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 612 ● WWW.PCON.CO.IL ● 23 יוני 2003

PCאון ©

למנהלים ומשתמשי מחשב בכירים

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

והפעם... איך למנוע מעילות והונאות ?

מסר אישי

מה המשותף בין הוצאת מספרי כרטיס אשראי במירמה לעובד עירייה המזין דו"חות כוזבים? בשניהם מדובר בכשלים תפעוליים שמאפשרים להוציא כספים או נכסים במרמה מהארגון. בעוד שהונאות מערבות גורם חיצוני, במקרה של מעילות מדובר בגורם פנימי. באירועי מעילות והונאות רבים שנותחו, נמצא שילוב בין השניים. לכן ארגונים - וארגונים פיננסים בפרט - חייבים ליישם כנגדם בקרות מספקות, במיוחד עם פתיחת המערכות לעולם החיצון.
השימוש הגובר במחשוב לניהול פיננסי הופך אותו לערוץ מועדף להונאות ומעילות. בו בזמן מספק המחשוב גם פתרונות לאיתורן ומניעתן. כיצד תמנע מהעוקץ ותהנה מהדבש? - בתחקיר שלפניך.

תמצית החדשות בעולם המחשוב — טור

תוכן התדרוך השבועי — טור

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק** B.Sc. ,MBA
עורך - **ערן דרור**
תחקיר וכתיבה - **עמית לוי**
טלפון - **03-9667939**, פקס - **03-9660310**
דואר - **ת.ד. 2340 ראשון לציון 75121**
E-Mail - editor@pcon.co.il

לתשומת לבך

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

___ כן אני רוצה להיות מנוי **PCאון**, לתקופה של 3 / 6 / 12 חודשים. אני מצרף סך בשקלים של $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

612.11– חדשות בקצרה

• **לא צפויה התאוששות משמעותית בשוק המחשוב העולמי עד סוף העשור!** זאת לפי **גיגה**. ההשקעות במחשוב יגדלו שנתית בקצב קבוע של כ-6%-5% בלבד. תחום ארגוני אחד לדוגמא, שאינו עומד בציפיות הגידול הקודמות, הוא תחום תוכנות ניהול קשרי הלקוחות. מכירת תוכנות **CRM** נמצאה ב-2002 בירידה בת 24.7% ביחס ל-2001, בה נראתה ירידה בת 6.4% (**גרטנר**).

• ההוצאה על אבטחת מידע גדלה מ-2001 בשיעור צמיחה שנתי של 28%, והגיע ל-5% מתקציב המחשוב, כך לפי **גרטנר**. **אריה דנון**, מנכ"ל **סימנטק ישראל** המצוטט ב**הארץ**, מספר כי ישראל ירדה בפעילות האקרים מהמקום הראשון למקום העשירי בעולם, בעקבות ירידה של 50% במספר הפריצות משטחה. עוד הוא מספר כי 70% עד 80% מהפריצות למערכות מחשוב בארגונים מתבצעות על ידי עובדי הארגון, ולא מבחוץ!

• לפי **YNET**: חברת **SCO** "ביטלה" את זכויות **IBM** להפיץ תוכנה מבוססת **יוניקס**, והגדילה את סכום הפיצויים שהיא דורשת מ-**IBM** ממיליארד דולר ל-3 מיליארד. **IBM** ממשיכה להצהיר כי טענות **SCO** חסרות ביסוס בעובדות. מי שנראית כאילו אינה מתרשמת מהתביעה היא **HP**, שהודיעה על פתיחת חטיבת **לינוקס**, שתהיה חלק מקבוצת האחסון והשרתים של החברה.

612.12– בארץ הסלולר

החידושים בתחום התקשורת והסלולר לא פוסקים:

• מנכ"לי החברות הסלולריות נפגשו בכדי לדון בשאלה האם בכוונתם להקים רשת דור שלישי (**3G**) משותפת. בעוד ש**פלאפון** ו**סלקום** אינן מתכוונות להקים רשת **3G** השנה, פרסמה **פרטנר** מכרז לבחירת ספק להקמתה. הקמת רשת משותפת עשויה להוזיל עלויות לשלושת החברות, אולם טרם נתקבל לכך אישור ממשרד התקשורת ומהממונה על ההגבלים העסקיים.

• החברות הסלולריות יחויבו לפרסם באתריהן, בנוסף לתעריפי שיחות ו-**SMS**, גם עלות זמן האויר עבור שיחה או משלוח **SMS** מחוץ לרשת. השינוי בהוראות משרד התקשורת התרחש לאחר שהמועצה לצרכנות התלוננה כי אי פרסום תעריף קישור הגומלין מטעה צרכנים, המניחים כי עלות השיחה המוצגת היא העלות הכוללת.

• חברות הסלולר בארץ מחוייבות על פי רישיון משרד התקשורת לספק מספר מודיעין (מעין **144**) חינם - כך מדווח מגזין **נענע**. לקוחות **סלקום** יכולים להתקשר ל-9886* (או ☎ 03-6299886), מודיעין **אורנג'** הוא ☎ 1-800-055666, ובפלאפון 166* (או ☎ 03-5727766).

