קורא יקר,

וירוסים, פרצות וספאם הולכים ומתרבים מיום ליום **באופן מבהיל.** מערכות המחשוב הופכות למורכבות וסבוכות. במקביל, הפס הרחב, הוירטואליזציה, BI - מציעים **הזדמנויות חדשות ומלהיבות** וגם תפקיד מנהלי המחשוב עובר טרנספורמציה **דרמטית ומבטיחה**. כך, לנוכח שטף חידושים וגלי תמורות, שרק מתעצמים ומואצים, קשה להתמקד במה שבאמת חשוב. **למי להאמין? על מי לסמוך?**

תחקירי PCאון מספקים בכל שבוע ריכוז של החדשות החשובות ביותר בעולם המחשוב והתקשורת, יחד עם תחקיר מקצועי שמתמקד בנושא מפתח מרכזי ומשמעותי. הם משרתים חלק גדול ממנהלי המחשוב המובילים של מדינת ישראל. חלקם מנויים לשירות קרוב לשש עשרה שנים כיוון ש:

- PCאון הוא מקור מידע **אמין ותכליתי.** הוא מתמקד רק **בנושאי המפתח** החשובים ביותר בעולם המחשוב והתקשורת, והוא **מדבר בשפתך המקצועית.**
- PCאון כולל את ריכוז **החדשות החשובות** ביותר וגם **מגמות, טיפים, ידע יישומי ושימושי** נוסף. הוא מאפשר בהשקעה של **פחות מ-10 דקות** בשבוע, להיות כל הזמן **עם יד על הדופק.**
- PCאון מביא תועלת בכך שהוא **רלוונטי לבעיות הנוכחיות שלך,** בנוסף לכך, הוא מסייע לך בהערכות מוקדמת בפני **סכנות ואיומים** למערך המחשוב **ו/או ניצול הזדמנויות עסקיות** חדשות.
- ניתן **להתרשם ממנו באופן אישי** באמצעות תחקיר הדוגמא המצורף או להסתמך על למעלה ממאה חוות דעת של מנהלי מחשוב מובילים (ראה - www.pcon.co.il/v5/103.asp).

PCאון נתפס כיום כ**מפתח מוכח להצלחה מהירה,** וככזה גם אתה תוכל ליהנות ממנו בקרוב. כמו ארגונים רבים תוכל להצטרף כמנוי ארגוני ותאפשר לכל העוסקים במחשוב בארגונך, ליהנות מכל היתרונות שלמעלה.

מחירי מנוי השנתי בגין 52 תחקירים:

מספר מנויים	המחיר בדולרים + מע"מ
1	516
5	1270
10	1970
20	3270
50	5970
100	7700
200 ויותר	9700

נכון, אפשר לנסות להתמודד לבד עם כל התמורות. להתעלם או לדגום מאמר אקראי ולקוות לטוב. **תחשוב על התוצאות.** מצד שני ניתן ללכת **בדרך סלולה ובטוחה** שבה הולכים המובילים במחשוב הישראלי, שגם ימשיכו להוביל בבטחה. כדי להצטרף אליהם, ללכת יחד איתם, אפשר לקרוא על תחקירי PCאון ולהצטרף באתר ב- www.pCon.co.il/promo טלפון 03-9667939, פקס 03-9660310 או מייל - sub@pcon.co.il

קובי שפיבק
העורך הראשי של PCאון

נ.ב. על כל תחקירי PCאון חלות כל ההגנות החוקיות של זכויות יוצרים. ביחד עם זה, אנו מתירים לשכפל ולהפיץ את תחקיר זה, **מבלי לשנותו, עד 31.12.2007 ורק יחד עם דף היתר זה!** למנהלים, עמיתים ואנשי מחשוב נוספים, שעשויים לדעתך למצוא בו עניין.

מה אתה מקבל? - מפתחות להצלחה

קורא יקר,

תיזכר ב"נפילה" האחרונה של מערכת בארגון, ב"פספוס" בבחירת טכנולוגיה, בפרוייקט שלא "סיפק את הסחורה". מדמיין? עכשיו קח לך פחות מחצי דקה ותחשוב על מי שקרא תחקיר דומה, לפני כשנה. באינטואיציה פנימית חזקה הוא הבין שמצא פיתרון אמיתי לצורך אמיתי - להיות ממוקד באיומים האמיתיים וההזדמנויות המבטיחות שרלוונטיים לארגון ולתפקיד שלו, למציאות שבה הוא חי. שוב ושוב הוא נוכח מאז, שהוא מתבסס על מקור מידע שמדבר אליו בשפתו, מקור תכליתי ואמין.

כאשר חבר קרוב מתקשר ושואל לחוות דעתו על תחקירי PCאון. "מה הם נותנים לך באופן מעשי?" באופן טבעי הוא נזכר ומספר על כמה מהדוגמאות הבאות:

- **בתחקיר - ה-IT מאיץ חדשנות** - הוא גילה את הטרנספורמציה שעוברת היום כגל סוחף בעולם העסקי. ה-IT הופך מכלי שתומך בעסקים, למנוע שמאיץ חדשנות ופותח הזדמנויות חדשות. התועלת עבורו הייתה דרך הסתכלות חדשה על היבטי ה-IT, כזאת שפתחה בפניו דלת לקידום מהיר...

- **בתחקיר - חוסכים חשמל** - הוא מצא נתונים לפיהם, עלויות החשמל של דטה סנטר בשנה יכולות להיות יקרות יותר מכל עלויות החומרה שבו. הוא גם קרא כיצד השינוי בצריכת החשמל בניידים לוקחת אותנו לעידן חדש. התועלת שהפיק מהתייחסות ויישום הייתה - הרבה כסף לארגון. איך זה נשמע?

- **בתחקיר - כללי אצבע למנמ"ר** - הוא מצא נתונים, מספרים, כללי אצבע ומקורות שחיוני לכל מנהל שעוסק במחשוב להיות מצויד בהם. התועלת שהפיק הייתה קבלת החלטות מהירות יותר, מבוססות ומוצלחות יותר. התוצאות נראות בשטח. מכיר אנשים כאלה?

- **בתחקיר - וירטואליזציה בשרתים** - הוא הבין את המשמעויות המעשיות של מגמה מרכזית שסוחפות כיום את עולם המחשוב, כאשר הוא גילה **איך** וירטואליזציה יכולה להעניק יותר גמישות, חיסכון עצום, שרידות, עבודה קלה ועוד יתרונות נוספים. פתאום הכול התחבר. אתה רואה זאת?

