שמירה על סודות הארגון

המציאות העסקית בה אנו חיים מחייבת התמודדות שוטפת של ארגונים וחברות מכל תחומי העיסוק – עם האיום של דליפת סודות מסחריים או מידע רגיש אחר לידי גורמים לא מוסמכים. ה"אויב" יכול להיות חברה מתחרה, משרדי חקירות, עובד ממורמר ועוד. כדי להבטיח התמודדות ברמה הבסיסית עם האיום של דליפת מידע או הגעתו אל גורם לא מוסמך חשוב להקפיד על מספר כללי יסוד, כולם תחת מסגרת אחריותו של מנהל הבטחון/הקב"ט. במאמר זה אמנה מספר נקודות חשובות וחיוניות למטרה זו.

מאת: רונן ביהם*

מיון הולם של מועמדים לעבודה: בעת פרסום מודעת "דרושים", בעיקר לתפקידים רגישים, מומלץ שלא לציין את שם החברה ולא לצרף את הלוגו שלה. ציון שם החברה עשוי להוות פתח לחברות המתחרות - להשתלת חפרפרת בארגון. בעת ראיון המועמד לעבודה יש להתייחס בין היתר למקומות עבודה קודמים, תקופות ההעסקה בהם על פי סדר כרונולוגי ולוודא רצף תעסוקתי , כמו כן לברר עם המועמד מה הייתה הסיבה להפסקת עבודתו בכל מקום עבודה כזה. יש להתייחס לבני משפחתו של הנבדק ומקומות התעסוקה שלהם - כדי לוודא שאין ניגודי עניינים (עבודה בחברות מתחרות וכו'). חשוב שכל מועמד לעבודה ירואיין במסגרת הליך הקליטה שלו גם ע"י נציג של מחלקת הבטחון אשר גם יחתים אותו על הצהרה לשמירה על סודיות, כמו כן בתפקידים המצריכים מידה רבה של מהימנות ויושר אישי כגון עיסוק בכספים, סחורות, תהליכי יצור וגישה למידע רגיש - מומלץ לבצע למועמדים בדיקת פוליגרף טרום תעסוקתית.

טיפול באורחים ומבקרים: יש לבנות הליך מסודר שבו כל אורח/מבקר נרשם ומוכנס אל משרדי או חצרי החברה רק לאחר וידוי מול הגורם שהזמין אותו או שאליו הגיע, שאכן הוא רשאי להיכנס לתחומי העסק.

יש למסד רישום מסודר של האורחים והמבקרים, תיוג בתג אורח והשארת תעודה מזהה בכניסה.

יש לוודא ליווי של האורחים והמבקרים ופיקוח עליהם בכל משך שהייתם בתחום הארגון או החברה - ולא לאפשר להם להסתובב ללא פיקוח או להימצא במקומות שאינם אמורים להגיע אליהם. אזורים רגישים חייבים להיות ממודרים ורצוי מבודדים ע"י דלת ובקר כניסה.

נעילת משרדים ובקרות כניסה: יש להנחות את העובדים להקפדה בנושא נעילת דלת המשרד בכל יציאה וכן שלא להשאיר מסמכים רגישים על השולחן אלא לנעול אותם בארון או בכספת .

מומלץ להתקין בקרות כניסה בכניסות למבנים/למחלקות באופן שלא יאפשר כניסה או הסתובבות של אנשים לא מורשים. ההתייחסות לנוכחות או הסתובבות של אדם לא מוכר או שאינו שייך למקום - ודיווח בזמן אמת למחלקת הבטחון תוך שמירה על קשר עין עם אותו אדם.