• **יוניסל תקשורת** (☎ 03-6821698) תאפשר לבעלי טלפונים סלולריים מכל החברות לבדוק תרגום מילים מעברית לאנגלית ולהיפך, באמצעות **SMS**. השירות, שמבוסס על מילון **מורפיקס** של חברת **מלינגו**, יתבצע על ידי שליחת **SMS** שמכיל סימן שאלה ואת המילה המבוקשת למספר 8080.

612.13– חוק וסדר

חוקים ותקדימים "מחשוביים" מייצרים כותרות:

• בהחלטה משפטית תקדימית קבע בית המשפט העליון בארה"ב כי כתובת **אינטרנט** היא רכוש פרטי, על כל המשתמע מכך משפטית. ההחלטה נפלה במשפט שנערך עקב תביעת בעלות של **סטיבן כהן** לגבי הדומיין (הרווחי מאוד) **Sex.com**.

• הצעת חוק חדשה בארה"ב מבקשת לאפשר לנפגעי **ספאם** לתבוע ספאמרים. הסכום המוגדר בה משמעותי עד **$1,000** פיצוי על מטרד בן הודעת ספאם בודדת. **מיקרוסופט** לוקחת על עצמה את מסע הצלב: החברה הגישה 15 תביעות ענק נגד מפיצי **ספאם** ששלחו מיליוני הודעות דואר-זבל לחשבונות **MSN** השונים, ואספו כתובות באופן בלתי חוקי.

• סכנה לארגון - האזנה ל-**E-Mail**. בארה"ב הודה נאשם בשתי אשמות תקיפה כלפי אתר חברת החדשות **אל ג'זירה**. במסגרת פעילותו הוא זייף תעודת זהות וחתימה בכדי להתחזות לאדמיניסטרטור של החברה ולקבל גישה לדומיין שלה, כולל האזנה לכל דואר נכנס.

• ובארץ - בית המשפט קבע שהאזנה לתא קולי איננה האזנת סתר. זאת במסגרת תביעה נגד אחד מהאחים **בדיר** אחים עוורים מ**כפר קאסם**, בעלי היסטוריה ארוכה של עבירות מחשב. הקביעה מבוססת על הטענה שהאזנת סתר הוא מצב בו מאזינים לשיחה המתקיימת בין שני אנשים והיא נועדה גם שלא להכביד על שרותי הבטחון, שאחרת ייתקשו להשיג אישורי האזנה.

• בארה"ב התקבלה חקיקה הבולמת במידה מסויימת הימורים ב**אינטרנט**, מצד קטינים ומכורים להימורים (יכול להיות גם עובד בארגונך!). הגישה החדשה כאן היא לאסור על חברות אשראי ומוסדות פיננסיים לכבד תשלומים לחברות הימורים כאלה.

612.14– בעיות בהתאמה

תסבוכת טכנית בלתי צפויה ולא נעימה התגלתה בין שפת XML לבין "חברה לעבודה" ה-Unicode. דו"ח ה-**Unicode Consortium** מזהיר שתכונות מסויימות של **Unicode** עלולות לגרום לתקלות במסמכי **XML** ובדפדפנים. בין השלכות התסבוכת הטכנית, נמצאת גם האפשרות לבעיות ביישומים עבריים המשתמשים ביוניקוד ו-**XML**, דוגמת **Web Services**. **Unicode** מגדיר סט **Characters** לטיפול סטנדרטי בשפות שונות וה"התנגשות" הטכנית עלולה להתרחש כאשר הוא מטפל בתכונות האותיות, כהטייה, הדגשה וכיוון טקסט. למרבה המזל ישנו שיתוף פעולה הדוק בין הקונסורטיום לבין ארגון **World Wide Web Consortium (W3C)**, המטפל בתקן ה-**XML**. בזכותו זכה הנושא לטיפול מהיר ויסודי והוצאו המלצות לכתיבה באופן שיצמצם את סכנות אי ההתאמה - www.unicode.org/reports/tr20

את גרסת תקן ה-**Unicode** העדכנית תמצא באתר - www.unicode.org/versions/Unicode4.0.0

וגרסת **Unicode** נוספת צפויה בסוף השנה.

לנושא **XML** ראה - www.w3.org/XML

612.21– מתחת לאף

לאחרונה נראה שמעילות והונאות מתרחשות כל הזמן ובכל מקום: פרשת Enron, WorldCom ואצלנו - המעילה בבנק למסחר. מאחר ומערכות כספיות וארגוניות מנוהלות כיום בהתערבות ממוחשבת כבדה, לא מאחרים אומני ההונאה לנצל גם אותן לביצוע פשע. התחזקות השימוש ברשת ה**אינטרנט** רק מקל על הפושעים. ואכן, בועידת ה-**CyberCrime** השנתית השלישית נאמר כי בחודשים האחרונים שומעים על יותר ויותר מקרי פשיעה ברשת, כולל הונאות. בארה"ב נעצרו במסגרת **Operation E-Con** 139 חשודים בהונאות מחשב מרחבי העולם, בסך 167 מיליון דולר, שלגביהן 89 אלף תלונות. תחום הידוע לשמצה כרגיש להונאות הוא התשלום בכרטיסי האשראי - שחדר ל**אינטרנט** ופתח עוד פתח לפשעי הונאה ומעילה. בנוסף לכל, המחשב מקל כיום על הפושע לבצע תהליכי זיוף שונים ומקל עליו את עצם הגישה לזירת הפשע, בגישה מרוחקת דרך רשתות שונות. גישה זו יכולה להתבצע גם ממדינה אחרת, הרחק מהישג ידו של החוק המקומי.