- **בתחקיר - Rootkit - חפרפרת במחשב** - הוא קרא כי ברשת הארגונית של כל ארגון חמישי באוסטרליה (וכנראה כך גם בארץ), חבויה כיום תוכנה נסתרת, שיכולה לפתוח דלתות לתוכנות מזיקות. בדרך כלל, לא ניתן לגלות אותה! גניבת מידע, שיבוש נתונים, האזנות, ציטוטים, חדירות, נזקים. חלק מהאיומים יכולים להביא לקריסה. הוא עשה את כל שניתן לטפל בכך וישן טוב בלילה. ואתה?

הוא גם לא היחידי שחושב כך. מאה המלצות נוספות עם מסר חד וברור מדברות בעד עצמן. אחרי הכול, עם הישגים שמוכחים בשטח, קשה להתווכח...

לכן אנו ממליצים לשתף מספר רחב ככל האפשר של חברים, עובדים ומנהלים, בארגון ומחוצה לו, בשימוש בתחקירי PCאון. בדומה לטלפון ופקס, ככל שרבים יותר המשתמשים בהם, כך גם גדלה התועלת. אתה ודאי מכיר זאת.

עכשיו אתה מוזמן לקרוא את התחקיר המצורף, להתרשם באופן בלתי אמצעי ולהתקשר - דרך האתר www.pCon.co.il/promo לטלפן 03-9667939, לפקסס 03-9660310 או מייל - sub@pcon.co.il

אחרי שתצטרף ותסתכל קדימה שנה מהיום, יתכן וגם אתה תחשוב כמוהו? מה דעתך?

PCאון ©

למנהלים ומשתמשי מחשב בכירים

תדרוך מקצועי קצר ומרוכז ● בחדשות ומידע שימושי ייחודי ● למיצוי המחשוב באופן מרבי

והפעם... למה לאבטח יישומים ?

מסר אישי

אנטי וירוס? יש. פיירוול? יש. סיסמאות "לאלפים"? יש. אך מה לגבי יישומיך? האם משתמש או קוד עוין מנצלים אותם ברגע זה לרעה? אבטחת יישומים הוא נושא "חם" שהופך בהדרגה למורכב ומאתגר יותר ויותר. כאן טמון ה"חור" הפוטנציאלי, ב"סכר האבטחה" הסטנדרטי, חור שעשוי לאפשר לתוקף נחוש ליצור נזק כואב במקום שבכלל לא חשבת עליו.

מה כוללת הגנת היישומים? במה היא שונה מההגנות המקובלות? מהם הפתרונות לכך? כיצד תתגונן בחזית זו וביעילות? על כך ועוד - בתחקיר שלפניך.

תמצית החדשות בעולם המחשוב טור

תוכן התדרוך השבועי טור

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק** B.Sc. ,MBA

עורך - **ערן דרור**

תחקיר וכתיבה - **עמית לוי**

טלפון - **03-9667939**, פקס - **03-9660310**

דואר - **ת.ד. 2340 ראשון לציון 75121**

E-Mail - editor@pcon.co.il

לתשומת לבך

לכבוד **קומרקטינג בע"מ**
פקס 03-9660310
ת.ד. 2340 ראשון לציון 75121

___ כן אני רוצה להיות מנוי **PCאון**, לתקופה של 3 / 6 / 12 חודשים. אני מצרף סך בשקלים של $129 / $239 / $449 + מע"מ (סמן בחירתך בעיגול), לפקודת **קומרקטינג בע"מ** ומחכה לגיליון הקרוב.

שם מלא_____

ארגון_____

תפקיד בארגון_____

כתובת_____מיקוד_____

טלפון_____פקס_____

תאריך_____חתימה_____

הערות _____

PCאון© למנהלים ומשתמשי מחשב בכירים

636.11– חדשות בקצרה

• **חברת Network Appliance הודיעה על השקתם של מספר מוצרי איחסון חדשים**. המוצרים החדשים מיועדים לקצה העליון של השוק ומוצר הדגל ה-**gFiler** מתאים לעבודה מול שרתי **TotalStorage** מבית **IBM** ויכול לגשת למידע דרך ממשק **iSCSI** החדש ולא רק דרך רשתות **IP**. מוצרים נוספים כוללים הרחבות למשפחת ה-**NAS** של החברה.

• **אינטל** הודיעה כי המעבד הבא שלה, בעל שם הקוד **Grantsdale** יכלול יכולות מובנות לתקשורת אלחוטית. המעבד צפוי לצאת לשוק במחצית הראשונה של 2004 ולתמוך בזיכרון **DDR2 (Double Data Rate)**, בסטנדרט ה-**PCI** החדש **PCI Express** וכן לכלול יכולות בסיסיות של גרפיקה וסאונד. כמו כן הדגימה החברה את הטכנולוגיה הבאה שלה לייצור שבבים. עד 2005 היא אמורה להציג מעבדים המתבססים על טכנולוגיית ייצור של 65 נאנומטר ועושים שימוש בזיכרון **SRAM**, המהיר ואמין מ-**DRAM**, אם כי יקר ממנו לייצור.

• שרות **הוטמייל** שודרג לאחרונה בכמה נקודות חשובות של ממשק ושימושיות. מערכת אנטי ספאם חדשה תקל על המשתמש להתמודד עם התופעה המטרידה, ששמה על הכוונת במיוחד כתובות בשרותי דואר בולטים כ-**Hotmail**. דיווחים של המשתמש לשרות, יקדמו את יכולת השרות לחסום הודעות כאלה עוד עם הגעתן. עוד נוספו שיפורי ממשק ואפשרות למענה מיידי בעזרת **Messenger**.

636.12– נאבקים ומתחרים

חדשות מחזית "המאבק" לינוקס - מיקרוסופט:

• **Red Hat**, יצרנית ה**לינוקס** הגדולה ביותר, הודיעה כי בקרוב תקבל אישור בטיחותי מסוג **Common Criteria Certification**. משמעות האישור היא שהחברה תוכל להתחיל למכור את מוצריה לממשלות מכל רחבי העולם, כולל ישראל, אשר דורשות עמידה בתקני בטיחות.

