



ארט קוביילו פותח את הכנס השנתי RSA 2012

ארגוני אבטחה. אני מציע דגם של אבטחה מונחית מודיעין, שמבוסס על הבנה מעמיקה ותעדוף מחדש של סיכונים עסקיים ומתמקד באסטרטגיות למיתון סיכונים. הטמעת אסטרטגיות אלה מייצרת ארגונים עמידים בפני איומים, הפועלים בהלימה ובתאימות לתקנות (Compliance). עוד תובנה שאני מציג בכל עת היא, שהמצב המצוי לעומת הרצוי הוא ש-80% מתקציב האבטחה בארגונים מיועד להגנה מפני פריצות ונוזקות למיניהן, ורק המעט שנותר הולך למעקב, ניטור ותגובה. המטרה היא ליצור איזון בין התקציבים, ולהביא למצב שבו תקציב התגובה, כלומר ההתקפה, יצמח לכדי שלישי.

"לגבי השאלה, מה יוצא לי ול-RSA מנאומי ה'תוכחה' שלי, ובכך כך מזהים אותי ואת RSA - כמבינים את התחום וכמובילים את אבטחת המידע בארגונים. הקהל שומע מה יש לנו להציע למנמ"רים כפתרונות מוכחים לבלימת ההתקפות להגנה על הנכסים הפיננסיים ונכסי המידע. RSA מוכרת בעולם כמובילה באבטחת המידע מאז התחלנו להציע פתרונות, ועתה המנמ"רים נוכחים שאנו מתחדשים ומתעדכנים, כי יש לנו מידע מובהק ומוכח של מציאות הסייבר ופתרונות האבטחה שלנו מדויקים ואמינים. ההוכחה היא שאנו ממשיכים לצמוח".

**כמי שמכיר ומוקיר את השוק הישראלי, חברות האבטחה בו והרמה הגבוהה של האנשים הפועלים בו, איך אתה רואה את התפתחות שוק אבטחת המידע הישראלי ומה בדבר רכישת ידע ו/או חברות מקומיות?**

"כולם מכירים את ה'סוד' וגם אני שותף לו: ישראל ואנשי אבטחת המידע שלה הם מהטובים בעולם. החממה הטובה בעולם היא הצבא הישראלי וזרועות המודיעין שלו, המובילים באבטחת מידע ובהתקפות מתקדמות ביותר - כך לפחות לפי המתפרסם במדיה הגלובלית. יש לנו פעילות מעמיקה ורחבה של ניטור הרשת העולמית מפני חדירות ופריצות, כשירות מתקדם לאלפי בנקים ומוסדות פיננסיים בעולם וגם מעבדות פיתוח למוצרי אבטחת מידע. בקרוב יתמנה מנכ"ל חדש לפעילות של הצוות, והוא יהיה איש מקצוע בכיר מהמעלה הראשונה. "ייתכן שבעתיד נרכוש טכנולוגיות או חברות אבטחה ישראליות נוספות. במבנה של EMC יש מנהל פיתוח עסקי ברמת החברה כולה וגם מנהל מיוחד לפיתוח עסקי ורכישות ומיזוגים, המקדיש את זמנו לחטיבת אבטחת המידע, RSA. כלומר, אנו רציניים ביותר להמשיך ולצמוח - הן

אחרים הקשורים אליהם בקשרים עסקיים. כל שרשרת הערך של כל ארגון חשובה להתקפה. לא מדובר רק בארגונים גדולים או ביטחוניים הקשורים לממשלות, אלא גם בעסקים קטנים המשמשים כספקים לאחרים. לכן, חייבים לשתף מידע ודרכי פעולה בהגנה.

"אפשר לראות את שיתוף הפעולה שקיים כבר שנים רבות בין הגופים הפיננסיים בעולם. הבנקים, הכפופים לרגולציה חזקה ונתונים לתקנות ממשלתיות, משתפים ביניהם פעולה כדי לשפר את תגובתיהם גם באבטחת מידע. סיבה חשובה נוספת היא המוצר של הבנקים, שהוא 'כסף', והערך של הגנה עליו מפני מתקפות ברור לכולם. אך כמו המגזר הפיננסי, יכולים לעשות זאת גם ארגונים במגזרים אחרים. בטווח הארוך, אני בטוח שיקומו שיתופי פעולה כאלה במגזרים נוספים, שייחצו גבולות מדינתיים ויגלו את הערך הגדול של שיתוף הפעולה לעומת התגוננות של כל גוף בנפרד - אפילו גורמים שמתחרים זה בזה".

**אתה פותח כל כנס של RSA בהטפה כיצד להתגונן, בהסברים לאן הולכת התעשייה ובעיקר מעודד את המנמ"רים בארגונים להעלות את המודעות שבחשיבות השקעת משאבים באבטחת המידע. מה יוצא ל-RSA מהרצאותיך? בסופו של יום, אתה אחראי להגדלת ההכנסות של החברה?**

"נכון שאני תמיד נושא נאומים ברמת-העל של תחום האבטחה ומקפיד לחשוף את המגמות החדשות בפריצות הגנה ובהתקפות על ארגונים. כיום כבר אין צורך לעורר את המודעות לאבטחת המידע ואף לא להגביר אותה, כי כולם מודעים - ממנהל אבטחת המידע בארגון, דרך המנמ"ר ועד צמרת ההנהלה והמנכ"ל. היום חייבים ללמד את הארגונים להשתמש בשיטות אבטחה מבוססות בינה עסקית ובמודיעין כלכלי ומעין צבאי. המודלים העדכניים של אבטחת המידע אינם מתקדמים במהירות מספקת לביצוע המעבר מאבטחה מבוססת היקף, לאבטחה מונחית מודיעין. זאת, בעוד שהאויבים הופכים למתוחכמים יותר. אסטרטגיות, גישות וטכנולוגיות מיושנות, מונעות מארגונים להתגונן בצורה יעילה מפני סיכונים שמתפתחים במהרה.

"אני גם טוען מעל כל במה שניתנת לי, שההקצאות הבלתי מאוזנות בתקציבי האבטחה, המחסור בכוח אדם מיומן ופער התפיסה לעומת המציאות, מהווים את האתגרים המרכזיים הפוגעים באפקטיביות של