פעולות הונאה עשויות לבוא ביוזמת גורמים פנים ארגוניים או חיצוניים. הן עשויות להתבטא כפעולות קטנות לזמן ארוך שרק בקרות פיננסיות, בקרות ע"א ותהליכי איכות אחרים יגלו, אך גם לבוא בדמות "מכות" גדולות בנקודה אחת, היכולות לגרום נזק חד פעמי רב, תוך העלמות או אי זיהוי המבצע. פשעים אלה עשויים להיות ממומשים על ידי ניצול תהליכים לא נכונים בארגון או ביצוע לקוי של תהליכי בקרה ואבטחה. גישה נוספת היא שיבוש פעילות מערכות המחשב וניצול פרצות בתהליכי הקלט והעיבוד.

במוקדם או במאוחר מתרחשות כמעט בכל ארגון מעילות או הונאות ונזקן עלול להיות כבד. לעתים לקוחות הארגון הם המדווחים לו על פעילות חשודה ולפעמים היא מתגלה על ידי הארגון, אבל בכל מקרה תדמית הארגון עלולה להיפגע קשות כאשר פרשה מסוג זה נחשפת. הרצון להסתיר מידע זה, מוסיף ומסבך את ההתמודדות, ולכן ברור כי מניעה עדיפה בהרבה על טיפול לאחר מעשה. חומר למחשבה: **סקר איגוד המורשים לבחינת מעילות בארה"ב** חשף משך זמן ממוצע של 18 חודש בין תחילת הונאה לבין חשיפתה!

במצב זה בולטת מוגבלות החוק ואכיפתו - לא תמיד מסיבות התלויות ברשויות. החדשות הטובות הן שניתן להתמודד היטב עם הסכנה ואף לרתום את המחשב לצידך במאבק זה, בעזרת הגדרת תהליכי בקרה נאותים, מיצוי יכולות כלי מחשוב קיימים ואף שימוש בכלי מחשוב מיוחדים כעזרי כריית מידע, לזיהוי נסיונות הונאה ומעילה. לצדך יעמדו מומחים רבים, היכולים לסייע בסקר סיכונים (בדומה למתבצע מול אתגרי אבטחה רגילים) ובהובלת השינויים הארגוניים הנחוצים, להתגוננות יעילה.

<u>לסיכום - וודא שהמערכות הממוחשבות ונהלי עבודה קיימים מעודכנים ובנויים מראש לסכל הונאות ומעילות. ודא קיומן של בקרות שגרתיות ויזומות, ובצע הערכה מיידית של הצורך בעדכון ושיפור הקיים.</u>

דגש – מאחורי הקלעים

על פי סקר איגוד המורשים לבחינת מעילות בארה"ב, 86% מהמעילות מתמקדות בשיבוש ניהול נכסי הארגון כמו למשל - זיופי שכר. 13% נוספים מהמקרים הם מקרי שוחד ועוד 5% - זיוף דו"חות כספיים.

612.22– המחשב מגנב פטור ?

איזה תפקיד משחק המחשוב בהונאות / מעילות? פשע וירטואלי לפעמים קשה יותר לבצע, אך בו בזמן גם קשה הרבה יותר לתפוס. תחום זה מתאפיין בקשיי הוכחה וקושי להשתמש במידע שבמסגרתו, כראיות. קשיי אכיפה מתבטאים באפשרות לאחסן חומר בשרת במדינה אחרת בה החוקים שונים מחוקי המדינה. במצב זה המחשב עשוי להיות מנוצל לשיבוש נתונים בקבצים - גם בדרכים העוקפות יישומי עריכה רגילים לקבצים אלה (כמצב **DoS**), לשיבוש פעולות עסקיות במסגרת היישומים הארגוניים הרגילים (כהגדרת ריבית הגבוהה פי 10 מהסטנדרט או ביטול עיקול במחשב ללא רשות).

הונאות ב**אינטרנט** עולות כפורחות. דוגמא אופיינית הוא התסריט האמיתי הבא: משתמש **AOL** או **Yahoo!** מקבל דואר, כביכול מהתמיכה הטכנית של חברות אלו, בו הוא מתבשר שמסד הנתונים עם כרטיסי האשראי נמחק. בכדי להמשיך לקבל שירות הוא נדרש להזין שוב את מספר כרטיס האשראי, שמגיע לבסוף לגנב. תחום בולט נוסף בהונאות **אינטרנט** הן הונאות במכירות פומביות וכן עצם פתיחת המערכות הארגוניות ל**אינטרנט** היא פתח לכניסה לבסיסי נתונים של הארגון.

