



סיכום מפגש שולחן-עגול

Zero Day Attacks

מאי 2013

מנחה

סיגל רוסין

לקוחות נכבדים שלום,

תודה על השתתפותכם במפגש שולחן עגול Round Table בנושא Zero Day Attacks.

מצ"ב סיכום עקרי הדברים שעלו במהלך המפגש. במפגש עלו נושאים מהותיים שתומצתו בסיכום כפי שעלו. אין בסיכום זה המלצה גורפת ללקוחות אלא מתן פרספקטיבה והצגה של ההתלבטויות שעלו במפגש כלומר "מהשטח".

מהות המילה סייבר והבשלות להתקפות ממוקדות zero day בארגונים מתקשה לבוא לידי ביטוי. לקוחות מתייחסים בצורה שונה לנושא הסייבר. מצד אחד, חלק מהלקוחות עושים שימוש בכלי אבטחת מידע קיימים, בדיקה של הקונפיגורציה של הכלים. מצד שני, יש לקוחות אשר מנסים לבדוק כלים חדשים הקשורים לתחום הסייבר. נושא המובייל גם מביא איתו התרחבות לעולם אבטחת המידע ועמדות הקצה ויש לקחת זאת בחשבון. כמו כן, מרבית הארגונים פועלים לשם הגברת המודעות בקרב עובדיהם בדרכים שונות וחשיבות מדיניות אבטחת המידע בארגון.

במלחמת הסייבר יש לזכור שלא מדובר אר ורק בשינוי מוצרי אבטחת מידע אלא גם בהסתכלות פנים ארגונית כללית על הגנת משאבי הארגון.

בברכה,

סיגל רוסינ

תוכן עניינים

3	רקע
6	התייחסות לסייבר בארגונים
8	מודעות משתמשי הארגון
9	מדיניות אבטחת מידע
10	כלי הגנה /zero day /סייבר
13	המלצות STKI בנושא סייבר
13	נספח מיוחד התייחסות ספקים ויצרנים לנאמר במפגש
13	התייחסות חברת WE
14	התייחסות חברת Prodware
14	התייחסות חברת Mobisec
17	התייחסות חברת מטריקס
19	התייחסות חברת טלדור תקשורת גלאסהאוס
20	התייחסות חברת HP

רקע

מלחמת הסייבר מורכבת ממספר סוגי התקפות:

- 1) **Cyber terror** - מלחמת סייבר המנוהלת באמצעות ארגון טרור או כנופיה, כנגד מדינה או אוכלוסייה של מדינה כלשהי.
 - 2) **Cyber warfare** - סידרת תקיפות של מערכות מחשבים (או מערכות אחרות המנוהלות באמצעות מחשבים), אשר מבוצעות מצד מדינה אחת (או קבוצות בה), או ארגון טרור, כנגד מטרות במדינה שניה (מערכות ממשלתיות, או ביטחוניות, תשתיות לאומיות או פרטיות).
 - 3) **Cyber crime** - התקפה או סדרת התקפות של גורם כלשהו, על מערכות מחשבים כלשהן, אשר המניע שמאחוריהן, גניבה/הונאה, או כל היבט כלכלי או טובת הנאה כספית אחרת.
 - 4) **Cyber security** - מתייחס להיבט הטכני של הגנת מערכות מידע, ללא קשר להיבט הרעיוני (פוליטי / פלילי / אחר).
- לעומת, המושג **hacking** (תקיפת מערכת מידע) מתייחס להיבט הטכני של תקיפת מערכות מידע, ללא קשר להיבט הרעיוני (פוליטי / פלילי / אחר).

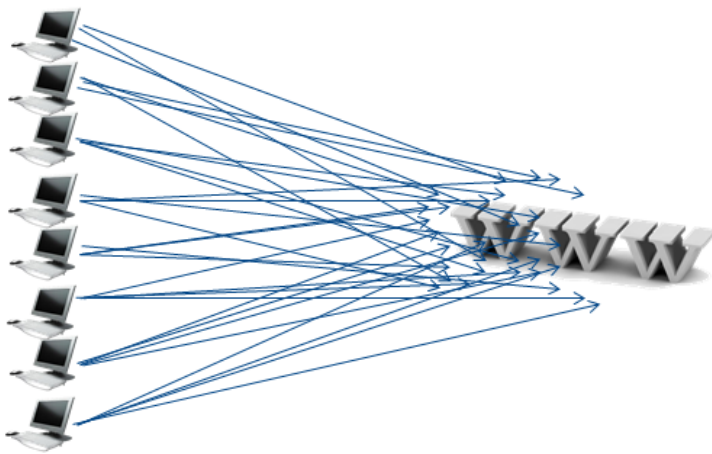
מתוך: see security בית ספר לאבטחת מידע וללוחמת מידע



מספר סוגי התקפות ידועות איתם ארגונים מתמודדים כיום:

- i. **DDOS** - Distributed Denial of Service Attack - התקפת מניעות שירות מפוצלת. התקפת DDOS היא הניסיון לגרום לשרת VPS, אתר אינטרנט או שירותים אחרים להפוך ללא זמינים ע"י ניצול מירבי של אחד מהמשאבים של השירות (מעבד, זיכרון, רוחב פס וכו').

Distributed Denial Of Service (DDOS)

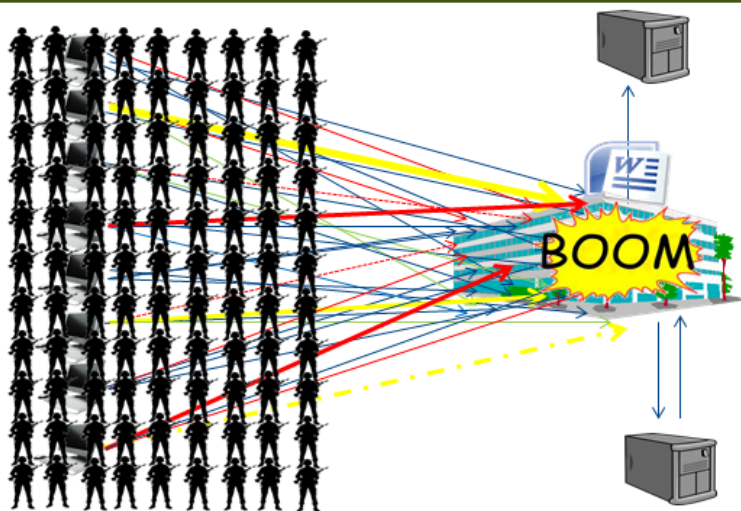


1. Targets websites, internet lines etc.
2. Legitimate traffic
3. Many different sources
4. From **all** over the world
5. Perfect timing



.ii **APT - Advanced Persistent Threat** - מצב בו "שמים את הארגון על הכוונת", ותוקפים אותו ספציפית בצורה שיטתית ומתחכמת, לאורך זמן. מדובר בתקיפות שמאחוריהן עומדים גופים עוצמתיים ובעלי משאבים גדולים במיוחד, שיכולים להרחיב את מאמציהם ולעשות זאת לאורך זמן, כמו למשל מדינות או ארגוני טרור.

Advanced and Persistent Threat (APT)



1. Group/ Org./ State
2. Ideological/ Nationalistic background
3. Multi-layered attack
4. Targeted
5. Variety of tools
6. **Impossible to detect in real time(???)**



.iii **Zero day attack** - מבוסס על פרצות אבטחה שקיימות במערכת אך אינן מוכרות לארגונים (לא ליצרן המערכת ולא לצרכנים שלה) עד 'יום האפס', כלומר עד היום שהם מגיעות לתודעה ציבורית. אחרי שפריצה כזו נודעת, כמובן שהארגון וחברות האנטי-וירוס פועלים מיד

לחסום אותה. אבל עד יום האפס, בעל המידע על הפריצה, מחזיק למעשה בנשק יקר מפז ואין שום מנגנון הגנה שמכיר אותו.

הסכנה בכך הינה באם הצלחת להמציא Zero-Day, אתה יכול למכור אותו בזירות מכירה מיוחדות במרחב הdark net. זה הופך אותו לנגיש יותר, כולל התמקדות בסביבה מסוימת, למשל ארגונים פיננסיים, בריאות, ביטחון וכד'.

