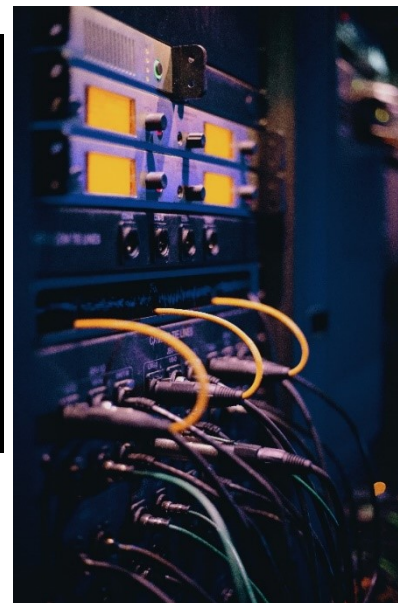


מושגי ייסוד בסייבר – חלק ב



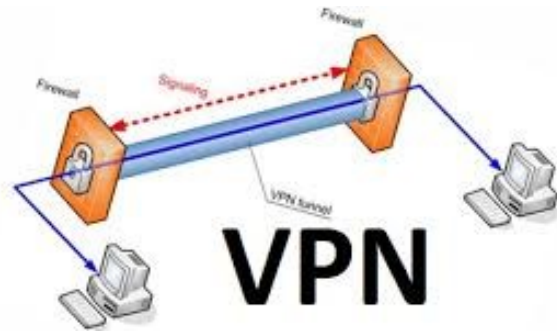
Yosi Shavit MBA, CISO, CISM, CDPSE - Information Security & Cyber Expert

Cellular: 058-6662242

Mail: yosish@gmail.com , yosish@sviva.gov.il

גישה מרחוק

לצורך גישה מרחוק נדרשים 3 דברים עיקריים:



1. תקשורת **מוצפנת** מהאינטרנט אל הארגון VPN רצוי מאד "לחתוך את ה-SESSION" המתחבר מבחוץ



2. זיהוי **חד-חד ערכי** של הגורם הניגש

3. רישום לוגים : מי התחבר, מתי נכנס, מתי יצא, לאיזה מערכות נכנס וכדומה.

שאלה: האם סיסמא מהווה זיהוי חד חד ערכי??

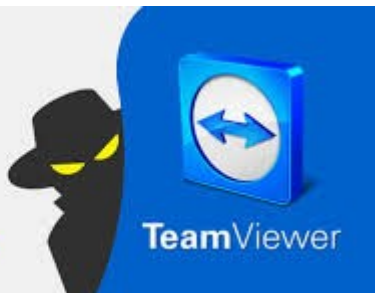
המלצות נוספות להתחברות מרחוק

□ משתמש חיצוני לארגון (ספק, נותן שירות) – יצירת משתמש חד – חד ערכי

User Name: matrix
Password: 123456

□ גישה מבחוץ אל ה-GATEWAY (חומת אש) ולא באמצעות גלישת WEB

Another
vulnerability,
this time
TeamViewer

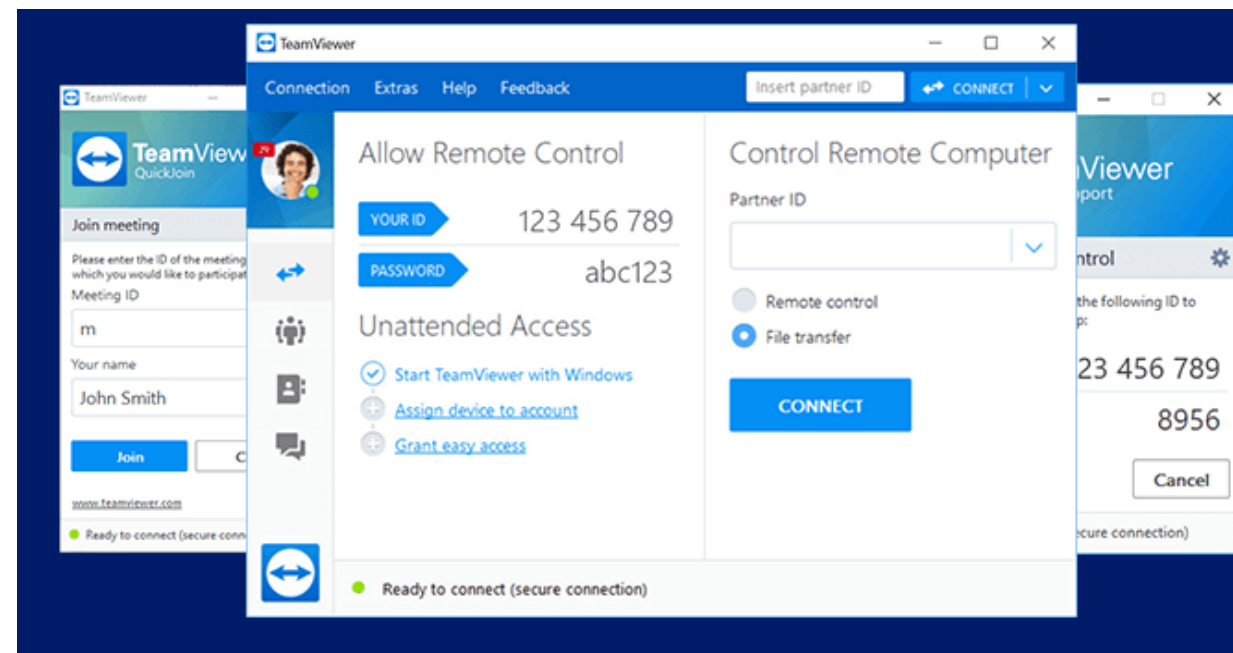


□ בדיקת תאימות התחנה המתחברת – עדכוני אבטחת מידע ואנטי-וירוס

□ החתמת משתמש /ספק חיצוני על הצהרה התחברות לצורך המטרה הספציפית שלשמה נועד

איך עובד TEAM-VIEWER?

