

האבטחה היא רק הבטחה...

היום, ברגע זה ממש, כל כך הרבה מידע אלקטרוני זורם אלינו "בעורקי ונימי" התקשורת, מה הסיכויים למצוא את אותו גורם טוין באותן מיליארדי חבילות המידע? מכאן, שהאבטחה היא רק הבטחה...

רואי כהן *

מה עושים? בונים מערכות ריגול חיצוניות, כגון אוניות בסגנון ליברטי, שהוטבעה בים התיכון (על ידי חיל הים שלנו), לווייני ריגול, מטוסי ריגול ועוד... כל אלה עסקו באזנות וריגול.

האמריקנים החלו אט אט להיות חרדים לבעיה, בשני העשורים האחרונים החלה מגמה חדשה, רעיונית בלבד, שאת סופה אין לצפות מראש.

הרשת כבר הייתה בידי הציבור, אז למה לא לשחררה לעולם ולנצלה לצורכי האזנה, יש האומרים גם האזנה לצורכי "ריגול עסקי" וגם לצורכי ביטחון פנים וחוץ.

האפשרויות הגלומות ברשת בינלאומית כוללת ללא גבולות גיאוגרפיים עם פוטנציאל מסחרי כמעט אין סופי (ראה ערך הבהלה להיי-טק) הוכיחו לאמריקנים כי עשו צעד אסטרטגי מהחשובים שנעשו בהיסטוריה צבאות העולם ואולי החשובה ביותר, פעולה זו תוביל אותם לבניית המערכת המודיעינית הגדולה ביותר על פני כדור הארץ.

בעבר נתן לנו להבין, כי אין ולא יהיה שום גורם יותר מכריע במלחמה מהיכולת המודיעינית לאיסוף מידע על האויב מהאויב עצמו.

מדוע אסורה הייתה ההצפנה ויוחסה לה רגישות כה גבוהה לפני עידן ההיי-טק?

הפחד מהיכולת שקיימת בידי גורם זר עוין לארה"ב, או למדינה אחרת, או של כל אדם אחר בעל היכולת לשגר מסר מוצפן ברשת או דרך קווי טלפון, החל להוות בעיה אסטרטגית מהדרגה הראשונה. אז מה עושים? משחררים את היכולת להצפנה עסקית ברמה שרק לממשל תהיה היכולת לפענח - דבר שמאוד לא מצא חן בעיני העולם העסקי (אירופה המאוחדת).

מכאן המצב החל לפעול כ"חרב פיפיות" נגד האמריקאים. בשוק האזרחי החלו מתפתחות טכנולוגיות הצפנה אדירות, בעלות אורך מפתח של אלפי ועשרות אלפי ביטים. האמריקנים לא יכלו עוד לעצור את "המגפה החדשה" הקרויה מערכות הצפנה מסחריות, שהופיעו בשווקים בתוך ומחוץ לארה"ב.

אותה רשת ממש, שפרצה דרכה החוצה במטרה לסייע למערכות הביון בנגישות תקשורתית למידע אצל האויב, הפכה למערכת ריגול מסחרית יותר מאשר צבאית או מודיעינית.

מבהינה הביטחונית, החלה לשחק כנגדם כעת ולאויב הייתה היכולת לשגר אינפורמציה מוצפנת אל ומחוץ לארה"ב בלא שום יכולת מעקב. דמיינו לכם אדם, המועסק בגוף צבאי או ביטחוני, הנשלח מטעם האויב ומושתל שנים במדינה שבה הוא צריך לרגל.

מה הקושי להיכנס לאותו גוף שבו הוא מועסק, לצלם ולהוציא חומר רגיש - בין עם עליו או דרך דואר אלקטרוני - ומשם להיכנס לאינטרנט קפה ולשגר את החומר מוצפן לאויב? הסינים כבר רואים כיום את האיום הראשוני נגדם בתחום בתי הקפה, הספריות הציבוריות וקיוסקי המידע המספקים אינטרנט, והם נמצאים תחת מעקב של מחשבים למניעת ריגול בממשל וכמו כן כל ספקי האינטרנט ונותני שירותים אחרים נמצאים גם הם תחת פיקוח מיוחד של תוכן וגלישה.

Uינוי ענק חל בעולם האבטחה בעולם בשנתיים האחרונות ובעיקר בשנה האחרונה לאחר ה-11 בספטמבר. נוכחנו לדעת עד כמה חזקה הרשת כאשר היא בידי האויב. היכולת לנצלה נגדנו עוד תחזור בשנים הקרובות ותלמדנו מה חזקה היא היכולת של התקשורת כאשר אין דרך לעוצרה או לנטרה.

מאות מיליארדים של דולרים הושקעו בפרויקטים כגון "אשלוך" ו"קרניבור" במטרה למנוע את האסון עוד בטרם התרחשותו.

מיד לאחר מלחמת העולם השנייה התבקשו אנשי הצבא האמריקני ומחלקות הפיתוח, המחקר והאסטרטגיה המיוחדים לתת את הדעת על ה"אניגמה", מכונת ההצפנה שנמצאה בידי הגרמנים בני העולה ועשתה שמות בכוחות בעלות הברית (ראה ערך צוללת U-741). כאשר אין רשת תקשורת מיוחדת והמידע מהאויב אמור לזרום, עד כמה מסוכנת וכואבת היא אי היכולת לדעת מה היה באותו מידע. בעברית "מודיעין אלקטרוני שקט". האמריקנים נכנסו לתקופה של מלחמה קרה ופחד מריגול והתנקשות בנשיא והפחד הגדול מכולם - ההתפשטות האפשרית של הקומוניזם ב"ארץ החופש", כדברי ההימנון האמריקני, העביר אותם על דעתם. גם כך נחשב הקומוניזם שם כמחלה שיש לעוצרה בעודה באיבה.

בעקבות השתלשלות האירועים החלו אנשי הפיתוח והמחקר לשדרג את מערכת פענוח הצופן וההאזנה. כספים אדירים ללא שום פרופרציות הושקעו.

שרתי ענק מרובי מעבדים, מערכות זיכרון ניידות, מערכי על לאחסון לצורכי ניתוח, בניית צומתי האזנה לרשתות הטלפונים, לווייני ריגול, צמתים אוטומטיים, מערכות רב תדר, כמעט כל אמצעי שנמצא על הכדור שלנו - ניתנה עליו הדעת.

שנים רבות נשמרה הרשת כסוד צבאי מסווג ביותר, מערכות שהגישה אליהן נעשתה רק ליודעי עניין. גם כיום עדיין יש הכחשה כוללת מהסינים בארה"ב ובאירופה לגבי קיום הפרויקט.

שנים לאחר סוף המלחמה הקרה הוסבה הרשת לצורכי אקדמיה וכאן נשאלת השאלה, האם בכזאת קלות דעת שחררו האמריקנים וה-ARPANET את הרשת לשימוש אזרחי ועוד שיתפו אותה עם העולם כולו ללא כל תמורה?

אז מה באמת קרה שם ?

"חרב פיפיות"

האמריקנים חששו לאחר תום המלחמה הקרה, כי המהפכה בברית המועצות עלולה, כמו גם בכל מקום אחר בעולם, לפתח משטרים מסוכנים לאמריקה ולעולם החופשי. ארצות הברית הבינה, שעולם התקשורת עלול להיות מסוכן גם מחוץ לגבולותיה של ארה"ב ולא רק מבפנים. כמו כל הפראנאוואידים הסטנדרטיים הבינו האמריקנים, כי יכולות ההאזנה מחוץ לגבולות החממה האמריקנית הן בעייתיות מאוד.

* רואי כהן הוא מומחה לאבטחת מידע, לטרוור קיברנטי ולריגול עסקי. חברת קוונטום סיסטמס, email: q@quantom.tk



"סטגונורפיה"

היכולת לבצע הצפנה של חומר מכל סוג והסתרתו בתמונה או קובץ קול. כן! הרוסים! זהו את הבעייתיות של חומר מוצפן במדיה אלקטרונית בסוף תקופת המלחמה הקרה, אך היעילות הרוסית בתקופת ברית המועצות פתרה ביעילות מרבית את בעיית חומרי בלתי קריא לעין על ידי הוצאה להורג בלא משפט בכיכר העיר הקרובה לבייתך. כן, שיטה יעילה וחשכונית, ואין צורך לבזבז משאבים כספיים על מחשבים רבי עוצמה לפענוח צפנים.

המחותרת וגופים דמוקרטיים שפעילותם נאסרה, החלו לפתח טכנולוגיות מקוריות מדהימות להצפנת מידע, למשל בתמונה: אדם רצה להעביר מידע לגורם עוין לממשל. בעזרת הטמעה בין צבע גוון ואור בנו מערכת המרה ממידע טקסטואלי למידע מוצפן ולמידע המוטמע בבר קוד גרפי בין אותם פיקסלים של תמונה סטנדרטית שלא מעלה שום חשד. כך, אם נבדקה על ידי גורם ממשלתי, היא נמצאה כשרה לחלוטין, אך היעד המקבל ידע שמידע רגיש אמור להגיע אליו, ובעזרת סיסמה מוסכמת מראש נחשפה האינפורמציה לאותו גורם והמסר הועבר. התוצאה: יעילות וחסיון מוחלט. האמריקנים התלהבו מאוד מהרעיון וציידו את המרגלים של ה-CIA באותה טכנולוגיה ממש. וכך העבירו ממדינות אויב ללא כל בעיה את המידע המודיעיני בחזרה לארה"ב דרך אתרים שונים ומשונים.

אבד הכל על הצורך בשימוש בטכנולוגיות ריגול ישנות כמו מורס, או שימוש במערכי קשר חדישים מוצפנים, שמי שיחפש אותם עלול לאתר אותם שהיו בעייתיים, כי קל היה להאזין להם, כי אין הרבה שידורים כאלה - "כשאין הרבה רעש אז קל לשמוע את המקור". לראיה, פרשת אלי כהן וכיצד נתפס לאחר שהרוסים סיפקו לסורים מכשירי מעקב חדישים, שבעזרתם האזינו, איתרו וזיהו אותו בזמן השידור. כיום ללא כהן זה לא היה קורה!!!

בימים אלה ממש, לפני שנה, ב-11 בספטמבר, ספג עולם הביון מכה שבקרוב תביא למותו. במצבו הנוכחי כיום, אותו גוף עוין שפגע ב-11 בספטמבר, שלמד וחקר את יכולות הרשת וניצל לטובתו את הידע, את רשת האינטרנט ואת אותה טכנולוגיית החבאת מידע בתמונות כדי לחקור, לתכנן ולהוציא לפועל את פיגוע הטרור הגדול ביותר בהיסטוריה, אותו פיגוע ממש שבמשך שנים ניסו האמריקנים עם מערכות הביון שלהם ובהשקעות עתק למנוע, כשל והוכח כחסר כל סיכוי למניעה. כל זאת עקב בעיה אחת, שהינה במקורה אסטרטגית ולא טכנולוגית. כאשר אתה נמצא במצב של מגננה מתמדת, זה רק עניין של זמן עד שתבוא המכה, אין ולא יהיה שום סיכוי לעצור את כל הסיכונים, וכל אותם אירועים שהצליחו לסכל - לעולם לא נדע עליהם!

בעקבות זאת ייתכנו שני תסריטים אפשריים בקשר להשקעה כספית באותם מערכות ביון אלקטרוניות:

לא נראה שישקיעו פי עשרה יותר כספים במערכות ניטור אלקטרוניות, מכיוון שמכה נוספת היום היא מחוץ לחשבון מבחינת האמריקנים.

או, יוקצה נתח נכבד מאוד מאותם תקציבי ענק למתן פתרון אנושי, כגון ניתור, בדיקות אחרי גורמים בסיכון גבוה ומעקבים.

היום, דור חדש של בעיות מתפתח ואין שום דרך לתת עליו את הדעת. "הכח השקט" - אותם האקרים המפתחים טכנולוגיות אדירות עוצמה, ששום חברת הגנה או מוצר הגנה לא יכול להגן ואנו רואים זאת יותר ויותר. בכל יום מתבצעות אלפי תקיפות של תשתיות ממוחשבות על ידי האקרים, בטכנולוגיה שאינה מוכרת לצבא או למערכות אכיפת החוק. אין ולא מסתמן שום מענה. חברות האבטחה לא עמדו במשימתן להגן על האתרים. מערכות שיווקיות הבטיחו לתת לנו מענה נגד אותם פורצים כשבפועל לא הייתה להם דרך טכנולוגית מקורית למניעת אותן פריצות, ואנו האמנו והמשכנו לרכוש תוכנות הגנה ושוב נפרצנו. כל המקוריות בנושא הזה הגיעה מאותם האקרים, שפיתחו דרכים גאוניות לגרימת הרס בזדון.

