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?

גיליון 479 ● ● ● ● ● 4 דצמבר 2000

PCאון ©

למנהלים ומשתמשי PC בכירים

תדרוך מקצועי קצר ומרוכז • בחדשות ומידע שימושי "יחודי" • למיצוי ה–PC באופן מרבי

...והפעם... אבטח את מחשבך האישי

מסר אישי

וירוס נאבידד, שהצליח לפני שבועיים להפתיע מאות (ואולי אלפי) משתמשים ברחבי הארץ, הצליח להמחיש עד כמה כולנו פגיעים, וזאת למרות אמצעי ההגנה הסטנדרטיים. מתברר כי תוכנות אנטי וירוס או פתרונות ארגוניים, אין בהם די כדי להגן על המחשב האישי איתו אנחנו עובדים ולתת פתרון מלא.
מהן הסכנות האורבות כיום לתחנות הקצה? מהם הפתרונות ומהן הדרכים להתמודדות? את כולם תגלה - בתחקיר זה.

תמצית החדשות בעולם ה-PC

תוכן התדרוך השבועי

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק** B.Sc. ,MBA
עורך - **נמרוד צוק**
תחקיר וכתיבה - **יחיאל שלום**
טלפון - **03-9667939**, פקס - **03-9660310**
דואר - **ת.ד. 2340 ראשון לציון 75121**

לתשומת לבך

לכבוד **קומרקטינג ישראל**
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 $119 / $214 / $394 + מע"מ (סמן בחירתך בעיגול), לפקודת **קומרקטינג ישראל** ומחכה לגיליון הקרוב.

שם מלא _____

תפקיד _____

ארגון _____

כתובת _____ מיקוד _____

טלפון _____ פקס _____

תאריך _____ חתימה _____

הערות _____

PCאון© למנהלים ומשתמשי PC בכירים

479.11 – חדשות בקצרה

• **נתונים מפתיעים על מכירות ה-PC ברבעון האחרון של 2000, עשויים להצביע על מגמות חדשות.** בניגוד לתחזיות על גידול במכירות ה-**PC** באוקטובר, עקב החגים בארה"ב ואירופה, ירד היקף המכירות ב-18% לעומת השנה שעברה, לפי נתוני **NPD**. לפי נתוני **PC-Data**, ניכרה האטה מתמשכת במכירות מאז אמצע אוקטובר ועד אמצע נובמבר, של 17% - עד 28% - לעומת השבועות המקבילים אשתקד. עליה ניכרה במכירת מחשבים נישאים, **PDA's** וציוד היקפי מתוחכם כגון מסכים שטוחים ומצלמות דיגיטליות. יחד עם החלשות שערי המניות של חברות כמו **אינטל**, **דל** ו**גייטוויי**, ייתכן ואלו הסימנים הראשונים של התממשות תחזיות שנשמעות מפי מנהלים מובילים בענף, על "מות ה-**PC**".

• למתקפת הוירוסים שסקרנו בשבוע שעבר, נוסף עוד מזיק שהחל לצבור תפוצה בשבוע שעבר - הוירוס/תולעת **W32.MTX**. מלבד גרימת נזק לקבצי מערכת והפצה עצמית בדואר אלקטרוני, יש לוירוס זה תכונה ייחודית שעלולה לחשוף את נפגעיו לנזקים מוירוסים אחרים - הוא מונע גישה לאתרים של כמה יצרני אנטי וירוס, כך שלא ניתן להוריד עדכוני חתימות. קובץ תיקון תמצא ב - www.symantec.com/avcenter/venc/data/w95.mtx.html

• שיטה נוחה לשליחת דואר מאובטחת מציע שירות הדואר **Yahoo! Mail**. השירות, במשתמש בטכנולוגיה של **ZixIt**, מעביר את ההודעה (כולל קבצים מצורפים) דרך תקשורת מאובטחת לאחסון בשרת מוצפן, ממנו יכול הנמען למשוך ולפענח אותה רק לאחר זיהוי ודאי. הרשמה בכתובת - mail.yahoo.com

479.12 – העתיד על פי קנון

מספר פיתוחים עתידיים מעניינים הוצגו בתערוכת Canon Expo 2000. ביניהן בלטו טכנולוגיות תקשורת אלחוטיות כמו מצלמה דיגיטלית השולחת תמונות להדפסה באמצעות פרוטוקול **Bluetooth** וכרטיס רשת אלחוטי לחיבור ציוד היקפי למחשב.

בתחום העברת המסמכים הוצגו טכנולוגיה להעברת מסמך מודפס לנמען דואר אלקטרוני באמצעות מכשיר שסורק את המסמך ומעביר אותו דרך שירות ניתוב מרכזי; ומכשיר פקס מופעל בפקודות קוליות הכולל טלפון אלחוטי. עוד הוצגה מצלמה דיגיטלית הכוללת מדפסת מובנית שמאפשרת להוציא תמונה בגודל כרטיס ביקור, באופן מיידי.

הטלויזיה היתה במוקד שורת פיתוחים נוספת - התקן המאפשר קבלת מידע על התוכניות המוצגות דרך **אינטרנט**; טכנולוגיה המשלבת מחשב כף יד וכרטיסים חכמים לביצוע רכישות מקוונות דרך טלויזיה המחוברת ל**אינטרנט**; מדפסת להדפסת דפי **WEB** ממסך הטלויזיה, ומסך מיוחד לצפיה בתמונה תלת ממדית על גבי הטלויזיה.

479.13 – סופו של מודל החינם ?

האם המודל הדומיננטי של חברות האינטרנט - תכנים ושרותים בחינם - עומד לפנות את הבמה לטובת גביית תשלום ממשתמשים? הצהרת מנכ"ל **יאהו**! כי החברה שוקלת לגבות תשלום עבור חלק משירותיה, עשויה לסמן מפנה לכיוון זה. זאת לאחר ירידה במניות חברות **אינטרנט** רבות, שכשלו בהצגת רווחים ממכירת פרסומות או משרותי סחר אלקטרוני לצרכנים, שגררו פיטורי אלפי עובדים בחו"ל. גם בארץ מתחילים להראות סימני הקשיים הכלכליים - **גלובס** מדווח כי **ידיעות אחרונות** החליט לאחד את מערכת התוכן של **YNET** עם זו של העיתון, והוא שוקל פיטורי עשרות עובדים. כמו כן, עורך **YNET זאב חספר** ועורך **נענע גדי שמשון** החליטו לפרוש ממשרותיהם.

