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 445 ● ● ● ● ● 10 אפריל 2000

PCאון ©

למנהלים ומשתמשי PC בכירים

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

בחר סיסמא בתבונה ...והפעם

מסר אישי

הסיסמאות שלך הרבה פחות בטוחות ממה שאתה חושב", כך טוענים המומחים ומוסיפים: "רוב הסיסמאות שבוחרים המשתמשים ניתנות לפיצוח ממוחשב **תוך פחות משנייה!**" תוכנות פריצה מתוחכמות שכוללות התקפות מילון ופענוח הצפנות סיסמא - מאפשרות כמעט לכל אחד לפרוץ את סיסמאות הרשת הארגונית, המסמכים המסווגים ואפילו חשבונות הבנק.

כיצד תבחר סיסמא מוצלחת? כיצד תעריך ותשפר את ניהול הסיסמאות בארגונך? סקירה מקיפה על בעיות אלה והפתרונות להן, תמצא בהמשך הגיליון.

תמצית החדשות בעולם ה-PC טור

תוכן התדרוך השבועי טור

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק** B.Sc. ,MBA

עורך - **נמרוד צוק**

תחקיר וכתיבה - **דורון בן-ארי**

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 _____

445.11– חדשות בקצרה

• **"מיקרוסופט חיזקה את כוחה המונופוליסטי באופן לא תחרותי, ניסתה להשיג מונופול על שוק הדפדפנים וקשרה את IE ל-Windows בניגוד לחוק, תוך הפרת פרקים 1 ו-2 בחוק שרמן", כך קבע בשבוע שעבר השופט הפדרלי תומס פנפילד ג'קסון בפסק הדין במשפט האנטי מונופוליסטי המתנהל נגד החברה, לאחר כשלון נסיון פשרה.** עם זאת, השופט דחה את טענות התביעה לגבי שימוש שעשתה החברה בהסכמי בלעדיות עם ספקי **OEM** על מנת לפגוע בתפוצת דפדפני **נטסקייפ**. גזר הדין, שיכול לנוע בין הגבלות עסקיות ועד פיצול החברה, ינתן תוך 60 יום. **מיקרוסופט** הודיעה כי היא תערער על פסק הדין, הליך שעשוי להמשך בין שנה לשנתיים, ובמקביל תמשיך לנסות ולהגיע לפשרה.

• **AOL** הכריזה על גרסת **Preview Release 1** של דפדפן הדור החדש שלה - **Netscape 6.0**. הדפדפן הרזה (מחצית מנפח **Netscape 4.07**), מבוסס על פרוייקט הקוד הפתוח **Mozilla** והוא בנוי סביב מנוע התצוגה **Gecko** המספק תצוגה מהירה וחלקה ותמיכה מדויקת בסטנדרטים כמו **XML** ו-**CSS**. כן הוא מציע ממשק חדש ומשופר שיאפשר קסטומיזציה נרחבת בעתיד, חלון צדדי שבו ניתן להציג מידע ושרותים מבין 400 אפשרויות, לקוח **Instant Messaging** מובנה, לקוח **E-Mail** מחודש, אבטחה משופרת הכוללת ניהול ססמאות ושליטה ב-**Cookies**, ולמשתמשים בארץ - תמיכה בעברית ויזואלית ללא צורך בהורדת גופנים. להוריד ב - www.netscape.com

• **דודי גולדמן מידיעות אחרונות** מדווח על "תולעת" מסוג חדש, שמנסה למחוק תוכנות אנטי וירוס במטרה למנוע התגוננות. **VBS.Irok.Trojan.Worm**, שהתגלתה על ידי **CA** (antivirus.ca.com) מגיעה כקובץ בשם **irok.exe** שמתחזה לשומר מסך של "מסע בין כוכבים". היא תתקין את עצמה בתיקית **Windows/System** ותשלח את הקובץ ל-60 הנמענים הראשונים בספר הכתובות של **Outlook**, במידה והתוכנה מותקנת על המחשב. עדכוני החתימות האחרונים של יצרני האנטי וירוסים יטפלו בה.

445.12– מה היה באינטרנט וורלד ?

את תערוכת אינטרנט וורלד 2000 שהתקיימה בשבוע שעבר בלאס וגאס, פתח מנכ"ל AOL סטיב קייס בהכרזה שלושה התקני אינטרנט שתייצר החברה בשיתוף עם Gateway. המכשירים, שצפויים לעלות פחות מ-**$500** ולהתבסס על **לינוקס**, כוללים התקן בעל מסך שטוח ומקלדת אלחוטית, התקן **WebPad** הנראה כמחברת נטולת מקלדת ומקושר ל**אינטרנט** דרך חיבור אלחוטי ליחידת בסיס, והתקן דמוי טלוויזיה. לדברי **קייס**, התקנים מסוג זה יביאו את מהפכת ה**אינטרנט** השניה והם יאפשרו למשתמשים ביתיים לגלוש ברשת בלי צורך להתמודד עם מורכבות ה-**PC**.

