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... אבטחה בכף היד

מסר אישי

איום חדש ומשמעותי הולך ומתפתח במהירות בארגונים, ורמת המודעות לו נמוכה במידה מסוכנת! מדובר במחשבי כף יד, המתרבים, מתחזקים ומהווים מטרה נוחה לגניבה, אבדן וויروסים מיוחדים. עם השימוש הגובר ב-**WLAN** וב**אינטרנט** הם עלולים לשמש כערוץ חדירה נוח לרשת הארגון ולמידע רגיש.

מהם האיומים האפשריים עבור ה-**PDA**? האם ישנם פתרונות הולמים עבורם? כיצד תנצל אותם מבלי להיפגע? על כך ועוד, בחרנו לעדכנך 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

595.11– חדשות בקצרה

• **מיקרוסופט פיתחה קונספט חדש של הצמדת "בול וירטואלי" לכל הודעת E-Mail, באמצעותו ייגבה תשלום זעיר, בסך חלקיק הסנט, מהשולח.** עבור המשתמש הסופי המחיר יהיה כמעט בלתי מורגש, אך ספאמרים, ששולחים דואר למיליונים, יתחילו, לדברי החברה, לשלם עשרות אלפי דולרים - דבר שיקטין את המוטיבציה להציף משתמשים בדואר מיותר. המתנגדים טוענים שזוהי דרך של **מיקרוסופט** לחטוף נתח נוסף מעוגת ה**אינטרנט**. **מיקרוסופט** תציע את הטכנולוגיה בקרוב לספקי **אינטרנט** ברחבי העולם.

• ממשל בוש חשף גירסה סופית לתוכנית מדיניות אבטחה ל**אינטרנט** ולרשתות מידע, שתוכננה בחודשים האחרונים. במקום לכפות אמצעי אבטחה על ארגונים, כפי שתוכנן, **National Strategy to Secure Cyberspace** תעודד שיתוף פעולה בין ארגונים פרטיים לבין הממשל בכדי ליצור מערכת לתגובת חירום למקרה התקפה מקוונת. בין השאר מתכוונת הרשות ליצור מערכת התראה רחבה, וקוד "התנהלות נאותה" לחברות **ISP** - אבל גם שני אלה לא ייכפו על הארגונים הפרטיים.

• חזית החברות **The Liberty Alliance**, בו חברות בין השאר **Sun**, **HP**, ו-**AOL** - שחררה מפרטי ספציפיקציה חדשה לעניין ניהול זהויות ב**אינטרנט**. צעד זה מסביר ומבהיר כי תהיה אינטראופרביליות בין פתרונם הפתוח (**federated identity model**) לבין פתרונות אחרים, כולל טכנולוגיית **NET.** ה**מיקרוסופט**ית (פתרון ה-**Passport**).

595.12– מכנס איגוד האינטרנט

"צמיחה וחברה" היה המוטו של כינוס איגוד האינטרנט הישראלי שהתקיים בשבוע שעבר בכפר המכבייה ברמת גן. את הכנס פתח **עודד טירה**, נשיא איגוד התעשיינים שסקר את מצב המשק והצביע על הצורך של הממשלה להשקיע בתשתיות לרבות תשתיות **אינטרנט**, כצעד הכרחי לחזרה לצמיחה. ד"ר **אמיר עציוני**, נשיא **איגוד האינטרנט הישראלי** סקר את פעילויות האיגוד וציין בין היתר כי יש כיום 53,000 דומיינים, כשבשנה האחרונה נרשמה ירידה כוללת של כ-10% במספר הדומיינים הרשומים. רוחב הפס של שדרת ה**אינטרנט** הישראלית עומד כיום על 1.4 ג'יגה, כאשר רק כמחצית מקיבולת זאת אכן מנוצלת. שני יעדים מרכזיים שהוא הציב לאיגוד לשנה הבאה היו: הטיפול בנגישות ל**אינטרנט** לנכים ובעלי מוגבלויות וכן עידוד הגישה ל**אינטרנט** לבני הגיל השלישי.

במהלך הכנס עצמו שמענו מפי **אורי אולניק**, מנכ"ל **משרד התקשורת** על העלייה המטאורית במעבר לפס הרחב. בעוד שבסוף 2001 עמד מספר המחוברים על 38,000, בסוף 2002 נרשם גידול של 445%, ומתחילת 2003 נרשם גידול נוסף של 59,000 מתחברים, לסך כולל של 266,000 או כ-15% ממשקי הבית בארץ(!)

בועז דולב מ**משרד האוצר** הציג את **Open Office** בעברית, תוכנה בקוד פתוח שתכלול את כל יישומי המשרד המקובלים, אשר צפויה לצאת לשוק ו<u>בחינם</u>, במהלך אפריל-מאי השנה.

מפאנל מסכם בהשתתפות **יוסי ורדי**, **אלי אופר** המדען הראשי ב**תמ"ס**, **חמי פרס** מקרן הון הסיכון **פיטנגו וגיא רולניק** העורך הראשי של **דה-מרקר**, הובעה הסכמה כי למרות המשברים ו"הבועה", **אינטרנט** רק בתחילת דרכה, והדברים הגדולים באמת עדיין לפנינו.

