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 438 ● ● ● ● ● 21 פברואר 2000

PCאון ©

למנהלים ומשתמשי PC בכירים

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

...והפעם... ה-Firewall - חומת המגן

מסר אישי

כמעט כל אחד מכיר את המונח "חומת אש" - Firewall בלעז, אבל רק מעטים יודעים מה <u>בדיוק</u> מסתתר מאחוריו. באופן כללי, ניתן לתארו כמעין ש.ג. בין רשתות המחוברות ביניהן בכלל ובין הרשת הארגונית **לאינטרנט**, בפרט. בפועל, יש הבדלים גדולים בין **Firewalls** שונים, בין תפקידיהם ואופן מימושם.

מה בדיוק עושה ה-**Firewall**? כיצד הוא פועל? על מה הוא יגן? על מה **לא**? אילו בעיות הוא יפתור ואילו בעיות חדשות יווצרו? כדי לסייע לך לרכוש **Firewall** ולעשות בו שימוש מועיל, ניסינו לענות על שאלות אלה, בגליון זה.

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 - **אסף אמיתי**

טלפון - **03-9667939**, פקס - **03-9660310**

דואר - **ת.ד. 2340 ראשון לציון 75121**

לתשומת לבך

לכבוד **קומרקטינג ישראל**
פקס 03-9660310
<u>ת.ד. 2340 ראשון לציון 75121</u>

___ כן אני רוצה להיות מנוי **PCאון**, לתקופה של 3 / 6 / 12 חודשים. אני מצרף סך בשקלים של $114 / $209 / $379 + מע"מ (סמן בחירתך בעיגול), לפקודת **קומרקטינג ישראל** ומחכה לגיליון הקרוב.

שם מלא_____

תפקיד_____

ארגון_____

כתובת_____מיקוד_____

טלפון_____פקס_____

תאריך_____חתימה_____

הערות _____

PCאון© למנהלים ומשתמשי PC בכירים

438.11– חדשות בקצרה

• **זירת המעבדים מתחממת:** בתגובה למעבד **Athlon** הנסיוני בקצב **1.1GHz** שהציגה **AMD** לפני שבועיים, הדגימה **אינטל** מעבד המבוסס על ליבת **Willamette** בקצב **1.5GHz! ובתחום המעבדים הנמכרים כיום בשוק - AMD** לקחה מ**אינטל** את כתר הביצועים פעם נוספת, עם מעבד **Athlon** במהירות 850 מה"ץ, שיעלה $849 בארה"ב. גם **Via** נכנסת למשחק, והיא תשיק השבוע את **Joshua**, מעבד לרמת הכניסה שיתחרה ב**סלרון**, בקצב 433 ו-466 מה"ץ, אליהן יצטרפו בהמשך דגמי 500 ו-566.

• גם הזכרון בתאוצה: **סמסונג** ו**יונדאי** הכריזו השבוע על זכרונות מהירים למאיצים גרפיים. **סמסונג** מציעה שבב **64MBit SDRAM** במהירות 266 מה"ץ, שצפוי להאיץ את מהירות המאיצים הגרפיים ב-30%. **יונדאי** הכריזה על **DDR SDRAM** במהירויות 143, 166 ו-183 מה"ץ.

• **פינג'אן** מזהירה מפני שני מזיקים חדשים - טרויאני בשם **Giri** (**Girigat.exe**) שיבצע פעולות כמו החלפת רקע המכתבה, תקיעת יישומים ושינוי מידע מערכת; ותולעת בשם **Haiku** שאינה גורמת נזק למחשב אבל מפיצה עצמה לנמעני **E-Mail**. מידע נוסף ב- www.finjan.com

438.12– חלונות 2000 כאן

בטקס רב רושם השיקה מיקרוסופט את Windows 2000, מערכת ההפעלה השאפתנית ביותר שלה עד כה, לאחר כ-4 שנות פיתוח. היא מגיעה ב-4 גרסאות - **Professional** מיועדת לתחנות שולחניות ומחשבים ניידים; **Server** לשרתי רמת הכניסה ו-**Advanced Server**, שתומכת בעד 8 מעבדים, לשרתים חזקים. הגרסה הרביעית, **Datacenter** שתומכת בעד 32 מעבדים, תוכרז תוך 120 ימים. הגרסה המוצעת כיום היא גרסה בינלאומית שמספקת רמת תמיכה בעברית בדומה לגרסאות **Hebrew Enabled**, כאשר תוך חודשיים צפויה לצאת הגרסה העברית המלאה הכוללת ממשק עברי.

Windows 2000 מציעה יציבות עדיפה וביצועים משופרים. כמערכת לקוח למחשבים שולחניים ובמיוחד לניידים, היא מציעה גם תמיכה רחבה בחומרה וב-**Plug & Play**, ממשק משופר, ניהול צריכת חשמל מתקדם ותמיכה מובנית בריבוי שפות. לשרתים וכפלטפורמה ארגונית, היא מציעה ניהול מרכזי דרך **Active Directory**, אבטחה חזקה, יכולות תחזוקה אוטומטית, שרידות גבוהה, אפשרות לגישה ליישומי **חלונות** בעזרת לקוח רזה ושיפורים נוספים רבים.