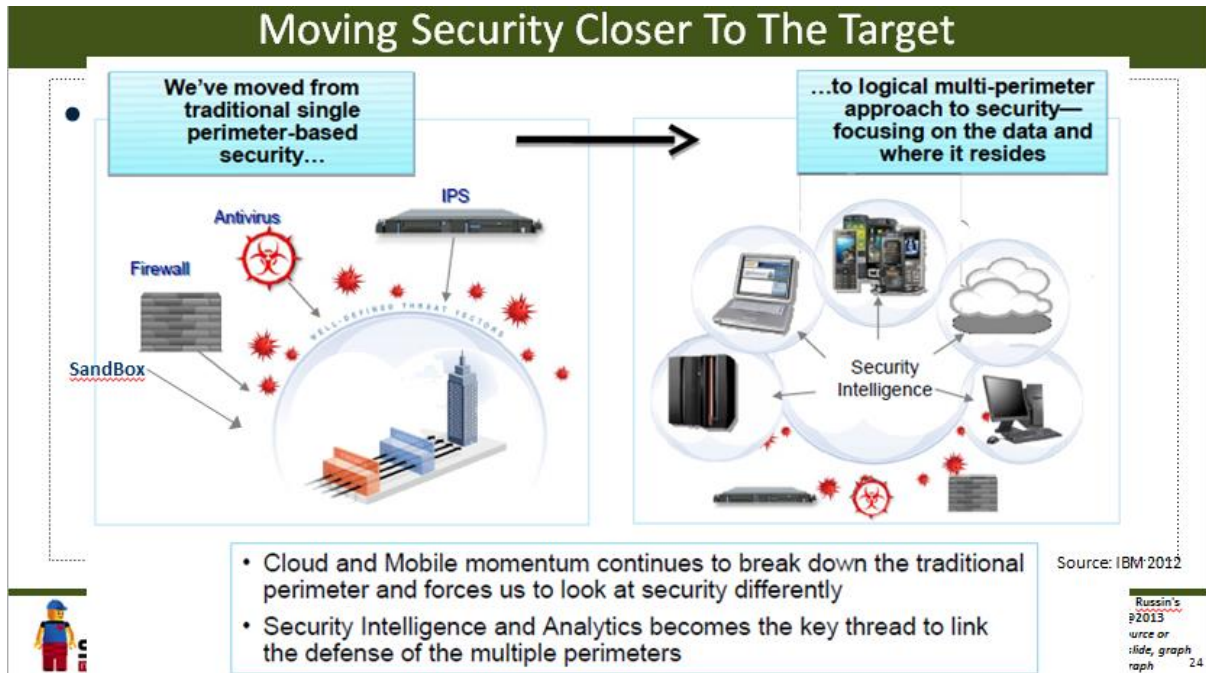
Zero day attack

- A zero-day (or zero-hour or day zero) attack or threat is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability.
- This means that the developers have had zero days to address and patch the vulnerability. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability. (Wikipedia)
- The meaning- no signature !
- Hackers can easily modify "known threats" and eliminate the signature



iv. **Rootkit** - ערכה (kit) המכילה אפליקציות קטנות ושימושיות שמאפשרת לתוקף להשיג גישה "Root" למחשב הנתקף – הגישה הכי גבוהה שיכולה להינתן למשתמש. כלומר, Rootkit הוא אוסף של אפליקציות ופונקציות אשר מאפשרים נוכחות קבועה ובלתי ניתנת לזיהוי של התוקף על המחשב של הנתקף, לרוב אלו נמצאים ברמת הקרנל (ה-Rootkit הוא דרייבר). קורה לפעמים לפני שמערכת ההפעלה עולה.

לסיכום, במלחמת הסייבר יש להמשיך ולהגן על השכבה החיצונית המסורתית העוטפת את משאבי הארגון כגון ANTI VIRUS,FW,IPS וכדומה. אך יש לשים לב לשכבה הפנימית בארגון ולנסות לזהות התנהגויות חשודות של המשתמשים או המערכות בארגון.



התייחסות לסייבר בארגונים

נראה שישנה שונות לא קטנה בהתייחסות לסייבר בקרב הארגונים השונים.

לקוח נוסף מספר כי לדעתו סייבר זה יכול להיות מעין buzzword אבל אבולוציה של אבטחת המידע השתנתה וכך גם כוונות ההאקרים. הארגון נקט אמצעי הגנה חיצוניים להגנה מפני DDOS. כעת אותו ארגון נמצא בסיום פרויקט המהווה גישה מאובטחת של משתמשים לאינטרנט. אותו ארגון מספר שיש יותר מדי עמדות קצה "כבדות" נוספות המשמשות אך ורק לגישה לאינטרנט. לכן הארגון הקים רשת נפרדת מעין סוג של DMZ שמתחברים אליה לגישה לאינטרנט כמו טרמינל בשימוש של סיטריקס או ג'טרו. למשתמש לוקח כמה שניות עד שדפדפן האינטרנט עולה אך לכאורה הכל שקוף למשתמש ויש לו גישה חיצונית לאינטרנט שאיננה קשורה כלל לעמדת הקצה שלו. אם רץ ברשת סוס טרויאני או סקריפט חשוד הוא ירוץ רק על הטרמינל ולא ידביק את כל עמדות הקצה של המשתמשים. הבעיה היא למרות החסימה באינטרנט של אתרים חשודים, כל עובד יכול לגלוש כבר דרך מכשיר המובייל שלו ברשת אלחוטית ששם לא חסום כלום. לדוגמה, אם נחסום פייסבוק במסגרת העבודה בארגון העובד יוכל לגלוש במובייל דרך 3G.

ארגון אחר מספר כי הם הגדירו את עמדות הקצה כשייכות לארגון עצמו לשם עבודה, כלומר רכוש עבודה, ולכן זכותו של הארגון לבדוק מה רץ בכל מחשב ולחסום בהתאם. לדוגמה רשתות חברתיות. במובייל אין חסימה וזו בעיה. הלקוח לא מודע כמה עולם הסייבר יכול לפגוע במובייל ובכלל במשאבי הארגון אם יש גישה במובייל. לדעתו עולם הסייבר יפרוץ יותר למובייל בעתיד.

כמו כן, בשולחן עגול הוזכר נושא הסייבר בהקשר של טלפוניה ועולם call center. התחזות דרך הטלפון, גניבת שיחות רגישות של לקוחות- השאלה אם זה סייבר? אי אפשר לקרוא לכל דבר סייבר.

לקוח אחר מספר כי הוא רואה ומרגיש את נוכחות הסייבר בשטח. ב7 לאפריל אמר כי ההתקפות השתכללו, אך מצד שני לא כל כך ברור היה מי נגד מי. כארגון הם רואים דרישות של משתמשים פנימיים לגישה למערכות הליבה של הארגון דרך המובייל. דבר המהווה סכנה של אבטחת מידע ואתגר לא פשוט.

לקוח אחר מספר כי יש רשימה של המלצות לחוקים בFW לחסימה ופותרים פורט רק במידה ויש אירוע קריטי הדורש זאת. הלקוח מספר כי התקפות יכולות לבוא מכל העולם אפילו מישראל עצמה ואין לסמוך על אף אחד. מצד שני, אי אפשר לסגור את הרשת הארגונית לגמרי, הארגון חייב להמשיך לתפקד.

בנוסף, עלה בשולחן עגול תפקיד חדש ותקן למשרת מנהל סייבר. בצבא כבר קיימים תקנים בנושא זה לעומת ארגונים אזרחיים שלא רואים זאת ובכלל תקני משרות אבטחת המידע בארגונים יחסית מצומצמים.

לקוח אחר ציין כי סייבר תרם למודעות של ההנהלה לנושא אבטחת מידע. הנושא עולה בישיבות דירקטוריון ואף מתוקצב בהתאם. סייבר מאיים תחילה על תשתיות לאומיות כגון, חשמל.

אחד הלקוחות מספר כי עולם אבטחת המידע השתנה מאד לעומת מה שהיה לפני 30 שנה. אבטחת המידע משתנה באופן דינמי והתרחבה באופן משמעותי. הלקוח ציין כי אצלו בארגון יש שלוחות בחו"ל והם חייבות להיות פתוחות. ישנה המון פעילות בתחום הסייבר בארגון. הלקוח מציין כי מה שהכי טוב בסייבר זו המודעות לאבטחת מידע אשר הגיעה להנהלה.

לקוח אחר טוען כי אין צורך לרוץ ולרכוש מוצרים להגנה מסייבר. לדעתו, כולם מוגנים מספיק טוב עם הכלים הנוכחים של אבטחת מידע היום. הלקוח ציין כי לפני ההתקפה הם סגרו עצמם הרמטית עם מוצרי אבטחת מידע קיימים גם ע"י חסימה מחו"ל. מצב זה לא פגע בשירות. דוגמה נוספת, בארגון ישנם גם שרתים שמוגנים ע"י ARBOR, ובזמן התקיפות המוצר לא הגן כל כך. היות והוא לא קונפג תקין. יש לשים לב ולעבור על קונפיגורציה וחוקיות במוצרים קיימים בארגון על מנת למצוא פרצות. זו דוגמה שכל ארגון צריך ליישם ולהביא את המוצרים הקיימים לאופטימיזציה.