595.13– חדש בשרתים

טכנולוגיית השרתים מרכזית למחשוב הארגוני ואין פלא כי היא מתקדמת ללא הרף. קונספט שרתי הבלייד המצליח ממשיך להתרחב כעת, כאשר **IBM** מרחיבה קו מוצרים זה אצלה. החברה מתכוונת להעלות מהירויות מעבדי **Xeon** בשרתי **BladeCenter HS20** מ-**2.4GHz** ל-**2.6GHz-2.8GHz**. מנהל השיווק **ג'ף בנק** הגדיר את גישתם ותוכניותיהם בנידון בראיון ל-**InfoWorld**, באומרו שעל פי **IBM**, 2003 היא שנת ה-**Blade**. ואכן, מתרבים היצרנים המציעים מוצרי **Blade**, שיתרונם לארגון בחסכון במקום, בכבלים ובמודולריות. לדוגמא: שרת **Blade** חדש מ-**SUN**, מבוסס מעבד **UltraSPARC 64-bit**. גם **HP** - שחקנית בולטת נוספת - מחזקת שרתיה. דגמי **איטניום** הציפסט החדש **sx1000** תומך ב-8-64 מעבדי **איטניום**! ארכיטקטורה חדשה בשם **mx2** תאפשר חיבור שני מעבדים כאלה לתושבת אחת ויצירת מערכות בנות עד 128 מעבדים!

גם בתחום התוכנה לניהול שרתים חלים שינויים מעניינים. על פי **Forrester Research**, תוכנות שרת מבוססות ג'ווה בקוד פתוח (כמו **Tomcat** ו-**JBoss**) נוגסות כעת נתחי שוק מפתרונות מותגיים מבוססי **ג'ווה (מחברות כאוראקל או IBM)**.

על התחרות העזה בין יצרני הפתרונות המסחריים עצמם ניתן ללמוד מהחלטת הענק היפני **מיטסובישי** לנטוש את תחום השרתים.

595.14– Web Services לשירותך

שירותי הרשת הופכים אט אט מעתיד להווה:

• לפי מחקר **גרטנר**, שלושת המובילות בתחום שירותי הרשת הן **מיקרוסופט**, **IBM** ו**אורקל**, כשהראשונה פופולרית במיוחד בקרב חברות קטנות. מהמחקר עולות עוד תוצאות מעניינות לגבי פילוח השוק: 58% מהמומחים והיועצים בחרו לישם שירותי רשת באמצעות **NET.** של **מיקרוסופט** ואילו 39% מהמשתמשים בחרו ב-**J2EE** כתשתית ל-**Web Services**.

• **Sun** מפתחת עדכון ל-**J2EE** המיועד לספק תאימות משופרת עם תקני ה-**Web Services**. גרסה 1.4 של **J2EE**, שתצא בקיץ הקרוב, תתמוך במפרט הבסיסי של ה-**WS-I**, תאפשר שימוש נוח, מהיר ואינטואיטיבי יותר ביכולות פיתוח שירותי ה-**Web**, ותמזער את הצורך בהסבת והתאמת נתונים לפלטפורמות שונות.

• "המכשולים העיקרי לאימוץ נרחב של ה-**Web Services** הם אבטחה ואמון", אמר **דיוויד ספרוט** בראיון ל-**ZDNET**. לפי הכתבה, אנו צפויים לראות עבודה בהולה על נושאי אבטחה בשנה הקרובה, לקראת אימוץ נרחב של ה-**WS**.

595.21– האבטחה בידיך

כמנהל מחשוב ארגוני, האם אתה ישן בשקט? שכן אחת הסכנות לרשת ולמידע הארגוני, נמצאת כעת בידי עובדיך ואולי גם בידיך, בצורת "מפתח", שאתה נושא כל הזמן בכיסך. מדובר במחשבי כף היד לסוגיהם, אשר במקביל לברכות שבהם, הם גם מהווים מוקד סיכון מהמעלה הראשונה, כשהמודעות לו בארגונים נמוכה למדי.

ה-**PDA** פותח במקור לשימוש אישי ולכן אבטחה לא הייתה שיקול מרכזי בתכנונו. כיום מאוחסן עליו מידע ארגוני רגיש כתכתובת **E-Mail**, פרטי לקוחות ומסמכים פנימיים שונים, כמו גם חיבור אלחוטי לרשת הארגונית, לסיסמאות ואף למפתחות הצפנה. בין הנפגעים מסכנות אלה הם המשתמש, הארגון ואף לקוחות שהמידע שלהם נאסף ב-**PDA**. לא מפתיע לכן שכבר בשנת 2000 הופיע הקוד העויין הראשון ל-**PDA** בשם **Palm.Liberty.A** - שמחק את כל הקבצים שלא הותקנו עם מערכת ההפעלה. מיד אחריו הופיעו שני וירוסים נוספים: **Vapor.741** ו-**Phage.963** - שהיה וירוס ה-**PDA** השלישי, והראשון שהשתמש גם ב-**E-Mail** כאמצעי הפצה. הסכנה הטמונה בוירוסים עדיין קטנה יחסית, אך המודעות ורמת היישום של אנטי-וירוסים ל-**PDA** נמוכים במידה מסוכנת.

ולא רק בתחום הוירוסים קטנה המודעות: סקר שנערך ביוני 2002 בארגונים בארה"ב גילה ש-41% ממשתמשי ה-**PDA** לעולם אינם מחליפים סיסמאות ו-71% מהמאחסנים מידע על לקוחות אינם מצפינים אותו. 6% מנשאלי סקר אחר (**PointSec**) דיווחו על אובדן או גניבה.