נקודה למחשבה: היום, ברגע זה ממש, כל כך הרבה מידע אלקטרוני זורם אלינו "בעורקי ונימי" התקשורת, מה הסיכויים למצוא את אותו גורם עוין באותן מיליארדי חבילות המידע?

מכאן, שהאבטחה היא רק הבטחה... □

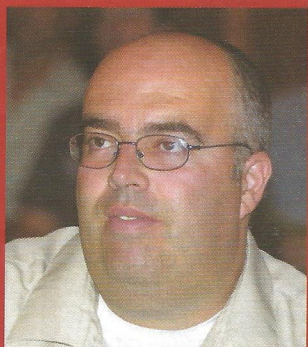


אבטחת מידע:

מגורם עלות לגורם המאפשר פעילות עסקית

1000 מנהלי אבטחת מידע ומקצוענים אחרים גדשו במשך יום שלם את אולמות המליאה של דן פנורמה. הם האזינו בקשב רב לסדרה של טובי המרצים בענף, שהאיר, כל אחד בתורו, זווית אחרת בתחום החם ביותר כיום. כל הדוברים הסכימו, שאבטחת מידע אינה נכללת עוד בסעיף ההוצאות של החברות, אלא היא חלק מהמערכת התפעולית ברמת קריטיות גבוהה ביותר

יוסי המוני



בוני דולב, ממשלה. זהות דיגיטלית לכל אזרח



ירון אוחנה, יבמ ישראל. TIVOLI בשלוש רמות

מול משרדי הממשלה השונים, חשבונות אלקטרוניות חתומות ועוד.

לגבי טרור קיברנטי, אמר דולב כי פרויקט תהלי"ה הוא אחד מהמותקפים ביותר במדינה, הן על ידי אזרחי המדינה, והן על ידי זרים העוברים את ישראל. "אנו מותקפים עשרות פעמים ביום", אמר והוסיף, כי אתר המוסד מותקף ללא הרף, בעיקר על ידי האקרים ישראלים.

מבחינת ההיערכות להתקפות, אמר דולב, שנבדקים כל מיני תרחישים, ביניהם שילוב של התקפות על מערכי המחשוב הממשלתיים, במקביל להתקפות פיזיות. לגבי איתור התוקפים אמר דולב, כי האקרים נוטים להתפאר במעשיהם באינטרנט וכי הם עוקבים אחריהם ונעזרים במידע המופץ על ידי ההאקרים עצמם.

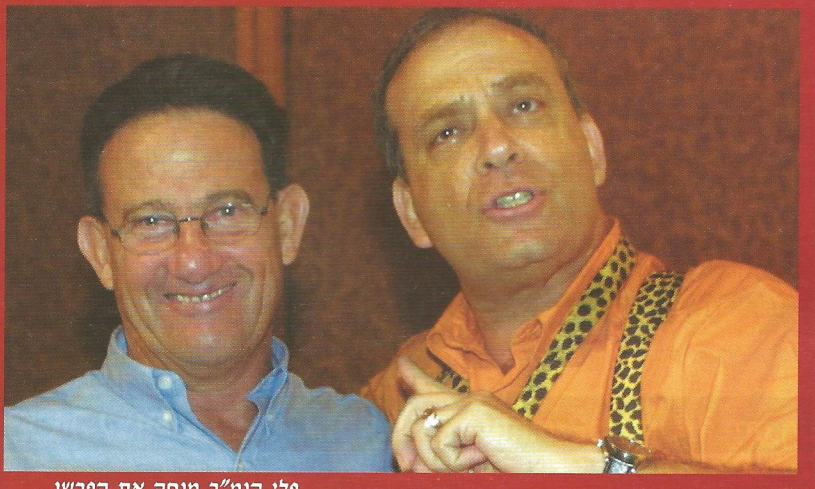
הוא ציין כי בשל השימוש בשפות מקומיות, עברית וערבית, יש קושי לעקוב אחר התוקפים. כדי למנוע התקפות אלה, ציין דולב כי דרוש שיתוף פעולה בין

על אלף משתתפים הגיעו לכנס אבטחת המידע CISO 2002, שנערך בחסות אנשים ומחשבים במלון דן פנורמה בתל אביב לפני שבועיים. את הכנס הנחו פלי הנמר ויהודה קונפורטס, עורך "InformationWeek".

ראשון הדוברים היה בוני דולב, מנהל פרויקט תהלי"ה באגף החשב הכללי במשרד האוצר. הוא תיאר את פתרון הממשלה לקישור מערכות מידע רגישות לאינטרנט. לדברי דולב, משימותיו של מנהל אבטחת המידע בארגון הן מגוונות: לחשוף את המידע הארגוני כלפי העולם החיצוני, ומנגד, לשמור עליו; להריץ פרויקטים קדימה, ובמקביל, לשמור על המידע. לשאלה "מהו מנגנון הקסמים שיחבר את מחשבי הארגון לרשת ללא חשש", ענה דולב שאין פתרון כזה, אלא שיש כמה שיטות לחיבור מאגרי מידע והציג את הדרך שבה הממשלה עושה זאת מול האזרחים.

האמצעים להזדהות של האזרחים ובתי העסק מול מערכות המיחשוב הממשלתיות יהיו כרטיסים חכמים וחתימה אלקטרונית, אמר דולב. הוא ציין, כי פרויקט זה מצוי בשלב בדיקת מכרז, כאשר ברבעון השני של 2003 יונפקו תעודות הזהות הראשונות. כך יוכלו 500,000 אזרחים לחתום ולהזדהות באופן דיגיטלי, ולקבל מידע אישי מקוון. בדצמבר השנה ייצא המכרז לגורמים מאשרים, שינפיקו תעודות זהות, וכן תעודות לעובדי הממשלה. בתחילת 2003 יוקם Directory מרכזי, שמולו יאומתו תעודות הזהות הדיגיטליות.

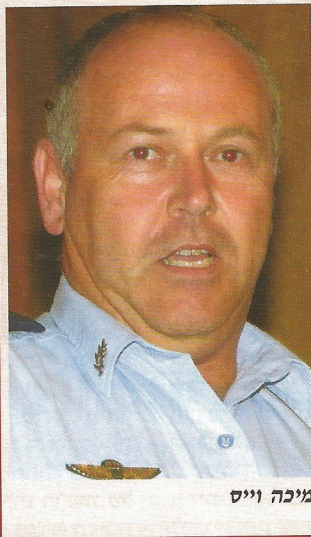
משמעות הפרויקטים היא, שלכל אזרח תהיה זהות דיגיטלית, וכך הוא יוכל לעבוד באופן מקוון מול משרדי הממשלה השונים ומאגרי המידע שלהם, הסביר דולב. כך יוקם, בין השאר, שירות טפסים, ובו יהיה פורטל מרכזי, וניתן יהיה לאתר בו את כל סוגי הטפסים הממשלתיים הקיימים, להזמין ולמלאם. פרויקט נוסף אותו ציין דולב הוא "כיספת": לכל אזרח תהיה אפשרות לפנות למשרדי הממשלה, לבקש ולקבל מידע אישי, ואישורים שונים, אשר יימסרו לתיבת דואר אלקטרונית, אישית ומאובטחת. הוא יוכל לקבל מידע מגוון, כגון מצב ההתחשבות שלו



פלי הנמר מנחה את הפרשן הצבאי רון בן ישי, המרצה האורח במליאת אחר הצהריים

סגן אלוף מיכה וייס, ראש ענף ביטחון מערכות מיחשוב במחלקת ביטחון שדה בצה"ל:

שת"פ מנצה לאבטחת מידע בצה"ל

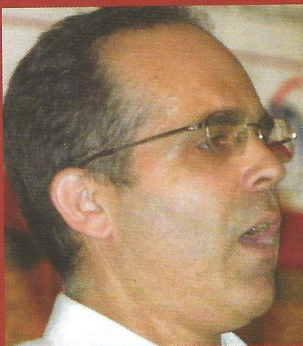


מיכה וייס

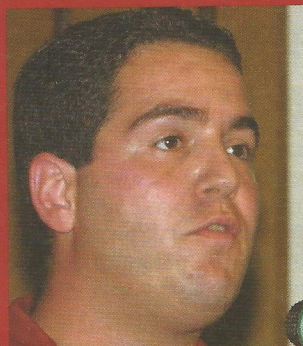
סגן אלוף מיכה וייס, ראש ענף ביטחון מערכות מיחשוב במחלקת ביטחון שדה בצה"ל, דיבר על אבטחת מידע במחשבי צה"ל. הוא אמר, כי קיים שיתוף פעולה הדוק בין גופי הביטחון השונים, הצבא והתעשייה, לבין גופים מסחריים, לקידום תחום אבטחת המידע, וכי שיתוף פעולה זה חשוב הן בהיבט הפיתוח והן בהיבט הייעוץ.

"בצה"ל יש אלפי חיילים המטפלים בתחום אבטחת המידע, תוך קבלת הנחיות מגורמי הביטחון במחלקת ביטחון שדה, והגורמים המקצועיים במקשר"ר ובחטיבת התקשורת", אמר וייס, והוסיף כי לשטח מסופקים אבני בניין להגנה על מערכות המידע בשלל תחומים: הגנה לוגית, הגנה פיזית, מהימנות, חסינות - הכוללת זמינות, סודיות ואמינות - ותחומים נוספים, כגון ניטור ושליטה ובקרה.

"המדובר בתהליך מתמשך, בעל אופי מעגלי, כאשר כל הזמן נבדקים סדרי העדיפויות, הסיכונים והסיכויים, ואבני הבניין הנגזרות מהם", ציין וייס, ואמר כי הצבא מתמודד באופן רציני עם עברייני מחשב. סגן אלוף וייס סיכם: "צה"ל ויחידותיו נערכים לשלל האיומים בצורה טובה, במסגרת המשאבים העומדים לרשותו".



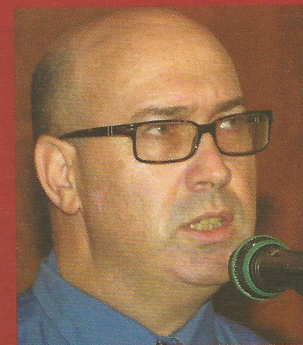
גלעד ירון, CA. גישה חדשה באבטחת מידע



יובל שחורי, א.מת. מיחשוב. החוליה החלשה



רואי כהן, יועץ ללוחמה אלקטרונית. כל הפריצות, כל השיטות. הכל פרוץ!



איל אדר, ITcon. כניסה לתחומים חדשים

לתחומים שטרם טופלו קודם", ציין אדר והוסיף כי כיום, בניגוד לבעבר, יש דרישה שמנהלי אבטחת מידע יטפלו בתחומי שרידות, זמינות, אמינות והמשכיות עסקית. הוא הדגיש, כי כיום, על מנהל אבטחת המידע להבין את התהליכים העסקיים ואת זרימת המידע הרלוונטית לביצועם. "ככל שהעולם פחות ברור, עם איומים רבים יותר - אנשי אבטחת המידע צריכים להבין יותר, לעסוק ביותר תחומים ולהיות עם ראש גדול יותר", סיכם אדר, "עולם האיומים השתנה, ותפיסת אבטחת המידע השתנתה גם היא ודורשת הסתכלות רחבה יותר". לדבריו, גורם אבטחת המידע בארגון הופך מגורם עליון לגורם המאפשר פעילות עסקית.

מרחב עצים

סול צבי, מנהלת תחום אבטחת מידע ו-Privacy במיקרוסופט, הציגה את תפיסתה לנושא אבטחת מידע. בשל ריבוי מוצרי אבטחת מידע, הארגון נותר ללא מידע. "כמה פעמים ראינו ארגון הדומה לשולחן המחובר לעשרים רגלים, עם שרטוט אבטחת מידע מסובך ומלא קווים!", שאלה צבי והוסיפה, כי ניתן לקיים אבטחת מידע בארגון בצורה חכמה, ללא סיבוך וברמה גבוהה יותר.