ג'ון פטריק, סגן נשיא לטכנולוגיות **אינטרנט** ב-**IBM**, דיבר על מתן כתובות **IP** לכל התקן המחובר לרשת, וטען כי פרוטוקול **IPv6** - הגרסה החדשה של **TCP/IP** - פותר את בעית מגבלת הכתובות והוא קרוב ליישום יותר ממה שנראה קודם לכן בשל הדרישה הגוברת לכתובות. הוא גם ניבא כי ה-**Cookies** יעלמו ויוחלפו ב"זיהויות דיגיטליות" מבוססות תקן **P3P**, שיאפשרו לגולשים לשלוט על המידע שנמסר עליהם לאתרי ה**אינטרנט** בהם הם מבקרים.

מגמות נוספות שבלטו בתערוכה היו טלפונים סלולריים תומכי **WAP**, מוצרים לשיתוף תמונות ומסמכי מולטימדיה דרך ה-**WEB** ושרותי קהילה וירטואלית הממוקדים בתחום מסוים ומציעים שרותים ייעודים למתעניינים בו.

445.13– מסרים מיידיים לעסקים

טכנולוגית ה"מסרים מיידיים" (Instant Messaging) מתרחבת משימושים ביתיים ואישיים, גם לתחום העסקי. חברות כמו **נובל**, **סאן-נטסקייפ** ו**לוטוס-IBM** מפתחות מוצרי **IM** המיועדים לשוק זה, בעלי יכולות אבטחה חזקות ואפשרות לשלב אודיו ווידאו בתקשורת הטקסטואלית.

נובל, לדוגמה, הכריזה על **InstantMe** - מערכת מסרים מיידיים המבוססת על **AIM** של **אמריקה אונליין** ומשתלבת עם **NDS** והספריה הציבורית **DigitalMe**. עד אמצעי השנה, היא מתכוונת לשלב יכולות הצפנה וחתימות דיגיטליות. ניתן להוריד גרסה ראשונית ב - www.novell.com/download/

לוטוס-IBM תשלב הודעות מיידיות בגרסה הבאה של **נוטס** עם יכולות תקשורת באודיו ווידאו וכן תרגום אוטומטי של הודעות טקסט בין 8 שפות. גם **מיקרוסופט** בתמונה - היא מתכוונת לשלב טכנולוגיות **IM** כחלק מאסטרטגיית מוצרי ה**אינטרנט** החדשה שלה.

גם השחקניות הותיקות בתחום משלבות במוצריהן תכונות שאמורות לקסום למשתמשים עסקיים - אחד השיפורים המרכזיים בגרסה הבאה של **ICQ**, **ICQ 2000**, הוא היכולת לעבוד גם מאחורי **Firewall** (גרסאות אלפא של התוכנה ניתן להוריד מעת לעת ב - www.icq.com/alpha). **Yahoo** הוציאה את **Yahoo Messenger 3.0**, הכולל יכולת משופרת לשיחה קולית ואפשרות לצפות בשערי מניות ולגשת ליומן הפגישות המקוון של **Yahoo**. להוריד ב - messenger.yahoo.com

445.14– חידושים למפתחים

עוד מספר מוצרים וחידושים למפתחים שהופיעו לאחרונה:

• **מיקרוסופט** פתחה אתר בשם **Code Librarian Update**, המציע קוד של החברה וגורמי צד ג' לשימוש חוזר ליישומים מבוססי **אופיס** ו-**VBA**, שמפתחים יכולים להוריד ולשלב ביישומיהם ועל ידי כך לחסוך בזמן הפיתוח. הכתובת - msdn.microsoft.com/officedev/downloads/codelibrarian.asp

• **בורלנד** מציעה את הגרסה החדשה של מהדר ה-**C++/C** שלה לסביבת **חלונות**, להורדה בחינם מ**אינטרנט**. הכתובת - www.borland.com/bcppbuilder/freecompiler/

• **אפל** שחררה את הוקד לגרסה 1.0 של **Darwin**, מערכת ההפעלה מבוססת הקוד הפתוח העתידית שלה המשלבת את ליבת מערכת **OS X** ומערכת ה**יוניקס BSD**. את הקוד ניתן להדר לא רק לסביבת **מקינטוש** ומעבדי **PowerPC**, אלא גם למחשבי **אינטל**. להוריד ב - www.publicsource.apple.com

445.21– לשמור על המפתח

כהרגלך, אתה מקליד את שם המשתמש ואחריו את צירוף האותיות המוכר - הסיסמה שלך. בלחיצה על "אישור" נעלמות הכוכביות המסתירות אותה מעיניים חטטניות, ואתה ניגש בנינוחות לקרוא הודעות **E-Mail**, לגשת לרשת הארגונית, לקרוא קובץ חסוי או לשנות עמוד באתר ה**אינטרנט** הארגוני - בידיעה כי הסיסמא, הנמצאת בידך בלבד, מגינה מפריצה וחיטוט. האמנם?