חשוב לציין שהפתרונות כבר קיימים בצורת מגוון עזרי אנטי-וירוס, הצפנה, אותנטיקציה ועוד. גם ברמת המדיניות הארגונית מגלים ארגונים וגופים שונים שקל וחשוב ביותר להתגונן טוב יותר. בארה"ב אף ייכנס השנה לתוקף חוק **Health Insurance Portability and Accountability Act** המטפל באבטחת מידע חולים המאוחסן ב-**PDA**. החוק יחייב בין השאר להצפין תקשורת ל-**PDA** ב-128 ביט והזדהות כפולה של משתמש ומכשיר גם יחד. חומר ב-**PDA** הנותר שבעה ימים ללא סנכרון (אבד? נגנב?) יימחק אוטומטית.

מספר מחשבי כף היד אמור להגיע השנה ל-19 מיליון (**IDC**). אנו צפויים לראות טלפונים סלולאריים מתקדמים ההופכים למעשה ל-**PDA**, על כל הסכנות הכרוכות בכך ואימוץ ה-**WLAN** יחמיר אתגרי אבטחת תקשורת ל-**PDA**. הנוזקה ל-**PDA** תתרבה ותשתכלל ומדענים בארה"ב כבר עובדים על התגוננות מקוד עויין אפשרי שיפעיל יישומים בצורה אינטנסיבית כדי לרוקן את הבטריות. בפתרונות צפוי שימוש נרחב בכרטיסים חכמים וביומטריה. פתרונות מתקדמים בפיתוח כוללים זיהוי מיקום וזיהוי תנועה כמעין סוויץ' סודי (למשל הטיית ה-**PDA** ימינה בזווית **X** וחזרה).

<u>לסיכום - אם ארגונך עושה שימוש במחשבי כף יד וודא בדחיפות שרמת אבטחתם מספקת. אם בכוונתכם לרכוש PDAs, שקול היטב גם את היבטי האבטחה.</u>

595.22– על הכוונת

ה-PDA עשוי להיות חשוף לסכנות האבטחה הבאות:

- **קודים עויינים** - תחום זה כולל כרגע מזיקים ידועים בודדים, אך צפוי לכלול בהדרגה מגוון ווירוסים, תולעי **E-Mail** וטרויאנים. אלה יפותחו וישתכללו על רקע מגוון התוכנות הגדל למחשבי כף היד וחוזק המכשירים המשתפר.
- **אבדן** - בגלל גודלם הקטן חשופים מחשבי כף היד לאבדן. הגודל עצמו הוא יתרון שמעודד לקיחתם לכל מקום, כולל נסיעות לחו"ל, עובדה המסבכת את איתורם.
- **גניבה** - התקני מחשוב הם מטרה טובה לגנבים, היכולים למכור אותם בקלות כציוד משומש. **PDA** מהווה גם מקור פוטנציאלי מצוין לגניבה על רקע ריגול תעשייתי. ההימור כי יש בו מידע ארגוני חיוני או פתח למידע כזה (סיסמאות) יהיה לרוב הימור מוצלח ביותר.
- **גניבת מידע** - משתמשי מחשבי כף היד הם לרוב בעלי תפקידים בכירים בארגון או אנשי שיווק ולכן מדובר פעמים רבות במידע רגיש במיוחד. לעתים אין צורך בגניבת המכשיר בכדי לגנוב את המידע - אפשר פשוט לסנכרן אותו למחשב השולחני, או לשלוח נתונים ל-**PDA** אחר באינפרה-אדום.
- **פתח לרשת הארגונית** - סנכרון מחשב כף היד עם המחשב האישי או אף המחשב בבית ותקשורת עם הרשת הארגונית ועם **אינטרנט** הופכים אותו תחנת מעבר לחומר רב, אך גם פתח אפשרי לפורץ להכנס למערכת הארגונית.
- **חוסר מודעות** - מודעות משתמשים לאבטחה מהווה אתגר תמידי למנמ"ר (זוכרים סיסמאות מצויינות עם פתק המודבק על המחשב..). ב-**PDA** האתגר גדול יותר, מאחר והמודעות עדיין קטנה ולכן קשה מאוד לפעול למניעתם.

595.23– נחלצים לעזרה

מהם הפתרונות להגנת מחשבי כף היד בארגון?

1. **הצפנה** - ישם זאת בכל מקרה בו מאוחסן מידע רגיש על ה-**PDA**. כך תבטיח שלאחר גניבה / אובדן מידע זה לא יוכל להיות מנוצל לרעה. פתרונות מתקדמים יבצעו זאת בזמן אמיתי ובצורה שקופה ומחירם אינו גבוה.
2. **אנטי ווירוסים** - פתרונות מוצעים מרוב יצרניות האנטי ווירוס והם פתרונות מיוחדים המותאמים למערכות ההפעלה של ה-**PDA** ולמשאבי החומרה המצומצמים. מומלץ שתישם אותם כבר כעת בכל **PDA**, גם אם האיום עוד בחיתוליו.
3. **תקשורת מאובטחת** - חיוני שכל תקשורת בין ה-**PDA** לסביבתו - מחשבים נוספים - **LAN** או **אינטרנט** - תהיה מאובטחת. הפתרונות רבים וזולים יחסית ובחלקם קיימים כבר במערכות ארגוניות (כמו **VPN**). ראה עוד בידיעה **595.52**.
4. **אמצעי הגנה פיסיים** - ישנו מגוון פתרונות להגנה פיזית כמו נרתיק עם מנעול, אזעקה או שרשרת שמחברת את ה-**PDA** ללבוש. הם עדיין לא נפוצים, אך ייתכן ותרצה לישמם להגנת **PDA** בעלי מידע קריטי במיוחד, בשימוש מחוץ לארגון.
5. **פתרונות ביומטריים** - פתרונות ראשונים מבוססי חומרה החלו להופיע עם טכנולוגיית זיהוי טביעת אצבע הקומפקטית והזולה יחסית, למשל במוצרי **iPaq** החדשים, וכלי זיהוי משתמש **PDA** לפי קול, קרנית העין ופנים נמצאים בפיתוח.