• **Helium 2100** הוא מחשב נייד חדש מבוסס **לינוקס** המחדש במחירו: $999 בלבד. חידוש חשוב נוסף הוא בצורה ה"גמישה" המאפשרת להזיז את המסך כך שמתקבל מעין **Tablet PC**. המחשב מתוצרת **Element Computer** והוא רץ על מעבד **Via 1GHz Antaur**. לפרטים נוספים - www.zdnet.com.au/newstech/os/story/0,2000048630,20281522,00.htm

• ארגון ה**לינוקס** הבלתי מסחרי **The Debian Project** חשף פגם אבטחה חמור בליבה הישנה שלפני **2.4.23**. ראה תיקון אצל יצרן הגרסה שברשותך. גרסה **2.6** צפוייה החודש.

• ומהצד השני: בדיווחים שונים בעיתונות דווח כי מחירים נמוכים במיוחד שהציגה **מיקרוסופט** עבור ממשלת **תאילנד** מהווים תקדים לגישה כוללת להוזלת מוצריה. בבירור שלנו עם החברה התברר כי לא כך הדבר: ב**תאילנד** מדובר היה בפרוייקט תרומה לקהילה שנועד לצמצם את הפער הדיגיטלי - והוא פרוייקט ממוקד וחד פעמי. **מיקרוסופט** לא צופה ירידת מחירים גורפת בעתיד הקרוב.

• **מיקרוסופט** הכריזה על מדיניות חדשה של הרחבת הגישה למאגרי קניין רוחני, גם לארגונים קטנים יותר. המדיניות החדשה הוכרזה יחד עם שתי תוכניות רישוי קניין רוחני חדשות: הראשונה עבור טכנולוגיית **ClearType** והשנייה עבור מערכת **FAT (File Allocation Table)**.

• **מיקרוסופט** גם נאבקת במפיצים פיראטיים ב**מאלזיה**, לאחר שבמדינה זו החלו להופיע גרסאות פיראטיות של מערכת ההפעלה העתידית **לונגהורן**. מערכת זו צפויה לצאת רשמית רק ב-2005, אך בהתבסס על תקליטור הדגמה שהופץ בעבר, היא נמכרת שם ב-$1.58 לתקליטור.

636.13– זהירות !

וירוסים ושאר מרעין בישין ממשיכים להוות אתגר:

• חברות האנטי וירוס מדווחות על גילויו של וירוס "סוס טרויאני" חדש. **Sysbug** מעתיק עצמו לספריית ההתקנה של **חלונות** ומוסיף רשומות לרג'יסטרי, בכדי להבטיח את פעילותו כל אימת שהמחשב נפתח. הסוס הטרויאני מופץ באמצעות הודעת דוא"ל שכותרתה ותוכנה נושאים את השם מרי **(Mary)** ומבטיחה לנמען תוכן פורנוגרפי.

• העיתון **DailyMaily** מפרסם מפי חברת האבטחה **רנסאנס**, כי ניתן לצפות החודש לעליה דרמטית בכמויות הנוזקה לסוגיה: וירוסים, טרויאנים, ספאם וכדומה. זאת בין השאר במסווה הודעות ברכה לחג המולד ומידע שיווקי רב במיוחד לארגונים, לקראת סוף השנה.

• מספר חורי אבטחה חדשים התגלו בדפדפן **IE** של **מיקרוסופט**. על פי **Secunia**, חברת האבטחה שגילתה זאת, ניצול הפגמים ביחד עשוי לאפשר הפעלת המחשב בצורה מזיקה. חורי אבטחה נוספים התגלו לאחרונה גם בתוכנת **Small Business Server 2003** של **מיקרוסופט**, ברכיב יצירת ה**אינטרה-נט SharePoint Services**.

• סוכנות הידיעות **AP** פרסמה כי **צה"ל** שוקל להתקין מערכות זיהוי ביומטרי שונות לזירוז הטיפול במעבר הגבול בעזה. בין המערכות יהיו מערכות זיהוי פנים וזיהוי כף יד - שייחסכו חיכוכים מיותרים בין חיילים לאוכלוסייה.

636.14– כיוונים מבטיעים

כמה התפתחויות מעניינות מסמנות כיוונים חדשים בענף:

• מחקר חדש מוצא שהמחשוב והתקשורת האלקטרונית דווקא מקטינים לחצים אצל רוב האנשים. יוצאי דופן היו הנשאלים בסקטור הפיננסי: 81% מהם אומרים כי המחשוב והתקשורת האלקטרונית מוסיפים מתח לעבודתם, על ידי הפרעות חוזרות.

• **פניקס טכנולוגיות**, מיצרניות הביוס **(BIOS)** הגדולות בעולם, הודיעה על גרסה חדשה לביוס מתוצרתה. ביוס היא תוכנה המקשרת בין החומרה למערכת ההפעלה, ותצורתה הבסיסית לא השתנתה כמעט בעשורים האחרונים. את הארכיטקטורה החדשה שלה מכנה החברה בשם **dNA** או **device networked architecture** ו**פניקס** מוסרת כי היא תכלול חידושים רבים עבור מנהלי רשתות. בין החידושים שיגיעו עם הביוס החדש ניתן למנות הגנה דיגטלית מתוגברת למניעת גניבה של מחשבים נישאים או התחברות לא מורשית לרשת הארגונית, יכולות של אחזור מידע ויכולות ניהול רשת מורחבות.

• **W32/Mimail-L** היא החדשה האחרונה בעולמו המופלא של הזבל הממוחשב. זו היא תולעת שכפי הנראה פותחה על ידי ספאמר, מאחר והיא "מחדשת" בנסיון לתקוף דווקא תקיפת אתרי אנטי ספאם, בשיטת **DDoS**.

• **No More Moore?** - לפי מדעני **אינטל**, עד 2018 יאט המזעור בשבבים ויוציא את "חוק מור" בהדרגה מתוקפו. יש לציין כי החידוש הוא בעיקר בכך ש**אינטל** עצמה מכריזה זאת. בניגוד להכרזות דומות מצד אנליסטים בעבר, כאן כבר אפשר לומר "אם בארזים נפלה שלכת, אולי אין זו אגדה".

636.21– אתה בטוח ?

