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... וירוסים ללא הפסקה !

מסר אישי

תוך 10 דקות בלבד סיימה התולעת Slammer להדביק כמעט את כל 75,000 נפגעיה המדווחים, ביניהם כ-200 חברות מקומיות! זוהי רק דוגמא אחת לנזקי וירוס נפוץ, וכאלו לא חסרים. מספרם ותחכומם גדלים בהתמדה והם חודרים בהדרגה גם לחזיתות טכנולוגיות חדשות. כתשובה לכך חייב הארגון להכיר ולישם את הפתרונות המודרניים ואת הגישה הארגונית הנכונה והעדכנית.

מה התחדש באופני התקיפה? מה התחדש בהגנות? האם אנטי וירוס מעודכן מספיק? באיזו מידה הנזק מאיים עליך ומה תוכל לעשות? על כך ועוד, יעדכן אותך התחקיר 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 $129 / $239 / $449 + 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

616.11– חדשות בקצרה

• **סקר ביוזמת EMC על מוכנות ארגונים בארה"ב לאסונות, חשף נתונים מעניינים**: רק 14% מהמנהלים העסקיים חש כי המידע הארגוני חשוף מאוד לאובדן במקרה אסון ו-9% מהם חושבים שייקח להם שלושה ימים או יותר להתאושש. הנתונים אצל מנהלי המחשוב שונים במידה מאירת עיניים: 52% חשים כי המידע הארגוני חשוף, ו-23% בהתאמה חושבים שייקח שלושה ימים או יותר להתאושש מאובדן המידע.

• **Ynet** דיווח לאחרונה כי אתר 144 של **בזק** איננו מתעדכן יותר, כפי הנראה כבר מזה חצי שנה, וזאת ללא הודעה מתאימה למשתמשים. מדוברת **בזק** שמענו בתגובה, כי האתר עובר כעת שדרוג לטובת הקמת גרסה חדשנית וידידותית יותר. גרסת הנסיון מתבססת על טכנולוגיה ישנה, שאינה מאפשרת שדרוגים.

• **CA** חשפה טכנולוגיה חדשה בשם **Sonar**, שתאפשר לארגונים להקצות משאבי מחשוב כגון שטח אחסון או שרתים באופן דינמי. המערכת תבצע זאת ללא התערבות אדם ואמורה לחסוך זמן וכסף. **Sonar** תנטר מערכות, תמפה קשרים בין יישומים למשאבים ותגיב בזמן אמת. המוצר אמור להיכלל במסגרת **Unicenter**.

616.12– "שיפוצים" במשרד

האם פני מחשוב המשרד המודרני משתנים?

• גרסה אחרונה של **Open Office** זמינה להורדה. גרסה זו תומכת בעברית, מתאימה ל**חלונות, לינוקס** ו**סולאריס** וכמובן – גם קוד המקור זמין בחינם למפתחים, לעיון והתאמה אישית - www.openoffice.org.il

• קבוצת **OGo** (או **OpenGroupware.org**) היא קבוצה אחות ל-**OpenOffice.org**, הארגון האחראי על פיתוח חבילת היישומים המשרדיים **OpenOffice**. **OGo** פתחה לאחרונה חזית נוספת מול **מיקרוסופט**, כשהכריזה על **OGo Server** - יישום קוד פתוח חדש שאמור להוות תחליף לשרת **Exchange** - www.opengroupware.org

• באוקטובר השנה צפויה להופיע בשוק **Office System** - גרסת **Office** הבאה. על פי **מיקרוסופט**, היא תחבר לראשונה את ה-**Desktop** עם מערכות ה-**BackOffice**, ותכלול גרסאות עדכניות של כל רכיבי החבילה המוכרים. הלקוח הארגוני יוכל לרכוש כל אחד בנפרד.

• מוצר חדש לטיפול בטפסים אלקטרוניים מבית **Adobe** צפוי להופיע בשנה הבאה, אם כי שמו עדיין לא פורסם. המוצר יעשה שימוש בפורמטי ה**PDF**- וה**XML**- ויתחרה במוצר ה-**InfoPath** (לשעבר **Xdocs**) של **מיקרוסופט**.

• **IBM** ו-**Adobe** חברו לשיפור אבטחת ההצפנה בשיטת **PKI** בתוכנת **Acrobat 6.0**. השיפור נעזר בשבב אבטחה של **IBM** ללוחות אם, המסייע להחזיק מידע הצפנה בחומרה. בצורה זו המידע בטוח יותר מאשר על הדיסק הקשיח, היכן שהוא זמין לגישה דרך מערכת ההפעלה. השבב כלול במחשבים הניידים מסדרת **IBM ThinkPad**.

616.13– לינוקס מתעדכנת

עולם הלינוקס ממשיך ודוהר (או מה שהפינגווינים עושים) קדימה:

• שוחרר גרעין **לינוקס** בגרסה חדשה. יוצר מערכת ההפעלה **לינוס טורוולדס**, הציג את גרסת **test**2.6, וכעת צפויה קהילת המפתחים לרכז מאמציה בפתרון בגים ולסיים עם פיתוח תכונות חדשות. - www.linux.org

• סקר עדכני של **CA** מגלה כי משתמשי **לינוקס** ארגוניים מעריכים את יציבות המערכת עוד יותר מאשר את ה-**TCO** המשופר. 95% מהנשאלים ציינו זאת כתרומה המשמעותית ביותר מבחינה עסקית.

