדוגמאות יבואו לרוב מהעולם הפיזי או תהליכים.
7. Directive (מנחה) – מהן אותן הפעילויות שאנחנו יכולים לעשות על מנת לשמר את המילוי של אותן הבקרות שעוסקות ב access control. דוגמאות: כל העולם הפיזי ומסתיים בתהליכים והעלאת המודעות של המשתמשים.

תמונהההההההההההההההה

לאחר שהבנו את 7 הסוגים של access control נראה איך ניישם אותם. היישומיים יכולים לבוא מעולם של Administrative, Logical/Technical ו Physical.

Administrative (ניהולי) – לרוב יהיה מדובר בכל המשפחות של תהליכים ונהלים.

Logical/Technical – תוכנה וחומרה.

Physical – כל החסם הפיזי, העולם המוחשי

**The Process of Accountability –**

אנחנו עוסקים בבקרת גישה כי אנחנו מדברים על לקיחת אחריות (Accountability), רוב הפעמים אי אפשר לדעת מי הפעיל את התהליך.  
תהליך ה Accountability מסביר את כך שברגע שאנשים מקבלים שם משתמש וסיסמה לכל משאב ארגוני הם מתחילים להיות אחראים על כל מה שקורה דרך השם משתמש שלהם.

לאחר שמשתמש עובר את כל התהליכים של identification, authentication, authorizationלא ניתן להגיד מי הבן אדם שעמד מאחורי הדברים האלה. לדוגמה אם השארתי את היוזר פתוח במחשב ולא נעלתי את המסך.

**Identification (הזדהות)** – השלב הראשון. תהליך ההזדהות מתחיל עם שם המשתמש, כל קומבינציה שהיא צריכה להיות חד חד ערכית מול בן אדם אמיתי לבן היוזר שלו.  
מהרגע שמישהו נכנס למערכת תחת שם המשתמש בעל השם משתמש אחראי על כל מה שיקרה.

**Authentication (אימות)** – השלב השני. מיועד להשלים את התהליך שהתחלתי. מיועד לאמת את המשתמש, עד כמה זה באמת הוא. נהוג לזהות 3 סוגים של authentication.

1. **Type 1** – something you know
   1. **Password –** סיסמה לא כדי להרכיב מת.ז, שם, טלפון וכל דבר שניתן לעלות עליו מהרשתות החברתיות.  
      שתי סוגי מתקפות brute force (עובדת על כלל התווים הקיימים ועושה הגרלה על התווים האלה) ו dictionary attack.
2. **Type 2** – something you have
3. **Type 3** – something you are, טביעת אצבע, צילום רשתית, דגימה גנטית, כל דבר שמאפשר לנו לעשות את שלב האימות הרבה יותר אמין.

בנוסף 2 נוספים שעוזרים לגלות אנומליות בעיסוק שלנו, מיקום, IP

1. Something you do – עיסוק, חלק מה something you are
2. Somewhere you are – מיקום

**Authorization (הרשאה) –** מתן או אי מתן הרשאות לשימוש באובייקטים. אחרי שעברנו את 2 השלבים הראשונים של הAC (Identification ו Authentication) עוד לא קיבלנו גישה אלא צריך לקבל הרשאה.  
יכול להיות מצב שנכנסו לרשת ארגונית אבל אין לנו הרשאה לעשות דברים ברשת.

2 מתודולוגיות בסיסיות :

centralized and decentralized (or distributed).

לכל אחת מהמתודולוגיות הללו יש יתרונות וחסרונות.

היתרון של centralized שאנחנו מנהלים את כל ההרשאות לאובייקטים ארגונים במקום אחד. זה זול יותר  
החסרון הוא נקודת הכשל היחידה.

Decentralized – לחלק מהמערכות יש בהתחלה אפשרות גישה למינימום האפשרי ולאחר מכן נבקש הרשאה בהתאם למה שצריך.

היתרון זה שמנתקים את הנקודת כשל של השיטה הקודמת.

החסרון זה המחיר.

לרוב ארגונים משלבים את שניהם.

**טכניקות ליישום המתודולוגיות:**

Single sign-on (SSO) – טכניקה ל centralize, לאחר שנכנסו פעם אחת לרשת קיבלנו סט הרשאות בסיסיות בהתאם להחלטה של הארגון.