אם "הגנת יישומים" הוא עדיין מונח מעורפל עבורך - סביר להניח שארגונך חשוף במידה רבה לפורצים ומזיקים. בשנים האחרונות הפכו היישומים הארגוניים למורכבים ונפוצים, וכעת ניתן לומר ש"ידם בכל התהליכים העסקיים בארגון". הפופולריים שבהם הפכו למטרה מועדפת לתוקפים - שסרקו את הקודים בחיפוש אחר כל נקודת תורפה שניתן לנצלה. נדגיש את מערכות ההפעלה, מטרה רגישה, המהווה יישום גדול במיוחד (הרבה באגים ואתגר דיבוג גדול במיוחד). להערכות מומחים, תוכנה כוללת ממוצע של 10-20 באגים ל-**1,000** שורות קוד (אם זה היה המצב בכתיבת **מובי דיק**, היו בו **3,120** טעויות דפוס!).

יישום ארגוני הוא לרוב בעל הרשאות גישה למידע מסוגים שונים וניתן לנצלו לשם שימוש לרעה בגישה זו. פורץ בעל שאיפות ריגול תעשייתי יוכל למשל לשנות שאילתא משאילתא לגיטימית לשאילתא רחבה יותר הכוללת מידע מסווג. כמה דוגמאות מהחיים להמחשה: התולעת **SQL Slammer** תקפה מערכות **SQL Server 2000** לא מעודכנות ובהצלחה רבה: היא הכפילה את מספר המחשבים הנגועים בה כל 8.5 שניות, בשלוש הדקות הראשונות להפצתה. ודוגמא מקומית: לפני כמה חודשים פורסם ב-**Ynet** כי התגלתה פרצה שאיפשרה גניבת פרטים אישיים של נרשמים, לשרות ה**ניוזלטר** (עדכונים וחדשות בדואר) של אתר **בנק הפועלים**.

פתרונות הגנת יישומים מתחילים לצוץ, ובשפע. חברות אבטחה מובילות, כגון **צ'קפוינט**, כמו גם חברות המציעות פתרונות ייעודיים - מציעים כלים המאפשרים ניטור, ניהול, הגבלה וכיוונון פעולת היישומים הארגוניים - במטרה לאתר ולמנוע פגיעה בהם או את ניצולם לרעה.

בעתיד אבטחת היישומים, צפויים אתגרים חדשים להעלות את רף אתגר ההגנה. שרותי **Web** ייצרו מערכות מחשב המקושרות בדרכים חדשות ומורכבות מתמיד. מחשוב **Grid** יפזר יישומים (אותם חייבים לנטר) על פני מערכות רבות.

מצד ההתגוננות, חשוב לציין שהפתרונות הקלאסיים אינם מספיקים, ויש לחפש ולחשוב על כללי אבטחה בסיסיים ועד פתרונות ייעודיים ומתוחכמים. חשוב להתגונן מכך עכשיו, מאחר ואיום זה מתגבר, מכוון ללב היישומים הקריטיים ופגיעתו עלולה להיות ממוקדת במטרה ספציפית, שלא תמיד מוגנת כראוי, כגון גניבת פרטי לקוחות!

<u>לסיכום - וודא בהקדם שהיישומים הארגוניים מוגנים היטב בפני תקיפה. ומעכשיו והלאה - טפל בכל יישום חדש המוכנס לארגון גם מזווית קריטית זו.</u>

636.22– הנתיב והמכה

בין סוגי היישומים שלרוב מותקפים, בולטים במיוחד:

1. **יישומים משרדיים** - יישומי דסקטופ נפוצים, כמעבדי תמלילים או דפדפן, מהווים מטרה נפוצה ביותר. לתוקף המחפש פרסום הם מבטיחים הגעה לכותרות. ל"מקצוען" הם מתאימים בגלל שפגמי האבטחה שבהם, נחשפים ומתפרסמים בידי מספר רב של אנשים וגורמים מקצועיים.
2. **יישומים ארגוניים** - יישומים דוגמת **CRM**, **ERP** או **SAP** עשויים להוות מטרה אטרקטיבית במיוחד, מאחר ויש להם בדרך כלל גישה למידע עסקי מהסוג החיוני ביותר לארגון.
3. **מסדי נתונים** - "כספות" המידע הראשיות בארגון מהוות באופן טבעי מוקד משיכה לניצול פגמים באבטחת היישומים. התוקף עשוי לנסות ולחדור למערכות אלה על ידי ניצול פרצות ביישומי מסד נתונים או בתוכנות העושות בהם שימוש נרחב.
4. **שרתים שונים** - תוכנות שרת הן עוד מטרה אטרקטיבית, מאחר והן שולטות על פעילויות מרכזיות בארגון, בין מחשבים קריטיים. באמצעות תקיפת יישומים אלה ניתן לרגל ולהפריע לפעילויות עסקיות, ולמידע קריטי מסוגים שונים.
5. **יישומי אבטחה** - ישנם כיום וירוסים המנסים להגן על עצמם על ידי תקיפת יישומי אבטחה נפוצים. תוקף מתוחכם עשוי לעשות זאת באופן חכם במיוחד ולכן אין לשכוח שגם יישום אבטחה זקוק להגנה, לפחות ככל יישום אחר.

בין הנזקים האפשריים תמצא:

1. **גניבת מידע** - מידע עסקי קריטי עשוי להיגנב למטרות ריגול עסקי. מידע זה וכן מידע לקוחות פרטי עשוי להיגנב בכדי למוכרו לצד שלישי (דוגמת ספאמרים).
2. **שינוי ושיבוש מידע** - תוקף מתוחכם עלול לשבש מידע בצורה שתובחן רק לאחר זמן מה, אך תגרום נזק רב. דמיין למשל שינוי מחירים באתר קניות או שינוי יתרה בחשבון בנק.
3. **שיבוש הפעילות העסקית** - מטרה זו עשויה להתממש במגוון דרכים ובהם פגיעה במידע או שיבוש פעילות מערכות קריטיות בארגון.
4. **פגיעה במוניטין** - אתר **אינטרנט** ייצוגי פרוץ או משובש, מידע לקוחות קריטי שנמכר לספאמרים, שרותים המשובשים בגלל פעולות שחזור מידע שהושחת - לכל אלה, אם יתפרסמו, השלכות חמורות על תדמית החברה בציבור.
5. **שימוש פלילי במערכותיך** - מערכות הארגון עשויות להירתם ללא ידיעתך לביצוע פעולות שונות: קישור ל**אינטרנט** ינוצל לתקיפה מבוזרת (**DDoS**), קישור למערכות שותף ינוצל לשאיבת מידע מסווג שלו (המוצג רק לשותפיו), מערכת **CRM** תנוצל לשידור סמוי (ב**אינטרנט**) של מידע על לקוחותיך.