• חברת **LINDOWS** - בעלת המוצר הייחודי המתמקד בידידותיות למשתמש - מציעה כעת גרסה חדשה ידידותית במיוחד. **LindowsCD** בנויה להפעלה ישירות מה-**CD** וכך ניתן להשתמש בה לנסיון, מבלי להוריד מערכות הפעלה מותקנות אחרות. - www.lindows.com

• **Novell** הכריזה על חבילת **Novell Nterprise Linux Services** הכוללת שירותי קבצים, הדפסה, מסרים, ספריית רשת וניהול בחבילה משולבת הפועלת על הפצות **לינוקס** ארגוניות של **Red Hat** ו-**SuSe**. ☎ 09-7429955.

• **IBM** החלה ביוזמה לקידום משמעותי של **לינוקס** לשבבי **PowerPC**. היוזמה מתבטאת בהרחבת אגף הפיתוח לנושא זה ובהצבת מטרות כשיפור המהירות והתאמה משופרת למערכות קצה עליון מרובות מעבדים.

616.14– מצפינים ומגינים

בעידן של פגיעה בפרטיות, פריצות, גנבות ורמאות, תחום ההצפנה ממשיך להתחדש:

• חברת **Voltage Security** הציגה פיתוח חדש להצפנת מסמכים. הפיתוח עושה שימוש בהצפנה מבוססת זהות, הממירה למספרים את כתובת הדוא"ל של הנמען. זאת בניגוד לשיטת ההצפנה המקובלת כיום, המסתמכת על מפתחות הצפנה אותם מקבלים המשתמשים לאחר הרשמה מוקדמת. לדברי החברה, הפיתוח החדש, שיהיה זמין ללא תשלום, מפשט את התהליך הקיים. ב - www.voltage.com

• חברת **CipherTrust** שדרגה את ה-**Gateway** שלה, **IronMail Secure Delivery**. ההתקן, הממוקם בין השרת ל-**Firewall** ומשמש כשרת דוא"ל, יכלול מעתה גם יכולות הצפנה. בין התכונות החדשות: כלי ניהול מדיניות, יכולות מניעת **Spam** והצפנת **PGP** של הודעות יוצאות ונכנסות. לפרטים- www.ciphertrust.com

• **Research Triangle Software** הודיעה על גרסה 2.0 לתוכנת ההצפנה **CryptoBuddy**. התוכנה מאפשרת להצפין, לכווץ ולפענח מסמכים והגרסה החדשה כוללת שיפורי אבטחה ומהירות. ב - www.cryptobuddy.com/downloads.php

• **AOL** שדרגה את גרסת **Enterprise** של תוכנת המסרים המיידים **AIM**. גרסה 5.2 מצויידת ביכולות הצפנה המבוססות על טכנולוגיה של **VeriSign**, המאפשרת להצפין מסרים מיידים, קבצים ושיחות המועברים באמצעות **AIM**.

PCאון© למנהלים ומשתמשי מחשב בכירים

616.21– הסיפור אינו נגמר

וירוסים אולי אינם נושא "זוהר" כהתקפות האקרים וטרור מקוון, אך מבחינת הארגון הממוצע, הם מהווים מטרד משמעותי בהרבה. הנזקים מתבטאים בפגיעה נרחבת במשאבי הארגון ובפגיעה כלכלית - וירוס **I Love You** הידוע גרם בארץ לבדה, לנזקים בשווי 50 מיליון ש"ח (**אינשורטק**). מחקר עדכני חשף כי התפשטות וירוסים מהירה מביאה לחוסר יציבות בנתבי **אינטרנט**. בתוך הארגון עצמו תתבטא כמובן ההתפשטות בפגיעה ברשת והפעלת הקוד העויין בנזקים מגוונים, שעלולים בקלות לשתק מערכות רבות.

כיום נראות מגמות חדשות בכתיבת הוירוסים ובהן עליה בקלות ייצורם ובתחכומם, עליה בתפוצה ובמהירות ההתפשטות ואף כניסה לחזיתות מחשוב חדשות. במחצית הראשונה של 2003 נראתה עליה שנתית בת 17.5% בוירוסים חדשים (**Sophos**). בעתיד צפוי שהאיום אף יתרחב. על פי **שי בליצבאו** מ**מגלן** (מצוטט ב**הארץ**), ניתן תאורטית לנצל אפילו זכרון של מדפסת ארגונית להפצת וירוסים. חשוב לדעת שכבר כעת האיום רחב מתמיד: ארגון בינוני עד גדול זקוק בדחיפות לפתרון כלל ארגוני - כיום כבר אין די בהגנת התחנות. כעת חובה להגן על כל התקן מחשוב - מה-**Gateway** ועד ה-**PDA**.