<u>PalmOS</u> מספקת אבטחת רשומות או מיסוך רשומות (אתה רואה רק פס במקום הרשומה) וחלק מהמכשירים נדלקים רק עם סיסמא. המערכת מציעה גם תמיכה בהצפנת **128-bit**, בתקשורת מאובטחת בשיטת **SSL**, הגבלת גישת יישומים למשאבים ומידע בעזרת חתימה אלקטרונית וזיהוי ייחודי של מכשירי כף יד ספציפיים. **<u>בסביבת PocketPC 2002</u>** (מבוססת **Windows CE**), כשמשתמש לא נוגע במחשב מעל זמן מסוים המערכת עוברת ל-**Stand by** ובכדי לחזור לפעולה תדרוש סיסמא. **PocketPC** תומכת בזיהוי ביומטרי, **PKI**, **SecureID** וכרטיסים חכמים, **VPN** והצפנת **128 bit**. תמיכה ב-**Crypto API** מאפשרת ליצור הרחבות אבטחה שונות.

<u>חשוב להדגיש שתמיכת מערכת ההפעלה בהצפנה מתקדמת, כרטיסים חכמים או זיהוי ביומטרי לא נותנת דבר ללא חומרה מתאימה (כגון סורק ביומטרי) או תוכנת הצפנה.</u>

PCאון© למנהלים ומשתמשי מחשב בכירים

595.31– טובה תוכנה ביד

להגנת ה-PDA מוצע שלל תוכנות אבטחה צד שלישי:

• **Applian** - מציעה מגוון תוכנות ל-**PDA**, כולל תוכנות אבטחה. **PocketLock** (**$19.95**) יסייע לך להצפין קבצים וספריות ספציפיים ו-**Virtual Wallet** (**$19.95**) יקל על גישה למגוון גדול של פרטי מידע רגישים. שני המוצרים מיועדים ל-**Pocket PC**. - www.applian.com

• **CheckPoint - SecureClient VPN-1** תומך גם ב-**Pocket PC 2002** ומאפשר על ידי כך אבטחת תקשורת ב-**VPN**, **Firewall** אישי וניהול אבטחה ארגוני מרוכז גם ל-**PDA**. מחירו החל מ-**$2,300**- ל-25 התקנים. ☎ 03-7534555.

• **Denton Software - Cradle Robber** (**$12.95**) היא תוכנת אזעקה המופעלת כאשר **PDA** נגנב מהתושבת הנייחת שלו שעל שולחנך. פתרון זה גם מנטרל אוטומטית את פעולת המכשיר. - www.dentonsoftware.com

• **Ilium - eWallet** הוא מוצר עזר לניהול ולאבטחת אחסון במחשבי כף יד מבוססי **PalmOS** ול-**PocketPC**. בעזרתו תגביל גישה למידע מאוחסן ותגבה מידע רגיש. מחיר **eWallet** מתחיל מ-**$19.95**-. - www.iliumsoft.com

• **CIC - Sign-On** הוא פתרון זיהוי בחתימה אלקטרונית - דרך זולה ויעילה יחסית ליישום אבטחה ביומטרית. הוא מגיע בגרסאות ל-**PalmOS** או ל-**PocketPC**, במחיר **$19.99** לכל אחת. ב - www.a2000d.com

• **PDA Defense** - פתרון הגנה בכמה רמות: הצפנה, ניהול סיסמאות מתקדם, נעילה אוטומטית בחשד לנסיון פריצה, מחיקת זכרון אוטומטית אם לא בוצע סנכרון כל זמן נתון (במקרה של גניבה או אובדן) ועוד. החל מ-**$19.95**- למכשירי **PalmOS** ו-**$29.95**- ל-**PocketPC**. **DSI** ☎ 03-5313333.

• **PointSec** - מציעה פתרון יסודי במיוחד ל-**PalmOS** או ל-**PocketPC**, המצפין אוטומטית ותוך כדי עבודה קבצים, נתוני **Microsoft Outlook**, מידע חיצוני בכרטיסי הרחבה, קבצי מערכת הפעלה ואף קבצים זמניים. www.pointsec.com

• **Trazoa - OnlyMe** נועל מכשירי **PalmOS** כשהם מכובים. האוטומציה חוסכת בצורך לנעול ידנית יישומים וקבצים. לאחר חמישה נסיונות כניסה כושלים מופעלת השהיה אוטומטית כנגד פריצה. - www.tranzoa.com

• **4T Personal** - מצפין נתונים כגון סיסמאות, חשבונות בנק, מספרי כרטיסי אשראי ומגן עליהם בסיסמא. ב - palmcomputing.palmgear.com/palm/product.cfm?prodID=7520

595.32– רואים בחומרה

בין עזרי החומרה לאבטחת ה-PDA תמצא:

• **CompSec** - מתמחה בפתרונות מיוחדים לממשל האמריקאי. **Secure PDA** (**Enhanced Palm csm125**) הוא מודיפיקציה מיוחדת ל-**Palm m125**, עם תכונות כמניעת ציטוט אינפרא אדום, סינכרון בלתי מורשה או קריאת המידע במחשב אחר. - www.compsecinc.com

• **eHOLSTER** - גישה פשוטה וזולה יחסית אך יעילה להגנת **PDA**, היא לשמור אותו קרוב לגופך ומוסתר. ראה פתרונות כאלה בדולרים בודדים - www.eholster.com

• **HP - iPaq 5450** (**$650** בחו"ל. לא נמכר עדיין בארץ) מכיל סורק תרמי שיכול ללמוד לזהות טביעת אצבע מסויימת. אחרי פרק זמן מוגדר ה-**PDA** ידרוש הזדהות חוזרת (אפשר לשלב גם זיהוי בסיסמא). ☎ 09-8304848.

