# הרצאה 1 - מבוא והגנה פיזית

## 1. מבוא

מטרת הקורס היא להכיר מהם סוגי האיומים על מערכות המחשב, הכרת הגישות להגנה על משאבי המחשב, הצגת התפתחויות בתחום אבטחת המידע והמחשבים והכרת דרך חשיבה באבטחת מידע (Security mindest).

תחילה נכיר מה היא מערכת מתוכנתת:

כל רכיב אלקטרוני המכיל מעבד או שערים לוגיים מהווה מערכת מתוכנתת. לדוגמא: מחשב ביתי (PC), רשת המחשבים של הטכניון, מכשיר כספומט, טלפון נייד, ממיר של חברת הכבלים, כרטיס חכם של רכבת, טלפון ועוד..

לעומת זאת לא נראה בקורס כיצד לתקוף מערכות מחשבים. כן נראה דוגמאות להתקפות שהיו, על מנת ללמוד ממה יש להיזהר וכיצד ניתן למנוע התקפות מסוגים שונים.

## 2. שלבי בניית מערכת הגנה

לפי בניה של כל מערכת הגנה, תחילה יש לזהות את האיומים הפוטנציאלים על אותה המערכת למשל במערכת בנקאית המאחסנת מידע רגיש על לקוחות הבנק, קיים איום תמידי של פריצה למאגרי המידע שלה וגניבת פרטי הלקוחות, ועל כן כל מערכת בנקאית כזו חייבת להיות מודעת לאיום זה.

לאחר זיהוי האיומים הפוטנציאלים יש לנתח את הסיכונים הנובעים מאיומים אלו, למשל באיום שזיהינו במערכת הבנקאית יש להבין כי הסיכון העיקרי בעת חשפית מידע רגיש או נגישות לא מבוקרת למידע זה הוא פגיעה הן בפרטיות לקוחות הבנק והן בשמו ובכספיו של הבנק עצמו.

כמובן שבמצב אידיאלי מערכת ההגנה תמנע את התרחשותם של כל האיומיים אשר זיהינו בשלב הקודם, אולם מניעת כל האיומים דורשת משאבים אשר לעיתים עולים על ערכו של מחיר הפגיעה כתוצאה ממימוש איום זה , ועל כן עלינו לבחור על מה ברצוננו להגן וכיצד. בסופו של דבר שם המשחק הוא כסף. אם מה שאנו מעוניינים להגן עליו שווה מליון דולר, אף אדם שפוי לא ישקיע שני מליון דולר בהגנה עליו.
ועל כן בשלב זה נצטרך לגבש את מדיניות ההגנה הטובה ביותר שנוכל להרשות לעצמנו לאור המסקנות שהסקנו מהשלבים הקודמים.

ולבסוף נצטרך לממש את מדיניות ההגנה שגיבשנו בעזרת מנגנוני הגנה (כגון: מצלמות אבטחה, כספות, פרוטוקולי אבטחה וכו').

# 3. איומים על מערכות

ניתן לסווג את האיומים על מערכת לאיומים על נתונים ולאיומים על משאבים.

<u>באימונים על נתונים</u>, האיומים הקיימים מחולקים ל-3 קטגוריות עיקריות:

- סודיות (secrecy) ופרטיות (privacy) – קריאה/ פרסום נתונים סודיים לדוגמא הפריצה למאגר המידע של משרד הפנים ופרסום כל הנתונים האישיים ברשת האינטרנט(פרסום התוכנה "רשומון").
- שלמות(integrity) – שינוי תוכן הנתונים ע"י אנשים לא מורשים לדוגמא פריצה למאגר הציונים בטכניון ושינוי הציונים.
- זמינות (availability) –פגיעה בנגישות לנתונים לדוגמא מתקפת DDoS על אתר (התקפה זו תלמד בהמשך הקורס).

התקפות ומימוש של איומים אילו על נתונים יכולים להתרחש בזמן שהם נשלחים ברשת, או כאשר הם שמורים במערכת. חשוב לזכור כי לפעמים בעל המערכת הוא המאיים על הנתונים (פרטים בהמשך).

<u>ובאיומים על משאבים</u> לעומת זאת קיימת פגיעה בזמינות ,או שימוש לא חוקי במשאבים (שגורם לפגיעה בזמינות עבור המשתמשים החוקיים) לדוגמא פגיעה ברכיבי החומרה, קווי התקשורת,גניבת שיחות וכו'...

# 4. תקיפה

## 4.1. מדוע להתקיף?

קיימות סיבות רבות לביצוע התקפה, החל מפגיעה במוניטין של המותקף (לדוגמא על ידי פרסום פרטים אישיים של המותקף ברשת האינטרנט או חשיפה של מידע רגיש לגביו כמו הפריצה )

כמו כן תוקפים לעיתים מבצעים את התקיפות לצורך פגיעה במותקף כגון גניבת כסף, מחיקת מאגרי מידע , ריגול עסקי או לוחמה ממוחשבת (למשל בין מדינות).