אריאל פיסצקי, מנהל אבטחת מידע בנטוויזן, דיבר על הדור הבא של הסוסים הטרויאניים. לדבריו, מטרת הסוס הטרויאני הוא החדרת סוכן למערכת המיחשוב בארגון ללא הרשאה, על מנת להשתלט, לגנוב מידע, או לנצל את עוצמת ה-CPU. העלמת החדירה חשובה, בשל יכולת האנטי וירוס לזהות חדירה עוינת.

לגבי דרכי החדירה, הזכיר פיסצקי את הדוא"ל, המחשב, וכן החדירה הפיזית לארגון. לגבי התגוננות, אמר פיסצקי, כי יש לחסום קבלת פרטי דואר מסוכנים, לעדכן את תוכנת האנטי וירוס ולמנוע התקשרות ישירה מחוץ לארגון. הוא ציין כי הדור החדש של סוסים טרויאניים מופץ באמצעות CD, המפעיל את המחשב עם מערכת הפעלה עצמית. "מיגון מלא דורש הרבה הקפדה על נוהלים", סיכם פיסצקי.

(המשך בעמ' 44)

ספקי האינטרנט והמדינות. הוא סיים את הרצאתו בציטוט של אנשי החיובאללה, המודים לאנשי תהליכה על שיהם מגינים על מערך המיחשוב הציוני".

סכנות מעורבות

דורון דרייר, מנכ"ל Network Associates ישראל, הרצה על התגוננות של ארגונים מפני סכנות מעורבות. "התקפות קורות, לא כולן מגיעות לתקשורת, ולמרות זאת, ארגונים נפגעים מדי יום בשל וירוסים", פתח דרייר את דבריו, "בפועל, הנוקים הגדולים מקורם בוירוסים ולא מהאקרים". המאפיין את הווירוסים כיום, אמר דרייר, הוא קיצור משך זמן ההתפשטות שלהם, מ-12 שעות לפני שנה לשש כיום. מאפיין נוסף הוא כמותם: הווירוס הראשון הופיע ב-86', שלוש שנים אחר כך הן 60 שישיה, ב-90' היו שמונים וירוסים וכיום יש כ-100 וירוסים ידועים.

לגבי מוקדי חדירת הווירוסים, אמר דרייר כי עם התפשטות השימוש בדוא"ל, עלתה כמות הווירוסים החדורים דרכו. אחת הדרכים הפופולריות להדבקות היא גלישה תמימה לאתרים נגועים: "הווירוסים שקטים וקטלניים. הם חודרים למערכת ומשתלטים עליה כמו סרטן", אמר דרייר, וציין כללי ברזל לבניית הגנה מפני איומים מורכבים: הגנה על כל רמות הרשת; ביצוע סקר סיכונים ספציפי לסכנות וירוסים; התקנת אנטי וירוס בכל רמה ברשת; כתיבת נוהלי טיפול במערכת במקרי חירום; חינוך המשתמשים לשימוש נכון ובטוח בדוא"ל; שמירה על עדכניות מרכיבי האנטי וירוס בארגון; ניהול מנקודה מרכזית אחת; הפקת דו"חות שבועיים על איכות ההגנה וההתפרצויות; אכיפת מדיניות האנטי וירוס על כל מחשבי הארגון. "אין 100 אחוזים אבטחת מידע, אלא שיש לשאוף לכך", סיכם.

שואלים יותר שאלות

איל אדר, מנכ"ל ITcon, דיבר על שינוי כיוון ותפיסה לתחום אבטחת המידע, בעקבות ה-11 בספטמבר. לדבריו, כיום מנהל אבטחת המידע בארגון נשאל יותר שאלות על ידי עובדי הארגון ומנהליו. "ההיבט המשמעותי הוא, שאבטחת המידע נכנסת

אבטחה כלל פלטפורמית

שרון בסר, מנהל מוצר בצ'ק פוינט, דיבר על הדור הבא בהגנה אקטיבית. לדבריו, הדרישות מצד הלקוחות הן לקבל מערכת הגנה שתטפל בשרתים, בלקוחות ובתוכן, ושתוכל לבצע אינטגרציה עם מערכות נוספות. "גישתנו היא להתמודד עם הבעיות של כולם ובנוסף, עם הבעיות הלא ידועות", אמר בסר.

לדבריו, צריך להיות מערך אבטחתי כולל, שניתן להתקינו על גבי כל הפלטפורמות, שיאופיין בכמה היבטים: יכולת לבצע חסימת התקפות, להגיב עליהן בזמן אמת ולהתריע מפניהן; ניהול מרכזי של כל הרכיבים הקריטיים לאבטחת המידע; אכיפת מדיניות האבטחה; והיכולת לבצע פעולות בזמן אמיתי.

ירון אוהנה, מנהל מוצר Tivoli יבמ ישראל, תיאר את תפיסת טיבולי בסביבת האבטחה ואת האסטרטגיה שלה לניהול אבטחת מידע במערך המיחשוב בארגון. לדבריו, הפתרון לניהול כולל מתבצע בשלוש הרמות של מערך המיחשוב של הארגון, כך שלבסוף נוצרת תפיסת אבטחה כוללת, כאשר כל המוצרים עובדים מנקודת שליטה מרכזית אחת.

יובל שחורי מספידר פתרונות מקבוצת א.מ.ת. מיחשוב, דיבר על האפליקציה כחוליה החלשה במערך המיחשוב, בהיבט אבטחת מידע. לדבריו, האיומים על האפליקציה לא נגמרים בווב, והמחשבה ש"יש לי פיירוול" לא תמיד מסייעת. ההגנה על האפליקציה, לדברי שחורי, צריכה לכלול: כתיבת קוד נכון ולא פגיע על ידי אנשי הפיתוח; הקשחת האפליקציות ומערכות ההפעלה; וכן ביצוע בחינת חדירה לפני עליית המערכת לאוויר.

ניהול הגישה

גלעד ירון CA-מ ישראל דיבר על גישה חדשה לאבטחת גישה. לדברי ירון, ניהול גישה הוא היכולת לאפשר למשתמשים תוכניות או תהליכים מורשים בלבד לגשת למשאבי המערכות. ניהול הגישה צריך להתחשב בכך, שמערכות ההפעלה אינן מושלמות, כל העולם נמצא ברשת וברשת יש חורים. לדבריו, הפירוול הוא תנאי הכרחי אך לא מספיק. "צריך להסתכל על כל רכיבי המערכת ולתת פתרון טכנולוגי, המזהה את כל האיומים בארגון טרם התגלתה הפריצה, כאשר אם מישחו מנסה לפרוץ אז יש לתפוס אותו בזמן אמת", אמר.

אבנר מיימון, סמנכ"ל מכירות ITC, שותף עסקי של סימנטק, דיבר על הערכת הפגיעות של מערך המיחשוב של הארגון, והסיכונים והאיומים הנובעים מכך. לדבריו, התהליך כולל חיפוש אחר חולשות קיימות במערכת ההפעלה, הערכת החומרה, הגדרת האויב והמוטיבציה שלו, הערכת הסבירות לפגיעה והגדרת הדרך המהירה לביצוע אבטחת המידע בצורה המהירה ביותר. "המדובר בתהליך זיהוי פגיעות, שיש בו מחזוריות", סיכם מיימון.

ליאור גולדברג, מהנדס מערכות בסיסקו ישראל, דיבר על הבעיות שיש למערך המיחשוב של ארגון כאשר הארגון נפתח לספקים וללקוחות ועובדיו עובדים מהבית או מחו"ל. בעיה נוספת שאותה ציין גולדברג היא הקלות שבה ניתן לפרוץ כיום למחשבי הארגון.

"צריך פתרונות שייצרו מנגנון אבטחת מידע אמיתי לכל מרכיבי הרשת", סיכם, "ולכן חייבים להכניס היבטי אבטחת מידע לכל מוצר במערכת".

שליש מהדואר רגיש

מיכאל בסין הוא מנהל התמיכה הטכנית ברנסאנס. לדבריו, נושא אבטחת המידע בדואר האלקטרוני לא היה מובנה. "כשליש מדברי הדוא"ל כוללים מידע רגיש", הזהיר בסין וציין, כי צפי שעד שנת 2004 כמות המסרים שתעבור בינם תהיה ארבעה מיליארד. לדבריו, כשהדואר נשלח הוא עובר דרך כמה שרתים בדרך, ולכל אדם יש יכולת להתחבר לקו בנקודה כלשהי. הפתרון לדבריו, הוא הצפנת הדוא"ל

ירון בלכמן, מנהל בפרייסוטר האוס קופרס דיבר על הצורך בניהול זיהוי, ועל הדרכים שיש לעשות זאת, בצורה שתועיל למערך המיחשובי של הארגון בעבודתו מול גורמי חוץ, כגון לקוחות וספקים, ובעבודה מול גורמי פנים - משתמשי הארגון.

העיתונאי **רון בן-ישי** דיבר על אבטחה וביטחון במזרח התיכון, בעידן ארגון אל-קעידה מצד אחד, וערב המתקפה האמריקנית על עיראק מצד שני.

רואי כהן, מומחה ללוחמה אלקטרונית, הציג טכנולוגיות ודרכי לוחמה אלקטרונית, מתודולוגיות באבטחת מידע וטכניקות פריצה עתידיות. □

גיליון הבא: מאמר מורחב המבוסס על הרצאת רואי כהן.



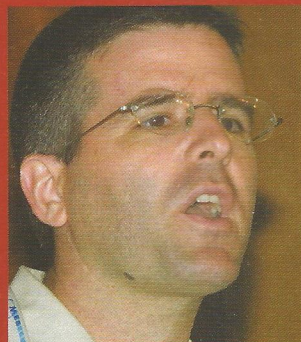
רון בן-ישי. מקורות אבטחה וביטחון במזרח התיכון



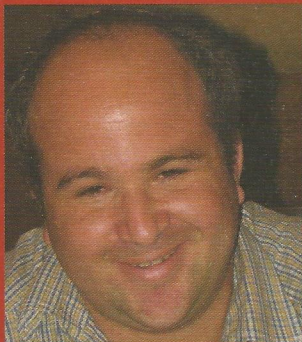
סול צבי, מיקרוסופט. בלבול בארגונים



אריאל פיסעקי, נטויז'ן. הדור הבא של הסוסים הטרויאניים



שרון בסר, צ'ק פוינט. הגנה אקטיבית, הדור הבא



דורון דריר, נטוורק אסוסיאטס. כל יום פגיעה מווירוסים



מיכאל בסין, רנסאנס. 4 מיליארדים מסרים עד 2004

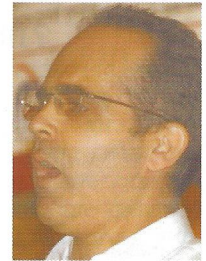


ירון בלכמן, PWC. ניהול הזיהוי - חובה בכל ארגון

מיקרוסופט תמשיך לבחון את הגדרות ברירת המחדל של מוצרים אשר ייצאו לשוק במהלך השנה, ותגביר את האבטחה ביישום באמצעות יצירת מוצרי אבטחת מידע חדשים. "מיחשוב אמין, הכולל בתוכו את המרכיב החשוב של אבטחת מידע, הוא תהליך ארוך", סיכמה צבי.

בקרת שינויים באבטחה

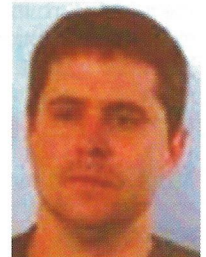
יובל שחורי, ספיידר פתרונות, קבוצת א.מ.ת. מיחשוב, דיבר על מערכות בקרת שינויים במערכות אבטחת מידע. לדבריו, אחת הבעיות הקשות שהם מזהים אצל מנהלי אבטחת מידע היא חוסר היכולת לדעת מה קורה בכל רגע בארגון. "מערכות אבטחת המידע בארגונים הן מורכבות ומבוזרות", אמר, "וקיים תמיד הסיכוי כי מישו מהמשתמשים יעשה שינוי כלשהו בזמן נתון". לפיכך, לדבריו, תפקידו של מנהל אבטחת המידע הוא לדעת אילו שינויים נעשו, בדרך של בקרה שוטפת. הוא דימה את המצב ל"תבשיל אחד - טבחים רבים". הפתרון, לדברי שחורי, הוא מערכת בקרת שינויים, שמפקחת בכל רגע על שינוי המבוצע במערכת, כדי לשמור על מדיניות אבטחת המידע בארגון.



