- אנשים ומחשבים – פורטל חדשות היי-טק, מיחשוב, טלקום, טכנולוגיות -
- https://www.pc.co.il

"חודשיים אחרי כניסת ה-GDPR – החברות הישראליות עדיין לא מוכנות"

Posted By *ג'ון בן-זקן* On 24 ביולי 2018 @ 14:47 In אבטחת מידע וסייבר,בראש הכותרות,חדשות,חדשות מתפרצות | No Comments

"על אף שרגולציית ה-GDPR האירופית ותקנות הגנת הפרטיות הישראליות נכנסו לתוקף כבר לפני כחודשיים, חלק גדול מהחברות בישראל לא השלימו ואף לא התחילו את הפעילות הנדרשת על מנת לעמוד בתקנות אלה", כך אמר רו"ח **חנן טויזר**, שותף ואחראי על תחום הפרטיות ב**פאהן קנה ניהול בקרה Grant Thornton Israel**. לדבריו, "חוסר היערכות זה של חברות ישראליות עלול ליצור חשיפה משמעותית לסנקציות מטעם הרגולטורים, לרבות קנסות מנהליים, ובמקרים חמורים אף להביא לכדי כתבי אישום".

הראיון עם טויזר נערך בעקבות סקר דירקטורים המכהנים כחברי ועדות ביקורת שערכה החברה, שחשף את מצב ההיערכות של חברות ציבוריות ישראליות ליישום דירקטיבת ה-GDPR ותקנות אבטחת המידע והפרטיות הישראליות החדשות. בסקר, שנערך בסוף יוני, השתתפו 59 דירקטורים המהווים מדגם מייצג של דירקטורים בחברות אלה. על פי הערכת מחלקת המחקר של הפירמה, יש בישראל כ-1,000 דירקטורים חברי ועדות ביקורת, המכהנים בדירקטוריונים של כ-500 חברות ציבוריות.

מהם הממצאים הבולטים של הסקר?

"הסקר מגלה שלמרות איומי הסייבר הרבים על ארגונים ישראליים בשנים האחרונות, חברות ציבוריות רבות בארץ עדיין לא מוכנות להתמודדות איתם. מבין הדירקטורים שתשאלנו, 41% מדווחים שבארגונים שבהם הם מכהנים לא התקיים בשנה האחרונה דיון דירקטוריון בנושא סיכוני סייבר ו-39% גילו שהארגון שבו הם ממונים חווה תקיפת סייבר או זליגת מידע בשנה האחרונה. בו בזמן, ב-53% מהארגונים לא בוצע סקר סיכוני סייבר, לרבות מבחני חדירה (Penetration Tests). ואם זה לא מספיק, 57% השיבו שהארגונים לא נערכו ליישום ה-GDPR ותקנות ההגנה על פרטיות ו-35% ענו כי הארגון בו הם מכהנים לא גיבש מדיניות פורמאלית בנושא אבטחת סייבר וזליגת מידע".

איום סייבר יכול לבוא בצורה של מתקפה חיצונית, אבל קיימים גם איומים מתוך הארגונים. האם בדקתם את המצב בישראל בתחום זה?

"כן. התמקדנו בגניבת מידע על ידי עובדים. שאלנו לאילו מאוכלוסיות העובדים קיים פוטנציאל גדול יותר לגניבת מידע מהארגון ו-61% הציבו בראש את עובדי מערכות המידע. 19.5% מהדירקטורים ענו שעובדי מחלקת הכספים הם בעלי הפוטנציאל הגבוה ביותר לגניבת המידע, 11.5% סימנו את חברי הנהלת הארגון ו-8% – את עובדי מחלקת שירות הלקוחות".

לדברי טויזר, הסיכון מצד אנשי ה-IT גדול כי "לרוב הם מחזיקים בהרשאות על (Superusers), שמאפשרות גישה לכלל המידע בארגון, ולכן יש קושי למדר אותם. יחד עם זאת, קיימים כלים לניטור פעילותם של אנשי מערכות המידע, לרבות הגדרת התראות למקרים שבהם מנהל ה-IT משבית את מנגנוני הניטור".

על מה ארגונים צריכים להקפיד בהיערכות לתקנות הגנת הפרטיות ול-GDPR?

"ארגונים בארץ צריכים להבין שיישום היערכות של בנק לא דומה ליישום היערכות של חברת מדיקל או סטארט-אפ. לכן, יש חשיבות רבה להיערכות ממוקדת, שתתאים לרמות הסיכון ולהיקף המשאבים של הארגון. גם ארגונים קטנים יכולים להיערך היטב לעמידה בתקנות ה-GDPR והגנת הפרטיות, בתקציב יישום צנוע. הסקר שלנו הוא קריאת השכמה לכל הארגונים שלא התעוררו, כדי שיבינו שחייבים ליישם – ועכשיו".
