
## היכרות

מור בסן , בן 35 , נשוי +3

תואר Bsc - הנדסת תוכנה ותקשורת

תואר Msc - הנדסת מערכות

ניסיון : עתודאי , 10 שנים יחידות טכנולוגיות בצבא

כיום סמנכ"ל בבית תוכנה

## דרישות קורס

- בדיקת נוכחות תחילת שיעור
- מיני פרויקט והצגה לקראת סוף הסמסטר - 20 אחוז מהציון
- תרגילים - חובת הגשה - 10 אחוז
- מבחן מסכם - 70 אחוז
- פניות דרך המייל בלבד

## מטרות הקורס

- עקרונות באבטחת מידע
- ידע נרחב במושגים
- כיצד לבדוק האם המערכת מוגנת
  כיצד לשפר את ההגנה על המערכות
- סוגי התקיפות נוספים
- שיטות ומוצרי הגנה

## פתיחה


האם ניתן לגנוב מידע ממחשב שמנותק מהאינטרנט
ונמצא בחדר נעול ללא אפשרות גישה ?

## אבטחת מידע

הגנה מפני גישה, שימוש, חשיפה, ציתות, שיבוש, העתקה או השמדה של מידע ומערכות מידע מצד גורמים שאינם מורשים.

שאלה:
איך הייתם מגדירים "אבטחת מידע" ?

## כמה כותרות מהחדשות בתקופה האחרונה

כלכליסט

**נחשף קמפיין סייבר מתקדם שהופעל בידי האקרים המקושרים לקרמלין**

חברת סייבר חשפו נזקה מתקדמת בשם GreyEnergy, שחדרה לתשתיות אנרגיה ותובלה באוקראינה ופולין. בריטניה האשימה את רוסיה ישירות, וכינתה את מבצע הסייבר "קמפיין גלובלי, חסר-אחריות ומסוכן"

רפאל קאהאן 18.10.18 14:36

TechNation

**פייסבוק: ה-FBI חוקר גניבת פרטים אישיים של 30 מיליון משתמשים**

פרשת דליפת המידע הגדולה ביותר במולדות הרשת החברתית נחשפה לפני כשבועיים, אולם החברה הצהירה כי מדובר ב-30 מיליון משתמשים ולא 50 ■ החברה גם מסבירה מה היקף המידע שנגנב על ידי התוקפים ■ הפרצה תוקנה, אך פייסבוק לא יכולה בשלב הזה לחשוף מי עומד מאחורי התקיפה

רפאלה גינזבן | הכתבות במייל

21:48 12.10.2018

שמור 6 3

נסעתם בכביש 6? הפרטים שלכם דלפו לרשת

TheMarker - 29 Aug 2018

לקוח שמספר תעודת הזהות שלו מסתיים בספרות 993 ומספר לוחית הזיהוי שלו מסתיים בספרות 563 (המספרים המלאים שמורים במערכת) עלה על כביש חוצה ישראל ...

## שאלה:

אוקי, אני אתקין ANTIVIRUS במחשב \ פלאפון -
למה אני צריך ללמוד את הקורס ?

Symantec. avast! be free McAfee Proven Security

## סוגי האקרים

- כובע לבן
- כובע אפור
- כובע שחור

הבנת המניעים ודרכי הפעולה
תסייע לנו במניעת תקיפות והתגוננות

## אופי\מניע של קבוצות תוקפים ?

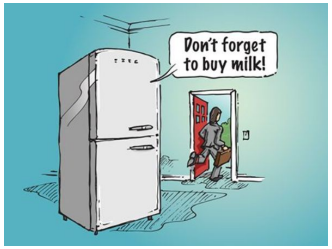
- פלילי
- גניבת כספים
- ריגול מדינה \ תעשיה
- גופי טרור
- וכו'

## מגמות בעולם הטכנולוגי

ריבוי מכשירים אלקטרונים חכמים

תלות רבה במחשוב ותקשורת

- Smartphone
- בלוקצ'יין (ביטקוין)
- בית חכם\IOT\מצלמות אבטחה
- רכב אוטונומי




ואיך זה יכול לפגוע בנו ?

## מתקפת סייבר ענקית על בתי חולים בבריטניה

16 בתי חולים גדולים בממלכה נפגעו, וכמה מהם נאלצו להעביר לבתי חולים אחרים מטופלים שהגיעו בשל מקרי חירום. בחלקם מחשבים ננעלו באמצעות תוכנות כופר. מוקדם יותר הוזהרו עובדי בתי החולים כי קיים איום ממשי של קבלת מיילים פוגעניים עם קבצים זדוניים. מפלגת הלייבור: "סיבה אמיתית לדאגה"

כלכליסט

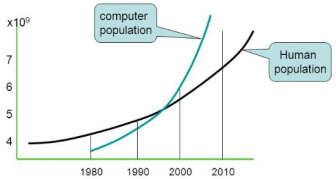
### יותר מאסון טבע: מתקפת סייבר עולמית תגרום נזק של 120 מיליארד דולר

