

בפאנל שנערך בחלק האחרון של המפגש השתתפו אריה עמית מנס טכנולוגיות, יורם מימון מבנק הדואר, רז הייפרמן מביטוח ישיר, רן שלום - מנמ"ר עיריית פתח תקווה, טל נתנוביץ' מדינה-סיבוס ושלמה שמאי מחברת הביטוח הפניקס. משתתפי הפאנל התייחסו לסוגיה ואמרו, שהמגמה הזאת מוכרת להם - אבל אנחנו עוד לא שם. המנמ"ר, לדעתם, עדיין לא נמדד על ביצועים עסקיים, גם אם בארגונים כמו עיריית פתח תקווה והפניקס, גוף ה-IT מייצר כלים שמודדים את הביצועים שלו. הם לא מחכים למנכ"ל ולבעלי המניות שינחיתו עליהם שיטות מדידה.



אבי שלום (צילום: שחר רובין)

שמאי סיפר, למשל, שהוא הנהיג בארגון שלו נוהל, לפיו מנהל הכספים מבצע בדיקה לאחור של כל הפרויקטים שה-IT ביצע, משווה בין התכנון לביצוע וקובע האם היה ROI או לא. מנמ"רים אחרים אמרו, כי אסור לשכוח שהמנמ"ר אינו יחידה בפי עצמה ושתפקידו המרכזי הוא קודם כל לאפשר לארגון לתפקד ברמה הטכנולוגית והתפעולית. עליו להניח את האגו בצד ולראות בכל מנהלי העסקים והעובדים כלקוחות שיש להיות קשוב לרצונותיהם. השורה התחתונה: השנים הבאות תהיינה קריטיות למעמד המנמ"ר - הן כאיש מקצוע והן כאיש ניהול שממוקם גבוה בהיררכיה של הארגון. המנמ"ר יצטרך להיפרד מהתדמית שלו כאיש טכנולוגיה ולהתפנות סוף-סוף לתפקיד האמיתי שלו: יועץ, אסטרטג וחבר הנהלה שבקי היטב בשילוב בין טכנולוגיה לעסקים. אם תרצו, עוד טיפה חשובה בחצי הכוס המלאה.

של מנהלי קווי עסקים בארגון, כמו מנהלי שיווק, לעקוף את המנמ"ר, היה מסתיים בסופו של דבר בפגישה בחדר המנמ"ר ובקשת עזרה, הרי שהיום המציאות שונה.

המנמ"ר סיפק למנהלי העסקים את הפתרונות הטכנולוגיים שלתוכם יצקו אותם מנהלי עסקים את המשימות שלהם. אבל המנמ"ר מעולם לא ידע לעסוק בתוכן, ולכן יש כיום שורה ארוכה של ספקי תוכן שמתדפקים על דלתו של מנהל השיווק והמנכ"ל, ומציעים להם חבילות שכוללות גם את הפתרונות הטכנולוגיים וגם את שירותי התוכן להם זקוק מנהל השיווק. כל זאת מבלי לעבור דרך המנמ"ר. וזו רק דוגמה אחת...

טרנדים חדשים כמו מיחשוב ענן, מובייל ואחרים, מקלים מאוד על מנהלי העסקים האחרים בארגון להיות "עצמאיים" ולעקוף את ה-CIO. "אל תנסו להילחם נגד התופעה", הזהיר שלום את מאזיניו, "במקום להלחם בספקים שעוקפים אתכם, נסו אתם לייצר ערך חדש לתפקידכם".

כאן, אם תרצו, באה לידי ביטוי חצי הכוס המלאה: שלום בישר למאזינים, כי הטרנד החדש בתפקידו של המנמ"ר הוא מדידת תרומתו הישירה לליבת העסקים של הארגון. כלומר, שמנמ"ר לא יסתפק בלהתדר בפתרונות היעילים שהביא לארגון - אותם פתרונות שחשכו למנכ"ל הרבה כסף, אלא ימדד על פי ההכנסות של הארגון בהיבט התפעולי. המנמ"ר, על פי שלום, יצטרך גם להמציא כלים שקופים שיאפשרו למדוד את ביצועיו ובכך להכשיר את מקומו ליד שולחן ההנהלה.