גלעד ירון, סמנכ"ל אבטחת מידע, CA

כולם עולים על הווב

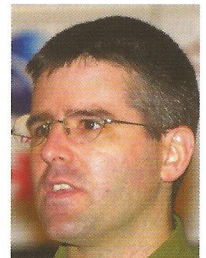
גלעד ירון, סמנכ"ל אבטחת מידע, CA, אמר כי "כולם עולים על הווב. היום כל יישום, החל מחנות מכולת, דרך אתרי תדמית ועד לאתרים המספקים שירות. בנוסף, גם אפליקציות תוך ארגוניות הופכות לווביות". לפיכך, לדברי ירון, מנהל אבטחת המידע בארגון צריך לדאוג שהשירותים המסופקים יהיו מאובטחים, ושחלוקת ההרשאות מיושמת בפועל. הוא ציין כי E TrustWeb Access Control מכיל 19 רכיבים טכנולוגיים, המשלימים זה את זה, ומאפשרים לבנות ארכיטקטורת אבטחת מידע המתאימה לצרכי העסקים של הארגון. "ניהול מרכזי הוא חיוני ולכן הוא חשוב", סיכם ירון.



זמיר סיון, מנהל טכני, פיניזלבר מערכות

אבטחה בדואר אלקטרוני

זמיר סיון, מנהל טכני, פיניזלבר מערכות, דיבר על החשיבות הקריטית של אבטחת תוכן בדוא"ל ליעילות מערכת אבטחת המידע בארגון. "יש הרבה מידע שיכול מצד אחד לדלוף מהארגון, מבלי שמנהל אבטחת המידע יידע על כך. מצד שני, תיתכן כניסת חומרים בלתי רצויים, כגון חומרים פורנוגרפיים, תוכנות משחקים, ודואר זבל". הפתרון, לדברי סיון, הוא iQ Mail Marshal Net, היושב בשער הארגון ומבצע סינון תוכן. לדברי סיון, הגדרות הסינון נקבעות על ידי מנהל ה-IT בארגון, או מנהל אבטחת המידע.



רון בר, מנהל אבטחת מידע, צ'ק פוינט

הגנה על הבלתי ידוע

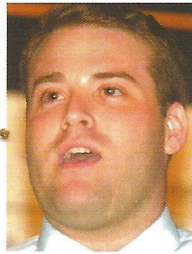
רון בר, מנהל אבטחת מידע, צ'ק פוינט, אמר כי הרעיון הוא לספק הגנה מול הבלתי ידוע. "על מנת שהתקפה תהיה מוצלחת, היא צריכה לנצל סוג של פגיעות. ההגנה נגד פגיעות ידועות קשה, והגנה מפני פוגעים בלתי ידועים קשה עוד יותר", אמר בר, "הפירוול הוא הבסיס, ולצדו אנתוז חיים בסביבת פתרונות משלמים". הוא הוסיף כי יתרונן של הפירוול הוא ביכולתו להגיב מהר, אפילו עוד בטרם קרה משהו. "דרך אינפורמציה ברמת הרשת, אנתוז מסוגלים להחליט החלטות ברמה גבוהה יותר".



חנניה כפרי, מנהל תחום אבטחת מידע, בנק לאומי

מנהל בלתי תלוי

חנניה כפרי, מנהל תחום אבטחת מידע, בנק לאומי, דיבר על דמותו של מנהל אבטחת מידע בארגון. הוא אמר שחשוב מאוד שיחידת אבטחת המידע בארגון תהיה בלתי תלויה. "בכל התהליכים הארגוניים, ניהול אבטחת מידע יוצר קונפליקטים ומתחרה על תקציבים ומשאבי אנוש". מצד אחד עומד מנהל ה-IT, הרוצה לסיים את הפרויקט, ומנגד - מנהל אבטחת המידע, הרוצה עוד ביטחון. עוד הוסיף כפרי, כי נחוץ שלמנהל אבטחת המידע יהיה גיבוי מההנהלה, ושהוא יעבוד בשיתוף פעולה עם שאר מנהלי המחלקות בארגון. הוא סיכם באומרו שיש להיערך להתקפות מראש על ידי בניית תרחישים שונים, להיות מוכנים עם הכלים, להתמודד עם אירוע אבטחת מידע, ולהכיר היטב את המערכת.



אריאל פיסצקי, מנהל אבטחת מידע, נטוויז'ן



ירון אוחנה, מנהל מוצר Tivoli, יבמ ישראל



דביר גורן, מנהל טכנולוגיות ומומחה NetIO, כלנית & כרמון מוצרים

פתרונות ל-DoS

אריאל פיסצקי, מנהל אבטחת מידע, נטוויז'ן, דיבר על פתרונות ממשיים ל-DoS. לדבריו, התקפות אלה הפכו להיות ממשיות בחודשים האחרונים. "המדובר בפעילות של גורם זדוני, הרוצה להשבית את מערכת המחשב שלי, באפליקציה, או באתר, אם בהתקפה עתירת תקשורת ואם בהתקפה על נקודת תורפה במחשב", הגדיר פיסצקי, וציין כי כיום ניתן לפגוע בכמה חלקים במערכת: בתשתית המפעיל, תשתית הספק, באפליקציות שונות ובאתר עצמו. המניע של התוקף, לדבריו, הוא פשטות ההתקפה, העדר הצורך במשאבים מיוחדים והידיעה כי ההתקפה תביא לפרסומו. הוא הוסיף כי בעולם האינטרנט יש תחושה של העדר פלגיות בעת ביצוע פעולות לא חוקיות, לעומת העולם הפיזי. הוא סיכם: "יש צורך במנגנונים מתקדמים לזיהוי התקפות DoS, שאינם נשענים על מוסכמות מהעבר, כגון זיהוי חתימה, יש מספר גדול של אלמנטים סטטיסטיים, שמשנתנים בעת התקפה, ניתן לאתרם ובכך לעצור את התעבורה המיותרת".

גורם מעכב?

ירון אוחנה, מנהל מוצר Tivoli, יבמ ישראל, דיבר על ניהול זיהוי וניהול אבטחת מידע בעזרת המוצר. הוא ציטט את חברת המחקר "מטה גרופ", שלפיה, אבטחת מידע בארגונים רבים נתפסת כגורם מעכב בדרך של הארגונים לעשות עסקים, ולא כגורם המסייע לארגון מבחינה עסקית. "אבטחת מידע צריכה לאפשר לנו לייצל את הארגון, להרוויח יותר כסף", אמר אוחנה, "היא חייבת להחזיר את ההשקעה במהירות".

המשימה: ייעול המערכת

דביר גורן, מנהל טכנולוגיות ומומחה NetIO, כלנית & כרמון מוצרים, דיבר על ניהול מרכזי של מערכות אבטחת מידע בעזרת המוצר. לדבריו, על אבטחת המידע מוטל תפקיד חשוב, של ייעול המערכת ופישוט תהליכיו של הארגון, ולא עיכובם. הוא הוסיף כי למרות הקיצוץ בתקציבי ה-IT, המודעות לנושא אבטחת המידע עלתה, ויחד איתה גדלה חשיבות הניהול המרכזי של מערכות אבטחת מידע. "המוצר עושה ניהול תוכן וסינון תוכן בצורה מהירה ויעילה, על פי המדיניות הנקבעת והגדרות הנגזרות ממנה, של מנהל אבטחת מידע, או מנהל ה-IT בארגון".

הדור הבא

אילאב לוי, מנהל טכנולוגיות, קבוצת קומסק, דיבר על הדור הבא

סיפורים מהזבל - פרק ב'

גלעד ירון *

נמען יקר שלום,

אני פונה אליך באופן סודי ובלעדי. המידע שאני עומד לחשוף לפניך במכתב זה הינו רגיש ביותר. אני סומך אל אמונך ומצפה לתגובתך ההולמת.

רק לפני שבוע כתבתי לך כאן בטור זה וסיפרתי לך על נפלאות דואר הזבל המשמש חזית מודרנית לתעשיית האשליות וממפה אותך לכל מנעמי העולם - מכסף, אושר, עושר ועד כושר בלתי מוגבל.

לא עברה שעה מפרסום הטור (עברו יומיים) ולהפתעתי הלא רבה מצאתי בתיבת הדואר האדומה שלי כמה דוגמאות קלאסיות לנושא זה. הרשה לי, אם כן, לשתף אותך (ואותך בלבד) בחוויה מרנינה זו ולהשלים את מה שכבר כתבתי בדוגמאות אחדות (כדבר לימור לשמעון - "לא ערכנו"). זיכרונות מאפריקה:

כותב אלי מר ניקו מוממבה מגאנה, העובד בחברת ביטוח גדולה. הוא קיבל מידע עלי מן היועץ המשפטי של החברה, חבר מאותו הכפר. הבחור אינו מכיר אותי אישית אך הוא סומך על חושי המחוודים והוא יודע שאפשר להאמין לי.

נכסים רבים שבעליהם אינם ידועים נמצאים בידי החברה. לפי מדיניות החברה, נכסים שבעליהם לא נודעו יותר מ-10 שנים יוצאים מהנחה כי הם מתים אלא אם כן סופקו להם מסמכים המעידים על בעליהם החוקיים של הנכסים. בידוי מסמכים המעידים על תיבה שבעליה הינו לוחם ותיק שנהרג במלחמת האזרחים. בתיבה אוצרות גלומים. כל מה שעלי לעשות הוא להעביר לאיש את פרטי האישיים והוא ידאג שאהיה בעליה של התיבה הקסומה!

עוד זיכרונות מאפריקה:

מכתב בו מסתובב באינטרנט יותר משנתיים - איני בטוח מה נפל בחלקי שזכיתי לקבלו עתה (ככל הנראה הטור שלי פופולארי ברחבי ניגריה). מר איו פרדריק, מנהל בכיר בחברת אחזקות בניגריה, פונה באופן אישי למנהל הבכיר בחברה (שוה, כידוע, אני). איש עסקים עירקני(!) בשם אחמד חסואמי הגיע לידידנו עם 25 מיליון דולרים וביקש ממנו להעביר סכום זה לארה"ב דרך ערוצים דיפלומטיים. האיש שכנע את העיראקי להפקיד את הסכום לתקופת ביניים בחברת האחזקות שלו. בדרכו לשדה התעופה הותקף האיש ונרצח. לאחר בדיקה מעמיקה הסתבר שלאיש אין כל קרוב משפחה. לאחר שנתיים של חיפושים קיבל איו מחבר המנהלים אורכה בת 21 יום לספק הוכחות מי הם קרובי משפחתו של המנוח. כל שעלי לעשות זה ליצור קשר עם ידידנו והאושר והעושר ייפול בחלקי. ממעיין הנעורים:

"ד"ר ג'ון ג'ונסון, נשיא האגודה הבינלאומית נגד הזדקנות, מציע לי באופן אישי ובלעדי תכשיר חדש שאינו רק עוצר את תהליך ההזדקנות, אלא אף מחזיר את הנעורים לבאים בימים כמוני. 40.2 אחוזים מלקוחות תכשיר הפלא הנ"ל חוו תופעות שלא תיאמנה, הכוללות צמיחה מחודשת של השיער, חזרת השיער לצבעו המקורי, העלמת הקמטים, שיפור ניכר בביצועים ההם, אובדן שומן, העלאת רמת האנרגיה, שיפור הזיכרון, האדרת הכוח, ובקיצור - מעיין הנעורים!

בגן הילדים שרנו במקלה: "פתי מאמין לכל דבר".

אגדות מקומון בספרי האגדות. מכתבי זבל מקומם בפה - אל תיפול אתה בפה במקומם!

שלך לעולם,

ידידך גלעד

* גלעד ירון, CISSP, מנהל תחום אבטחת מידע, CA ישראל, Gilad.yaron@ca.com

בתחום אבטחת המידע. לדבריו, בפני מנהלי אבטחת המידע עומדים אתגרים חדשים ואיומים חדשים, כאשר באופק מסתמנות שתי מגמות: האחת, SOC (Security Operation Center) - מרכז מבצעי לניהול אבטחת מידע. המגמה השנייה אותה זוהה לוי היא SIM (Security Incident Management) כלומר, היכולת לטפל באירוע אבטחת מידע בצורה ניהולית ומרוכזת, בזמן אמת.