המטרה שלו להקטין את מספר הבקשות של היוזר להזדהות.  
יתרון – נוח למשתמש  
חסרון – מסוכן

24.4.22

שיעור 9:

כאשר מדברים טכניקות לבקרת גישה מתבססים על ACL – Access control list.

יישום של המתודולוגיות centralized ו Decentralized

discretionary– מבודלת, שייך ל Decentralized, יש מנהלים שונים שעובדים על ACL שונים.  
אנחנו יכולים לזהות את המשתמשים לפי זהות המשתמש או לקבץ אותם לפי תנאים מסוימים.

Nondiscretionary – לא מבודל, לא מבוסס על ישות המשתמש הספציפי או קבוצות המשמשים, בדר"כ עובד לפי סט חוקים שמוגדרים מראש.   
לרוב נראה 3 סוגי חוקים בארגונים : mandatory, role base, task base.

Mandatory – לפי דרגה לדוגמה בצבא, נותנים גישה לכולם

role base – נותנים גישה לפי התפקיד.

task base – נותנים גישה לפי משימה.

Auditing and Accountability –

Accountability, האחריות על הפרסונה הדיגיטלית.

Auditing – תהליך של בקרה.

**Protect - Infrastructure Security**

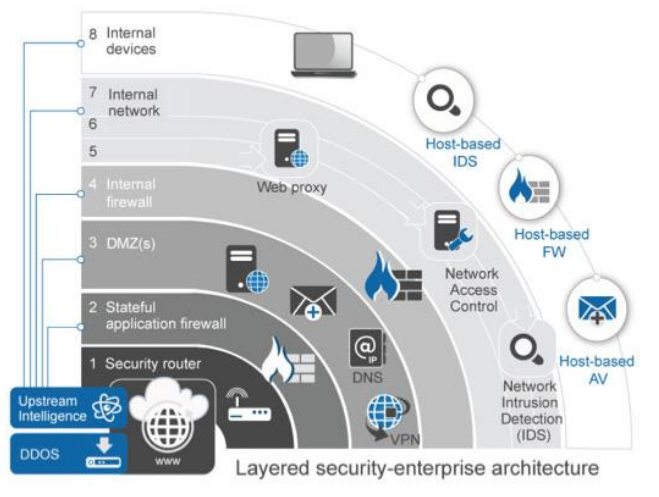
הגנה לפי שכבות, כדי שאם לא נעצור את המתקפה בשלב אחד נוכל לעצור אותה בשלב אחר.



הגנה במרחב הפיזי

תשתיות – כל מה שמהווה את התנאים ההכרחיים לקיום העסק, כל הנושא של אופרציה לניהול התשתיות (רשת לדוג'). מדברים על מגוון רחב של טכנולוגיות, כלים ונהלים וגם משתמשים ספציפיים הם אלה שיעסקו לרוב בניהול של התשתיות שלנו.

Network Security – תהליך מורכב שמכיל בתוכו סט של אסטרטגיות, תהליכים וטכנולוגיות כדי לוודא שהרשת הארגונית שלנו חסינה משימוש לא מורשה. צריך לראות שהרשת שלנו גם מוגנת וחסינה מפני התקפות ופעילויות בתוך הרשת הזאת.

יש מספר טכנולוגיות מאוד בסיסיות:

1. Access control
2. Firewall
3. IDS&IPS

חומת האש היא שערי כניסה ויציאה מהארגון. חומת האש הבסיסית היא פתרון שמההתחלה היה מאוד מגובל ביכולות גילוי שלו.

DMZ – נועד לתת מענה לצורך של תקשורת עם משתמשים חיצוניים לארגון שצריך לאפשר גישה גם מבפנים וגם מבחוץ. במקור נועד לסנן וליצור הגנה בין העולם בחוץ לעולם שבפנים.

בדר"כ בארכיטקטורה היו 2 חומות אש אחת לפני הDMZ ואחד אחרי.

IDS&IPS – אנחנו בתוך הרשת הארגונית ויש סט של טכנולוגיות \ מערכות\ סנסורים ששייכות למשפחה של IDS&IPS.

IDS – detective , מזהה

IPS – prevention, שדרוג של IDS בנוסף לגלות היא גם מונעת

שתיהן יכולות להיות גם ברמת הרשת וגם ברמת יחידות קצה.

IDS – זו מערכת שבדר"כ מבוססת על יכולת הסתכלות אל תוך המידע של הפקטות והיא מסוגלת לגלות את החתימות האלקטרוניות. ברגע שהיא מזהה לפי החתימה האלקטרונית חבילות מידע שמזוהות כזדוניות המערכת מתריעה.