מגמה נוספת הניכרת בשטח היא מאמץ מצד ספקי הפתרונות להתבלט וזה הזמן לנצל זאת. לדוגמא: הצעות רבות מתמיד הבאות להגנתך בזמן הפגיע שבין הופעת וירוס להתעדכנות המוצר, הגנה פרואקטיבית ושרותי תמיכה מיוחדים (לאחרונה דווח באתר **Wired** כי קבוצת לקוחות המנויים על שירות **DeepSight Threat Management System** של **סימנטק** ידעו על מתקפת ה-**SQL Slammer** שעות לפני כולם). **TrendMicro** נותנת מענה גם לקודים שלא מוגדרים בהכרח כוירוס (דוגמת **Slammer**) ומשדרת הודעה בזמן אמת כשהקוד מזוהה במעבדות **TrendMicro** והמלצה מה לעשות (כסגירת פורטים). שרות **Damage Cleanup Server** של **חילן טק** מאפשר שחזור קבצים שנפגעו מרחוק, אם ניתן, וניקוי אם נפגעת מוירוס.

כיום כבר ידוע היטב, לכותבי הוירוסים, ש"טכנולוגיות הפצת הוירוסים" היעילות ביותר מגיעות מתחום הפסיכולוגיה ואינן מורכבות במיוחד. כותבי הוירוסים מנצלים חולשות אנושיות בסיסיות כסקרנות וחוסר זהירות. דוגמאות עדכניות כוללות וירוסים שהופצו במסווה מידע על מלחמת **עיראק** או על מגפת ה-**SARS**. מצד שני, פעילויות הוירוסים צוברות תחכום, כאשר **BugBear.B** כולל ניסיון מיוחד ומדאיג לכוון ל-**1,200** מוסדות בנקאיים. וירוסים אחרים החלו לשמש ספאמרים לאיסוף כתובות דואר ואף ל"ייצור" ממסרי דואר (**Open Relays**) מחשבים המאפשרים להעביר דרכם דואר הלאה, לשם הסתרת כתובת השולח). חזית חדשה ומדאיגה היא הפצה באמצעות **Sharing** שיתוף דיסקים, קבצים, ספריות ושיתוף בלתי מורשה או מבוקר דרך תוכנות **File Sharing** פופולריות.

חדשה מעניינת היא כניסת **מיקרוסופט** לתחום כספקית פתרונות. פעילות נוספת ומתרחבת שלה היא שיתוף פעולה עם ספקי אנטי וירוס מובילים במסגרת מאגר מידע מקוון של איומים על מוצרי **מיקרוסופט** (**Virus Information Alliance**).

<u>לסיכום - יש להערך לעתיד בו איום הוירוסים רק ילך ויחמיר ולוודא בהקדם שלארגון פתרונות מספקים, תוך דגש על וידוא פתרון ארגוני כולל.</u>

616.22– עדכון ממשה הקרב

אלו כמה מגמות הנראות כיום בכתיבת הוירוסים:

- **עלייה בתפוצה** - דו"ח **Internet Security Systems** חושף עליה דרמטית בת 84% בהתקפות ווירוסים, תולעי דואר והאקינג בשלושת חודשי השנה הראשונים.
- **קלות ייצור** - תובנה נוספת מהדו"ח היא שכעת קל יותר לייצר וירוסים מזיקים. יש כיום כלי ייצור נוזקה המשתמשים בצורה מודולרית בקטעי קוד קיימים וכך ניתן לנצלם גם ללא ידע נרחב בתכנות.
- **ישראל בכותרות** - מטרות ישראליות ב**אינטרנט** מקבלות יותר נוזקה, במיוחד ב-**E-Mail**. בו בזמן, גם בין כותבי הוירוסים יש לישראלים "מקום של כבוד", כפי שמדגים מקרה של חמישה צעירים שהואשמו בכתיבת הוירוס **Goner**. רשימת וירוסים ממקור מקומי תמצא באתר - www.f-secure.com/v-descs/_israel.shtml
- **כניסה לחזיתות חדשות** - כותבי הוירוסים נהנים כיום מחשיפת פרצות מתרחבת ונסיון מצטבר בניצולן, כולל בתחומים חדשים כמערכת ההפעלה **לינוקס**, מכשירי **PDA** ואף טלפונים סלולריים.
- **תחכום גובר** - וירוסים משלבים כיום מגוון מנגנוני הפצה ופגיעה, להגדלת סיכוייהם להצלחה. מקלה על כך הגישה המודולרית (אבולוציונית אם תרצה) בה מנצלים כיום בקלות קוד עויין קיים, לכתיבת וירוס חדש.

616.23– ישם והגן

כך תיישם התגוננות יעילה מוירוסים בארגונך:

1. **בחר מוצר איכותי** - מאחר ומדובר בפתרון כולל מספק אחד, חשוב במיוחד להקפיד על איכות ולבדוק את כל חלקי החבילה. העזר בהשוואות מוצרי אנטי וירוס שונים על מגוון פלטפורמות ב-**Virus Bulletin** - www.virusbtn.com/vb100
2. **חשוב במונחים כלל ארגוניים** - בגלל התרחבות איום הוירוסים לחזיתות חדשות, חובה למצוא ולישם פתרון יסודי. לכן התקן פתרון כלל ארגוני, המכסה לא רק את תחנות העבודה. ראה עוד בידיעה 616.31.
3. **ישם פתרון ניהול מרכזי** - חוליה חלשה אחת היא פתח לוירוס בודד העלול להדביק את כל הארגון במהירות. לכן הקפד על ניהול מרכזי חזק ונוח. בדוק זאת ביכולות המוצר הנרכש וישם בהקפדה - החל מפריסה, דרך עדכונים ודיווחים ועד ווידוא קיום מדיניות האבטחה. רכז גם את הצד האנושי לניהול האתגר במתן כתובת אחת לאחריות לנושא וירוסים בארגון, לשאלות בנושא ולדיווח על פגיעות.
4. **הגדר וישם מדיניות** - הגדר במסגרת מדיניות האבטחה הארגונית התייחסות ברורה לנהלים בנושא וירוסים, כולל שימוש בתוכנות ההגנה המותקנות בארגון. תוכל להעזר בעזרי ניהול מדיניות ממוחשבים דוגמת **F-Secure Policy Manager** (**רנסאנס** ☎ 09-7643567).
5. **הגן בזמן הפגיע** - בדוק היטב מה מציע ספק הפתרון להגנתך בין הופעת וירוס להתעדכנות המוצר. לדוגמא: שרות **Outbreak Prevention** של **TrendMicro** מספק לך מיידית **Rules** שהמערכת מנצלת לזיהוי מאפיינים כלליים שכבר ידועים על הוירוס (כשם הקובץ המצורף בדואר). **חילן טק.**

PCאון© למנהלים ומשתמשי מחשב בכירים

616.31– מבט כולל

חפש נקודות אלה כדי לבחון פתרונות אנטי וירוס:

1. **פתרון כולל** - בחר פתרון שיכסה את כל תחומי המחשוב הרלוונטיים ובהם: תחנות עבודה, שרתים, **Gateways**, מחשבים ניידים ואף **PDA**.
2. **יכולות ארגוניות** - הדגש נקודות שרלוונטיות ליישום ארגוני כמו יכולת סריקה ברשת, ניהול מרכזי ונוח, סריקת דואר מתקדמת ועוד.
3. **מהירות סריקה** - מהירות סריקה עשויה להיות משמעותית, במיוחד ביישום ארגוני אינטנסיבי ותוכל לשפרה בעזרת התקני סריקה (**Appliance**). במקרה זה השיפור עשוי לאפשר הוספת אמצעי סריקה או שיפור מאפייני הסריקה (כהרחבת סוגי הקבצים הנסרקים).
4. **הגנה פרואקטיבית** - כיוון שמרבית הנפגעים מכל וירוס נפגעים לפני שחברות האנטי-וירוס מספיקות לזהות ולעדכן את מוצריהן, חיוני לכלול בהגנה שלמה גם רכיב פרו-אקטיבי, שיזהה פעילות חשודה, ניסיון הדבקה או גישה למשאבים אסורים - וידע למנוע נזק עד אשר תתעדכן רשימת הוירוסים וניתן יהיה להסיר את המזיק.
5. **בלימה ב-Gateway** - ראה את הכניסה לארגון כחזית בה תרכז את מירב מאמציך. בדוק ומצה את יכולות פתרון האנטי וירוס להגנתה וכך תמנע מוירוסים לחדור לעומק הארגון.
6. **הגנה על שרת הדואר** - שרת הדואר מהווה נקודת כניסה לאמצעי ההדבקה הנפוץ ביותר כיום: **Attachement** נגוע המגיע כחלק מהודעת **E-Mail**. לכן וודא שתוכל ליישם עבורו סריקה יסודית במיוחד.
7. **הגנה על תחנות עבודה** - זהו אלמנט המחשוב הנפוץ ביותר בארגון ובו נמצאת נקודת תורפה מרכזית בצורת משתמש בלתי אחראי או בלתי מתודרך. התייחס ל-**Desktop** כ"עורף" אליו אסור שיגיע כל אוייב ועליו חייב הפתרון להגן היטב. אנטי וירוס הממוקם שם ישמש כקו ההגנה האחרון.
8. **הגנה על PDA** - וירוסי **PDA** עדיין אינם נפוצים אך חשוב להיות מוכן, מה גם שפתרונות כאלה כבר זמינים. לדוגמא: **Panda Platinum 7** לתחנות עבודה מתאים גם ל-**Laptops** וסורק גם **PDA** המתחברים אליהם. המחיר ל-5 רשיונות **$105**. **פיינזילבר הנדסה** (☎ 09-8859611).

616.32– בארון התרופות

אלה כמה מהפתרונות המובילים שתוכל לישם:

• **אלדין** - **eSafe Mail** (**$1,440** ל-25 משתמשים) מטפל בתעבורת **E-Mail**. **eSafe Gateway** (**$1,800** ל-25 משתמשים). מגן על תקשורת **SMTP** (**E-Mail**), **HTTP** (דפי **Web**) ו-**FTP** (הורדת קבצים). גרסת **Appliance** עם אחד משניהם תעלה כ-**$1,000** יותר. ניתן להוסיף גם אנטי וירוס של **קספרסקי** המתמחה בסוסים טרויאניים (תוספת **$375** ל-25 משתמשים). ☎ 03-6362222.

• **נץ מחשוב** - **InVircible** היא מערכת הגנה פרואקטיבית מפני נוזקה, הכוללת שליטה מרכזית, לדיווח ותגובה בזמן אמת ממקום מרכזי ובכח אדם מצומצם. המחיר: **$235** לשנה ראשונה לחמישה משתמשים. ☎ 03-9027777.