שלמה טובול, מייסד ומנכ"ל פינג'אן

אבטחה אצל הגדולים בעולם

שלמה טובול, מייסד ומנכ"ל פינג'אן, סקר את לקוחותיו, שממנה עולה כי המדובר בלקוחות אסטרטגיים גדולים בעולם, כגון דיסני, קוקה קולה, צבא ארה"ב, הפנטגון, ה-CIA ובנקים של מדינות ברחבי העולם. "המדובר בארגונים בעלי ריסק גבוה מאוד, אלא שהם הפנימו שיש להם בעיה", אמר טובול. הוא בשנת 2000 תם עידן הדבקות וירוסים, והחל עידן וירוסים שאינם וירוסים, כי אם קוד נייד זדוני. המוצר של טובול מטפל בסוג וירוסים זה, קוד זדוני נייד, באופן גנרי.



יאטריס סירקיס, מנהלת פרייקטים לאבטחת מידע במחשבים ובתקשורת, בזק

ההיבט הפסיכולוגי

ביאטריס סירקיס, מנהלת פרייקטים לאבטחת מידע במחשבים ובתקשורת, בזק, דיברה על ההיבטים הפסיכולוגיים ביישום פרויקטי אבטחת מידע בארגונים. היא תדרכה את המאזינים כיצד להתמודד עם ההתנגדויות הצצות מתוך הארגון בעת יישום פרויקט אבטחת מידע.

כך, לדוגמה, התנגדות שכזו יכולה להגיע מכיוון מחלקת ה-IT בארגון. "המסר צריכים להעביר מנהלי אבטחת המידע בארגון לעובדים ולהנהלה הוא 'אנחנו לא שוטרים, אנחנו מנסים לשמור על הארגון. איננו נותנים הנחיות כי אם המלצות, כדי שכולנו נעבוד ביחד'. המסר הזה צריך לחלחל לעובדים ולהנהלה", סיכמה סירקיס.



רואי כהן, מומחה ללוחמה אלקטרונית באבטחת מידע, Quantom

הטכניקות החדשות

רואי כהן, מומחה ללוחמה אלקטרונית באבטחת מידע, Quantom, דיבר על "לוחמה אלקטרונית במיטבה". כהן הציג מגוון רחב של טכניקות מודרניות, שבהן משתמשים, ועלולים להשתמש, גורמים טרוריסטיים קיברנטיים, על מנת לתקוף אתרים של יחידים, ארגונים ומדינות, בעולם ה-IT. כהן ציין ופירט את האיומים השונים העומדים בפני אתרים ומערכות מיושבות ארגוניות בשל חשש מהתקפות שאלו.

סטארט-אפים במבחן

בפאנל מיוחד, שסיים את היום הארוך, עלה סטיב האנט לבמה, עם נציגי שש חברות סטרט-אפ ישראליות, העוסקות בתחום אבטחת מידע: Technology, Riverhead Networks, Kavado, Vidius, CyberArk, PineApp, B-Safe Software. כל אחד מהם דיבר על המוצר שלו במישור המכירתי. האנט שאל אותם שאלות מנקודת המבט של לקוח, בראיית אבטחת מידע.

המסר של האנט בדבריו היה כי כישלונן של החברות הישראליות בתחום אבטחת המידע הוא, שהן מפרטות יתר על המידה את ההיבטים הטכנולוגיים של המוצרים, ואינן מספקות מידע מספיק על הפתרון, כמסייע לארגון. "אני שאלתי פתרון, אתם עניתם לי טכנולוגיה", סיכם האנט. □

הכוח להשחית




רואי כהן

במאמר זה נביא מבט מעניין מאוד לגבי ההתפתחויות הטכנולוגיות שבאו לעולם בששת החודשים האחרונים, כאשר הדגש המיוחד הוא לזמינות הטכנולוגית והיכולת לרכוש את אותם כלים לביצוע טורר אלקטרוני על ידי האזרח הפשוט

רואי כהן *



הבה ניקח לדוגמה ארגון ציבורי גדול שלא נזכיר את שמו, שכל רשת המחשבים וכלי התקשורת שבו פועלים על רשתות אלחוטיות מסוג 802.11 WLAN בתדר 2.4 GHz, הנותן שירותים ליותר מ-3400 אזרחים בחיי היום יום בנושאים הרגישים והפרטיים ביותר שלהם. לכל המשתמשים ברשת רשום של ה-ID החומרתי שלהם וקיים אישור גישה למחשב על ידי ססמה ושם משתמש ובנוסף יש מערכת הצפנה בין העמדות לשרת. מדובר במחשבים שולחניים (מטרות ניחות), מחשבי



Q@QUANTOM.TK

Electrical Specifications		Mechanical Specifications	
Frequency	2400 - 2500 MHz	Weight	2.5g / 1.19g
Gain	15 DBi	Length	38 / 107cm
Impedance	50 ohm	Width	4 / 10cm
Max Input Power	100 Watts	Connector	N-Type Female
VSWR	< 1.5:1 avg	Polarization	Vertical & Horizontal

The [antenna] is a 15DBi highly directional antenna designed for applications needing long range point to point connections in the 2.4GHz ISM band. The [antenna] can be vertically or horizontally polarized.

(copyright 2002)

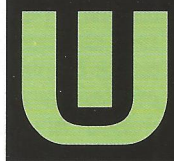
תמונה 1

כף יד ומחשבים ניידים (מטרות ניידות).

הכלים לביצוע ההתקפה:

- מערכת סריקת תדרים זעירה, המזהה את פעילות רשת WAN.
- 1 מחשב נייד
- 1 מחשב כף יד
- 1 סולר FIREWALL + תוכנת ניהול המגיעה איתו לשינוי תדרים.
- 1 אנטנה להרחבת קליטה ושידור ל 802.11 (ראה תמונה 1)
- 1 רכב מסחרי, עדיף בעל חלונות כהים למניעת חשיפה, או עמדה בטווח של 800 עד 1250 מטרים, מוסתרת, בעלת קו ראייה נקי אל המבנה.
- 3 תוכנות עיקריות:
 - א. Packet Sniffer and viewer
 - ב. WLAN analyzer and sync
 - ג. WLAN analyzer and syn for wince
 - ד. תוכנת P2P לחלוקת משאבי CPU לצורך פענוח צפנים בזמן אמת, מסמאות, פקטים, ועוד... (ראה תמונה 2)
- 1 טלפון סלולרי ברשת GSM, בעל יכולת של HSCSD להעברה מהירה ו-GPRS לשהייה מתמדת ברשת ולהעברת מסרים ונתונים. הפעולה:
- הרכיבים שמנינו מעלה ניתנים להשגה ללא קושי בחנויות המתאימות

(המשך בעמ' 62)



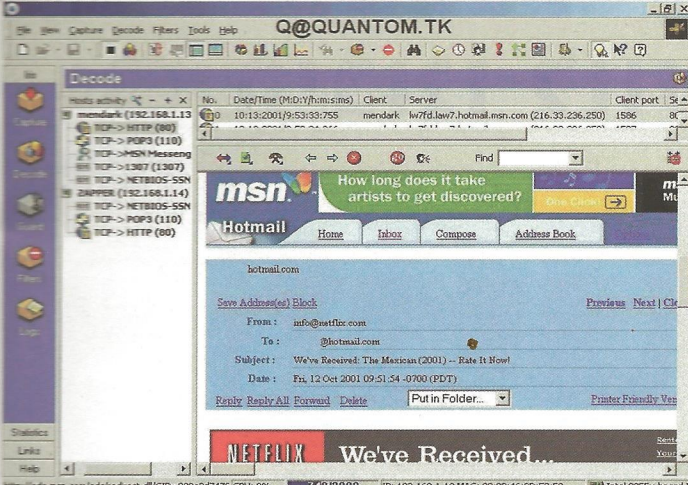
ש
אלה: מה ההבדל העיקרי בין אקדח למחשב?
תשובה: ההכרה של מוסדות החוק בייעוד של אותו כלי ירייה לביצוע ירי למטרות הרג או הגנה עצמית, כאשר הנזק ניתן לשליטה על ידי היריה עצמו. לכאורה נשמע פשוט, אולם מתי חלה התפנית? כשכל מחשב יוכל לבצע יותר מעיבוד תמלילים, הנהלת חשבונות או משחקים. מה קורה אם למחשב יש יכולת לבצע הרג המוני, הרג ממוקד או גרימת נזקים ללא יכולת לחזור אחורה.
מה ההבדל בין אקדח למחשב?
 תשובה: בידיים הנכונות "המקצועיות" אין שום הבדל. הסבר: פורץ ברמה עולמית יכול לגרום נזק גדול באפלי מונים מאדם המיומן בשימוש בכלי ירייה.
איך ולמה?
 כאשר הטכנולוגיה קיימת, באפשרותו של האדם השולט בה באופן מוחלט לתמרן אותה כראות עיניו.

טורר בקליק

נשיאת מחשב אישי או כף יד בליווי טלפון סלולרי, מתאם רשת רגיל או אלחוטי, אינה מוגדרת בחוק כעבירה עקב הגדרת השימוש בה. לעומת זאת, נשיאת כלי ירייה ללא רשיון היא עבירה חמורה על החוק מכיוון שהוגדרה כך. אדם פשוט יכול לבצע פעולות בטורר קיברנטי ואלקטרוני בקלות רבה בעזרת כלים זמינים, בצורה חוקית, לכל דורש ובלא כל רישום. דוגמה ראשונה: WARDRIVE - נסיעת מלחמה - בסרטים ראינו דוגמאות רבות לנוק שיכול להיגרם על ידי מחשב ליחיד או לקבוצה, ראה לדוגמה את הסרט הרשת בהשתתפות **סנדרה בולוק**. הרעיון לחדור לתיקו הפרטי של חולה המאושפז ולשנות לו את המינון וסוג התרופה שהוא אלרגי אליה, והרי לכם התנקשות פשוטה, שקטה וחכמה. בכל יום שעובר, מערכות המחשב משתלטות על חיינו יותר ויותר. לדוגמה, הכניסה עם כלי ירייה לבית חולים היא בעייתית, אולם הכניסה עם מחשב נייד וטלפון סלולרי פשוטה ואפשרית, והשומר לא ידרוש מכם בכניסה רשיון שימוש במחשב או היתר מסוג זה או אחר. ולמה? כי עד שלא יקרה אסון אף אחד לא יתעורר.

איך מזהים מתנקש או פורץ מחשבים מיומן לפי המראה...?
 הטכנולוגיה הופכת מיום ליום זמינה יותר, וזוהי יותר, קלה יותר והכי חשוב, פרוצה יותר. השימוש ברשתות אלחוטיות 802.11 ו"שן כחולה" ודומיהן הופך לשימוש וזול, כאשר החיסכון הן בתשתיות והן בזמינות/גישה הופכים את אותם ארגונים לטרף קל.

* רואי כהן, מומחה לתקשורת, לוחמה אלקטרונית וטורר קיברנטי, חברת Q@QUANTOM.TK, QUANTOM SYSTEMS INT



2 תמונה

שהכלים העומדים לרשותו הופכים להיות קשים מאוד לאיתור והיכולות שלו להוציא סודות מן הארגון הולכות וגדלות. בואו ננתח גוף צבאי כלשהו המוגן כולו בגדרות חשמליים, בגלאי תזווה, במצלמות תנועה רגישות לחום ולאור רגשי לחץ וחשמל ועוד אמצעי מיגון כאלה ואחרים. השאלה היא למה הם שם? ולא דווקא כדי למנוע חדירה פנימה אלא כדי למנוע בריחת אדם עם אינפורמציה רגישה החוצה.

לפני שנים לא רבות, בטרם עידן הרשת, היו קיימים אמצעי ריגול תעשייתי פשוטים אך קשים להשגה, היום המצב הפך להיות גן עדן לריגול תעשייתי. בשרות הבאות נתח הברחת אינפורמציה רגישה מארגון בעל רמת סיווג גבוהה מאוד.

להלן דוגמאות לאמצעי ריגול ישנים: מצלמת מיקרופוני רגישה לאור עם ASA גבוה, מיקרופון וטייפ מנהלים זעיר, משדר (BUG) ועוד. באם נתפסת כשאלה ברשותך, יכלו מיד להגדיר את ייעודם ואתה היית מוגדר כמרגל. בימים אלה ממש החלה חברה סלולרית בישראל לתת שירותי GPRS מהירים, הכוללים גישה מתמדת לרשת, כולל כתובת IP וטלפונים מזור 2.5 ו-3 חדישים מאוד, שלפעמים גורמים לי לחשוב כי אין אלה טלפונים אלא ציוד מתקדם לריגול.