גם מודל הגישה ל**אינטרנט** בחינם תמורת צפיה בפרסומות אינו מחזיק מעמד, כך טוען **פורבס** - חברות המספקות שרותים כאלה בחו"ל נתונות בקשיים, וגם בארץ נותק לאחרונה הקשר של ספק החינם המקומי **סרפרי** למבואות 136 של **בזק**, דרכן התחברו משתמשיו, בשל חוב כספי שלא שולם (נדגיש כי השירות פעיל ומשתמשיו יכולים להתחבר דרך שרתים מקומיים).

479.14 – הפינגווין צועד קדימה

עוד כמה ידיעות מעניינות מתחום הלינוקס המתפתח:

• מחקר חדש של **Zona Research** צופה אימוץ נרחב של **לינוקס** בארגונים גדולים וחברות קטנות - כמחצית הנשאלים (109 מקבלי החלטות בתחום המחשוב) אמרו כי בארגוניהם כבר משתמשים ב**לינוקס** ליישומים כגון שרתי **WEB**, **E-Mail**, קבצים, הדפסה, **אינטרה-נט** או **Firewall**, אצל 38% משתמשים בה כשרת **Database** ו-21% מיישמים אפליקציות **E-Commerce**. יותר ממחצית הנשאלים מארגונים גדולים, צפו גידול של 25% במספר המשתמשים.

• דחיפה משמעותית לשימוש המסחרי ב**לינוקס** נתנה **IBM**, עם ההכרזה על מכירת 15 אלף שרתי **IBM** מבוססי **לינוקס** לחברת **Lawson** היפנית - עסקת ה**לינוקס** הגדולה ביותר מסוג זה שנחתמה עד היום.

• **Dell** תתחיל להציע את **Red Hat 7.0** כאופציה בכל קשת מוצרי ה-**PC** שלה - שרתים, תחנות ונייידים. הגרסה החדשה מציעה שיפורים למשתמשי הקצה בממשק המשתמש ובהתקנה, כמו גם התאמה טובה יותר לשרתים חזקים.

• גרסה 2.4 של ליבת **לינוקס**, שאמורה להביא קפיצת מדרגה בסקלביליות המערכת, צפויה לצאת במהדורה סופית בתחילת החודש הנוכחי - כך אמר מפתח המערכת, **לינוס טורוולדס**. בין השיפורים שהיא תציע - תמיכה רחבה ב-**USB**, ניצול יעיל של ריבוי מעבדים ומודול רשת חדש.

• התקדמות נוספת לקראת ביסוס **לינוקס** כמתחרה רצינית ל**חלונות** על המכתבה, התבצעה עם הכרזת גרסה 2.0 של הסביבה הגרפית **KDE**, הכוללת שיפורים רבים. עם זאת, היריבות בינה לבין הסביבה הגרפית המתחרה, **GNOME**, שמתחזקת בעקבות ייסוד קבוצת חברות התומכות ב-**KDE**, עלולה דווקא להוות מכשול בדרך למשתמשים.

479.21– תחנה קוראת לגנב

ברגעים אלה ממש, בשעה שאתה גולש באינטרנט, קורא דואר אלקטרוני או כותב מסמך וורד, ייתכן שמישהו - או משהו - חודרים למחשב שלך ללא רשות. זה יכול להיות וירוס מאקרו שהגיע עם מסמך **אופיס** תמים ועוסק בהרס שיטתי של הקבצים בדיסק הקשיח שלך בלי שתבחין בכך, תולעת שנשלחה אליך ב-**E-Mail** והחלה להפיץ עצמה למכריך או האקר ש"משחק" להנאתו במערכת ההפעלה שלך או מנצל את מחשבך כדי להשיג גישה למערכות מחשב רגישות בארגון.

תחנות הקצה הן החוליה החלשה ביותר באבטחת המידע: הן מפוזרות במשרדי הארגון ולא נעולות מאחורי סורג ובריח בחדר שרתים מוגן, כך שקל להגיע אליהן פיזית ולהוריד מידע רגיש לדיסקט או להחדיר וירוס הרסני; רובן מריצות את **Windows 9x**, מערכת הפעלה שחסרה אמצעי הגנה מספיקים ולרוב הן משמשות עובדים בעלי מודעות נמוכה לאבטחה שאינם מצוידים ביכולת לזהות פריצות או להתגונן מפניהן. כך במקרים רבים, ה"פרצה" היא בעצם המשתמש עצמו, שפותח הודעות **E-Mail** קטלניות ללא בדיקה או מוסר את ססמתו מבלי להיות מודע לכך, לאדם לא מוכר.

אינטרנט הפכה איתור קורבנות פוטנציאליים לפריצה או נקודות תורפה ברשתות ארגוניות, למשימות קלות בהרבה; הקלות בה ניתן להשיג כיום כלי פריצה מתוחכמים שאינם מצריכים כמעט ידע טכני, הביאה לגידול מהיר במספר הפורצים החובבנים. **E-Mail** הופך אמצעי התפשטות מהיר לוירוסים ותולעים, והופעת חיבורי ה**אינטרנט** הקבועים חושפת את התחנות גם לסכנת פריצה ישירה. איום נוסף הוא ניצול לרעה של מחשבים המחוברים ל**אינטרנט** כאמצעי להתקפות **Denial-Of-Service** או משלוח **SPAM**. התגברות השימוש במחשבים ניידים, שקל לגנוב ולפרוץ, כמו גם העבודה מהבית המצריכה פתיחת הרשת הארגונית לגישה מרחוק, מגדילות את הסיכון עוד יותר.

החדשות הטובות - גם יכולות המגננה משתפרות: הופעת מוצרי **Firewall** אישיים, תוכנות אנטי וירוס המשלבות טכנולוגיות חדשניות לאיתור וירוסים מוקדם, מערכות הפעלה חסינות יותר לתחנות הקצה, כגון **Windows 2000** ו**לינוקס**, מערכות התרעה על פריצות (שוק שגדל פי 4 בין 1997 ל-1999) ואמצעי אבטחה ביומטריים שהופכים לאופציה מעשית, יסייעו כולם למנהל לצמצם את הסכנות מתחנות הקצה.