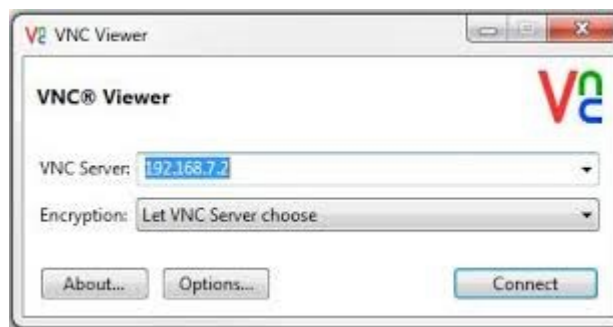
השתלטות ממחשב
השתלטות מטל סלולרי



תוכנות נוספות להשתלטות מרחוק מבוססות אינטרנט



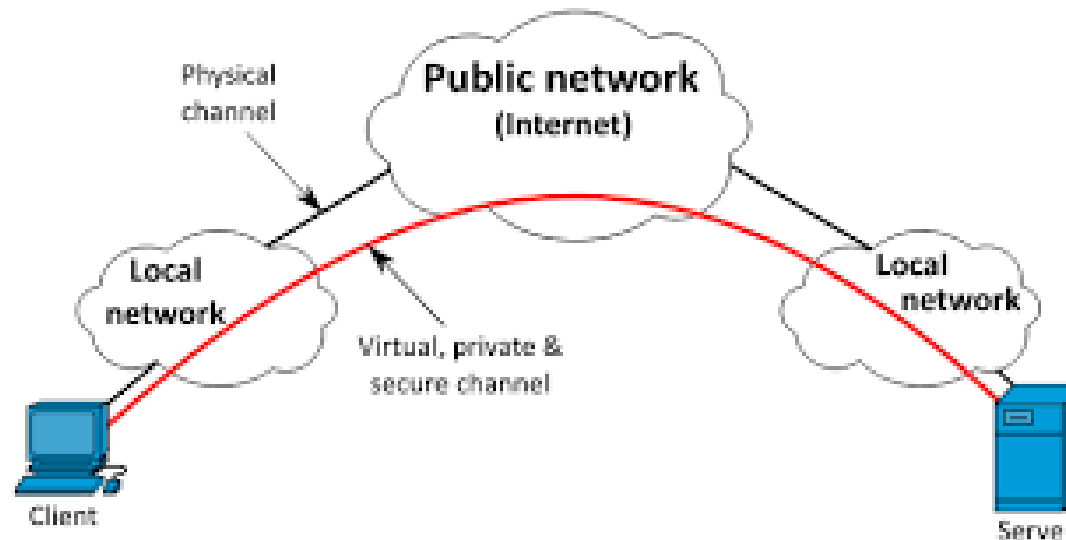
לא לאפשר אלא אם כן השימוש הוא פנימי בלבד למשל תכנת VNC.



