

"עיריית ראשל"צ משפרת את אבטחת המידע"

איציק כרמלי, מנמ"ר עיריית ראשון לציון, אמר ש"רק אחרי שנכנסתי לתפקידי הבנתי את המורכבות והאתגרים שיש ברשות עירונית שמשרתת 250 אלף תושבים, שיש לה 30 אתרים ו-4,500 עובדים, ששליש מהם עובדים בסביבת מחשב".



איציק כרמלי

"אנחנו מצויים בשנה וחצי האחרונה בתהליך שיפור היבטי אבטחת מידע", מסר. "הוספנו מערכות, עיבנו את מערך אבטחת המידע בעירייה ואנחנו מיישמים קו עם שאר השוק". הוא סיים בציינו, כי "ההתנהלות בעולם אבטחת המידע היא בעיקרה באגף מערכות מידע בעירייה. אין רגולציה ברשויות - כל רשות לעצמה". "ראיית הסייבר והמתקפות הקיברנטיות היא מעבר לראייה הכוללת של אבטחת מידע יומיומית, אלא אירוע טרוו. סייבר הוא

לא עוד כלי להשגת כסף, אלא משהו אחר", כך אמר עו"ד **אופיר ליבר**, מנהל אבטחת



אופיר ליבר

מידע ומניעת הונאה במגדל טכנולוגיות. לדברי עו"ד ליבר, "במסגרת הפעילות הנעשית להבנת שדה הקרב החדש נכנסו ההיבט של מודיעין. אנחנו מתחילים להבין מה קורה מחוץ לרשת, כמה אני על המפה של גורמים אחרים. כעת זה חלק מההסתכלות". "אנחנו כפופים להנחיות שונות, של המפקח על הביטוח, שהוא הרגולטור שלנו לתחום", הוסיף. "מדובר בתפיסה שונה. אנחנו עושים בימים אלה מיפוי של סיכונים, על מנת לראות איך נוכל להפחית ולמצמצם את ההשפעה האסטרטגית של פגיעת סייבר".

"חווית הסייבר שונה מבתהליכי אבטחת מידע מסורתיים"

עופר סמדרי, מנהל אבטחת המידע של

דואר ישראל ובנק הדואר, אמר ש"חווית הסייבר שונה מזו שיש בתהליכי אבטחת מידע מסורתיים".

לדבריו, "מימד הסייבר לא מביא עוד כסף, כי אם מבהיר את מקומן של התשתיות, מקומם של העובדים, מה הם הסיכונים בחוץ ואיזה מין יעד אנחנו".



עופר סמדרי

בהיבט הרגולציה, ציין סמדרי, "יש עלינו מפקח במשרד התקשורת, נהיה מפקחים כמו הבנקים, עם בקרה בהיבט הפרטיות מצד רמו"ט שבמשרד המשפטים". עוד הוא אמר, כי "קיבלתי כמה פניות מהמטה הקיברנטי הלאומי, על מנת להבין איפה אני עומד ביחס למה שמצופה מאיתנו להיות. נכון תוכנית המשכיות עסקית מלאה. צפויה לנו הרבה עבודה בתחום".

יוסי הטוני

המשתמש הפכה להיות הגבול החדש של הסייבר".

לדבריו, "האבטחה המרבית על זהות המשתמש נמצאת כיום מאחורי מנגנון עני ביכולות ההגנה שלו". ברודנר ציין בהקשר זה יוזמה של הארגון האמריקני NSTIC (National Strategy for Trusted Identity in Cyberspace), שלדבריו



דניאל ברונר

"מספקת מימון חלקי והדרכה מתאימה לארגונים, כך שיהפכו לספקי זהות אמינה ומוגנת למשתמשים, באמצעות מעין תעודת זהות דיגיטלית שאותה אפשר להציג ברשת בצורה פשוטה". "צריך למצוא דרכים לוודא זהות בצורה זולה ומיטבית ולזהות סיכון שמופנה נגד משתמשים כגון ילדים", הוסיף ברודנר. "זה דורש תאימות וטכנולוגיות federation. אנחנו, ב-CA, יודעים לוודא שהזהות שמורה, לאתר סיכון ולתת גישה למשאבים בארגון תוך כדי סיווג המידע".

מחשב כך שיהיה ניתן לטפל באיום בצורה מבוקרת", אמר תדהר. "השכבה החמישית היא ה-Threat Cloud. זהו ענן מיחשוב שמאפשר להכיר את האיומים ולתת להם מענה. החיבור לענן מאפשר לקבל את כל העדכונים על האיומים ולזהות מתקפות בעזרת רשת חיישנים של צ'ק פוינט ואמצעים אחרים. ניתן לזהות התקפה חדשה ברגע שבו היא מופיעה ומייד להפיץ את העדכון לגביה. כך, זיהינו 250 מיליון כתובות אינטרנט בעייתיות, 300 אלף אתרים עם נזקות ו-1,000 כתובות אינטרנט בעייתיות בכל יום", ציין.

תדהר הוסיף, כי הנדבך השישי הוא הגנה מפני מתקפות מניעת שירות מבזרות (DDoS), "הן בשכבת הרשת והן בשכבת היישומים. המוצר של צ'ק פוינט חוסם מתקפות מסוג זה ללא התערבות האדמיניסטרטור". "השכבה השביעית היא של שירותי האבטחה", ציין. "האדמיניסטרטור הממוצע צריך סיוע כדי לדעת איך מתייחסים למכלול הדיווחים על פגיעות באבטחת מידע. המערכת מאפשרת לשלוח לוגים למומחי צ'ק פוינט, שניתחו אותם ויפיקו מענה בהתאם. כך ניתן לזהות, למשל, מתקפה על שרת מסוים ולוודא שהוא יהיה מוגן". הוא סיכם באמרו, כי "הדרך של צ'ק פוינט היא לנהל אבטחת מידע באופן רב שכבתי - אך ממקום מרכזי יחיד".

"זהות המשתמש - הגבול החדש של הסייבר"

דניאל ברונר, יועץ אבטחת מידע בכיר ב-CA ישראל, אמר ש"זהות