• **פנדה** - **Panda Appliance** בודק וירוסים ב-**Gateway** ב-7 פרוטוקולים, כולל **POP3**, **IMAP 4**, **ANTP** ו-**SOCKS**. ההתקנה פשוטה ואין צורך בקינפוג (אף לא של **FireWall**). **Panda Perimeter Scan** מגינה על שרתים היקפיים כשרתי **ISA** (החל מ-**$26** לרשיון ל-6 משתמשים). חבילת **Enterprise** כוללת פתרון לתחנות, שרתי **Exchange**, **Firewall** **צ'קפוינט**, שרתי **Notes Domino** ופרוקסי. המחיר ל-6 משתמשים החל מ-**$60** לרשיון (מחיר מחירון). **פיינזילבר** ☎ 09-8859611.

• **Antigen** - מתמחה ב-**Exchange** וב-**SharePoint**. כולל ממשק ניהול מרכזי, יכולת התקנה וניהול מרחוק, שליחת **Logs** ל-**NT Event log** וסטטיסטיקות ב-**Performance Monitor**. **Antigen** מסוגל לעבוד עם עד שישה מנועי סריקה צד שלישי בו זמנית. תאימותו ל-**SharePoint** מתבטאת בתמיכה ב-**Virus-Scanning Application Program) VS API 2** של **מיקרוסופט**) וב-**Interface ESE API** (**Extensible Storage Engine API** - ממשק תכנות ל-**Exchange**). **DataSafe** ☎ **03-5497740**.

• **CA - eTrust Antivirus** הוא פתרון ארגוני לתחנות, שרתים, **PDA**, **Gateway** ו-**Groupware** כ-**Microsoft Exchange**. הוא כולל שני מנועי סריקה, בלימת וירוס מהירה בעזרת מניעת גישה מיידית לסוגי קבצים מוגדרים ושרות **eTrust Threat Analysis and Response Global Emergency Team (TARGET)** המוסיף נדבך מודיעין ותגובה מהירה להתפרצויות וירוסים. ☎ 03-7661313.

• **Finjan** - פלטפורמת **Vital Security** מהווה פתרון אבטחת תוכן ארגוני רב שכבתי - ל-**Web**, ל-**E-Mail** ול-**Desktops**, כולל ניהול מרכזי. ברמת ה-**Gateway** ישנה הגנה פרואקטיבית מקוד עויין וגם הגנה מסורתית בטכנולוגיה של **McAfee**. ברמת ה-**Desktop** הקוד ירוץ ב"ארגז חול", המנטר נסיונות לפרוץ ממסגרת הרשאות שהגדיר מנהל אבטחת המידע. בהרשאות אלה ניתן להגדיר גם **Exceptions**. ☎ 09-8659440.

• **F-Secure** - פתרונות בסיסיים: **F-Secure Anti-Virus 2003** (**$53**) ו-**F-Secure Internet Security 2003** (**$65**). פתרונות בראיה ארגונית כוללים: **F-Secure Anti-Virus for Workstations** (**$80**), **F-Secure Anti-Virus for Servers** (**$424**) **ואת F-Secure Anti-Virus Total Suite** - פתרון כולל להגנת ארגונים מפני וירוסים, מתחנות, שרתים ועד ה-**Gateway**. **רנסאנס** ☎ 09-7643567.

• **McAfee - VirusScan Professional** (**$79.99**) כולל הגנה פרואקטיבית בשם **Hostile Activity Watch Kernel** (**HAWK**), איטגרציה לתוך דפדפן **IE** ויישומי **Office** ועזרים נוספים ובהם **Firewall** מובנה ויכולות ניקוי דיסק ומחיקת קבצים יסודית (למניעת שחזור). **רנסאנס** ☎ 09-7643567.

• **Norton - Symantec Antivirus Enterprise Edition** כולל גם סריקת תעבורת מסרים מידיים לקוד עויין. מחירו מתחיל מ-**$45** + **$49** לכל רשיון. **Symantec Web Security 3.0** הוא פתרון אבטחה לשער ה**אינטרנט**, המשלב אנטי וירוס וסינון תוכן. ניהול מדיניות מרכזי מרובה שרתים מקל על הנטל המנהלי. **רנסאנס** ☎ 09-7643567.

• **PF1 Systems - Appliance** (**$3,500**) של **BlueCoat** סורק וירוסים ובודק אוטומטית כל גולש. כל קובץ שמור למחשב נסרק ואתרים נבדקים עם אחד מכמה פתרונות ובהם **Norton Antivitus for BluECoat**. ה-**Appliance** משמש גם כפרוקסי וכך פעילות האנטי וירוס אינה מאטה אותך אלא אפילו מאיצה פעילות. ☎ 03-7649284.

• **Trend Micro** - מציעה מגוון פתרונות אנטי-וירוס לתחנה ולארגון, בהם **Trend Micro Control Manager** לניהול ההגנה ברמה הארגונית, **Internet Gateway** להגנה על שרת הדואר הארגוני, ו-**Desktop&Client** להגנה על התחנה השולחנית ועל ה-**PDA**. **חילן טק** ☎ 03-6383807.