פן נוסף הוא השימוש במחשב ככלי עבודה לזייפן. מחשבים רבי עוצמה במחיר שווה לכל נפש, תוכנות עריכת תמונה רבות אפשרויות ומדפסות איכות זולות העלו את אומנות הזיוף מדרגה. לדוגמא: "צילום" פסל עתיק שאת מקום הימצאו גם הטוב שבחוקרי המשטרה לא יגלה, מאחר שהוא נוצר במחשב- **tinyurl.com/74vi** דוגמא נוספת: ניתן ליצור עותק חתימה מעולה על ידי סורק ומדפסת, כאשר רק בדיקה גרפולוגית מקרוב תזהה שזהו זיוף (מאחר ויהיו חסרים שם סימני לחץ מכתיבת עט על הנייר). אמצעי התגוננות נפוץ מזיופים כאלה היא הפקת מסמכים מתקדמת ויקרה, כנייר מיוחד לצ'קים, ערבויות וכו'. תוכל לנצל אספקט זה להכנת מסמכים רגישים מיוחדים בארגון בצורות אלה, להוספת נדבך אבטחה נוסף המתייחס לסכנת ההונאה.

מצד שני, ניתן לרתום את המחשב גם לטובתך, לסיוע בהתגוננות מפני הונאות ומעילות. הדבר מתחיל בשימוש מושכל במערכות המחשב לצמצום אפשרויות שימוש בלתי מורשה. בנוסף, תוכל להגדיר בקרות שונות על תהליכים עסקיים גם במסגרת המערכות הממוחשבות. ולבסוף - אמצעי כריית מידע ותקני **Data Integrity** יסייעו לזהות כשלים לוגיים. לדוגמא: זיהוי שינוי לא סביר ביתרה (כאשר לא התרחש אף ארוע לגיטימי שיכול להביא לעידכונה).

PCאון© למנהלים ומשתמשי מחשב בכירים

612.31– מסכמים נזקים

סקר ארגון CSI (Computer Security Institute) בנושא Computer Crime & Security לשנת 2002 שנערך בשיתוף ה-FBI, קבע כי הונאה היא בין מקורות ההפסד העיקריים לארגונים, כמו בשנה שלפניה. 25 מתוך 506 משתתפים דיווחו לעורכי הסקר על הפסדים כוללים בסך **$115,753,000**.

גם בארץ ההפסדים כתוצאה מהונאות ומעילות ממוחשבות יכולים להיות רציניים ביותר - ואף לחסל חברות, כפי שפרשיות אחרונות הראו לכל המפקפקים.

מצד התקציב, ההשקעה במניעת הונאות ומעילות אינה בהכרח יקרה: באלפי דולרים בודדים עד עשרות אלפים ניתן לרכוש מערכת שלמה למעקב ואיתור מעילות והונאות. לשכור מומחה לחקירות מסוג זה, בעלויות הקרובות לערכים אלה.

אך גם מי שלא יכול להשקיע אלפי דולרים במניעה, יכול - באמצעות עירנות, מודעות בסינון עובדים ושימוש בכלי כריית מידע קיימים - לצמצם את הנזקים ולאתר מקרים שכבר קרו, ובעיקר הכנה ובקרה של נהלים מתאימים.

מוצר כמו **Actimize** (www.actimize.com) מאפשר אינטגרציה עם מספר רב של מערכות מידע קיימות, ואיתור חריגות המצביעות על מעילות או הונאות.

<u>בשורה התחתונה - מומלץ להתייחס לנושא כפי שמתייחסים לביטוח: להשקיע מעט בכל חודש כדי להיות מוכן מראש ולמנוע אסון.</u>

612.32– פתרונות על המדף

פתרונות בולטים להתגוננות מפני הונאות ומעילות:

- **ACL** - חברה המתמחה בתוכנות כריית מידע, כשאחד הדגשים הבולטים הוא זיהוי הונאות. בין מוצריה: **ACL for Windows** (מחיר הרשיונות מתחיל מ-$2,235) המאפשרת זיהוי חשד להונאה על פי השוואת וניתוח קבצים על פי קריטריונים שמזין המשתמש. **ACL Client Server System** מחבר פתרון זה אל **ACL for OS/390** לקבלת יכולות הניתוח גם בסביבת **מיינפריים**. **פתרון מערכות** ☎ 04-8211112.
- **BMC - ControlB** הוא מוצר ל**מיינפריים** המיועד לחיפוש נתונים חריגים בקבצים או נסיונות לפגוע בהם. הוא משמש גם לביצע חתימה אלקטרונית למסמך, מעקב אחר תנועות חריגות בחשבונות לא פעילים, זיהוי פעילות חריגה עם סכומים גדולים, בדיקת רציפות הפקת קבצים או דו"חות ובדיקת קבצי תנועות כספיות לפני שיכנסו כקלט לעיבוד. **ניו אפליקום** ☎ 09-9598731.
- **CA - CleverPath** הוא פתרון הכולל מנוע חוקים וגם טכנולוגיית חיזוי מבוססת רשתות ניורונים. הוא מתמקד בהגנה ברמת האפליקציה וכולל פתרונות של **Anti - AML Money Laundring** וגם **Fraud Detection**. ☎ 03-7661313.
- **DSIT - NetMap** הוא פתרון **Data Mining** המאפשר להבחין במהירות בתבנית קשרים לא רגילה ולבצע עליה תחקור מפורט יותר, באמצעות כלי **Drill Down**. התוכנה מתמקדת בהצגה ויזואלית המדגישה פשטות ומהירות תחקור. המחיר: בעשרות אלפי דולרים. ☎ 03-5319303.
- **IDEA** - מציעה פתרון כריית מידע היכול לשמש גם לזיהוי הונאות. **IDEA** מיישם את הכללים הסטטיסטיים הידועים כ-**Benford's Law**, שנמצאו מסייעים לזיהוי פעילויות חשודות. הוא מאפשר שימוש באינדקסי קבצים לזרוז ניתוח בסיסי נתונים גדולים, פיתוח בשפת המאקרו **IDEAScript** ועוד - www.caseware-idea.com
- **SPSS - Clementine** הוא כלי כריית מידע היכול גם לשמש ליצירת פתרונות זיהוי הונאות. ממשק המחקר לא עברי, אם כי תומך בנתונים בעברית. המחיר עשרות אלפי דולרים. **ג'ניוס מערכות** ☎ 03-9222204.