עם זאת, גורמים שונים הסתייגו מהתחזית הורודה: לטענת **אינטל**, **Windows 2000** תדרוש חומרה חזקה יותר (תוספת של 200-250 מה"ץ למהירות המעבד) כדי לפעול במהירות מקבילה לזו של **NT 4.0**; לפי מסמך פנימי של **מיקרוסופט** שנחשף על ידי **Sm@rt Reseller**, עדיין ישנם בקוד הסופי כ-63,000 באגים פוטנציאליים; מחקר של **גרטנר** טוען כי אחת מכל 4 חברות שיבצעו הסבה בהיקף רחב תתקל בקשיים עקב אי התאמה למערכות תוכנה קיימות.

מנגד, טוענת **מיקרוסופט**, המעבר ל-**Win 2000** יוריד את עלות הבעלות הכוללת ב-30%-5%, דבר שיאפשר להחזיר את ההשקעה תוך שנה לכל היותר, והוא יאפשר לארגונים גדולים לחסוך 8-10 מיליון דולר לשנה בהוצאות הפעלת **HelpDesk**.

438.13– כנס האינטרנט הישראלי

בכנס השנתי של איגוד האינטרנט הישראלי שהתקיים בשבוע שעבר בכפר המכביה, שמענו על חיבורים רחבי פס, אבטחת מידע, לימוד מרחוק ומסחר אלקטרוני. את הכנס פתחו יו"ר האיגוד **דורון שקמוני** ויו"ר ועדת ה**אינטרנט** של הכנסת, ח"כ **מיכאל איתן**, שסיפר על אתר של הועדה המוקם בימים אלה, שיאפשר לאזרחים לקחת חלק בחקיקה בנושאי **אינטרנט**. הרצאה המרכזית ניבאה **אסתר דייסון**, יו"ר גוף התקינה **ICANN**, כי מודל הפרסום ב**אינטרנט** לא ימריא והחברות יתמקדו באספקת שרותים ממשיים בתשלום.

שר התקשורת **בנימין בן אליעזר**, אמר כי טכנולוגיות הפס הרחב והמסחר האלקטרוני, יביאו לגידול בפריון הלאומי, בתל"ג ולחסכון בעלויות. בנושאי אבטחה, שמענו את **דורון שקמוני** שסקר את הבעיות במערכות איתור חדירות, את **הנק נוסבכר** מ-**IBM** שחשף כי ב-1999 דווחו 238 נסיונות פריצה שמקורם בארץ, ואת יועץ האבטחה **עופר שיזף** שהראה כיצד גורמים מסחריים וממשלתיים אוספים מידע רב על משתמשי **אינטרנט**. בנושא הלימוד מרחוק, שמענו מד"ר **גליה קורץ** על המהפכה שתחום שצפויה להתרחש עם כניסת הגישה רחבת הפס, שצפויה להחדיר את התפיסה גם לשימוש עסקי וארגוני.

438.14– חדש בתקשורת

חידושים בתחום התקשורת מציעים קשר מהיר, קל ונוח:

• **10 Gigabit Ethernet Alliance**, קבוצה הכוללת את **3Com**, **אינטל**, **נורטל**, **סאן**, **סיסקו** ואחרות הוקמה בשבוע שעבר כדי ליצור תקנים ל**את'רנט** במהירות 10 גסל"ש, שיענו על הצורך ההולך וגדל ברוחב-פס, ויוכלו גם להחליף תשתיות **ATM** יקרות יותר. מוצרים ראשונים צפויים באביב 2002.

• **Hybrid Optical Ring Network (HORNET)**, פיתוח של **ספרינט** וחוקרים מאוניברסיטת **סטנפורד** שיוצג בחודש הבא, יאפשר לנתב מנות ברמה האופטית, וכך ליצור רשתות אופטיות לחלוטין, תוך שיפור הביצועים והוזלת התשתיות.

• **לוסנט** תשיק החודש סדרת מוצרים לרשתות **LAN** אלחוטיות במהירות 11 מסל"ש לפי תקן **IEEE 802.11b**. בין השאר, תכלול סדרת המוצרים כרטיס **PCMCIA**, שיאפשר למחשבים ניידים להתחבר לרשת המקומית.

• **AMD** הציגה את טכנולוגית **SwitchIT**, משפחת שבבי מיתוג המשלבת יכולות קול, נתונים ותקשורת-מודעת-יישום על שבב אחד, במהירויות 10-1000 מסל"ש. היא תאפשר לייצרני מתגים להוזיל את עלות הייצור וכך לקדם את המעבר לרשתות המבוססות על מתגים בלבד.

רשום ביומנך – E-Business

יום עיון בנושא "E-Business - מתוכנית עסקית לגידול במכירות" של הירחון סטטוס, יערך ב-28.2 במלון שרתון סיטי טאואר בר"ג. יום העיון, בהנחיית **ירון לונדון**, יעסוק בתכנון **E-Business**, **B2B** ועוד. הרשמה ב-☎ 03-5181341.

438.21– מגדר עץ לחומת בטון

ההגדרה המילונית של Firewall היא חומה או קיר הנבנים לצורך מניעת התפשטות של אש בין חדרים במבנה. בהקשר של רשתות מחשבים, **Firewall** היא למעשה כל מערכת שחוצצת בין רשתות מקושרות ומפקחת על התעבורה ביניהן. למעשה, זהו יותר קונספט מופשט ממוצר ספציפי, שיכול להיות מורכב מחומרה, תוכנה או שילוב של השניים. **Firewall** בסיסי אפשר לממש בנתב או בעזרת תוכנה פשוטה (שרת **פרוקסי** או תוכנת סינון ב-**Gateway**), אבל **Firewall** מתקדם ידרוש תוכנה ייעודית ולעיתים אף מערכת הפעלה מיוחדת.