636.23– מרשמים להגנה

אלו גישות הגנת היישומים הנפוצות:

- **כיווני הגנה שבמסגרת היישום** - צמצום אפשרויות הפעולה של היישומים, רק לאלה שבאמת נחוצים מבחינה עסקית, יצמצם את סכנת ניצולם לרעה.
- **עדכוני ותיקוני אבטחה** - כיום ברורה לכל חשיבות עדכוני התוכנות, אשר מתחלקים לשניים: עדכוני תוכנה כלליים (כולל שיפורי אבטחה) ותיקונים (**Patches**) המתייחסים לתקלות אבטחה ספציפיות שזוהו. עדכון אוטומטי מומלץ.
- **הגבלת גישה** - ניהול גישה ליישומים, למשל עם עזרים כמו **BEA WebLogic Enterprise Security** (**ליעם ☎ 03-7677977**), מהווה עוד נדבך להגבלת שימוש לרעה ביישום.
- **ניטור פעילות היישום** - פתרונות ייעודיים לאבטחת יישומים יודעים לבודד יישום ב"ארגז חול" וירטואלי. מצב זה מאפשר לנטר ובמידת הצורך לבלום כל פעילות שלו.
- **ניטור תקשורת** - בדיקת תוכן התקשורת בין היישום לסביבתו עשויה לחשוף פעילות חשודה. זה יכול להתבטא במבנה תקשורת לא סטנדרטי (לא תואם את הפרוטוקול המדובר) או בתוכן חשוד, במידע הנשלח על גבי אותו פרוטוקול תקשורת.
- **בדיקות אבטחה יזומות** - כלי עזר נוסף בהגנת היישומים הן סריקות ותקיפות בדיקה יזומות. אלו חשובות במיוחד מאחר וביכולתן לגלות פרצות ונקודות תורפה שאינן מכוסות ושלא היו מתגלות אחרת.

PCאון© למנהלים ומשתמשי מחשב בכירים

636.31 – זה משתלם ?

הערכת הצד הכלכלי של אבטחת היישומים היא לכאורה פשוטה: המחיר הוא הנזק המשוער כפול הסיכוי להתממשותו. אלא שטווח הנזקים בהם מדובר כאן רחב ביותר ואינו ניתן בקלות לכימות, וודאי לא במספרים המתאימים לכל ארגון. הערכה אינדיבידואלית כזו מציעים יועצי אבטחה כ**סנקטום**, שתנתח עבורך עלות חדירה מול ה-**ROI** שבהשקעה בפתרונות. הערכות **גרטנר** מדברות על כך שמכל הארגונים שנמצאו חשופים להתקפות ברשת, ב-75% הפרצות נמצאו ברמת היישום.

בכל מקרה ניתן לומר שמדובר מחד בנזקים שהם פוטנציאלית קריטיים מבחינה כלכלית (כשיבוש פעילות הארגון או פגיעה חמורה בתדמיתו). מאידך, הפתרונות אינם יקרים ביחס לחשיבותם. הם מתחילים מצעדים זולים ביותר של מיצוי יכולות אבטחה קיימות ביישומים המדוברים ובפתרונות הגנה שכבר ברשות הארגון. דוגמא ממחישה "מהחיים": לאחרונה הותקפה חברה מקומית בולטת דרך אתרה, המבוסס בסיס נתונים, עליו ניתן היה להריץ שאילתות ללא הרשאה מתאימה. מעבר לנזק הכלכלי שלא נחשף, הנזק הפוטנציאלי למוניטין יכל להיות כבד ביותר. ראה עוד בידיעה **636.51**.

הסיכוי לפגיעה אם נמנעים מהגנה גדול ביותר - ממרואיינים שמענו כי עד 80% מיישומי ה**אינטרנט** הם בעלי בעיות אבטחת מידע חמורות. כך גם הנזק: תולעי ה**אינטרנט** **Blaster** ו-**Sobig** הצליחו להביא ביחד לנזקים בהיקף של שני מיליארד דולר!

636.32 – מעבר לטריוויאלי

עקוב אחר שיקולים מיוחדים אלה, לבחירת פתרונות הגנת יישומים שיתאימו לארגונך:

1. **חפש נציגות מקומית** - בתחום ייחודי זה, החברות מעטות והתמיכה הטכנית היא לרוב עניין דחוף. לכן חשוב ביותר למצוא חברה בעלת נציגות מקומית. החדשות הטובות הן שלחברות ישראליות מקום של כבוד בתחום.
2. **התחשב בתאימות** - וודא שהמוצר תואם לסביבות הארגוניות בהן הוא יעבוד. חשוב במיוחד לשים לב לתאימות מול מוצרי אבטחה אחרים, דוגמת **Firewalls**.
3. **שים לב ליכולות מיוחדות** - בדוק אם החברה מתמחה או מתמקדת במוצרים או בסביבות מסויימות. לדוגמא: מוצר הדגל של **Lucid Security** - **ipANGEL** הוא מוצר הגנת יישומים העובד רק עם ומשלים את **Firewall-1** של **CheckPoint**. ב- www.lucidsecurity.com
4. **חפש קלות שימוש** - פתרון פשוט וקל לשימוש (כולל בסביבה ארגונית מרובת מחשבים), יטיל עומס מינימלי על מערך האבטחה שלך (שממילא מורכב למדי).
5. **וודא דיווח מפורט** - חשוב שהמערכת תהיה מסוגלת לספק דיווחים מפורטים במקרה של תקלה. בנוסף, וודא שבפעילותה השוטפת היא יודעת לייצר קבצי **Log** מפורטים ונוחים ל"פיענוח".

דגש – טביעת אצבע ליישום

ביומטריה עשויה לתגבר כל מערכת אבטחה ברמת ביקורת הכניסה, וניתן לנצל זאת גם להגנת יישומים. בתחום רחב זה כבר ישנם פתרונות בשלים וזולים כמו זיהוי טביעת אצבע. אמינותם אינה מוחלטת וכבר הודגמו שיטות להטעייתם, אך התקן כזה יוסיף בכל מקרה קו הגנה נוסף, יעיל ויוצא דופן. ראה עוד בתחקיר **531**.