<u>לסיכום - רק דאגה לאבטחה ראויה של תחנות הקצה בארגון, תבטיח כי ההשקעה הגדולה באבטחת הרשת והמערכות הקריטיות, לא תרד לטמיון.</u>

479.22– מסדר זיהוי

את הפרצות בתחנה עשויים לנצל מגוון תוקפים:

- **וירוס** - אבי כל המזיקים, ה"מדביק" קבצי הפעלה למחייתו. שמותיהם יתחילו לרוב ב-**W95**, **W32** או **WNT**.
- **תולעת** - וירוס שוכן זיכרון, המשכפל עצמו ב"זחילה" ברחבי הרשת ועשוי לכלול גם קוד מזיק. בנוסף לשימוש באנטי וירוס שתומך בלקוח ה-**E-Mail** ומבצע ניטור ברקע, חשוב לנקוט זהירות בפתיחת הודעות **E-Mail** (ראה 479.51).
- **וירוסי מאקרו** - וירוסים המנצלים את התפוצה הנרחבת ויכולות הפיתוח החזקות של יישומי **Office**. שמותיהם יתחילו ב-**WM**, **W97M** (**Word**), **XM** / **X97M** / **XF** (**Excel**) או **AM** ל-**Access**. הפעלת ההגנה הפנימית של **אופיס** בשילוב אנטי וירוס מתאים יסייעו - אבל בשל קצב הופעת וירוסים ווריאנטים חדשים, אנו ממליצים להגביל את השימוש בקבצי **DOC** לעבודה מקומית ולהעדיף פורמטים בטוחים כגון **RTF**, **PDF** או **HTML** להפצת מסמכים לאחרים.
- **טרויאנים** - מזיקים כמו **Back Orifice** מסווים עצמם כתוכנה בלתי מזיקה, בשעה שלמעשה הם שותלים "דלת אחורית" שתאפשר לפורצים להיכנס למחשב בקלות ולעשות בו כרצונם. הגנה טובה תשלב **Firewall** ואנטי וירוס.
- **פורצים** - יכולים לתקוף את המחשב על ידי גישה פיסית או דרך **אינטרנט** - החל מהתקפות **Denial of Service** ועד לטכניקות **Buffer Overflow** להשתלטות על המערכת.
- **ונדלים** - טכנולוגיות **Java** ו-**ActiveX** מהוות בסיס נוח לקוד עוין בדפי **WEB** והודעות **E-Mail**.
- **מתיחות** - "אזעקות שווא" על וירוסים מדומים וסכנות מפוברקות נפוצות ב**אינטרנט** בשפע, והן יכולות לגרום נזק עקיף על ידי יצירת פאניקה מיותרת ובזבוז משאבים.

479.23– הכן מחשבך לחורף

מה עליך לעשות בכדי להגן על התחנות כראוי?

1. **ברר היכן אתה עומד** - דאג לכלול את תחנות הקצה בסקרי סיכונים והדמיות חדירה. לבדיקת רמת האבטחה של מחשב בודד, תוכל להיעזר באתרים כגון **Shields UP!**, שמחפש פרצות ומדווח לך עליהן - grc.com/su-help.htm
2. **מדיניות, מודעות ונהלים** - כלול התייחסות מפורטת לתחנות הקצה במדיניות האבטחה הארגונית, דאג ליצירת נהלי אבטחה ברורים לשימוש ב-**PC** והקפד "לחנך" את העובדים לקיימם ולהיות מודעים לסיכונים.
3. **בחר תוכנה בחכמה** - מערכות הפעלה חסינות כגון **NT**, **Win 2000** או **לינוקס**, כמו גם פתרונות "לקוח רזה", יהפכו את סביבת התחנה למוגנת יותר. מעבר לכך, חשוב לבדוק היבטי אבטחה בבחירת תוכנות **אינטרנט**.
4. **מנע מחדל בבריות המחדל** - דאג לכוונן את הגדרות האבטחה של מערכות ההפעלה, הדפדפנים והיישומים, ואל תסתפק בברירות המחדל. ראה 479.42 ו-479.52.
5. **הפעל כלי הגנה** - הקפד על אנטי וירוס שרץ תמיד ברקע ובדיקות תקופתיות עם שתיים-שלוש תוכנות. בנוסף, מומלץ להתקין בתחנות **Firewall** אישי (ראה 479.31).
6. **עדכן והתעדכן** - דפדפנים, מערכת הפעלה, יישומי **Office** ותוכנות אנטי וירוס - לכולם יוצאים עדכוני אבטחה, שחשוב להתקין. חשוב לא פחות להשאר מעודכן באיומים ובפתרונות האחרונים. **iALERT 2.0** תסייע בכך - www.idefense.com
7. **שמור על המידע** - מידע רגיש עדיף לאחסן במקום בטוח - על שרת קבצים מאובטח, נגיש רק למי שבאמת צריך אותו. דאג שהמשתמשים לא יוציאו מידע כזה מהארגון בדרכים לא מאובטחות, והשתמש בהצפנה חזקה במקרה הצורך.
8. **אל תשכח את הגיבוי** - לכל צרה שלא תבוא, חשוב לבצע גיבוי תכוף של כל הנתונים והמסמכים החשובים, ועדיף של המערכת כולה - ובכל מקרה להכין דיסקט הצלה.

479.31– חליפה חסינת אש

ישנם מקרים בהם ה-Firewall הארגוני אינו מספיק - למשל בתחנות **Stand Alone** המחוברות ל**אינטרנט** באופן עצמאי (במיוחד דרך חיבור **DSL** או חיבור כבלים קבוע), במחשבים שמשמשים עובדים לעבודה מהבית או ביניידים. כדי למנוע ממחשבים אלה להפוך קרש קפיצה לרשת הארגונית להאקרים, כדאי להשתמש ב-**Firewall** אישי. מספר מוצרים קיימים בשוק:

- **BlackICE Defender** - מוצר ייחודי שמאתר וחוסם נסיונות חדירה על ידי זיהוי דפוסי תקשורת אופייניים לסוגי התקפות מוכרים. יכול לשמש באופן עצמאי או כהשלמה ל-**Firewall**. **$39.95** - www.networkice.com
- **InfoExpress CyberArmor Firewall** - אישי בשל המתאים במיוחד להגנת תחנות ניידות, כולל אפשרות ניהול מרכזי - www.infoexpress.com/products/pf/
- **Mcafee Personal Firewall** - **Firewall** אישי שניתן לשכור כשירות, בהתקנה דרך הדפדפן, או להתקין כמוצר מדף. גרסת התנסות ל-10 ימים - www.mcafee.com
- **Symantec** מציעה את **Desktop Firewall 2.0** המיועד להגנת מחשבים ניידים ותחנות מרוחקות המתחברות לרשת הארגונית בגישה מרחוק. כן היא מציעה את **Norton Personal Firewall 2001** להגנת תחנות בודדות, וכן את **Personal Security 2001** הכולל גם אנטי וירוס וחסימת פרסומות. www.symantec.com או ☎ 09-7438850.
- **Sygate Personal Firewall** - מאחורי הממשק המעוצב של מוצר זה (חופשי לשימוש אישי) מסתתרת יכולת הגנה בסיסית שקופה למשתמש, ושפע אפשרויות התאמה מתקדמות - www.sygate.com/products/shield_ov.htm
- **ZoneAlarm Firewall** - אישי פופולרי, חופשי ופשוט לתפעול של **Zone Labs**. מאפשר לבחור רמת אבטחה, לשלוט בגישת יישומי לקוח ושרת ל**אינטרנט** ולנעול את החיבור לאחר שהמערכת אינה בשימוש זמן מסוים. הוא גם מגן מפני תולעי **E-Mail**. גרסת **Pro**, במחיר **$39.95**, מאפשרת שליטה גמישה יותר, דיווח מורחב ותמיכה משופרת ברשתות. הכתובת - www.zonelabs.com
- **Gnat Box** - מציעה מוצרי **Firewall** שונים בחומרה ותוכנה. תוכל להתרשם מגרסה חינם ל-5 משתמשים הזמינה מ-www.gnatbox.com. **קומארט** ☎ 08-9773838

479.32– מחסלי הוירוסים

האנטי וירוס דורש רענון? תוכל לבחור בין:

- **AVG 6.0** - תוכנת אנטי וירוס בעלת תוי תקן של **ICSA** ו-**Virus Bulletin**, הניתנת חינם לשימוש אישי (כולל עדכונים). להוריד ב - www.grisoft.com
- **InoculateIT CA** מוצע בחינם לשימוש אישי (antivirus.cai.com) והוא מציע גילוי היוריסטי, התאמה ל-**PALM**, עדכון נוח, משלוח התרעות ב-**E-Mail**, וניהול מרכזי לטיפול בתחנות. מחירו ההתחלתי **$39** לתחנה, למינימום של 30 משתמשים. **CA** - ☎ 03-7661313
- **סימנטק** מציעה את **Norton Anti Virus** הותיק, המספק עדכונים אוטומטיים. קובץ נגוע מועבר ל"אזורי הסגר" בתחנה, משם הוא יועבר לשרת וממנו ל**סימנטק**.
- **McAfee - VirusScan** הוא אנטי וירוס וותיק ומוביל. בין תכונותיו החדשות "תחנת הסגר" לבידוד קבצים חשודים. להשיג מ**צ'יפ שיווק** - ☎ 03-9585588.
- **F-Secure** של **Data Fellows** כולל את **CounterSign**, פיתוח של החברה המאפשר שילוב של מוצרי אנטי וירוס שונים לסריקה משותפת. **רנסנס** - ☎ 09-7643567.
- **Trend Micro** מציעה אנטי וירוס לתחנות בשם **OfficeScan Corporate Edition** ב-**$900** למאה משתמשים. בדיקת וירוסים מקוונת, בחינם, תמצא ב - housecall.antivirus.com. **חילן** - ☎ 03-6874555.
- **InVircible** של **נץ מחשוב** הוא אנטי וירוס גנרי. (**$47** עד 10 תחנות). ☎ 03-9386868.
- **eSafe Desktop** כולל מודול אנטי וירוס ומודול **sand box** להגנה גנרית. לתוכנה גם ממשק עברי ומחירה **$39** לתחנה, עם תמיכה טכנית לשנה. **אלדין** ☎ - 03-6362222.

479.33– רשת ביטחון

באבטחת מידע - ההגנה הטובה ביותר היא הידיעה:

1. ארגון **CERT** מספק התרעות שוטפות על איומים, הדרכה בנושאי אבטחה למיניהם, איסוף דיווחים מהציבור על פגמי אבטחה בתוכנות ועוד - www.cert.org
2. **ZDNet** מציע עדכונים שונים לתוכנה וחומרה ובדיקת עדכניות מקוונת - www.zdnet.com/enterprise/security
3. **ICSA** הוא ארגון הבודק במעבדותיו מוצרי אבטחה. תוכל למצוא רשימות מוצרים "מאושרים" על ידם, התראות, מאמרים, קישורים ועוד - www.icsa.net
4. באתר חברת **ISS** תמצא מקור מסודר ביותר לחדשות בתחום, "ספרייה" הכוללת מצגות, קישורים ועוד, ואפילו חידון אבטחת רשת מקוון - xforce.iss.net
5. אתר האבטחה של **מיקרוסופט** מציע מידע אבטחה כללי. כמו כן מוצעות המלצות ועדכונים לתוכנות **מיקרוסופט** השונות - www.microsoft.com/security
6. בדיקות אבטחה מקוונות תוכל למצוא אצל **סימנטק**, בכתובת - www.symantec.com/securitycheck
7. חדשות על וירוסים, "מתיחות" (**Hoaxes**) ועוד, ארכיב תוכנות הצפנה, מדריך אבטחה ופורום תמצא ב-**SECURITYPORTAL** - www.securityportal.com
8. ב-**AntiOnline** תוכל להציג שאלות ל"ייועץ" מקוון ולקרוא חדשות והסברים מפורטים, המתמקדים בעיקר בהתגוננות מהאקרים - www.antionline.com
9. חדשות עדכניות בנושא, מאמרים שונים ועוד, תמצא גם בחלק האבטחה של **Planet IT** - www.planetit.com/techcenters/security
10. **Firewall.com** מציע תקציר חדשות, פורומים ובעיקר קישורים רבים מסודרים לפי נושא - www.firewall.com
11. הפניות למוצרי **Firewall** אישיים, למידע ולכלים נוספים תמצא באתר ה"האקרים הלבנים" - www.happyhacker.org/defend/index.shtml
12. בעברית תוכל להסתייע בספר "**פריצה! לא במחשב שלי!**" - 89 ש"ח אצל **הוד עמי**, ☎ - 09-9564716.

