

בעקבות מתקפת הסייבר על שירביט: הרשות להגנת הפרטיות מפרסמת דגשים לאבטחת מידע

ביום 6.12.20 הרשות להגנת הפרטיות ("הרשות") פרסמה מסמך דגשים לאבטחת מידע בחברות וארגונים בעקבות מתקפת הסייבר על חברת שירביט.

לדברי הרשות, מתקפת הסייבר על שירביט ממחישה את ההכרח של חברות מכלל מגזרי המשק להגן על מידע אישי אודות לקוחות המצוי אצלן, ואת חשיבות עמידתן בחוק הגנת הפרטיות ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("תקנות אבטחת מידע").

בתוך כך, הרשות עמדה על כך שתקנות אבטחת מידע מחייבות כל גורם במשק בישראל, ציבורי ופרטי, המנהל מידע אישי, לקיים דרישות אבטחת מידע בהתאם לרמת הסיכון שיוצרת פעילות עיבוד המידע אצלו בארגון.

בין השאר, הרשות הדגישה כי על ארגונים לוודא כי הם מקפידים על ביצוען ויישומן של בקורות ניהוליות ועל מימוש ויישום מדיניות אבטחת מידע, לרבות:

1. גיבויים - יש לוודא ביצועם וקיומם של גיבויים תקינים;
2. הרשאות - רק על פי המינימום הנדרש למטרת הארגון; יש להימנע מהרשאות רחבות מדי;
3. חיבור מרחוק - רק על פי צורך, בהרשאה מותאמת ובעדיפות לכתובות מוגדרות;
4. עדכונים - לשמור על מערכות ותוכנות מעודכנות בגרסאותיהם ובעדכוני האבטחה;
5. סיסמאות - לעבוד בכפוף למדיניות סיסמאות וגישה מוקשחת;
6. סגמנטציה - להקפיד על הפרדה בין רשתות והמערכות השונות בארגון;
7. ניטור ובקרה - לקיים ניטור ובקרה של התחברויות ופעילות ברשת לשם זיהויה של פעילות אנומלית;
8. מערכות זיהוי - ישומן של מערכות IDS/IPS לזיהוי והתרעה מפני חדירה בנוסף למערכות ההגנה והאנטי-וירוס.

אירועי סייבר כדוגמת זה שאירע בחברת שירביט טומנים בחובם עלויות רבות, חשיפה משפטית לתביעות ופגיעה משמעותית במוניטין החברה. על רקע זה, קיימת חשיבות רבה לנקוט צעדי היערכות הולמים ובכלל זה לוודא הטמעתן של תקנות אבטחת מידע בארגון.

לפרטים נוספים:

עו"ד אסף הראל, שותף
assafh@gornitzky.com

