גיליון מספר 10
ספטמבר 2019

עיונים בביקורת הפנימית

תוכן עניינים

עורכת כתב העת — **שרון ויטקובסקי טביב**, רו״ח, CIA, CRMA

סגן העורכת — **אורן שחר**, רו״ח, MBA, CISA, CIA

חברי המערכת — **דוד אגרנט**, CIA, רו״ח

איל אורון, עו״ד

שלומית איתן, עו״ד, CIA

יוסי אליאס, רו״ח

דרור בר משה, רו״ח, LLM, CIA, CISA, CRMA, CRISC

ננסי זכאכ אבו אלנסר, רו"ח, MA, QAR

נאוה חלמיש, רו״ח, MA

ד״ר יוסי נטוביץ, רו״ח

ליאור סגל, רו״ח, עו״ד, MBA

ד״ר גבי סייג, D.E.A

בועז ענר, רו״ח, MA, CIA

דורון רונן, רו״ח, CIA, CRMA, QAR, CRISC, CFE, MA, LLM

רונית שוורץ, MBA

מרגלית שפרבר, רו״ח, MBA, CIA

מנהלת לשכת נשיא האיגוד — **אינה גולדרביטר**

עיצוב ועריכה גרפית — **סטודיו דגה**

עריכה לשונית והגהה — **אודי לוינגר**

מו״ל — **IIA ישראל - איגוד מבקרים פנימיים בישראל בע״מ**

IIA ישראל - איגוד מבקרים פנימיים בישראל בע״מ

כתובת למשלוח דואר **ת.ד. 29281 תל אביב 61292**

טל **03-5116617** | פקס **03-5116647** | לתגובות והערות **theiiaisrael@gmail.com**

דבר הנשיא

דורון כהן, רו"ח
נשיא IIA ישראל - איגוד המבקרים הפנימיים

בדברי הפתיחה לכנס המשותף שערך לאחרונה האיגוד יחד עם איגוד מבקרי מערכות המידע ISACA, עמדתי על ההיבטים המשתנים בעולם הביקורת ובהם הטכנולוגיה. המבקר הפנימי אינו יכול לטמון את ראשו בחול ולהתעלם ממנה, הוא חייב להתעדכן בשינויים הטכנולוגיים ולהבין את האיומים וההזדמנויות שטומנת הטכנולוגיה לגבי הסביבה הכללית ועל הארגון הוא משרת. על ארגון הביקורת להיות בעל יכולת להעריך את מסגרת הבקרה של הארגון ואת הבקרות הטכנולוגיות כדי לסייע בשיפורם ולהוסיף ערך. נוסף על כך, בעולם שבו יש "לעשות יותר בפחות" אין למבקר הפנימי ברירה אלא לרתום את הטכנולוגיה לשיפור תהליכי הביקורת הפנימית ולייעולם.

גיליון זה, כמו הכנס המוצלח מאוד שהוזכר לעיל, נועדו להגביר את המודעות של המבקרים הפנימיים לאתגרי הטכנולוגיה ולתת בידם כלים פרקטיים לשיפור מיומנותם בנושא. אני מברך על שיתוף הפעולה המוצלח עם ISACA , מאות משתתפים מילאו את אולמות הכנס עד אפס מקום ונהנו מהרצאות מקצועיות מרתקות ומהזדמנות להכיר עמיתים מהדיסציפלינה המקבילה. מה שתואם את הצורך בביקורות אינטגרטיביות הבוחנות את התהליכים העסקיים ואת מערכות המידע במקביל.

אני מבקש לקדם בברכה ולאחל הצלחה למבקר המדינה הנכנס רו"ח מתניהו אנגלמן ולמנכ"ל משרדו, חברנו אל"מ (מיל') ישי וקנין. בכנס נפרדנו ממבקר המדינה היוצא, כבוד השופט יוסף צבי שפירא, המסיים את תפקידו והודינו לו על פועלו. אנו מודים למבקר המדינה היוצא על פועלו לחיזוק מעמד המבקרים הפנימיים בכלל ועל תרומתו לאיחוד ארגוני המבקרים הפנימיים בפרט. המבקר הטיל את המשימה על מנכ"ל משרדו, מר אלי מרזל, שניצח על מלאכת האיחוד והוביל אותה בהצלחה.

איחוד לשכות המבקרים הפנימיים נמצא בהילוך גבוה. אני מעריך כי עד סוף שנה זו נוכל לברך על המוגמר ולהקים לשכה חזקה ומאוחדת המשרתת את כל המבקרים הפנימיים ופועלת בתיאום מלא עם לשכת המבקרים הפנימיים העולמית ובהתאם לתקנים המקצועיים הבינלאומיים.