479.41– רשמים מ"שדה הקרב"

מה אומרים המומחים? להלן רשמים ועצות ששמענו:

אהוד אבנר, מנכ"ל **Info-Fort** (☎ 03-9696837) ממליץ להשתמש בשומר מסך + סיסמא כשהעובד עוזב את התחנה פועלת, ובסוף היום, כשמבוצעת תחזוקה והעובדים אינם. **אהוד** ממליץ לקבוע במדיניות שכל מידע רלוונטי יישמר בשרת, ולא בתחנות. לדבריו, עוד לא הגענו לגל וירוסים העשוי להתפתח סביב נקודות התורפה של **חלונות 2000.**

גיא אלפסי, סמנכ"ל טכנולוגיות ב**קומסק** (☎ 03-9234646), מציין כי משתמשים נוטים להתאים תחנות לנוחותם, דבר שעלול להתנגש עם אינטרס האבטחה, וליצור בעיות שעל קיומן והיקפן ההנהלה לא יודעת. דוגמא אופיינית היא חיבור מודם העוקף את ההתקשרות המאובטחת דרך השרת. לדבריו, יש הטועים ומתמקדים באבטחת השרת, בתור "הקשר לעולם החיצון", מבלי להתייחס מספיק לתחנות.

נעמי אברמסון ו**שי חיימוביץ'** מ-**DataSec** (☎ 03-6128010) אומרים כי האבטחה החזקה ביותר היא מודעות העובדים. בנוסף, הם ממליצים: לזכור שמודם הוא נקודת תורפה שאינה חיונית בכל תחנה ובסוף יום העבודה לא לשכוח לבצע **logout**. כמו כן, לפני הכנת נהלים חשוב לוודא שמבינים בדיוק כיצד המשתמשים עובדים בתחנה. **שי** מזכיר כי **smart card** יכול לשמש להחתמת כרטיס עובד וגם להפעלת וכיבוי התחנות.

עמיחי שולמן, סמנכ"ל ייעוץ וטכנולוגיות ב-**eDvice** (☎ 03-6120133) מדגיש את חשיבות הניהול המרכזי בבחירת מוצר לאבטחת התחנות, כדי להבטיח **TCO** נמוך. לדבריו, ההוצאות גדלות עקב פגיעות וירוסים, שגם כאשר הן אינן פוגעות במידע, הן מביאות לבזבוז זמן, התקנות מחדש וכדומה. לגבי סיכונים עתידיים הוא צופה פיתוח וירוסים הפוגעים בחומרה (דוגמת **CIH** שידע לפגוע ב-**BIOS**) בעקבות התגברות שילוב רכיבי תוכנה בהתקני חומרה בסיסיים.

479.42– לאטום את החלונות

מערכות ההפעלה ממשפחת חלונות, במיוחד Windows 9x, אינן מוגדרות בתצורה מאובטחת במיוחד כברירת מחדל. כדי להקשיח אותן, שנה את ההגדרות הבאות:

- **משתמשים וסיסמאות** - ב-**Windows 9x** אין הרבה טעם בהפעלת אימות המשתמש בכניסה למערכת, שכן ניתן לעקוף אותה בקלות. ב-**Windows 2000** ו-**NT** מומלץ לחסום את חשבון **guest** כדי למנוע כניסה מאורחים לא רצויים, לשנות את שם חשבון האדמינסטרטור כדי להסוותו, ולהפעיל הגבלות על אורך סיסמאות ומשך השימוש בהן.
- כברירת מחדל, **חלונות** מתקינה ומפעילה את רכיב לקוח **Microsoft Network** ואת שיתוף הקבצים והמדפסות בהתקנת רכיבי התחברות ל**אינטרנט**, שפורצים יכולים לנצל לחדירה למחשב. אם מדובר במחשב בודד המתחבר במודם או כזה שאינו מחובר לרשת **NT**, כדאי לוותר עליהם לחלוטין (ב-**Windows 9x** תמצא אותם בלוח הבקרה **רשת**, וב-**Win 2000** במאפייני החיבור ל**אינטרנט**) במחשב המחובר לרשת, מומלץ לנתק את הקשרים הצולבים בין רכיבי התקשורת. הנחיות מפורטות, תמצא ב- grc.com/su-bondage.htm
- **הפסק את השיתוף** - ב-**Windows 2000**, שיתוף כוננים ברשת מופעל כברירת מחדל. אם אינך זקוק לו, סמן את הכונן הרצוי, בחר **Properties** מתפריט הכפתור הימני, ובחר את **Do not share this folder** מלשונית **File Sharing**.
- **בחר מערכת קבצים חזקה** - במחשב המריץ את **NT 4.0** או **Win 2000**, עדיף להשתמש ב-**NTFS** המאובטחת, ולא ב-**FAT/FAT32** הבטוחה פחות.

דגש – להחדיר מודעות

איך תגביר את מוטיבציית העובדים להתייחס להנחיותיך על בטיחות ברשת יותר ברצינות?

1. **הסבר** - דאג שהעובדים יבינו את האיומים הקיימים ומתוכם את משמעות הכללים. תן הדרכה מרוכזת קצרה, עם דוגמאות מהשטח.
2. **המחש** - שתף עובדים בתוצאות פריצות בדיקה, והסבר נקודות תורפה בתחנות וביישומים אתם הם עצמם עובדים.
3. **אל תכביד** - שים לב שמדיניות האבטחה, ככל הניתן, תימנע מלהכביד על מהלך וקצב העבודה להם רגילים העובדים. שאל עצמך האם היא מעודדת "קיצורי דרך".

479.43– ה-PC כנשק

PC ממוצע, חמוש בחיבור לאינטרנט ובארסנל תוכנות שניתן למצוא בכל אחד מאתרי ההאקרים הפזורים ברשת, יכול לשמש כלי יעיל לתקיפת המערכות המאובטחות ביותר, גם בידיו של אדם חסר ידע טכני מעמיק. עובדה זו תורמת לפופולריות גוברת לעיסוק בפריצות, ובהתאם לגידול בהיקף הסיכון. מצד השני, אחראי האבטחה יכול להגיע לכלים אלה באותה קלות - וללמוד כיצד להתגונן מפניהם.