636.33 – מי ה"תותחים" ?

בין מוצרי ההגנה הבולטים שלרשותך, (לפי א'-ב'):

- **פינג אן** - **Vital Security** הוא פתרון הגנה כולל לכל יישומי **אינטרנט** של הארגון, כולל **E-Mail**. **SurfinGuard Pro** מגן מפני נוזקה בלתי מוכרת המגיעה מה-**E-Mail** ומה**אינטרנט** בכלל. זאת על ידי ניטור פעולות יישומים ב"ארגז חול" וירטואלי. **SurfinShield Corporate** עושה זאת כפתרון ארגוני. ☎ 09-8659440.
- **Network Associates** - מציעה את סדרת **Entercept**, בגירסאותיה השונות, המאפשרות הגנה על יישומים ארגוניים - כולל שרתי רשת ומסדי נתונים. לפרטים ☎ 09-7643585 .
- **פנדה** - חבילת האנטי-וירוס **פנדה טיטניום 2004** כוללת גם מערך הגנה על היישומים אשר "מאתר ומתקן נקודות תורפה בתוכנות המותקנות במחשב". בדרך זו מונעת התוכנה ניצול פרצות במוצרים שונים ע"י וירוס. ☎ 09-8859611.
- **צ'קפוינט** - מוצר הדגל שלה - **Next Generation**, משלב **VPN**, **Firewall** ופתרון אבטחת יישומים בשם **Application Intelligence**. כלי חדש זה יודע להגן על היישומים מפני התקפות ידועות, אך גם מאפשר להגדיר את סוגי התקשורת המקובלים ברמת האפליקציה והתוכן - ולא רק ברמת המקור וה-**Port**. המחיר תלוי במספר הכתובות עליהן התוכנה מגינה והוא מתחיל מ-**$3,000**. עדכון לשנה יעלה **$1,000** לכל **Site**. לפרטים נוספים ☎ 03-7534555.
- **Aliroo** - **PrivaWall** (החל מ-25 משתמשים ב-**$3,750**) הוא שרת, היכול להיות שרת **Gateway** או **PlugIn** לאאוטלוק. הוא מבצע הצפנה, סינון תכנים, אנטי וירוס וחתימה דיגיטלית. **PrivaWall** מאפשר להגדיר חוקים מורכבים (כמו: אם גורם מסוים שלח בשעה מסויימת מסר מסוים, הצפן אותו ושלח למקום אחר). **Secure Sentry Pro** מאפשר להגדיר במחשבים מסויימים אילו יישומים יעבדו ואילו לא (**$125** כולל **Token**). החברה מציעה גם שרות **E-Mail** מאובטח. ☎ 03-6345552.
- **Application Security** - מציעה פתרונות ארגוניים שונים להגנת יישומים ובכללם פתרון להערכת מצב אבטחה היישומים, פתרון הצפנת בסיסי נתונים ומערכת להגנת בסיסי נתונים. ב- www.appsecinc.com
- **FaceTime** - מציעה מוצר ייעודי להגנת יישומי **P2P** ומסרים מידיים. יישומים מסוג זה מותקנים בארגונים רבים ללא פיקוח ומהווים סכנה של ממש, אליה לא מתייחסים פתרונות נפוצים - www.facetime.com
- **Quadrasis** - **EASI Security Unifier** מספק מעין פתרון אינטגרציה למערכות אבטחה קיימות בארגון, ובכך משפר את אבטחת היישומים, על בסיסי הפתרונות הקיימים. לפרטים נוספים - www.quadrasis.com

עוד יסייעו לך בייעוץ לנושא חברות כגון **IBM Global Services** (☎ 03-5313558) ו**תים** (☎ 03-9278444).

636.41– מה מציעים ?

ממומחים שמענו על אבטחת יישומים:

נפתלי קרן, מנהל אזור המזה"ת ב**צ'קפוינט** (☎ 03-7534555) אומר כי הם רואים עליה כמעט אקספוננציאלית בשנים האחרונות בהתקפות. ברוב הארגונים ישנה אבטחה הקפית עם **פיירוולים** שידעו עד היום לטפל בהתקפות ברמת הרשת. מאחר שרוב ה**פיירוולים** כבר חוסמים התקפות אלו, התוקפים נהיו מתוחכמים יותר ומכוונים כעת את התקפותיהם יותר כלפי היישומים. בו בזמן, בארגון הממוצע ישנה שורת מערכות חשופות, דוגמת שרתי **E-Mail**, שרתי **FTP**, משתמשי שיתוף קבצים או מדפסות משותפות. **נפתלי** ממליץ להיות מודע קודם כל למה שקורה בארגון - למשל אם מישהו משתמש ב-**Kazaa** ברשת, ולדעת לטפל בזה כמו שצריך. השימוש ביישומים מתרחב וצריך להיות מודעים לסכנות ולמשמעויות.

עמית ברקן, מנכ"ל **סנקטום ישראל** ו**עמית קליין**, דיירקטור אבטחה ומחקר (☎ 09-9586077) מציגים את המיתוס מול המציאות: המיתוס אומר שאם יש באתר אמצעי הגנה בסיסיים כ-**Firewall**, הצפנה ומדיניות פרטיות, האתר בטוח. בו בזמן, על אף התרבות מוצרי האבטחה מסוג זה, מספר הפריצות גדל והולך כל שנה. מעבר לכניסת ה-**XML** כחידוש שישפיע על תקיפת והגנת יישומים, מצפים שהשנה ובוודאי בהמשך, זו תהיה שנת שרותי ה-**Web**, ושם יצטרכו לתת פתרונות מתאימים. זה הוא תחום המציב אתגרים חדשים. אם ברמת המשתמשים שם המשחק יהיה **XML** ושרותי וב, הרי שברמת המוצרים תהיה אינטגרציה עם מוצרים נוספים. לקוחות רוצים לראות פחות קופסאות וניהול אחיד. המלצתם למנמ"רים: לכל הפחות הזמינו בדיקה שתיתן תמונת מצב לגבי מצבכם.