לפי ניתוח שערכה חברת הביטוח לוידס, מתקפת סייבר גלובלית תגרום לנזק כספי עצום. לשם השוואה, ההוריקן קתרינה גרם לנזק של 108 מיליארד דולר. תרחיש יום הדין יהיה נפילת שרתי גוגל, אמזון או מיקרוסופט

רפאל קאהאן 17.07.17 12:15

## כפר גלובאלי

- מעל ל־3.3 מיליארד משתמשים
- מעל ל0.5 מליארד אתרים - נכון לשנת 2016
- 100 מליון מיילים ביום

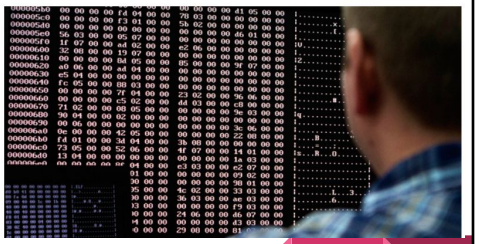



| משתמשי אינטרנט ברחבי העולם | | | |
|---|---|---|---|
| | 2005 | 2010 | 2016 |
| אוכלוסיית העולם | 6.5 מיליארד | 6.9 מיליארד | 7.3 מיליארד |
| משתמשים בכל העולם | 16% | 30% | 47% |
| משתמשים בעולם המתפתח | 8% | 21% | 40% |
| משתמשים בעולם המפותח | 51% | 67% | 81% |

## מתקפת הסייבר - בגלל מכשירים "חכמים"

מאות אלפי מצלמות רשת וסטרימרים שנדבקו בתוכנה זדונית הם שגרמו למתקפה הנרחבת ביותר מסוגה, שהפילה כמה מהאתרים הגדולים ביותר בעולם - כך סבורים מומחי אבטחת מידע. החשש: פרצות אבטחה יובילו למתקפות נוספות

חדשות 2 | החדשות | פורסם 22/10/16 10:34 | עודכן 22/10/16 15:44



## עקרונות אבטחה

- שלמות (integrity)
- סודיות (confidentiality)
- זמינות (availability)

מניעת שרות - DDOS

## רוצים לראות אילו מתקפות קורות כעת ?

לינק

## סיסמת אבטחה

"חוזק השרשרת הינה

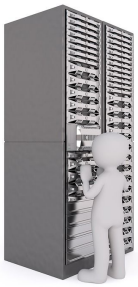
כחוזק החוליה החלשה"

## עקרונות אבטחה

לפי העקרונות שלמדנו :

במידה ואני מכבה את השרת של חברה כלשהי

האם זה גם סוג של בעיית אבטחה ?



Disaster recovery plan - DRP

## סיכום גורמי סיכון

- משתמשים (אי נעילת מחשב, חיבור USB נגוע)
- טכנולוגיות (מערכת הפעלה לא מעודכנת ועם פרצה)
- תהליכים (אי אבטחת מחשבים באמצעות סיסמה)

נוחות ⟷ אבטחה

## האתגר בהתגוננות

- משתמשים (מה יכולות התוקף?)
- טכנולוגיות (ZeroDays, שבירת קוד הצפנה)
- תהליכים (צירוף מקרים לא ידוע שיוצר חולשה)

**ריבוי אפשרויות תקיפה**

עלות גבוהה ⟷ סיכון איבוד אמון הציבר

Balance Game

## דוגמא לבעיות תהליכיות

דואר אלקטרוני - אירוע מזכירת מדינה שרה פיילין

אמזון - פירצה תהליך רכישה אשראי

## האתגר בהתגוננות

DARPA Challenge - security operating system

## כיצד נבנה תוכנית אבטחה

הגדרת תהליכים עיקריים

הגדרת מדיניות

הגדרת הרשאות

בחינת נקודות תורפה וחיזוקם

שכבת הגנה

## חולשות משתמשים

המחשב מוגן בסיסמה - אבל איזה סיסמה...

riva11

View Profile

Symantec Official Blog

### The Top 500 Worst Passwords of All Time

By: riva11

Created 13 Apr 2010 1 Comment

Do you think your password is unique in the world ? Please take some minutes to read the The Top 500 Worst P
of All Time .
Many interesting information are shown in this article, for example do you know that the all time most used pas
*123456* ? and the second is (of course) *password* ?

Here an extract: :

Lists the top 500 worst passwords

| NO | Top 1-100 | Top 101–200 | Top 201–300 | Top 301–400 | Top 401–500 |
|---|---|---|---|---|---|
| 1 | 123456 | porsche | firebird | prince | rosebud |
| 2 | password | guitar | butter | beach | jaguar |
| 3 | 12345678 | chelsea | united | amateur | great |