616.41– מדברים עליהם

מומחים מהשטח סייעו לנו בעוד כמה תובנות:

צבי נתיב, מנכ"ל **נץ מחשוב** (☎ 03-9027777) אומר כי בשנתיים האחרונות השתנתה לחלוטין זירת הווירוסים. מה שהכרנו כוירוס בעבר (שכפול לתוך קבצים נוספים) כמעט ולא קיים יותר. וירוסים עכשוויים הם צירוף מרכיבים כמו "תולעת", סוס טרויאני, "דלת אחורית", ובמקרים ספורים בלבד, גם וירוס קלאסי. ההפצה של רבים מן הוירוסים מבוססת עדיין על **E-mail**, אך מספר גדל והולך של "וירוסים" חדשים כלל אינו עובר דרך הדואר אלא מופץ באמצעות **Shares** בלבד! **צבי** מוסיף כי השימוש במונח ווירוס לגיטימי כיום גם לגבי "תולעים". אחרי הכל, "וירוס" מוכר לנו יותר, וגם מרשים יותר מסתם "תולעת". לדבריו, בעיית הווירוסים נובעת מכיוון של פחות משני תריסרי וירוסים בסה"כ, בעיקר חדשים. הוא ממליץ "לרדת מהעץ" ולהפסיק לבזבז משאבים על זיהוי 70,000 וירוסים שאיש לעולם לא ראה וגם לא יראה, ולעבור להתרעה העובדת בצורה גנרית. **צבי** מוסיף כי כל תוכנות ההגנה לסוגיהן, הן לא יותר מחגורת בטיחות, שלא תעזור אם אתה מתעקש להיכנס ברכב שבא ממול. עוד נקודה כאובה לסיום – מנסיונו, רוב מנהלי המחשוב אינם מבינים את הקשר בין **Sharing** ואבטחה מפני וירוסים. בדיקה פשוטה של ה-**Sharing** בארגון המוצעת על ידי **צבי**: צפה בצלמית כונן **C** תחת "המחשב שלי", אם מופיעה יד האוחזת בכונן, אז סיכוייך להפגע מווירוס מודרני הם גבוהים עד ודאיים.

מוטי כהן, בעל חברת **אם. סי. מערכות** (☎ 03-9217542) מייעץ שלא לזלזל בנושא ההתגוננות מפני וירוסים, כיוון שכשנפגעים מדובר בנזקים גדולים. לדבריו, חל שיפור ניכר במודעות לנושא זה בארגונים בשנה וחצי האחרונה ודבר זה התרחש כתוצאה ממקרי התקיפה הרבים ומפרסומם. בין המגמות בתחום הוא מציין התקפות המשלבות שיטות הפצה ו"דגירה" שונות, כפי שהדגים וירוס **Nimda**. לדעתו המגמות העתידיות יכללו יותר שיתוף פעולה בין חברות לארגונים בדמות עזרה בקינפוג מערכות, שליחת מידע מקדים, שיתוף מידע ואף שיתוף פעולה בין חברות האנטי וירוס השונות.

הוגו פליישמן, סמנכ"ל מכירות ב-**PF1 Systems** (☎ 03-7679284) אומר כי מדי יום נכתבים וירוסים חדשים עם וריאציות קטנות מה שגורם להאצת כתיבת חתימות אצל ספקי תוכנות האנטי וירוס. ישנה גם מגמה חזקה של וירוסים המועברים דרך הורדות קבצים נגועים מאתרים. בגישות ההתגוננות בולטת מגמת הגנת הארגון בכניסה, עוד לפני שהוירוס מגיע לתחנות. **הוגו** מתאר כטעות נפוצה בהרבה מאוד ארגונים את התחושה שדי בהתקנת פתרון אנטי וירוס מחברה מכובדת על תחנות הקצה. לדבריו, אין דבר כזה יתר-אבטחת מידע - כל שכבת הגנה שתוסיף תועיל, כמובן תוך בדיקת שיקולי עלות תועלת.

616.42– מה שביטוח

האם ניתן לבטח את הארגון מפני סכנות ההיפגעות מוירוסים? נושא זה הוא חלק מענף ה-**Network Risk Insurance**, הקיים כ-3 שנים ומתחזק בעקבות התרחבות הפסדי חברות עקב פגיעת נוזקה. מומחי ביטוח חוזים כי ערכו יזנק משווי 100 מיליון הדולר הנוכחי שלו ל-2.5 מיליארד דולר עד 2005. מאחר שמדובר בתחום לא מוכר, שבו מושגים כגון "צעדים הגיוניים" לאבטחה אינם מוגדרים במדוייק, עלולה מחלוקת בין הלקוח לחברת הביטוח להיות קשה לפתרון. שקול הצעות כאלה במקרים בהם הסיכון גדול במיוחד. כמה דוגמאות: **InsureTech** מספקת ביטוח לאתרי מסחר מקוון (☎ **03-6391515**). משרד **אנגל סימקין** מציע פתרונות ביטוחיים לארגוני טכנולוגיה (☎ **03-6243380**) ומשרד **אמנון פלץ** מציע מגוון פתרונות ללקוחות עסקיים, כולל חברות הפועלות **באינטרנט** (☎ **03-5490117**). דוגמא לאפשרות נוספת ונפוצה: **חילן טק** משווקת **TrendMicro** מציעה שרות **SLA**, שבדומה לביטוח - מציע לך פיצוי במקרה בו נפגעת מוירוס (☎ 03-6383860).