IPS – מערכת מתקדמת יותר מהIDS, יש להן מערכות sandbox.

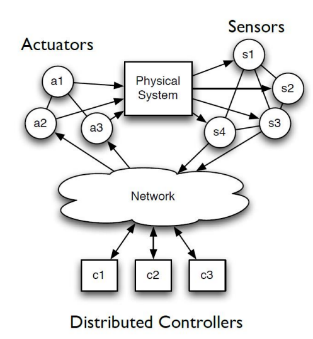
Next-Generation Firewall (NGFW) – לוקח את המערכות ומאחד אותן ביחד. נותנים את הפונקציונלית של ניצוח ברמת הפקטות. במקום שיהיו 3 מוצרים יהיה מוצר אחד . לא יושב בנקודת אחת, יושב גם ביחידות הקצה וגם ברמת הרשת.

Unified Threat Management (UTM) HW/SW for SMBs. – מיועד בדרך כלל לארגונים בינוניים קטנים, שאין לארגון יכולות מתקדמות לבניית השכבות (פיזור הסנסורים וכו') זה ייתן להם פתרון ברמה הפשטנית בבת אחת.

Hardware Security - מודלי חומרה ייעודיים בדרך בכלל למנגנוני הצפנה והם מכניסים רמה נוספת של אבטחה.

Cyber-Physical Systems **(CPS)** – מערכת את 2 העולמות, הפיזי והסייבר.

הרעיון הוא איך אנחנו יכולים לתת מענה לאתגרים המשותפים לכלל המערכת שמאגדות את 2 עולמות התוכן (הפיזי והדיגיטלי).

האלמנטים שתמיד יופיעו הם sensors, actuators, control processing units, and communication devices.

Sensors – חיישנים, תפקידים לחוש משהו, טמפ', גז, לחות, לחץ וכו'. רובם עובדים בשיטה אנלוגית ולא דיגיטלית לדוג' מערכת השקיה

Actuators – סנסור מתקדם, הוא לא רק מסוגל לחוש ולדווח אלא הוא מסוגל גם לבצע פקודה בסיסית כגון להדליק\ לכבות, לפתוח\ לסגור.

מי שנותן ל actuators ול Sensors פקודות הם הdistributed controllers.

סוגי התקפות הקיימים בכל אחד מרשתות הCPS:

Attack 1: An attacker compromised a sensor – בסטקסנט הצנטריפוגות הסתובבו מאוד מהר, ייתכן שה Sensors לא עבדו או שהם דיווח מידע שגוי.

Attack 2: delay or block the information from the sensors to the controller – השהיה או פגיעה בתקשורת של הסנסור.

Attack 3: compromised the controller and sends incorrect control signals to the actuators – הבקרים צריכים לאסוף כדי להעביר הלאה. הקונטרול לא עושה את מה שהוא צריך לעשות וכתוצאה מכך הוא לא מעיר פקודה ל Actuators. לדוג' בסטקסנט יש בקרים והם אמורים לזהות את מהירות הסיבוב של הצנטריפוגה ולתת פקודה ל Actuators לשנות את המהירות.

Attack 4: who can delay or block any control command – ה Actuators לא התערבו בתהליך שינוי המהירות של המנועים שסובבו את הצנטריפוגות.

Attack 5: who can compromise the actuators and execute a control action that is different to what the controller intended. – Actuators לא נתן פקודה או נתן פקודה לא נכונה, ייתכן ועשה גם וגם.

Attack 6: physically attack the system – מדברת על שינוי התהליכים הפיזים, לדוגמה לפגוע בצינור.

Attack 7: delay or block communications – התקפות על מערכת התקשורת, פגיעה בין התקשורת של הקונטרולים לSCADA (המערכת שמנהלת הכל)

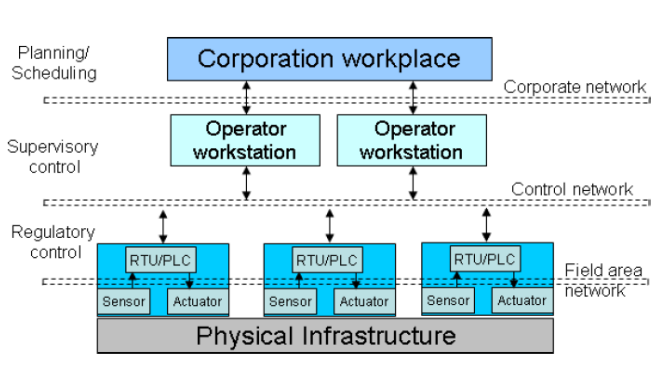
Attack 8: send malicious control or configuration changes to the controller – המערכת מוטעית ונופלת לא נכון, נותנת פקודות שגויות.