August 11th, 2008
**Coordinated Russia vs Georgia cyber attack in progress**
Posted by Dancho Danchev @ 4:23 pm
http://blogs.zdnet.com/security/?p=1670&tag=nl.e539

**ניסיון לגניבת פרטים של לקוחות בנק אוצר החייל**
נוכלים מתחזים ל"בנק הפועלים" ובנק אוצר החייל, ומנסים לגנוב פרטים של לקוחות להתחברות לחשבון באמצעות הונאה, על ידי הקמת אתר מזוייף לבנק
אהוד קינן
פורסם: 24.08.08, 11:19
http://www.ynet.co.il/articles/0,7340,L-3586719,00.html

## 4.2. כיצד מתקיפים?

דרכי התקיפה מתחלקות לשתי קטגוריות עיקריות:

- התקפה פסיבית – למשל ציטוט לנתונים המועברים ממחשב זה לרשת.
- התקפה אקטיבית – למשל שינוי תכני ההודעות הנשלחות מהמחשב אל הרשת והפוך

וכמו כן פריצה אל המחשב המותקף.

לפני ביצוע התקפה בדרך כלל מגיע שלב של תכנון אך לא תמיד (למשל במקרים בהם מתבצעת התקפה לא מתוכננת כמו באגים או כאשר משתמש שוכח את הסיסמא שלו...)

במהלך שלב התכנון מתמקד התוקף בצורה בה הוא ינצל את המידע הקיים ברשותו וינסה לפגוע בנקודות חלשות במערכת כגון:

- ניצול feature אצל המותקף – כגון ניצול Buffer Overflow בישום finger במערכת unix אשר יפורט בתרגול.
- Worm - אפקט כדור השלג :התפשטות במהירות גבוהה.
- Social Engineering - זהו מושג מתחום האבטחה שמשמעותו שילוב של טכניקות הונאה, התחזות ושכנוע הגורמות לאנשים לציית לבקשת הפורץ .למשל, לספק לו מידע רגיש כגון שמות משתמשים וסיסמאות או לבצע עבורו פעולות כגון הרצת תוכנה לבקשתו. ההאקר הידוע ,קווין מיטניק ,משתמש רבות במונח וטוען שהנדסה חברתית היא הטכניקה האפקטיבית ביותר ב-"ארגז הכלים" שלו.

כיום, מנהלי אבטחת מידע רבים מעריכים כי איום זה לחיסיון המידע הארגוני, גדול משמעותית מכל איום טכנולוגי "קלאסי."

הנדסה חברתית הינה שיטה להונות את משתמשי הרשת תוך כדי התחזות לאדם המוכר, או לאתר המוכר למותקף ועקיפת כל מנגנוני האבטחה המקובלים כגון-FireWall-IDS AntiVirus ועוד ציוד אבטחה רב. גישה אחת להתמודד ולהגן בפני תופעות אלו הינה העלאת המודעות בקרב הציבור מפני סוגי התקפה של הנדסה חברתית, גישה אחרת היא לתכנן מערכות בצורה שיהיו תלויות פחות בגורם האנושי, כך שיהיו פחות חשופות להתקפות מהסוג הזה. (בעצם כל סוג של "עוקץ" שמנצל נקודת תורפה אנושית ניתן לכנות כ-Social Engineering).

דוגמא להתקפה מסוג זה היא התקפת דיוג **Phishing:**

הוא ניסיון לגניבת מידע רגיש על ידי התחזות ברשת האינטרנט .המידע עשוי להיות, בין היתר, שמות משתמש וסיסמאות או פרטים פיננסיים. פישינג מתבצע באמצעות התחזות לגורם לגיטימי המעוניין לקבל את המידע, כמו כן קיימים קיטים מוכנים שינתן להוריד מהאינטרנט שבאמצעותם ניתן לבצע דיוג באופן אוטמטי על מספר רק של משתמשים, הקיטים העדכניים ביותר מאפשרים אף יצירת עמוד Web אוטומטית על פי תבנית של אתרים ידועים כגון Gmail, !Yahoo ועוד. לרוב שולח הגורם המתחזה הודעת מסרים מידיים או דואר אלקטרוני בשם אתר אינטרנט מוכר, בה מתבקש המשתמש ללחוץ על קישור .לאחר לחיצה על הקישור מגיע המשתמש לאתר מזויף בו הוא מתבקש להכניס את הפרטים אותם מבקש המתחזה לגנוב.

אתרים נפוצים שפעולות פישינג מתבצעות בשמם הם אתרי רשתות חברתיות כגון יו טיוב,ופייסבוק , אתרי מכירות פומביות כגון איבי ואתרי בנקים כגון בנק אוף אמריקה.