נוסיף כי ביטוחי אתרים כוללים לרוב גם כיסוי צד שלישי המטפל בנזקים עקיפים ללקוחותיך ולרוב הם יחייבו לבטח קודם את מערך המחשוב שלך. בשעת צרה הם יסייעו לפצות על הוצאות ניקוי המערכות, שחזור המצב המקורי ואובדן הרווחים בזמן ההשבתה.

דגש – מודעות ואחריות

בנושא התגוננות מוירוסים ישנו גורם סיכון מרכזי בצורת שאננות וחוסר מודעות של עובדים. אזן זאת באמצעות מאמצי הסברה ויצירת מודעות כבר ברמת ההנהלה, המחשת הסכנה והנזקים לעובדים וכן הגדרת והסברת האחריות האישית שלהם להידבקויות.

616.43– מחשבה אחרת

אלו עוד כמה כיווני מחשבה אפשריים להתמודדות:

- **בקר יישומים מסוכנים** - מלבד חסימה גורפת לסוגי קוד מסוכן פוטנציאלית כ-**ActiveX Controls**, תוכל לבקר אותם בצורה גמישה יותר, למשל בעזרת הפתרונות של חברת **פינג'אן**.
- **חשוב רזה** - שקול הרחבת השימוש הארגוני בלקוחות רזים (**Thin Clients**). שים לב שבין שיקולי הבחירה בפתרונות אלה נמצאת עמידות משופרת לנוזקה. ראה **תחקיר 593**.
- **חשוב כיווץ** - קובץ נגוע בוירוס עשוי להישלח בדואר כשהוא מכווץ בשיטה מסויימת (כ-**Zip**), מכווץ שנית בשיטה נוספת ואף בשלישית. וודא שתוכנת האנטי וירוס יודעת לטפל בכך וכן שאופציה זו מאופשרת.
- **הגן על ניידים** - התקן אנטי וירוס מקומי על כל מחשב נייד. הדגש בפני המשתמשים כי חשוב להתחבר לרשת לעדכונו ואף בקר וכפה זאת באמצעות מערכת אכיפה. (**Laptops** מעצם טבעם נמצאים בדרכים, מחוברים פחות ל**אינטרנט** וכך האנטי וירוס שעליהם עדכני פחות מאשר בתחנה הממוצעת).
- **בלום מטרד ה-Hoax** - מנע בזבוז משאבים מיותרים על טיפול ב-**Hoaxes**. הסבר לעובדים שישנן הודעות **E-Mail** המזהירות כביכול על וירוסים ומעודדות לביצוע פעולות בלתי אחראיות. ראה הסבר מפורט ב**תחקיר 597**.

PCאון© למנהלים ומשתמשי מחשב בכירים

616.51– הנוף שמחוץ לחלון

כיום שומעים חדשות לבקרים על פרצות אבטחה גם במערכות ארגוניות נפוצות כ-SQL Server, שכותבי נוזקה ממהרים לנצל. דוגמאות בולטות במיוחד הן מערכות ההפעלה הפופולריות **לינוקס** ו**יוניקס.** אלה נהנות ממוניטין רב בנושא האבטחה ואמורות להיות לכאורה בטוחות יותר מ**חלונות**. אחת ה"ראיות": מיעוט הוירוסים לסביבות אלה. אלא שיש לאזן זאת בכמה הערות: וירוסים לסביבות אלה זוכים לפרסום מועט ביחס לוירוסים ל**חלונות** ולכן מלכתחילה מעניינים פחות את כותבי הנוזקה. הפרסום המועט מגביר תחושת בטחון לא לגמרי מוצדקת של משתמשי המערכות ובכך יוצר מיד פתח בדמות גישה שאננה מדי לאבטחה. עדכוני גרסה מסובכים ביחס לחלונות, קוד המקור חשוף לציבור, הטענה בדבר חסינות קבצי המערכת לוירוסים כבר אינה רלוונטית, מאחר והדגש כיום הוא על הדבקת **Attachments** לדואר, ספריות משותפות ויישומי שרת. הבדל נוסף מול **חלונות** ולרעת מערכות אלה הוא ריבוי תכונות רגישות כברירת מחדל, בצורת פורטים פתוחים ושרותים כניהול מרחוק (במילים אחרות - כשהמערכת כבר נפגעת - היא פגיעה יותר). צפה לכך שוירוסים ל**לינוקס** יתרבו מאוד כתגובה לעליה בפופולריות מערכת הפעלה זו. מצד פתרונות ההגנה תמצא כבר כעת גרסאות אנטי וירוס בולטים לסביבות ארגוניות נפוצות כ**לינוקס** ו**סולאריס** וגם לסביבות חדשות כ-PDA. לדוגמא: **חילן טק** מציעה למחשבי כף יד מסוגים שונים את **PC-Cillin for Wireless** (מחירו **52$** כחלק מחבילת **PC-Cillin 2003**).