1.5.22

שיעור 10:

כל דבר שקשור IOT אנחנו מקנים להם תכונות של בן אדם, האובייקט יכול לחוש משהו ולספר מה הוא חש. העולמות הפיזיים, הייצור, פסי הייצור.

עולם הCPS נולד כמענה לצורך למצוא מכנה משותף על מנת להגדיר, לזהות, לחקור ולתת מענה לבעיות שהן משותפות לכלל העולמות הפיזיים כאשר אנחנו רוצים את העולם הפיזי לכללי, לזהות מה משותף.

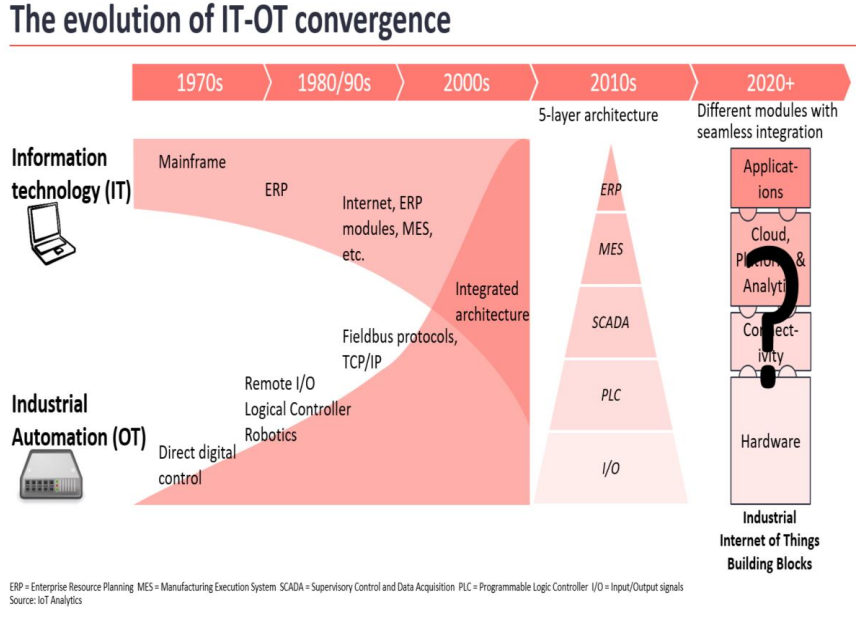


Industrial Control Systems – מערכות בקרה תעשייתיות, ניהול של התהליכים הפיזים:

רואים בהן את כל אותם האלמנטים:

Physical infrastructure -בסטקנט אפשר להתייחס למתקנים שבהם מעשירים את האורניום, כורים...  
לדוגמה ברכבת, המסילות, התשתית הפיזית של הרמזורים, מסילות. הsensor יודע איפה הרכבת נמצאת והוא מעביר לactuator והוא נותן פקודה להזיז את המסילה של הרכבת. היא מנוטרת ע"י בקרים (PLC – Programable logical controller), מכונה הכי בסיסית שמיושמת על בקרים הכי פשוטים ופרימיטיביים בדרך כלל ללא מערכת הפעלה, בתוכם מיישמים state machine, הם מיושמים כדבר הכי בסיסים, אם מגיע interrupt X לregistry צריך לבצע Y.

Sensor\ actuator – ברכבות יש הרבה Sensor, actuators והם מנוטרים על ידי PLC, ה actuatorsעושה את זה בפועל.RTU (remote terminal unit) – בקר הרבה יותר משוכלל שבדר"כ מפקח על מספר actuators , סנסורים וPLC. איפשהו יושבת יחידת בקרה מתוחכמת שהיא מפקחת על מספר אלמנטים המחוברים אליה. המערכות RTU הם בקרים שבדר"כ יש בתוכם מערכת הפעלה ייעודית למערכות של הReal Time.