שיטות Phishing :

## דואר זבל אלקטרוני

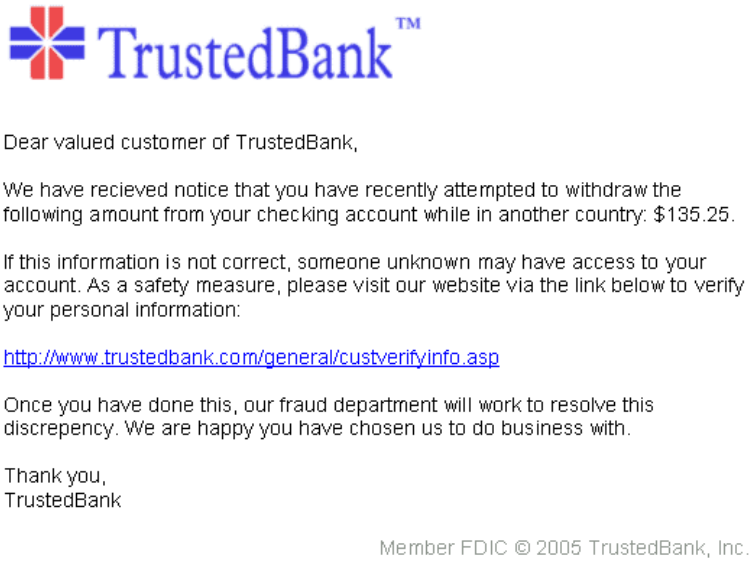
פעולות דיוג נעשות בדרך כלל בדואר זבל אלקטרוני ,כלומר באמצעות פנייה למספר גדול מאוד של נמענים, כך שמבחינתו של השולח, די באחוז קטן מאוד של נופלים בפח כדי להוות הצלחה מבחינתו. הפנייה בהודעות אלה בדרך כלל אינה אישית (למשל: "לקוח יקר"), אך לעתים מתבסס השולח על רשימת שמות שנפלה לידיו, כגון רשימת כל העובדים או הלקוחות בארגון מסוים ,ופונה באופן אישי לכל נמען, צעד המגביר את אמינותה של הודעת הדיוג.

## שינוי קישורים

בשיטה זו משתמשים המתחזים בקישור המטעה את המשתמש לחשוב שהקישור עליו הוא מקיש והאתר אליו הוא מגיע שייכים לחברה לגיטימית. למשל, הלינק HTTP://WWW.bank.credit.com עשוי להטעות משתמש לחשוב שהוא נכנס לעמוד האשראי באתר bank.com כאשר למעשה הוא נכנס לעמוד הנקרא bank תחת האתר credit.com . אם העמוד מעוצב כמו דף הכניסה של הבנק ,המשתמש עשוי להכניס את פרטיו וכך לאפשר למתחזה לבצע פעולות בשמו.

שיטה נוספת היא יצירת קישור בעל טקסט המטעה את המשתמש. למשל הקישור בנק עשוי להטעות את המשתמש לחשוב שהוא לוחץ על קישור שיוביל אותו לעמוד בנק כאשר למעשה הקישור יוביל אותו לעמוד הונאה.

דוגמא:


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

### זיוף אתרים

לחיצה על קישור עשויה להוביל משתמש לדף מזויף הנראה כמו דף של אתר לגיטימי. כאשר המשתמש מכניס את פרטיו הדף מפנה אותו באופן אוטומטי לאתר האמיתי ומכניס עבורו את הפרטים כך שהמשתמש אינו יודע שמסר את פרטיו לאתר מזויף. שיטות מסוג זה נקראות "אדם באמצע".(Man in the Middle) "

שיטות מתוחכמות יותר כוללות את שינוי הכתובת בשורת הכתובת של הדפדפן והצגת תמונה של הכתובת הנכונה או סגירת שורת הכתובת האמיתית והצגת שורת כתובת מזויפת בדפדפן. שיטות XSS מאפשרות לאתר להפעיל תוכנה במחשב הקורבן כך שניתן למעשה לבצע כל פעולה מתוך המחשב בהרשאות המשתמש. שיטה זו קשה מאוד לזיהוי על ידי מי שאינו מומחה. בשנת 2006 נתגלתה פרצה מסוג זה באתרPayPal . למעשה הקורבנות אשר נגשו אל כתובת אשר אכן הייתה מאוכסנת על השרת של PayPal הכתובת אכן הייתה מוגנת על ידי SSL וזוהתה ואושרה ככתובת של PayPal אולם כאשר הקורבנות ביקרו בכתובת זו הוצגה לפניהם הודעה אשר "הוכנסה" לאתר של PayPal אשר אמרה:

> "Your account is currently disabled because we think it has been accessed by a third party. You will now be redirected to Resolution Center."