גריסת פסולת הנייר: פחי האשפה משמשים מקור זמין למידע עסקי לכל סוחר מידע ולכל מתחרה וכל חוקר פרטי מתחיל יודע לגשת ולנבור בהם. יש לבחון נושא הטיפול בפסולת הנייר בארגון ולמסד נוהל גריסת כל פסולת הנייר. ניתן לבצע זאת באמצעות

גריסה מקומית משרדית/ מחלקתית עם מגרסות, או באמצעות התקשרות עם חברה חיצונית לביצוע גריסת הנייר. בעת התקשרות עם חברה חיצונית לנושא יש לתת את הדעת לכך ששירות של איסוף של נייר למיחזור אינו שירות של גריסת נייר ואינו מספיק בהיבט של אבטחת מידע. ישנן רמות שונות של התקשרות לעניין זה וכמובן שהעלויות הן בהתאם. במקומות מסוימים מחליטים להסתפק באיסוף שקי נייר לגריסה - השקים נאספים ע"י רכב של חברת הגריסה ונגרסים באתר שלה, ובמקומות אחרים מעדיפים ללכת על הפתרון הטוב המומלץ והיקר יותר - של גריסה באמצעות רכב מגרסה ניידת אשר מגיע בתיאום מראש ומבצע גריסה באתר הלקוח תחת פיקוח נציג מחלקת הבטחון. יש לתת את הדעת גם לתחנות שטיפת הרכבים - ישנם ארגונים בהם עובדים שיש ברשותם רכב חברה נהנים מהסדר שטיפת הרכב בתחנות שטיפה קבועות. גם פחי האשפה בתחנות השטיפה הנ"ל עשויים להיות יעד לסוחרי מידע.

פיקוח על עובדי קבלן: עובדי הנקיון ואחרים הנמצאים במקרים רבים גם בזמנים שבהם אין כמעט פעילות בארגון ובמשרדיו עשויים לשמש אם בידיעתם ואם שלא בידיעתם כצינור להוצאה של מידע מהארגון.

כשם שכל מועמד לעבודה אמור לעבור ראיון של נציג מחלקת הבטחון, חשוב לא פחות כי עובדי הנקיון יעברו ראיונות דומים. מומלץ לוודא גיבוש צוות קבוע המאושר ע"י נציג מחלקת הבטחון ולא לאפשר הצבת עובד מחליף או חדש אשר לא עבר ראיון קב"ט. גם במקרה של עובדי נקיון, מומלץ לשקול ביצוע בדיקות פוליגרף תקופתיות לצמצום האפשרות של הוצאת מידע או מסמכים מהארגון . כאשר מדובר על משרדים רגישים כגון הנהלה/ שיווק/כספים - מומלץ לבצע את עבודות הקבלן בזמן שהעובדים נמצאים בחדרים ולא בזמנים שאינם זמני פעילות. לפני מספר שנים פורסמה בתקשורת פרשת הפעלה של עובדת נקיון באחת מחברות הסלולר ע"י בנה החוקר הפרטי - להוצאת מידע ומסמכים ממשרדי החברה. משרדנו טיפל בעבר בחקירה מורכבת שבמהלכה התברר כי עובדת נקיון אשר הועסקה בלשכת מנכ"ל בחברה גדולה שימשה בלא ידיעתה כצינור להוצאה של מידע מהחברה. העובדת המדוברת נהגה לנסוע הביתה באוטובוס בסיום כל יום עבודה ובאחת מהנסיעות פנתה אליה בחורה צעירה שטענה כי למדה עם ביתה בתיכון והיא כיום סטודנטית לשיווק כביכול ושאלה את העובדת היכן היא עובדת. לאחר מספר נסיעות משותפות באוטובוס - ה"סטודנטית" אמרה לעובדת הנקיון כי היא עושה עבודה באוניברסיטה בתחום השיווק וקיבלה לדבריה כנושא לעבודת הגמר את התחום שבו פועלת החברה בה עובדת הנקיון מועסקת. היא שאלה את עובדת הנקיון אם תוכל להביא לה ניירת מפחי האשפה של החברה כביכול כדי לסייע לה בעבודה שאותה עליה להגיש ועובדת הנקיון אשר "שמחה לעזור" הביאה לה מסמכים שמצאה בפחי האשפה של חדרי ההנהלה של החברה. בחקירתנו התברר כי אותה "סטודנטית" פעלה עבור משרד חקירות - אשר נשכר כדי להוציא מידע עסקי מהחברה.

