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?

תחקיר 608 ● WWW.PCON.CO.IL ● 26 מאי 2003

PCאון ©

למנהלים ומשתמשי מחשב בכירים

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

והפעם... לשתף בלי להחשף

מסר אישי

58% ממנהלי האבטחה מעריכים ששימוש לא זהיר באמצעי תקשורת אישיים כמסרים מידיים (IM) היא הסכנה העיקרית לבטיחות הרשת, ולמרות זאת, פחות מאחוז אחד מהעסקים מאבטחים את סביבת ה-IM שלהם! (לפי נתוני גרטנר). תוכנות IM ושיתוף קבצים ב-P2P, שהותקנו בתום לב, נפוצות מאוד. למרות זאת, אבטחתן והמודעות לנושא, ברמת המשתמש, לוקים בחסר חמור. הנזק עשוי להתבטא בחדירות וירוסים, פריצות, חשיפת או אבדן מידע.

מהי מידת הסכנה? כיצד קורה שסיכון זה אינו מטופל במסגרת מדיניות האבטחה הרגילה? מה ביכולתך לעשות בנידון? - בתחקיר שלפניך.

תמצית החדשות בעולם המחשוב טור

- חדשות בקצרה 3
- בטיחות מעל הכל 3
- **לינוקס** מתקדמת 4
- חלון לעתיד 4

תוכן התדרוך השבועי טור

להתמקד בעיקר

- מחילה מתחת לאף 5
- הארגון בסיכון ? 5
- הבן כדי להתגונן 6

תועלות, הזדמנויות והיבטי רכש

- IM - האפשרויות לבחירה 7
- תרופות להקלה מיידית 7
- במסגרת ארגונית 8

המיוחד ביישומי מחשב בישראל

- משתפים מסרים ולקחים 9
- טיפ ליישום טוב 9
- ארגן ואבטח 10

להעמיק בנושאי מפתח

- שותפות טובה 11
- הבטיחות היא המסר 11
- יום בחיי הארגון 12

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

- כל הזכויות שמורות **לקומרקטינג בע"מ** ©. אין לצלם או להפיץ את הגיליון ללא היתר ובכל צורה שהיא.
- אנו משתדלים להביא מידע אמין ומדויק אולם האחריות לתוצאות השימוש בו תחול על המשתמשים.
- שמות המוצרים והחברות המוזכרים ב-**PCאון**, הם שמות שמורים של בעליהם.
- ככלל המחירים בגיליון הם בדולרים וללא מע"מ. מחירי ספרים ניתנים בש"ח כולל מע"מ.
- לאתרים **באינטרנט** יש להוסיף הקידומת **http://**

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

___ כן אני רוצה להיות מנוי **PCאון**, לתקופה של 3 / 6 / 12 חודשים. אני מצרף סך בשקלים של $119 / $214 / $394 + מע"מ (סמן בחירתך בעיגול), לפקודת **קומרקטינג בע"מ** ומחכה לגיליון הקרוב.

שם מלא_____

ארגון_____

תפקיד בארגון_____

כתובת_____מיקוד_____

טלפון_____פקס_____

תאריך_____חתימה_____

הערות _____

PCאון© למנהלים ומשתמשי מחשב בכירים

608.11– חדשות בקצרה

• **על פי החלטת ועדת הכלכלה של הכנסת, ייפתח שוק הטלפוניה הפנים ארצית לתחרות חופשית בראשון בספטמבר 2004**. ההחלטה באה כפשרה בין שתי הצעות: המלצת דו"ח **ועדת קרול** לקבוע את המועד לאוגוסט 2004 ובקשת משרד התקשורת לדחות זאת לאפריל 2005. אחת המתחרות הבולטות צפוייה להיות חברת הכבלים, אם תקבל אישור להתאחד.

• לפי **גרטנר**, שנת 2002 היתה השנה הראשונה מאז החלה לעקוב אחרי השוק, בה התכווצו רווחיו ביחס לשנה הקודמת. בשל הצורך לצמצם בהוצאות, המשיכו חברות רבות לתפקד עם ציוד ותוכנה קיימים, בין היתר בגלל שלא הוצגו מוצרים רבים בעלי ערך חדשני ומהפכני, שהיו מציעים לרוכשים יתרונות תחרותיים משמעותיים.

• **אוראקל** ו-**SUN** מתכננות להתקרב ולהדק את שיתוף הפעולה ביניהן בכמה יוזמות חדשות ובהן: מבצעי מכירות משותפים ושיתופי פעולה טכניים (למשל בין **SUN StarOffice** לבין **Oracle's Collaboration suite**). בהקשר זה נזכיר גם את שיתוף הפעולה שהוכרז לאחרונה בין **אורקל** לבין חברת **Dell**, בו יוצעו שרתי **Dell** עם **לינוקס** ומסד הנתונים של **אורקל** במחיר מיוחד.

608.12– בטיחות מעל הכל

הימור בטוח הוא... שעולם המחשוב לעולם לא יהיה בטוח ב-100%. בינתיים, לא מוותרים ומשתדלים:

• **זהירות! -** תולעת חדשה מופצת במסווה הודעת **E-Mail** מ**מיקרוסופט** (support@microsoft.com). **Mankx** (או **Sobig.B**) מנצלת את שמה המוכר היטב של **מיקרוסופט** ואת העובדה שרוב המשתמשים הביתיים והארגוניים משתמש במוצריה. שם הקובץ המצורף ונושא ההודעה אינם קבועים. ההדבקה מתבטאת בקובץ **MSCCN32.Exe** בספריית **Windows**, הפעלה עם אתחול והתפשטות באמצעות כתובות דואר שמורות. מעבר ליצירת עומס על הרשת הוירוס אינו גורם נזק, ומומחים משערים כי הוא נכתב כניסוי, אולי לקראת גרסה מתקדמת ומזיקה יותר.

