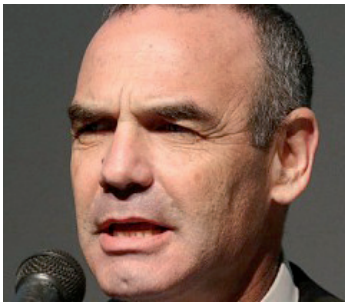
ארז קריינר, לשעבר ראש רא"ם: "ישראל לא מוכנה מספיק טוב מול האיומים הקיברנטיים נגדה"

"התשתיות הקריטיות של ישראל מוגנות ברמה טובה, אבל במקומות אחרים, היכן שהגופים לא מונחים על ידי השב"כ והזרועות המתאימות, הרמה בינונית ופחות מזה", אמר קריינר, כיום נשיא Five C ♦ הוא דיבר בפורום CISO של אנשים ומחשבים על אוסינט והסביר איך הוא מעריך את האויב האיראני

יניב הלפרין

"ישראל לא מוכנה מספיק טוב מול האיומים הקיברנטיים שיש עליה. התשתיות הקריטיות של ישראל מוגנות ברמה טובה, אבל במקומות אחרים, היכן שהגופים לא מונחים על ידי השב"כ והזרועות המתאימות, הרמה בינונית ופחות מזה", כך אמר **ארז קריינר**, לשעבר ראש רא"ם בשירות הביטחון הכללי וכיום נשיא Five C, שעוסקת במתן פתרונות סייבר.


ארז קריינר

קריינר אמר את הדברים במפגש של פורום CISO מבית אנשים ומחשבים, שנערך באחרונה בתל אביב בהנחיית אבי וייסמן, מנכ"ל שיא סקיוריטי.

לדבריו, הצעד הראשון לקראת שיפור אבטחת המידע כבר נעשה: הגברת המודעות לאיומים ולחשיבות שלה. עם זאת, "ההבנה של ארגונים שהאבטחה היא חלק אינטגרלי כמו התפעול עדיין לא קיימת במלואה. אבטחת המידע היא חלק אינהרנטי מאספקת הגז או החשמל בחברות רלוונטיות ובהרבה מקרים, הן עדיין לא מבינות את זה. עד שתהיה תובנה ברורה של חשיבותה המצב לא ישתפר".

יחידת רא"ם הוקמה ב-2002 ומאז מיפתה את המשק הישראלי, במטרה להגדיר מהן תשתיות קריטיות ואילו הן החברות שעוסקות בכך. ככלל, אמר קריינר, "מנהלים רבים בארגונים שנפגשתי איתם אמרו לי: 'לי זה לא יקרה'. אחד המקרים היה במפעל כימי בצפון. בהנהלת המפעל אמרו לי: 'עשינו גיבויים רבים, כי אנחנו מפעל כימי'. למחרת אותה שיחה היה באותו מפעל פיצוץ אדיר. הטלפון השני שהם עשו היה אליי, לשאול האם ביצענו תרגיל שהתחרבש. זאת דוגמה להבנה טובה של מרחב האיומים שמדברים עליו".

"בשנה האחרונה אני מסתובב הרבה מאוד בעולם ורואה שיש השתוקקות לידע הישראלי בסייבר. אנחנו מובילים בתחום", ציין קריינר. לדבריו, הסיבה שיש בישראל ידע רב בתחום היא הימצאותה "בשכונה קשה. זה הופך אותנו לסוג של מגדלור לגופים בחו"ל".

בהמשך דיבר קריינר על האוסינט - המודיעין הגלוי. "כשמדברים על זה, כל אחד רואה בעיני רוחו משהו אחר", אמר. הוא ציין כי חברות גלובליות מבצעות אוסינט עקב הערך הכלכלי שטמון בכך. "מנהל צריך לשאול איך משתמשים באוסינט ומה זה נותן לחברה", אמר. "ארגוני מודיעין צריכים לבור את המוץ מן התבן. יש הרבה מאוד שיטות לאסוף מידע - החל ממנועי חיפוש דרך זחלנים בכל מיני מקומות ועד לתוכנות לשליטה באווטארים - דמויות מקבילות עם חשבונות ברשתות החברתיות שיש להן חיים משלהן והן אוספות הרבה מידע".

הוא הציע דרך מעניינת להגדיר מה זה אוסינט: "תחשבו מה זה לא אוסינט ודרך זה תגיע ההגדרה שלו", אמר. "ככלל, מה שחשוב הוא איך הארגון משתקף כלפי חוץ ואיך הוא יכול להשתמש באוסינט לטובתו ולטובת הצרכים שלו שהוגדרו". קריינר המליץ למשתתפים: "תגדירו טוב את הצרכים. לקבל הרבה מידע זה פיתיון לא קטן, מעניין, מסקרן ומרחיב אופקים, אבל לא כל כך ברור ולא תמיד פשוט להבין מה אנחנו באמת צריכים".

"לא לחכות לתקיפה של היריב"

קריינר הציע "לא לחכות לתקיפה של היריב, אפשר ליצור דרך לתעל את התוקף לאן שנוח להתעמת איתו, משום שזה יותר קל. התוקף ינסה ללכת למקומות שהוא צריך להשקיע פחות עבודה כדי להגיע אליהם. חיסכון במשאבים זה דבר שמדבר גם אליו".

"צריך להיות כמה שיותר מודעים לכך שהמידע נמצא באינטרנט, להבין מה עובר על הארגון במתקפות סייבר ואם זה פוגע בו - איך הוא יכול לנטרל את הפגיעה", הוסיף.

לשאלת וייסמן על "הרא"ם האיראני" השיב קריינר: "תמיד לקחנו ברא"ם שלנו בחשבון שהיריב מאוד חכם, גם האיראני. יש לנו כמה יריבים עם היסטוריה מאוד עתיקה של חוכמה: המצרים בנו את הפירמידות, הסינים ירו רקטות לאוויר פחות או יותר באותה התקופה והאיראנים המציאו את השחמט. יש להם מסורות מראות שהם יכולים לעשות פרויקטים מאוד גדולים. שידרתי לאנשים שלי שאנחנו צריכים להתייחס ליריב האיראני כאילו הוא חכם יותר מאתנו ולמרות זאת, לא מצליח לעשות את מה שהוא מתכנן. יש לאיראנים יכולות טובות והם כל הזמן משפרים אותן, ואני מעריך מאוד את יכולות הפקת הלקחים וביצוע הדברים שלהם".

"הפוקוס של התוקפים עובר לארגונים עם רצפת ייצור"

"היקפי הגניבות העיקריים באמצעות מתקפות סייבר ימשיכו להיות ממוסדות פיננסיים שלא העלו את רמת האבטחה יותר מאשר כזו שמסוגלת לעקוף את התקיפות הפשוטות. עם זאת, הפוקוס מתחיל לעבור למידע ששווה יותר כסף, רחוק מהסקטור הפיננסי. יהיו הרבה