מסמך עזר לניהול מהימנות ולמניעת איומים פנימיים

המלצות החוקרים למניעת הונאה מצד גורמים פנימיים

מה עולה מניתוח של 36 מקרי הונאה מצד גורמים פנימיים בארגונים בארצות הברית.

החוקרים ניתחו 36 מקרים מתועדים ו-401 אירועים התנהגותיים, ממסמכי בתי משפט, פרסומי משרד המשפטים האמריקאי ודיווחים בתקשורת. הם לא מצאו פרופיל אחיד של מבצע ההונאה, וכמעט מחצית המבצעים החזיקו בתפקידי הנהגה. ההונאה התפתחה כתהליך שבו התנהגויות אנושיות וטכנולוגיות קשורות זו לזו, ובמקרים מסוימים המבצעים חשפו מידע על פעילותם לפני שימוש לרעה במערכות או גישה בלתי מורשית.[1]

36
מקרי הונאה שנבדקו

401
אירועים התנהגותיים

17/36
בתפקידי הנהגה וניהול

החוקרים מבססים את ההמלצות על תיאוריית מניעת הפשיעה המצבית (Situational Crime Prevention), שמתמקדת בשינוי התנאים שמאפשרים את העבירה.[1]

ההמלצות לארגונים

1. **שילוב זיהוי טכנולוגי ודיווח.** לפי החוקרים, הזיהוי עשוי להשתפר באמצעות זיהוי דיגיטלי אוטומטי וגם באמצעות דיווח של אנשים.
2. **בקרת הרשאות.** להגביל את העובדים להרשאות הנחוצות לתפקידם בלבד, כדי לצמצם הזדמנויות.
3. **ניטור טכנולוגי.** ניטור הדוק יותר של גישה בלתי מורשית למערכות. זיהוי אוטומטי צריך לחרוג מזיהוי שימוש לרעה בהרשאות.
4. **תרבות דיווח.** עמיתים שגורם פנימי סיפר להם על כוונה לבצע הונאה צריכים מקום בטוח לדווח על כך.
5. **ניתוח תקשורת.** ניטור התקשורת האלקטרונית לאיתור חשיפה של עבירה. כלי עיבוד שפה טבעית (NLP) לזיהוי דליפה של עבירה או של כוונה לבצע עבירה יכולים להיות חלק מארגז הכלים. יעילותם לא נבדקה במחקר.
6. **קשר עם מתחרים.** מדיניות שמגבילה פגישות של עובדים עם מתחרים, או מזהה פגישות חשאיות.
7. **אחריות של מי שמסייע.** האחריות צריכה לחול גם על מי שמסייע לגורם הפנימי, למשל בשיתוף סיסמאות או בהשארתן גלויות.
8. **שקיפות ארגונית.** פרסום מתאים על כך שגורמים פנימיים פנו לארגונים מסוימים עשוי להגביר את הערנות.
9. **נקודות התערבות.** בחינה נוספת של המעברים בין ההתנהגויות עשויה לעזור לארגונים לזהות נקודות שבהן אפשר להתערב לפני שנגרם נזק.

האינדיקציות השכיחות במקרים שנבדקו

- מסירת הצהרות או דיווחים כוזבים: **77**
- שימוש לרעה במערכות הארגון: **20**
- הסתרת ניגוד עניינים: **10**
- נסיעות לחו"ל: **9**
- תקשורת הנוגעת לפעילות ההונאה: **50**
- גישה בלתי מורשית למידע ולמערכות: **15**
- מכירת מידע או נכסים: **9**
- התנהגות בעייתית במקום העבודה: **9**

מספר מופעים ולא מספר עובדים. אותה התנהגות יכולה להופיע כמה פעמים באותו מקרה.[1]

הסייג

לדברי החוקרים, ההמלצות נגזרות מדפוסים שזוהו בדיעבד, ונדרשת הערכה לפני שניתן לקבוע את יעילותן.[1] המחקר מבוסס על 36 מקרים מארצות הברית שהתגלו ותועדו בפומבי, והוא אינו מודל חיזוי. קושי כלכלי, נסיעה לחו"ל, קשר עסקי חיצוני או שינוי בהתנהגות אינם כשלעצמם ראיה לכוונה זדונית. כל ניטור או איסוף מידע חייב להיות חוקי ומידתי, לשמור על פרטיות העובדים ולכלול בחינה אנושית של הממצאים.

הסקירה המלאה במוקד הידע: **profcheck.co/he/knowledge/insider-fraud-behavioural-pathways**

מקור

1. Whitty, M.T., Ruddy, C., Keatley, D. & Jamil, H. (2026). Insider threat detection: a socio-technical analysis of behavioural pathways in malicious insider fraud. Journal of Financial Crime, 1-19. CC BY 4.0. doi.org/10.1108/JFC-04-2026-0185