• המשטרה עצרה לאחרונה נער ישראלי, בחשד שכתב וירוס בשם **Yipper** המתפשט ברשת. הנער הודה וסיפר כי הוירוס לא נועד לפגוע אלא לאסוף כתובות **E-Mail** לשם מכירתן למפיצי **Spam**.

• **Network Associates** הציגה את **Weblmmune 2.0** - גרסה חדשה וחינמית לשירות אבטחת וירוסים ברשת. **Weblmmune** מספק הגנה **24 X 7**, עם פונקציות מתקדמות וכלי ניתוח הכוללים מעקב גלובלי רחב ושליחת קבצים באופן מאובטח בטכנולוגיית **SSL** ללא צורך בסיסמא ואבטחה באמצעות פורמט **ZIP**.

• מאגר גדול ומקוון של כרטיסי אשראי שהחזיקה חברה גדולה בארץ נפרץ לאחרונה וגרם נזק של מעל חצי מיליון שקלים. שני חשודים מאילת נעצרו על ידי המשטרה, אך נאסר פרסום פרטי החברה בה מדובר.

• שגיאה במעבדי **Itanium 2** עלולה להפיל שרתים! על פי הודעת **אינטל**, חלק ממעבדיה (בגרסאות **900MHz** ו-**1GHz**) סובלים מכך והחברה תחליפם עבור לקוחותיה במידת הצורך.

608.13– לינוקס מתקדמת

כל הסימנים בשטח מעידים על כך שלינוקס הפכה למוצר חם שאין להתעלם ממנו, לקוחות כספקים:

• **SCO** תובעת את **IBM** על שימוש ב**לינוקס**, ואף הפיצה אזהרה למשתמשי המערכת, על בסיס טענה כי גרסות **לינוקס** מסחריות רבות כוללות קוד שהיא כתבה עבור **יוניקס**. משתמשי **לינוקס** ארגוניים אף הוזהרו מפני צעדים משפטיים העלולים להינקט נגדם עקב הפרת זכויות יוצרים כזו. לאחרונה מותנה אזהרה זו - **SCO** ציינה כי פעלה לפי המלצות עורכי דינה וכי אין כרגע כוונה לתבוע משתמשים.

• **מיקרוסופט** תרכוש מ-**SCO** קוד מקור של **יוניקס**, צעד שיסייע לה להתמודד מול **לינוקס**. **IBM** בתגובה הודיעה כי צעד זה אינו משנה את סרובה לשלם תמלוגים ל-**SCO**.

• **מיקרוסופט** מפעילה את ה-**Education and Government Incentive program** - תכנית המאפשרת לה להציע לממשלות מוצרים במחיר זול במיוחד, זאת על פי דיווח **ComputerWorld**. זאת כפי הנראה עקב העובדה שממשלות רבות שוקלות תחליפי **לינוקס** זולים למוצריה.

• על הורדות מחירים של **מיקרוסופט** בנסיון להילחם ב**לינוקס** מרמז גם העיתון **אינטרנשיונל הראלד טריביון**. לטענתו, מדובר באסטרטגיה הנחשפת על פי מסמכים פנימיים של החברה שהגיעו לידיו.

• **Sendmail**, יצרנית פתרונות ה-**Messaging** מפתחת שרת דואר מבוסס לינוקס בשיתוף **HP** ואינטל. מטרתו למשוך לשימוש בדואר גם עובדים ניידים שלרוב אינם נעזרים בו, בסיוע פלטפורמת **Centrino** האלחוטית של אינטל.

• דפדפן **אופרה** יצא בגרסה **ל לינוקס**. התוכנה כוללת ייצור קישורים לפי דף בו ביקרת, גלישה "אחורה" לפי דומיינים קודמים בהם ביקרת (ולא דפים) ועוד - www.opera.com

608.14– חלון לעתיד

חלונות XP רק בת כ-20 חודש וכבר נראית באופק גרסת חלונות החדשה Longhorn, האמורה להופיע בשוק בשנת 2005. משמועות ראשוניות על סמך גרסאות אלפא ומפרטים מעטים שפורסמו על ידי החברה, ניתן לספר על המערכת כמה פרטים ראשוניים: מערכות קבצים חדשה בשם **WinFS**, המבוססת על עקרונות בסיס נתונים, תשפר יכולות אחסון ותאפשר גישה נוחה ואינטואיטיבית יותר. ה-**Desktop** יכלול מראה מתוחכם יותר, שיעשה למשל שימוש בחלונות שקופים למחצה. המחיר יהיה גידול בצריכת משאבי מחשוב. למרות שנראה כי בעתיד יהיו המחשבים האישיים מהירים וזולים יותר, לא בטוח שארגונים ימהרו לשדרג חומרה בהתאם. גם טכנולוגיית האבטחה השנויה במחלוקת **Palladium** תיכלל בגרסה זו. היא אמורה לספק למערכת שליטה משופרת על האבטחה בעזרת פעולה גם ברמת החומרה. יכולות אלה יקלו על **מיקרוסופט** לזהות משתמשים ולעקוב אחר גרסאות לא חוקיות. יש הטוענים שהן גם יסכנו פרטיות משתמשים.