לקוח אחר מספר כי המילה סייבר גרמה לארגונים להיערך יותר בנושא אבטחת מידע ולשים דגש על מודעות העובדים והלקוחות בארגון. הלקוח ציין כי שבועיים לפני המתקפה שהייתה באפריל הם התייעצו עם אבנט ועשו הערכת מצב כולל סידור חוקים בFW ובשאר מוצרי האבטחה. מה שגרם לנושא להצליח הינו שיתוף הפעולה בין הצוותים בארגון- צוות הסיסטם, האבטחה, והhelp desk. כמובן שגם הנהלים תרמו לכך. הארגון הכניס מספר מוצרים SWAT-NAC לבדיקת פוליסי וחסימה של גורמים חיצוניים, גלישת אינטרנט מאובטחת, גם fireeye תרם לנושא. הייתה גם היערכות גדולה מבחינת משתמשי הארגון.

לקוח אחר מאמין במהות של המילה סייבר. הוא טוען שאם ספקים מנסים למכור מוצרים שונים זה אומר שאכן קיים משהו בשטח. לדעתו אין מענה אמיתי לסייבר, רק הקמה של חמ"ל, עם כ"א ומערכות שיושבים 24/7. לדעתו תחום הסייבר יחסית צעיר היום ולא כולם מודעים אליו. אבטחת מידע המסורתית יודעת להתמודד מול איומים קטנים כמו סוס טרויאני. השאלה אם ארגונים יודעים להתמודד מול ארגוני פשע הקיימים בסין? ארגונים בהם מתמקדים על ארגון אחד ומנסים להפיל אותו. ישנם האקרים שיושבים בארגון מספר שנים ואף אחד לא יודע מקיומם. לדעתו סייבר זה לא רק

buzzword זה אכן ריאלי. הלקוח מספר כי חוו מתקפה רצינית במשך מספר ימים. לכן לדעתו אי אפשר להגיד שהתקפות לא קיימות היות והם התמודדו מול מתקפה של אנונימוס. לסייבר אין תשובות ברורות וארגונים בוחנים המון מוצרים בנושא. הלקוח טוען כי ניתן לפרוץ כל מוצר אם מתאמצים מאד למרות penetration test. אי אפשר להתעלם מזה ואי אפשר לסמוך על אף אחד.

אחד הלקוחות דווקא מתחום ביקורת אבטחת מידע מספר על היערכות הארגון ובשלותו בנושא סייבר, נערך בעזרת סטרטאפ בשם cyber arm. למעשה, הספק לקח את כל התוקפים המוכרים, יכולות התקיפה, הסתברות לתקיפה, מערכות ארגוניות הקשורות לתקיפה ויצרו אקסל גדול בו ניתן לראות מהם הסיכונים הרלוונטיים לארגון. בעזרת זה הארגון ראה את רמת הבשלות של המערכות הארגוניות לסייבר. הלקוח מציין כי חשוב לדעת איפה כדאי להתמקד, להשקיע ובאילו מערכות ארגוניות בעלות חולשות. לקוח אחר טוען כי זו גישה טובה אך מאד קשה לערוך זאת. המדדים הם לא כמותיים ואיכותיים וקשה לקלוע לסבירות ולהסתברות בצורה נכונה לכל איום שהיה כלפי הארגון או המגזר בכלל. אך מצד שני זה נותן הערכה וראייה למצב הארגוני כיום. בנוסף, הלקוח טוען כי זו נקודת פתיחה מצוינת אך עקב הערכה שגויה ייתכן ולא יטפלו במשאבים למטה ועלולים לפספס דברים שהם קטנים וחשודים יותר. ניתן לעשות זאת גם ברשתות חברתיות הקשורות לארגון או ברשת ארגונית מסוימת.

מודעות משתמשי הארגון

אחד הלקוחות מספר כי קיימת מודעות רבה לנושא אבטחת המידע בארגון. בתקופה האחרונה מפורסמות מתקפות רבות בחדשות והעובדים נלחצים ואף מודיעים אם מגיע אליהם מייל מזר. הם מדווחים למחלקת אבטחת מידע בנושא. נושא המודעות צף למעלה להנהלה. גם המנהלים נלחצים מהנושא ומקיימים פורום אבטחת מידע אחת לשבועיים, מה שלא היה בעבר, בנוסף יש ועדות תכופות בנושא. בארגון אין חדר מצב להתקפות או חמ"ל בו הכל מנוהל.

לקוח אחר מספר כי בנושא מודעות העובדים עושים הרבה. עדיין לא עושים תרגול של אנשי אבטחת מידע. ישנם הרבה רגולציות שדרכם נערכים ביקורות בנושא אבטחת מידע. הארגון מאד מתמקד בנושא מודעות העובדים וauditing בתוך הארגון. הם פיתחו תהליך בו יכולים לדעת מי המשתמש שניגש לDB לא כלים חיצוניים. כמו כן, הלקוח ציין כי כל שנה נושא ה SIEM עולה ונדחה לשנה הבאה. הבעיה הגדולה היא הרגולציה היות והמידע בארגון רגיש ויש לדעת איפה הוא נמצא לא כמו בענן. קשה להוציא מידע ארגוני החוצה כי לא ידוע איפה הוא עובר וזו בעיה מבחינת הארגון.

לקוח נוסף מספר כי אצלם נושא המודעות בא לידי ביטוי בעזרת הדרכות לעובדים, סרטונים בנושא אבטחת מידע, לקוח אחר מספר על ניוזלטר שמוציאים עם מחקרים חדשים באיומי אבטחת מידע ווירוסים.

לקוח אחר מספר כי הסייבר עושה באזז ולצער לא הוקצו משאבים רבים לנושא, ואף לא כח אדם. לכן, הם ממשיכים לטפל בנושא אבטחת מידע כמו שהיה עד היום ולנסות לנצל את הכלים הקיימים בארגון. בנושא מודעות העובדים הם לא עושים מספיק לפי טענת הלקוח.

לקוח נוסף מספר כי בארגון השקיעו בשנה האחרונה בנושא מודעות כל רבעון יוצא מייל לכלל עובדי הארגון בנושאים חדשים. בנוסף, יצרו מצגת פשוטה ומובנת בנושאי הגנת המידע הארגוני והכריחו את המשתמשים לעבור 20 דקות עליה פעם בשנה.

ארגון אחר מספר כי יצרו הדרכה ייעודית של מחלקת ההדרכה פעם בחצי שנה, מעין מיני כנס של אבטחת מידע להעלאת מודעות העובדים. מבחינת מדיניות אבטחת מידע יש מילים שוטפים באם מתוכננת מתקפה וערנות בנושא. הארגון עשה קורס של 5 ימים לכל מנהלי מחשוב ממוקד סייבר. לדוגמה אחד השיעורים היה בנושא פיתוח אפליקציות מאובטחות. נושא שלא היה כלל מודעות אליו בארגון ובעוד הרבה ארגונים. בקוד פיתוח יכולים להיות המון פרצות וחולשות. הלקוח מספר כי היה קשה להכניס את המשמעות של אבטחה בפיתוח וביצירת קוד מאובטח. לא הכל זה false positive. יש לציין כי גם כל צוותי הפיתוח עברו קורס של קוד מאובטח. כיום הארגון עובד עם checkmarks. קצת קשה לאנשי הפיתוח להבין זאת אבל אין ברירה. דרישה זו הביאה את אנשי אבטחת המידע לבדוק תקינות וחולשות בקוד.

לקוח אחר מציין כי נושא המודעות חשוב היות וסייבר יכול להביא לפגיעה במוניטין הארגון. בארגון יש מודעות- עובדים ערניים למיילים או למשהו חשוד בעמדות המחשוב שלהם. יש הדרכות פנימיות לעובדים וכולם עוברים לומדה בנושא פעם בשנה או פעמיים, עם מבחן סופי חובה. יתר על כן, יש סרטונים בנושא אבטחת מידע וחדשות מהעולם ומדיניות אבטחת מידע מתעדכנת בהתאם ומופצת.

