

העובד החדש שלכם הוא AI - מי מבטח את הטעות שלו?

הבינה המלאכותית כבר מזמן אינה רק "עוזרת לעובדים". היא מתחילה לקבל החלטות, להפעיל מערכות ולבצע פעולות באופן עצמאי. השאלה הגדולה שאיתה מתמודדים כיום ארגונים היא: מי נושא באחריות כאשר המערכת טועה?

מאת: אורן בילבסקי ושלמה מוסלי - קבוצת בילבסקי גלובל - מומחים לביטוחי אחריות, סיכונים מיוחדים וביטוח בינלאומי

העובד החדש נכנס לארגון

עד לא מזמן, כאשר עובד ביצע פעולה שגרמה נזק ללקוח, לספק או לצד שלישי, שרשת האחריות הייתה ברורה דיה: העובד פעל, המעסיק נשא באחריות שילוחית, והביטוח הרלוונטי נכנס לתמונה.

אבל מה קורה כאשר "העובד" הוא מערכת בינה מלאכותית?

מערכות AI מתקדמות מסוגלות כיום לנתח מידע, לנסח מסמכים, להמליץ על החלטות, להפעיל תוכנות, לתקשר מול לקוחות ובמקרים רבים אף לבצע רצף פעולות שלם ללא אישור אנושי בכל שלב. השלב הבא שכבר מיושם בשטח הוא **AI Agent** - סוכן אוטונומי שמקבל מטרה וגישה למערכות הארגון, ומבצע בעצמו סדרת פעולות מורכבת כדי להשיגה.

התפתחות זו משנה לחלוטין את מפת הסיכונים. אירועים שנחשפו לאחרונה, כפי שדווח בין היתר ב**סוכנות הידיעות Reuters**, ממחישים כי סוכני AI עלולים לפעול באופן בלתי צפוי ואף לבצע פעולות סייבר ללא הנחיה אנושית ישירה. בעקבות זאת, חברות ביטוח בינלאומיות כבר בוחנות מחדש כיצד פוליסות Cyber Liability (חבויות) מסורתיות צריכות להתמודד עם אירועים שנגרמו על ידי מערכות אוטונומיות.

מה יכול להשתבש?

נניח שחברה מפעילה AI Agent המחובר למערכות הארגון. המערכת מורשית לקרוא דואר אלקטרוני, להפיק הצעות מחיר, לנתח חוזים, להזין נתונים ב-CRM, לתקשר מול לקוחות, לבצע פעולות ב-CRM ולקבל מידע ממקורות חיצוניים.

כעת, נניח שהמערכת ביצעה טעות. לא מדובר בהכרח ב"הזיה" חמודה של צ'אטבוט, אלא בטעות תפעולית או מקצועית שעלולה מיליוני שקלים.

תרחיש 1: ה-AI נתן ייעוץ שגוי

חברת ייעוץ משתמשת במערכת AI להכנת ניתוח עבור לקוח. המערכת הציגה נתונים שגויים, והלקוח הסתמך עליהם וקיבל החלטה עסקית שגרמה לו הפסד של 2 מיליון שקלים. מבחינת הלקוח, שרשרת הטיעון פשוטה: "אתם סיפקתם לי את השירות - לא המחשב". מקרה זה נכנס ישירות לעולם הקלאסי של "ביטוח אחריות מקצועית" (Omissions & Professional Indemnity / Errors).

תרחיש 2: שליחת מידע חסוי ללקוח הלא נכון

מערכת AI המנהלת את שירות הלקוחות מקבלת פנייה ומחזירה תשובה הכוללת בטעות מידע רגיש השייך ללקוח אחר. התוצאה: הפרת סודיות, אירוע פרטיות חמור, חשיפה לתביעה, הוצאות משפטיות, חובת דיווח לנפגעים, חקירה רגולטורית ופגיעה קשה במוניטין.

אירוע כזה מעלה שאלה מורכבת: האם מדובר באירוע סייבר? באחריות מקצועית? או באירוע הפרת פרטיות? התשובה היא ש-AI אינו יוצר בהכרח סיכון חדש אחד - הוא מחבר כמה סיכונים קיימים לאירוע משולב אחד.

תרחיש 3: AI Agent ביצע פעולה בלתי מורשית

חברה מעניקה ל-AI הרשאה לזהות חולשות אבטחה. ה-Agent מזהה חולשה, אך במקום לעצור ולדווח, הוא ממשיך באופן אוטונומי, עובר למערכות נוספות וגורם לחשיפת מידע.

כאן נוצרת שאלה ביטוחית מרכזית: אם החברה עצמה מעניקה למערכת הרשאת גישה מלכתחילה - האם מדובר בכלל ב"חדירה בלתי מורשית" (Unauthorized Access)? בשוק ביטוחי הסייבר מעסיקים את עצמם כיום בשאלה כיצד להחיל הגדרות מסורתיות של סייבר על פעולות שמבוצעות מתוך הרשאה קיימת, לצד סיכוני הגדרת מערכת שגויה (Misconfiguration).