616.52– לא קונבנציונלי

מעבר לפתרונות אנטי וירוס קונבנציונליים תמצא גם:

- **שרותי ייעוץ** - גם אם רכישת והתקנת פתרונות אנטי וירוס נראית פשוטה למדי, יש גם בה מקום להסתייעות במומחים. לדוגמא: חברת **אם. סי. מערכות** מציעה לארגונים יעוץ, הדרכה, תכנון והטמעת מערכות אנטי וירוס מתקדמות. ☎ 03-9217542.
- **בדיקות וירוסים און-ליין** - צורת צריכה זו הופכת את האנטי וירוס לשרות במקום למוצר נרכש. ראה לדוגמא את שרות **VirusScan Online** שמציעה **McAfee** (**34.95$** לשנה) בכתובת - www.mcafee.com/myapps/vso דוגמאות בולטות נוספות: **ActiveScan** של **פנדה** www.pandasoftware.com של **Security Check** של **סימנטק** www.symantec.com/securitycheck וסורק מקוון של **טרנד מיקרו** housecall.antivirus.com
- **הגנה על מוצרים ייחודיים** - בין פתרונות האנטי וירוס לארגונים תמצא גם כאלה המיועדים להגנת מוצרים ארגוניים ייחודיים. לדוגמא: **TrendMicro** מציעה את **Portal Protect** להגנת **Sharepoint** של **מיקרוסופט**, לצד **Server Protect** המגן על **Windows Server 2003**. מחיר כל אחד מהם כ-**30$** ל-25 משתמשים. **חילן טק.**
- **בדיקת E-Mail מקוונת** - אם אתה מיישם שרותי E-Mail מקוונים כלשהם, בדוק את יכולותיהם לטיפול בוירוסים. **Tmicha.net** הוא דוגמא לשרות **Forwarding** ל-E-Mail הכולל בדיקת וירוסים. - www.tmicha.net **עזרה ראשונה - פנדה** כוללת בחינם בסל השרות שלה שרות בשם **Virus SOS**. במסגרתו מתחייבת החברה להגיע פיזית לאתר הלקוח תוך 24 שעות ולטפל בהידבקות, במידה ופתרון האנטי וירוס שלה לא הצליח לטפל בכך (**פיינזילבר הנדסה**).

דגש – הכשרה וריענון

הכשרה יסודית בדרכי ההתגוננות היעילה חשובה ביותר. כך תוודא שאכן נעשה בהם שימוש נכון, הכולל בין היתר עדכון תקופתי, הפעלת סריקת זמן אמת וסריקת קבצים ממדיות כדיסקטים ותקליטורים. מעבר לכך יש לבצע הדרכת עובדים חדשים וכן רענון שנתי לכל אחד מהמשתמשים בארגון. ראה קורסים בנושא אצל ספקי פתרונות האנטי וירוס ואצל חברות הדרכה כ**ג'ון ברייס** (☎ 03-7535619) וכן **בלוח ההכשרות של PCאון** - www.pcon.co.il/smartmanager3/courses.asp

616.53– עתיד ורוד (לוירוס)

לא רק PC וחלונות - עולם המחשוב הארגוני מתרחב כיום לכיוונים חדשים וכותבי הוירוסים אינם נשארים מאחור. בעתיד צפוי שנראה אותם פועלים בתחומים חדשים כטלפונים סלולרים (כבר בשנת 2000 הפתיע הוירוס **Timofonica** את משתמשי הטלפונים הסלולריים), מכשירי **PDA** ואף התקני **TabletPC** ומערכות **דוט.נט**. תחומים אלה צפויים להגדיל בהרבה את מספר פרצות האבטחה, שכבר מתגלות בהיקפים ובתדירויות גבוהות: לפי ארגון האבטחה **CERT**, בשנת 2001 דווח על **2,437** פרצות ומספר זה זינק ל-**4,129** ב-2002.

אך גם מצד אמצעי ההתגוננות צפויה התקדמות: **מיקרוסופט** משקיעה מאמצים רבים לשיפור אבטחת מוצריה, הדומיננטיים בשוק ובהם: "**Next-Generation Secure Computing Base**" (לשעבר **Palladium**) ושיפורי אבטחה במסגרת **Windows Server 2003** (לדוגמא: יאפשר לחייב כל מחשב שמנסה להתחבר לרשת להיות בעל אנטי וירוס עדכני). **מיקרוסופט** גם שותפה עם **AMD**, **IBM**, **HP** ו**אינטל** בהקמת ה-**Trusted Computing Group** השואפת לפתח מחשבים בטוחים מבוססי הצפנה, שבין השאר יקשו על וירוסים לפגוע בקבצים. יוזמה נוספת היא ה-**Generally Accepted Information Security Principles** המפותח כיום בארה"ב כסט כללים מנחים ליצירת מדיניות אבטחה ארגונית. **GAISP** מחקה גישה המיושמת בהנהלת חשבונות ומחייבת חברות בארה"ב, והוא צפוי להציג טיפול סטנדרטי ויסודי גם בוירוסים. חברות שיישמו אותו יוכלו להעיד בכך על רמת אבטחתן, בדומה לתאימות לתקני **ISO**.

שפה משותפת מתחילה להתפתח בתחום הוירוסים וצפויה ליעל כלי ותהליכי התגוננות מפניהם: **CVE** היא גרסת **XML** המפותחת עבור דיווחי וכלי אבטחה ו-**VGREP** מפותח כסטנדרט למתן שמות לוירוסים.