בינתיים, **גרטנר** מציינת כי יותר ויותר ארגונים מחפשים אלטרנטיבות זולות למוצרי **מיקרוסופט**, כשמובילות את המגמה חברות מחוץ לארה"ב. גם המוטיבציה לשדרוגים במסגרת מוצרי **מיקרוסופט** נחלשת: לפי **גרטנר**, עד 70% משרתי חלונות הקיימים רצים על **NT 4** ובסוף 2004 רק כשליש מהם ישודרגו ל-**Windows Server 2003**.

608.21– מחילה מתחת לאף

לפי Forrester Research, כשליש מהמבוגרים בארה"ב כבר משתמשים בתוכנות מסרים מידיים (Instant Messaging). **Radicati Group** חוזה כי מספר המשתמשים הארגוניים יצמח מ-41 מיליון בשנה שעברה ל-67 מיליון השנה, ועל פי **גרטנר**, פתרון מסרים מידיים יותקן השנה בלפחות 70% מהארגונים הגדולים. מסתבר כי בארגונים רבים כבר נפוצות תוכנות כאלה גם באופן בלתי רשמי, כשלצידן תמצא תוכנות **Peer To Peer (P2P)** המשמשות לשיתוף קבצים **(File Sharing)**. הצרה היא שהמנמ"רים לרוב לא מודעים להיקף השימוש הנרחב בתוכנות ולכך שמדובר באוסף סכנות אבטחה חדשות, המחייב טיפול מונע ובהקדם.

בדומה לשימוש ב-**E-Mail** ואף יותר מכך, תקשורת כזו פותחת פתח להעברת קבצים ישירה וזריזה, לחדירת **Spam** וקוד עוין ואף לדליפת מידע רגיש מחוץ לארגון. כבר במאי 2001 הזהירה **מיקרוסופט** מוירוס **W32/Hello** שהופץ ב-**MSN Messenger** כקובץ **Hello.exe** והפיץ עצמו לאחר ההפעלה לכל החברים בספר הכתובות של הנדבק. מאז הופצו וירוסים רבים שמנצלים אפשרות העברת קבצים בתוכנות מסרים מיידיים, וגם בתוכנות שיתוף קבצים. בעייה נוספת בתוכנות שיתוף קבצים היא יצירת מעמסה גדולה על הרשת. מספר עובדים קטן יחסית שמשתמש בהן עלול לגרום להאטת תעבורה לכל הארגון.

הפתרונות לסכנות אלו זמינים ואינם מסובכים ליישום. מדובר בשימוש זהיר בתוכנות בסיסיות קיימות, דוגמת יישומי מסרים מידיים שב**חלונות** או בשימוש בתוכנות מתקדמות שפותחו במיוחד לארגונים **(Enterprise Instant Messaging - EIM)**, תוך הדגשת טכניקות אבטחה כניטור פעילות והצפנה.

הצפי הוא ששימוש ארגוני בתוכנות מסרים מידיים ושיתוף קבצים על סכנותיהם יתרחב ויגיע גם למכשירי מחשוב ניידים כ-**PDA**. מאחר וטכנית התוכנות אינן מורכבות ביחס ליישומים ארגוניים אחרים, ניתן לצפות שהתחרות ביניהן תתמקד בין השאר ברמת האבטחה. **מטה גרופ** מעריכה כי הדבר יתבטא בהצפנה, בפתרונות **PKI** כתוספים למוצרי **IM** ובמדיניות הגנה ארגונית שתתרחב מה-**E-Mail** לתוכנות אלה עם טכניקות התגוננות דומות (מפני וירוסים ו-**Spam**).

חשוב לאזן את התמונה ולהדגיש שתוכנות מסרים מידיים ושיתוף קבצים צפויות להיות חלק לגיטימי ואף חיוני מהמחשוב הארגוני, וכבר עתה מציעות יתרונות עסקיים שכדאי לשקול, ביניהם: שיפור התקשורת הפנים ארגונית, צמצום הוצאות סטנדרטיות לתקשורת ולנסיעות, שכלול עבודת עובדים וסניפים מרוחקים וצמצום תעבורת ה-**E-Mail**. בגלל כל אלה מומלץ שלא למהר ולהכריז על וויתור גורף.

<u>לסיכום - בדוק מיידית שימוש בלתי מורשה בתוכנות אלה בארגונך, ונקוט בצעדים להפחית כמה שניתן את הסיכונים. מצד שני, היה מודע לפוטנציאל העסקי הגלום בהן.</u>

608.22– הארגון בסיכון ?

מהן הסכנות הגלומות בתוכנות אלו?