מעבר לכך תוכל להסתייע גם ביישומי מעקב באמצעות מחשב. אלה מסייעים לאיסוף מידע על פעולות הנעשות במחשב, כאמצעי לזיהוי פעילות חשודה ולאיסוף ראיות. ראה פתרונות כאלה ב-www.spy-software-source.com

דגש – שקרן, שקרן

ישנן תוכנות מיוחדות המסייעות לזיהוי שקרים על ידי ניתוח קול הדובר, דוגמת Truster ($99.9). (www.truster.com). תוכל להעזר בהן בתקשורת דרך קווי הטלפון במסגרת חקירות מעילה פנימיות או בכדי לבדוק גורם חיצוני החשוד בהונאת הארגון. עם זאת, יש לזכור כי מידת הדיוק של אמצעים אלה עדיין נתונה בספק, ולא ניתן להרשיע אדם על סמך בדיקה זו בלבד.

612.33– חוקרים ומבקרים

בין המומחים שיסייעו לך מול הונאות ומעילות:

- **משרד עו"ד ברלב** (☎ 03-5608222) - משרד עו"ד המתעסק בעבירות מחשב.
- **מוטי לוי** (☎ 03-6911433) - משרד עורכי דין שמתמחה בעבירות מחשב.
- **פאהן קנה** (☎ 03-7106666) - משרד לביקורת חקירתית.
- **קומסק** (☎ 03-9234646) - מספקת פתרונות אבטחה שונים, כולל הגנה וייעוץ למניעת הונאות ומעילות.
- **קרוכמל חקירות** (☎ 03-5621020) - מתמחים בנושא הונאות/מעילות ממוחשבות.
- **B.GRG** (☎ 03-6357444) - מתמחים באיסוף עדויות ממוחשבות לצרכים משפטיים, כמו גם שחזור מידע אבוד.
- **HMS** (**הלפרין שרותי ניהול,** ☎ 03-5223738).

סיוע נוסף תמצא באתרי **אינטרנט** המתמחים בכך:

- **4law** - אתר חברת **B.GRG** מכיל קישורים איכותיים רבים למקורות **אינטרנט** בנושאי חוק ואבטחת המחשוב. ראה במדור **Whats New** תמצית חדשות בנושאים אלה - www.4law.co.il
- **The Internet Fraud Complaint Center (IFCC)** - באתרזה תמצא מגוון טיפים להתגוננות, חדשות על הונאה ותוצאות מחקרים סטטיסטיים שהמרכז ערך לאורך השנים. בכתובת - www1.ifccfbi.gov
- **Fraud.Org** - באתר זה תמצא חדשות על הונאות, הסברים על סוגי הונאה שונים בהם אתה עשוי להיתקל ועצות להתגוננות - www.fraud.org
- **משרד עורכי הדין מוטי לוי** - בדף זה באתרם תמצא ריכוז מעניין של חדשות משפט מקומיות בתחום המחשוב. כתובת האתר - www.motilevy.co.il/news_comp.php

612.41– המומחים בחקירה

מאנשי השטח שמענו עצות ותובנות:

דב הלפרין, מנכ"ל HMS - **הלפרין שרותי ניהול** (☎ 03-5223738) אומר כי בתחום הבנקאות יש מודעות לנושא כבר שנים רבות, כולל (בעיקר בגדולים) הפעלת יחידות ביקורת ענ"א (עיבוד נתונים אלקטרוני), שזהו בין היתר תפקידן. המודעות והמשאבים קטנים יותר בבנקים בינוניים וקטנים, וכן בארגונים לא פיננסיים. לדבריו, מעילות מהשנים האחרונות נעזרו משמעותית במחשב לביצוען, מאחר והמחשב מאפשר למי שמכיר ומבין את המערכות לבצע מעילות רחבות היקף ולהסתירן לאורך זמן. ביטוי אופייני לכך הוא התערבות בקבצי משכורות - מעילה הפופולרית במיוחד בארגון המעסיק עובדים זמניים רבים. מדובר קודם כל במודעות, מאחר שכאשר יש מודעות, אתה יכול לבצע מיידית פעולות לשיפור. חשוב להבין שגם אנשים עליהם אתה סומך בעיניים עצומות יכולים לעשות זאת, ולעולם אינך יודע מי יהיה העבריין.