ואכן כעבור זמן קצר הם הוכוונו אל אתר מזוייף של אשר ביקש מהם את שם המשתמש שלהם ואת הסיסמא. הנקודה החשובה פה היא שכאשר הקורבן נכנס בהתחלה לאתר אשר זוהה ואומת כאתר של PayPal הוא לא חשב שלאחר מכן הוא יכוון לאתר עויין אשר ינסה לגנוב את הסיסמא שלו.(ראה פירוט בקישור למטה)

## 4.3. את מי/ מה מתקיפים?

יעדי התקיפה האפשריים הם:

- יעד תקיפה נקודתי (שרת מסויים או מאגר נתונים מסויים).
- מערכת מחשוב שלמה (רשת הטכניון).
- כל מערכות המחשוב המחוברות לרשת

<u>דוגמאות לתקיפות:</u>

- העברת חלקי אגורות לחשבונו של עובד הבנק
- גניבת סרטי גיבוי ומחיקת דיסקים ע"י עובד החברה
- הצפת מרכז המחשבים
- וירוסים ב-mail attachments, לדוגמא I Love you ( ILOVEYOU היה תולעת מחשבים שפגע במחשבים רבים בשנת 2000, כאשר היה זה כקובץ מצורף להודעת דוא"ל עם הטקסט "ILOVEYOU" בשורת הנושא. התולעת הגיעה לתיבות דואר אלקטרוני ב- 4 במאי 2000, עם נושא פשוט של "ILOVEYOU" ואת קובץ מצורף-"LOVE-LETTER-FOR-YOU.TXT.vbs". עם פתיחת הקובץ המצורף, התולעת שלחה עותק של עצמה לכל מי שנמצא ברשימת הכתובות של המשתמש, מתחזה למשתמש. זה גם עשה מספר שינויים זדוניים במערכת של המשתמש.)

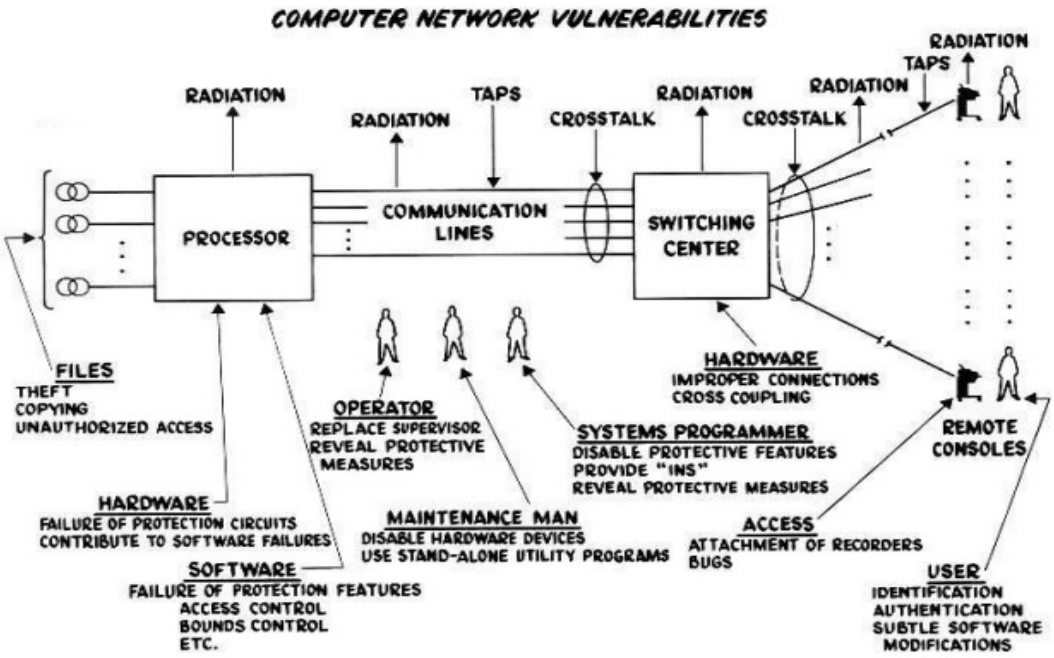
- תשלומים בעזרת כרטיסי אשראי בטלפון( ב( Internet -
- סוס טרויאניWindows NT registration - בשנת 1999 נשלח מייל לאנשים המציע להם לשדרג את האקספלורר. מי שהוריד את התוסף הודבק בסוס הטוריאני . הקובץ היה בשם ie0199.exe
- שינוי דף הבית של הC.I.A - ב19 בספטמבר 1996 שינו האקרים את דף הבית של הCIA כך שיהיה כתוב :.Welcome to the Central Stupidity Agency
- Internet Worm, MSBlaster, SQL Slammer,NACHI, Nimda, MyDoom
- פרסום הדיסק של יזהר אשדות בסוף שנות ה90 -
- התקפת ה DDoS -על Yahoo, Amazon ,CNN ועוד.

**(DDoS)** היא משפחת תקיפות שנועדה להשבית מערכת מחשב על ידי יצירת עומס חריג על משאביה. מתקפה כזו יכולה למנוע מקבוצת משתמשים גישה למשאב מחשב מסוים על ידי העמסת אותו המשאב כך שלמשתמשים הלגיטימיים לא יישארו משאבים .

במרבית המקרים מדובר בניסיון של אדם או קבוצת אנשים למנוע מאתרי אינטרנט או שירותי אינטרנט אחרים מלפעול בצורה תקינה או מלפעול בכלל. מטרות נפוצות הם בדרך כלל אתרים או שירותים בעלי פרופיל גבוה כגון אתרי בנקים, אתרים פוליטיים, ממשלתיים ואף שרתי השורש של.DNS

שיטה אחת להתקפת מניעת שירות היא סינכרון מספר רב של מחשבים (לעתים באמצעות סוס טרויאני) השולחים לשרת היעד בו-זמנית בקשה לשירות כלשהו וכך בעצם מונעים מבקשות לגיטימיות אחרות לקבל את אותו השירות אם בשל עומס משאבי-מחשב על השרת עצמו ואם בשל חוסר נגישות רשתית לאותו השרת.

