**שיעור #2**

**לסייבר אין משמעות מוגדרת.**

0 DAY- מתקפה בחומרה שעוד לא מצאו לה פרצה. ברגע שהנפגע הותקף, יש לו 0 ימים לתקן את זה לפני שזה משתלט. היום קשה מאוד לגלות פירצות כאלה, עולה המון כסף (=העסקת מומחים, יש ממש שוק )

RAT - REAMOT ADMINISTRATION TOOL

Security Cracker-מנסים לפרוץ חומות אבטחה, יכולים להיות טובים או רעים(טובים-בשביל לעשות בדיקות ורעים כדי לפגוע נזק במחשבים ולהשתמש במידע גנוב)

Hacker=Security Cracker

**3 רמות תקיפה:**

1. - script kidiss ילדים שלא מבינים באמת משהו,לא ממוקצעים ומשתמשים בכלים קיימים פשוטים, לא מעריכים את חומרת הנזק שעלול לגרום הדבר ולא יודעים להסתיר אחריהם עקבות ולכן יכולים להתפס בקלות.

2. מתכנתים שקצת יודעים מה הם עושים, מתכנתים מנוסים, בונים את הכלים שלהם בעצמם, מבוסס על פגיעות ופריצות שהם גילו(יום ה0) או כאלה שפורסמו. יעשו זאת לכייף\תרגול\אתגר טכנולוגי\כסף\נקמה\האקרטיביסם

WHITE-מומחי אבטחה, מנסים לפרוץ תחת בקשה מסויימת, למצוא ולדווח על פריצות ופגיעות תוך מאמץ לגרום כמה שפחות נזק

BLACK- מטרות זדוניות, רווח למטרה עצמית, לא ידווח על הפריצות ועלול לשתף עם עוד האקרים את כוונותיו.

Gray- בין שחור ולבן, יכול להיות שידווח, יכול להיות שידווח לנפגע קודם כל, יכול לבקש כסף על פרטי פריצה

3.פשע מאורגן,מדינות

כופרה או חוטפה,הצפנה של הקבצים תמורת תשלום,PHISHING

**3 קטגוריות של הגנת סייבר: ברמת הארגון**

**הגנות:**

**תמיד תמיד לעדכן תוכנות גדולות על המחשב,לא לסמוך על קבצי הורדה באינטרנט,על כל לינק לראות שהכתובת היא כתובת השרת האמיתי ואפשר לבדוק את זה ע"י העתק הלינק\HOVER**

***PASIVE(***Preventive***)***

1. fire wall- תוכנה שיושבת בראוטר והיא יושבת ומסתכלת על כל חבילה שמגיעה למחשב(מהאינטרנט לאינטרנט הביתי),האם מותר לה להכנס או אסור לה להכנס. רוב הראוטרים כוללים בתוכם כבר פייר וול.

האם עכשיו כבחברה אני בטוחה?לא

2. אנטי וירוס

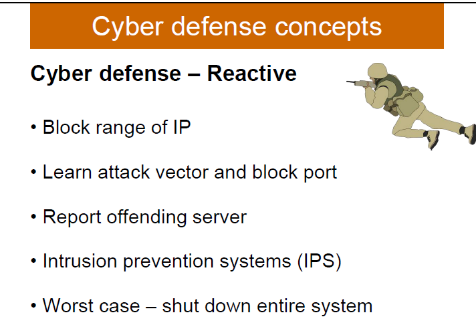
האם עכשיו כחברה אני בטוחה?לא

3. IDS- שמים בעיקר בארגונים. אם פייר וול רואה מי שלח ולמי זה מיועד, האיידיאס רואה מה יש גם בתוך החבילה.נניתוח מעמיק יותר ולא מסתכל רק על החבילה הנוכחית אלא זוכר גם את החבילות הקודמות ומנסה לחבר ביניהן ולראות האם יש בקומבינציה ביניהן מתקפה.

לא מספיק

4.לא נשים פייר וול אחד אלא שניים לפחות של יצרנים שונים לשם לוודא שאין אף פרצה שיכלה לפרוץ בפייר וול אחד והאחר עמיד לה.

5.עדכונים...

לא מספיק...

אלו הם מקטגוריית הגנה פסיבית ,והיא,לא מספיקה.

***REACTIVE***

תמיד צריך שיהיה תוכנית פעולה. מה אני עושה,איך, מי מנהל את האירוע.

אגירת לוגים של הארגון בארכיון ושליחתם לשרת נפרד.

***PROACTIVE***Preemptive)

במקום לחכות שיחדרו אלי ואפעיל תוכנית פעולה,אני כבר אהיה מוכן לכך שלא יתקפו אותי

למשל:ארגון יפתח שרת פיקטיבי ובאופן מקרי לחלוטין ידליף את פרטי השרת,התוקפים ינסו לתקוף את השרת הגלוי לפני שיגיעו לאמיתי וכך הארגון ימצא את אופן הפעולה שהאקרים מנסים לתקוף אותם כל פעם.

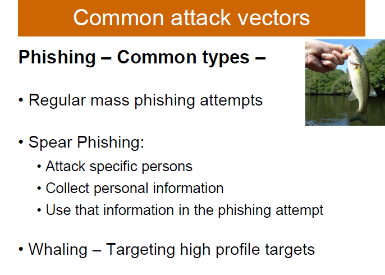
**איך תוקפים גורמים לנו להתקין את הקוד?**

INSIDERS : התקפות פנים ארגוניות

זדוני – מישהו בארגון שרוצה לגרום נזק לארגון MAYA

אדיש- אחד שלא אכפת לו (גוגל מזהיר אותך ואתה נכנס בכל זאת)

נאיבים – כאלה שאין להם מושג PISHING

\*הקשחה: ברגע שמחברים למשל דיסקאוןקי המערכת הלפעלה לא ישר מופעלת

גם אם יש הקשחה אפשר להכנס דרך מקלדת או פורט.

