סימנטק-מגנים ומאבטחים את המידע

שמוליק אנג'ל, מנכ"ל סימנטק ישראל, אופטימי לגבי מה שצפוי בשוק הישראלי השנה, וממליץ למנמ"רים לצמצם את כמות הספקים בדטה סנטר שלהם ● "רוחב ההיצע שלנו הוא נקודת המפתח", אומר אנג'ל, "לאף אחד מהמתחרים שלנו אין את ההיצע שיש לנו. בנוסף, סימנטק אגנוסטית - אנו מאפשרים ללקוחות להטמיע את המוצרים שלנו על גבי כל חומרה"

הילל יוסף

"המשימה שלנו היא לספק למנמ"רים ולמקבלי ההחלטות ערך מוסף, מעבר להיבטי ההגנה והשמירה על המידע. בשל הגישה הרחבה של סימנטק, אנו מספקים מענה נרחב וכולל לארגונים, תוך צמצום כמות הספקים בדטה סנטר הארגוני", כך אומר **שמוליק אנג'ל**, מנכ"ל סימנטק ישראל, בראיון מיוחד לגיליון במלאת 30 שנים לאנשים ומחשבים.

"לא הייתי צרכן של IT", מספר אנג'ל, בעברו קצין בכיר בחיל האוויר, שהשתחרר ב-2000. "לאחר שחרורי הצטרפתי לפרסייס, שנרכשה על ידי וריטאס, שבעצמה נרכשה על ידי סימנטק ב-2005. כך יוצא, שאני עובד סימנטק מזה תריסר שנים".

באחרונה, אמר אנג'ל, "קיימנו את כנס הטכנולוגיות השנתי שלנו, תחת המוטו של שוק שחור, למסחר במידע, נתונים פיננסיים ולגניבת זהויות. השוק השחור למסחר בפריטים דיגיטליים גנובים, דוגמת זהות וכרטיסי אשראי, הוא שוק שמגלגל מיליארדים רבים. רק קצה קצהו של הקרחון הענק הזה גלוי וידוע. הכלכלה המחתרתית הבשילה והפכה לשוק גלובלי יעיל. היא מבוזרת גיאוגרפית ומייצרת עבור הפושעים הקיברנטיים הכנסות של מיליוני דולרים". אנג'ל דיבר על דו"ח שפרסמה סימנטק בנושא ואמר, כי "השווי הפוטנציאלי של מוצרים שפורסמו בתקופת המחקר בשרתי כלכלת המחתרת, כפי שזוהה על ידי סימנטק, היה יותר מ-276 מיליון דולרים. במהלך תקופת הדו"ח זיהתה סימנטק 69,130 מפרסמים פעילים ו-44,321,095 הודעות שפורסמו בפורומי המחתרת. כלי התקיפה הנפוץ ביותר הוא בוטנט, שמחירו הממוצע עמד על 225 דולרים".

> "עולם אבטחת המידע עובר שלב - מריגול לחבלה. לאור זה, על מנהלי אבטחת המידע לבצע חשיבה מחדש על האופן שבו יש להגן על מערכי ה-IT הארגוניים ועל המידע שמצוי בידי העובדים."

השוק השחור הדיגיטלי - מערכת המזינה את עצמה

לדברי אנג'ל, "השוק השחור הדיגיטלי הוא בבחינת מערכת המזינה את עצמה. כלים שמסייעים בהונאות וגניבות ניתנים לרכישה והמידע הגנוב שמושג על ידם יכול להימכר". כך, אמר, "מידע על כרטיסי אשראי הינו הקטגוריה שאותה מפרסמים ביותר בתשלום מבין המוצרים והשירותים הנמכרים בכלכלת המחתרת, ומהווה 28% מהסך הכול. עלות דף פרטים שכזה עומדת על בין 1 ל-30 דולרים". לדבריו, הפופולריות של מידע בנוגע לכרטיסי אשראי נובעת מכמה סיבות: הדרכים הרבות שבהן ניתן להשיג מידע שכזה ולהשתמש בו להונאות; השימוש הנרחב בכרטיסי אשראי; קלות השימוש בקניות מקוונות; יכולת של נוכלים להשלים טרנזקציות ולקבל סחורות לפני שהסוחרים נוכחים שנפלו קורבן להונאה; והעובדה שמידע כרטיסי אשראי נמכר לעתים קרובות בכמויות לנוכלים, עם הנחות או מספרים חופשיים המסופקים ברכישות גדולות".

גניבת המידע, אמר אנג'ל, "נעשית מטעמי מסחר במידע, בשל ריגול תעשייתי או בשל גניבה לצרכים ביטחוניים. ארגונים נדרשים להשקיע בשלוש חזיתות: הגנה על תשתיות המידע ועל המידע עצמו, היערכות לקראת אסון והתאוששות מהירה אם קרה אסון. על מנת להצליח ליישם תפיסה זו, ארגונים צריכים לבחון את תשתיות ה-IT שלהם, לבדוק מהו המידע הארגוני ומה בתוכו הינו מידע קריטי, ועל בסיס זה לבצע את מתווה ההגנה הארגוני. לנו יש את הפתרונות הנדרשים ליישום תפיסת האבטחה, לרבות מענה לעולמות הווירטואליזציה, מיחשוב הענן והמיחשוב הנייד".

איומים מורכבים וממוקדים

מהם האיומים מולם ניצבים מנהלי אבטחת המידע והמנמ"רים?

"איומי אבטחת המידע כיום מורכבים ומתוחכמים יותר מבעבר, ובעיקר ממוקדים. הם כבר לא איומים גנריים כמו פעם, אלא דינמיים ומשתנים. הנוזקות 'רעילות' הרבה יותר מכפי שהכרנו. מאפיין בעייתי נוסף של האיומים הוא שהם לא נראים, מה שמקשה על ההמחשה שלהם בפני הנהלות ארגונים. בנוסף, הכמות שלהם עולה באופן דרמטי: ב-2010 הייתה כמות הנוזקות החדשות שנוצרו גדולה יותר מסך הנוזקות שנוצרו בשלושת העשורים האחרונים.

האסטרטגיה של סימנטק נחלקת להגנה על המידע; הגנה על התשתיות והיישומים של הארגונים, לטובת שרידות וזמינות; והיערכות לקראת אסון והתאוששות מהירה אם וכאשר הוא אכן קרה.

מנהלי האבטחה הארגוניים נאלצים להתמודד עם שלל אתגרים, כשאחד המרכזיים שבהם הוא התפוצצות המידע. נהוג היה לומר כי המידע הארגוני מוכפל מדי 18 חודשים . כבר כיום נוצרים במערכי ה-IT הארגוניים מדי שנה 800 פטה-בייט של מידע. מגמה נוספת היא מתקפות שנועדו לפגוע במערכות הפיזיות של ארגונים ולשבש את פעילות הייצור שלהם, דוגמת סטוקסנט ודוקו".

וירטואליזציה, ענן ומיחשוב נייד

מה עוד משפיע על ההגנה על ה-IT?

"שלוש מגמות נוספות משפיעות אף הן על האופן שבו יש להגן על המיחשוב הארגוני. האחת היא וירטואליזציה, שכבר נמצאת במיינסטרים. השנייה היא מיחשוב ענן, שלגביה יש לוודא שהוצאת שירותים ויישומים מחוץ לארגון לא תביא לו נזק. המגמה השלישית היא מיחשוב נייד. העובדים מביאים רכיבי מיחשוב נייד וטלפונים חכמים מהבית - דבר הדורש התייחסות מיוחדת למידע הארגוני