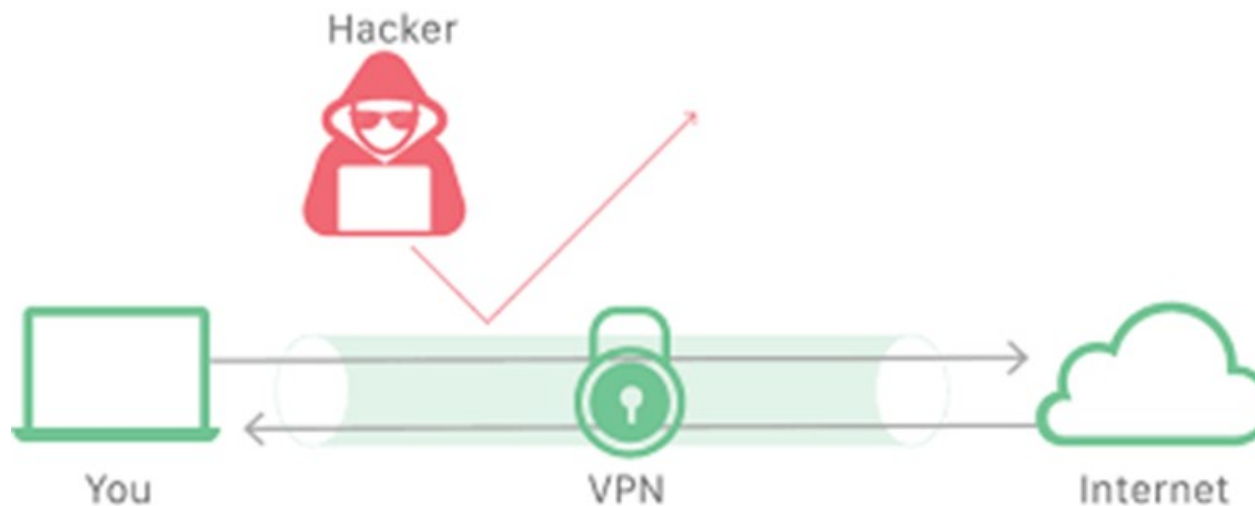
תקשורת אל הארגון - באמצעות VPN



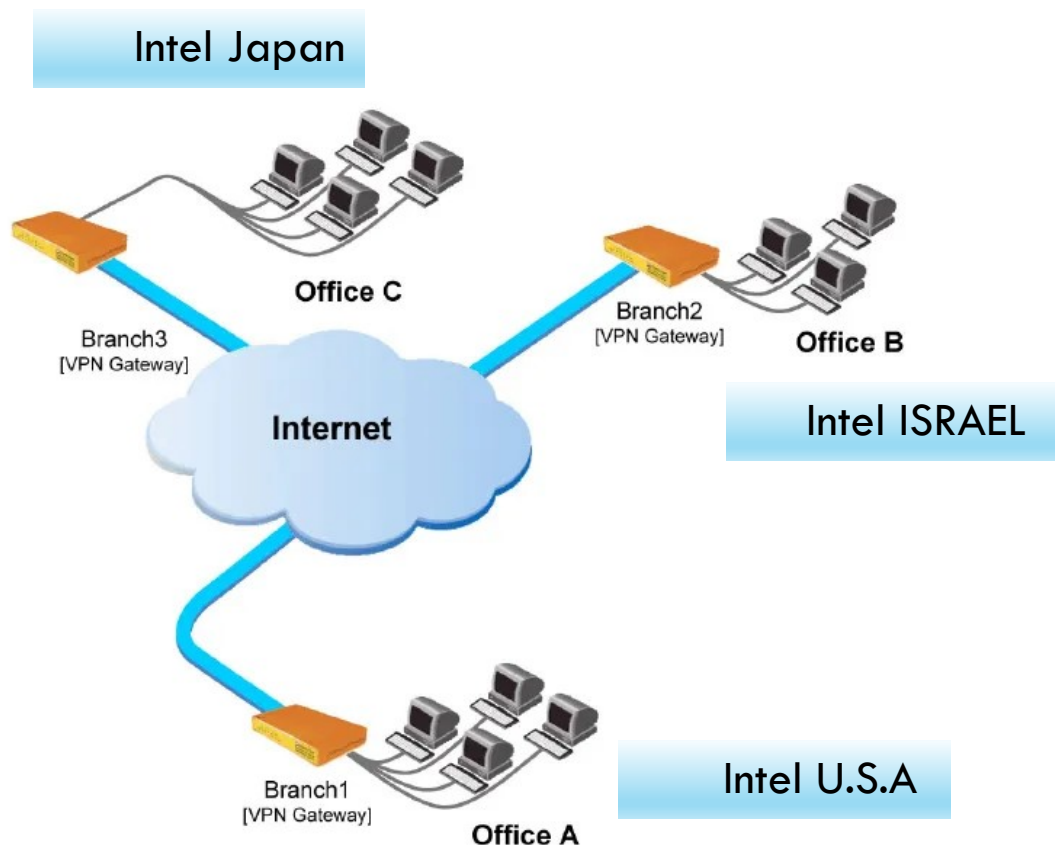
VPN = VIRTUAL PRIVATE NETWORK



תקשורת עוברת בצינור (TUNNEL) מוצפן

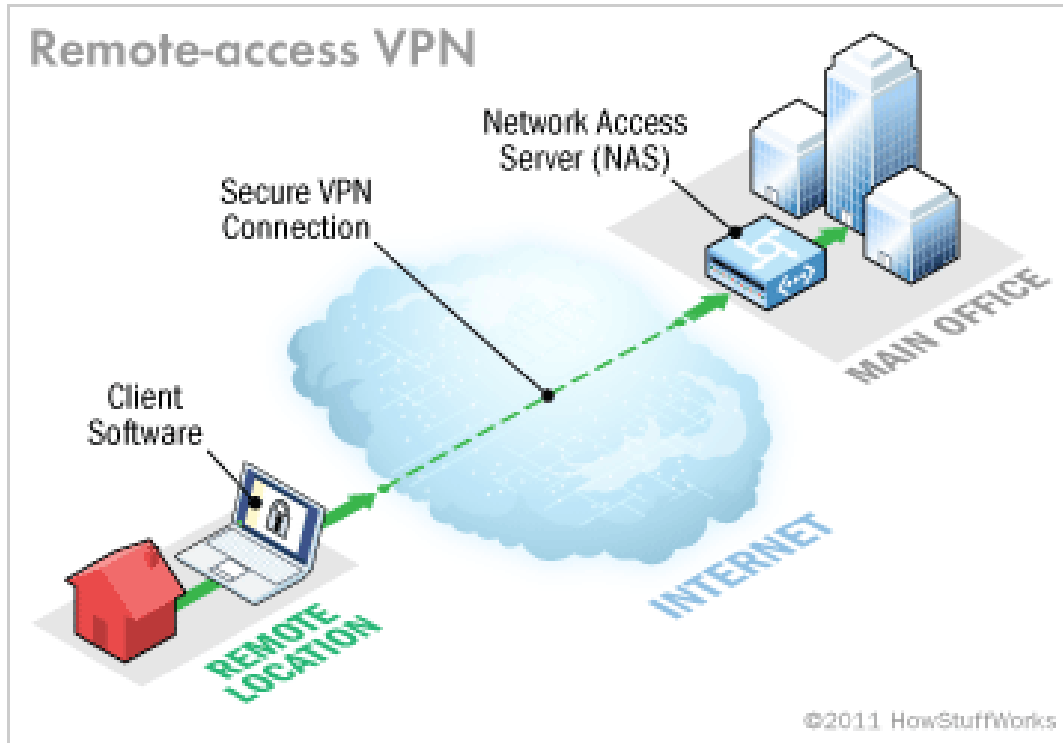


תקשורת אל הארגון - באמצעות VPN - שימושים



ארגון מפורז על פני שטח גיאוגרפי גדול

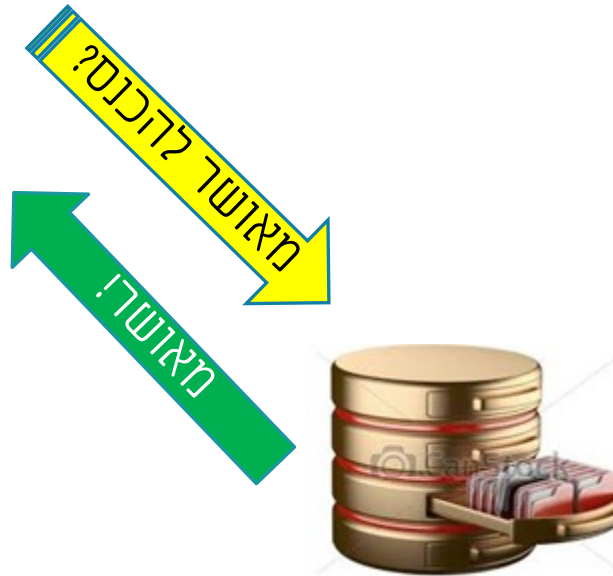
גישה מרחוק של משתמשים



הזדהות למערכת



שם משתמש: Hr105
 סיסמא: 123456



איך עובדת הזדהות ?