ה-**Firewall** הופך כיום לחיוני יותר ויותר. בעוד בעבר ארגונים חיברו ל**אינטרנט** תחנות בודדות בלבד, היום כמעט כל ארגון מחבר את הרשת כולה ומפעיל אתר **WEB**. סקר של **ICSA** בקרב 61 אירגונים גדולים גילה 142 נסיונות חדירה "מוצלחים" תוך שלושה חודשים! לא רק יישומים שוליים יחסית אלא גם יישומים קריטיים המהווים את הליבה העסקית (כמו מסחר אלקטרוני) משתמשים ב**אינטרנט**. כניסת החיבורים הקבועים דוגמת **ADSL** וכבלים, תצריך התקנת **Firewall** גם בתחנות קצה. מגמה בולטת נוספת היא שילוב מוצרי **Firewall** במערכות אבטחה מקיפות ובמוצרי **VPN (Virtual Private Network)** - רשת תקשורת מאובטחת הפועלת על גבי **אינטרנט**).

חשוב לזכור כי ה-**Firewall** יגן מפני סוגי התקפות מסויימים, אבל לא יתן כלל מענה לבעיות אבטחה אחרות, ולכן הוא מהווה רק נדבך אחד ביישום מדיניות אבטחה של ארגון. מנגנונים נוספים דוגמת הצפנה, גלאי וירוסים, גלאי התרעה וסורקים המיועדים לאתר פריצות לרשת, נדרשים גם הם כדי להשיג פתרון אבטחה מקיף.

ל-**Firewall** גם שימושים נוספים. אפשר להשתמש בו לניטור מרוכז, סריקה וחסימה של תכנים, ניהול וחלוקת רוחב הפס של הארגון. הוא יכול לסייע בניצול יעיל יותר של כתובות **IP** בעזרת **NAT** (תרגום כתובות פנימיות למרחב **IP** קטן יותר של **אינטרנט**). ניתן להשתמש בו גם כהגנה פנימית ולהפרדה בין חלקים של הארגון, דבר שיגן מפני פגיעה מפבנים ויועיל במקרה של מיזוג חברות. בנוסף, ה-**Firewall** מפשט את האבטחה הכוללת בארגון על-ידי קונסולידציה של מערכות האבטחה.

<u>לסיכום - ה-Firewall כשלעצמו אינו פתרון אבטחה שלם, אלא רק שלד או ליבה. כדי לקבל הגנה מלאה ויעילה, יש להקים מערך שלם של פתרונות הגנה, אשר במרכזו נמצא Firewall מוגדר ומתוחזק כהלכה.</u>

438.22– איפה, כיצד ומפני מה ?

בבסיסו, ה-Firewall הוא "שומר סף", המחליט איזה מידע יעבור בין רשתות. הוא יגן במקומות הבאים:

1. **LAN, WAN ואינטרה-נט -** הגנה על רשתות המחשבים הפנימיות של הארגון מפני התקפות חיצוניות דרך **אינטרנט**, ומפני גישה לא מורשה מחלקים אחרים בארגון.
2. **שרתי אינטרנט -** הגנה על שרתי **Web, E-Mail, FTP** ומסחר אלקטרוני מפני תקיפה מבחוץ מחד, ומפני שימוש בהם כ"קרש קפיצה" לתוך הרשת הארגונית מאידך, על-ידי הצבתם בשטח המפורז (**DMZ** - ראה 438.54) שבין שתי חומות אש.
3. **מערכות מרכזיות -** יגן על בסיסי נתונים, מערכות **ERP**, **Groupware**, מערכות תפעוליות ומערכות פיננסיות.
4. **אקסטרה-נט -** הגנה והצפנה של מידע העובר מרשת פנימית אחת של הארגון לרשת פנימית אחרת דרך **אינטרנט**.
5. **תחנה בודדת -** **Firewall** אישי שמבודד מהעולם החיצון.

ה-**Firewall** ימלא את התפקידים הבאים:

1. **הגנה מפני התקפות ברמת הרשת -** התקפות המנצלות חולשות בפרוטוקולי תקשורת, כדי להשבית שרתים ומערכות (בדומה להתקפות **Denial Of Service** האחרונות).
2. **הגנה מפני התקפות ברמת היישומים -** התקפות המנצלות חולשות במערכת ההפעלה וביישומים כדי לחדור לארגון (למשל - התקפה על שרת **Web** בעזרת סקריפט **CGI**).
3. **הרשאות ובקרת גישה -** יישום ופיקוח על מערך הרשאות המתירות למחשבים מסוימים לשלוח מידע דרך קיר האש מרשת אחת לשניה, ולמשתמשים לגשת למחשבים.
4. **רישום ומעקב -** רישום לצורך מעקב של כל התחברות או ניסיון התחברות לצורך העברת מידע, המאפשר מעקב אחר אודות ניסיונות לפגוע ברשת הפנימית, והתראה מפני התקפות.
5. **הסתרת והמרת כתובות -** הסתרת הכתובות הפנימיות של רשת המחשבים בארגון מקטינה את הסיכוי לפריצה לתוך הרשת, וחוסכת בכתובות **IP** יקרות של **אינטרנט**.
6. **סינון תכנים -** ניתן להגדיר פילטרים לסינון כניסה ויציאה של יישומים עוינים או תכנים לא הולמים אל ומהארגון.