PISHING :

כמו דייג רגיל. זורקת מלא אימיילים ומקווה שמישהו יתפוס ויפול בפח.

DRIVEBY : ערכת ניצול שיורדת אופן אוטומטי

התקפה שמבוססת על דפדפנים ואם נכנסים לאתר\מייל, קוד יתחיל לרוץ ולהכנס למערכת ההפעלה של המחשב שלי . איך להמנע? תוכנת מחשב מעודכנת,אנטי וירוס טוב מעודכן,להמנע מאתרים חשודים,לא ללחוץ על כל דבר.

\*אקספלוייט קיטEXPLOIT KIT - מנצלים פרצות בדפדנים . הרוב באקספלורר ופלאש ולכן כרום לא מריץ היום פלאש.

דפדפן מאובטח,עדכונים ועוד משהו זה הדרך להתמודד הכי טוב.

התקפות וייפי-ויפי שמוגן בססמא,ניתוק ויפי,חדירה ולראות תעבורה-אתרים ותמונות שהוא רואה,אפשר להסניף ססמאות לאתרים,שליטה על התעבורה ולשנות תוכן של אתרים שגולשים בהם.

Ransomware- תוכנת כופר- היא נוזקה המגבילה גישה למערכות המחשב הנגוע בדרך מסוימת, ומשמשת לסחוט מהמשתמש תשלום כסף על מנת שתוסר מגבלת הגישה.(קבצים,תמונות או ממש חסימת גיש למחשב עצמו)

**שיעור #4**

Vishing-Voice

phishing -emails

sm ishing –sms

***פסיכולוגיה אנושית-דחפים נפוצים:***

תוקפים נוטים לביים מניפולציות רגשיות על האנשים-גורמים למותקף לחשוב שהוא ירגיש מוערך,יוקירו לו תודה,יהיה שייך.

***הפחדים הנפוצים:***

להפסיד כסף,שיגנבו לנו מידע רגיש ואישי,פחד מטכנולוגיה,מהבוס,מלהפר את החוק

***טקטיקות נפוצות:***

דחיפות,עובדות מזוייפות,הגברת. סקרנות,התחזות למישהו שאנחנו מכירים,רגשות

***איך עושים כסף מהתקפות סייבר?***

להשיג פרטי חשבון ולגנוב כסף.

להשיג מידע רגיש.

להשתמש בפרטי משתמש בשביל להשתמש בנטפילקס וכו.

***סוגי התקפות- פירוט:***

1. ***Vishing***

דוגמאות:

התראת טלפון להתראת חסימת האשראי

התראה על מיסים ע"י המס הכנסה

הודעה קולית ממייקרוסופט

1. ***Phishing***

* גורמים ללאתר מזוייף להראות אמיתי-כתובת האתר תהיה דומה מאוד לאמיתית ומתעתעת
* הודעה מזוייפת מהבנק

סוגי אימייל פישינג:

* REGULAR-שולח את הלינק לכמה שיותר אנשים, אוספים מידע על בן אדם וגורמים לו ע"י מידע לרצות ללחוץ על הלינק
* SPEAR- אוסף מידע על בן אדם ספציפי
* WHALING- מנסה לתפוס דג שמן של חברה,מתחזה למנכל של חברה

1. ***Smishing***

מי ששולח לי אסמס לעולם לא ישלח לינק עם BIT\..

**Lesson5-**

**מה האקרים עושים בשביל להגן על עצמם?**

1. האקרים קונים מעין מכונה וירטואלית למחשב שזו מעין קופסה סגורה. מ2007 הקופסא כבר לא סגורה... ולכן הקבצים על המחשב של האקר חשופים בפני אלו שיתפסו את המחשב ממנו נעשתה הפרצה.

2. עוד דבר הוא לא להשתמש בוייפי שלך(למשל בבית) ולכן האקרים בדרך כלל ישבו בבתי קפה,רכבת וכו- או יותר מתוחכם:חונה בשכונת מגורים רחוקה ממך ופורץ לוויפי של מישהו ועושה הכל משם.

3. שימוש בPROXY- להקשות על מי שמנסה לגלות את ההתקפה. לא רצוי פרוקסי חינמי כי זה לרוב כאלה שמשמשים שוטרים לתפוס עוקץ,או כאלה שלא באמת טובים.

4. לא להשתמש בכתובת MAC שלך. אפשר להחליף פיזית במכשיר. אפשר בווינדאוס לשנות את זה בהגדרות. בלינוקס יש פקודה כזו

5.בוחרים את אלו שהולכים לתקוף טוב טוב ונזהרים ממלכודות.

**התקפות WIFI**

חדירה לWIFI שהוא לא שלי.

יתרונות: אינטרנט חינם,להדביק את המחשב המותקף במלאוור,גניבת ססמאות

מה זה WPA-לדעת(אין צורך לדעת איך פורצים)

הגנה של הוויפי.

WPS – תוסף לנוחות עבודה, טכנולוגיה שקיימת בחלק מהראוטרים ואי אפשר לנתק את זה.

אוסף של טכניקות איך אפשר להתחבר בקלות,למי שלא זוכר ססמאות ארוכות.

הכי פחות מאובטח להכי מאובטח:

OPEN

WEB

WPA+WPS

WPA2!!!