1. **ערוץ לעומק הארגון -** תוכנות מסרים מידיים ושיתוף קבצים יוצרות קשרים ישירים ועשירים בין מחשבים ברשת הארגונית למחשבים מחוצה לה. אלו דלתות ל"עומק" הארגון ולמידע רגיש. לדוגמא: פעולות המתבצעות דרכן חושפות את כתובת ה-**IP** וכך חושפות את המחשב הספציפי לתקיפות.
2. **חדירת קוד עויין -** ארגון האבטחה **CERT** הזהיר כי התקבלו כבר עשרות אלפי דיווחים על האקרים השולחים הצעות לקבלת תוכנות כעזרי האצת גלישה. בפועל תוכנות אלה משתילות **Backdoor** המאפשר מאוחר יותר השתלטות מרחוק על מחשבך. נזק אפשרי נוסף הוא רתימת המחשב להתקפת **DDoS (Distributed Denial of Service)**.
3. **חשיפת מידע רגיש -** האוירה בצ'טים - במיוחד ישירים ו"פרטיים" בנוסח **IM** - מעודדת חופשיות שעלולה להביא לחשיפת מידע רגיש (בו בזמן קל מאוד לצד השני לשמור **Log** של שיחות כאלה בלי שתדע) ודליפת חומר ארגוני החוצה.
4. **חשיפת פרצות מהירה -** החשפותן המהירה של תוכנות אלה לקהל ביתי רחב, מביאה לחשיפת פרצות במהירות יחסית. אלה עשויות להיות מנוצלות באותה מהירות ליישום תכסיסי התקפה.
5. **חשיפה ל-Spam -** לאחרונה מסתבר כי תוכנות מסרים מידיים התגלו גם על ידי ספאמרים כערוצים לפרסומות אגרסיביות לא רצויות, שיבזבזו את זמנך ואת זמן העובדים גם אם לא יגרמו לנזק אחר.
6. **שימוש בלתי מורשה -** התוכנות עשויות להיות מותקנות ומופעלות בקלות על ידי משתמשים שלא מודעים לסכנה וללא ידיעת המנמ"ר. רבים רגילים לכך משימוש ביתי שבו הן נתפסות ככלי בטוח לשימוש. מסיבה זו אופייני שהיישומים חודרים לארגונים ביוזמת המשתמשים עצמם, עוד לפני יישום ארגוני מסודר. בכך הם גם יוצרים בעיית ניהול מבוקר.
7. **מוצרים בלתי בשלים -** בשוק נמצאות תוכנות רבות שהינן חדשות יחסית ולכן לא בשלות או מדובגות די הצורך. לדוגמא: פרצה בתוכנת שיתוף הקבצים הפופולרית **BearShare** איפשרה להוריד מהמחשב גם קבצים שלא הוגדרו כמשותפים.

608.23– הבן כדי להתגונן

אלו האמצעים העומדים לרשותך לאבטחת התוכנות למסרים מידיים ולשיתוף קבצים:

- **מודעות ארגונית -** אמצעי ההתגוננות הראשון במעלה הוא יצירת ושמירת מודעות המשתמשים לסכנות. זאת מאחר ו<u>משתמש שאינו מודע לסכנות הוא גורם הסיכון העיקרי</u>.
- **כללי שימוש ברורים -** התנהגות מונעת שתבוסס על הגדרת מדיניות ארגונית ברורה, תצמצם שימוש בלתי מורשה ותמנע אי הבנות לגבי שימוש בטוח או מסוכן.
- **בחירת תוכנות זהירה -** בתחומים חדשים אלה מבחר התוכנות גדול, עם הבדלי איכות גדולים בין האחת לרעותה. בחירה זהירה בפתרונות **IM** ושיתוף קבצים בשלים ומתקדמים יחסית - מוטב כאלה המיועדים במיוחד לארגונים - תבטיח מינימום חשיפה לנזקים.
- **פתרונות בלימה -** בדומה לטיפול המוכר בוירוסים, פתרונות אבטחה שונים יכולים לנטר ולצמצם תעבורת מסרים מידיים ושיתוף קבצים. פתרונות כסינון תוכן, הגבלת גלישה, **Firewall**, **Airgap** עשויים לצמצם פורטים פתוחים, להגביל גדלי קבצים מועברים או להתריע על פעילות חשודה.
- **פתרונות ניטור וסריקה** - פתרונות אבטחה מבוססי ניטור התנהגות יישומים לתפיסת הנוזקה כשהיא מופעלת **(Real Time)** או סריקת קבצים על פי דרישה **(On Demand)** לקבצים שהתקבלו דרך התוכנות.
- **הצפנה להשלמת ההגנה** - הצפנה תסייע לך במידה ותוקף כבר חדר למערכת ומנסה לאחזר ממנה מידע רגיש. פתרונות כאלה תמצא בשפע, דוגמת **SecureSentryPro** של **Aliroo** **($125)** המצפין אוטומטית מידע רגיש. (☎ 03-6345552).

608.31 – IM – האפשרויות לבחירה

כבר בסוף שנה שעברה זיהה מחקר ינקי גרופ את האבטחה הבלתי מספקת כגורם מעכב לאימוץ תוכנות מסרים מידיים בארגונים. המחקר הוסיף והגדיר מגמת התפצלות במסרים המידיים לכמה כיוונים ביניהם יצטרך כל ארגון לבחור:

1. **פתרון פומבי** - זהו כעיקרון פתרון לצרכן הפרטי כמו **AOL Instant Messaging** או **MSN Messenger**. רמת האבטחה לרוב בסיסית ומומלץ לישמו בזהירות, כאופציה זולה המתאימה לשימוש מצומצם או במסגרת ניסוי ראשוני.
2. **פתרון מותגי** - פתרונות כ-**Lotus Sametime** או **Novell Groupwise** בנויים מהיסוד עבור ארגונים, על כל המשתמע מכך מבחינת גישה לניהול ולאבטחה. לדוגמא: כל הזדהות המתחברים מנוהלת דרך שרת ואתה בטוח יותר בזהות המשתמש שמולך. מומלץ עבור שימוש נרחב או רגיש במיוחד.
3. **פתרון פנים ארגוני המתחבר לפומבי** - ישנם גם פתרונות מסרים מידיים המשפרים אבטחת תקשורת בין תוכנת מסרים מידיים פנים ארגונית לתוכנות פומביות כאלה. לדוגמא: **AIM Enterprise Gateway** מנהל קשר בין משתמשי תוכנת **AIM Messenger** מאחורי **Firewall** ארגוני למשתמשים הפרטיים ב-**AIM** - enterprise.netscape.com/products/aimsvcs והחל מ-**Exchange 2000** נכללת בשרת **אקסצ'יינג'** שרת **Messenger** ארגוני מאובטח בשם **IM Service**.
4. **פתרון פתוח** - פתרונות קוד פתוח מסופקים לרוב חינם כמו תוכנות פומביות נפוצות ויאפשרו לך התאמה אישית משופרת של היישומים. לדוגמא: **Jabber** - www.jabber.org
5. **שרות IM** - סוג נוסף של פתרון מסרים מידיים הוא **Hosted IM Solution** - פתרון בתשלום המתאים לארגונים גדולים מבוזרים, ליישום זמני או כדי להתרשם מהטכנולוגיה. לדוגמא: **Omnipod** - www.omnipod.com