לקוח נוסף מספר כי הגבירו את מודעות המשתמשים ע"י שליחת וירוס בסיסי מספר פעמים דרך PDF, או PPT בהם מזינים פרטי עובד לשם הגרלות. התוצאה היו עובדים בודדים שהתפתו ופתחו את הקובץ. למשל, שלחו אקסל עם משכורות של מנהלים בארגון ואנשים נכנסו ללחץ עד שהגיעו למנהל משאבי אנוש על כך שמתקיפים אותם. המשתמשים פוחדים לפתוח כל מייל חשוד וזה מעולה.

מדיניות אבטחת מידע

דיברנו בשולחן עגול על נושא תכיפות ההתקפות. יש הנחיות של רגולציה לנושא של סייבר, גנריות ואין הנחיות ספציפיות לנושא. הכל בצורה לא פורמלית בינתיים. לכן, כל ארגון צריך לשים לב למדיניות, לבצע זיהוי ואיסוף מידע מודיעיני בחוץ ובפנים לבנות הגנה פרו-אקטיבית של כלי אבטחת מידע. אי אפשר לנצח הכל! חשובה ההיערכות מראש של נהלים, תהליכים, תרגולים והתמודדות לאחר אירוע. חשוב להתכונן ליום שאחרי ההתקפה והתגובה בארגון. חשוב לשים לב שמצליחים להטמיע נהלים ולא רק לתת אותם. מבחן התוצאה הוא הטמעת המוצרים והאם הם עוזרים בשטח כנגד מציאות הסייבר. בנוסף, יש לקיים תירגולים של צוות אבטחת המידע בפרקטיקה. כלומר, את מי צריך ליידע בזמן אירוע, איך לפעול ועד נוהל לטיפול בנושאים קריטיים.

לקוח אחר מספר כי נושא הסייבר בא לידי ביטוי במדיניות אבטחת מידע קיימת. הארגון הכניס הרחבה לנושא אבטחת המידע במדיניות בעזרת כמה סעיפים בעקבות הסייבר. הארגון בחן לפני שנה פתרון מאד כללי לסייבר הנקרא cyber sense שעוד היו בהתחלה. הפתרון מתעסק בהoney pots ברשת. כרגע ממתינים לסיום הפרויקטים עד להתקדמות שאר הפרויקטים. הבעיה שאין הרבה כ"א הקשור לאבטחת מידע.

לקוח אחר מספר כי יש מעקב מסודר על מדיניות אבטחת המתעדכנת מפעם לפעם. חובה להעלות פעם בשנה את מסמכי המדיניות לדיסקטוריון ואז באישורם מפיצים לכלל הארגון.

כלי הגנה /zero day /סייבר

לקוח אחד מתאר כי יש להיעזר בכלים שיושבים ברשת, מאזינים ומזהים אנומאליות. חשוב לציין כי הכלל במונחים עסקיים- שפה עסקית לא רק פורטים ופרוטוקולים. לדוגמה, אם אדם הדפיס יותר ממה שאמור היה להדפיס, פניות לDNS או העתקה לדיסק חיצוני מה שאסור בארגון, כל הדוגמאות הללו מהווים התנהגויות חשודות אשר יש לבדוק ולטפל בהתאם.

באותו ארגון מי שאחראי לאכיפה ולפיקוח הוא אגף הביטחון. יש מנהל אבטחת מידע המגדיר מהו המידע הרגיש וזרוע טכנולוגית האחראית על כלים וטכנולוגיות ליישום בארגון. אם משתמש הדפיס יותר מדי, אנשי הטכנולוגיה מקבלים את ההתראות על הפעולה החשודה. הם אומרים לביטחון לבדוק את הנושא ולמה המשתמש הדפיס יתר על המידה או העתיק קבצים רגישים להתקן חיצוני והם פועלים בהתאם. יש תחקור של הנושא ודו"ח על התקרית. דבר כזה מתגלה לדוגמה בעזרת מערכת SIEM SOC בארגון.

הארגון מתמקד גם בעולם המובייל בו מלחמת הסייבר עלולה גם להתרחש. הדרישות עסקיות גוברות וישנם המון פרויקטים שיש להתמודד איתם ועם האבטחה בנושא. לדעת הלקוח, חשוב לבנות מדיניות וארכיטקטורה לכל נושא המובייל. כל מערכת הפעלה היום כוללת פיצ'רים חדשים וחייבים לאפשר זאת לארגון ולהנהלה. בעבר אנשי אבטחת מידע אמרו לכל דבר לא, היום זה נגמר. אותו ארגון מתמקד גם במערכות לזיהוי אנומליה. הלקוח טועם כי כל המעטפת החיצונית בארגון כבר מכוסה בכלי אבטחת מידע כגון: AV,IPS,FW. איך מאפשרים למשתמש להוציא מידע ללקוחות החוצה? ניתן להשתמש במוצרים לניהול הרשאות כמו ורוניס, מוצרי DLP. איך נתפוס משתמשים לגיטימיים המבצעים פעולות חשודות ברשת? יש כלים כמו netwitness האוספים המון לוגים ואז ניתן להבין מה קורה ברשת ולבדוק כל פעולה. הלקוח ציין כי ביצעו פיילוט עם סטרטאפ בשם light cyber המורכב מאלגוריתם חכם שלא צובר המון לוגים אלא מחפש אנומליות ברשת בזמן אמת. הלקוח מספר כי העולם השתכלל וניתן להגיע למשאבי הארגון דרך ספקי הארגון ולקוחותיו.

לקוח אחר מספר כי אין להם כלים המתמודדים עם zero day, נושא התקנת patches מאד מורכב אצלם ולא יוצא לעדכן בתכיפות. כרגע לא בחנו שום מוצרים חדשים בנושא סייבר. ישנם ארגונים המטפלים בנושא zero day בעזרת כלי DLP- זליגת מידע.

לקוח אחר מתאר כי מי שאחראי להתנהגויות חשודות ברשת זה מחלקת אבטחת המידע והסיסטם בשילוב. אם יש משהו קריטי ברשת הארגונית יש התערבות של קצין הביטחון. אותו ארגון משתמש בשירות של ספק אינטרנט להגנה מפני DDOS. לקוח אחר מוטרד מאד מהקלות בה יכולים היום להפיל אתרי אינטרנט של ארגונים בלי להתאמץ או להגיע לתוך הארגון. אותו ארגון מספר כי הטמעת patches הינה מהירה אצלם- גג 2-3 חודשים על השרתים. הארגון עובר על לוגים ומסמן שרתים קריטיים יותר בהם האתחול יותר בעייתי. רוב השרתים בארגון לא מספיק קריטיים וניתן לבצע איתחול בשעות הלילה ולכן התקנת patches מהירה. הלקוח מספר כי בסופו של דבר אבטחת מידע נותנים הנחיות ונהלים לסיסטם האחראים על שרתים ומבצעים את המדיניות בפועל. אותו ארגון מספר כי הם מריצים את אותו patch על שרת וירטואלי או סביבה מצומצמת על מנת לבדוק שאין בעיה באותו עדכון. כמו כן, אותו לקוח מספר כי עשו פיילוט של מוצר בשם fireeye שלא הוכיח את עצמו באופן מלא. כמו כן, מספר לקוחות טענו כי המחיר יקר מדי. מרבית המשתמשים בארגון לא בעלי הרשאות על התחנות, ולכן לא מורשים להריץ קבצי הרצה. הארגון עושה שימוש

בעמדות קצה "רזות" thin client וכתוצאה מכך ייתכן כי fireeye לא הועיל. [לא הבנתי את העניין-אומנם המשתמש הארגוני אין סימט אדמין אבל האם לא ניתן להריץ את fireeye מהמרכז עם הרשאות של אדמין?] הלקוח טוען כי מערכות אבטחה אחרות לא מספיק בשלות לנושא האנומליה. בנוסף הלקוח אומר כי לדעתו אין מערכת שיכולה לתפוס zero day בצורה ממש טובה.

ארגון אחר מספר כי הם שוקלים פתרון אנומליה של sourcefire שהוא גם FW, IPS, ובודק אנומליה ברשת. הארגון טוען כי נראה שיש למוצר יכולות מדהימות על סמך המסמך אך עדיין לא יושם בפועל. המוצר יקר מדי. הארגון כרגע נמצא בתהליך בחינת IPS, שיעזור להם להתמודד עם מתקפות הסייבר. כמו כן, הארגון שוקל להכניס SIEM להתמודדות עם zero day. הארגון טוען שכנראה לא תהיה ברירה להכניס מוצר אנומליה לרשת הארגונית גם. הארגון חוסם תקשורת מחו"ל, ברמת ISP, וגם ארגונית. יש להבין אם צריך גישה לחו"ל היות ולא כל דבר מהווה צורך עסקי. למשל, עובד בינלאומי שרוצה לראות את האתר של הארגון מחו"ל חד פעמי- האם באמת צריך לפתוח את כל הפורטים לחו"ל?