מרבית הסיכויים שהסיסמאות שלך ושל המשתמשים בארגונך אינן בטוחות. אם אינך מכיר את הכללים לבחירת סיסמאות ואינך משתמש בתוכנות המתאימות - סביר להניח שניתן לפצח את סיסמאותיך תוך **פחות משניה**. גם העובדים בארגונך ודאי אינם מודעים לכל הכללים, כאשר התרבות והצטברות הסיסמאות עשויה להוביל לשמירה ממושכת, מחזור והגעת הססמאות לידיים הלא נכונות. עוד נדגיש כי חשיפת ססמאות במחשבים המריצים את **Windows 9x** ניתנת לביצוע בכלים פשוטים וזמינים ועם ידע טכני מינימלי.

מעשית, ניתן לוותר בכלל על השימוש בסיסמאות ולעבור לאמצעי זיהוי מתקדמים יותר: כרטיסים חכמים, מחוללי סיסמאות דינאמיים ואמצעי זיהוי ביומטריים - כולם אמצעים יעילים יותר, יציבים יותר ובטוחים יותר, אבל גם יקרים יותר. למי שמעדיף להשאר עם האמצעי המוכר והנפוץ, חשוב להקפיד על אמצעי זהירות: מהפצת נהלי בחירת סיסמאות, דרך אמצעיים אוטומטיים להבטחת בטיחות הססמאות ועד פתרונות **Single Sign On** שיאפשרו שימוש בטוח בסיסמה אחת לכל הפלטפורמות והאפליקציות. אם גם אצלך הסיסמאות הן הקו הראשון של אבטחת המידע - חשוב שתדע כיצד להשתמש בהן נכון.

<u>השורה הסופית - ססמאות לא בטוחות הן פרצה הקוראת לגנב. יישום השיטות והכלים המובאים בגליון יחזק את מערך האבטחה, ישפר את האפשרות לעבוד ולגלוש בפרטיות ובבטחה וימזער את הסיכויים לנזקים.</u>

445.22– מאיימים

חשיפת סיסמה היא הצעד הראשון - לעתים הסופי - בדרך לגרימת נזק כלכלי ואישי, לך ולארגון. "האקר" חובב שמחפש אתגרים, עובד ממורמר שרוצה להתנקם בארגון או בממונה עליו, עבריין מחשבים מתוחכם או אפילו חברה מתחרה, כולם עלולים לנסות להניח יד על ססמאות רגישות ולהכנס בעזרתן למקומות שהם לא אמורים להיות שם.

הנזק מפריצת סיסמה יכול להתחיל בשימוש לא מורשה שמישהו יעשה בחשבון ה**אינטרנט** שלך על חשבונך, גניבת מספר **ICQ** או חשיפת הודעות ה-**E-Mail** המאוחסנות על שרת הדואר וקבצים הנמצאים על המחשב, לעיניים לא רצויות. נזק ברמה גבוהה יותר ייגרם מפריצת ססמאות שרתי הארגון - החל מהשחתת דף הבית באתר ה-**WEB**, דרך שיבוש פעילות מערכות חיוניות ועד להשתלטות על הרשאת ה-**root** (ההרשאה העליונה ב-**UNIX**) או האדמיניסטרייטור ב-**NT**, שיאפשרו לפורץ לעשות ככל העולה על רוחו במערכת שנפרצה.

נזק כלכלי חמור במיוחד, שיכול להגיע לעשרות אלפי ומליוני דולרים, ייגרם מגניבת ססמאות גישה למערכות פיננסיות, כאלה המכילות מידע שיווקי, טכנולוגי או בטחוני או מערכות מחשוב תפעוליות - ראה 445.42.

הצעה – תרופות לשכחנים

אבדן סיסמה כרוך לא רק באי נעימות, אלא גם בהפרעה ממשית לעבודה ובהטרדת אנשי התמיכה. לכן כדאי להשתמש בסיסמאות קלות לזכירה. לדוגמה:

- ראשי תיבות של ביטויים או משפטים מתוך שירים. למשל, הסיסמא: **LiAUN** היא ראשי התיבות של שורה בשיר של ה**ביטלס**: **Love is All You Need**.
- וריאציות על שמות מכרים - **Jacob+David** נותן לנו בהפוך מעורבב: **dbiovcaaDJ.**
- מילים משפה זרה, כתובות באותיות לועזיות. דוגמא: **BaGdiKatan.**
- ססמאות אסוציאטיביות - דגי **piranha**, החיים בנהר האמזונס, יכולים לשמש כסיסמה ל-**Amazone.Com**. חשוב לבחור באסוציאציות אישיות ולא טריויאליות.