608.32 – תרופות להקלה מיידית

אלו כמה מוצרים שיסייעו לך בהתגוננות:

- **נץ מחשוב** - **InVircible** היא מערכת הגנה בזמן אמת מפני נוזקה, הכוללת שליטה מרכזית לדיווח ותגובה בזמן אמת ממקום מרכזי ובכח אדם מצומצם. המחיר: **$235** לשנה ראשונה לחמישה משתמשים. ☎ 03-9027777.
- **Akonix** - **Akonix L7** הוא פתרון המשפר אבטחת שימוש ארגוני בתוכנות מסרים מידיים ושיתוף קבצים ציבוריות (דוגמת **ICQ**). הוא כופה שימוש בגרסאות עדכניות, מגן מפני **Spam** ווירוסים, מאפשר משלוח התראות, הפקת דו"חות ועוד - www.akonix.com
- **Blue Coat Systems** - מספקת פתרון לאבטחה, ניהול, שליטה ובקרת תשתיות **האינטרנט** בארגון - בהתקן חומרה. המוצר כולל אבטחת תוכנות מסרים מידיים של **Yahoo, MSN ו-AOL.** החל מ**$3,500**- ל-**Appliance** מדגם **SG-400-0**. **PF1 Systems** ☎ 03-7679284.
- **CheckPoint** - זו הייתה בין החלוצות בהתאמת פתרונותיה לטיפול גם בתעבורת מסרים מידיים ו-**P2P**, במסגרת המוצר הנפוץ **FireWall-1.** למחירים ראה - pricelist.checkpoint.com
- **BitDefender** - מציעה פתרונות תוכנה חינמיים להגנת סביבות המסרים המידיים **ICQ**, **Yahoo! Messenger**, **NetMeeting**, **MSN Messenger** ו-**mIRC**. - www.bitdefender.com/html/instant_messaging.php
- **IMpasse** - **IMpasse Systems** הוא פתרון תוכנה המשמש ל"חיזוק" תוכנות פופולריות למסרים מידיים באמצעות הצפנה. מחירו **$19.99** - www.im-passe.com
- **Ipswitch** - תוכנת המסרים המיידים **Ipswitch Instant Messenger** מכילה רכיב הצפנה לתקשורת בטוחה בין משתמשים. **$695**. **רנסאנס** (☎ **09-7643571**).
- **NetIQ ImMarshal** - **NetIQ ImMarshal ל-MSN Messenger** מיועד לאכיפת מדיניות שימוש ארגונית במסרים מידיים (**IM**). הוא מספק ניתוח תוכן בזמן אמת, ניהול גישה, ארכיון שיחות, בקרת העברת קבצים ודו"חות פעילות וכן אכיפת כללים ופעולות שנקבעו מראש. מחיר מומלץ לעד 75 משתמשים: **$1,528**. **פייניזילבר הנדסה** (☎ **09-8859611**).
- **Norton** - מוצר האנטי וירוס **Symantec Antivirus Enterprise Edition** כולל גם סריקת תעבורת מסרים מידיים לקוד עויין. מחירו מתחיל מ-**$45** + **$49** לכל רשיון. **כלנית** ☎ 03-6253030.

608.33 – במסגרת ארגונית

כמה פתרונות שמציעות סביבות ארגוניות מבוססות מבחינת מסרים מידיים ושיתוף קבצים:

- **מיקרוסופט** - **MSN Messenger** (messenger.msn.co.il) הוא פתרון מסרים מידיים חינמי נפוץ ו-**Windows Messenger** היא גרסתו המובנה ב**חלונות XP**. גם במסגרת **Microsoft Exchange** תמצא פתרון בשם **Instant Messaging Service**. **מיקרוסופט** מתכוונת להציע בעתיד פתרון **IM** ארגוני בשם **MSN Messenger Connect** בעל תכונות אבטחה, ניהול וארכיב משופרות. בין השאר ייכללו אזורי שליטה ובקרה פנים ארגוניים על מסרים מידיים. המוצר מתוכנן לעלות כ-**$24** למשתמש. עם הכרזת **Windows Server 2003** הוצג גם שרת **IM** ארגוני מתקדם בטכנולוגיית **.NET**. בשם **Real-Time Communications Server** (לשעבר "**Greenwich**") - שייצא כתוסף ברבעון השלישי של 2003, ויאפשר אינטגרציית פלטפורמת מסרים מיידים מאובטחת עם מערכת ההפעלה.
- **IBM** - **Lotus Sametime IM** הוא חלק מפתרון ה-**Conferencing** והמסרים המידיים **Lotus Sametime** (**$40** למשתמש). הפתרון מצפין שיחות **IM** וגם מאפשר העברת קבצים (אם כי לא **Sharing**). ☎ 03-9188451.
- **Novell** - **Novell Groupwise** (החל מ**$650**- ל-5 משתמשים) מאפשר בין השאר שימוש ארגוני בטוח במסרים מידיים. זאת על ידי הגנתם בתוך הארגון בעזרת **Firewall** ארגוני ומחוצה לו בעזרת **VPN**. ☎ 09-9514455.
- **Sun** - **Sun One Instant Messaging 6.0** הוא שרת מסרים מידיים התומך בתקשורת מוצפנת **SSL** בין שרתים ובין שרת ללקוח. סביבת פיתוח מאפשרת לישם מנגנוני הזדהות מתקדמים ו-**Message Conversion API** מאפשר לתפור עבורו גם יישומי אנטי וירוס או אנטי ספאמינג מיוחדים. ☎ 09-9710506.