לקוח אחר טוען כי ההגנה ההיקפית ברמת ISP כבר לא מספיקה כיום ויש לבחון מוצרים לזיהוי אנומליה כמו netwitness שבחנו. לסוף, גם הטמיעו light cyber. הלקוח מספר כי המוצר מאד יפה ובעזרתו הצליחו לזהות דברים שלא ידעו עליהם ברשת. כיום בודקים את הלוגים ומעבדים אותם לSIEM שעדיין גם בהטמעה. הלקוח טוען כי בעזרת מוצרים קיימים קשה לזהות zero day צריך ממש לחפור בתוך הרשת לשם זה.

אחד הארגון מספר כי אצלו יש גלישה לאינטרנט דרך VDI, עמדות נפרדות כולל whitelist של אתרים חשודים או לא. הארגון משתמש בכלי לניהול לוגים של HP בשם ארקסייט אשר זורק התראות בהתאם. בארגון יש הפרדה בין מחלקת אבטחת המידע לID. לארגון יש מערכת לניטור לוגים והתראות- פיתוח עצמי שלהם ונושא של מודיעין SOC גם. נושא המודיעין תורם לארגון להשוות עצמו מול ארגונים אחרים ומתחרים בכלל. בעזרת נושא המודיעין הארגון יודע מה קורה ברשת החיצונית באינטרנט, מה הולך לקרות, מתי וכמה. הם יודעים אם מתוכננת התקפה בכל האתרים ואז לוקחים ויוצרים עותק של האתר בענן לשם הגנה.

לקוח אחר אומר כי השינויים הקטנים במערכות כיום הם אלה שנותנים מענה אמיתי כמו למשל חסימת פורטים מחו"ל [אבל אמרנו שגם מישראל יכולים לתקוף לא?]. במתקפה שהייתה באותו הארגון זה מה שעשו כצעד ראשון. זו בעיה לחסום גישה מחו"ל היות ויש לקוחות מסתובבים בעולם ורוצים גישה לשירות בארגון. יש להבין כי קיים סיכון גדול בגישה לחו"ל. הלקוח מספר כי יש הבדל עצום בנושא הגלישה לאינטרנט דרך סביבה נפרדת ו ישירות. לארגון קשה להתמודד עם כל כך הרבה IP פתוחים החוצה. הכל זו תוצאה של ניהול סיכונים והאם כל ארגון מאפשר לעצמו זאת. למשל, בארגונים ביטחוניים חוסמים הכל ולא לוקחים סיכון. במקרה של סייבר שעומדים מול ההנהלה באמת יאפשרו לך כלים וכח אדם- השאלה איזה ואיך. באותה התקפה הלקוח ציין כי ספקיות האינטרנט לא נערכו להתקפה מבחינת קינפוג המוצרים. לכן, היה תהליך מסודר של הפקת לקחים מול הספקיות והחמרה בחוקים וקינפוג הכלים. בנוסף, הארגון הריץ במקביל המון סריקות על האתרים שלו והקשיח בצורה יותר משמעותית כלים כמו WAF. היום הארגון לא מאובטח ב 100% כי תמיד תהיה איזו פרצה או חולשה מסוימת ואפילו קטנה. למשל, עדכונים לשרתים זו בעיה בארגון. היות ויש חשיפה לסיכון בייצור אם יש פגיעה באבטחת המידע וזה מאד רגיש.

לקוח אחר מספר כי הגיע מהצבא שם הסביבה הייתה פרנואידיה. לכל סיכון עשו ניתוח איומים, גם ברשת סגורה הרמטית יש איומים. כיום בארגון שלו יש פחות דגש על אבטחת מידע. גם אם הכל מנותק מהאינטרנט עדיין יש איומים. איומים יכולים להגיע מלקוחות חיצוניים ואף ספקים הניגשים למשאבי הארגון. הלקוח מספר כי שיבוש מידע, זמינות מידע ודליפת מידע הם הנושאים הקריטיים עליהם הארגון צריך לשים דגש. באותו ארגון קשה מאד לעשות denial of service אם לא מחוברים לרשת. הארגון בחן מוצרי zero day המטפלים בכתיבת וירוסים ייעודיים לארגון. הלקוח חושב שהם לא מעניינים האקרים אך עדיין יש לנקוט בפעולות מתאימות לסייבר. אנטי וירוס כבר לא רלוונטי היום. כיום ישנם תרחישים בהם טכנאי חיצוני או מנקה יכולים גם לפגוע בארגון ע"י גניבת מידע רגיש או העתקתו. לפי ניתוח איומים שעשו הלקוח חושב שהאקרים לא ישימו אותו בראש סדר העדיפויות. יכול להיות שזה ישתנה בעתיד. הארגון בחן את סימנטק whitelist ויש מוצר גם של מקאפי בנושא. במוצר עצמו מגדירים אילו קבצים ירוצו במערכת וכל השאר שאינם ברשימה נחשבים חשודים. זה למעשה ההפך ממוצרים אחרים בהם מגדירים אילו קבצים חשודים עלולים לכלול וירוס. אנטי וירוס רגיל צורך משאבים גבוהים מהמחשב. לכן המוצא לא מנטר כל קובץ אלא רק קבצים מעניינים ומי שמנסה לשנות אותם הוא מתריע. המוצר לא נותן לשנות את הקבצים ואם השתנה אז איר.

לקוח נוסף מספר כי גם לא הצליחו לממש באופן מלא fireeye. כעת בוחנים מוצר אחר של websense שעובד בשיטה של sandbox, גם לפאלו אלטו יש סוג של sandbox. כלי ה DLP משמש את הארגון בינתיים ל zero day. יש בדיקה של הרשאות המשתמשים בתחנות, segregation of duties, חסימת התקנים חיצוניים. מנסים לבחון גם את Sourcefire מצד אחד חדשני ומצד שני מזכיר את snort שכבר קיים.

התרחבות עמדות הקצה המובייל גם גרם לחשש נוסף בקרב מנהלי אבטחת מידע בארגונים. יש ניסיון להטמיע מודולים של מוצרים פעילים כיום גם במובייל.

לקוח אחר מספר כי נושא ה network access control – NAC גם חשוב מאד בארגונים. כיום עובדים עם SWAT. בעקבות הבאז על הסייבר נערכו במרבית הארגונים penetration test לכלים הקיימים ולמציאת חולשות ואיומים ברשת.

המלצות STKI בנושא סייבר

Recommendations

- 1) Install fast patches
- 2) Education- Employee awareness
- 3) Training
- 4) Forensics process
- 5) Strong authentication- segregation of duties
- 6) Focus on behaviors **inside** your business – explore and analyze.



נספח מיוחד התייחסות ספקים ויצרנים לנאמר במפגש

התייחסות חברת WE

איש קשר: דורי פישר 0523239774 dori@we-can.co.il

בחברת We! אנו מאמינים כי העידן הנוכחי באיומים הוא עידן ה Post Prevention, הכוונה הינה לכך שווקטור ההדבקה של תחנות \ שרתים בארגון אינו ידוע ואינו ניתן

לחיזוי מראש. יתכן ויצרן התוכנה החביב על הארגון, אפשר קוד זדוני בתוך הדיסקים שסופקו וכך דיסקים מקוריים של יצרנים אינם עוברים הלבנה או לחלופין שדיסק חיצוני

חובר פיזית או שמדובר במחשב נייד שהדביק וכן הלאה.

מכיוון שווקטור ההדבקה אינו ניתן לחיזוי ואף סביר שכבר קיימת הדבקה מסוימת בארגון, אנו מאמינים שיש לרכז את המאמצים בזיהוי מוקדם ככול האפשר של הנוזקה.

בסקר שבצעה וריזון (<http://www.verizonenterprise.com/DBIR/2013>), המתייחס ל 47,000 אירועי אבטחת מידע, נמצא כי זמן זיהוי הנוזקה עומד על חודשים בכ 66% מהארגונים!

הנזק שנגרם בחודשים בהם פעלה הנוזקה ללא הפרעה הוא זה אשר ארגון חייב למזער באופן משמעותי.

אתגר נוסף שקיים בארגונים שכבר הטמיעו מערכות ניהול אירועי אבטחת מידע (SIEM), הינו שלאחר זיהוי מוצלח של תחנה או משאב פנימי שסורק את הרשת למשל או מבצע כישלונות רבים בהזדהות,

הארגון חסר את הידע והניסיון לאתר את הנוזקה בתחנה שבהרבה מקרים אינה מזוהה על ידי האנטי וירוס המותקן.