ארנסט קציר, מנהל פיתוח עסקי ב**קומסק** (☎ 03-9234646) ממליץ בכל פיתוח או הטמעת מערכת מידע, לתת את הדעת לאבטחת המידע ברמת היישום, להגדיר אחוז תקציב מסוים שילך לכך, ולהקפיד לשלב אבטחת מידע בכל שלבי פיתוח המערכת. ב**קומסק** רואים התחזקות לאבטחת מערכות וארגונים מתחילים להבין שיש כאן בעיה אמיתית, המצריכה משאבים משמעותיים. לדעתו יותר ארגונים ישקיעו בעתיד בנושא זה. עם זאת, הוא לא רואה פריצת דרך ברמת מוצר ההולך לפתור את כל הבעיות האלה, בגלל אתגר ריבוי הפלטפורמות, הסביבות והאיומים.

636.42– מומלץ בחום

ישם טיפים אלה לשיפור אבטחת יישומים בארגונך:

- **בדוק פרצות** - ישם בדיקות קבועות לאיתור פרצות ביישומים. ראה למשל בדיקות דוגמא באתר חברת **פינג'אן** - www.finjan.com/mcrc/sec_test.cfm
- **עדכן ביעילות** - חיוני ביותר לעדכן בהקפדה יישומים וכן את יישומי התשתית עליהם הם רצים (מערכות הפעלה, שרתי **אינטרנט**). העזר ככל הניתן במנגנוני עדכון אוטומטיים של היצרן.
- **הורד כלים מספקי היישומים** - רבים מספקי היישומים הארגוניים דוגמת **מיקרוסופט**, **SAP** ואחרות, מציעים להורדה באתריהם כלים המסייעים להגנה על יישומיהם באמצעות איתור הגדרות מסוכנות, עדכונים חסרים, פורטים פתוחים או חריגות בשימוש השוטף.
- **התמקד במרכז** - מומלץ להקפיד במיוחד על אבטחת מערכות פנים ארגוניות ברמת היישום. לרוב, הן אלה שמחזיקות את המידע העסקי הקריטי ביותר. ומהיבט אחר: ידוע כי האיום על אבטחת הארגון חזק יותר מבפנים מאשר מתוקפים חיצוניים.
- **התרחק מהמסוכנים** - צמצם ככל הניתן בשימוש ביישומים הידועים כמסוכנים. לדוגמא: יישומי שיתוף קבצים או תוכנות מסרים מידיים בגרסאות בסיסיות או ללא הגנות מיוחדות להם.
- **שאלת הקוד הפתוח** - יישומי קוד פתוח הם אופציה שארגונים רבים שוקלים כיום. האם אבטחת יישומים אלה שונה? לא בהכרח, אך כדאי לשים לב לנקודה זו: הקוד הפתוח זמין לעיון תוקפים באשר הם, אך בה במידה לעיון ישיר של מפתחים ומשתמשים רבים (הרגילים "לרדת לקרביו" לשם פיתוח אישי, ובכך לחשוף פרצות שונות). לכן, עדיף לשפוט כל יישום לגופו - לפי מדיניות העדכונים והיסטוריית הפריצות.

636.43– המסלול הבטוח

עקוב אחר צעדים אלה להגנת היישומים בארגון:

1. **התייעץ במומחים** - מאחר ומדובר בנושא אבטחה "בלתי שגרתי" מבחינת רוב הארגונים, מומלץ מאוד להתייעץ עם מומחים. אלה יסייעו לך לנתח את השלכות הנושא לארגונך ולהציג את הפתרונות האפשריים (אם כי שים לב שהם עשויים להיות ספקי פתרון מסויים אחד בלבד, שלכיוונו יהיו "משוחדים" במידה מסויימת.
2. **מפה** - מפה את היישומים העיקריים שבשימוש הארגון. מהם היישומים הסטנדרטיים המותקנים בדסקטופ הממוצע? היישומים המיוחדים שבשימוש גורמים בודדים (אנשי פיתוח, הנהלת חשבונות), יישומים ארגוניים שבשימוש נרחב (**SAP**, **CRM**, **ERP**)?
3. **הערך מידת הסיכון** - הערך את הסיכון בפניו ניצב היישום. האם הוא מתחבר ל**אינטרנט**? מה ביכולתו לעשות ולמי הרשאות לכך? עד כמה היישום מוכר ומהווה מטרה מקובלת לחושפי פרצות ולמנצליהן?
4. **קבע הגבלות** - שאל עצמך עד כמה חיוניות יכולות שונות של היישום ועד כמה ניתן, בהתאם, להגבילן. עד כמה ניתן להגביל משתמשים בהרשאות גישה ופעולה במסגרת היישום? קבע הגבלות גם בעזרת תכונות האבטחה המובנות ביישום עצמו.
5. **שקול פתרונות ייעודים** - מעבר לאמצעים בסיסיים אלה, ישם פתרונות משלימים. מוצרים תמצא ב-636.33. הגנה על יישומי **Web** - 636.51. פיתוח - 636.52.
6. **בדוק ושמור לאורך זמן** באופן שוטף, הקפד לבדוק שכיווני האבטחה השונים בתוקף, שמערכות האבטחה פועלות היטב וששיישומים אינם מתווספים למערכת ללא ידיעה והגנה מתאימה.

636.51– החורים ברשת

כיום כשאינטרנט הפכה לכלי עסקי מרכזי בארגונים, לכל הפחות ברמת הגלישה מהדסקטופ הממוצע, אבטחת יישומי האינטרנט נעשית חשובה במיוחד.

מ**סנקטום** שמענו כי ה-**FBI** מעריך ש-91% מהארגונים מותקפים בהתקפות ממוחשבות, 64% מכירים בכך שהם סובלים מהפסדים כספיים עקב כך ו-70% מודעים לכך שאתרם הוא נקודת התקיפה. **סנקטום** ביצעה כאלף בדיקות אתרים, ומסקנותיה הן: 98% מהאתרים הם בעלי נקודות תורפה. 21% חשופים לגניבת מידע ולשליטה מלאה. 27% מציגים סיכון כלשהוא לפרטיות מידע וב-32% מהם ניתן לגנוב זהות משתמש אחר. לדבריהם, חשוב לזכור שאתה חשוף למספר רמות פגיעות: ברמת יישומי התשתית של האתר, ביישומי צד שלישי שבשימוש ובפרצות יישומים שיצרו המתכנתים שלך. אפשרויות ניצול לרעה של המצב כוללות כבר עכשיו שינוי או העתקת קבצים אליהם יש גישה מהיישום, השחתת אתר, חסימת הכניסה אליו ועוד.