שם משתמש	סיסמא	סטטוס אישור
Uv451	123123	
Db633	11qq11	
Hr105	123456	
tp423	password	✓
-----	-----	
-----	-----	

סיסמאות נפוצות

208 הסיסמאות הנפוצות לפי נתונים שנאספו על ידי פורצים טורקיים רוב הסיסמאות נאספו, ככל הנראה, מהומלס ומפיצה האט, יש לא מעט סיסמאות שקשורות לשני האתרים האלה. המידע מבוסס על סט של כ-110,000 סיסמאות.

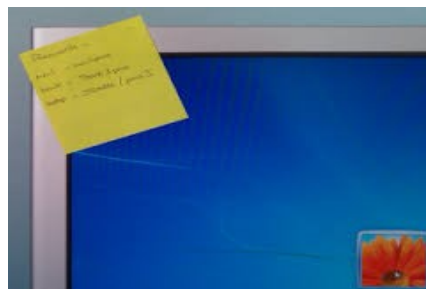
מספר סידורי	סיסמה	מופעים
1	123456	2419
2	1234	1875
3	12345	1115
4	12345678	445
5	123123	218
6	1111	216
7	qazwsx	189
8	1234567	164
9	0	155
10	123	154
11	121212	152
12	1212	139
13	111111	122
14	55555	109
15	pizza	100

הבעיה:
שימוש בסיסמאות חלשות

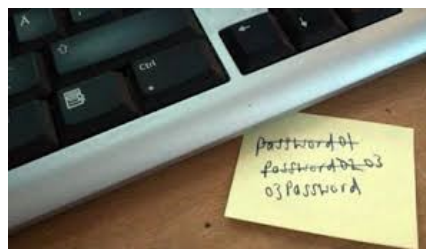
בעיות עם סיסמאות



➤ סיסמא קלה



➤ תולים על מסך המחשב



➤ שמים מתחת למקלדת

יש לזכור:

קיימות טכנולוגיות BRUTE FORCE וטכנולוגיות DICTIONARY מתקדמות לזיהוי סיסמאות ברשת

פתרונות לבעיית סיסמאות

פתרון:

- ✓ רצוי מאד 8 תווים אך לא פחות מ- 6 תווים
- ✓ מורכבות סיסמא (אות גדולה, קטנה, מספר, תו מיוחד) 3 מתוך ה-4

דוגמאות לסיסמאות שקל לזכור וקשה לפרוץ:



1. P@55w0rd

2. Pשדד'סרג

מהירות הפריצה לסיסמא קלה

(96^8)

P@55w0rd

26^8

password

Test a New Password

Enter in a password to see the maximum time it would take to crack that password. Use the slider under the year to see how much the maximum crack time has increased since 1982. Also slide up to 2020 to see how quickly a password might be cracked in the future.

Password: P@55w0rd Year: 2020

9 YEARS **6** MONTHS **2** WEEKS **4** DAYS **5** HOURS **54** MINUTES **32** SECONDS **79** JIFFIES **8** MILLISECONDS

Keys per second in 2020: 17042497.3 kps Word List: On Off

Better Buys

Test a New Password

Enter in a password to see the maximum time it would take to crack that password. Use the slider under the year to see how much the maximum crack time has increased since 1982. Also slide up to 2020 to see how quickly a password might be cracked in the future.

Password: password Year: 2020

0.19 MILLISECONDS

Keys per second in 2020: 17042497.3 kps Word List: On Off

Better Buys

<https://www.betterbuys.com/estimating-password-cracking-times/#:~:text=Nine%2Dcharacter%20passwords%20take%20five,bad%20for%20one%20little%20letter.>

מהירות הפריצה לסיסמאות

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %\$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

דאגו שהסיסמה תהיה באורך של 8 תווים לפחות ותכלול:

- שילוב של אותיות קטנות וגדולות (a-z, A-Z)
- ספרה אחת לפחות (0-9)
- תו מיוחד אחד לפחות (\$,%,&,@)

השאירו את פרטיכם האישיים ופרטים אודותיכם מחוץ לסיסמה.

שמות משמעותיים: שקלו להשתמש בהקשר - אם מדובר בניח בחשבון מקוון, חישוב על מילה המתקשרת אליו. למשל: אפשר לקשר את הסיסמה של חשבון הבנק, לשם הרחוב שבו הסיני מתנהל בהתחשבות בהמלצות ה"ל".

זכרו: שימוש בתו "רווח" יכול לעזור בהגנת הסיסמה.

קחו משפט שלם וארוך שיהיה לכם קל לזכור והפכו אותו לראשי תיבות. למשל My dog's name is Mooshi. הסיסמה תהיה: MdniM. לאחר הוספת ספרה ותו מיוחד, הסיסמה תהיה: MdniM1!

במידה ואורך הסיסמה מאפשר זאת, שיקלו להשתמש ב Passphrases כסיסמתכם - הנה סיסמה המורכבת ממשפט או מחיבור של כמה מילים:

עוד אפשרות הנה סיסמה המבוססת על תרגיל חשבון פשוט עם שילוב מילים במקום ספרות. לדוגמה, הסיסמה 3 Hundred - 3 =297

שקלו להשתמש במחזורת קבועה - כמו ביטוי, מילים משי, ציטוט מסרט ולהוסיף לה סימנים ותווים מיוחדים, למשל Wish1You@WereHere!

כיצד בונים סיסמא חזקה?