פריצה ל-**PC** יכולה להיות עניין לא נעים ואף לגרום נזק רב, אבל הסיכון האמיתי ברמה הארגונית הוא שימוש ב-**PC** כאמצעי להיכנס לארגון או לגרום נזק למחשבים אחרים. דוגמה נפוצה היא "תולעים" דוגמת **Melissa**, שמשתמשות ביכולות **Outlook** כדי להפיץ עצמה לנמענים בספר הכתובות, או סוסים טרויאנים ותוכנות "רחרוח" שישלחו את סמאות הרשת של המשתמש אל הפורץ שהחדיר אותן לתחנה. מרגע שהפורץ השתלט עליה, האמון לו הוא זוכה ברשת חושף בפניו שלל הזדמנויות. הרשאות גישה (למשל בתחנה של מנהל בכיר) עשויות לשמש לחדירה למאגרי מידע ויישומים ארגוניים. כמה דוגמאות עדכניות ימחישו את רצינות הבעיה:

- **DEFCON 8 2.1** הוא "דלת אחורית" כללית, סביבה מנסים האקרים "רעיונות יצירתיים" שונים. עם ההדבקה תתחבר התחנה ל-**IRC** ותודיע לאדונה החדש שהיא מוכנה לפעולה.
- הארגון לבטיחות **CERT** הזהיר כי האקרים השתלטו על מאות מחשבים המחוברים ל**אינטרנט**, והם עשויים לנצלם כ"צבא זומבים" שמסוגל לבצע התקפת **Denial of Dervice** משולבת בעוצמה אדירה שיכולה לשתק אתרי ענק.

PCאון© למנהלים ומשתמשי PC בכירים

479.51 – מעטפת נפץ בדואר האלקטרוני

לפני שתפתח מעטפה שקיבלת בדואר האלקטרוני, כדאי שתדע מה אתה עלול למצוא בפנים:

- **קבצי הפעלה** - קבצים עם סיומת **exe** או **com**, שיפעילו תכנית וירוס, תולעת או וירוס טרויאני. מתחזים לעתים קרובות לגימיקים או משחקים תמימים.
- **קבצי סקריפט** - קבצים אלה יופיעו כ-**attachement** עם סיומת **vbs**, או בגוף ההודעה בהודעות **HTML**. הם עלולים לפעול אפילו מצפיה מוקדמת בהודעה.
- **קבצי משנה נגועים** - גם קבצי **Word**, **Access** או **Excel** המצורפים ל-**E-Mail**, עלולים לכלול פקודות מקרו מזיקות, שיופעלו מייד עם פתיחת הקובץ.

כיצד תתגונן בפני מזיקי הדואר?

1. **פעל נכון** - צא מנקודת הנחה שהדואר אינו בטוח, גם אם הוא מגיע מאדם מוכר - זו יכולה להיות תולעת שנשלחה ללא ידיעתו מהמחשב שלו או פורץ ששינה את כתובת השולח כדי להסוות עצמו. אם אינך בטוח, ברר עם השולח האם ומה הוא שלח. טפל בבעיה גם ברמה הארגונית - על ידי הגדרת ואכיפת נהלים מתאימים, ועל ידי פתרונות סינון הודעות ב-**Gateway** (למשל **Email Gateway** של **Symantec**) או בשרת ה-**Exchange**.
2. **כוונן ועדכן** - השתמש ביכולות האבטחה המובנות ב-**Outlook** ו-**Outlook Express**. בשני, בחר ב-**Options** מתפריט **Tools**, ושנה את ה-**Security Zone** לפתיחת הודעות **HTML** מ-**Internet Zone** ל-**Restricted Zone**.
3. **טפל באנטי-וירוס** - תוכנות אנטי וירוס עדכניות יודעות לסרוק את תכולת הדואר בזמן אמת ולמנוע נזק לפני התרחשותו - הצטייד בהתאם. ישנם גם פתרונות ייעודיים לנושא, כמו **eTrust Mail Watcher** של **CA** - www.cai.com/solutions/enterprise/etrust/

479.52 – מחזקים את היישומים

מספר פרצות ביישומים נפוצים ופתרונות להם:

- **Office** - מטרה מרכזית לפגיעה. שפת המאקרו החזקה שלה פותחת אפשרויות רבות של ניצול לרעה. לדוגמא - פרצה שהתגלתה ב-**MS Access** מאפשרת לקובץ **Word** המוצמד ל-**E-Mail** לתפקד כ-**Trojan**, בעזרת יבוא בסיס נתונים של **Access** הכולל אפליקציות **Visual Basic**. הגדרת סממת אדמיניסטרטור ל-**Access** תפתור את הבעיה. עדכוני אבטחה תמצא ב - officeupdate.microsoft.com
- **דפדפנים** - מסוכנים בגלל התמיכה שלהם ב-**JAVA**, **JavaScript**, **VBScript** ובמיוחד **ActiveX**. ניתן לבטל חלק מיכולות אלה בהגדרות האבטחה של הדפדפנים, או להתנות את הפעלתן באישור המשתמש. אפשרות אחרת, נוחה ובטוחה יותר, היא שימוש בתוכנות הגנה דוגמת **SurfinShield** של **פינג'אן** או **eSafe** של **אלאדין**. גם פה חשוב לעדכן: עדכוני **IE** - www.microsoft.com/windows/IE. חדשות בטיחות ועדכוני **Netscape** - home.netscape.com/security
- **IM - ICQ**, הנפוצה מביניהן, משמשת להאקרים אמצעי קל ופשוט למצוא קורבנות פוטנציאליים - ובגרסאות מסוימות, היא חושפת את כתובת ה-**IP** של המשתמש כברירת מחדל.

בנוסף, קיים מגוון עצום של "כלי תקיפה" מבוססי **ICQ** - ולכן כדאי להקפיד על הפעלת מרב אמצעי האבטחה המובנים בתוכנה ועל שימוש ב-**Firewall** אישי במקביל. ראה - www.icq.com/features/security/security-tutorial.html

דרך נוספת להתגונן היא בחירה בתוכנות מוכרות פחות, שאינן מהוות מטרה נפוצה להתקפות - למשל **Eudora** לדואר, **Yahoo IM** להודעות מיידיות ו-**Opera** לגלישה.