PCאון© למנהלים ומשתמשי מחשב בכירים

608.41– משתפים מסרים ולקחים

מהשטח קיבלנו כמה תובנות נוספות על השימוש הארגוני בתוכנות מסרים מידיים ובשיתוף קבצים:

לדברי **צבי נתיב**, מנכ"ל **נץ מחשוב** (☎ 03-9027777), וירוסים כפי שהכרנו בעבר כמעט ואינם קיימים כיום והנושא החם הוא **Malware** המתפשט על גבי **Shares**. זו הבעיה המרכזית של אבטחת המחשוב כיום והשלכותיה הרבה יותר רחבות. כשמסתכלים על המגמות בתחום, ברור שכותבי **Malware** למדו "לנצל הצלחה" וזיהו היטב כי הפצה בעזרת זחילה על גבי **Sharing** הוא הכיוון המבטיח ביותר. לכן, אין כמעט נוזקה חדשה שלא כוללת רכיב זחילה על אזורי שיתוף, או מבוססת כולה על כך. הכיוון החדש התחיל להסתמן בצורה בולטת באוקטובר 2002 עם נוזקה כ-**BugBear** ו-**Opasoft**. **צבי** אומר כי אנטי וירוסים קלאסיים אינם מתמודדים עם התופעה, באופן גורף. לפני חמש שנים ויותר הדגש היה על סריקה, אך היום אין בכך טעם, אלא רק להגנה בזמן אמת. השימוש בסריקה כיום דומה לפתיחת מטריה אחרי הגשם.

זמיר סיון, מנהל טכני ב**פיינזילבר הנדסה** (☎ 09-8859611) מתאר זאת כחור אבטחה גדול מאוד בארגונים היום. יש פה בעיית מודעות וכך קורה ש"בדלת האחורית" נכנסים קבצים דרך ה-**Instant Messaging**. לדבריו, רוב השימוש שנעשה בתוכנות הוא לא לצרכי עבודה ומדובר בבזבוז זמן עבודה יקר וגם בצריכת רוחב פס העולה פלאים. השימוש בתוכנות מסבך מאוד את אתגר האבטחה. זאת בעיקר בגלל ריבוי תוכנות, שכל אחת עובדת על פורטים אחרים. לגבי יישום מסודר של תוכנת מסרים מיידיים בארגון, **זמיר** מעיר שבסופו של דבר אנשים אוהבים לעבוד עם מה שהם רגילים, וישתמשו גם בתוכנות לא מורשות. ברוב המקומות חוסמים זאת לחלוטין על ידי חסימת פורטים בחסימה גורפת שמונעת שימוש בתוכנות, כאשר מסרים מידיים הם כלי עבודה שחבל לא לנצל.

608.42– טיפ ליישום טוב

ישם טיפים אלה לשיפור הבטיחות בשימוש הארגוני בתוכנות מסרים מידיים ושיתוף קבצים:

- **ישם מוצרים משולבים** - אם יש צורך בשיתוף קבצים, חפש זאת במסגרת יישומים ארגוניים למסרים מידיים. ערך מוסף שלהם עשוי להיות ניהול משותף ובטוח יותר.
- **הגבל שיתוף קבצים** - בטל תכונות ברירת מחדל לשיתוף קבצים ביישומי המסרים המידיים. אם כבר מדובר על שיתוף קבצים, הנחה עובדים שלא לאפשר זאת על כל הדיסק הקשיח, אלא רק בספריה מיוחדת לכך. המנע והזהר את העובדים להמנע מהורדת קבצים לא ידועים ובמיוחד מהפעלת קבצי הפעלה שנשלחו אליהם, אפילו מעמית, כל עוד אינם יודעים בוודאות במה מדובר.
- **מנע כתיבה לדיסק** - עד כמה שניתן, הגבל את קהילת משתפי הקבצים לקריאה בלבד מספריות מקומיות (הנחה עובדים שלא להגדיר הרשאות כתיבה לספריה המיועדת לשיתוף קבצים).
- **הצפן הודעות** - הגדל בטיחות בעזרת הצפנה. חפש תכונות כאלה בתוכנות השונות, לגבי השיחות עצמן ולגבי רישומיהן (**Logs**). על פי **מטה גרופ**, תוך כשנתיים תהיה ההצפנה בשימוש סטנדרטי בתוכנות האלה.
- **צמצם דיבור עם זרים** - כשניתן, הגבל את ה-**IM** לתקשורת פנים ארגונית בלבד. בארגון גדול זו יכולה להיות פעילות **IM** ענפה ומועילה ב**אינטרה-נט** בלבד או בארגון רב סניפים, פעילות המוגבלת לסביבת **VPN**.
- **צמצם שימוש מקוון** - עבוד עם התוכנות כפי הנדרש, אך עודד עובדים להתנתק מהרשת כשניתן. אם תוכנות הניהול מאפשרות זאת, השתמש בהן לחסימת תקשורת כזו בזמנים מסויימים, כהפסקות ומעבר לשעות העבודה.