438.23– שאלה של גישה

אחד הנושאים השנויים ביותר במחלוקת היא הגישה העדיפה למימוש חומת האש. שתי גישות עיקריות נפוצות כיום כבסיס למוצרי ה-**Firewall** המתקדמים:

- **Stateful Packet Inspection -** היורשת המתוחכמת של גישת סינון המנות המסורתית (**Packet Filtering**), בה נבדקו מקור המנות ואופן (כתובת **IP**, פורטים ו-**Headers** אופניים) וסוננו לפי כללים קבועים מראש. הגישה החדשה, שמיושמת למשל ב-**Firewall-1** של **צ'ק פוינט**, סורקת את המנות בכל שכבות התקשורת ובוחנת קבוצות של מנות בעזרת טבלאות מצב. מוצרים כאלה מציעים בדרך כלל ביצועים טובים, והם מספקים הגנה טובה ושקופה למשתמש הקצה.
- **פרוקסי -** בשיטה זו, ה-**Firewall** משמש כ"מיופה כוח" של היישום. הוא בודק האם המנות תואמות את אופי התקשורת של כל יישום, "אורז" אותן מחדש ושולח ללקוח. מאחר וסינון כזה הוא ספציפי לכל יישום, הוא יכול לתת מענה לאיומים ספציפיים המנצלים פרצות ביישום, ולהתייחס לצירופים של מנות מידע. גישה זו נותנת הגנה עמוקה יותר, ומסוגלת להדוף התקפות מתוחכמות יותר (דוגמת **Buffer Overflow**), אבל היא מחייבת את הספק לשלב במוצר מודול פרוקסי ייעודי לכל יישום. גישה זו גם סובלת מביצועים נמוכים יותר, ומפגיעות גבוהה יותר של ה-**Firewall** עצמו.

ככלל אצבע, מוצרי סינון מנות יפגעו פחות בביצועים ויהיו גמישים יותר, בעוד מוצרים מבוססי פרוקסי יספקו הגנה נוקשה ומקיפה יותר. בשורה התחתונה, התרשמנו שמוצרי **Firewalls** משתי הגישות יספקו רמת הגנה טובה, והבחירה תלויה בתחומים עליהם הארגון מוכן להתפשר יותר.

438.31– מה תחפש ?

כדי לבחור מערכת בחוכמה, כדאי שתשתמש ברשימה הבאה כ"רשימת קניות" להתאמת המערכת לצרכיך:

1. **הגישה הבסיסית -** יש לבחור בין סינון מנות מול סינון ברמת האפליקציה בעזרת **Proxies**.
2. **פלטפורמה -** חלק מה-**Firewalls** פועלים על חומרה ייעודית שתחייב השקעה נוספת, ולחלקם גירסאות עבור יותר מפלטפורמה אחת, דבר שמגדיל את הגמישות. מוצרים המגיעים עם מערכת הפעלה עצמאית יהיו בדרך כלל חסינים יותר, מכיוון שהמערכת מוגדרת מלכתחילה באופן מאובטח. נציין כי למבחן שערך **Network Computing**, העדיפו רוב היצרנים לשלוח את גרסאות ה-**UNIX** על פני גרסאות ה-**NT**. **Firewalls** מבוססי **לינוקס** יצטיינו בדרך כלל במחיר נמוך וביחס עלות/תועלת גבוה.
3. **אפשרויות השליטה והבקרה -** האם הניהול מתבצע בעזרת ממשק גרפי או משורת הפקודה? האם קיימת אפשרות לניהול מרחוק? כלים נוחים להגדרת חוקים?
4. **ביצועים -** עד כמה פוגע ה-**Firewall** בקצב התעבורה?
5. **גמישות -** אפשרויות הכיוונון ישפיעו באופן ישיר על יכולות הניצול של המערכת. שים לב לאפשרות להוסיף יישומים חדשים ולחיתוכים לפיהם מסונן מידע.
6. **עלות -** לתגל המחיר, כמו בכל החלטת רכש, השפעה ניכרת, אבל חשוב לזכור שלאור הנזק הגדול שעלול להגרם מפריצה, השקעה ב-**Firewall** חזק ויקר תשתלם.
7. **יכולת הרחבה -** התכונן מראש למקרה של הרחבה עתידית - עומסים גדולים יותר ואפשרויות אחרות. שים לב גם לקיום **API** להוספת מוצרי צד ג'.
8. **רישום ומעקב -** אפשרות להתאם את תצוגת הלוגים ולבצע מיונים וחיתוכים.
9. **תמיכה ועדכונים -** שים לב לתמיכה אותה מעניק המשווק, ולאפשרות לעדכן בקלות לגירסאות מתקדמות יותר, שיעניקו אבטחה טובה יותר וימנעו בעיות.
10. **עמידה בתקנים -** שים לב לעמידת המוצר בתקנים ובבחינות של ארגוני אבטחה (**ICSA, Check-Mark**).

