

שילה ג'ורדן מונתה למנמ"רית סימנטק העולמית

ג'ורדן עוזבת את סיסקו לאחר תשע שנים שבהן שימשה כסגנית נשיא בכירה ל-IT, תקשורת ושיתופי פעולה ♦ מסימנטק נמסר, כי "ג'ורדן תניע את אסטרטגיית ותפעול ה-IT בחברה, עם דגש על בניית התמיכה של ה-IT בפעילות העסקית"



סמיר קפוריה, סגן נשיא בקבוצת אבטחת המידע של סימנטק

שילה ג'ורדן, בכירה בסיסקו, מונתה למנמ"רית הראשית של סימנטק. בהודעה על מינויה מסרה ענקית אבטחת המידע כי "ג'ורדן תניע את אסטרטגיית ותפעול ה-IT בחברה, עם דגש על בניית התמיכה של ה-IT בפעילות העסקית". המנמ"רית החדשה תדווח לסטיבן ג'ילט, סמנכ"ל התפעול של החברה.

ג'ורדן עבדה בסיסקו במשך תשע שנים, שם שימשה כסגנית נשיא בכירה ל-IT, תקשורת ושיתופי פעולה. בתפקידה זה הייתה אחראית לאספקה והטמעה של שירותי מפתח של ה-IT לעובדי סיסקו בעולם. לפני כן שימשה ג'ורדן בתפקידי הנהלה בכירים בוולט דיסני ובמרטין מריאטה. היא מרבה להרצות על שיתופיות, ניידות, מגמת ה-BYOD ומנהיגות נשית. ג'ורדן בעלת תואר ראשון בחשבונאות מאוניברסיטת פלורידה ותואר שני במנהל עסקים מהמכון טכנולוגי של פלורידה.

מסימנטק נמסר כי "ג'ורדן מביאה עימה מומחיות נרחבת בהנעת שיתוף פעולה ארגוני, על פני מספר רב של ערוצים, בכלל זה פלטפורמות ניידות שונות".

יוסי הטוני

קפוריה הוסיף כי עתיד אבטחת המידע קשור לבנייה ושילוב של שלוש תפיסות על שלא בהכרח קשורות לטכנולוגיה: "יצירת פתרון טכנולוגי שכל רכיבו 'מדרים' זה עם זה באופן אינטגרטיבי, יצירת יכולת בינה ומודיעין על האבטחה, תוך למידת 'הבטן הרכה' של הארגון; ובניית מערך תגובה שכולל את התפיסה לפיה החדירה כבר נעשתה".

בהתייחסו לתעשיית אבטחת המידע הישראלית אמר קפוריה, כי "יש בישראל יכולות רבות ומעניינות בתחום, סטארט-אפים רבים שעוסקים בו, והארגונים בארץ נחשבים כמאמצים מוקדמים של טכנולוגיות".

"על מנת להוביל את המהלך לשינוי התפיסתי הנדרש, סימנטק עורכת ללקוחותיה משחקי מלחמה מקוונים. במסגרת ההדמיות הללו נבנים מערכי IT ברמת מדינה"

"באנלוגיה", הסביר קפוריה, "אם הקירות חסומים והחלונות סגורים ואטומים, אבל יש דלת אחת שהעובד פתח לרווחה, כל מערכי ההגנה והחומות הבצורות לא יעזרו. הרעים תוקפים את המשתמשים, והם עושים זאת במקרים רבים תוך שימוש בהנדוס חברתי, מאחר שבני האדם הם החוליה החלשה במערכי ה-IT. עובדים נוטים לפתוח אי-מיילים והם לא ישימו לב שאי-מייל מסוים הגיע ממקור לא מזוהה ושיש סיכוי שהוא מכיל נזקה מוסתרת. בנוסף, הרעים הולכים תמיד לחוליה החלשה בשרשרת ה-IT, זו שקשה להגן עליה, או לוקח זמן להטילא טלאי אבטחת מידע".

"קל לפרוץ יותר מאשר להגן"

קפוריה אמר כי "הסיבה להצלחה החלקית של הרעים היא העובדה שקל יותר לפרוץ מאשר להגן. לכן, נדרש לשנות את תפיסת אבטחת המידע המסורתית - מהלך אותו מוביל מנכ"ל סימנטק, סטיב בנט. באבטחת הקלאסית מדובר על מניעה, מעקב ותגובה. במסגרת שינוי התפיסה, אנחנו צריכים להבין, עם כל הכאב הכרוך בכך, שאי אפשר למנוע חדירה ב-100%, ולעתים לא ניתן למנוע חדירה כלל. מה שיש לעשות הוא לצמצם את משך הזמן של החדירה ולהשקיע יותר משאבים בתגובה, על מנת שתהיה מהירה ויעילה. ארגונים לא יכולים להרשות לעצמם מצב בו פעולת הונאה כספית של האקרים תתגלה אחרי חמש שנים. אם היא לא תתגלה תוך ימים או שבועות - הארגון יקרוס".

"אם האקרים שמים לעצמם יעד לפרוץ, בסופו של דבר הם יצליחו בכך. השאלה היא כמה זמן ייקח למנהל האבטחה עד שהוא יידע על כך וייצור תגובת נגד", הוסיף. "רק מעקב, בלי תגובה הולמת, הוא בבחינת אזעקה בלי כוח משטרה שתטפל בעניין. אי אפשר להגן על הכול. ניסיון להגן על הכול מביא להגנה על כלום".

משחק המלחמה: 12 אלף מתקפות מקוונות בשבוע

על מנת להוביל את המהלך לשינוי התפיסתי הנדרש, ציין קפוריה, סימנטק עורכת ללקוחותיה משחקי מלחמה מקוונים. במסגרת ההדמיות הללו נבנים מערכי IT ברמת מדינה, שכוללים ארגוני צבא וביטחון, בנקאות ותעשייה, בתי חולים ועוד - ואלה חווים במשך שבוע 12 אלף מתקפות מקוונות. "בדרך זו, הלקוחות מבינים שעליהם לשנות את מערך ההגנה שלהם ואת אופן פעולתם", הסביר.

שינוי נוסף שציין קפוריה קשור לאופן בו יש להטמיע את פתרונות אבטחת המידע וההגנה מפני סייבר. "על מנת למקסם את האבטחה בארגון יש להטמיע תפיסת אבטחה כוללת, ולא אסופות של פתרונות", אמר. "הפתרונות צריכים 'לדבר' אחד עם השני, ליצור שכבות אבטחה מסודרות - על היישומים, על היישומים הניידים, על הרשת הארגונית, על תפעול ה-IT, פתרונות המשכיות עסקית, ממשל IT וממשל אבטחה. בסופו של דבר, על מנהל האבטחה לקבל נראות, הנראות קשורה למיפוי של הנכסים הארגוניים, לתעדוף שלהם, להגנה עליהם וליצירת מכלול פתרונות של תגובה במקרה אירוע אבטחה. רק בדרך זו הם יכולים להגן בצורה מוכללת".

"הפעילויות של ההאקרים מביאות לכך שהארגונים נדמים בעיניהם לתינוק שמשכתשך באמבטיה של צבע, בעוד הוריו לא מבינים כיצד הוא בכלל התלכלך. הכוונה היא שמנהלי הארגון לא מבינים כיצד ייתכן שהארגון כה חשוף בהיבטי אבטחת המידע השונים, כאשר הם אלה שסיפקו לו את הצבעים"