SECAUDIT
IT & CYBER AUDIT EXPERTS

שימוש ב AI על ידי ספקים חיצוניים – איך מנהלים את הסיכון

הטמעת מערכות בינה מלאכותית (AI) בארגונים הפכה למגמה עולמית, המאפשרת אוטומציה, שיפור תהליכים והפקת תובנות מתקדמות. יחד עם זאת, השימוש ב AI ובמיוחד כאשר הוא נעשה על ידי ספק חיצוני, מעלה סיכונים מהותיים בתחום אבטחת המידע והגנת הפרטיות. אחד הסיכונים המרכזיים הוא חשיפת מידע רגיש של הלקוח לסביבות שאינן בשליטתו הישירה של הארגון.

מהות הסיכון

כאשר ספק חיצוני מקבל נתונים רגישים מלקוח ומזין אותם למערכת AI (לרוב מבוססת ענן ציבורי), נוצר מצב שבו המידע יוצא מסביבת הבקרה של הארגון. מידע זה עלול להישמר בשרתי צד שלישי, להיות מועבר למדינות אחרות, ואף לשמש לאימון המודל או לפעילויות נוספות מבלי שהלקוח מודע לכך או מאשר זאת.

הסיכונים העיקריים כוללים:

- **אובדן שליטה על המידע**: הלקוח אינו יכול לדעת היכן נשמר המידע, לכמה זמן, ומי יכול לגשת אליו.
- **דליפת מידע**: כתוצאה מפריצה, שימוש לרעה, או מנגנוני המודל המאפשרים חילוץ מידע.
- **הפרת רגולציה** –שימוש במידע באופן שאינו תואם תקנים וחוקים, כגון GDPR, חוק הגנת הפרטיות, או תקנות/הוראות רלוונטיות.

כיצד הסיכון נוצר

1. **מידע יוצא את הארגון** בשיטות העברה מידע מקובלות ומאובטחות (למשל כספות ארגוניות). מכאן והלאה המידע נמצא בידי הספק וביכולתו לשמור אותו מקומית, להעלות לענן, או להריץ מול מודל AI.
2. **העברת המידע למודול AI**: בעת הזנת נתונים למודל AI בענן, המידע נשלח לשרתי הספק, ולעיתים עובר בין מדינות שונות.
3. **שמירה ושימוש חוזר במידע** :ספקי AI רבים שומרים את הנתונים לפרקי זמן קצובים לצורכי ניטור או שיפור המודל, מה שעלול להוביל לשימוש עתידי בלתי מורשה.
4. **חשיפה דרך ממשקים אחרים**: במקרים מסוימים, מידע שנשמר עשוי להיחשף דרך בקשות של משתמשים אחרים או פריצות מתוחכמות , כגון במקרה של פריצה שבוצעה ל ChatGPT (חוקרי חברת Zenity הצליחו להשתלט על חשבונות, לגשת לשיחות ולחדור לקבצים אישיים בגוגל דרייב).

דוגמאות לספקים חיצוניים היוצרים את הסיכון

- **יועצים משפטיים**: מזינים נוסחי חוזים, כתבי טענות או מסמכים פנימיים הכוללים מידע עסקי סודי, פרטי לקוחות או פרטי עסקאות למערכות AI לצורך ניסוח, תרגום או ניתוח.

- **יועצי אבטחת מידע**: מנתחים בעזרת AI קונפיגורציות של מערכות אבטחה, חומות אש, מערכות זיהוי חדירות או כלי הצפנה, ובכך חושפים מפת הגנה וסודות טכניים.
- **יועצי משאבי אנוש:** מזינים נתונים אישיים של עובדים או מועמדים (קורות חיים, הערכות ביצועים) למודלים לניתוח או דירוג.
- **רואי חשבון ויועצי מס:** מעבדים בעזרת AI דוחות כספיים, ניתוחים כלכליים או פרטי עסקאות אסטרטגיות.
- **חברות מחקר ושיווק**: מזינות נתוני לקוחות, מאגרי CRM ותוצאות סקרים ל AI לצורך הפקת תובנות שיווקיות, תוך חשיפת מידע עסקי ופרטי לקוחות.

דרכי טיפול והפחתת הסיכון

צעדים טכנולוגיים

- **הסכמי עיבוד נתונ**ים: קביעת מגבלות ברורות, מעוגנות בהסכמים, על שמירת המידע ושימושו, כולל איסור על אימון המודל בנתוני הלקוח.
- **שימוש במודלים מקומיים** –העדפת מודלים המותקנים בסביבת הארגון(On-Premise או בענן פרטי מבוקר).
- **אנונימיזציה ופסאודונימיזציה** –הצבת דרישה ברורה כי אם מבוצע שימוש ב AI תבוצע הסרת מזהים ומידע מובהק לפני העברת הנתונים למודל.
- **הדרכת עובדים וספקים**: הבהרת כללים ברורים לגבי סוגי המידע שניתן להזין למערכות AI ותחת אילו תנאים.
- **בקרה תקופתית** –ביצוע ביקורות ובדיקות אקראיות לשימוש ב AI-אצל הספק.

סיכום

שימוש ב AI על ידי ספקים חיצוניים טומן בחובו פוטנציאל עסקי רב אך גם סיכון משמעותי לחשיפת מידע רגיש. ניהול הסיכון מחייב גישה רב-שכבתית הכוללת אמצעים טכנולוגיים, משפטיים ותפעוליים. ארגון שיפעל במודע ובזהירות יוכל לנצל את היתרונות שב AI מבלי לפגוע בביטחון המידע ובאמון הלקוחות.