גם אם למרות כל האמצעים, שכחת את הסיסמה - יש מספר דרכים לשחזר אותה. באתרי **אינטרנט** מסוימים ובתוכנות כמו **ICQ**, ניתן לבקש שהסיסמה תשלח לכתובת ה-**E-Mail** שרשומה בחשבון; באחרים, ניתן להגדיר תזכורת לסיסמה - שאלה שתוצג לך כאשר תשכח את הסיסמה. תשובה נכונה תביא להצגת הסיסמה על המסך (למשל ב-**Hotmail**).

445.23– הכל סיסמאות

המשתמש הארגוני צובר אוסף סיסמאות עצום שעשוי לייאש כל אחד. לאבטחה גבוהה הוא נדרש לסיסמא ב:

1. תחנת העבודה ברשת **NT** או **Novell**
2. גישה למחשבים מרכזיים ושרתים.
3. מאגרי נתונים ארגוניים או אחרים.
4. מסמכי **Office** מסווגים.
5. חיוג במודם לשרתים אחרים. דוגמא: הבנק.
6. תוכנות הצפנה על הדיסק: לשמירת מידע מסווג.
7. כניסה ל-**Laptop** - דרך סיסמת **BIOS**.
8. סיסמת גישה ל**אינטרנט** בחיוג.
9. סיסמאות דואר אלקטרוני (בד"כ זהה לקודם).
10. גישה מרחוק לרשת המקומית.
11. חשבונות **אינטרנט** אישיים: חנויות וירטואליות, עיתונים און-ליין, קהילות רשת, שירותי מנויים.
12. אתרי **FTP**: להורדה ישירה של תוכנות.

הצטברות הסיסמאות עשויה לגרום מספר בעיות:

- המשתמש **ישכח** סיסמאות (ראה דגש למעלה).
- המשתמש **ירשום** סיסמאות (ויאבד את הפתק).
- המשתמש ישתמש **באותה סיסמא** לכל האפליקציות והפלטפורמות, (ואם אחת תיפרץ, כולן יפלו יחד איתה).

פתרונות לבעיית ריבוי הססמאות מצויים בתוכנות עזר הזוכרות אותן במקומך ומחייבות לזכור סיסמה אחת בלבד, במערכות **Single Sign On**, באפשרויות שמירת סיסמה אוטומטית (למשל בחיוג ל**אינטרנט** או בגלישה ב-**IE 5.0**) או בהחלפת הססמאות באמצעי זיהוי אחר.

445.31– 13 צעדים לסיסמא בטוחה

במידה והחלטת לאפשר למשתמשים לבחור את סיסמאותיהם בעצמם, חשוב לפרסם נוהל שימוש נכון בסיסמאות. 13 הכללים החשובים שמצאנו הם:

1. **השתמש לפחות ב-6 סימנים** - האורך האופטימלי עליו ממליצים רוב המומחים הוא 7.
2. **השתמש באותיות גדולות וקטנות במעורבב.**
3. **השתמש במספרים.** מקם אותם לאו דווקא בסוף.
4. **השתמש בסימנים אחרים** כמו $ או ^. גם אותם מקם לאו דווקא בסוף הסיסמא.
5. **אל תשתמש במילים אמיתיות או בשמות אנשים ומקומות.** קיימות תוכנות שבודקות מילה במילון.
6. **אל תשתמש בסיסמא שמישהו שמכיר אותך עשוי לנחש.** לא שם האישה, הילד או הכלב.
7. **נסה לבחור סיסמא קלה לזכירה ותרגל את השימוש בה כדי לזכור אותה.**
8. **השתדל שלא לרשום את סיסמתך.** אם אתה מוכרח, שמור על הפתק כאילו היה כרטיס האשראי שלך.
9. **החלף סיסמא לעתים קרובות** - ההחלפה תתבצע כל 30 עד 90 יום, בהתאם לדרישות האבטחה של הארגון.
10. **אין להעביר סיסמאות בשום אופן** - לא לעובדים אחרים, לא בטלפון ולא ב-E-Mail. יש להבהיר שמנהלי הרשת **לעולם** לא יבקשו סיסמא שלא פנים אל פנים.
11. **אין להשתמש בסיסמאות חוזרות** - לכל אפליקציה תהיה סיסמא משלה, כך שאם בין היישומים תתגלה סיסמא אחת, לא יקרוס כל מערך האבטחה.
12. **אין להשתמש בסיסמאות דומות** - כך שלאחר שתחליף סיסמא, תוכל לסמוך עליה גם אם נפרצה הסיסמא הקודמת שלך.
13. **אין להשתמש בהקלדות רצופות** - כגון Qwerty או Lkjhgf. גם לפורצים אותה המקלדת.

