

HP העולמית פרסמה לאחרונה נתונים המוכיחים את הצורך באימוץ גישה חדשה ומקיפה בעולם ניהול סיכונים בתוך סביבה ואיומים מורכבים יותר ויותר



איל דאלי

שלהם גדלו במהלך השנה האחרונה, 27% הודו שבשנה האחרונה חוו פרצת אבטחה על ידי גישה לא מורשית פנימית, 20% הודו כי הם חוו מפרצת אבטחה חיצונית.

21% מהמשיבים אמרו כי ארגונים סבלו מבעיות אבטחה בשל כשלים בזיהוי ובמתן הרשות, 28% אחוז נאלצו להתמודד עם בעיות תאימות ורגולציה.

יותר ממחצית מהמשיבים ציינו כי אבטחת מידע תהיה

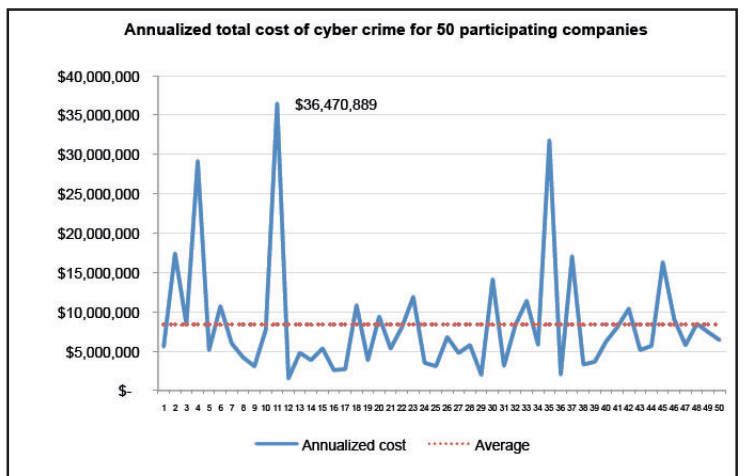
בעדיפות עליונה עבור 2012, 48% מהם סבורים כי תקציב האבטחה שלהם יגדל בתקציב לשנה הבאה.

פתרונות אבטחת המידע של HP, משנה את היבטי אבטחת המידע הארגונית בעזרת הפלטפורמה הייחודית - SIRM "הכלב" קרברוס, בעל שלושת הראשים ששמר על מפתן ממלכת אדונו, כך גם הפתרונות של חטיבת אבטחת המידע החדשה של HP Security Enterprise Product, מספקים שלוש זוויות הגנה שונות שיחדיו מספקות הגנה מקיפה מפני מתקפות cyber. פלטפורמת ה-SIRM של HP מתבססת על פתרונות אבטחת מידע מובילות בעולם שנרכשו על-ידי HP במהלך השנה האחרונה: Fortify, ArcSight, ו-TippingPoint. בעזרתם מתאפשר לארגון לנקוט בגישה פרואקטיבית המשלבת שילוב וניתוח אירועי אבטחה מידע, ניתוח עמוק והגנה של אבטחת יישומים ברמת הקוד, הגנה פרואקטיבית להתקפות ברמת התשתית ועוד. ההבנה ש-92% מניצול הפירצות מקורן בפרצות הקיימות בתוכנה, מובילה אותנו לזוית הראשונה בפתרון הכולל של אבטחת המידע של HP.

הזווית הראשונה מערכת - Fortify, מספקת את היכולת לבדוק ולזהות בפירצות אבטחה בפתרונות התוכנה, ללא תלות במקור התוכנה (פיתוח עצמי, תוכנה מסחרית, קוד פתוח...). הפתרון תומך במחזור חיי התוכנה, בשלב הפיתוח ובשלב הבדיקות, ותואם את Microsoft Development (Security Life Cycle (SDL).

על פי הסקר של HP בחסות מכון Ponemon, בקרב כ-50 ארגוני אנטרפרייז גלובליים בארה"ב - למרות רמת מודעות הנרחבת, להתקפות סייבר השפעה כספית משמעותית על עסקים וארגונים ממשלתיים. המחקר הצביע על:

- בחציון האחרון של 2011 מחיר הפשע הקיברנטי הממוצע עבור 50 ארגונים במחקר הוא \$5.9M.
- יותר מ-90% מההתקפות נגרמו על ידי קוד דדוני, DDos Attack, גניבת מידע ומכשירים, Web-Based Attack.
- במהלך תקופה של ארבעה שבועות, ארגונים שהשתתפו בסקר חוו בממוצע 72 התקפות בשבוע "מוצלח", גידול של כמעט 45% לעומת השנה שעברה.
- הזמן הממוצע לחזרה לשגרה לאחר מתקפת סייבר הוא 18 יום, עם עלות ממוצעת של כמעט \$416,000. זוהי עלייה של כ-70% מתוצאות השנה שעברה שעמדו על \$250,000 ותקופת התאוששות של 14 יום.



מחקר אחר של Coleman Parkes, שהוזמן ומומן על ידי HP, וכלל ראיונות בקרב 550 מנהלים בכירים ומנהלי הטכנולוגיה בארגונים עם יותר מ-1,000 ברחבי העולם, התמקד בנקודות המבט שלהם על איומי אבטחה בדק את סדר העדיפויות שלהם בתחום אבטחת המידע. להלן עיקרי הממצאים:

- רק 29% אחוז ממנהלי הטכנולוגיה ציינו כי הארגונים שלהם מוגנים היטב מפני איומי אבטחה אך עם זאת הם פחות בטוחים ביכולת של הארגון להתמודד עם היבטים של ניהול הסיכונים. המשתתפים בסקר ציינו כי נפח ומורכבות האיומים ממשיך להסלים. כמעט 70% אחוז אמרו כי המורכבות ורמת האיומים גדלה.
- יותר מ-50% אחוז מהמנהלים מאמינים כי פרצות אבטחה בארגונים