• **Kensington - PDA Saver** מדגים פתרון בסיסי פשוט להגנה פיזית בצורת מנעול פלדה (חזק, אם כי לא עמיד בפני כל אמצעי חיתוך!), המעגן **PDA** לריהוט כלשהו, ומגיע עם מפתח מתאים. **PDA Saver** מתאים לכמה מכשירי **Palm** ו-**Handspring Visor** (**$39.99**). - www.pdamart.com/kenpdaseclea.html

• **SentryCom - MobilVoice** היא אפליקציה שניתן לצרף ל-**PDA** מכל סוג לגישה מאובטחת ל-**Web**. כניסה לעמוד תדרוש להקליד ב-**PDA** מספר טלפון סלולרי, המערכת תתקשר אליו חזרה, תקבל דרכו אותנטיקציה (שיכולה להיות גם בזיהוי קולי) ולאחר אישור זהותו תציג ב-**PDA** את הדף. המחיר **$40**-**$20**, על פי מספר המשתמשים. ☎ 04-8122250.

דגש – גיבוי קטן, צעד גדול

הסיכון הגדול יחסית לאובדן מידע, בשילוב העובדה שהנפחים הקטנים מאפשרים גיבוי מהיר מביאים למסקנה: גיבוי ה-PDA - משתלם. הגיבוי יתבצע בעזרת תוכנות שרובן מייצרות קובץ קטן ובודד הכולל הכל, בדומה לתוכנת **Ghost**. כך גם פעולת השחזור תהיה מהירה מאוד. **מיקרוסופט** מציעה את **ActiveSync** לגיבוי ה-**PocketPC**, להורדה ב - microsoft.com/mobile/pocketpc/downloads

עבור מכשיר מבוסס **PalmOS** ראה **BackupBuddy**, בעלות **$29.95**. להורדה בכתובת - www.backupbuddy.com

595.33– תופסים וירוסים

בתחום האנטי-וירוסים תמצא את הפתרונות הבאים:

• **סימנטק - Antivirus for Palm** כולל בדיקה בזמן אמת או לפי דרישה. עדכון אוטומטי מאפשר לקבל עדכונים למחשב האישי בכל התחברות ל**אינטרנט**, שיועברו אוטומטית למחשב כף היד בעת סנכרונו עם המחשב האישי. ☎ 09-7438853.

• **CA - eTrust Antivirus for PalmOS** הוא אנטי וירוס המגיע כחלק ממשפחת רכיבי האבטחה **eTrust**. כתוצאה מכך מתקבלת גם אפשרות ניהול והפצה מרכזית. ☎ 03-7661313.

• **F-Secure - F-Secure Antivirus for PocketPC** (**$180**) כולל סורק **On demand** וגם סורק אוטומטית בהכנסת כרטיס זכרון כלשהוא. **FileCrypto for PocketPC** (**$448**) מצפין את כל המידע על המכשיר. **רנסאנס** ☎ 09-7643567.

• **McAfee - Viruscan Wireless** (החל מ-**$45**) מותקן בתחנה וסוקר בסנכרון חומר הנכנס ל-**PDA** וכל העברה באינפרא אדום. **ThreatScan** (החל מ-**$24** למכשיר) לרשת מאתר סיכונים בארגון, דוגמת **PC** המחובר למחשב כף יד אך אין לו בדיקה בסנכרון. **Network Associates** ☎ 09-7643565.

• **Panda - Panda Platinum 7** (**$53**) יודע בין השאר לבצע סריקת קבצי רשת ונתונים מועברים ממחשבי **PC** למחשבי כף יד. **פייזילבר הנדסה** (☎ 09-8859611).

• **TrendMicro - PC-Cillin for PocketPC** הוא סורק קבצים. **PC-Cillin for Wireless** סורק תקשורת אלחוטית והורדות קבצים בזמן אמת ומתאים ל-**PocketPC** ול-**Palm**. שניהם **מוצעים חינם** באתר - www.trendmicro.com

PCאון© למנהלים ומשתמשי מחשב בכירים

595.41– הקול מהשטח

כמה מומחים מהשטח חלקו איתנו תובנות נוספות:

סול צבי, מנהלת תחום אבטחה ב**מיקרוסופט ישראל** (☎ 09-9525361) מעריכה כי היצע הפתרונות לא בהכרח ידוע לעומק, לעוסקים בדבר, ואין ספק שיש מה ללמוד וליישם כשמדובר בתחום מרתק זה. **סול** אומרת כי כניסה לתחום מחשבי כף היד מעודדת תמיכה במוצרי טכנולוגיה נלווים כטכנולוגיית **Wireless**. אלה מביאים את אנשי אבטחת המידע להתמודד עם אתגרים טכנולוגיים מאוד מעניינים המובנים מעצם הטכנולוגיה. התגוננות מאיומי וירוסים נראית לה כיום כהכרח וכמו כן היא רואה דרישה מתגברת מלקוחות לפתרונות הצפנת מסמכים רגישים במכשירים הניידים.