בועז גוטמן, מרצה לדיני מחשבים (☎ 03-6357444), אומר כי יש היום מודעות רחבה מאוד לנושא, שהולך ומוטמע. ידוע כנתון שמרבית עברות המחשב מתבצעות בארגונים עצמם ולכן יצרני היישומים מכניסים גם הצפנה פנים ארגונית בתוך קבצים כתוצאה מלקחי מחקרי עומק בארגונים. למשטרת ישראל אין מידע אמין וזמין, מאחר והונאות פנים ארגוניות לרוב לא מגיעות לידיעתה. אינפורמציה זורמת רק בין הגופים הנפגעים עצמם, כפי שקורה למשל במערכת הבנקאית באירופה. **בועז** אומר כי יש בארץ מקרים רבים של מערכות מניעת הונאות שאינן מותקנות ומתופעלות לפי הוראות היצרן. לדבריו, הכללים החשובים ביותר הם: "לעולם בדוק" - גם אם הפתרון שבידיך מגיע מפירמה ידועה - וכלל שני: להפעיל את הכלי המועיל והחשוב ביותר, הלא הוא השכל הישר.

עופר אלקלעי, מנהל חשבונאות חקירתית במשרד **פאהן קנה** (☎ 03-7106555) אומר כי מבחינת מודעות, המנהל הישראלי נקט בעבר במדיניות בת יענה, עם גישות בנוסח: "אצלי זה לא יקרה", "אצלי זה עסק משפחתי", "אני מכיר את כולם" וכדומה. בשנתיים האחרונות, בעקבות כל הפרשות שנחשפו לציבור, המודעות בארץ ובעולם עולה. פרשת **הבנק למסחר** גרמה לתפנית, אשר הבהירה שהנזק לארגון יכול להיות סופני. עם זאת, להערכתו המודעות עדיין לא מספיקה. יש כאן שיקולים הקשורים למיתון, מאחר ושיפור תהליכי עבודה והכנסת בקרות עולה כסף ואנשים מנסים לחסוך בכל דבר. השימוש בכלים ממוחשבים לאיתור מעילות והונאות תופס תאוצה ובסופו של דבר הנסיון מלמד שמי שמשקיע בבקרות, בעיקר בבקרות פתע, מקטין את נזקיו בצורה משמעותית.

612.42– טיפ לטיפול שורש

ישם טיפים אלה להעמקת חוסן הארגון מול נסיונות הונאה ומעילה ולטיפול משופר בם:

- **הטכנולוגיה אינה כל התשובה! - מטה גרוף** מזהירה שבארגונים יש תחושת בטחון מוטעית, כאילו הטכנולוגיה שהם מיישמים מספיקה לטיפול בנושאים אלה. היזהר מהסתמכות עיוורת על הבקרות הכלולות בפתרונות התוכנה שברשותך וחקור את מגבלותיהם.
- **נהל הרשאות היטב** - עוד לפני שימוש מתוחכם במערכות מחשוב ארגוניות לשם הונאה ומעילה, ישנן לרוב אפשרויות רבות של ניצול לרעה של הרשאות קיימות. לכן הקפד לנטר היטב הרשאות ולצמצמן ככל הניתן (הקפד למשל על ביטול מהיר להרשאות שאין בהן צורך, כמו אצל עובד שעזב). הגבל גישה למחשבים וחיבורם לרשתות, כשהעובד לא לידם.
- **ישם Workflow** - יישומי **Workflow** יכולים לסייע להקטנת סיכוני מעילה והונאה, בכך שהם "עושים סדר" בתהליכים עסקיים ומספקים הזדמנויות רבות יותר לבקרת ותיעוד תהליכים. ראה תחקיר **584**.
- **ישם חתימה אלקטרונית** - העזר בכלי חתימה אלקטרונית בכדי לצמצם יכולת שינוי בלתי מורשה במסמכים. בכדי שלא לסרבל מנגנונים יותר מדי, ישם זאת על פי מידת הרגישות העסקית של אותם מסמכים. ראה עוד על כך בתחקיר **508**.
- **פזר סמכויות** - יישם מנגנוני עורך ומאשר ויעץ להנהלה שלא לרכז יותר מדי כח בידי מנהל בודד ועובדים בעמדות כח. מודעות לנקודה זו תצמצם אפשרויות מעילה ונזקיה אם היא תתרחש, באמצעות "איזונים ובלמים" ופיקוח מתמיד.
- **שפר אווירה** - חשוב לוודא שישנה אוירה נעימה וקשובה כלפי העובדים. עובד ממורמר הינו לא אחת מקור למעילה, ולעיתים כל שדרוש למנוע זאת הינם דברים פשוטים כאוזן קשבת ודלת פתוחה.
- **פקח עיניים** - כהמשך לעצה הקודמת - היה קשוב למצוקות העובדים. דוגמא מובהקת ניתנה לאחרונה, במקרה המעילה בבנק למסחר, במרכזה עמדה עובדת בכירה שאחיה היה מעורב בחובות הימורים.

