

"מדינת ישראל צריכה ליצור רגולציה ברורה בתחום אבטחת מידע"

כך אמר גבריאל חי, יועץ ומנתח מערכות בכיר לכלכלת אבטחת מידע, בפורום CISO שעסק בכלכלת אבטחת מידע ♦ חי קרא להקמת לשכה ייעודית בתחום אבטחת המידע כפי שקיימת בקרב רואי החשבון ועורכי הדין

רן מירון

לימודים בתיכון". עם זאת, ויסמן סיים את דבריו בנימה אופטימית. "השנה הוחלט על תוכנית שבמסגרתה 22 בתי ספר תיכוניים ישתתפו בפייולוט בתחום ההכשרה לאבטחת מידע. התוכנית תופעל במימון משותף של המטה הקיברנטי הצבאי ומשרד החינוך. בנוסף, השנה צפויות להיפתח שלוש פקולטות ללימודי אבטחת מידע - באוניברסיטאות בן גוריון, תל אביב והטכניון, אף הן במימון משותף של המטה הקיברנטי הצבאי".

מטריקות ומדדים באבטחת מידע

איתי ינובסקי, יועץ לאסטרטגיית אבטחת מידע וסניבר CISO, הרצה בפורום על מטריקות ומדדים באבטחת מידע. "מנהלי אבטחת מידע מתקשים סביב האופן שיש לדווח על פעולות המבוצעות בתחום אבטחת המידע ולהציג את הערך של מה שבוצע", אמר. "זה שלא אידע שום דבר, אולם כיצד ניתן לדעת האם האירוע קרה מאחר שמנהל האבטחה עשה משהו - או לא עשה?"

הוא הוסיף, כי "יחידת אבטחת המידע נחשבת בארגון כמרכז הוצאה - יחידה שמבקשת כסף מההנהלה, אולם לא ממש ברור מה נעשה איתו". לדברי ינובסקי, נדרשת הכנסת שפה וסטנדרטיזציה לעולם אבטחת המידע בארגון. "מנהלי אבטחת מידע צריכים לאמץ מתודולוגיה ברורה, שמסדירה מה יש לדווח להנהלה ובאיזו שפה לעשות זאת".

בהרצאתו הציג ינובסקי מתודולוגיה המאפשרת לקשור בין הסיכון של הארגון, מאמצי האבטחה, ההשקעה הנדרשת וההון המוקצה לכך. זאת, במטרה שניתן יהיה להצדיק את הפעולות של מנהל אבטחת המידע בתוכניות הארגון לשנה הבאה ולטווח רחוק יותר. "המודל שפיתחנו מציג נוסחה המאפשרת לקשר בין הבקורות לבין רמות הסיכון השונות, וכך מתאפשרת תפירת חליפת אבטחה לארגון, שמשקפת נאמנה את רמת הסיכון, ללא תלות עוד נתונים לא רלוונטיים או מגמות שוק חולפות", אמר.

ינובסקי הדגיש את הצורך של מנהלי האבטחה להציג בפני מקבלי ההחלטות בארגון נתונים ברורים. "לנהל עסקים זה לנהל סיכונים, וכשהמנהלים הבכירים מבינים את הנתונים זה נותן להם תשתית טובה לקבלת החלטה נכונה יותר", ציין. "הם אלה שמנהלים את הסיכון עבור הארגון בכללותו".

מפגש הפורום נחתם בהרצאתו של **דודי פישר**, סמנכ"ל טכנולוגיות אבטחת מידע ב-WeI, שהציג מתודולוגיה לזיהוי וטיפול באירועי עוינים בלתי מזוהים (SIEM).

מנהל אבטחה בארגון צריך להיות מחויב להתנהלות מסוימת. במקרה של כישלון - הוא יהיה זה שיישא בתוצאות, בין אם זה איבוד המשרה או רשיונו לעסוק במקצוע", אמר **גבריאל חי**, יועץ ומנתח מערכות בכיר לכלכלת אבטחת מידע, במפגש פורום CISO, שעסק בכלכלת אבטחת מידע. המפגש נערך במלון לאונרדו בשרתון סיטי טאואר שברמת גן.

לדבריו, "רק באמצעות אכיפת מודל של תשלום אישי עבור מחדל נראה בשוק הישראלי אבטחה טובה וסדורה יותר". חי הוסיף, כי אמנם, מונופול אבטחת המידע נמצא בידי מדינת ישראל, אך היא מתנהגת באופן לא בוגר ולא לוקחת אחריות בתחום. "הגיע הזמן שמדינת ישראל תקבע גורם מאשר בתחום האבטחה ורמת האבטחה הרצויה במגזרים השונים", אמר. הוא קרא להקמת לשכה ייעודית בתחום אבטחת המידע, כפי שקיימת בקרב רואי החשבון ועורכי הדין.

אבי ויסמן, מנחה האירוע, אמר במפגש שראוי שתהיה לכלכלת אבטחת מידע בארגון. לדבריו, אבטחת מידע נמדדת במונחים כספיים, כיוון שהיא מתבטאת בעלויות ישירות ובעלויות מצטברות בארגון. "כפי שיש לכלכלת מחלקת רכב בארגון, שקובעת האם כדאי לשטוף את הרכבים ובאיזו תדירות, כך צריך לייצר מקצוענות גם בתחום אבטחת המידע", המליץ. "כל פעילות בתחום צריכה להיות מתומחרת וניתנת לאמידה".

לדברי ויסמן, מן הראוי שכפי שמשפטים ורופאים לומדים היבטים כלכליים הקשורים במקצוע כך אמור להיות אף בתחום אבטחת המידע. לעומת הצורך במדידה ותרגום אבטחת מידע למונחים כספיים, הודה ויסמן, כי שלא כמו בעבר, כיום מומחים כבר לא ממערים להגיע לארגונים ולהבטיח להם מדידה של ROI בתחום אבטחת המידע, כיוון שהלקוחות הבינו שקשה מאוד עד בלתי אפשרי למדוד החזר השקעה בתחום.

אין אבטחת מידע באקדמיה

עוד הוא אמר, כי ישראל היא אחת המדינות המערביות הבודדות שבה לא ניתן ללמוד באקדמיה את תחום אבטחת המידע, על אף שמדובר במקצוע לכל דבר. "זה אולי לא פוליטיקלי קורקט להגיד, אבל ישראל היא לא מעצמת סייבר, אלא אפריקה. אולי יש לנו גופי תקיפה מצוינים, אבל ההתרשמות שלי היא שזה מתחיל ונגמר בזה". לדבריו, "אם בעבר ישראל הייתה במקום ה-30 בתחום אבטחת המידע, כיום היא הידרדרה מתחת לקו ה-50. ישראל היא אף לא בין 15 המדינות שמפעילות תוכניות