הקפדה על כללים אלה תיצור סיסמאות, שזמן הפריצה המשוער שלהן לפי Soft4You יגיע עד ל-4 חודשים (עם תוכנה שבודקת 100,000 סמאות בשניה) והוא יגדל **פי 50** עם כל סימן שיתווסף לסיסמא!

445.32– עוברים לאכיפה אוטומטית

אכיפת משמעת סיסמאות יכולה להתבצע באופן אוטומטי:

• בהגדרות של Windows NT או ב-Novell NetWare ניתן לקבוע דרישות מינימאליות לסיסמא, כגון אורך, סיבוך וזמן החלפה. בנוסף ניתן לקבוע אחרי כמה ניסיונות חיבור כושלים ינעל החשבון.

• תוכנות מיוחדות מנסות לפרוץ את הסיסמאות לפני שהן מאשרות אותן ואינן מקבלות סיסמאות קלות לפריצה. הבולטת בהן היא Password Policy Enforcer (ראה ידיעה **33**).

• קיימות גם תוכנות המגרילות סיסמאות בטוחות לשימוש: תוכנה כזו היא Random Password Generator Pro, אותה ניתן להשיג באתר - www.hirtlesoftware.com

• לארגונים שעובדים על מספר פלטפורמות, מגוון מוצרי Single Sign-On ישמרו על סנכרון בין הסיסמאות במערכות השונות, ויאפשרו למשתמשים להשתמש בסיסמא אחת, בטוחה במיוחד. דוגמה טובה היא התוכנה AcessMaster, שניתן להשיג באתר - www.bullsoft.com

גם לסמאות ב**אינטרנט** קיימות תוכנות עזר מועילות:

• Password Manager - מציעה הצפנה חזקה, לשמירת סיסמאות, מספרי כרטיסי אשראי וכו'. ניתן להשתמש בה מתוך כל אפליקציה, ופשוט להעתיק את הסיסמאות לשדה הדרוש. ישנה גירסת דמו, המחיר למוצר המלא - **14.95$**. האתר - www.celcoserv.com/download.html

• Password Tracker - מצפינה את הסיסמאות שלך ומכניסה אותן באופן אוטומטי לשדה הדרוש. צריך לזכור רק סיסמא אחת, בטוחה במיוחד - www.clrpc.com/ptd

דגש – שאלה של אחסון

הדרך בה נשמרות הסיסמאות, נקבעת על ידי המערכת שמשתמשת בהן. ברוב המערכות קיימת הצפנה, שמונעת את האפשרות לגלות את הסיסמא ללא השקעת מאמץ ניכר. הצפנת הסיסמאות היא חזקה במערכות ארגוניות כמו Windows NT, Novell NetWare ו-Windows 2000, בה בוצע שיפור ניכר בתחום זה.

במערכות הפעלה כמו Win 9x, האבטחה היא חלשה בהרבה - בעזרת תוכנה כמו WASP, ניתן לחשוף את כל סמאות הרשת שנשמרו במחשב. כדי להשתכנע, הורד ונסה אותה מ - www.iopus.com/wasp.htm

445.33– מחזיקי המפתחות

הכלים הנבחרים הבאים יסייעו לך לנהל את הסמאות ולהטמיע הרגלים נכונים לשימוש בהן:

• Password Policy Enforcer - יאפשר לאכוף משמעת סיסמאות חזקה ויבדוק כל סיסמא **לפני** קבלתה. הוא יריץ התקפות מילון ויבדוק את עמידותה של הסיסמה לפריצות. במקרה של סיסמא חלשה, נפוצה או פשוטה מדי, המשתמש יתבקש לנסות שוב. ניתן להוריד גרסת ניסיון, המחיר הוא **99$** ל-50 רשיונות - www.tpis.com.au/products/ppe

• Passgo - יסייע למשתמשים הארגוניים לשמור על סנכרון בין הסיסמאות, בכל הפלטפורמות והאפליקציות. סיסמא אחת לכל משתמש, תמנע ממנו לשכוח סיסמאות, לרשום סיסמאות או לבזבז זמן. ברגע שתשתנה הסיסמא באחת הפלטפורמות היא תשונה מיידית גם בשאר הפלטפורמות. פרטים באתר - www.passgo.com

• PassMan - תסייע למשתמשי Windows לנהל את כל הסיסמאות והקודים ברשת ומחוצה לה. היא גם תוכל להציע סיסמאות חדשות ובטוחות ולנעול את המחשב תחת סיסמא, בהקשת מקש. גרסת חינם ב - www.ijen.net/pmmain.htm

• Focal Point - של Okiok, היא תוכנת Single Sign-On, המאפשרת לסנכרן סיסמאות משתמשים במערכות: Unix, NetWare, Windows NT, AS/400 ו-OS/390. להשיג באתר - www.okiok.com/pages/focal.html

445.41– מה אומרים המומחים ?