מקור: באדיבות משרד הבריאות

הפתרון: הזדהות חזקה (MFA)



הזדהות ב-2 רמות (2 Factor Authentication)

הזדהות ב-3 רמות (3 Factor Authentication)

רמה I – משהו שאתה יודע – **Something you know**

רמה II – משהו שיש לך – **Something you have**

רמה III – משהו בך – **Something you are**

הזדהות ברמה שניה - משהו שיש לך (פיסית)



➤ מכשיר סלולרי - קבלת SMS



➤ טוקן ייעודי



➤ כרטיס חכם

הזדהות ברמה שלישית - משהו בכך (ביולוגית)



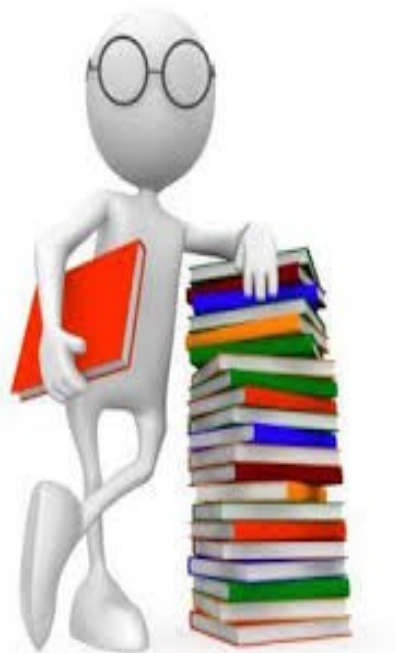
טביעת אצבע ✓

זיהוי רשתית ✓

תווי פנים ✓

זיהוי קולי ✓

מאפייני התנהגות ✓



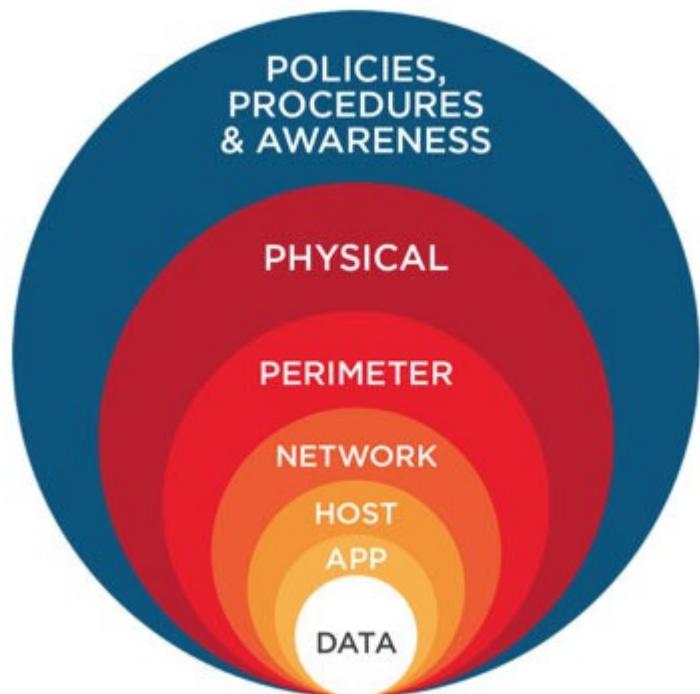
נושאי הלימוד

- מודל "הגנה בשכבות" (Defense in Depth)
- התקפות ZERO DAY ודרכי התגוננות
- התקפת DOS , DDOS
- הגנה על האפליקציה – WAF
- הגנה על בסיס הנתונים – DAF
- הגנה על הכנסת רכיבים זרים לרשת – NAC
- הגנה על זליגת מידע – DLP

עקרונות DEFENSE-IN-DEPTH



העיקרון אומר: הגנה על כל רכיב כאילו הוא לבד.



- ✓ הגנה על בסיס הנתונים
- ✓ הגנה על האפליקציות
- ✓ הגנה על המחשבים
- ✓ הגנה על הרשת
- ✓ הגנה פיסית על חדרי השרתים
- ✓ בקורות גישה בתוך הארגון
- ✓ הגנה היקפית של הארגון (גדרות, מצלמות, שומרים)
- ✓ מודעות עובדים
- ✓ נהלים ופרוצדורות עבודה

התקפה על האפליקציה

Vulnerability – חולשה

Exploit – ניצול חולשה

אנלוגיה לעולם המיחשוב:

חולשה: באג בתוכנת דפדפן אקספלורר של מיקרוסופט המאפשר פריצה אל המחשב שלנו

ניצול החולשה: תוכנות שהאקרים כתבו ופרסמו באינטרנט על מנת ל"התנקם" בחברת מיקרוסופט

מי מנצל: כל מי שמוריד את התכנה



התקפת DOS , DDOS



התקפת Denial of Service – DOS

התקפת Distributed Denial of Service – DDOS

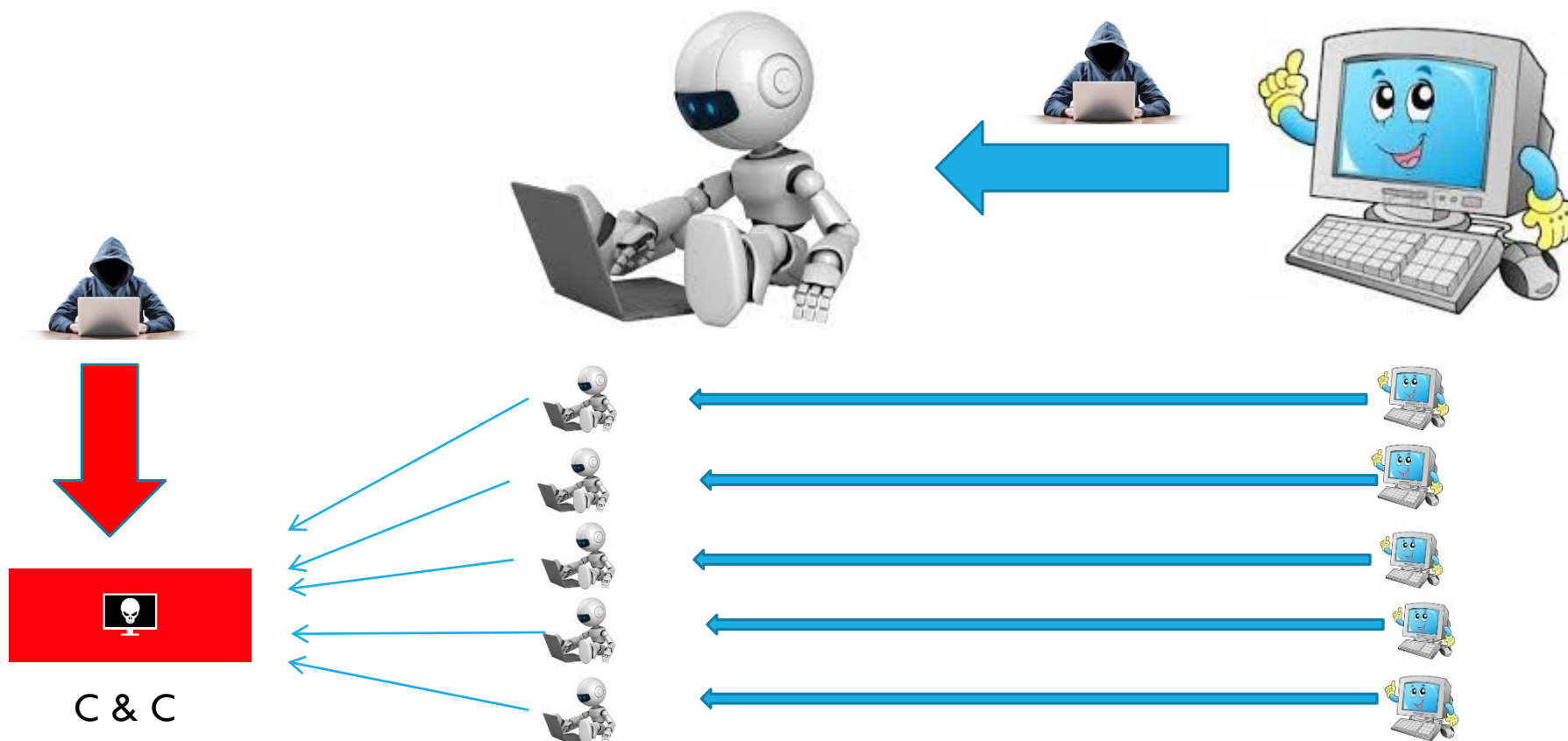
הרכיבים המעורבים:

- אתר אינטרנט כלשהו שנפרץ (למשל hotels.com)
- מחשב הקורבן שהופך לבוט
- מחשב התוקף
- תחנת ניהול הבוטים שמקים התוקף

בוט – מחשב שנמצא תחת שליטה חסויה של האקר

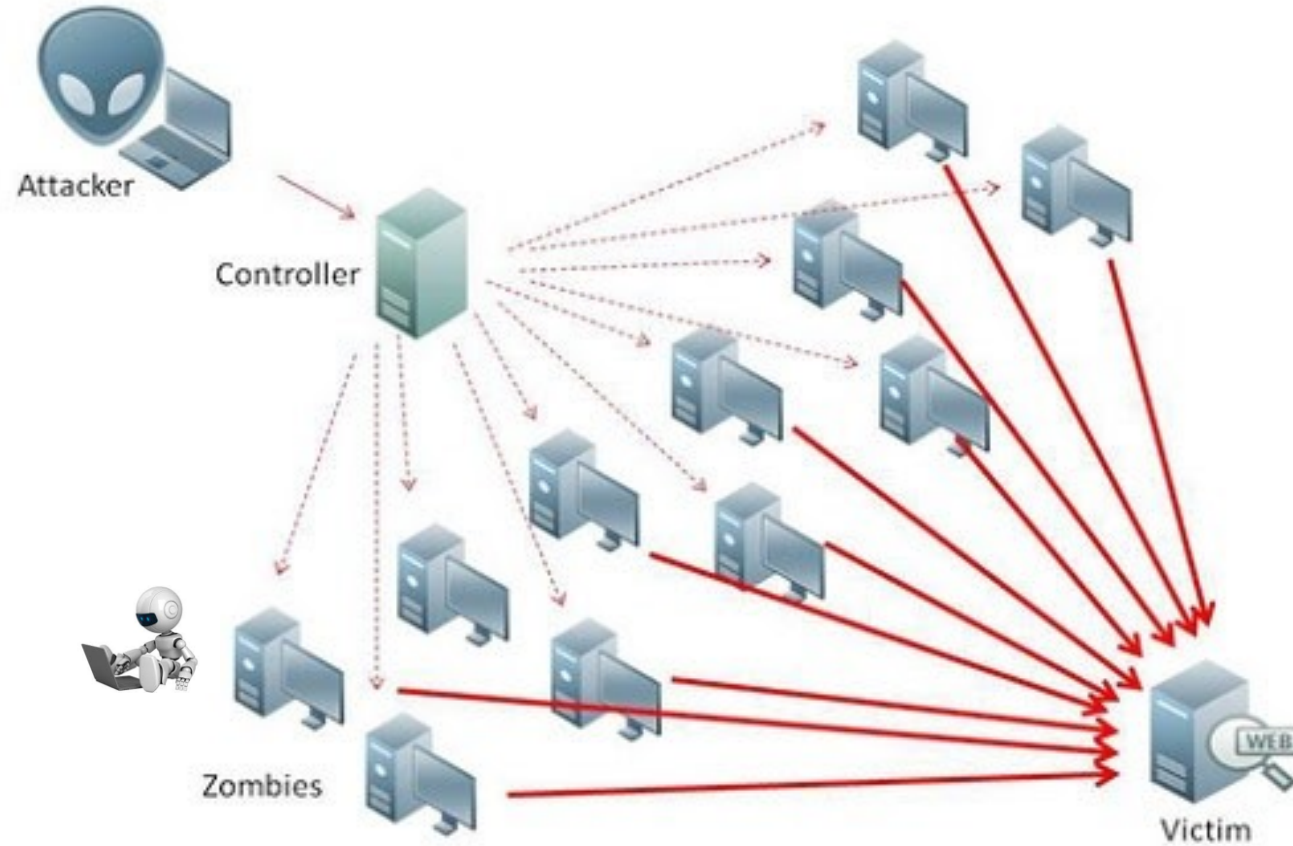
שלבי ההתקפה בהתקפת DOS

התוקף הופך מחשב ל-BOT





ביצוע ההתקפה



אפשר גם לקנות התקפות מוכנות באינטרנט

<http://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html>

How much costs a DDoS attack service? Which factors influence the final price?

March 26, 2017 By [Pierluigi Paganini](#)

How much costs a DDoS attack service? Kaspersky Lab published an analysis on the cost of a DDoS attack and services available in the black markets.