שתי יצרניות ענק של טלפונים סלולריים משווקים טלפון שמוכנת בו מצלמה רגישה מאוד, צבעונית, עם חיבור לרשת. אחד מהם לא חושף את העובדה שיש בו מצלמה והוא נראה כטלפון תמים לחלוטין, אבל שערו בנפשכם מה ניתן לעשות בו. בעבר וגם היום נאסרה היציאה מארגון רגיש או גוף צבאי עם מדיה אלקטרונית כגון CD, דיסקטים ועוד, ללא אישור.

בארגונים מסוימים אין אינטרנט או כל גישה אחרת לרשת האינטרנט מחשב לפריצה פנימה או הברחת חומר החוצה. אבל אין מניעה להכנסת טלפונים סלולריים. במקרים מסוימים הטלפון ניתן על ידי הארגון כך שהשימוש בו עקב הצורך להיות זמין הוא הכרחי לעובד ולארגון.

אותו מכשיר טלפון יכול להיות גן עדן לאותו גורם עוין, המסוגל לצלם בזמן אמת תמונות או קטעי וידאו קצרים בזמן אמת לשלוח אותם החוצה לצד שלישי עוין.

מספיק מחשב נייד, המחובר לרשת הפנימית, שיש לו יציאת תת אדום. קיימת היכולת המיידית לגרום לאותו מחשב להיות שער גישה לרשת לכל הארגון כולו. כיצד? חיבור מצד אחד לרשת ומצד שני לטלפון שמחובר לאינטרנט. מדהים בפשטות ומפחיד.

גניבת רשת סלולר

חברות רבות נוטות להתקין במשרדיהם מגברים סלולריים או מעבירי רשת באזורים מסוימים. אותו סלולר FIREWALL יכול לאפשר לפרוץ להעביר את הרשת אליו בטכניקה הקרויה CELLULARJACK, בעזרת שימוש בשתי מזוודות. בקרוב לתחנת הממסר יש אפשרות לשבש את התחנה המקורית ולהתחזות אליה עם היחידה השנייה על ידי שימוש בכלים מיוחדים (כלים אזרחיים) ותוכנות מתאימות, וכך להיות ה-GATEWAY לכל הטלפונים בסביבה, ומצד שני לדמות פעילות ברשת המקורית כדי למנוע חשדות מצד חברת הסלולר. כל מה שיעבור ברשת, נתונים או קול, יהיו תחת האזנה של אותו פורץ. □

(ראה פרשנות בעמוד 10 בגיליון זה)

טור קיברנטי

הנח להשחית (המשך מעמ' 60)

והם חוקיים לחלוטין. סריקת הרשת: בעזרת מקלט ה-GPS, תוכנת הסריקה ל-WINCE ומחשב כף היד נוזה פעילות של כתובות WLAN, תדרים וערוצים זמינים הנמצאים בשימוש, תוך כדי תנועה מסביב למבנה המטרה.

הפורץ ימקם את הרכב בטווח של בין 800 ל-1250 מטרים מהמטרה, בקו ראייה פתוח ללא מכשולים בינו לבין המטרה על מנת לא להיחשף, הפעלת המחשב והאנטנה במאוזן או במאונך למטרה ללא כיוון מיוחד. הפעלת תוכנת ניתוח הרשת, סריקת כל הכתובות-תדרים-ערוצים-פרוטוקולים-פורטים-שערי גישה לרשת תוך דקות ספורות והכנסתם לניתוח מהיר על ידי אותה תוכנה. לאחר מיפוי מדויק ומחלט של הרשת ביצוע נעילה על ערוץ מבוקש של ID מסוים באותה רשת וניתורו ופענוח הניתור על ידי תוכנת הפענוח ה-SNIFFER וה-DECODER. כעת ייגש הפורץ לביצוע השיבוש והחטיפה של אותו ערוץ וכמובן ההתחזות. הפורץ ייגש בעזרת תוכנה ל-FLASH של כרטיס הרשת שלו וישנה אותו אחד לאחד בהתאם לאותו קורבן מיועד שחבר לעצמו ברשת הנפרצת.

הרמת הסלולר FIREWALL המצוי במזוודה (ראה תמונות 6 ו-7) וכיוונו לעבר המבנה, חיבורה של מערכת הכיול ושינוי התדר (ראה תמונה 5), סנכרון שעונים בין כל המערכות.

איך זה טובד?

כעת יפעיל התוקף ל-8 שניות מדויקות את הסלולר FIREWALL וישתק את כל הרשת האלחוטית בבניין או באזור שאליו כוונתה המערכת ל-8 שניות, שלפי ההגדרה יגרמו להתנתקות של כל המנויים מהשרת וממערכת השרידור והקליטה של ה-802.11.

עם חזרת המערכת לפעולה יפעיל הפורץ את המחשב הנייד ואת אותה תוכנת האזנה וימתין לאותה התחברות מוצפנת מאומתת של הקורבן בבניין שעליו הוא השתלט. כעת יבצע הקורבן התחברות מחודשת לרשת ולא יחשוד בתקינות הציוד שבו הוא משתמש. ההתחברות המוצפנת תישלח לשרת, שיאמת את ה-ID החומרתי של כרטיס הרשת של המשתמש, שם המשתמש והססמה המוצפנת, ובכל אותו זמן הפורץ יאזין לחבילות מידע אלה, יאסוף ויעביר אותם דרך ה-GPRS ותוכנת ה-P2P לרשת של מחשבים (תבריש שלו או מחשבים שעליהם השתלט מבעוד מועד בעזרת תוכנת "קליינט" מתאימה, ללא ידיעתם, כגון אוניברסיטאות, ספריות ציבוריות וכדו'). וכעת כולם יקבלו שברירים מוצפנים ויפענוח אותם עבורו.

המחשב האישי ברכב שלו ינהל בעזרת תוכנת ה-P2P את המשימה והתוצאה תחזור תוך מספר שניות עד דקות. כעת, כשיהיה לו את הססמה ושם המשתמש, ישיבת שנית את הרשת, אבל כעת ממאזין הוא יהפוך למשדר, כאשר הוא ישר את הנתונים בעוצמה גדולה משמיד הקורבן, דבר שישתק בו הקורבן לחלוטין, מה עוד שכעת ההתחברות שלו גרמה לחטיפה של המספר הסידורי של חומרת הקורבן, כך שלא תהיה דרך למנוע את חיבורו לרשת. לאחר האזנות מרובות ייצור מפגעי רשת, סוסים טרויאניים, שישתלטו עבורו על הרשת כולה.

מרגע זה החדרה של וירוסים, סגירת מנגנוני הגנה כגון FIREWALLS וגניבת מפתחות ההצפנה של השרת תלויים ברצון הפורץ בלבד. כעת, כאשר הבנו את הבעיה, אז מה ההבדל בין אקדה למחשב? אם הוא נמצא בידיים של מקצוען ובעקבות השימוש בו יכולים למות אנשים מה היה קורה אם אדם זה היה בית חולים או חברת השתיות כלשהי?

לוחמה פנים ארגונית

אחת הבעיות הכאובות היום היא חוסר היכולת להכשיר את קציני הביטחון. בעולם של טור קיברנטי, ניתן להכשיר את איש אבטחת המידע להיות קצין ביטחון, אבל עקב מורכבות עולם ה-IT, אין באפשרותנו להכשיר את קצין הביטחון לאיש אבטחת מידע, אלא בהסבת מקצוע מסובכת שדורשת זמן רב ויכולות נוספות שאינם תמיד בנמצא. הבעיה הכי כאובה היא היכולת ליהוות גורם עוין בתוך החברה שלך, היכול לבגוד בארגון, למכור את סודותיו או לגרום לקריסתו. הסיכויים לאתר אותו שואפים לאפס והבעיה הולכת ומסתבכת ככל

העולם כולו על 13 שרתים

בעקבות מתקפת שרתי האינטרנט: מומחים מעריכים שריכוז משאבי האינטרנט במספר כה קטן של שרתים - נקודת תורפה לרשת כולה

ISP מורשה או מאומת. והשנייה מנהלת redundancy, המאפשרת חלוקת עומסים וגיבוי באתרי משנה נגד פגיעה בשוגג או בזמני.

התקפות כאלה הן התקפות ברוטליות, המראות על חוסר מקצועיות וונדליזם מצד התוקפים והם טופולוגיות של התקפה שעברו מן העולם. ישנם כיום דרכים הרסניות באלפי מונים יותר מאשר התקפות מסוג זה.

ובכל זאת כל עולם המיחשוב היה מזועזע?

כחן: "לדעתנו תחכום לא היה הצד החזק כאן ואם משהו רציני היה רוצה למוטט את אותם שרתים יכול היה לעשות זאת ברגע אחד ולבד ללא תיאום התקפה מסודרת של מאות תוקפים בו זמנית וזאת בעזרת כשרון וידע אמיתי לפגיעה בעקב אכילס של אותם שרתים. נקודה נוספת היא הפצה וירלית מקיפה של סוכני התקיפה, שלא הייתה הפעם, וזאת בניגוד לפעמים קודמות.

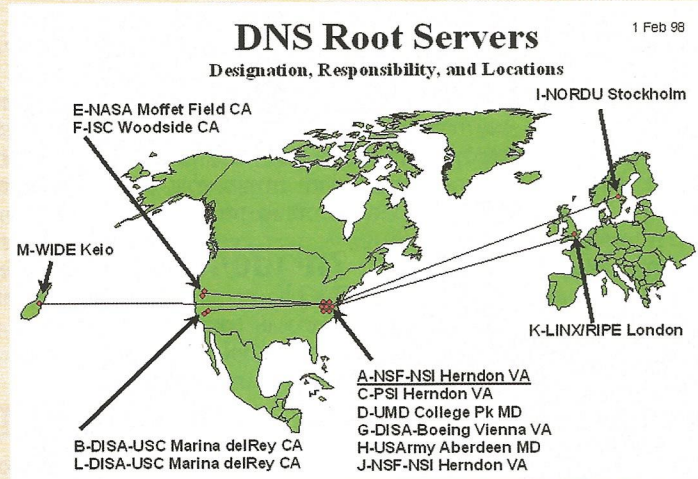
איך זה עובד בכלל?

בכדי לגלוש או לנצל שירות זה או אחר של מחשב מסוים ברשת צריך המחשב של הגולש לקבל כתובת ברשת כמספר בטווח מספרי כתובות של 255.255.255.255. יש גם טכנולוגיות חלוקת כתובות חדשות, הפועלות בטווחים אחרים, אך לא זה המקום להרחיב עליהן ויש שרתים, הנקראים שרתי DNS, המתרגמים שמות למספרים ולהיפך.

כדי להסביר מה קרה שם בפשטות, נדמיין לנו בניין שבו יש מספר דלתות משוריינות וכבדות. בתוך הבניין יש טבלה, ובאותה טבלה רשומות שתי עמודות, עמודה של מספרים ועמודה של כתובות בתים ואנשים. כדי להגיע לבית מסוים אנו צריכים לבקש יפה משומר הבניין שיחפש לנו מספר מסוים, בעוד אנו ממתנינים בחוץ שיחזור עם תשובה היכן נמצא אותו מספר. אם ייפול הבניין או יישרף, לאף אחד לא תהיה הכתובת ואף אחד לא יוכל להמיר שום מספר לשום כתובת.

או באו אנשים רבים עם פטישים כבדים, וכולם ביחד החלו בצורה מסודרת ומסונכרנת לדפוק בכל הכוח על הדלתות במטרה למוטט אותן ולחדור פנימה, או למוטט את הבניין כולו כך שאף אחד לא יוכל לנצל את שירותי הבניין. תקיפה זו נקראת תקיפת מניעת שירות DOS, או תקיפה מפורזת למניעת שירות DDOS. אבל השרתים עמדו בעומס ושום דבר לא קרה."

אבי בליזובסקי



הפיזור הגיאוגרפי של 13 שרתי השורש

הגלובלית. יש לציין, שההתקפה לא הייתה מורכבת או מתוחכמת במיוחד.

"שרתי שורש אלו נותנים שירות כשרתי שמות ראשיים באינטרנט ופעילות של מספר רב של שרתים כאלה, העובדים בו זמנית וביכולת מלאה, היא קריטית כדי שכל אחד מאיתנו שמחובר לאינטרנט יוכל לגלוש במהירות ויוכל להגיע לאתרים השונים. בצורה האופטימלית, כל שרת כזה מצפה לפניות ועליו להחזיר תשובה למבקש."