479.53 – שריון מסיליקון

לא על התוכנה לבדה יתגונן האדם. יש גם פתרונות חומרה:

- **אימות ביומטרי** - מבין פתרונות אלה, הכוללים זיהוי לפי טביעת אצבע, כף יד, אישונים ועוד, נראים פתרונות הזיהוי הקולי כזולים ביותר ליישום נרחב בתחנות, שכן הם דורשים מינימום חומרה (ראה **Configate** - ☎08-9316701). זיהוי טביעות אצבע נראית כטכנולוגיה שתהפוך נפוצה בעתיד.
- **סוויץ' סודי** - התקנים כמו הפלאגים של **אלדין** (☎03-6362222) יוודאו שרק אנשים מורשים ייגשו לתחנה.
- **הגנה בשחזור** - שינויים בטעות או בזדון, כמו פרמוט, מחיקת קבצים, שינויי הגדרות **CMOS** ועוד, ניתנים לשחזור מלא. **Magic Card** הוא כרטיס העושה זאת פשוט ומהר (בתהליך של הפעלה מחדש). אצל **רוגב** - ☎09-7741495. פתרון נוסף מסוג זה תמצא אצל **Radix** - ☎03-9606350.
- **Voltaire** מציעה את **2in1 PC** ו-**2in1 NET** - הראשון מיועד לחלק **PC** בודד לשני מחשבים לוגיים נפרדים, כך שניתן לחבר אחד מהם ל**אינטרנט** או לרשת ועל השני לאחסן מידע רגיש; השני מאפשר להפעיל שתי רשתות מקבילות - ציבורית ומסווגת. מידע נוסף ב - ☎09-9512177.

479.54 – קלים לסחיבה

כולם אוהבים ניידים ומחשבי כף יד. גנבים במיוחד. הם קלים לזיהוי וגם לסחיבה (תרתי משמע). מה שיתגלה בפנים עולה לרוב על תוכן תחנה ממוצעת בארגון, במיוחד כאשר מדובר במחשב של בכיר - ראה לדוגמה גניבת מחשבו של מנכ"ל **קוואלקום** או והשעית שגריר ארה"ב בישראל, **מרטין אינדיק**, בשל מידע חסוי שנשמר על הנייד. כיצד תתגונן?

- **היכון לדרך** - שמור פרטים מזהים (שם יצרן, דגם ומספר סידורי), וודא שהמידע החשוב מגובה היטב ושהמידע החשוב במיוחד אינו מאוחסן במחשב ניידי!
- **זהירות בדרכים** - פקח עיניים והרחק מעיניים סקרניות. שמור נעול היכן שניתן, באמצעות כבלים (**אריג'נט**, ☎03-6850113), או אפילו כספת (בבית מלון).
- **בקרת גישה** - השתמש בסיסמאות ובהצפנה להגבלת הגישה לחומר (**קומדע** ☎03-6485255). **SecureSentryPro** של **אליראו** (☎09-7677732) מספק אימות באמצעות **Token** ("אסימון") דרך כניסת ה-**USB**. בניסיון כניסה לא חוקי, המערכת תצפין מיידית כל חומר רגיש. שיטת **RFID** מאפשרת זיהוי רדיו ובקרה מרחוק על אוסף מחשבים. ראה **ODEM** (☎03-9660340) ו-**InfoRay** (☎09-9712350). **קומפאק** מציעה זיהוי בטביעת אצבע לניידים (☎09-7623222-).
- **הצילו! גנב!** - השתמש באזעקה (**$99** אצל **MCO** - ☎03-6392806) ושקול שימוש במערכת מעקב, המנטרת מיקום המחשב לאחר שנגנב.

479.61– הפנטיום הרביעי

פנטיום 4 שהושק רשמית בשבוע שעבר, נוטש את ליבת הפנטיום-פרו עליה התבססו הפנטיום II, III והסלרון, לטובת ארכיטקטורה חדשה לגמרי. היא מאפשרת ל**אינטל** להתקדם בצעד מהיר לקצבי שעון של **1-2GHz**, להציג עדיפות טכנולוגית על פני ה-**Athlon** של **AMD** ולהניח מצע מתאים ליישומי העתיד.

עם זאת, מבחני ביצועים שהתפרסמו באתרי חומרה מובילים כגון **Tom's Hardware Guide** ו-**AnandTech**, מראים כי ה-**Athlon** הפועל בקצב שעון נמוך יותר, עולה על ה**פנטיום 4** במרבית המבחנים - במיוחד יישומי מכתבה וחישובי נקודה-צפה אינטנסיביים. במקרים מסוימים ה**פנטיום 4** הראה שיפור מזערי לעומת **פנטיום 3**, ולעתים אפילו פעל לאט יותר. ביצועים טובים יותר צפוים בעתיד, עם הגידול בקצבי השעון, התאמת קוד ל**פנטיום 4** ושימוש ביחידת ה-**SSE 2**.

המעבד מגיע בקצבי **1.4GHz** ו-**1.5GHz**, במחיר **$644** ו-**$819** בהתאמה בארה"ב. בין תכונותיו המתקדמות - יחידות עיבוד במהירות כפולה, מטמון המאחסן פקודות לאחר פענוחן, יחידת ניבוי חכמה, **SSE 2** - סט של 144 פקודות לביצוע מהיר של פעולות מולטימדיה ו-**3D**, וערוץ מערכת (**BUS**) של **100** מה"ץ **X 4** (רוחב פס של **3.2Gbps**). הוא מחייב לוח אם מסוג חדש, מבוסס שבב **i850** ותושבת חדשה, ספק כוח מיוחד וזכרון **RDRAM**. ב**פלונטר** ניתן להשיג מערכות המבוססות עליו כבר עכשיו, החל מ-**$2,052** ללא מסך - אבל לאור השיפור המועט בביצועים, אנו ממליצים לעת עתה להמתין.

479.62– מה נדאי לקנות ?

אלה התצורות המומלצות על ידנו כיום, כ"כללי אצבע". המעבדים המומלצים עודכנו בהתאם לתמורות בשוק:

פריט \ תצורה	תחנה בסיסית	תחנה מתקדמת	שרת רשת
לוח אם	440BX / 810	440BX / VIA 133A	450GX
מעבד	Celeron 633 - 700 MHz	P-III "E" 650 - 800 MHz	Xeon 512K 833MHz
זיכרון	64MB	64-128MB	256MB
דיסק	10GB	15-30GB	20-50GB
מאיץ גרפי	AGP 8MB	AGP 16/32MB	8MB
מסך	17"	17" / 19"	17"
מ' הפעלה	Win 98	Win 2000	Win NT

לתצורה יש להוסיף מארז **ATX**, מקלדת מותאמת ל-**Win 9x**, עכבר, כונן דיסקטים, **CD-ROM**, כרטיס קול ורמקולים.