נהלי בטחון מידע: מומלץ לגבש נהלים והנחיות בנושא בטחון מידע/ מחשבים. האמור כולל גיבוש מדיניות בנושא רשתות חברתיות והגישה אליהן ממחשבי החברה, גיבוש מדיניות בנושא גישה לאינטרנט ולתיבות דוא"ל פרטיות ממחשבי הארגון, ניתוק שקעי USB ואיסור על חיבור התקנים נתיקים אל מחשבי החברה, וידוא קיום סיסמאות משתמש אישיות והחלפה תקופתית שלהן - וכמובן איסור רישום הסיסמה על פתקים המודבקים על גבי צג המחשב - הדרכת עובדים לגבי איסור פתיחת הודעות דוא"ל המגיעות מגורם לא מוכר, הדרכת עובדים לגבי איסור שליחת מכתבי שרשרת/בקשות לעזרה רפואית או תרומות, הדרכת עובדים לגבי איסור התקנת תוכנות פרטיות על מחשבי הארגון.

טיפול בעובדים המסיימים תפקיד: עובד ממורמר או מנהל שעוזב לטובת עבודה בחברה מתחרה יכולים להסב נזק גדול ומשמעותי לארגון. יש לתת על כך את הדעת ולוודא קיום ראיון מסודר במהלכו יתוזכר אותו עובד אשר לחובת הסודיות שלו לארגון ולהצהרת השמירה על סודיות שעליה הוא חתום. יש לבצע במקביל הגבלת הגישה של אותו עובד מרגע שידוע על כך שהוא עומד לסיים את תפקידו - לכל מידע רגיש או חיוני של הארגון. האמור מתייחס לביטול הרשאות הגישה שלו למאגרי הנתונים, הגבלות גישה פיסית שלו למקומות מסווגים ושלילת הרשאות שלו במערכות בקרת הכניסה, הגבלת האפשרות שלו להתחברות מהמחשב הארגוני שלו לאינטרנט ולתיבות דוא"ל פרטיות גם אם הייתה לו אפשרות כזו בעבר ושלילת האפשרות - אם הייתה לו כזו - להתחברות מרחוק למחשב/שרתהארגון (לצמצום האפשרות לשליחת או העתקת קבצים וחומרים השייכים לארגון), כמו כן, יש לבצע ניטרול שקעי USB וכן ביטול אפשרות חיבור התקנים נתיקים למחשב הארגוני. עם עזיבתו יש לוודא קבלת כל ציוד השייך לחברה אשר היה ברשותו לרבות מפתחות, כרטיסים, מחשב נייד, סמרטפון, התקנים נתיקים וכו'.

הדרכות עובדים והגברת מודעות: מומלץ לקיים הדרכות תקופתית לעובדים ולחדד את חשיבות ההקפדה על כל הכללים החיוניים לנושא אבטחת מידע - מסמכים ושמירה על סודות הארגון.

ההדרכה תכלול דגשים והנחיות בנושא מודעות עובדים לאנשים זרים או לא מוכרים המסתובבים בחברה, חשיבות ליווי ופיקוח על אורחים ומבקרים, חשיבות גריסת פסולת הנייר ואי השלכה לפחי האשפה, נעילת משרדים ונעילת מסמכים רגישים בארונות נעולים, הדרכת בעלי רכב חברה להקפדה שלא להשליך פסולת נייר מהרכבים בתחנות השטיפה החיצוניות הידועות כמקור לנבירה של גורמים מתחרים איסור השארת מסמכים וחומר רגיש אחר ברכבים, הקפדה על כללי זהירות - מחשוב ועוד.

*נכתב על ידי **רונן ביהם**, מנכ"ל ובעלים של החברות - ביהם רונן חקירות ייעוץ בטחוני ופוליגרף בע"מ וביהם רונן חברה לחקירות, הפועלות במשולב ומספקות שירותי קב"ט וניהול בטחון במיקור חוץ, שירותי חקירות פרטיות ושירותי פוליגרף. ניתן להפנות שאלות לכותב בדוא"ל: Ronen@911pi.co.il