"הפעילות ההתקפית על שרתי השורש הסתכמה בהגברת העומס על השרתים, כך שמשפר הפניות אליהם היה גבוה מאוד. כך קיוו התוקפים שאותם שרתים ייפלו או ינתקו ולא יוכלו לשרת פניות נוספות עקב עומס יתר. לשמחנתנו הרבה, ניסיון פריצה זה לא צלח במיוחד ושרתי השורש, המורכבים בתצורת גיבוי הדדי - עמדו בעומס. מומחי אבטחת המידע פעלו מהר, ובזכות פעילותם מיהרו התוקפים להינתק על מנת שלא יתגלו עקבותיהם."

הוומה על לא מאומה

רואי כהן, מומחה ללוחמה אלקטרונית ואבטחת מידע בחברת קואנטום אומר, כי אין צורך להתרגש מהמתקפה. בכל יום נעשות עשרות תקיפות של DDOS או DOS, תקיפות לחץ ברוטליות כדי למנוע שירות או כדי לפגוע כלכלית בחברה זו או אחרת, ראה התקיפות על CNN ו-YAHOO. תקיפות מסוג זה הן יעילות לזמן קצר או רק לאותו זמן של הפצצה על אותו שרת. שנית, התקיפה המסוימת הזאת ניתנת למניעה די בקלות בעזרת שני מנגנונים: מנגנון מניעת תקשורת עוינת בגישה ישירה שלא מספק

13 שרתים בסך הכל מנהלים את כל מערכת הכתובות באינטרנט. מספר כה נמוך של שרתים מהווה נקודת תורפה לרשת כולה, וכעת גם האקרים וטרוויסטים גילו זאת.

בלילה שבין יום שני לשלישי השבוע נערכה התקפה אלקטרונית רבת עוצמה על תשעה מ-13 השרתים המנהלים את תעבורת האינטרנט, כך אישרו אתמול גורמים רשמיים בווינגטון. ההתקפה נמשכה שעה והיא הביאה להאטה מסוימת בגלישה. דובר האף-בי-איי מסר כי החל

לחקור את המתקפה, שתוארה על ידי מומחי אבטחה אחדים כחסרת תקדים.

מדובר בשרתים המפורזים ברחבי העולם - בארה"ב, בריטניה, שוודיה ויפן, ועל פני קשת של מוסדות וחברות פרטיות. מערכת שרתי השורש היא למעשה ספריית-על לכל כתובות האינטרנט בדומיניים ברמה העליונה כמו למשל .com; net; .uk,ca,fr,il. השרתים ממירים את הכתובות הטקסטואליות לכתובות IP נומריות. אל שרתים אלה מגיעים רק אם שרת הכתובות המקומי אצל ספק האינטרנט לא מכיר את הכתובת. שרתי הכתובות מסתנכרנים עם שרתי השורש אחת לתקופה כדי לעדכן את המידע המקומי. מספיק אמנם שרת שורש אחד, אך כאשר פועלים פחות מתשעה, התנועה אטית ביותר.

ככל הנראה, מדובר במתקפת שלילת שירות מבזרת (DDoS), שבמהלכה משתלטים המתקיפים על שרתים ותוקפים באמצעותם מתקפה על מערכת מסוימת. המתקיפים מציפים את היעד נתונים וברקשות רבות, במקרה הנוכחי פי 30 או 40 מהרגיל, לקבלת מידע באופן שעלול להביא להאטה רבה במערכת, עד כדי שלילת השירות למשתמשים לגיטימיים.

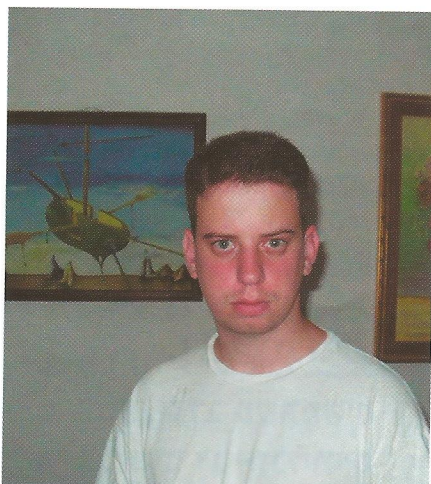
תופעה חדשה

שי אלמוג, מומחה לאבטחת נתונים בחברת סקוירנט, אומר, כי נראה שתופעת ניסיונות תקיפה של שרתים באינטרנט הולכת ומתרחבת. לעתים התוקף הוא אדם בעל ידע בסיסי בלבד ומטרות התוקפים שונות ומגוונות. לאחרונה החלה התקפה מול מספר שרתי שורש, שפעילותם היא מרכזית וחשובה במערך הרשת

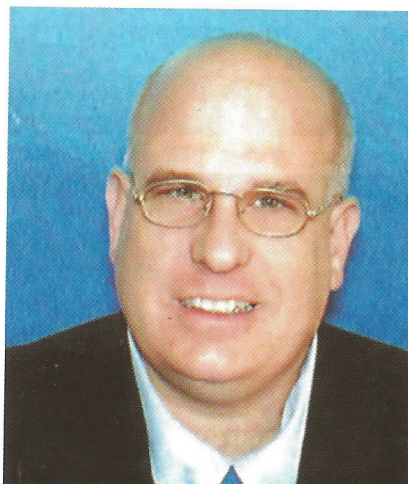
מלחמה במעגל קסם

עולם אבטחת המידע, אשר עבר מהפכות טכנולוגיות מרשימות בשנים האחרונות, נמצא תחת מתקפה בלתי פוסקת של האקרים אשר עושים הכל על מנת לחדור דרך הביצורים המסיביים אשר מציבות חברות האבטחה מסביב למאגרי המידע של הארגון. הכתבה סוקרת את הגישות והפתרונות של מספר גופי אבטחה, המציגים ברובם אופטימיות זהירה ולמולן האקר מיומן האומר, שבקרב הזה, המבוסס על מגננה מתמדת, ההפסד הוא רק עניין של זמן

מיכאל עציין



רואי כהן, מומחה ללוחמה אלקטרונית, חברת קואנטום



אריה דנון, מנכ"ל סימנטק ישראל

קואנטום ומדמה עבור החברות המעסיקות אותו את פעולתו של ההאקר המנסה לחדור לארגון. לדברי רואי מצב האבטחה קשה הרבה יותר ממה שמוכנות חברות האבטחה להודות. "יקח למשל את נושא ההצפנה", הוא אומר. "הבעיה היא שכל הצפנים מבוססים על אלגוריתם מתמטי ומחשב יוצר אותם, וזה רק עניין של זמן עד שמחשב אחר יפרוץ אותם. כאן מסתמנת מגמה חדשה אצל ההאקרים - P2P centralized hacking - חיבור עשרות אלפי מעבדים בזמן אמת וחלוקת משאבים מדויקת לחלוטין לפיצוח מהיר ויעיל של כל צופן מסחרי ואפילו צבאי. כל נשכה את מחוללי הסוסים הטרויאניים המאפשרים

המשך בעמוד 16

אחר שהכרנו בעבר ולגרום לנזקים גבוהים במיוחד - הן פגיעה כספית והן פגיעה במוניטין החברה הנפגעת. CodeRed לבדו גרם בשנה שעברה לנזק בשיעור של למעלה מ-2.6 מיליארד דולר ו-Nimda גרם לנזקים בשיעור 635 מיליון דולר. האימונים המשולבים שינו לחלוטין את תשתית האבטחה הנדרשת להתגוננות מולם. מעתה ברור כי התפיסה "פתרון נקודתי לאיום נקודתי", אינה עובדת עוד, שכן היא אינה מסוגלת להתמודד עם מגוון טכניקות התקיפה של האיום המשולב. יש צורך בתפיסת אבטחה יעילה יותר ומתוחכמת יותר.

עניין של זמן

רואי כהן, בחור נמרץ בן 26, הינו מומחה ללוחמה אלקטרונית ואבטחת מידע בחברת

אסון התאומים בניו-יורק ומספר וירוסים קטלניים במיוחד שתקפו בשנה האחרונה, העלו את המודעות ברוב הארגונים לחשיבות העצומה שיש באבטחת המידע ואכן סקרים שנערכו בין מנהלי אבטחה בשנה האחרונה הצביעו על ירידה בכמות הפגיעות כתוצאה מהקשחת מערך האבטחה וקביעת מדיניות נוקשה ובלתי מתפשרת בנוגע לזיהוי של מתקפות וירוסים, סוסים טרויאנים או תולעים. אולם נושא אבטחת המידע אינו רק עניין של מרוץ טכנולוגי, למעשה עתידה של הכלכלה המודרנית, המושתת כולה על מחשבים ותקשורת, תלוי ביכולתה להגן באופן מושלם על מערכות המידע. לדוגמה, שטרות הכסף שכל אחד מאתנו מחזיק בארנק, נתפסות על ידינו כבעלות ערך רק משום שהושקעו מאמצים גדולים על מנת לגרום לכך שניתן יהיה לזהות אותם באופן חד ערכי. כל חריגה ממצב זה מביאה מייד לכאוס כלכלי. אך הסכנות שבקיומן של נקודות תורפה במערכות האבטחה אינו מסתכמות בכלכלה, חישוב על מחשבי הצבא, חברת החשמל, בתי חולים, מערכות הרמזורים, רשת הטלפונים.

האימונים המשולבים

"שוק אבטחת המידע הושפע מאוד בשנה שעברה מהופעתם של סוג אימונים חדש ומתוחכם - האימונים המשולבים (Blended Threats)", אומר אריה דנון, מנכ"ל סימנטק בישראל. "האימונים המשולבים, כדוגמת CodeRed ו-Nimda, אשר הופיעו במחצית השנייה של שנת 2001, ו-Klez, אשר הופיע בראשית 2002, עושים שימוש במספר טכניקות על מנת לתקוף ולהתרבות ועל כן דורשים מספר אמצעי הגנה לשם ניטרולם. רמת התחכום הגבוהה של אימונים אלה מאפשרת להם להתפשט מהר יותר מכל איום



נפתלי קרון, מנהל אזור המזרח התיכון בצ'ק-פוינט



חיים מלמד, מנהל שיווק ופיתוח עסקי, סיסקו ישראל

המכשיר לרשת האינטרנט, לבצע פריצה ולאחר מכן להשמיד את הטלפון והנה קיבלנו פורץ אנונימי ללא יכולת איתור. כל אחד יכול היום להיכנס לאינטרנט קפה להדביק את אחד המחשבים בסוס טרויאני, לצאת לפרוץ אל אותו מחשב ממחשב אחר ולהשמיד את הראיות. שוב, פורץ ללא יכולות איתור."

בית ללא מגנולים

חברות כמו צ'ק-פוינט, אשר ביססו את קווי המוצרים שלהן על תוכנה באופן טהור, משנות כיום כיוון ומציעות פתרונות מגוונים יותר וקלים יותר לניהול כנגד האיומים החדשים: "אתה לא יודע אם נכנסים ומחטטים לך בתוך המחשב, אבל זה שאתה לא יודע לא אומר שזה לא קורה." אומר **נפתלי קרון**, מנהל אזור המזרח התיכון בצ'ק-פוינט, ומסמן את המטרה הבאה של עולם אבטחת המידע - הארגונים הגדולים הקטנים עד בינוניים. "הארגונים הגדולים שפכו" ממון רב על מנת לבצר את המידע החסוי שלהם. לא כך הדבר עם הארגונים הקטנים יותר. הבעיה מתחילה, כשהארגון קטן ואין לו את האמצעים לרכוש פתרונות אבטחה כוללים ויקרים, וממשיכה אל אנשים פרטיים, המשתמשים במחשב מהבית לצורכי עבודה או בידור. השווקים הספציפיים הללו נדרשים ליותר ויותר פתרונות אבטחה בעידן הנוכחי. משרדים קטנים רבים נפתחים כשלוחות מרוחקות של ארגונים גדולים יותר. הם זקוקים לפתרון אבטחה היקפי של המשרד עצמו, והן לאבטחת המידע אל ארגון האב. גם הבית הפרטי הופך לא פעם לשלוחה של המשרד, וככל שגובר השימוש במחשב הביתי כך גדלים סיכויי הפגיעה במידע שהוא אוצר

נקודות מועדות לפריצה ברשת, לאבטחה כוללת של כל הרשת. אם בעבר התקנה של Firewall בחיבור לאינטרנט הספיקה להגן על הארגון, כיום יש צורך בשילוב של מערכות זיהוי, הצפנה, זיהוי פריצות, ו-Firewalls בהרבה נקודות ברשת, וניהול מאוחד של כל המרכיבים למתן פתרון כולל. דוגמה לארכיטקטורה המתבססת על תפיסה זו, הינה ארכיטקטורת SAFE של חברת סיסקו, המפרטת את הדרכים הנכונות לביצוע אבטחת מידע כוללת בארגון.