תרחיש 4: החלטה אלגוריתמית מפלה

מערכת AI המשמשת לסינון וגיוס עובדים מנתחת אלפי מועמדים. לאחר מספר חודשים מתברר כי האלגוריתם יצר תוצאה מפלה. מועמד שלא התקבל תובע את החברה. הטענה "האלגוריתם החליט" אינה קבילה מבחינה משפטית או ניהולית; החברה היא שבחרה להשתמש במערכת, להגדיר אותה ולהזין את הנתונים, והיא שוויתרה על פיקוח אנושי הדוק.

תרחיש 5: הפרת זכויות יוצרים על ידי AI

מערכת AI מייצרת תמונה, טקסט, סרטון או קוד תוכנה, והחברה משלבת אותם במוצריה. בהמשך מגיעה דרישת פיצוי על הפרת זכויות יוצרים. במקרה זה מתעוררות שאלות של "אחריות קניין רוחני" (Intellectual Property Liability), לצד בחינת היקף הכיסוי בפוליסות האחריות המקצועית וסיכוני הסייבר הקיימות.

הבעיה הגדולה: לא כל AI Risk הוא Cyber

אחת הטעויות הנפוצות כיום בארגונים היא המחשבה: "יש לנו פוליטת Cyber, אז אנחנו מכוסים".

זהו אינו המצב בהכרח. פוליטת סייבר מסורתית בנויה בעיקרה סביב אירועים חיצוניים - כגון חדירת האקר, כופרה, או גניבת מידע זדונית. אולם AI Agent יכול לגרום לנזק כבד גם ללא גורם זדוני חיצוני, אלא פשוט על ידי שימוש שגוי בהרשאות הניתנות לו כדין או בשל כשל תפעולי פנימי (internal). כיום, חלק מהמבטחים מנסים להבהיר כיצד פוליסות קיימות מגיבות לאירועים אלו, בעוד אחרים מפתחים כיסויים ייעודיים.

אז מי באמת אחראי?

בעת אירוע נזק, האחריות המשפטית והחוזית עשויה להתחלק בין מספר גורמים:

1. **החברה המפעילה:** האם הפעילה את המערכת באופן סביר והציבה בקרות?
2. **ספק ומפתח ה-AI:** האם קיימים פגמים בקוד, במודל או בארכיטקטורה? (תחום המכוסה לרוב תחת פוליסות אחריות המוצר של הספק).
3. **הגורם המטמיע/המגדיר:** האם ניתנו למערכת הוראות או הגדרות קונפיגורציה שגויות?
4. **ספקי מידע צד-שלישי:** האם ה-AI הסתמך על מידע חיצוני שגוי?
5. **הנהלת החברה והדירקטוריון:** האם נקבעה מדיניות AI ארגונית, והאם היה פיקוח סביר על השימוש בטכנולוגיה?

רגולציה וניהול סיכונים: תקן חדש בשוק

החשיפה אינה מתמצה בתביעות של לקוחות, אלא מגיעה גם מצד הרגולציה. באיחוד האירופי, למשל, חוק ה-AI (AI Act) מציג סיווג של מערכות לפי רמות סיכון ומטיל חובות רגולטוריות משמעותיות על מפעילים וספקים - לרבות דרישות תיעוד, שמירת לוגים, ניהול סיכונים ופיקוח אנושי. בכך הופך ה-AI Governance מנושא טכנולוגי לעניין ניהולי ומשפטי ראשון במעלה.

בעולם ניהול הסיכונים הגישה הרווחת כיום, כפי שבאה לידי ביטוי בקווי המנחה של מכון התקנים האמריקאי (NIST AI Risk Management Framework), מבוססת על עיקרון מנחה: **קודם כל מנהלים את הסיכון שה-AI יוצר - ולאחר מכן מבטחים את הסיכון השיורי**. המסגרת מדגישה אמינות, בטיחות, שקיפות, הגנת פרטיות וניהול הטיות כחלק בלתי נפרד מהפעילות הארגונית.

הפתרון הביטוחי: ארכיטקטורת ביטוח סיכונים של בינה מלאכותית AI Risk Insurance Architecture

להערכתנו, הפתרון הנדרש אינו מסתכם ברכישת פוליסה בודדת, אלא בבניית ארכיטקטורת כיסוי מורכבת (AI Risk Insurance Architecture) שממפה את כל שרשרת הסיכונים ומותאמת לאופי הארגון:

- **שכבה ראשונה – ביטוח אחריות מקצועית (Professional Indemnity):** שכבת ההגנה המרכזית כאשר ה-AI משולב במתן שירות מקצועי ללקוחות. מומלץ לוודא כי הפוליסה מכסה באופן מפורש שירותים המבוצעים באמצעות AI, הסתמכות על תוצרי אלגוריתם, פעולות אוטומטיות, ואחריות לשגיאות ספקים.
- **שכבה שנייה - ביטוח סיכוני סייבר (Cyber Insurance):** בחינה מדוקדקת של כיסויי פריצת נתונים וכיסוי פרטיות ואירועי תפעול. הדגש כאן אינו רק על שם הפוליסה, אלא עמידה על הניסוח המדויק לגבי אירועים שנוצרו על ידי AI Agent או שימוש לרעה בהרשאות קיימות.
- **שכבה שלישית – ביטוח אחריות כללית וביטוח אחריות כלפי צד שלישי (General / Third Party Liability):** חיונית כאשר פעולת ה-AI משפיעה על מערכות פיזיות ועלולה לגרום לנזק לרכוש או לגוף.
- **שכבה רביעית – ביטוח נושאי משרה (Officers & Directors):** להערכתנו, זהו תחום שיקבל חשיבות הולכת וגדלה. במידה וייגרם לארגון נזק משמעותי משימוש ב-AI, בעלי מניות או רגולטורים עלולים לבחון האם הדירקטוריון והנהלה כוננו בקרות, הרשאות ומדיניות סבירות.
- **שכבה חמישית - ביטוח ספציפי לבינה מלאכותית (AI-specific Insurance):** מוצרי מדף מתפתחים המיועדים לחשיפות ייעודיות, כגון כשלים בביצועי מודל (Model Performance), הזיות (Hallucinations) והפרות IP. מדובר בפתרון משלים, כאשר לעיתים קרובות ניתן להגיע לכיסוי מיטבי באמצעות הרחבות מדויקות לפוליסות הקיימות.

תוכנית עבודה מומלצת לארגון

ארגון המפעיל מערכות AI נדרש לבצע ניתוח של פערים בביטוח של בינה מלאכותית מקיף:

1. **מיפוי מערכות:** רישום מלא של כלל מערכות ה-AI בארגון (מערכות CRM, שירות לקוחות, כוח אדם, מערכות פיננסים מערכות ייצור ואוטומציה).
2. **בחינת הרשאות:** אבחנה ברורה בין AI שמציע המלצה בלבד לבין AI שמבצע פעולה באופן אוטומטי.
3. **מעורבות אנושית באוטומציה:** הטמעת מגננוני אישור אנושי בפעולות קריטיות לצמצום החשיפה.

4. **תיעוד:** וידוא יכולת תחקור לאחר אירוע - איזה מידע נקלט, איזו הוראה ניתנה, מה הוחלט ומי אישר.

5. **בדיקת תיק הביטוח:** הבלטת שאלות ייעודיות מול הברוקר ומנהל הסיכונים.

שאלות מפתח לבחינה מול הברוקר:

- האם פוליסת ביטוח אחריות מקצועית (PI) מכסה שירותים או טעויות שמקורם ב-AI?
- האם פוליסת הסייבר מכסה אירוע שנגרם על ידי AI Agent הפועל בהרשאה?
- האם קיימות החרגות ל-AI או למערכות אוטונומיות (Autonomous Systems)?
- כיצד מוגדרת חשיפת הפרת קניין רוחני או הפרת פרטיות שנוצרה על ידי אלגוריתם?
- האם קיימות דרישות אבטחה או ניהול בינה מלאכותית המהוות תנאי מוקדם לתוקף הכיסוי?

מה אנחנו מציעים?

בקבוצת בילבסקי גלובל אנו מאמינים כי ניהול סיכונים נכון אינו מתחיל ממוצר הביטוח - אלא מהבנת הסיכון.

אנו מלווים ארגונים בתהליך סדור של סקירת סיכונים וביטוח של בינה מלאכותית הכולל:
מיפוי השימוש ב-AI ← זיהוי תרחישי נזק ← ניתוח אחריות משפטית וחוזית ← בדיקת תאימות של פוליסות שהוזכרו מעלה ← איתור פערי כיסוי ← ובניית פתרון ביטוחי מותאם בשווקים המקומיים והבינלאומיים.

העתידי כבר כאן

היום כבר לא שואלים "האם העסק משתמש בבינה מלאכותית?", אלא "עד כמה העסק מאפשר לבינה המלאכותית לפעול בשמו?".

AI מסוגל להקטין עלויות ולהגדיל פריון באופן דרמטי, אך כמו עובד אנושי - הוא עלול לטעות. ההבדל היחיד הוא שבינה מלאכותית מסוגלת לבצע טעויות בקצב של אלפי פעולות בדקה.

כשעידן ה-AI כבר כאן, זה הזמן לוודא שגם מעטפת ניהול הסיכונים והביטוח שלכם מותאמת למציאות החדשה.

האמור במאמר מהווה מידע מקצועי כללי בלבד ואינו מהווה ייעוץ משפטי או התחייבות לכיסוי ביטוחי. היקף הכיסוי נקבע בהתאם לנוסח הפוליסה, תנאיה, חריגה והרחבותיה, ולנסיבות כל מקרה לגופו.