438.32– להזין את האש

למרות העלות הגבוהה של רכישת ואחזקת Firewall, ההוצאה תהיה נמוכה עשרות מונים מהנזק הפוטנציאלי שהיא תמנע (סקר שערך ICSA מראה כי הנזק מפריצה יכול להגיע ל-100 אלף דולר ויותר). אלו הם מרכיבי העלות:

- **רכש ראשוני -** מרכיב החומרה יעלה כמה אלפי דולרים בשימוש בחומרה סטנדרטית (או עד עשרות אלפי דולרים בחומרה ייעודית - דוגמת שרת **סאן** או כרטיסים לביצוע סינון בחומרה). תוכנה מתאימה תוכל לקבל בחינם, או לרכוש חבילה מסחרית, עבור מאות דולרים ועד לכמה עשרות אלפים.
- **התקנה -** בהתקנה הראשונית תצטרך להתוות מדיניות סינון וגישה (לבד או בעזרת אנשי מקצוע), להקשיח את מערכת ההפעלה, להגדיר את ה-**Firewall** ולבדוק אותו.
- **תחזוקה ועדכון -** המערכת אינה מסוג "התקן ושכח", אלא דורשת תחזוקה שוטפת ומתמדת כדי לתקן פרצות שמתגלות ולתת מענה לבעיות. מומלץ גם לשדרג את ה-**Firewall** ומערכת ההפעלה מייד עם יציאת עדכוני תחזוקה או טלאים לפרצות.
- **ניטור -** כדי לנצל את יכולות ההתרעה של המערכת, תצטרך להקצות זמן וכוח אדם למעקב אחר קבצי הלוג.

438.33– שומרי החצר

להלן מגוון מייצג ממבחר המוצרים הגדול שבשוק:

- **אלרון** (☎ 04-8545000) מציעים את **CommandView Firewall**, עם יכולות **NAT**, **DMZ** ו-**VPN** - $1495 בארה"ב.
- **הד-און** (☎ 03-5759010) מציעה את **Raptor Firewall** מבית **Axent** המבוסס על סינון ברמת האפליקציה. חומת האש מבצעת הקשחה של מערכת ההפעלה, וכוללת ממשק נוח המאפשר לכוונן אותה בקלות. כמו כן, היא כוללת יכולות **VPN** תואמות **IPSec** שאושרו על-ידי **ICSA**. מחיר בארץ - החל מ-$1,600, תלוי במספר המשתמשים ובמודולים. כמו כן, מציעה **הד-און** "חומת אש אישית", המיועדת לארגונים קטנים ופועלת ברמת התחנה, ללא צורך בשרת.
- **סיסקו** (☎ 09-9700000) מציעה את **Secure PIX**, עם מערכת הפעלה עצמאית - $9,000. חומת אש זו מצטיינת במהירות גבוהה מאוד, אבל ממשק שורת הפקודה שלה מסורבל יחסית והוא עלול להקשות על התפעול.
- **נובל** (☎ 09-9514455) מציעה את **Novell Firewall for NT** ב-$2,245 ל-25 משתמשים. כמו כן, מוצע גם **BorderManager Enterprise** לשרתי **NetWare** עבור $1,995 ל-5 משתמשים.
- **נורטון (PF1 -** ☎ 03-5617175) מציעה את **Norton Internet Security 2000** להגנה על תחנה בודדת - $53.95 בארה"ב.
- **צ'קפוינט** (☎ 03-7534555) מציעה את חומת האש **Firewall-1** המבוססת על סינון מנות, תוך שילוב טכנולוגיות **Proxy**. סינון אתרים מתאפשר תוך שימוש במוצרי צד ג'. חומת האש כוללת גם ממשק ניהול ידידותי, שמאפשר לשלוט על מודולים מרחוק ויודע לנהל וליישם סינון ביישומים חיצוניים. כמו כן, מציעה **צ'קפוינט** את נתב **VPN Appliance** (בשיתוף עם **נוקיה**) הכולל **Firewall** מובנה.
- **רד-גארד** (☎ 03-7657999) מציעים את חומת האש **CryptoSystem PyroWall -** $4,500 - $13,000 בארה"ב.
- **3COM** (☎ 03-6361720) מציעה את **OfficeConnect Firewall 25** עבור עד 100 תחנות ב-$695, **OfficeConnect Internet Firewall DMZ** ב-**$1,495**, ו-**OfficeConnect Web Site Filter** ב-$195 (המחירים בארה"ב, כולל שנת עדכונים).
- **Algorithmic Research** (☎ 03-9279500) מציעה את **Private Wire** עבור **חלונות** ו**סולאריס**.
- **CA** (☎ 03-7661313) מציעים את סדרת **Platinum** של **ממקו** הפועלת תחת מערכת ההפעלה **Memco SeOS**, וכוללת **Firewall** מבית **אבירנט** - $1495 בארה"ב.
- **HP** (☎ 03-5380300) משווקת את **Raptor Firewall**, ומציעה פתרונות הכוללים חומרה ותוכנה.
- **IBM** (☎ 03-6978500) מציעה את **SecureWay Firewall** התומך בסינון, **Circuit Gateway** ו-**Application Gateway**.
- מבין המוצרים החופשיים, נזכיר את **Socks - Firewall** ותיק מבוסס **Proxy** (**www.socks.nec.com**). מוצרי **לינוקס** יש ב - **linuxberg.inter.net.il/conhtml/adm_firewall.html**

החברות הבאות יעזרו לך בייעוץ והרכבת פתרון מתאים:

- **אייפקס-ICS** (☎ 03-9250300)
- **קומסק** (☎ 03-9234646)
- **תדיראן מערכת מידע** (☎ 03-5313501)

438.41– בנאים מספרים

על המגמות העיקריות בתחום ה-Firewall בישראל, שמענו מחברות אבטחה ומשווקי חומות אש:

דקר נאוי, מנהל תחום טכנולוגיות אבטחת מידע ב**תדיראן מערכות מידע** (☎ 03-5313731) אומר כי יש מקום לוויכוח מקצועי בין גישת סינון המנות לגישת הסינון ברמת האפליקציה, אבל זה אינו הפרמטר המרכזי לפיו בוחרים **Firewall**, ובשורה התחתונה, שתי הגישות מספקות רמת הגנה גבוהה. **דקר** מדגיש כי חשוב יותר לשים לב לרכיבים הנוספים שמציע ה-**Firewall** כגון אותנטיזציה מרוחקת, שילוב עם **PKI**, **VPN**, קישור לשרתי **RAS** וריכוז מדיניות אבטחה כוללת. חשוב גם לשים לב למחיר ולביצועים, ולאפשרויות לעקוף את ה-**Firewall** ברמות נמוכות (מערכת ההפעלה שמתחתיו).