יחד עם העלאת מהירויות החיבור לרשת של המשתמשים המקומיים (מ-Ethernet ל-Gigabit Ethernet Fast), והעלאת מהירות חיבורי ה-WAN של הארגון, יש צורך לשדרג גם את מהירות התקני אבטחת המידע ברשת. מוצרי Firewall ו-VPN, שהתבססו עד היום על תוכנה מותקנת על מחשבים, עושים מעבר חד לכיוון התקני חומרה משולבים, המבצעים את אבטחת המידע וההצפנה בעזרת חומרה. קיימת מגמה הולכת וגוברת של שילוב יכולות אבטחת המידע המתקדמות פנימה לתוך תשתית התקשורת הארגונית. יצרני חומרה מובילים של תשתיות רשת (מתגים ונתבים) מכניסים יכולת אינטגרלית לביצוע Firewaling, IPSec VPN, IDS, SSL ועוד, ישירות לתוך המתגים. יכולת זו מאפשרת יכולת גידול וניהול טובה הרבה יותר מפתרונות חיצוניים נקודתיים."

נשאר אלמוני

רואי כהן מקואנטום נשמע הרבה יותר פסימי: "כיום, כל אדם יכול להיכנס לרשת קניות ציבורית להוציא מזומן מכיסו ולרכוש טלפון סלולרי בעל כרטיס משולם מראש ללא שום יכולת זיהוי. אותו אדם יכול לגלוש בעזרת

יצירת סוס טרויאני המיועד לקורבן הרצוי באופן שלא ניתן לזיהוי על ידי תוכנת אנטי וירוס, מכיוון שמעולם אף אחד לא נידבק בוירוס זה ולכן הקורבן הראשוני לא יזהה אותו כעיון. לאחר החזירה כל הקשות המקלדת התמונות על המסך או פעילות העכבר תוקלט ותשלח לדואר אלקטרוני אנונימי ברשת ולעוצמת ההצפנה אין שום ערך. כבר היום המעבדים הם מעל ומעבר לצריכה של משתמש רגיל. הפתרון נעוץ בבניית מערכת הצפנה חדשה לחלוטין שטרם נראתה ושאינה מבוססת על אלגוריתם מתמטי ולכן שום מחשב לא יוכל לנתח אותה ובטח שלא לפצח אותה. בכך נוכל ליצור סביבה מוגנת בפני עוצמת מחשב או יכולות מקבילות לה."

רואי כהן, קואנטום: "הפתרון נעוץ בבניית מערכת הצפנה חדשה לחלוטין שטרם נראתה ושאינה מבוססת על אלגוריתם מתמטי ולכן שום מחשב לא יוכל לנתח אותה ובטח שלא לפצח אותה. בכך נוכל ליצור סביבה מוגנת בפני עוצמת מחשב או יכולות מקבילות לה"

איומים מתוך הארגון

אולם הסכנות שלהן חשוף הארגון אינן מסתכמות בחדירות מבחוץ של האקרים זדוניים ווירוסים קטלניים. הסכנה הגדולה ביותר של רוב הארגונים מגיעה דווקא מן הבית פנימה. רוב הגניבות של הסודות המקצועיים הגדולים בארגונים התבצעו על ידי אנשים מתוך הארגון. הצורך להגן על משאבי הארגון מפני עובדיו שלו, יצר צורך במערכות ניטור ואימות זהות חדשות לחלוטין, תוך התמודדות עם האופי המבוזר כל כך של מערכות המחשוב הארגוניות, היוצרות מספר בלתי מוגבל כמעט של נקודות גישה למאגרי המידע.

חיים מלמד, מנהל שיווק ופיתוח עסקי בסיסקו ישראל, מתאר את האתגר המשולב מנקודת ראותה של סיסקו: "עולם אבטחת המידע מתפתח במהירות במקביל להתפתחות רשתות התקשורת, מערכות ההפעלה, פלטפורמות המחשוב, והאפליקציות. ניתן לזהות שלוש מגמות עיקריות בהתפתחות מערכות אבטחת המידע בתקשורת הארגונית: מכיוון שהאיומים של היום מגיעים מתוך הארגון, כמו גם מחוזה לו, ומכיוון שכלי הפריצה הופכים יותר ויותר מתוחכמים - קיימות מגמה של מעבר מאבטחת נקודתית של

מציין כי צורכי האבטחה של הארגונים נגזרים מהצורך הבלתי נמנע בקישוריות מוגברת בין חלקי הארגון השונים, אנשי השטח עם המחשבים הניידים והחשיפה של חלקים נרחבים יותר של מידע ארגוני לציבור הרחב. "כיום, מנגנוני האבטחה אינם יכולים עוד להתבסס על רכיב הגנה יחיד, כמו FireWall למשל", אומר גינדין, ומציין כי מגוון הרכיבים הנוספים, כגון: ניהול סקויריטי, זיהוי חדירות, אנטי וירוסים, הגבלות גישה וכדומה דוחפים את



ברוך גינדין, מנכ"ל גרטנר בישראל

ברוך גינדין, גרטנר: "עומס כלכלי בלתי נסבל עבור הארגונים דוחף אותם למציאת פתרונות מיקור חוץ לנושא האבטחה. עבור ספקיות תשתית התקשורת, מצב זה יוצר הזדמנות פז למקור הכנסה חדש של ערוצי תקשורת מאובטחים בתשלום, בשילוב מנגנוני אבטחה פנימיים"

הארגונים להתעדכנות מתמדת של רכיבי האבטחה, הנובעת מהעלייה ההדרגתית ברמות התחכום של הפורצים למיניהם. גינדין: "כל אלה יוצרים עומס כלכלי בלתי נסבל עבור הארגונים ודוחפים אותם למציאת פתרונות מיקור חוץ לנושא האבטחה. עבור ספקיות תשתית התקשורת, מצב זה יוצר הזדמנות פז למקור הכנסה חדש של ערוצי תקשורת מאובטחים בתשלום. על פי מחקר עדכני של גרטנר, עד לשנת 2006 50% מהארגונים הגדולים יעשו שימוש בשירותי אבטחה שניתנו על ידי חברות התקשורת, בשילוב עם מנגנוני אבטחה פנימיים. עד לשנת 2004 כל ספקי התקשורת בצפון אמריקה כבר יציעו ערוצי תקשורת מאובטחים ללקוחותיהם. עד לשנת 2005 יאמצו 50% מהארגונים הקטנים והבינוניים פתרון אבטחה זה ויחסכו בכך את הצורך לרכוש ציוד ותוכנות ייעודיות לאבטחה."

"נוצרה פה הזדמנות פז עבור ספקיות התקשורת מכיוון שהטכנולוגיה כבר קיימת, אין צורך להמציא אותה, ומה שנותר זה פשוט לשווק את השירות לקהלי היעד הפוטנציאליים ובכלל זה כמובן גם המשתמשים הביתיים שיוכלו להנות מקו תקשורת מאובטח ומוגן ללא התקנות או הגדרות מיוחדות במחשב הביתי שלהם ובהתחשב שהרשתות הביתיות תופסות תאוצה ומכניסות אלמנט סיכון חדש נוסף", מסכם ברוך גינדין מגרטנר. ■

בקרבו. יש את אלה שלא יודעים על הבעיה או אדישים אליה ולא נותנים שום פתרון אבטחה. הם משולים לאנשים שגרים בבית עם דלתות ללא מנעולים. אחרים מודעים לבעיה ואף רוכשים פיירוול בסיסי או תוכנת אנטי וירוס אך סובלים ממספר בעיות: ראשית, לרוב, המוצר לא נותן פתרון לכלל האיומים, ושנית, בדרך כלל מדובר במוצרים שדורשים משמשים מתוחכמים השולטים ברזי האפיון והניהול של תוכנות כאלה. עבור כל אלה פיתחנו את ה-S-box על ידי חברת הבת סופהור. זהו התקן חומרה הניצב בין הרשת הארגונית או המחשב בבית המשתמש, לבין הרשת הציבורית. ההתקן הזה כולל בתוכו גרסאות של הפירוול וה-VPN של ציק-פוינט, שהותאמו במיוחד עבורו."

מרכיבי הרשת המאובטחת

ניהול של אבטחת מידע מקצה לקצה היא הדרך היחידה לאבטח את הארגון **חיים מלמד**, מנהל שיווק ופיתוח עסקי בסיסקו ישראל, מסכם את המרכיבים העיקריים של רשת תקשורת מאובטחת:

מערכות זיהוי - מערכות זיהוי המשתמשים הארגוניות, כמו תחומים טכנולוגיים אחרים, עוברות סטנדרטיזציה ומעבר לכיוון ברור אחד - התבססות על LDAP ו-Directories כתשתית תפעולית למערכות Single Sign On. גם בעולם התקשורת נעשה שימוש בתשתית זו. המשימה של זיהוי המשתמש הראשוני הועברה אל נקודת הכניסה של המשתמש לרשת. פרוטוקולים מבוססי EAP (Extensible Authentication Protocol) - פרוטוקול גינרי המשמש לזיהוי משתמשים ברשת התקשורת, כדוגמת 802.1x ל-Wireless LAN ו-LEAP ל-LAN Switches מאפשרים כיום לזהות את המשתמש לפני כניסתו לרשת התקשורת עצמה (Layer 2), תוך שימוש בשירותי Radius המזונים מ-LDAP (Lightweight Directory Access Protocol) - פרוטוקול גישה סטנדרטי ל-Directory הארגוני

התקני VPN - עולם ה-VPN הופך להיות בשל וקל יותר ויותר למימוש. יותר ויותר ספקי שירות מציעים שירותי VPN מעל רשתות ציבוריות למיניהן. שתי הטכנולוגיות המובילות בתחום כיום הינן IPSec ו-MPLS, או שילוב של שתיהן. השילוב של MPLS במהירויות גבוהות, וצורך ב-IPSec מעליה, דורש מעבר מהתקני VPN מבוססי תוכנה, לשילוב של יכולות VPN בחומרה בנתבים ובמתגים ברשת.

Firewalls - כמו במוצרי VPN, כך גם ב-Firewalls, או רואים צורך הולך וגובר בביצועים הולכים וגדלים, תוך אינטגרציה עם רשת התקשורת הארגונית. בארגונים מבוזרים או רואים צורך בשירותי Firewall בכל סניף של הארגון, כתוצאה מריבוי נקודות קישור של הרשת הארגונית ללקוחות, ספקים ואל האינטרנט.

Intruder Detection - הגידול הרב ביותר בשוק אבטחת המידע הינו הגידול בדרישה למוצרי IDS. ארגונים מבינים כי השימוש ב-Firewall אומנם נותן לארגון "הרגשה" שהוא מאובטח, אך לא מספק לארגון ידיעה אמיתית שהאבטחה אכן עובדת. התקנה של התקני IDS חכמים בנקודות הנכונות ברשת מספקת יכולת לזיהוי של פרצות וסגירתן, לעיתים באופן אוטומטי.

ניהול אבטחת המידע - זהו התחום הבעייתי ביותר כיום. ברוב הארגונים עדיין קיימות מערכות שונות לאבטחת מידע בנקודות שונות ברשת. כל אחת מהמערכות הנ"ל מנוהלת לרוב על-ידי מערכת בקרה אחרת, ללא קישוריות ביניהן. אינטגרציה של יכולות אבטחת המידע אל תוך רשת התקשורת, על-ידי יצרן יחיד, מאפשרת ניהול אחיד, קצה לקצה, של כל מרכיבי אבטחת המידע ברשת. יש לציין כי ניהול נקודתי של אבטחת מידע יכול ליצור סתירות במדיניות בין התקנים שונים, או גרוע מזה - "חורים" באבטחת המידע ברשת. ניהול של אבטחת מידע מקצה לקצה היא הדרך היחידה לאבטח את הארגון.

מקור הכנסה חדש

ברוך גינדין, מנכ"ל גרטנר בישראל, מתייחס להתפתחות מעניינת הצפויה בשוק אבטחת המידע בשנים הקרובות. אף הוא