שאלנו מומחי אבטחה על המודעות לנושא הסיסמאות והצעדים שכדאי לנקוט. אלה הדברים ששמענו:

מרים דולב מ**הד-און** (☎ **03-5759010**) מסבירה שבעקבות הקשחת הכללים לבחירת סיסמאות, וריבוי הפלטפורמות והסיסמאות - השימוש בסיסמאות הופך מסורבל יותר ויותר. לדבריה, קיימים שני סוגי פתרונות לבעיה: מערכות סנכרון סיסמאות או **Single Sign-On** ואמצעים חיצוניים, כגון זיהוי ביומטרי וכרטיסים חכמים. הסיסמאות הן אמצעי בטוח פחות, בין השאר משום שאתרי האקרים רבים, מפיצים תוכנות פריצה וביטול **Masking**. היא אומרת כי הצפנת הסיסמאות ב-**Win NT** וב-**Win 2000** טובה יחסית, אך ב-**Win 95/98** האמצעים אינם מספקים והם ניתנים לפיצוח.

גיא אלפסי, סמנכ"ל יעוץ וטכנולוגיה ב**קומסק** (☎ **03-9234646**), אומר שישנה מגמה של מעבר לאמצעים חיצוניים כגון מחוללי סיסמאות דינאמיים ואמצעים ביומטריים. הוא מזהיר שהשיטות הטריוויאליות לפריצת סיסמאות עדיין עובדות יפה מאוד: החל מהצצה מעבר לכתף וכלה בהתקפות מילון, בעלות 30/40 אלף מילות מפתח שעשויות לפצח סיסמאות מילוליות תוך זמן קצר. בנוסף, הוא טוען, הצפנת הסיסמאות ברוב המערכות אינה מספיקה. **גיא** ממליץ בחום להקפיד על **תקן 1495** לסיסמאות (ניתן להשיגו ממכון התקנים הישראלי, ☎ **03-6465154**, תמורת **16.40 ש"ח**).

נעמי אברמסון, מנהלת תחום שירותי אבטחת מידע ב**תדיראן מערכות מידע** (☎ **03-5313501**), אומרת שזיהוי באמצעות סיסמאות מהווה עקב אכילס גם במערכות מתקדמות כמו **Windows NT**, לכן כדאי לבחון אמצעים מתקדמים יותר, ובכל מקרה יש להחליף את הסיסמאות כל פרק זמן סביר - לדוגמה כל 60 יום. ברוב הארגונים, היא אומרת, קיימות סיסמאות רבות שכל כלי-פריצה פשוט או אינטליגנציה בסיסית יכולים לפרוץ. בבדיקות שביצעה החברה, הצליחו תוכנות פריצה לפצח סיסמאות מבוססות אותיות **תוך פחות משנייה**, בעוד סיסמאות המורכבות גם ממספרים וסימנים, נפרצות רק אחרי זמן ממושך. על כל ארגון, היא מסבירה, לערוך חישוב, כמה זמן ומשאבים עשויים הפורצים להשקיע בפריצה, ואז להחליט על אמצעי האבטחה בהם ינקוט. הצפנת הסיסמאות בחלק מהמערכות אינה מספקת, וחלק מהן, היא מזהירה, אינן מוצפנות כלל! גם **נעמי** ממליצה ליישם את **תקן 1495**.

445.42– על מה חשוב להגן ?

לא על כל דבר חשוב להגן. הסיסמאות החשובות הן:

- **כל סיסמאות הרשת הארגונית -** מבפנים קל יותר לפרוץ ולכן יש להגן אפילו על סיסמאות בעלות הרשאות מעטות, שנראות כלא חשובות.
- **התחברות מרחוק -** אלו הסיסמאות שמותקפות לעתים קרובות ביותר, ובעזרתן ניתן לגרום נזק רב. רצוי לבצע בדיקות תקופתיות של קבצי ה-**Log** כדי לבדוק התחברויות חשודות.
- **סיסמאות הצפנת קבצים -** מגינות על המסמכים המסווגים והמידע הרגיש ביותר של הארגון.

המידע הפגיע ביותר הוא:

- **מידע פיננסי -** חשבונות בנק, משכורות, תזרים מזומנים. זה המידע שחשוב ביותר לשמור עליו.
- **תכניות -** טכנולוגיות, תכנונים לעתיד, מאגרי מידע.
- **מידע על עובדים -** בעזרת מידע כזה, ניתן לפעמים להוציא מידע רגיש או אפילו סיסמאות מהעובדים.
- **מידע על לקוחות -** בעיקר לארגונים השומרים מאגרי-מידע על לקוחות. פרסום של מידע כזה יכול לגרום לנזק תדמיתי או לתביעה - ועשוי גם לשמש מתחרים בפיתוי לקוחות.
- **מידע הדרוש לפעילות השוטפת -** כל מידע, תוכנה או מאגר מידע שהעובדים יתקשו להסתדר בלעדיו. אפילו אם הוא אינו סודי - יש לשמור עליו ממחיקה או משינוי.