דגש – גם ביוניקס

לא רק למערכת ההפעלה חלונות - גם לסביבות יוניקס ולינוקס תמצא גרסאות של תוכנות מסרים מידיים ושיתוף קבצים. מבחר התוכנות מצומצם ביחס למוצע לסביבת **חלונות**, אך לא בהכרח באיכות נמוכה. מבחינת אבטחה, מדובר במערכת הפעלה שעמידותה לנוזקה גדולה בכמה סדרי גודל - כתיבת נוזקה עבורן פחות "מתגמלת" (מייצרת פחות "רעש" תקשורתי), האפשרויות הטכניות עבור כותב הנוזקה מצומצמות ביחס ל**חלונות** והמערכות נחשבות בטוחות יותר מיסודן. עם זאת, חשוב להקפיד גם בהן לנצל את תכונות האבטחה השונות שמציעות תוכנות מתקדמות. שתי דוגמאות בולטות לפתרונות מסרים מידיים חינמיים ואיכותיים המפותחים בקוד פתוח הן התוכנות **Gaim** (**gaim.sourceforge.net**) ו-**Jabber** (**www.jabber.org**).

608.43– ארגן ואבטח

אבטח השימוש בתוכנות מסרים מידיים ושיתוף קבצים בארגון, בעזרת שלבים אלה:

1. **תפוס שליטה** - דאג לשליטה בשימוש הארגוני במסרים מידיים והפסק מיידית כל שימוש בלתי מורשה. בהתאם להיקף השימוש ולצורך בניטור הפעילות, ישם שרת מרכזי לניהול ולניטור דוגמת הפתרונות של חברת **WiredRed** - www.wiredred.com
2. **הגדר מדיניות** - צור והפעל מדיניות שימוש ברורה לתוכנות המסרים המידיים ושיתוף הקבצים. התייחס לתוכנות מורשות, שימושים ארגוניים לגיטימיים וכיוונים (**Settings**) הכרחיים שרלבנטיים לאבטחה.
3. **צור מודעות** - צור מודעות ארגונית לנושא בעזרת הדרכה, במיוחד לעובדים חדשים, כך שלא יופיע מחדש שימוש בלתי מורשה. דאג לשמר את המודעות שיצרת בעזרת המחשה מתמדת: ידע עובדים על חדשות עדכניות המדגימות סכנות כאלו. מודעות זו היא קו ההגנה הראשון והחשוב ביותר מפני נזקי יישומים אלה!
4. **שקול פתרון ארגוני** - אם מדובר בנושא שהפך להיות מיושם באופן נרחב בארגון ומידת בטיחות היישום המשמש לכך מוטלת בספק - עבור לפתרון איכותי יותר, המיועד ספציפית לארגונים. בדוק האם יש מקום להרחיב או להתחיל שימוש במסרים מידיים או בשיתוף קבצים. סביר שתמצא אפשרויות התייעלות מעניינות במחיר נמוך (ראה תחקיר **568**). שיתוף קבצים בינתיים שימושי פחות (ראה תחקיר **502**).

608.51– שותפות טובה

יישום טכנולוגיית שיתוף הקבצים למטרות ארגוניות עסקיות עדיין אינו נפוץ במיוחד, אך ישנו שימוש בלתי רשמי רב ביישומי שיתוף, לצרכים פרטיים כהורדת קבצי מוזיקה. אי הידיעה על פעילות כזו פותחת פתח משמעותי לאיומי אבטחה וכבר נכתבו וירוסים להפצה במיוחד למדיה זו, דוגמת **Duload** שהופץ בין משתמשי **Kazaa**. **צבי נתיב**, מנכ"ל **נץ מחשוב**, מספר כי מצא וירוסים שנכתבו במיוחד עבור **Kazaa** בלפחות שני ארגונים מקומיים גדולים. האחד הוא מפעל הייטק בו "עבריין" האבטחה היה מנהל המחשוב בכבודו ועצמו. לדבריו, אנטי וירוס קלאסי לא מסוגל למנוע חדירת קוד עוין המושתל מרחוק דרך **Share**, אלא רק להתריע לאחר שהוחדר. מנהלי מחשוב עדיין מטפלים בנושא בשיטות שהיו רלוונטיות לפני עשר שנים. הגנה מפני **Agents** כאלה לא ניתן להשיג באמצעות סריקת קבצים, אלא רק ע"י ניטור התנהגות מערכת ההפעלה והיישומים, בזמן אמת. מה שהתחיל עם **נאפסטר** הידועה, המשיך עם תוכנות שיתוף חופשיות רבות ובהן **Kazaa**, **Aimster**, **Gnutella** ו**מורפאוס**. חלקן מתייחסות לנושא האבטחה. לדוגמא: **eDonkey** - יישום שיתוף קבצים המסייע לזהותם בעזרת חתימה דיגיטלית ייחודית. עם זאת, בינתיים אין להן שימוש משמעותי בארגונים ולכן מוטב שלא להתקין **Clients** לתוכנות כאלו.