נפתלי קרן, מנהל איזור המזרח התיכון ב**צ'קפוינט** (☎ 03-7534643) אומר כי כדי לנצל את **אינטרנט** כתשתית תקשורת מתקדמת וזולה יש צורך בכלי אבטחה וניהול - **VPN** וכלי **QoS**. מגמה נוספת שלדבריו מתחילה לתפוס תאוצה בעולם, היא השירות המנוהל - חברות תקשורת מוכרות לא רק קישוריות אלא גם אבטחה כשירות, והן יהפכו ל-**Managed Service Providers (MSP)**. חברת התקשורת היא זאת שתתקין את כלי ההגנה דוגמת **Firewall** ו-**VPN**, והיא תנהל ותתחזק אותם מרחוק.

גור נדיבי, מנהל תחום תוכנה ב-**HP** (☎ 03-5380300) אומר שמגמה העיקרית בשוק ה-**Firewalls** בארץ כיום היא המעבר מ-**Firewall** עצמאי למערכת אבטחה מלאה, שכוללת גם הגנה על בסיסי מידע, יישומים ונתונים, הן ברמת הגישה והן ברמת הטרנסאקציות. **גור** ממליץ לבחור מוצר של חברה גדולה עם בסיס לקוחות רחב, כדי להנות מהידע המצטבר שלה. הוא מוסיף כי הפרדה בין מרכיבי ההגנה כנגד חדירה (**Firewall**) להגנה כנגד התקפות רשת (דוגמת **Denial of Service, Ping of death**) תסייע להגדיל את העמידות.

438.42– לידיעת המנהל

כדי להבהיר ולחדד את הנושאים החשובים, ריכזנו את לקט הדגשים העיקריים:

1. **ה-Firewall אינו "פתרון קסם"** - מערכת ה-**Firewall** תהייה אפקטיבית רק כחלק ממערך אבטחה כולל, שמכוונן ליישום מדיניות ארגונית מתאימה.
2. **גבולות ההגנה** - ה-**Firewall** עלול להעניק הגנה חלקית בלבד או לא להעניק הגנה כלל כנגד פרצות אבטחה במערכת ההפעלה ובשרתים. יש להקפיד להתעדכן בגירסאות חדשות ו"טלאי אבטחה" מתאימים, הזמינים באתרי היצרנים.
3. **לפעמים אחד זה לא מספיק** - לא תמיד מספיק **Firewall** אחד בכניסה לארגון, ולעתים יש למקם **Firewalls** גם בין חלקים שונים של הרשת, כדי ליצור הפרדה והגנה מפני התקפות בתוך הארגון. קונפיגורציה כזאת יכולה לסייע גם לארגונים שאינם מחוברים ל**אינטרנט**.
4. **יישום נכון** - גם ה-**Firewall** הטוב בעולם עלול להכשל בתפקידו אם לא יכוון כראוי, לא יתוחזק ולא תעמוד מאחוריו מדיניות ברורה. השימוש השוטף ב-**Firewall** הוא שיקבע את ערכו האמיתי ואת מידת ההגנה שהוא יספק.
5. **טיפול ושימון** - **Firewall** בלתי מכוונן ובלתי מעודכן יכול דווקא לסייע לפורצים, בייחוד עקב תחושת הבטיחות המדומה שהוא מעניק למנהלי הרשת.
6. **התנהגות בעת משבר** - האם בשעת קריסה תאפשר המערכת תנועה ללא כל הגנה? או תחסום את התנועה בכלל? עד כמה עמידה המערכת עצמה בפני התקפות שונות? כמה זמן יקח להחזירה לפעילות תקינה לאחר קריסה?

הארה – הפתרון השלם

Firewall הוא רק מרכיב אחד במערכת הגנה ארגונית כוללת. את המרכיבים האחרים ניתן לעתים לשלב עם ה-**Firewall** לקבלת פתרון אינטגרטיבי יותר (למשל, בעזרת ממשק **OPSEC** - **www.checkpoint.com/opsec**):

- **אנטי-וירוס** - וירוסים יכולים לחדור מכמה כיוונים (דואר אלקטרוני, דיסקים ודיסקטים, דפי **Web**, ועוד), והם דורשים אמצעי הגנה ייעודיים במספר רמות.
- **"ארגז חול"** - כדי לבחון יישומים המוטלים בספק, העלולים להתקלות כוונדלים.
- **מערכת ניטור ו"רחרחנים" (Sniffers)** - לבדיקה מתמדת של פריצות ו"חורי אבטחה".
- **כלי מעקב וניתוח לוגים** - כלים אוטומטיים יכולים לסנן פעולות חשודות מתוך קבצי ה-**Log**.
- **כלי הצפנה** - ישמרו על סודיות המידע גם במקרה של חדירה למערכת.
- **סיסמאות חזקות ומערכת בקרת גישה** - ימנעו חדירה לא מורשה מתוך הארגון.