כיום, מעל 10,000 תחנות ושרתים במדינת ישראל כבר מוגנים ע"י - ECAT <http://www.siliciumsecurity.com> ואנו מזהים וחוקרים קוד עיון באותן תחנות.

ברמה הרשתית חברת ווי מייצגת את דמבלה <https://www.damballa.com> אשר מאפשרת זיהוי של תעבורה חשודה ע"י Sandbox ברמת הענן וניתוח מבוסס פטנט של DNS, כחמישה מתוך 10 ספקי האינטרנט העולמיים עושים שימוש בפתרון של דמבלה ללקוחותיהם.

התייחסות חברת Prodware

איש קשר: אלון בן-טולילה 0732770001 abentolila@prodware.fr

כאינטגרטורים למערכות ERP, CRM, SharePoint, ומערכות IT אחרות, אנו נחשפים לארגונים רבים בהיבטים של אבטחת מידע, סיווג ומידור מידע.

הניסיון שלנו מראה שהגופים המסווגים בטחונות משקיעים תקציב גבוה יותר באבטחת מידע מאשר הגופים המסווגים עסקית.

בנוסף, מנסיונינו, המודעות להיבטי אבטחת מידע גבוהה יותר בקרב גופים הבטחוניים מאשר בגופים העסקיים.

מכאן, המלצתינו היא לשתף ידע ממוקד Cyber ואבטחת מידע בכל הדרכים האפשריות, בין הגופים הבטחוניים לגופים העסקיים וכך לצמצם את הפער.

התייחסות חברת Mobisec

איש קשר: ליאור דולפין 0547345679 lior@sourcefire.com

התאמת אמות מידה של הגנה לגל האיומים הבא

נראה שכל חמש שנים בערך אנו עומדים בפני מחזור איומים חדש – החל בוורוסים, עד 'תולעים', תוכנות ריגול (spyware) וערכות שורש (rootkit). היום אנו מוצאים עצמנו נאבקים בגל האחרון – תוכנה זדונית מתקדמת, מוכוונת להתקפות ולאיומים מתקדמים נמשכים (APT). בזמן שאיומים אלו הוכיחו עצמם כהרסניים יותר, עלינו רק לבחור באלו טכנולוגיות מתאימות לנו וליישם אותם בצורה נכונה.

בנוף איומים זה, המתפתח כל הזמן, עליך לשאול את עצמך: האם אני נוקט באמות המידה הנכונות בבואי להגדיר את הדרך הטובה ביותר להגנה על הארגון שלי מפני מתקפות מתקדמות?

מודול AMP – Advance Malware Protection

חברת Sourcefire פיתחה טכנולוגיה חדישה המאפשר זיהוי קוד זדוני בקבצים העוברים ברשת והתנהגות תעבורת רשת של רוגלות, קיים גם מודול endpoint למערכות הפעלה מבוססות windows ו-Android. (מתוכנן גם מודול עבור MAC ו-iOS). טכנולוגיה זו מתבססת על טכנולוגיית ענן כך שכל קובץ העובר דרך הסנסורים של חברת Sourcefire לוקח "תביעת אצבע" (Fingerprinting) של כל קובץ אשר נשלח אל הענן (למען הסר ספק, קבצים לא מועלים לענן, אלא רק תביעות האצבע שלהם) ומשם מתקבלת תשובה לגבי מהות הקובץ – האם הקובץ לגיטימי ומוכר? האם הקובץ זדוני ומוכר? האם הקובץ אינו ידוע? במידה והקובץ אינו ידוע תמשיך המערכת לעקוב אחרי תנועה שלו על המחשב ולא ברשת עד לקבלת מידע חדש לגביו.

במסגרת מחשוב הענן חברת Sourcefire מנתחת מליוני קבצים ביום. ניתוח קבצים אלו מתבצע בארבעה אלמנטים עיקריים:

1. ניתוח מבוסס חתימות
 2. ניתוח היוריסטי – ניתוח באלגוריתמים ייחודיים הממפים מספר פולימורפים בקובץ לזיהוי קוד זדוני.
 3. ניתוח קובץ למול האפליקציה המריצה.
 4. ניתוח מבוסס Sandboxing – בין מערכות הניתוח קיימות למעלה מ-400 מערכות Sandbox לניתוח של קבצים על מערכות חיות.
 5. ניתוח מבוסס מנועים אנליטיים.
- השימוש ב-AMP נותן בידי גופי אבטחת המידע בארגון כלים לניהול התפרצות (Outbreak Control) תחת התקפה. בין הכלים ניתן למנות:

- חסימת קובץ/קוד
 - יצירת חתימה
 - יצירת Group Policy Control (באמצעות ה-Real-time User Awareness)
 - יצירת Whitelisting לקבצים לגיטימיים וקבצים שנכתבו "בבית" (Homegrown Applications).
 - חסימת תקשורת ויצירת Blacklist
- בנוסף, המערכת תייצר תרשים זרימת של מעבר הקבצים השונים ברשת המאפשרים להסיק איזה קובץ ייצר קובץ זדוני ועם מי ברשת נוצר קשר/הדבקה וכיו"ב על פני ציר הזמן:

בגישה של לפני ההתקפה, תוך כדי ואחרי ההתקפה אנו מספקים פיתרון הגנה מלא מפני רוגלות Zero Day לרשתות הארגוניות, למחשבים והתקנים ניידים, אשר יוצאים מהארגון והם ללא ההגנה אותה מספק הארגון מקיים ביציאה לאינטרנט מהרשת הארגונית ולמכשירים מבוססי אנדרואיד.

על מנת לספק את מירב ההגנה, חברת סורספייר מאמינה כי על הפיתרון להיות משולב רשת ומכשירי קצה. הטכנולוגיה מספקת אפשרות "לחזור" בזמן ולנתח בכל זמן ארוע שהתרחש בארגון ולספק נראות והגנה מפני שרשרת התקיפה "Attack Chain", ומציגה כיצד היתבססות על פתרונות אנטי רוגלה (כמו אנטי וירוסים) ופתרונות מבוססי טכנולוגיית Sandbox בלבד יכולים לייצר תחושה מוטעת של אבטחה.

בהינתן שרשרת ההתקפה (Attack Chain), אנו יכולים בקלות לראות שתוקפים מתוחכמים ובעלי מוטיבציה יכולים ואף בפועל גוברים על טכנולוגיות גילוי גם רב שכבתיות.

למעשה, דוח חקירות פריצות המידע משנת 2012 (Verizon 2012 Data Breach Investigations Report) גילה שבכמחצית מהמקרים שנחקרו, נדרשו חודשים ולפעמים אף שנים לגלות פריצה קיימת בארגון.

זה הרבה יותר מהזמן הנדרש לתוקף להשלים את משימתו, למחוק עדויות ואולי אף לבסס "דלת אחורית" שתאפשר גישה עתידית לפריצות שיבואו לאחר מכן.

גילויים תמיד יהיו חשובים, אך טכנולוגיות גילוי סורקות קבצים רק פעם אחת. בנקודת זמן מסוימת. על מנת לזהות אם הן דדוניות או לא. אם הקובץ לא זוהה כחשוד או אם הוא מתפתח והופך לדדוני לאחר שכבר חדר לסביבה, בשלב זה טכנולוגיות גילוי כבר לא יעילות בזיהוי פעילות מתקדמות של התוקף. ומכאן לא קיימת נראות של הארגון ביחס לארוע זה, אלא אם משלבים טכנולוגיות ואנשי מחקר (Forensic).

סיכול תקיפות אינו מסתכם בגילוי אלא גם בהקטנת ההשפעה בהנחה שתוקף חדר למערכת. כשעוסקים באבטחת מידע לעולם יש להניח את ההנחה "אילו כלים \ טכנולוגיות \ ידע יעמוד ברשותי כאשר אהיה תחת תקיפה?"

יש לנקוט בעמדה פרואקטיבית להבנה ואומדן הנזק, להכיל את הארוע, לתקנו ולהבין שבחלון זמן שהיינו תחת התקפה על מחשב מסוים. האם יש בידנו כלים לדעת עם מי המחשב הנגוע תיקשר? מהרגע שהוא נחשף לרוגלה ועד לרגע שניקינו אותו? תוכנת רוגלה לרוב לא באה לבד, היא באה עם רוגלות נוספות... גם אם נתקן את הנזק שיצרה רוגלה מסוימת, אנחנו יכולים בוודאות לדעת כי לא באו עוד רוגלות? מה הנקודה בה נכריז כי הארע הסתיים ונחזיר את התפעול לשגרה? טכנולוגיות המאפשרות ניתוח אבטחה רטרואקטיבית (היכולת להביט לאחור, לנקודת זמן מסוימת ולהבין מה התרחש מאותו רגע ואילך) באופן שוטף הינן הכרחיות לסיכול תוכנות רוגלה.