לדברי **מיכה בורד**, מנמ"ר **קבוצת אירון** (☎ 03-5751415), רוב הארגונים לא מבצעים את הדרוש בכדי להתגונן מול סכנות האבטחה במחשבי כף יד וגם מודעות העובדים לכך מאוד נמוכה. אם העובד לא משתף פעולה לא יעזרו כל אמצעי ההגנה ולכן המנמ"ר צריך לעבוד גם ברמת ההסברה. חשוב לדוגמא להגביר מודעות עובדים למידע שהם לוקחים איתם ב-**PDA** למקרה שהמכשיר יאבד. לדעתו, ככל שה-**PDA** נפוצים יותר כך גדלים הסיכונים הכרוכים בשימוש בהם, אך כך גם מתקדמים פתרונות האבטחה הזמינים.

אבי כהן, מנהל שיווק ומכירות ב-**WE!** (☎ 09-9718222) אומר שמנהלי מחשוב בארץ לא מודעים בכלל לנושא אבטחת מחשבי כף היד. לדעתו החשוב ביותר הוא ליישם אנטי וירוס ומערכת הצפנה. **אבי** צופה שככל שהמודעות לאבטחת מחשבי כף היד תגדל גם ההאקרים יתעניינו בכך יותר ובסופו של דבר נהיה חייבים לתת לאבטחת ה-**PDA** דגש יותר חזק. לדעתו כבר היום צריך לישם פתרונות כמנגנוני אימות, הצפנה ותקשורת בטוחה מול ה-**PDA**, אך הוא מעריך שכל אתגרי האבטחה נראים כפתירים.

595.42– טיפ בטוח

העזר בטיפים הבאים למיצוי אבטחת ה-PDA:

- **התמד וסנכרן** - סנכרן את ה-**PDA** לעתים קרובות עם המחשב האישי כעזר גיבוי לשעת צרה. כך, לאחר איבוד מידע מכל סיבה שהיא תוכל להתאושש במהירות.
- **הצג עצמך** - הצג את פרטיך האישיים ב-**Login Prompt** של ה-**PDA**, על תיק הנשיאה שלו או אפילו בכרטיס סביר שמוצא ישר יוכל להחזירו.
- **פרוץ לארגונך** - תוכל להעזר בחברות אבטחה כ**קומסק** (☎ 03-9234646) המציעות פריצות הדגמה לארגון. בעזרת שרות כזה תקבלו אתה והעובדים המחשה לסיכוני האבטחה הגלומים במערך ה-**PDA** ואתה תזכה לייעוץ נקודתי להתמודדות איתן.
- **זהירות בדרכים** - משתמש **PDA** המתחבר בדרכים לנקודות שידור ציבוריות (**HotSpots**) אינו יודע איזו מידת אבטחה מיושמת בהן ועשוי לחשוף דרכן מידע רגיש. לכן מוטב לצמצם שימוש ברשתות אלה במקומות כשדות תעופה או מלונות, אלא אם הם מפרסמים נתונים מספקים לגבי רמת האבטחה והפרטיות במקום.
- **עצור באור אדום** - בטל את קליטת שידורי האינפרא האדום (**Beaming**) המגיעה כברירת מחדל. כך תדע שאיש אינו משדר לך ללא ידיעתך (שים לב שכבר פותחה תוכנה המאזינה לשידורים אלה ומנצלת תכונת סינכרון אוטומטי בכדי לגרום ל-**PDA** שלך לשלוח לה סיסמאות).
- **מה שבטוח ביטוח** - סוכני ביטוח לא ששים לבטח מחשבי כף יד ומטילים הגבלות רבות על כך (למשל בגניבת המכשיר מרכב). עם זאת, שקול ביטוח מכשירים ספציפיים, שעליהם צפוי להיות מידע רגיש במיוחד.

595.43– ABC ל-PDA מוגן

כך תוודא שמערך ה-PDAs הארגוני מוגן:

1. **סדר ונהל** - כצעד ראשוני ולאורך זמן, הקפד לרשום כל **PDA** שבארגון, כך שיהיה לך מעקב מסודר אחריהם ואחר שימושיהם. שים לב במיוחד ל-**PDA** שלא נרכשו בתוך הארגון בצורה מסודרת, דוגמת מכשיר שהובא מהבית.
2. **הערך רגישות** - בדוק איזה מידע רגיש נמצא על כל **PDA**, מה צפוי להיות מאוחסן בו ומה הם השימושים המיועדים. בהתאם ספק לבעליו אמצעי והנחיות אבטחה. במכשירים קריטיים דאג לפתרונות הצפנה חזקים. לרגישים במיוחד הנחה משתמשים לנעול את המכשיר בכספת בארגון או במלון (בדרכים), כשהוא לא בשימוש.
3. **הגדר מדיניות ברורה** - במדיניות התייחס להגנות מינימליות נדרשות, להגבלות על הוצאת **PDA** מהארגון ולהשלכות הפגיעה בכללים (אחריות העובד על המכשיר). אסור שימוש במכשירים אישיים למידע רגיש או לחלופין החל עליהם את אותם הנהלים התקפים לגבי מכשירים ארגוניים.
4. **טפל בגורם האנושי** - נקודת תורפה עיקרית באבטחת מחשבי כף יד היא דווקא מודעות המשתמשים ונכונותם לשים לב להנחיות בטיחות. אלה לא תמיד נוחות להם לביצוע. לכן, חיוני שהמשתמש יבין מדוע מצפים שישתמש דווקא בסיסמאות ארוכות ומורכבות עם ממשק המשתמש שב-**PDA**, המסורבל יחסית להזנה.
5. **הגן על התקשורת** - תקשורת תתבצע רק דרך ערוצי תקשורת מאובטחים כ-**VPN** מורשה, מערכות בטוחות כ-**Microsoft Mobile Information Server** או סביבת **CA eTrust** וכלים תואמים כדפדפן תומך **SSL**. החלט על רמת זיהוי דרושה - שם משתמש וסיסמא, שימוש בכרטיס חכם או אפילו זיהוי ביומטרי. ראה עוד בידיעה 595.53.
6. **אחסן מידע לפי חשיבותו** - לא כל מידע חייב להיות על ה-**PDA** עצמו. שקול מה ראוי שיישאר בשרת מרכזי או מחשב אישי (אליו יכול ה-**PDA** לגשת לקריאה) ואיזה מידע תהיה מוכן ש"ייטיילי" עם ה-**PDA**. בהערכת הרגישות לכל **PDA** גם כל התקן אחסון חיצוני שבו אולי מסתייע המשתמש.
7. **סגור פרצות** - צמצם סיכונים על ידי הגבלת פעולות ותכונות מסוכנים שאינם חיוניים לכל משתמש, דוגמת השימוש באלחוטיות. הגדר למי מותר ולמי אסור להוציא **PDA** מתחומי הארגון והתקן **Patches**. הסתייע בפתרון כ-**PDASecure Enterprise** למניעת סנכרון בלתי מורשה. לרכישת גרסה אישית או ארגונית (החל מ-$29) - www.trustdigital.com/pdasecure.htm

595.51 – כף יד מול נייד

אלו כמה הבדלי אבטחה בין מחשבי Laptop ל-PDA:

1. **מערכת ההפעלה -** הבדל מרכזי שמציינים יודעי דבר היא מערכת ההפעלה. משתמשי ומתחזקי מחשבים ניידים נהנים ממערכות הפעלה משוכללות וותיקות, להן מוצע מבחר תוכנות גדול. מערכות אלה תואמות במקרים רבים גם לתוכנות ישנות שנמצאות בארגון. **PDAs** עובדים על מערכות הפעלה לנישה מיוחדת ומבחר התוכנות מצומצם בהתאם. לדוגמא: תזדקק לגרסת אנטי וירוס מיוחדת ל-**PDA**.
2. **מגניב אך גניב -** ממדיו הקטנים במיוחד, גם ביחס למחשב נייד, הופכים את ה-**PDA** למטרה נוחה במיוחד לגניבה או לאיבוד. גודלו גם מקל על הגנב להסתירו.
3. **חלק סטנדרטי מהמערכות? -** מחשבים ניידים יקרים יותר ולכן לרוב אינם גאדג'ט פרטי של המשתמש והם בהחלט מהווים חלק מוכר, רשום ומבוקר מהמערכת.
4. **תחכום = פגיעות -** מחשבי **Laptop** מורכבים מה-**PDA** בנקודות טכניות רבות ככח המעבד, גודל זכרון, נפחי דיסק ומורכבות מערכת ההפעלה. תחכום זה חושף בפני ווירוסים והאקרים נקודות תורפה רבות יותר.
5. **וותק = פגיעות -** מחשבים ניידים עובדים עם טכנולוגיות וותיקות יחסית בחומרה ובתוכנה. הפרצות שבמערכות אלה כבר מוכרות היטב לתוקפים. ה-**PDA**, לעומת זאת, עדיין אינו ממש "מושך אליו את האש".
6. **וותק = מודעות וניסיון -** הניסיון בהגנה על **Laptops** שפועלים כ-**PC** רגיל, רב הרבה יותר - והמודעות לנושא גדולה יותר. שימוש באנטי-וירוסים, **Firewall**, **VPN**, אימות מתקדם, הצפנה ואף הגנה מגניבות גדולה יותר.

595.52 – רשת בלי ביטחון

ה-PDA עומד בפני סיכוני אבטחה שונים גם במסגרת התקשורת הארגונית. הפתרון מתמקד בעיקר באותנטיקציה (כאן מומלץ להפעיל אמצעים מתקדמים מעבר לאימות רגיל בסיסמא) ובהצפנת התקשורת. יישום פרוטוקול **CHAP (Challenge-Handshake Authentication Protocol)** יאפשר לשרת לשלוח ל-**PDA** מפתח להצפנת שם וסיסמא, כך שלא ישודרו חשופים. שרת יכול גם לזהות **PDA** ספציפי בגישות שונות כמו **Mobile Access Number**, **Device ID** או **Electronic Serial Number (ESN)**. זיהוי המכשיר יצטרף לזיהוי המשתמש בסיסמא, בכדי לספק מחסום הזדהות מחמיר במיוחד. בטווח שידור קצר עדיין יש יתרון לאינפרה אדום הוותיק והנפוץ על פני **BlueTooth**. זאת דווקא בזכות הטווח הקצר והצורך להיות בקו ראייה לשם קליטה.