בארץ החקיקה בעניין אבטחת יישומים ב**אינטרנט** עדיין לא מפותחת. עם זאת, כדאי לבדוק אם ישנם חוקי אבטחה מיוחדים, העשויים להיות רלוונטיים בארצות אחרות, מהן יש לך קונים (או שותפים) מקוונים רבים.

במבט לעתיד הקרוב, נציין כי ב-**XML** ו-**Web Services** גלומים סיכוני אבטחה פוטנציאליים חדשים ובהם: סטנדרטים לנושא אבטחה שעדיין לא גובשו במלואם, עולם ה-**XML** הדורש גישות אבטחה חדשות והעומס שאבטחת שרותי **Web** תטיל כנראה על רשתות.

בין המומחים ל-**Web Application Security**:

- **סנקטום** - **AppShield** (**$15,000**) מזהה התקפות ובולם אותן, בכך שהוא מבין מה הקלט החוקי ליישום ומאפשר רק אותו. זה הוא פתרון המבודד את היישום מהעולם החיצון. **AppScan**, שמחירו כמה אלפי דולרים, מאפשר לבדוק אבטחת יישום **Web** לפני פריסתו. הוא מדמה משתמש ומאתר פרצות בשימוש בו. **AppAudit** הוא שרות בדיקה של החברה. ☎ 09-9586077.
- **NetContinuum** - מציעה התקן הגנת **Port 80** - כניסה ממנה מגיעות התקפות רבות. נציין כי פתרונות **Firewall** לא בודקים זאת, אלא רק חוסמים או מאפשרים את ה-**Port**. - **www.netcontinuum.com**
- **KaVaDo** - מספקת סורק בשם **ScanDo** (ממספר אלפי דולרים בודדים עד כעשרים אלף) ו-**InterDo** (**$15,000**) - מעין "**Firewall** יישומי" שמבודד את היישומים ברמת התקשורת, המשתמש והפלטפורמה ומונע ניצולם לרעה. **קומסק** ☎ 03-9234646.

636.52– איך תסייע למפתחים ?

כיצד תפתח נכון? מ**קומסק**, שמענו כי אין כלים בולטים המסייעים לכך תוך כדי הכתיבה, אך יש מה לעשות: בשלב התכנון חשוב על השלכות האבטחה וקבע פתרונות מתאימים, בשלב הכתיבה ישם היטב את פתרונות האבטחה והימנע ככל הניתן מבאגים בנושאים קריטיים, שים לב לצמצם פעילויות יישום שניתן לנצלן לרעה - דוגמת פתיחת שערים רגישים, גישה ישירה למידע קריטי, או תכנות ב-**Low Level**. בבדיקות תן דגש על נושא האבטחה: בדוק סוגי קלט לא חוקיים ומזיקים באופן פוטנציאלי, בדוק כיצד מגיבה המערכת לניסיונות פריצה.

כמה כיוונים העשויים לסייע בפיתוח:

- **יועצים** - יועצי פיתוח עשויים להביא איתם מומחיות בשפת הפיתוח בה מדובר וכן בפיתוח לסביבה שלך או לתחום ספסציפי בו מדובר. חברת ייעוץ תוכל לסייע החל מתכנון אבטחת המוצר, דרך ייעוץ למפתחים לגבי פיתוח נכון, סקירת קוד קיים ובדיקות אבטחה.
- **כלי הגנה מוטמעים** - לדוגמא: **Soft Defender** הוא כלי עזר המוסיף לתוכנה הכתובה יכולות הגנה מסויימות, כנגד נסיונות "חיטוט" בקוד בעזרת **Debuggers** או גישות אחרות של **Reverse Engineering**. נסיונות אלה עשויים להניב "גרסאות בלתי רשמיות" של התוכנה שלך, כולל גרסאות עוקפות רשיון ("פרוצות") ואף גרסאות עם קוד מזיק נסתר (לדוגמא: קוד הגונב בחשאי מידע **Login** לסוגיו). המחיר: **$69**. - **www.softdefender.com**
- **לימוד עצמי** - התעמקות באספקט האבטחתי של התכנות ניתנת לביצוע גם באמצעות ספרים המתמקדים בכך. לדוגמא: **Secure Programming Cookbook for C and C++** (**$49.95**) - **www.oreilly.com/catalog/secureprgckbk**
- **בדיקות יעילות** - ב-2002 העריך ה-**National Institute of Standards and Technology** שבאגים בתוכנה עולים לכלכלה המקומית 60 מיליארד דולר וכי 22 מיליארד מכך ניתן היה לחסוך, בעזרת שיפור בדיקות התוכנה. מקובל שבכל תוכנה ישנה רמה סבירה מסויימת של באגים. סביר שחלק מהם ניתן יהיה לנצל למטרות זדוניות, אך יש לשאוף לצמצם סיכון זה למינימום.

636.53– להעמיק ולהרחיב

מקורות אלה יסייעו לך להרחיב בנושא:

- **The Open Web Application Security project** - **OWASP** הוא יוזמה לשיתוף ידע מצד מומחים ובעלי מקצוע בתחום יישומי **אינטרנט**, לקידום האבטחה ביישומים אלה. - **www.owasp.org**
- **20 הפרצות העיקריות** - ארגון האבטחה המעולה **The SANS Institute** מציע כשרות לציבור פרוט של 20 הפרצות הקריטיות ביותר ב**אינטרנט.** מומלץ מאוד להתעמקות ויישום. - **www.sans.org/top20**
- **אבטחת יישומים ובסיסי נתונים** - עוד תמצא באתר SANS סדרת מאמרים בנושא אבטחת יישומים ובסיסי נתונים. - **www.sans.org/rr/catindex.php?cat_id=3**
- **SearchSecurity.com** - ראה קטגוריית **E-Commerce Security** במסגרת אתר זה מבית **SearchTechTarget** - **searchsecurity.techtarget.com/whitepapersByCategory**
- **Security Forums** - אתר המרכז פורומים בנושאי אבטחה שונים. כאן תמצא התייחסות לתחומי יישומים ספציפיים, דוגמת **Exchange** ויישומי אלחוט, כמו גם לפיתוח בטוח. ב - **www.security-forums.com**