438.43– השער להכרת החומה

מידע והסברים נוספים על Firewalls תמצא בכתובות:

- **ICSA Firewall Buyer's Guide** - **www.icsa.net/html/communities/firewalls/buyers_guide**
- **Seven Firewalls Fit Your Enterprise** - **www.networkcomputing.com/921/921f2.html**
- **Build your own firewall** - **www.fwtk.org**
- **CERT** - **www.cert.org/other_sources/firewalls.html**
- **Check-Mark** - **www.check-mark.com**
- **C|Net Web Security Center** - **www.builder.com/Servers/SecCenter/**
- **C|Net Firewalls Center** - **home.cnet.com/category/0,10000,0-9422,00.html**
- **Firewall FAQ** - **www.clark.net/pub/mjr/pubs/fwfaq**
- **Firewall.com** - **www.firewall.com**
- **Internet Firewalls and Security** - **www.3com.com/nsc/500619s.html**
- **Network Computing Buying Guide** - **www.networkcomputing.com/1023/1023buyers2.html**
- **קישורים ליצרני Firewalls** - **www.waterw.com/~manowar/vendor.html**

438.51– להציב חומה ב–5 צעדים

בבואך להציב Firewall, פעל לפי הצעדים הבאים:

1. **זהה את הסיכונים -** נסה להעריך (בעזרת מומחים חיצוניים, במידת הצורך) "מהיכן תפתח הרעה?" - אילו סכנות אורבות לארגון? מהם גורמי הסיכון ומהו היקף הנזק שעלול להיגרם?
2. **בחר מוצר -** בחר Firewall מתאים שיענה על הסיכונים ויאפשר את מימוש המדיניות הרצויה, בהשקעה התואמת את מידת הסיכון הצפוי.
3. **בחר מיקום -** ככלל אצבע, מקם Firewall בין כל רשת המאובטחת לכל רשת שאינה מאובטחת (ובמיוחד **אינטרנט**). מיקום לא נכון יגרום ל-Firewall להיות חסר תועלת, וייצור תחושת אבטחה מדומה שעלולה להזיק.
4. **קבע עמדת המוצא -** ברוב המקרים מומלץ לעבוד לפי גישת "אסור כל מה שלא מותר". כלומר, חסימה מקיפה וכוללת של כל כיווני הגישה, והיתרים ספציפיים ונקודתיים לכניסה ויציאה. הגישה ההפוכה מתירה את כל התעבורה בשני הכיוונים, וחוסמת נקודתית.
5. **הגדר מדיניות -** חשוב לשלב את ה-Firewall כחלק ממדיניות האבטחה הארגונית, ולהחליט לאילו קבוצות משתמשים מותר ואסור להשתמש ביישומים ופרוטוקולים. בחר את הגבול בין הגמישות למשתמש לבין הצורך בהגנה על הארגון, ומנע מהעובדים יצירת פרצות ומעקפים. הגבל את השימוש במערכות הארגון והגדר את גבולות השימוש הלגיטימי.

438.52– טבילת אש

Firewall שלא נבדק כהלכה אינו מהווה אמצעי אבטחה שניתן לסמוך עליו. כדי לישון בשקט, הקפד לבדוק:

- **עיתוי -** בדוק את המערכת לאחר ההתקנה הראשונית (כדי לוודא שהיא אכן מוגדרת כראוי), לאחר שינויים מהותיים בקונפיגורציה, ובאופן תקופתי.
- **נסיונות חדירה מבחוץ -** נסה לדמות פורץ שחודר מבחוץ. בדוק את העמידות של פרוטוקולים שונים. בצע **Port Scan** (סריקה של פורטים בנסיון למצוא פרצות). נסה התקפות נפוצות. נסה לחדור ממקומות שונים - מתוך ה-**DMZ**, מחיבור דרך ספק **אינטרנט** חיצוני, ועוד. הקפד להשתמש בכלי בדיקה יסודיים ועדכניים.
- **כלים אוטומטיים -** כלים אוטומטיים יוכלו לבדוק מגוון של בעיות נפוצות, והם נמצאים בשימוש גם אצל פורצים. בין הכלים המקובלים: **Pingware** (www.bellcore.com), **SATAN** (ftp.porcupine.org/pub/security/index.html) ו-**Internet Scanner** (www.iss.net). כלים נוספים תמצא בידיעה **393.32**.

438.53– התקפות ללא מענה

למרות חשיבותו הרבה של ה-Firewall, חשוב לזכור גם את מגבלותיו ואת הבעיות שהוא גורם. האיומים שנותרים ללא מענה ראוי הם:

- **מעקף -** משתמשים המתחברים מתוך הארגון לספק **אינטרנט** חיצוני מאפשרים לעקוף את ה-**Firewall**. גם מודמים שמותקנים על תחנות עלולים להיות מקור לצרות.
- **חדירה ישירה -** יישומים עוינים ווירוסים יכולים לחדור לארגון גם דרך תקליטורים ודיסקטים.
- **הנדסה חברתית (Social Engineering) -** השגת סיסמאות וגישה לא מורשה למחשבי הארגון בעזרת עובדי הארגון או בעזרת התחזות לעובד ופנייה לגורמי תמיכה בארגון.
- **פריצת שרשרת -** לאחר שנפרץ מחשב אחד, יכול הפורץ לגשת בעזרתו אל מחשבים אחרים אליהם הוא אינו מורשה לגשת מבחוץ.
- **התקפות נתונים -** ניצול של **Buffer Overflows** ושיטות דומות כדי לגרום הרצה של קוד הרסני המוסווה בתוך תוכן. ה-**Firewall** גם יוצר בעיות חדשות שלא היו קיימות קודם:
- **פגיעה בביצועים -** הניתוב והסינון דרך ה-**Firewall** פוגעים בביצועים, במיוחד כשהעומסים מתחילים לגדול.
- **יישומים מוגבלים -** יישומים מסויימים עלולים שלא לפעול או לפעול באופן מוגבל מאחורי **Firewall**.
- **סיבוכיות בתחנת הקצה -** שימוש ב-**Proxies** ומסננים ברמת האפליקציה/פרוטוקול ידרשו לעיתים קרובות כיוונון מיוחד בתחנות הקצה על-מנת להכיר בהם.
- **התראות שווא -** נסיונות גישה לגיטימיים עלולים להראות כהתקפות וליצור עומס מיותר על אנשי האבטחה.
- **מניעת גישה ממורשים -** משתמשים רצויים ולקוחות עלולים להתקל בקשיים בנסיונות רצויים להתחבר לארגון.