סיסמאות **Office** לנעילת מסמכים, הן אמצעי יעיל להגנה מפני פתיחה מקרית, אבל הן אינן כלי מתאים למניעת פריצות מכוונות. לכן, במקרים של מסמכים מסווגים באמת, רצוי להשתמש בתוכנת הצפנה מקצועית ולהקפיד על הרשאות משתמשים מתאימות.

445.43– שקט נפשי

הדרך הטובה ביותר לאבטחת מידע היא שימוש בפתרונות טכנולוגיים כתחליף לסיסמא (ראה גיליון **343**, **לא צריך יותר סיסמא** או ידיעה **52** בגיליון זה). אולם אם תעדיף להמשיך בדרך הקיימת, אלו הן המלצותינו:

1. בחר סיסמאות טובות (ראה ידיעה **31**)
2. רשום את הסיסמאות על פתק ושמור בארנקך או השתמש בתוכנות שמסתירות סיסמאות (ידיעה **32**).
3. היעזר בכלים מתאימים (ראה ידיעה **33**)
4. הקפד על סיסמאות זכירות (ראה דגש בטור **6**)
5. נסה לפרוץ את סיסמאותיך (ראה ידיעה **52**)
6. אחת ל-60 יום או בסוף כל חודש זוגי עשה הרגל להחליף את מאגר הסיסמאות שלך.

ברמה הארגונית מומלץ:

1. ליזום כנס הסברה שבו תציג את עיקרי הדברים המוצגים בגליון זה, ובמיוחד תדגים בעזרת כלי ההדגמה שבגיליון, כמה קל לפצח סיסמאות.
2. הפץ את נהלי בחירת סיסמאות, לפי ידיעה **31**.
3. אסור באופן מוחלט על העברת סיסמאות בין משתמשים ועל כתיבת הסיסמא במקום בולט.
4. בחר נהלים אוטומטיים ב-**Windows NT** או ב-**Novell NetWare**. קבע את האורך המינימלי והגיל המקסימלי של הסיסמאות. מנע שימוש חוזר בסיסמאות ובחר אחרי כמה ניסיונות חיבור כושלים ינעל החשבון.
5. לפני קבלת חשבון יעבור העובד סדנת אבטחת מידע.
6. הנחה את הקב"ט הארגוני לבצע מבדקי יעילות תקופתיים של הסיסמאות בארגון, ושוב עם הכלים שהזכרנו בידיעה **52**.

445.51– מעבר לסיסמא

הסיסמאות נמנות על שיטות האבטחה הוותיקות ביותר - אבל לאו דווקא היעילות ביותר. למרות כל נהלי הבטיחות, האבטחה עלולה לקרוס בגלל משתמש קל-דעת או בגלל פריצה מתוחכמת. במקומות בהם צרכי הביטחון גבוהים, כגון משרדי ממשלה, חברות היי-טק וארגונים בטחוניים - הסיסמא פשוט אינה מספיקה.

הגישות המתקדמות לאבטחת מידע מתחלקות לשני סוגים עיקריים: אמצעי זיהוי ביומטריים (זיהוי טביעות אצבעות, עיניים קול או פנים) והתקני זיהוי חיצוניים נישאים (כגון כרטיסים חכמים, **IPK Tokens**, ומתאמי סיסמאות דינאמיים). כולם מתאפיינים באמינות גבוהה ביותר, בקלות שימוש יחסית, ביציבות ובאי-תלות במשתמש. בזמן האחרון מחיריהם יורדים בהתמדה, ומדובר כיום בחלופה מעשית שבהחלט כדאי לבחון.

פתרונות מתקדמים יותר, יספקו המוצרים הבאים:

- **Identicator** למשל, מציעה סורק טביעות אצבע המשולב בעכבר או במקלדת - www.identicator.com
- **American Biometric Company** מציעה מגוון פתרונות - החל מקורא טביעות אצבעות ועד כרטיסים חכמים. מידע נוסף באתר - www.abio.com
- **InteliTrak** מציעה תוכנה לזיהוי קולי, שמשלבת סיסמא וטביעת קול - www.intelitrak.com
- **IriScan** תזהה אותך לפי התבנית הבלתי ניתנת לחיקוי של קרנית העין - www.iriscan.com
- **TrueFace** היא תכנת זיהוי פנים, המתאימה לכל מחשב המפעיל את **Windows** - www.miros.com
- כשתחבר את **Ikey2000** למחזיק המפתחות שלך, תדע שרק לך יש גישה למידע המסווג - www.rainbow.com
- **SecurID** של **RSA**, משלבת כרטיס חכם, סיסמאות מתחלפות וסיסמא נזכרת - www.securid.com