מעבר לכך, קיים תמיד הסיכון שנובע מההיבט הלא חוקי של שיתוף מוסיקה ותוכנות באמצעות תוכנות כגון אלה. ארגון שייתפס כשמחשביו משמשים להעתקת חומר מוגן בזכויות יוצרים עשויי להפסיד יותר מאשר כמה מאות דולרים. במידת הצורך, קבצים יכולים להישלח במדיום רגיל של **E-Mail** או להיות משותפים באמצעות פתרון המאפשר פעולות **Peer To Peer** (כ"ט ושיתוף קבצים) ושתוכנן במיוחד ליישום ארגוני בטוח.

608.52– הבטיחות היא המסר

יישומי IM נפוצים באופן רשמי או לא ב-84% מהארגונים ונתון זה צפוי לטפס ל-93% עד סוף השנה (Osterman Research). על פי **IDC**, מספר המשתמשים הארגוניים צפוי להגיע עד 180 מיליון בשנת 2004. מאחר וכניסתן לארגון מציגה מיידית שלל סכנות, יש המכנים אותן בצחוק, מנקודת מבט של מנהל מחשוב, דווקא **Instant Headache**. בשנה שעברה, לדוגמא, נמצאה בסביבת **MSN Messenger** הנפוצה תולעת שכונתה **JS Exploit-Messenger**. תולעת זו ניסתה להפיץ עצמה בעזרת רשימת אנשי הקשר שבתוכנת המסרים המיידיים - שיטה המוכיחה עצמה היטב בהעברת וירוסים ב-**E-Mail**. נוזקה כזו מנצלת בין השאר את קלות כתיבת הסקריפטים ברוב תוכנות ה-**IM** הפופולריות. עם זאת, המודעות אצל ספקי התוכנות לנושא האבטחה עולה. כמה דוגמאות להמחשה: חברת **FaceTime** משלבת במוצרי ה-**IM** שלה פתרונות אנטי וירוס של **מקאפי** (www.facetime.com). **Yahoo Messenger Enterprise Edition** (enterprise.yahoo.com) ו-**AIM Enterprise** של **AOL** (www.aim.com/get_aim/enterprise) הן גרסאות ארגוניות משופרות, עם ניהול מרכזי, חסימת משתמשים, רישום וניטור שיחות והפקת דו"חות. **ICQ** מציעה עזרה מפורטת לנושא האבטחה, כולל הסתרת כתובת **IP** ופרטים אישיים, התגוננות מוירוסים ו-**spam** והגנת סיסמאות (www.icq.com/support/security). **Trillian** של **Cerulean** נחשב פתרון **IM** בטוח יחסית מיסודו, המאפשר אותנטיקציה, מצפין מידע ואף את השיחות עצמן (חינם ב-www.trillian.cc). **Imlogic** מציעה את **IM Manager 5.0**, הכולל סריקת וירוסים, סינון תוכן ומניעת **Spam** (www.imlogic.com).

דגש – ה-Spam אשם

מטרד חדש המתפשט בתוכנות מסרים מידיים ונמצא על גבול תחום האבטחה, הוא Spam. שולחי הודעות אלה עשויים לאסוף עליך מידע שיווקי חשוב גם באמצעות תוכנות שיתוף קבצים (למשל איזו מוזיקה בדיוק אתה אוהב). איסוף מידע כזה באמצעות תוכנות **Spyware** המותקנות עם יישום שיתוף הקבצים, הוא מקור הכנסה המאפשר לתוכנות להיות מוצעות בחינם. תוכנות כ-**MSN Messanger** מאפשרות לשוחח רק עם מי שנתת הסכמתך לקבלת מסרים ממנו וכך מקטינות את המטרד. תוכל גם להכניס שולחי **Spam** ל-**Block List**.

608.53– יום בחיי הארגון

דני, המנמ"ר החדש ברשת חצילים בע"מ, התבקש לטפל בדחיפות במגפת הנוזקה שפשטה בארגון לאחרונה. נראה שיש לכך מקור שלא אותר כהלכה. בסיכום התחקיר המוגש למנכ"ל מוזכר כי: כעשרה עובדים, רובם מאגף הפיתוח, משתמשים אינטנסיבית ב-**ICQ**, בעיקר לצרכים פרטיים. עוד כמה עובדים מהשיווק התרגלו לשימוש ב-**Windows Messenger** לצרכי תקשורת מהירה מול סניפים מרוחקים ולהחלפת קבצים קטנים - לצרכי עבודה, וכפי הנראה לא רק. והפתעה לסיום: נראה ש**ירוחם** מהנהלת החשבונות התקין **Kazaa** ומשתמש ברשת הארגונית המהירה להורדת קבצים מסוג שלא בדיוק קשור לעיסוקו.

דני ממליץ להפסיק מיידית שימוש בלתי מורשה בתוכנות מסרים מידיים ושיתוף קבצים, לארגן במהירות הדרכה ראשונית מתאימה לעובדים, אך גם לבחון לעומק את התועלות העסקיות של שימוש מסודר בתוכנות מסרים מידיים, תועלות שאגף השיווק התחיל כבר לנצל כאמור, מתוך צורך ממשי וזמינות הפתרון במסגרת **חלונות**.

חודשיים לאחר מכן: תוכנה ייעודית ליישום מסרים מידיים בארגונים מסדר גודל של **חצילים בע"מ** מופעלת רק בידי עובדים מורשים מאגף השיווק וכמה אנשי הנהלה. מגפת הנוזקה חלפה ואיננה עוד. ולסיום - תופעה בלתי מוסברת חדשה: **ירוחם** מהנה"ח עובד פחות שעות נוספות, אבל מספיק הרבה יותר.