# איומים על מערכות מחשב




## 4.4. התוקפים

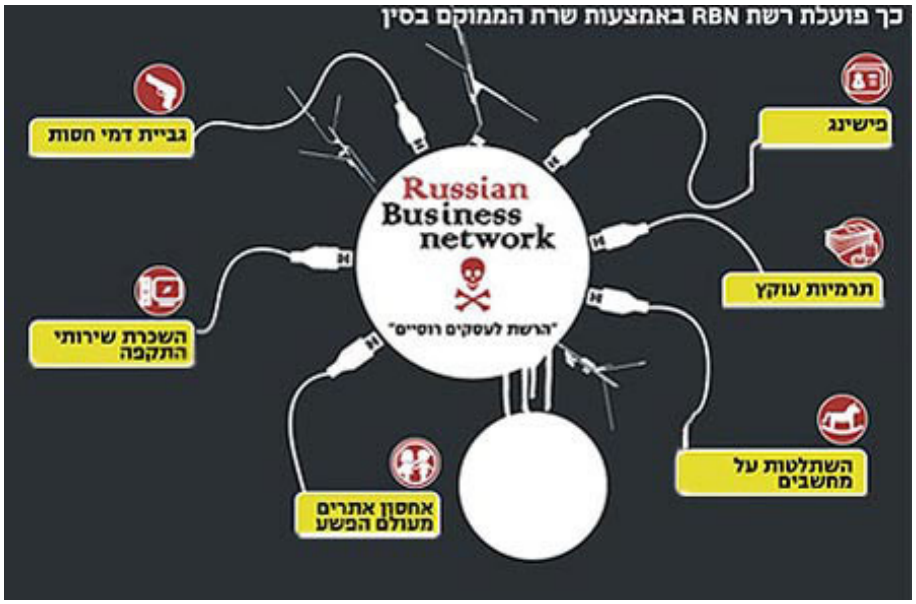
יש מספר סוגים של תוקפים, כמובן בגלל שישנם אנשים אשר האינטרס שלהם הוא לתקוף קמו אנשים אשר האינטרס שלהם הוא להגן,כל אחד מהם פועל להשגת מטרות שונות. מבין האנשים אשר מגנים מפני התקפות ישנם צוותי מחקר במוסדות אקדמאיים אשר המטרה שלהם היא אנליזה של מערכות (למשל http://www.isaac.cs.berkeley.edu ).

כמו כן קיימים גורמים מחוץ לקהילת המחקר המכונים White hats אשר מועסקים ע"י חברות למטרות בדיקת מערכות או פועלים עצמאית לזיהוי חולשות במערכות ומדווחים עליהם לחברות. בנוסף קיימים גורמים הנקראים Gray hats אשר פועלים עצמאית ,לעיתים מדווחים ,ולעיתים לא על פרצות אבטחה שמצאו.

בניגוד ל White hats אשר תורמים להגנה על מערכת (ואפילו בניגוד לGray hats אשר לא תמיד מזיקים) קיימים ה- Black hats שהם בפרוש זדוניים ,ולא חוקיים ובעלי מוטיבציה – כלכלית או פוליטית.
אסכולה נוספת היא ה-חובבים, אשר לרוב משתמשים בקוד וכלים שנכתבו ע"י אחרים, וגם משאירים עקבות. דוגמא למשתמשים חובבים כאלה היא ה-Script Kiddies. (Script Kiddies- הוא מונח המשמש לתיאור גנאי למי שהשתמש בסקריפטים או בתוכניות שפותחו על ידי אחרים כדי לתקוף מערכות מחשב ורשתות. ההנחה היא כי בדרך כלל אלו הם בני נוער שאין להם את היכולת לכתוב תוכניות פריצה מתוחכמת בעצמם, כי המטרה שלהם היא לנסות להרשים את החברים שלהם או לקבל קרדיט בקהילת המחשבים. )

כמו בכל דבר אחר המניע העיקרי את התוקפים למינהם הוא התמריץ הכלכלי, תעשייה זו מגלגלת סכומי עתק בכל שנה (ניתן למצוא בקישורים את עבודתם של דן גיר ודניאל קונווי, אשר החל מינואר 2008 מפרסמים מדד שנתי למחירי הכלכלה המחתרתית, כגון מחירי שירותי דואר זבל הדבקות של בוטנטים וכו')