612.43– התארגן והתגונן

כך תתמודד באופן שיטתי מול מעילות והונאות:

1. **התייעץ** - זכור שמדובר בנושא ייחודי, שאינו נופל בדיוק לתחום מומחיות המנמ"ר, גם באספקטים המחשוביים שלו. לכן פתח בהתייעצות עם מומחים, שגם יבצעו בארגון סקר סיכונים מתאים. ראה גם **תחקיר 606**.
2. **ישם והטמע פתרונות** - ישם והטמע המלצות המומחים. ישם בקרות על תהליכים עסקיים שונים, כולל - במידת הצורך - הטמעת כלי ביקורת ממוחשבים למערכות הארגון הממוחשבות.
3. **הגדר נהלים** - בעזרת היועצים נסח נהלים ברורים לתהליכים ארגוניים שונים, שיקשו על ביצוע מעילות והונאות ויקלו על זיהוין ותיעודן. צעדים דוגמת חיוב חתימה כפולה על צ'קים בסכומים גדולים. שים לב כי על פי סקר **איגוד המורשים לבחינת מעילות** בארה"ב, בין המקורות לחשיפת הונאה בולטים תהליכי בקרה פנימית האחראים ל-34% מהחשיפות.
4. **הבהר אתיקה** - בכדי למנוע אי הבנות לגבי מובנה של פעילות עסקית נאותה ובכדי להדגיש שהארגון מודע לנושא הונאות ומעילות, נסח והפץ כללי אתיקה מקצועית ענייניים וחד משמעיים.
5. **צמצם אפשרות העסקת מועל** - בכדי לצמצם מלכתחילה את האפשרות שהארגון יעסיק עובד בלתי ישר, הדגש נקודה זו במסגרת תהליכי מיון עובדים. שלב התייחסות לכך למשל כנהלי בדיקת עברו של מועמד.
6. **בצע בדיקות עומק** - מסיבות של מגבלת משאבים, לא תוכל לבצע ניטור עומק לכל דבר, כל הזמן. לכן, הגדר תוכנית לביצוע בדיקות עומק כבדיקות פתע מעת לעת. מקד זאת בתהליכים קריטיים בארגון ושקול ביצוע סמוי אך גם גלוי (מעורר מודעות).
7. **רכז ועדכן מידע** - על אירועי כשל שקרו ואירועים שנמנעו, על מנת ליצור בסיס מידע וכלי להפקת לקחים ומניעה עתידית.

612.51– מה אומר החוק ?

מה אומר החוק בנושא הונאות ומעילות ומחשבים? בארה"ב החלו רשויות החוק לפעול משפטית במאמץ כלל ארצי מתואם כנגד 19 מקורות של הונאות מקוונות. פושעים אלה הוציאו עד כה מאנשים מיליוני דולרים במרמה, תוך "תפירת" הונאות סביב תחומים כ-**Spam**, מכירות פומביות ועבודה מהבית. חשוב לציין שמעל מחצית ההונאות נסבו סביב מכירות פומביות, באתרים בולטים שונים דוגמת **eBay** ו-**Yahoo**. לא תמיד מדובר בהונאה מתוחכמת במיוחד - בין המקרים היו גם מכירות פומביות בהן המוכר פשוט לקח את הכסף ו"שכח" לספק את הסחורה.

רוב מקרי ההונאה והמעילה אינם מדווחים לרשויות מחשש לפגיעה בשם הארגון. אמנם חוק עוולות מסחריות מאפשר לטפל במקרים אלה בדלתיים סגורות, אבל ארגונים לא מנצלים זאת. כך קורה גם בחו"ל: לפי סקר מפלג עבירות מחשב ב**סן פרנסיסקו**, רק כמחצית מעבירות המחשב שהתגלו בכארבע מאות חברות ענק בארה"ב דווחו לרשויות אכיפת החוק. מבחינת טיפול המשטרה - כבר בשנה שעברה קבע דו"ח מבקר המדינה כי הטיפול בעבירות מחשב בארץ לקוי. דבר זה נובע מקשיים תקציביים של המשטרה ומעומס הנגרם עקב המצב הבטחוני וכל זאת מביא לכך שבפועל אין למשטרה די כח אדם לטיפול יעיל בנושאים אלה. מסיבה זו חשוב במיוחד ל**שים דגש מיוחד על טיפול אישי במניעה**, אם כי לשם הטיפול אפשר ומומלץ לפנות למשטרה, תוך זכירת האפשרות לשיפוט בדלתיים סגורות. הכתובת לפניה במשטרה בנושא עבירות מחשב היא **מפלג עבירות מחשב ביחידה הארצית לחקירות הונאה:** ☎ 03-5555342.