479.63– להיזכר בזכרון

כאשר מחירי הזכרון ירדו לפחות מ-$90 ל-128MB זכרון SDRAM, משתלם לרכוש זכרון מרווח למחשבים חדשים ולהרחיב זכרון לקיימים. בעוד למהירות המעבד תהיה השפעה מועטה על השימוש היומיומי ביישומים הנפוצים, זכרון לא מספיק יסרבל את העבודה בריבוי יישומים ומסמכים, יעכב את הגישה לדיסק, יפגע ביציבות ובביצועים ואף ימנע הפעלת תוכנות כבדות הדורשות זכרון רב כתנאי הכרחי. למחשבים המריצים את **Win 2000**, מומלץ במיוחד **96MB** כמינימום.

סוג הזכרון הנפוץ והמקובל הוא **SDRAM** בקצב **133MHz**, כאשר שבבי זכרון מאיכות גבוהה במיוחד של יצרנים כגון **Kingston**, יעלו יותר אבל יבטיחו פעולה אמינה במהירות המקסימלית - למשל במחשבים מבוססי **Athlon**. שני סוגי זכרונות מתקדמים, **RDRAM** ו-**DDR SDRAM**, נכנסים כיום לשוק והם מבטיחים להרחיב את צוואר הבקבוק של הזכרון - אבל מחירו של הראשון מגיע לפי 3 מזה של זכרונות **SDRAM** רגילים, והוא אינו נטול בעיות, ולכן נמליץ לחכות להבשלת הטכנולוגיות המתקדמות, ולהמשיך עם המקובל.

479.64– איך השתנו המדדים ?

כדי לתת תמונה כוללת, אנו נותנים מבט מרוכז על "מדד PCאון" ומדד הדיסקים בשנים שעברו:

התקופה	מדד PCאון	מדד הדיסקים
1993	70.7%	52.9%
1994	56.4%	61.2%
1995	67.6%	54.4%
1996	48.6%	60.3%
1997	55.1%	51%
1998	54.7%	51.1%
1999	85.4%	54.8%

479.65– מדד PCאון – 73.7%

מדד PCאון ירד בחודש נובמבר ב-0.2% והגיע ל-73.7%. החודש שדרגנו את מהירות מעבדי שלושת התצורות הראשונות, בשל השינויים בשוק. מדד הדיסקים טיפס ב-0.4%, ל-58.7%. ירידת מחירי הזכרון נמשכת - לאחר ירידה של כ-13%, הם עומדים כיום על **$1.5**-**$0.5** ל-**1MB**.

בחודש זה היו מחירי התצורות שכללו: לוח אם מבוסס **BX/820/810/GX**, **64MB** זכרון, כונן **1.44MB**, כרטיס קול, **CD-ROM x50**, מאיץ גרפי **16MB AGP**, מסך **"17**, עכבר, מקלדת ו-**Windows 98**:

Celeron 600 MHz	-	**$735 - $875**
Celeron 633 MHz	-	**$720 - $970**
600 MHz פנטיום III	-	**$825 - $1015**
650 MHz פנטיום III	-	**$845 - $1030**
733 MHz פנטיום III	-	**$855 - $1060**
Xeon 512KB 550 MHz	-	**$2310 - $3205**

מחירי הדיסקים הממוצעים היו: **$106** ל-**10GB**, **$148** ל-**20GB** ו-**$219** ל-**35GB** (ייתכנו שינויים של **5%** בנפח הדיסקים לכל צד).

פקס בקשת מידע ממנוי - PCאון©

לברורים ומידע נוסף - טלפון 03-9667939 פקס 03-9660310

דחוף

תאריך_____

לכבוד מנהל השיווק/מכירות

	מספר הפקס	ידיעה
____ סימנטק	09-7438860	(31)
____ קומארט	08-9773830	(31)
____ CA	03-7661414	(32)
____ צ'יף	03-9584488	(32)
____ רנסאנס	09-7643566	(32)
____ חילן	03-6871977	(32)
____ נץ	03-9386869	(32)
____ אלדין	03-5375796	(32)
____ הוד עמי	09-9571582	(32)
____ Info-Fort	03-9679216	(41)
____ קומסק	03-9230020	(41)
____ DataSec	03-6128020	(41)

	מספר הפקס	ידיעה
____ eDvice	03-6954837	(41)
____ Configate	08-9316702	(53)
____ רוגב	09-7741494	(53)
____ RADIX	03-9607104	(53)
____ Voltair	09-9512177	(53)
____ אריג'נט	03-6857137	(54)
____ קומדע	03-6474206	(54)
____ אליראו	09-7677739	(54)
____ InfoRay	03-9712355	(54)
____ ODEM	03-9660345	(54)
____ קומפאק	09-7440066	(54)
____ MCO	03-6875523	(54)

א.ג.נ.

הנדון: בקשת מידע מפורט

בעקבות הפרסום ב-**PCאון** בנושא_____

אבקש לקבל מכם מידע על_____

_____

_____

אודה למשלוח המידע לפי הפרטים הבאים:

שם ומשפחה_____חתימה_____

תפקיד_____ ארגון_____

טלפון_____ פקס_____

כתובת_____מיקוד_____

מנוי יקר !

דף זה הוא שירות נוסף של **PCאון** אשר נועד לסייע לך לקבל מידע מפורט ומהיר ישירות מהספקים המוזכרים בגיליון. סמן **V** מול שמות הגורמים שמהם תרצה לקבל מידע נוסף, הגדר הנושא או צרף הידיעה האמורה, סמן כיצד תרצה לקבל את המידע, מלא את פרטיך ושלח אל הספק/ים המתאים.

משווק נכבד !

פקס בקשת מידע זה, נשלח אליך על ידי מנוי **PCאון** - שרות תדרוך מקצועי של מנהלי המחשוב ומשתמשי **PC** בכירים בישראל, בעקבות אזכורכם בפרסומינו. הענות מהירה ומלאה לבקשת המידע, תסייע לעסקיך ותאפשר לנו לאזכרם גם בפרסומים עתידיים שלנו. תודה מראש על שיתוף הפעולה.