את כוחו של התמריץ הכלכלי ניתן לראות בהתפתחות רשת ה-RBN( Russian Business Network), שהיא גם דוגמא להתפתחות ה-hacking בשנים האחרונות לתעשייה לא חוקית אך משגשגת. RBN הוא אחד הארגונים הגדולים בעולם לפשיעה מכוונת, בין השאר הכנסות RBN מגיעות מאירוח אתרים: הוא גובה 600 דולר לחודש תמורת מתן דיסקרטיות מלאה לבעלי האתר ומניעת הורדתו מהרשת (הנתונים מתוך כתבה על RBN בעיתון "כלכליסט", ראה קישור למטרה). האתרים ב RBN עוסקים בפדופיליה, פישינג (התחזות לאתרי בנקים וחברות אשראי כדי להונות גולשים ולגנוב את סיסמאותיהם), וכן אתרים תמימים למראה שמדביקים את הגולשים שמבקרים בהם ברוגלות, וירוסים וסוסים טרויאנים. לפי הדו"ח של וריסיין, ב־2007 פעלו בשרתי RBNיותר מ־2,000 אתרים שעסקו בפעילות פלילית ברשת.




http://www.calcalist.co.il/internet/articles/0,7340,L-3082407,00.html

# 5. הגנה

## 5.1. מדיניות הגנה

מדיניות ההגנה קובעת על מה רוצים להגן וכנגד אילו איומים. כמו כן במי ניתן לבטוח ואיך מגיבים נגד התקפות.

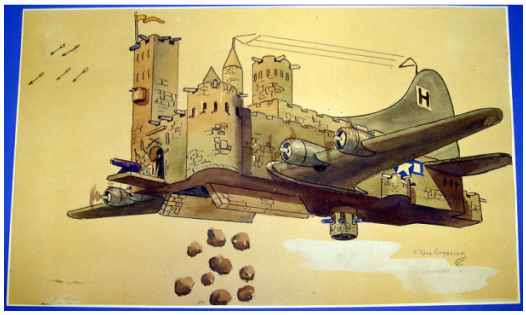
לגבי כל אחד מהאיומים הפוטנציאלים יש לשקול:

- האם ההתקפה היא מעשית – לדוגמא במידה ואין גישה לאף אדם אל כבלי התקשרות לא קיימת סבירות לציטוט אל כבלי התקשורת ע"י התחברות ישירה אליהם.

- הנזק העלול להיגרם כתוצאה מההתקפה- במידה והנזק מתקיפה הינו מזערי אז לא נשקיע מאמצים גבוהים מדי בניסיון למנוע את ההתקפה הזו.

- עלות ההגנה נגד האיום- במידה ועולה לתחזק את ההגנה נגד האיום יותר מאשר השווי של המידע המוגן אין סיבה להשתמש בהגנה מסוג זה.

- פגיעות בנוחות המשתמש כתוצאה מהגנה זו- לעיתים הגנה על מערכת מסרבלת מאוד את השימוש בה , דבר שלעיתים יוצר אי רצון להשתמש במערכת זו ובכך מנענו את ההתקפה אבל מנענו את הרצון שלנו להשתמש במערכת.



## 5.2. דוגמאות למדיניות הגנה

- אין הגנה- במידה וגישה למערכת מבחוץ לא יכולה לגרום נזק אין הגנה על המערכת בכלל.

- הגנה ע"י הסתרה- הסתרת המימוש לצורך אבטחת המערכת. מערכת המשתמשת בשיטה זו עשויה להכיל חולשות אבטחה אך מסתמכת על כך שהחולשות אינן ידועות לתוקפים, כך שהם יתקשו בחשיפתן.אבטחה באמצעות הסתרה היא שיטה שנויה במחלוקת. חברות מסחריות משתמשות בשיטה זו בכך שאינן מפרסמות בדרך כלל את קוד המקור שלהן ואינן מתעדות בצורה מקיפה את השגרות בהן הן משתמשות. בצורה זו מקשות החברות על תוקפים פוטנציאליים למצוא את פרצות האבטחה בתוכניות שלהן. מתנגדי השימוש בשיטה זו טוענים כי ניתן לאתר את הפרצות בכל מערכת ללא התחשבות במידת העמימות שלה.

- הגנה ברמת המחשוב –הגנה זו מספקת רמת אבטחה גבוהה אשר הנחת היסוד שלה כי יתכן נסיון פריצה של המערכת מבפנים וכי אין נסיונות פריצה מהרשת.

- הגנה ברמת הרשת- הגנה של המערכת מפני גישה של תוקפים באמצעות הרשת, גישה זו מניחה כי אין נסיונות חדירה מתוך המערכת

- שילוב בן הגנה הן ברמת המחשוב והן ברמת הרשת.

קיימות כיום חברות ברשת שדורשות סטנדרטים מסויימים לגבי מדיניות ההגנה אשר תיוסם על המוצרים אותם הם רוכשים וכמו כן על המוצרים אותם הם מיצרים. דוגמא טובה לכך הם המפעלים הביטחוניים אשר עוסקים ביצור נשק. פגיעה במערכת נשק הינה דבר חמור מאוד ובמידה וקיימת פרצת ביטחון במערכת מסוג זה אשר תאפשר לגורם עוין לפגוע במערכת או אפילו להשתלט על המערכת איננה דבר שיש לקחת אותו בקלות ראש. על כן כיום קיימים תקנים במוסדות בטחוניים ובצבא אשר כוללים חוקים מפורטים עד לפרט

האחרון את הצורה שבה יש ליצר את המוצר ואת הבדיקות שעליו לעבור לפני שהוא יהיה מאושר לשיווק. אחד התקנים המפורסמים הינו תקן ISO27001 אשר מפרט בין היתר גם את הצורה שבה חייבת להירשם התוכנה אשר עומדת בלב המוצר.