שאלה חשובה שמתעוררת בהקשר המיחשובי של מעילות והונאות היא תקפות מידע ממוחשב כראיה משפטית (ראה גם **דגש משמאל**). לראיה כזו אין בהכרח משמעות אחת - היא תלויה גם בתוכנה שמציגה אותה (גרסה, תכונות נסתרות). בנוסף, שינויים בראיה כזו לרוב קלים לביצוע ואינם מותירים סימנים והיא גם משבשת את עניין המקור וההעתקים המוכר מראיות רגילות (בצילום מסמך ניתן לראות הבדל איכות בין המקור להעתק. לא כך בהעתקת קובץ).

612.52– שאלה של אשראי

עולם כרטיסי האשראי מהווה כר נרחב לפעילויות הונאה. לפי פרסומי **משטרת ישראל**, קל מאוד לבצע בתחום זה הונאות, מה גם שחברות אשראי מעדיפות משיקולים כלכליים לספוג הפסדים במקום לשפר הגנות. זאת בזמן שקיימים פתרונות טובים להתמודדות עם הונאות ומעילות בתחום כרטיסי האשראי, כשדוגמא בולטת היא תוכנת **Falcon Fraud Manager** (ראה www.fairisaac.com). להחמרת המצב תורמת הפופולריות הגואה של כרטיס האשראי: אם בשנת **1991** היה היחס בין תשלום בצ'קים לתשלום בכרטיסי אשראי שני שלישים מול שליש, הרי שכבר ב-2000 התהפך היחס לשני שליש לטובת כרטיסי האשראי.

מבחינת הארגון הממוצע, מדובר בשתי סכנות פוטנציאליות: שימוש בלתי תקין של עובדים בכרטיסי אשראי או שימוש עבריני של נותני שרותים בהיתר החברה לחייב אותה בכרטיס אשראי. עבריינים עשויים גם לעשות שימוש באמצעים מתוחכמים, בין השאר תוכנות מחשב מיוחדות, לגניבת ושכפול כרטיסים.

להגנת השימוש בכרטיסי אשראי: בדוק דו"ח חודשי מחברת האשראי וגם הורדות בחשבונות בנק, בזמן קניה באשראי וודא ויזואלית שהכרטיס מועבר רק בקורא הרשמי (ולא בקורא נוסף - אולי בכיסו של המוכר - לשם העתקה), וודא לאחר קניה שקיבלת בחזרה את הכרטיס (ושאכן זהו כרטיסך) ולבסוף - זכור שברשותך ביטוח לכרטיס, למקרי שימוש בלתי הולם.

דגש – היכן הראייה ?

החוק הישראלי התמודד עם נושא הראיות הממוחשבות עד כה בעדכון לחוק הראיות המוסיף התייחסות לראיות ממוחשבות ובחוק החתימה האלקטרונית שאושר כבר בשנת 2001. ממאמר של **עו"ד חיים רביה** למדנו כי מהימנות מסמך אלקטרוני של הארגון תלויה בכך שהוא נערך על ידי מוסד במהלך פעילותו הרגילה ושאופן איסוף הנתונים ועריכתם אמינים. לגבי פלט מחשב, יש להוכיח אמינות הפקתו ושהארגון נוקט בהגנה סבירה מפני חדירה לחומר המחשב ושיבוש עבודתו. בנוסף, העתק שלו עשוי לזכות למעמד של מקור. נקודות לאמינות חתימה אלקטרונית: עליה להיות ייחודית לבעל אמצעי החתימה, לאפשר זיהויו, להיות מופקת באמצעי שבשליטתו הבלעדית ולאפשר זיהוי שינוי שבוצע במסמך לאחר חתימתו.

612.53– בגרסה מקומית

ומה בארץ? באיזו מידה מתבטאים אצלנו מעשי הונאה ומעילה באמצעות מחשב? לא מפתיע לגלות שנסיונות רבים מתרחשים במערכת הבנקאית, היכן שישנם כסף רב ופעולות כספיות עניפות, לצד מערכת מחשב משוכללת. המפקח על הבנקים ציין בשנה שעברה כי מדובר בכ-140 מעילות ב-7 השנים האחרונות. פרשת המעילה הגדולה ב**בנק למסחר** "העירה" את הבנקים במידה מסויימת, והביאה לפעילות מוגברת בעולם הבנקאות הישראלי.

דוגמא פיקנטית ששמענו להונאת מחשב מקומית היא על עובד עירייה במחלקת גבייה, שתמורת שוחד הזין נתונים כוזבים על חובות אזרחים. ועוד - מנהלת חשבונות בחברת מסחר ב**אינטרנט** גנבה מעל חצי מיליון ש"ח. לאחר הכנת קובץ תשלומים היא ביצעה שינויים של חשבונות בנק של ספקים לחשבונות בנק שלה, באמצעות חבר איש מחשבים. העבירה כוסתה באמצעות רישום פעולות פיקטיביות.

המדינה עושה צעדים רבים להתגונן בנושא זה, כולל תקנון של **בנק ישראל** המתייחס למעילות, והצעה של האוצר לחייב חברות ביטוח למנות ממונה להונאות ולקבוע נהלים ומדיניות לנושא זה. כמו כן הרשות לניירות ערך תחייב את הבנקים לדווח על מעילות מנהלי תיקים ויועצי השקעות.