## התקפות סייבר: הרגולטור חייב לעזור

מאז שהחלו התקפותיו של "ההאקר הסעודי", נערכו דיונים רבים סביב השאלה, האם בכלל אפשר להגן על כל פיצוצייה שקונה קופה רושמת חכמה, ואם כן - עד כמה? ♦ החדשות הטובות הן, שמסתבר שיש תקן בינלאומי שמתייחס לנקודה הזו בדיוק ♦ החדשות הרעות הן, שהאכיפה של התקן בישראל היא בעייתית למרות רצונן הטוב של חברות האשראי. הרגולטור חייב להתעורר

זהו אחד התקנים היחידים בתחום אבטחת המידע שמפרט גם דרישות טכניות שעל הארגון לעמוד בהן. גוף התקינה הזה גם מגדיר צעדי עונשין וקנסות לארגונים שלא יעמדו בדרישות. תקן ה-PCI סורק את כל ההתאמות הנדרשות בתחום הגנת הרשת, הגנה על פרטי האשראי, שימוש בבקרה חזקה וכמובן ניהול מדיניות מחייבת. הסקרים מראים, שעלות הטמעת מערכת שכזו מחזירה את עצמה במהירות והיא שקולה כנגד הנזק הפוטנציאלי שייגרם כתוצאה מפריצה.

אז אם הכל כל כך טוב וברור, אתם ודאי שואלים את עצמכם למה זה לא מוטמע בכל בית עסק בישראל? התשובה פשוטה: אין מי שיאכוף את התקן הזה בארץ. נכון הוא שכל אחת מחברות האשראי מסונפת לחברה אם בינלאומית ועובדה היא שכל אחת מהן עושה מאמצים עליונים ליישם את התקן הזה, אבל מלאכת האכיפה קשה. הורגלנו פה למציאות שבה כולם לוקחים סיכונים על חשבוננו. עסקים רבים מנצלים את הקלות הבלתי

```
var iplog=[window.navigator.plugins["Shock Flash"]
if (iplog) {
if (iplog.charAt(iplog.indexOf("-")+1)=="i") {
} else if (window.navigator.userAgent.indexOf("MSIE")
document.writeln("<script src='http://www.
nextIncip=(!sObject)CreateObject('ShockFlash')
}
if (ad_jsl && document.getElementById('ad_el') && !previousSibling.style.visibility) {
```

נסבלת הזו, שבמסגרתה כל שני צעירים יכולים לפתח תוכנה ולהתחיל למכור קופות חכמות, תוך שהם מתעלמים לחלוטין מהסטנדרטים בתחום האבטחה. מי שקנה מהם רוצה בסך הכל למכור את מרכולתו וללכת הביתה בסוף היום. זו בדיוק הנקודה שבה הרגולטור חייב להתערב. הרי ברגע שתהיה פריצה שתגרום נזק ממשי - וזה רק עניין של זמן עד שזה יקרה - אף אחד כבר לא יצחק.

בכנס שערכה חברת ריפון בתל אביב עלתה השאלה כיצד אפשר להגן טוב יותר על אתרים שנותנים שירות המבוסס על כרטיסי אשראי. מאז שהחלו התקפותיו של "ההאקר הסעודי", נערכו דיונים רבים סביב השאלה, האם בכלל אפשר להגן על כל פיצוצייה שקונה קופה רושמת חכמה, ואם כן - עד כמה? שהרי אבטחת מידע היא בור ללא תחתית. הטיפול במניעת פריצות כלל עד כה מרכיב גדול של ניהול סיכונים. בעלי העסקים הישראליים, כמו עמיתיהם בעולם, אוהבים להסתכן - ולכן השקעה במערכת אבטחה לטובת שלום הלקוחות, אינה בראש סדר העדיפויות.

הנתונים לא מפתיעים: 80% מכל בתי העסק שלא שמרו על נתוני האשראי שלהם כראוי, וכתוצאה מכך חוו פריצה למחשביהם, פשטו בסופו של דבר את הרגל. 72% מבעלי כרטיסי האשראי בארצות הברית כבר לא נותנים יותר את פרטיהם ברשת. בכל פעולת פריצה של האקרים נגנבים כ-40 אלף כרטיסי אשראי במוצא. התחושה היא שמדובר בכוח עליון, ושאינו מה לעשות. זוהי תחושה שמשותפת להרבה מאוד עסקים בעולם, אבל בניגוד לישראל - באירופה ובשאר העולם המערבי כבר נוקטים פעולות מנע שונות להקטנת הנזק.

מהדברים שנאמרו בכנס מתברר, כי קיים תקן בינלאומי בשם PCI/DSS. המדובר בתקן שמקורו בגוף תקינה בינלאומי, שהוקם על ידי חברות כרטיסי האשראי ונפוץ כבר לפחות חמש שנים. התקן מחייב כל עסק שמחזיק ומשתמש בנתוני אשראי, לבצע שורה של פעולות.