## 5.3. כתיבת מדיניות הגנה טובה

בעת כתיבת מדיניות הגנה ישנם קשיים רבים. כפי שציינו מקודם, לרוב בגלל גורם כלכלי, לא קיימת אפשרות להגן מפני כל האיומים ועל כן קיימים אילוצים על מתכנן מדיניות ההגנה שבגללם עליו להשאיר פרצות בתקווה שהנזק אשר יגרם מכך לא יהיה רב. כמו כן לא תמיד מזהים בשלב הגדרת מערכת ההגנה את כל הפרצות אשר קיימות במערכת. כאשר באים לכתוב מדיניות הגנה מומלץ:

- לבדוק את עלויות מימוש המדיניות.
- לבדוק כי הפונקציונאליות של המערכת נשמרת.
- לבדוק דרישות חוקיות (חסיון של מידע רפואי או יחסי עו"ד ולקוח)
- לצרף הסברים לאנשים בכדי שיבינו כיצד יש להשתמש במערכת. (לדוגמא שאין לגלות את הסיסמא ).
- להסביר מה התפקיד של כל אדם במערכת החל מהעובדים ועד המנכ"ל.
- מעקב בכדי לוודא שלא עוברים על המדיניות (כמו בטחון מידע בצה"ל)
- תהליך של עדכון וטיפול בפרצות שמתגלים במדיניות או במערכת.
- למי מגיעים חשבונות ועל אילו מחשבים.
- רמת האבטחה הנדרשת מתחנה לפני שהיא יכולה לקבל שירות – לדוגמא מתחנה שבתוך מקום העבודה נדרשת רמת אבטחה נמוכה יותר מאשר גישה חיצונית לכל עמדת אינטרנט.
- כיצד מוגן מידע עיסקי רגיש.
- כיצד מוגן מידע אישי רגיש (גם מבחינת מה שמחייב החוק).
- אילו קבצים מותר להכניס מבחוץ.
- מה היא התגובה על חדירת ווירוס למערכת.

## 5.4. מנגנוני הגנה

לאחר בחירה של מדיניות ההגנה יש לבחור במנגנוני ההגנה אשר ימלאו אותה. מנגנוני הגנה יכולים להיות שונים ומגוונים. בקורס בין היתר נלמד על: הגנה פיזית, סיסמאות, פרוטקולי אבטחה, חומות אש ועוד..

### 5.4.1. הגנה פיזית

מערכות מחשב נתונות לאיומים פיזיקלים מוחשיים. חלקם מכוונים ליצור נזק וחלקם ללא כוונה מגוף אחר. לדוגמא: הפסקות חשמל (מכוונות ולא מכוונות), איתני טבע כגון רעידות אדמה הרי געש מתפרצים וכו', שדות חשמליים ומגנטים חזקים, גניבה פיזית של מחשב או חומרה רגישה, חיתוך כבלי תקשורת ועוד....

ההגנה מפני מתקפות אילו בעיקר גם היא פיזית ונעשית על ידי הצוות מחסומים פיזיים כגון מנעולים ודלתות אבטחה, חומות ויצירת מתקני גיבוי כמו גנרטורים וכבלי תקשורת חלופיים.

לעיתים קיימת פגיעה "מבפנים" הנעשית על ידי עובדים ואורחים. לצורך הגנה מפני פגיעות מסוג זה בדרך כלל ישנו סיווג של מידע בתוך האירגון ומניעה של גישה למידע רגיש על ידי גורמים הלא מוסמכים לכך. אמצעי הגנה אפשריים הם: שומר בדלת, קודן בדלת, מנגנון סריקת רשתית או טביעת אצבע וכו'...