- אבטחה רטרואקטיבית עושה שימוש בידע המבוסס על אבטחה בזמן אמת על מנת לקבוע את גודל הנזק, להכיל אותו ולתקן את הנזק. רוגלות והתקפות שנמשכו שבועות ואף חודשים כעת ניתנות לזיהוי, הגדרה, הכלה וניקוי מהיר ובעיקר נותנות לך כלים להבין מאותו רגע נתון שהתרחש ארוע מסוים על מחשב מסוים תוכל לקבל מידע מאד חשוב שבראייה לאחור אף קריטי – עם מי המחשב הנגוע דיבר? מול אילו מערכות? האם שונו קבצים במחשב? ועוד.

איומים יכולים לחצות היום את ההגנות הקיימות, כיום, כבר לא מספיק שיהיה גילוי וחסומה בנקודת זמן מסוימת. טכנולוגיות צריכות לפנות לרצף המתקפה השלם –

לפני ההתקפה, במהלכה ולאחריה, באמצעות שימוש ביכולת רציפה, תקבל נראות ותזהה גישות אבטחה שמשתמשות בניתוחים בענן, כדי להעריך קבצים חשודים או לא מוכרים אל מול מודיעין האיום המתקדם ביותר, לתקופה מורחבת של זמן ולקבל בזמן אמת מקהיליית המשתמשים במידע מודיעיני זה, להשגת 'חיסון' קולקטיבי'. היכולת לבצע ניתוח עמוק כדי לקשור בין אירועים, למצוא מערכות שמדגימות סימפטומים של פשרה פעילה ולאחר מכן להפוך לאוטומטי את הניתוח וסדרי

ההעדפה של הסיכונים, יכולה לשכך את הנזק ולהאיץ את תהליך השיקום בארוע מסוים. שאלות עיקריות שכדאי לשאול:

- כיצד ניתוח התוכנה הזדונית שאתה עושה מעדכן באופן אוטומטי את יכולות הגילוי בנקודות השליטה ואצל כל הלקוחות?

- איך אתה אוסף מידע מודיעיני לגבי איומים שמופיעים?

- איך אתה מסוגל לוודא אם בהתקן או במערכת מתקיימת פשרה עכשיו, או האם התקיימה פשרה אתמול?

IOC - Indicator Of Compromise - גישה זו, באה לתת מענה וציון לכל קובץ. ישנם תהליכי בדיקה מורכבים לכל קובץ ולכל סוג של קובץ.

למשל –

1. קבצים יקבלו ציונים "גרועים" אם הם בודקים האם על המערכת הפעלה קיימת סביבת VM (קבצים אילו מנסות לעקוף מערכות SANDBOX)

2. קבצים אשר מחפשים שרתי DNS שהם לא שרתי הארגון (למשל, קובץ אשר פונה לשרת DNS של חברת גוגל, אקמאי ואחרים)

3. קבצים אשר בזמן הרצתם בודקים אם קיימות תוכנות כגון Wireshark ותוכנות DEBUG אחרות

4. קבצים אשר פונים לשרתי תעודות בעולם (שרתי CA) ומבקשים לשנות או לעדכן רשומות

דבר אחד בטוח, אין שום סיבה שניתן לקבצים מסוג זה לרוץ על תשתיות ארגוניות ובטח לא על ניידים אשר נמצאים מחוץ לארגון נטולי הגנה של ה GATEWAY וכאשר חוזרים לארגון, הם בתוך הארגון ומפה מתחיל ארוע שעד היום היה מאד קשה לקבל נראות לגביו

כשזה נוגע להגנה על הרשת שלך כיום, זה דיי ברור כי אין באמת פתרונות מידיים (silver bullets) ואולי אפשר לומר גם כי הן לא קיימים. לא עובר יום מבלי שנשמע על פריצה שהצליחה. תוקפים חושבים מחוץ לקופסא וכך גם עלינו לעשות.

התייחסות חברת מטריקס

איש קשר: שלומי בוטנרו, מנהל מרכז התמחות אבטחת מידע וסייבר במטריקס, טל': 054-2278456, אימייל: ShlomiBo@tangram-soft.co.il

האקסיומה הבסיסית בעולם הגנת הסייבר הנה שניתן לעקוף כל שכבת הגנה. מתחברת אליה העובדה כי כנראה לעד יהיו קיימים Zero Days ולכן יש לספק לארגון יכולת לזהות ולהיערך למצבים אלה.

על מנת לזהות איומי סייבר מתקדמים (APT) יש לבצע Auditing במערכות הארגון, אולם לא להסתפק רק בעולם התוכן של קבצי הלוג ברכיבים השונים ברשת, אלא לחבר אותם עם התקשורת הזורמת בארגון.

לשם ביצוע פעולות אלה, נדרשת מערכת בעלת מנוע קורלציה ואנליזה מתקדמים כדוגמת QRadar מביית IBM. מספק פתרון לחיבור של עולמות תוכן המגיעים מקבצי לוג וחיבורם למידע הזורם בתקשורת (למשל בעזרת תקנים כדוגמת NetFlow, SFlow ו-JFlow). בנוסף, קיימת היכולת של QFlow אשר מאפשר לבצע DPI (Deep Packet Inspection) למידע הזורם ברשת ולזהות חריגות (למשל כמות תעבורה גדולה של תקשורת לכיוון VLAN מדפסות שאינה במבנה של Spooler, או תעבורה בפורט 80 שאינה HTTP) – קיימת יכולת כזאת גם לסביבות וירטואלית הנקרא VFlow. בעזרת יכולות אלו ניתן ליצור Baseline של אופן עבודת המערכות בארגון, לזהות אנומליות ולאתר את אותן התקפות מתקדמות.

חשוב לזכור שעצם זיהוי האירוע רק מתחיל את הטיפול בו (אירוע מזוהה שאינו מטופל דינו כאירוע שלא זוהה) ולכן יש צורך באנשים מיומנים ומתורגלים שיגיבו בזמן וברמה הנדרשת. לשם כך יש לתרגל את האנשים הרלוונטיים (למשל גופי SOC) ולהכשיר אותם בהתאם.

מרכז התמחות אבטחת מידע וסייבר במטריקס, מסייע לארגונים בבניית "המערכת החיסונית" של הארגון ושימורה, מול איומי סייבר ואבטחת המידע. המרכז מספק כלים ופתרונות להתמודדות עם איומים ואתגרים בתחומי אבטחת המידע והסייבר. מומחי מרכז ההתמחות הינם בעלי מומחיות ייחודית בתחומי הסייבר ופעילים בארגונים המובילים בתחום. המרכז מציע מגוון פתרונות לאיזון בין השקעות לסיכון, ליווי ארגונים גדולים בתהליך הפיכתם לגופים מונחי רגולציה, ליווי הקמת "חמ"ל סייבר" (מרכז מודיעין ומבצעים שנועד לעקוב אחרי איומים מתפתחים, לאתר התקפות ולטפל במתקפות ובתהליכי ההתאוששות מהן), ייעוץ הכולל ניתוח צרכים ואיומים ובניית תכניות רב-שנתיות להיערכות ולהתמודדות עמם וכן חבילת קורסי הכשרה והדרכה באמצעות מרכז ההדרכה ג'ון ברייס מכללת הי-טק.

בנוסף, מרכז התמחות טכנולוגיות למידה במטריקס, העוסק בפיתוח הדרכה והפקת תוצרי הדרכה והטמעה, פיתח ערכה הכוללת יחידת לימוד, מהלך של הטמעת השינוי, כלי לניהול ובקרת תהליך הלמידה ומנגנון תחזוקה שוטף לעדכון תכנים משתנים אשר מאפשרת למנהל אבטחת המידע הארגוני להוביל את הטמעת השינוי ולשמור על תכנים עדכניים בארגון. הערכה מספקת מענה לצורך עקרוני של שינוי התנהגות עובדים בתוך עולם משתנה, בו הארגונים חשופים באופן מתמיד לחדירות והתקפות סייבר ממוקדות.