במרכזי שליטה ובקרה (שו"ב) יש SCADA (Supervisory control and data acquisition) מקבלות DATA מערוצי תקשורת פרטיים והמערכות האלה מאפשרות לאנשים שיושבים במרכזים הללו לנהל את רשת החשמל.

IT OT convergence – מה שהתחיל לקרות בשנות ה2000 וממשיך עד היום, כתוצאה מהתהליך הזה אנחנו נמצאים כל הזמן באתגר.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

Supply Chain – בשרשרת האספקה יש ניצול של שכבת האמון, כאשר אנחנו עובדים הספקים שלנו אנחנו סומכים עליהם ומכוח ההרגל אנחנו סומכים עליהם יותר שלפעמים אנחנו עושים הרבה מאוד טובות והקלות בדרך ברמת העבודה שלנו איתם.

כדי לקבוע מהי הרמה של מדיניות שצריך לקבוע .

מחשוב ענן:

לקראת שנות ה2000 היה לחץ גדול על אנשי המקצוע ואחת מההכנות לקראת השינוי היה גיבוי. וכך נוצר צורך במקום אחסון (שרתים פיזיים) וקמו חברות שהקימו חוות שרתים והן שימשו את החברות והלקוחות לאחסון. החברות הללו החליטו לתת עוד שירותים וזה גרם לעידן של מחשוב הענן.

כשאנחנו מדברים על מחשוב אנחנו מדברים על 5 המאפיינים, 3 מודלי האישיות ו4 מודלי הטעמת המערכות.

חמשת המאפיינים של הטכנולוגיה:

1. Network access - הרעיון הוא שללא קשר ליכולת המחשוב ביחידת הקצה אני מסוגל להגיע ולהנות מרוב השירותים שאקבל מהענן. אם יש לי גישה לאינטרנט אני אקבל את השירותים, היחידת קצה יכולה להיות הכי פשוטה או הכי מתוחכמת אבל כל עוד יש לי חיבור לאינטרנט אני אקבל שירותים.
2. Rapid clasticity – אני יכול לקבל את המשאבים בתור נותן שירות\ משתמש שירותי ענן בצורה נורא גמישה, אם אצטרך יותר אקבל יותר אם פחות אז פחות
3. Measured service – שירות שניתן למדידה, בלי עקרון זה השניים הקודמים לא יכולים להתקיים.  
   טכנולוגית מחשוב ענן מאפשרת לי לדעת ברזולוציה הכי נמוכה שיש מה השתמשתי, כמה השתמשתי ומתי השתמשתי.
4. On demand self service – אומר שאם אני עכשיו בתור צרכן שירותי ענן רוצה להגדיל את יכולות המחשוב\ חישוב\ אחסון. אם אני רוצה להגדיל אחת מהם אפשר לעשות את זה מתי שרוצים ואיך שרוצים ולא צריך שום דבר באמצע (אפילו לא בן אדם).
5. Resource pooling – טכנולוגיה מיוחדת שפיתחו ספקי מחשוב ענן. מונח שאומר שאני ספק טכנולוגיה מתייחס לכלל הטכנולוגיות של הטיפול ואני מחלק אותן בין הלקוחות שלי ללא שום קשר למשאבים הפיזיים. על אותו שרת יכולות לרוץ לי אפליקציות של לקוח X ולקוח Y. זה אפשרי על ידי העקרון של Resource pooling. זה סוג של ערוצים וירטואליים וחלוקה וירטואלית של תהליכים פיזיים (חומרה) וניתן להריץ מגוון ערוצים וירטואליים על אותה חומרה.

חמשת המאפיינים מאפשרים את כל היופי של מחשוב ענן.

IaaS – לדוג' מחשב ללא מערכת הפעלה, עבודה דרך CMD. כל הנושא של ניהול החומרה ויצירת סביבת העבודה והתקנת מערכת ההפעלה כל אלה יכולים לעשות רק על ידי אנשים מקצועיים. מי שיש לו ידע בשרתים זה מתאים לו.

PaaS – לדוג' מחשב עם מערכת הפעלה, יכול לעשות מה שבאלי. מקבלים מערכת הפעלה בענן, לא צריך להכיר פקודות CMD ולקנפג, יש מערכת הפעלה.\

SaaS – פתרונות תוכנה, ממנפים את כל היתרונות של מחשוב ענן. מספקים שירות ללקוחות מבלי לדרוש מהם משהו שקשור לטכנולוגיה.