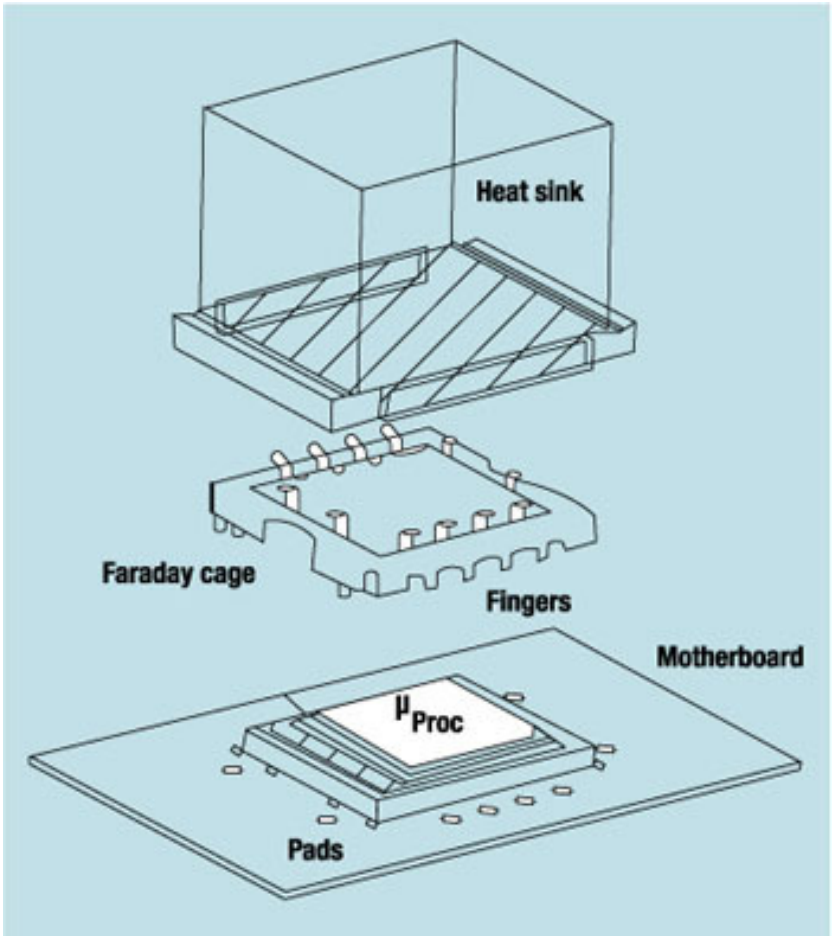
#### 5.4.1.1. זליגת מידע פיזית

לעיתים מידע יכול לזלוג בצורה לא מכוונת. אחת הדוגמאות למצב מסוג זה הוא קרינה אלקטרומגנטית.

מערכות המחשב פולטת קרינה מסוג זה(בין אם המעבד, הדיסקים הקשיחים ואפילו המסך...) כמו כן גם קווי התקשרת יוצרים שדות מגנטים מסביבם.

מערכות המחשב פולטות מידע בדרכים נוספות: זמן החישוב מעיד על איזו פעולה מבוצעת, רעש מהמעבד יכול להעיד על איזו פעולה מבוצעת במעבד, צריכת האנרגיה מוסרת מידע על איזו פעולה מתבצעת בחומרה, חום מהמעבד יכול להעיד על אילו פעולות מבוצעות בו.

בכדי להגן מפני ציטוט על ידי גורם זר לקרינה המגנטית דבר שיכול לאפשר לו לפענח את המידע המועבר מגנים על המידע במספר דרכים למשל ע"י סיכוך קווי התקשורת והפרדתם מרשת הטלפון, הגנה באמצעות כלוב פרדיי המונע זליגה של קרינה אלקטרומגנטית כפי שמתואר למטה בציור ויצירת "רעש לבן" במכוון אשר מסתיר את הקרינה.




http://www.ce-mag.com/archive/01/Spring/Raza.html

## 5.5. EMP- Electro Magnetic Pulse

תקיפה באמצעות EMP היא בעצם פיצוץ מעל האטמוספרה הגורם ליצירת קרינה אלקטרומגנטית. אותה הקרינה הורסת את כל המערכות האלקטרוניות ברדיוס עליו היא משפיעה וזאת כמובן מבלי לפגוע בבני אדם או בבעלי חיים.

כיום גודלה של פצצת EMP הינו קטן מאוד וניתן אף לשלוח אותה במזוודה דבר ששימושי מאוד לארגוני טרור.

הגנה מפני פצצות אילו יכול להיעשות על ידי כלוב פרדיי כמו בהגנה מזליגת מידע (כלום לא יוצא ולא נכנס לכלוב). כמו כן ניתן להשתמש במערכות ישנות לצורך גיבוי במקרה של התקפה מהסוג הזה.( למשל שפורפרות רדיו פחות רגישות לתקיפה כזו מאשר דרכי התקשורת הנפוצים היום ובכללם סלולר).

(ניתן לראות מה עלולות להיות התוצאה של תקיפה מסוג זה על ארה״ב בקישור המצורף במקורות)

# 6. מקורות


1. "DIY phishing kits introducing new features", Ryan Naraine, Dancho Danchev Available at: http://blogs.zdnet.com/security/?p=1104
2. "Phish" definition from "Answers.com", http://www.answers.com/topic/phishing
3. "PayPal Security flaw allows identity theft", NetCraft Available at: http://www.geekblue.net/archives/2006/06/netcraft_paypal.html
4. Electromagnetic pulse attack- Future weapons serial http://www.youtube.com/watch?v=MnYGHA5asj4 .
5. מדד שנתי למחירי הכלכלה המחתרתית, דן גיר ודניאל קונווי "IEEE Security & Privacy", http://geer.tinho.net/ieee/ieee.sp.geer.0901.pdf .
6. Russian Business Network study http://www.bizeul.org/files/RBN_study.pdf .