הערכה מאפשרת למידה אקטיבית, יעילה התורמת להטמעת השינוי וכוללת לומדה אינטראקטיבית המבוססת על תרחישים מחיי הארגון בהם נדרש העובד לזהות כשלי אבטחת מידע ולהפעיל שיקול דעת בעניין דיווח והמשך טיפול ו/או מניעת התנהגות דומה בהמשך. הנושאים אליהם נחשף הלומד הם: הגורם האנושי – ריגול, הנדסה חברתית, פשינג, גניבת זהויות, אבטחה פיזית – משרדים, מתקנים, מבקרים ואורחים, אבטחה דיגיטאלית – מערכות מידע, דואר אלקטרוני, שימוש באינטרנט, טלפונים חכמים, וירוסים והתחברות מרחוק, דרכי הימנעות – הגנה, דיווח, ניהול, בקרה, אחריות ומודעות.

לפרטים נוספים: שחר טביב, מנהל מרכז התמחות טכנולוגיות למידה במטריקס, טל': 052-6058300 אימייל: stabib@johnbryce.co.il

התייחסות חברת טלדור תקשורת גלאסהאוס

איש קשר: ניר שפריר, nirsha@taldor.co.il, 054-7007936

בעת הזו אנו נתקלים בהרבה שאלות ותהיות מצד לקוחותינו בנוגע למהות הגנת הסייבר ולאיומים הקשורים לעולם הסייבר, אז כאן המקום כמובן לומר שעולם הסייבר ועולם אבטחת המידע המוכר לנו כבר 15 שנה הינם למעשה אותה הגברת בשינוי אדרת.

תחום אבטחת המידע כיום מכיל מוצרים המגנים הן מפני התקפות ידועות, מבוססות חתימות, והן מפני התקפות Zero Day שאינן ידועות ולא קיימות בעבורן חתימות, נוסף על כך, עולם החיתום (יצירת חתימות חדשות - מונח מעולם הביטוח שהשתחל לעולם אבטחת המידע) כיום איננו מצליח להתמודד עם כמות ההתקפות החדשות וכן איננו מסוגל להתמודד עם אובייקטים זדוניים בעלי יכולת הסתרה ופולימורפיזם אשר הנדסתם נעשתה מתוך כוונה לחמוק מכל המוצרים מבוססי חתימות.

בעוד שבעת הזו מרבית מוצרי אבטחת המידע הקיימים בארגונים הינם בעלי יכולת זיהוי וחיסוי המבוססים על חתימות ונגזרותיהן, ההתקפות המשמעותיות המתרחשות חדשות לבקרים הינן דווקא התקפות מבוססות Zero Day שאינן רלוונטיות למוצרים אלו, כאן המקום לומר כי מוצרים אלו קיימים כבר למעלה מ-15 שנים ובבסיסם יוצרו לצורכי מניעה של התקפות שהיו נכונות לתקופה היא.

אם כן, כל ארגון שמבין כי עליו להתגונן ממתקפות עכשויות ובין היתר ממתקפות Zero Day, חזקה עליו שיצטייד במערכות המתאימות להתגוננות ממתקפות אלו, יש להסב נתח השקעה שמבוצעת במוצרים קונבנציונליים להשקעה במוצרים מתקדמים בעלי יכולות המתאימות למתקפות המתקדמות, נוסף על כך יש להסב שעות אדם מטיפול שוטף במוצרים קונבנציונליים (הגדרות, תקלות, חוקים ועוד) לטובת חקירת אירועים אנומליים ברשת הפנימית והחיצונית באמצעות המוצרים המתאימים לכך.

מבחינת סט המוצרים הנכון למתקפות העת החדשה, יש לשים דגש על מוצרים הנותנים Visibility (נראות) על המתרחש ברשת התקשורת ובתחנות הקצה, יש לבחון ולהטמיע מוצרים המנתרים פעילות החורגת מהשגרה הן ברמת תעבורת רשת התקשורת והן ברמת מערכות ההפעלה בתחנות הקצה, לעניין זה, רק מערכות המבינות את המתרחש ברמת מערכת ההפעלה וה-Kernel יכולות לראות אירועים הקשורים לפעילות של rootkit ואף פעילות של Bot'ים מתוחכמים, כמו כן, רק מערכות המבינות התנהגות פרוטוקולי תקשורת גלויים ומוצפנים, יזהו אירועים זדוניים בהסתברות גבוהה.

ולבסוף, יש להקנות לצוותים המקומיים את יכולות הניתוח וההבנה של אירועי רשת ואירועים על תחנות הקצה לצרכי הסקת מסקנות, הלבנת תהליכים לגיטימיים והתראה ממוקדת בעת זיהוי חריגות או אירועים בעלי אופי זדוני, בארגונים אשר אין בנמצא יכולות שכאלו או צוותים מתאימים, יש להסתייע בשירותי PS של מומחי אבטחת מידע חיצוניים ברמה רבעונית לפחות.

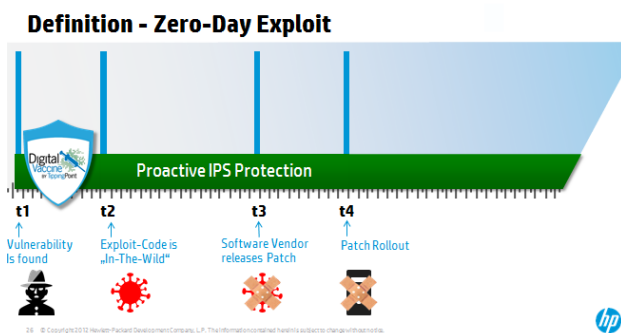
התייחסות חברת HP

איש קשר: אייל דאלי Eyal.dali@hp.com 052 4840866

HP TippingPoint Zero Day Initiative

אחד הכלים הבסיסיים להתמודדות עם להתקפות ממוקדות zero day שילוב Intrusion Prevention ברשת הארגונית. כאשר משקיעים במערכת Intrusion Prevention, הנתון המרכזי לרכישה היא היכולת להבין שמהערכת שהארגון החליט לרכוש תוכיח את עצמה. כלומר, שהמערכת תעמוד באיומים ותתן את ההגנה הנדרשת ברגע האמת.

כדי להבין את יכולתו של כל אחד מהיצרני ה-IPS על הלקוח להכיר את יכולת הספק להגיב לאיומים, את היכולת לנתח את בסיס הידע של כל ספק ואת היכולת שלו להיות ערוך ברגע האמת.



יצרני FW/IPS רבים בונים את יכולות הכיסוי שלהם על גופים בלתי תלויים (צד שלישי). הגופים הללו מספקים ליצרן את המידע על פגיעיות ונוזקות שנמצאו ברגע שהם הופכים להיות פומביים. ברגע שהיצרן מקבל את המידע, הם מייצרים את מנגנון הגנה (חתימה).

דוגמא בולטת למנגנון המפיק מידע שכזה / TELUS

Assurant. רוב הספקים מוסיפים מידע שמספקים חברות התוכנה והיישומים (מיקרוסופט למשל) Microsoft Active (MAPP). MAP ©.

במקורות אלה של מידע, חלק גדול מהמידע שיש לספקים הוא דומה, והמאבחן היחיד הוא להבין איך אותו ספק הגיב למידע.

נקודות תורפה הבולטת במנגנון הזה הוא שהמידע מגיע לא פעם לידיים הלא נכונות -> התוקפים.

נכון להיום, יש שני מקורות מחקר עצמאיים וזמינים לטובת ציבור הלקוחות שיכולים לסייע להם להבין איזה מהספקים יכול לעזור על בסיס ההשקעה משקיעים במחקר הפגיעיות וכתצואה מכך למי יש את הסיכוי הטוב ביותר להישאר ביתרון ברגע המאיים ולתת את ההגנה האפקטיבית ביותר.

Frost & Sullivan הוא אחד מהמקורות העצמאיים שמשחרר אחת לרבעון דוח המרכז את ממצאי נקודות התורפה שנמצאו ומדרגת את הארגוני האבטחה שגילו אותם. בנוסף לכך, חלק מחברת התשתיות והתוכנה משחררים עלוני אבטחה המתארים את נקודות תורפה שנתגלו במוצריהם ונותנים קרדיט לארגונים שהשתתפו בגילוי נקודת התורפה.

HP TippingPoint מובילים ב-3 השנים האחרונות באופן קבוע את תחום המחקר ומציאת פגיעיות וממשיכים להגדיל את תרומתם לקהילת המחקר הגדולה יותר. פירות ותוצרים שהן תוצר של השקעה חזקה ופיתוח המהיר של אבטחה. במערכות המתקדמות והחדשניות של HP TP ניתן למצוא יכולות חיזוי מתקדמות להתנהגות חשודה – אנומליה ברשת. המערכת יכולה להבין התנהגות חשודה ולתת התראה ו/או הגנה בהתאם.