להערכת **גרטנר**, 85% מארועי האבטחה בשנים הקרובות ייתמקדו במכשירים ולא ב"לכידה מהאוויר" של מידע משודר. עם זאת, הערוץ האלחוטי עדיין מהווה סיכון. אם בכוונתך להקים **LAN** אלחוטי, שים לב שתשדר לרוב ממבנה הארגון ברדיוס הכולל את כל שטח הקליטה (המרובע) הרצוי. מעגל השידור עלול לחרוג מגבולות המבנה ולשמש מטרה קלה לציטוט באמצעות מחשב נייד או אף **PDA** שזה עתה נגנב (ועדיין מאפשר להתחבר לרשת עם פרטי בעליו). כאמצעי נגד התעמק בתכונות האבטחה (כאותנטיקציה והצפנה) מבוססות פרוטוקול **Wireless Equivalent Privacy (WEP)**, המובנות במוצרי **WLAN**. בחר בהצפנת 128 ביט שהוא מציע ולא ב-40 ביט והמצא סיסמאות מורכבות. תוכל אף להשיג אבטחה טובה יותר, אם תוותר על פשטות ה-**WEP** לטובת יישום **VPN** או התבססות על פרוטוקול **IPSec**. ראה עוד **<u>בתחקיר 543</u>**.

595.53 – סוחרים בדרכים

מסחר מקוון אולי אינו מיושם בכל ארגון, אך הוא תחום המשקיע רבות באימוץ טכנולוגיות חדשות. בבנקאות במיוחד, כל השקעה כזו נתפסת כהשקעה אסטרטגית חשובה, העשויה להנמיך עלויות שרות ולהגדיל הכנסות מאותו לקוח. לדוגמא: לפי מקורות שונים, **בנק לאומי** רואה צמיחה שנתית בת לפחות 100% במספר משתמשי שרותיו המקוונים. מאחר וגישה זו מוכיחה עצמה היטב, השלב הבא הטבעי - בבנקאות ובכלל - הוא לאפשר ללקוח אותה אינטראקציה מכל מקום. עוד אספקט לאבטחה במסחר אלחוטי: אנשי מכירות שיבצעו עסקאות בדרכים כבר לא ייצטרכו להסתובב עם צ'קים, מזומן או מידע אשראי (גניבים ובירי איבוד) עד הגיעם למשרד.

פתרונות מסחר-מקוון נייד מדברים על **PDA** עם כרטיס סלולרי. תקשורת מסוג זה תאובטח ברמת ספקיות הסלולר כ**סלקום** ו**פרטנר**, בין השאר בעזרת ערוצים מוגנים בשיטת ה-**VPN**. היישום הארגוני במסחר יעסוק לרוב במכירת מוצרים או שרותים ללקוח נייד, כאשר יישומי "חנות וירטואלית", עגלת קניות ומנגנוני תשלום שונים תומכים כיום גם במצב זה. בצד ה-**PDA** האבטחה לא שונה בהרבה מה-**PC** ומכשירי כף יד רבים כבר כוללים דפדפנים תומכי תקשורת מאובטחת בשיטת **SSL**. לדוגמא: דפדפן **Blazer** המותקן ב-**Handspring Treo** (**יער דטה קום** ☎ 03-9025586).

אתגר אחרון לאבטחה הוא המכשיר עצמו, העשוי לאצור בתוכו מידע היכול לאפשר לגנב לפעול במסחר מקוון כאילו היה בעל המכשיר. נקודה זו פירושה ש-**PDA** המשמש למסחר מקוון עשוי להוות סיכון אבטחתי גדול מהרגיל והמודעות לאבטחה תהיה לגביו משמעותית במיוחד. מודעות זו תזכה לפריחה גדולה אם יתגשם חזון ה-**PDA** כארנק אלקטרוני.

595.54 – לאן גולש ה-PDA ?

אתרים אלה יסייעו לך להרחיב ידיעותיך:

- **PalmGear** - באתר **PalmGear** העשיר מאוד בחומר בנושא מחשבי כף תמצא גם דף הורדות תוכנה. בדף זה ישנו בין השאר פרוט תוכנות אבטחה שימושיות שונות להורדה - **<u>www.palmgear.com/software/answer_category.cfm?categoryIDs=133</u>**
- **Palm** - דף זה באתר חברת **Palm** מציע מדריך ליישום אבטחת **PDA** בארגונים. לנוחותך, מומלץ להוריד אותו כקובץ **Pdf** מהדף הראשי. - **<u>www.palm.com/enterprise/resources/securing</u>**
- **Firewall Guide** - אתר זה מתמחה בסקירות על נושאי ומוצרי אבטחה למשרדים קטנים / ביתיים (**SOHO**). בדף שלפניך תמצא סקירות המתמקדות ב-**PDA**, כולל קישורים למאמרים עדכניים - **<u>www.firewallguide.com/pda.htm</u>**
- באתר האבטחה של ארגון **SANS** תמצא דף זה, המרכז מאמרים ממקורות שונים בנושא אבטחת מחשבי כף יד. בגלל איכות החומרים כדאי לדעתנו לעיין גם בישנים יותר שמבניהם - **<u>www.sans.org/rr/pdas</u>**
- מאמר זה ימחיש עבורך את נושא אבטחת מחשבי כף היד בתחום וורטיקלי מוגדר - במקרה זה תחום שרותי הבריאות. בעזרתו תבין טוב יותר כיצד אתגרי ופתרונות אבטחת ה-**PDA** מתבטאים בשטח. ראה בסופו גם אוסף גדול של קישורים למאמרים נוספים **<u>www.sans.org/rr/pdas/health_care.php</u>**
- **Pocket** - אתר מקצועי ישראלי בנושאי **Palm**, **PocketPC** וגאדג'טים אחרים. באתר פורומים מקצועיים וייעוץ בנושאים שונים. הכתובת - **<u>www.pocket.co.il</u>**