438.54– מרשת פרטית לאיזור מפורז

VPN (Virtual Private Network) היא למעשה רשת WAN על גבי תשתית ציבורית זולה לשימוש כמו אינטרנט, עם תנאי אבטחה וניהול של רשת פרטית. כדי לממש אותה יש ליצור "מנהרה" **(Tunnel)** של תקשורת מאובטחת בין הצד השולח לצד המקבל. היות וה-**Firewall** הוא בדרך כלל ה"שער הראשי" של הארגון, נוח ופשוט ליישם הצפנה וניתוב בין חלקים שונים של הרשת הוירטואלית בעזרתו.

מעשית, מדובר בהצפנת נתונים שקופה למשתמש המתבצעת ב-**Firewall** שביציאה מהארגון, כאשר ה-**Firewall** בצד המקבל מפענח אותם. כך הנתונים חשופים רק במהלך תנועתם בתוך הרשתות המאובטחות וניתן להעביר גם מידע מסווג. מרבית מוצרי ה-**Firewall** מציעים כיום יכולת **VPN** בפרוטוקול **IPSec** שפותח על ידי **IETF** ומבוסס על מפתחות ציבוריים (עוד על הפרוטוקול תמצא ב-**www.ipsec.com**) אבל תאימות מלאה בין מוצרים שונים היא עדיין נדירה יחסית.

מיקומו של ה-**Firewall** יעיל גם לשימושים נוספים:

- **שטחים מפורזים (Demilitarized Zone - DMZ) -** מהווים, את הרשת החיצונית, או "רשת השירות" של הארגון, וכוללים בדרך כלל שרתי דואר ו-**Web** ציבוריים של הארגון. ה-**Firewall** משמש כאן כחוצץ כפול, ומונע מהשרתים להפוך לנקודה דרכה יותקף הארגון, כפי שקרה במקרים רבים.
- **Network Address Translating (NAT) -** מסתיר את מבנה הרשת הארגונית הפנימית וחוסך בכתובות **IP** על-ידי תרגום כתובות ממרחב כתובות פנימי למרחב כתובות חיצוני.
- **סינון תכנים -** מניעת כניסה ויציאה של וירוסים דרך **E-Mail**, קוד אקטיבי **(ActiveX ,Java)** ודואר זבל.

פקס בקשת מידע ממנוי - PCאון©

לברורים ומידע נוסף - טלפון 03-9667939 פקס 03-9660310

דחוף

תאריך_____

לכבוד מנהל השיווק/מכירות

	מספר הפקס	ידיעה
____ אלרון	04-8550248	(33)
____ הד-און	03-5759014	(33)
____ סיסקו	09-9700022	(33)
____ נובל	09-9514466	(33)
____ נורטון - PF1	03-5623607	(33)
____ צ'קפוינט	03-5759256	(33)
____ רד-גארד	03-6480859	(33)
____ 3COM	03-6361733	(33)

	מספר הפקס	ידיעה
____ Algorithmic Res.	03-9230864	(33)
____ CA	03-7661414	(33)
____ HP	03-5375055	(33)
____ IBM	03-6978883	(33)
____ אייפקס-ICS	09-9250305	(33)
____ קומסק	03-9230020	(33)
____ תדיראן מע. מידע	03-5313500	(33)

א.ג.נ.

הנדון: בקשת מידע מפורט

בעקבות הפרסום ב-**PCאון** בנושא_____

אבקש לקבל מכם מידע על_____

_____

_____

אודה למשלוח המידע לפי הפרטים הבאים:

שם ומשפחה_____חתימה_____

תפקיד_____ארגון_____

טלפון_____פקס_____

כתובת_____מיקוד_____

מנוי יקר !

דף זה הוא שירות נוסף של **PCאון** אשר נועד לסייע לך לקבל מידע מפורט ומהיר ישירות מהספקים המוזכרים בגיליון. סמן V מול שמות הגורמים שמהם תרצה לקבל מידע נוסף, הגדר הנושא או צרף הידיעה האמורה, סמן כיצד תרצה לקבל את המידע, מלא את פרטיך ושלח אל הספק/ים המתאים.

משווק נכבד !

פקס בקשת מידע זה, נשלח אליך על ידי מנוי **PCאון** - שרות תדרוך מקצועי של מנהלי המחשוב ומשתמשי **PC** בכירים בישראל, בעקבות אזכורכם בפרסומינו. הענות מהירה ומלאה לבקשת המידע, תסייע לעסקיך ותאפשר לנו לאזכרם גם בפרסומים עתידיים שלנו. תודה מראש על שיתוף הפעולה.