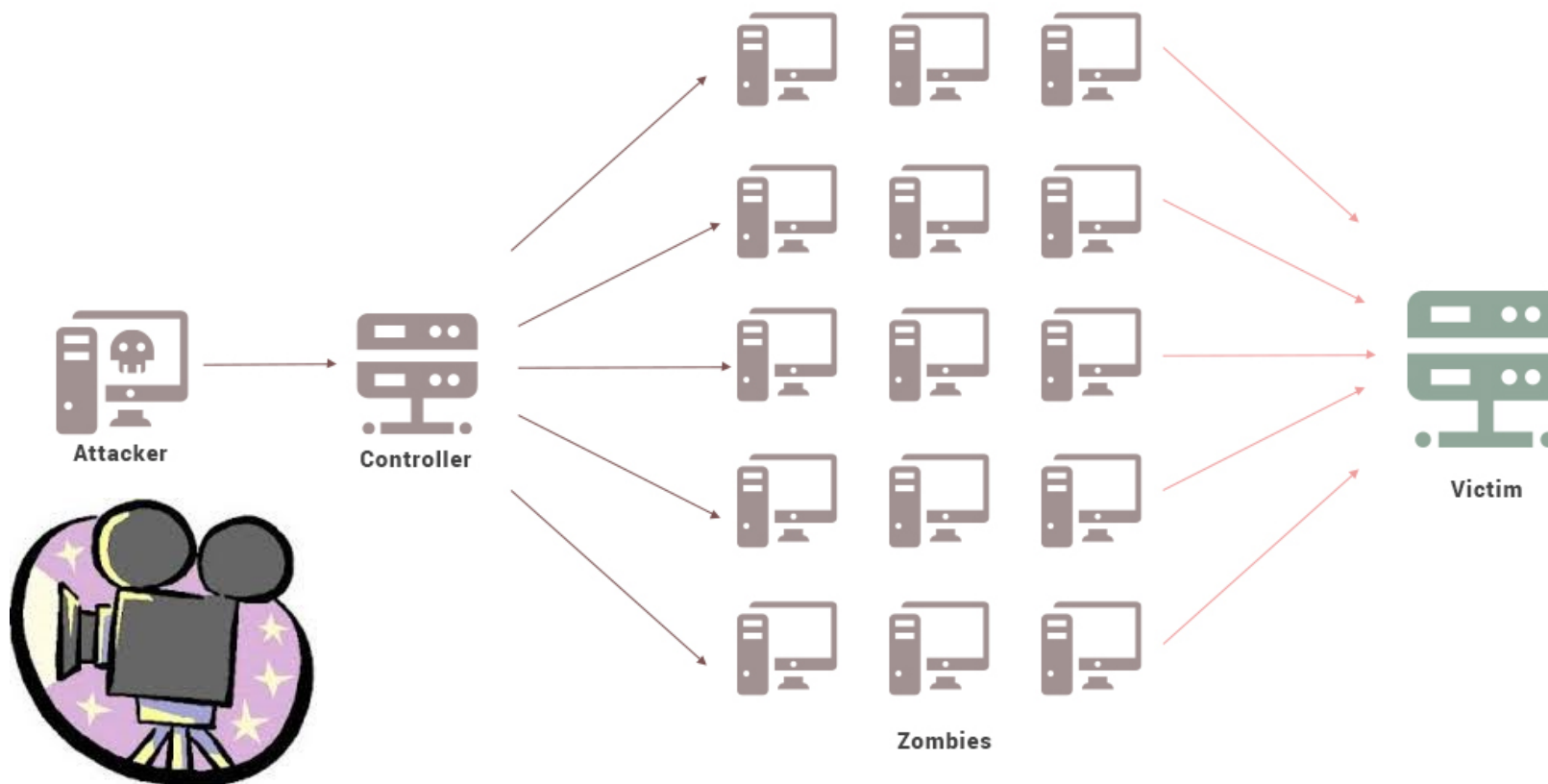
Kaspersky Lab has published an interesting analysis on the cost of DDoS attacks. The experts estimated that the cost to power a DDoS attack using a **cloud-based botnet of 1,000 desktops is about \$7 per hour**. A DDoS attack service typically goes for \$25 an hour, this means that the expected profit for crooks is around $\$25 - \$7 = \$18$ per hour.

Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

התקפת DDOS - סרטון

התקפת DDOS - סרטון



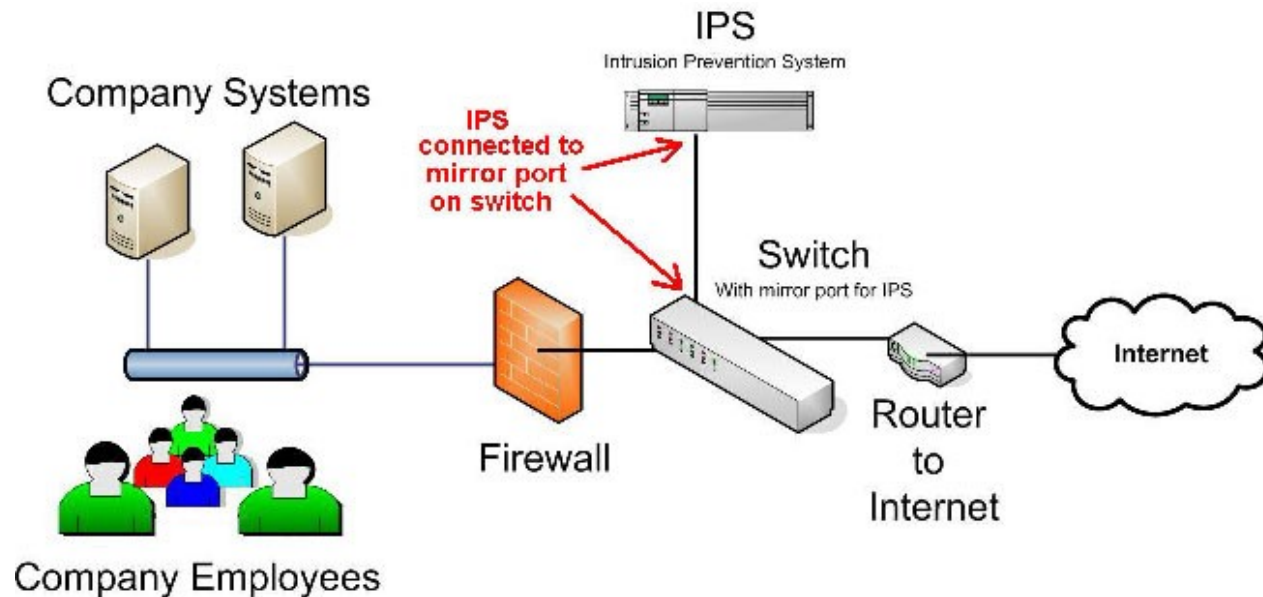
IDS , IPS - הגנה כנגד התקפות

IDS = INTRUDER DETECTION SERVICE

IPS = INTRUDER PROTECTION SERVICE

IDS - במקרה של התקפה על הארגון - מתריע בלבד

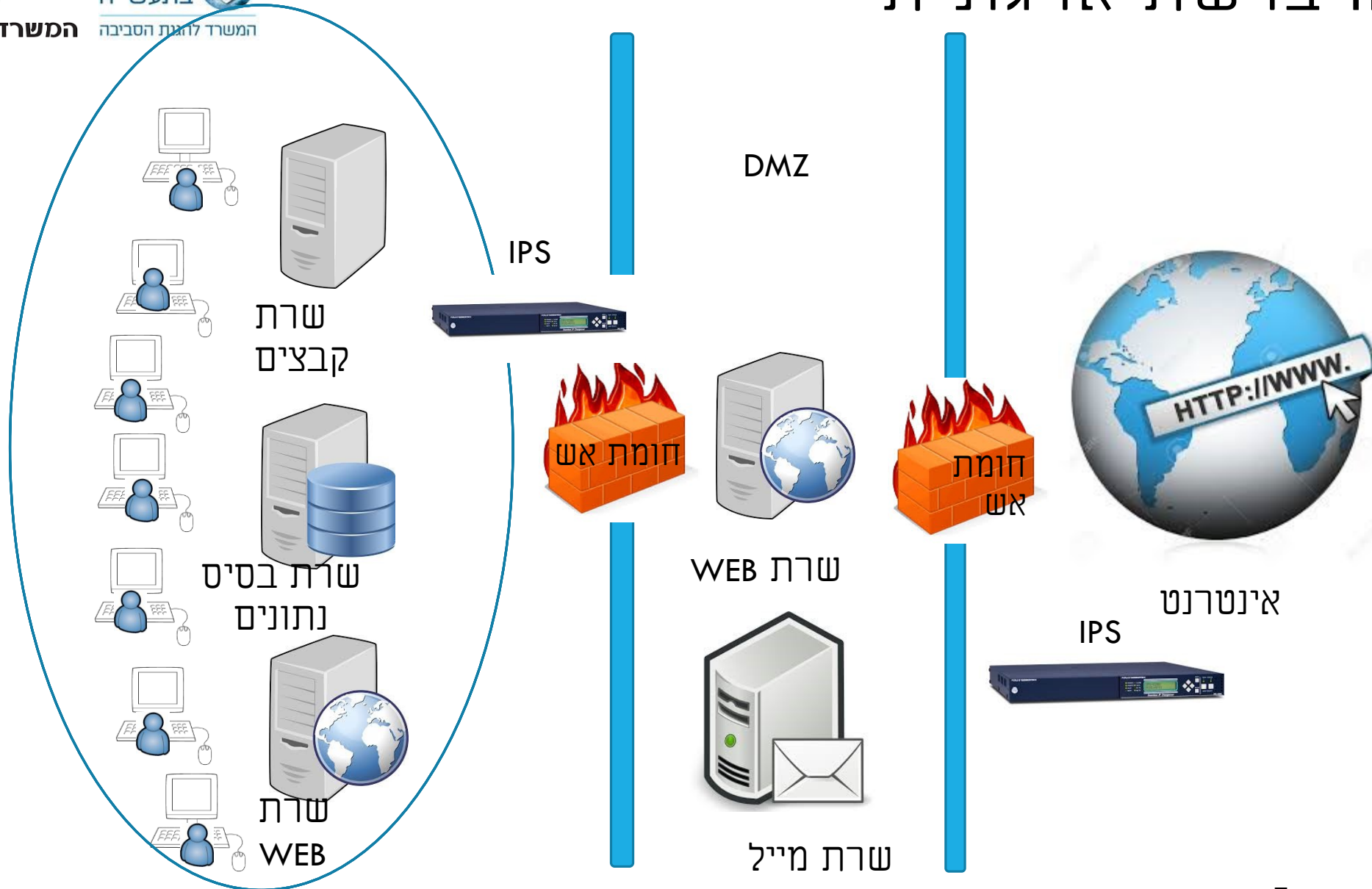
IPS - מתפקד כ-IDS ובמידת הצורך, אם קינפגנו אותו כך - יכול לחסום התקפות בצורה אקטיבית



הצורך:

- חסימת התקפות מחוץ לארגון
- חסימת התקפות מתוך הארגון

מיקום IPS ברשת ארגונית



בעיות בחסימת התקפות

ב-IPS יש לקחת בחשבון **חסימת תעבורה לגיטימית***

מצב חסימה	סוג התעבורה	מצב
מאפשר	לגיטימית	1
1 בעיה חוסם	לגיטימית	2
2 בעיה מאפשר	לא לגיטימית (התקפה)	3
חוסם	לא לגיטימית (התקפה)	4

מי יותר גרוע לארגון ??

בעיה 1 או בעיה 2?

בעיות בחסימת התקפות במערכת IPS



בעולם ה-זו – השבתת גישה למערכת מידע



בעולם ה-זס – פס ייצור **מושבת!!**

איך להתגבר על החסרון? הפעלת IDS ולאחר קבלת התראה שיקול דעת אנושי מה לחסום בפועל