445.52– לפרוץ כדי להגן

כדי לדעת עד כמה פגיעות הסיסמאות בארגונך, כדאי לנסות לפרוץ אותן בדרכים שונות. לרוב ניתן **לנחש** את סיסמת המשתמש, במידה והוא בוחר בסיסמא משמעותית מבחינתו, כגון שם של מישהו קרוב, מספר טלפון או ביטוח לאומי. פורצים רבים מחפשים פרטים על האדם שאת חשבונו הם רוצים לפרוץ. אחר-כך באות ההתקפות המילוניות: תוכנות חכמות בודקות ואריאציות של כ-40 אלף מילים הנפוצות ביותר בסיסמאות, כולל שמות פרטיים, שמות משפחה, שמות שחקני קולנוע או כדורגל. התוכנות בודקות גם אפשרות של שילוב מספרים או סימנים בסוף הסיסמא, ואפשרות של רצפי הקשות על המקלדת. רוב הסיסמאות נפרצות כך מהר מאוד. השלב הבא, במקרה ששלב זה נכשל, הוא שימוש בכלים המחפשים חולשות ופרצות ידועות במערכת ההגנה. לעיתים אפשר להשיג בקלות גרסא מוצפנת של הסיסמא - ואז ניתן לפצח אותה בקלות יחסית, במידה וההצפנה היא פשוטה.

- **L0phtCrack** היא התוכנה המומלצת ביותר כדי להתנסות בפריצה. בתוך זמן קצר היא תוכיח לך בדיוק כמה קלות לפריצה הן סיסמאות העובדים בארגונך, וגם תתן ציון על קושי הפיצוח. בעזרת שימוש בטכניקות המתוארות למעלה, ספק אם היא תחמיץ סיסמאות רבות! מומלץ להורדה ולהתנסות ב - www.L0pht.com
- אוסף כלים לפריצת סיסמאות תמצא ב - thn.cjb.net
- **WASP** - התוכנה שתפענח את קובץ ה-**PWL** של **Windows 95/98** ותראה לך כמה באמת הוא מוצפן. להוריד באתר - www.iopus.com/wasp.htm

445.53– המפתח למשרד

הסיסמאות משחקות תפקיד חשוב גם ביישומי מיקרוסופט המוכרים. כולנו מכירים את הסיסמא של תחנת העבודה ב-**Windows NT**, אבל הן שימושיות גם ביישומים אחרים:

- **סיסמא לפתיחת מסמך Office** - לך ל**שמירה בשם**, בחר ב**אפשרויות** והקש את סיסמתך בשדה: **סיסמה לפתיחה.** משתמש שינסה לפתוח את המסמך יתבקש בפעם הבאה להקיש את הסיסמא. עם זאת, סיסמה זו נתנת לפריצה בקלות יחסית בעזרת כלים שניתן למצוא ב**אינטרנט**, ואין להסתמך עליה להגנה על מסמכים מסווגים.
- **סיסמא לשינוי מסמך Office** - לך ל**שמירה בשם**, בחר ב**אפשרויות** והקש את סיסמתך בשדה: **סיסמא לשינוי**. כל משתמש יוכל לקרוא את המסמך, אולם כדי לשנות אותו יהיה עליו לשמור אותו בשם אחר, או להקיש את הסיסמא.
- **קביעת מדיניות ב-Office 2000** - בתפריט **כלים** ביישום **Office** כלשהו, ניתן לקבוע מדיניות הכוללת: חסימת שימוש באפליקציות או בפונקציות מסוימות ב-**Office**. מניעת שינוי הסרגלים והתפריטים וכדומה. כך למשל, בכל פעם שמשתמש ינסה לשנות את אחד מאלה הוא יתבקש להקיש סיסמא.

445.54– מעמיקים ברשת

לעיון מעמיק ורחב יותר, התחל בכתובות הבאות:

- **NetSecurity** של **About**, מציע מגוון כלים ומאמרים בנושא אבטחת מידע - netsecurity.about.com
- **Soft4You** - הוא אתר מסחרי המכיל כמה כלים וכמה מאמרים נהדרים, כולל טבלאות לדירוג סיסמאות לפי זמן הפריצה הדרוש כדי לפצחן - www.soft4you.com
- **InfoWar** הוא אתר מצוין המכיל מלאי מאמרים וכלים. כתובתו - www.infowar.com
- **Info Security Magazine** הוא מגזין מקצועי ומעניין בנושא - www.infosecuritymag.com
- **גם למיקרוסופט** יש מה להגיד בתחום. האתר של **מיקרוסופט** כולל מאמרים, פיתוחים חדשים וגם את אוסף הפרצות הידועות ביישומי **Office**, **Windows** ו-**Explorer**, כולל טלאים הפותרים את הבעיות, להורדה בחינם בכתובת - www.microsoft.com/security
- **Anti Online** - www.antionline.com
- **SecurityPortal** - www.securityportal.com
- **Secure Computing** - www.westcoast.com