אסיים בברכת שנה טובה וקריאה מהנה,
דורון כהן

דבר העורכת

שרון ויטקובסקי טביב, רו"ח, CIA, CRMA
סגנית נשיא IIA ישראל - איגוד המבקרים הפנימיים

העידן הדיגיטלי הנוכחי מתאפיין בשילוב מואץ של טכנולוגיות בתהליכים עסקיים הגורמים לשינויים בסיכונים ובאיומים שארגונים נדרשים להיערך אליהם. בהתאמה משתנים גם תהליכי הביקורת, הכלים שבהם משתמש המבקר ומיקוד עבודת הביקורת.

בגיליון הנוכחי נרחיב על ארבעה מוקדים בעלי השפעה על עבודת הביקורת בעידן הדיגיטלי:

סיכון הסייבר: טכנולוגיות חדשניות צצות מדי יום, ועימן חשיפות אבטחה וסיכוני סייבר שעלולים לפגוע בלקוח בודד או למוטט ארגון שלם ואף מדינות. על פי דוח מיפוי האיומים הגדולים בעולם שנערך השנה, מתקפת סייבר היא בין חמשת האיומים הקריטיים ביותר. ככזאת היא חייבת לקבל ביטוי באופן שוטף בתוכנית הביקורת של המבקר.

חדשנות וטכנולוגיה: ענן, מובייל, רשתות חברתיות, יכולות אנליטיות, אינטרנט של הדברים, רובוטיקה ואוטומציה, כל אלה הם הכוחות שמניעים את החדשנות הדיגיטלית. ארגונים נדרשים להיות מודעים לחידושים ולהתפתחויות טכנולוגיות ולשלבם בעסקיהם, ותפקידו של המבקר הוא מצד אחד לנצל את היכולות החדשות, ומאידך להכיר כלים ומתודולוגיות לבדיקת תהליכים המנוהלים בדרכים חדשניות.

יכולות ניתוח אנליטי ותחקור נתונים: ההתבססות על מידע, בכל פעילות, מייצרת יתרון משמעותי למבקר המסוגל לנתחו. הכלים הקיימים היום בשוק מספקים יכולות לבצע ניתוח נתונים ואנליזה המאפשרת הסקת מסקנות ואף זיהוי מגמות עוד בטרם קרות אירוע.

הכשרת המבקר הפנימי בעולם ביקורת מערכות מידע: התהליכים העסקיים מבוססים על מערכות מידע תומכות, והמבקר הפנימי נדרש לבסס את יכולותיו גם באמצעות הפעלת כלי ביקורת טכנולוגיים שיאפשרו לו לבצע ביקורות על המערכות.

העולם שהכרנו משתנה ממש לנגד עינינו, טכנולוגיות מתקדמות ופתרונות מבוססי מערכות מידע הופכים להיות במרכז העולם החדש.

האסטרופיזיקאי הנודע סטיבן הוקינג נהג להביע את עמדותיו על מגוון סוגיות בחיים, ואמר ש"אינטגרציה היא היכולת להסתגל לשינויים". אנו כמבקרים צריכים להיות ערים לשינויים שמתרחשים בעולמנו, ונדרשים להסתגל אליהם ולהביא ערך בעולם המשתנה.

בגיליון הנוכחי שמנו לנו למטרה להרחיב את ארגז הכלים של מבקרים שחפצים להביא ערך לארגונם באמצעות ביקורת פנימית רלוונטית בעידן הדיגיטלי.

בברכת שנה טובה וקריאה מהנה,
שרון ויטקובסקי טביב

דבר העורכת הטכנולוגית

גלית מור, ראש אגף ביקורת מערכות מידע בבנק לאומי
סגנית נשיא ISACA ישראל - איגוד ביקורת מערכות מידע

בעידן המידע בעולמנו הטכנולוגי, תפקיד המבקר הפנימי נעשה מורכב ומאתגר משנה לשנה.

כמעט כל תהליך מבוסס על טכנולוגיה חדשנית, מגוון מידעים, אוטומציה, רובוטיקה ומוצרים טכנולוגיים מתקדמים. כך לדוגמה, תהליך הקנייה בסופר, קבלת המרשם מהרופא, איתור פושע על ידי המשטרה, או העברת כספים בבנק, כולם מבוצעים היום על בסיס מערכות מידע, רובוטיקה אוטומציה או כלים טכנולוגיים מתקדמים, ולכן מחייבים תהליכי בדיקה חדשניים ויצירתיים.

תהליכים פשוטים שנבדקו בעבר על ידי תצפית או תשאול, מבוססים כיום על טכנולוגיה מתקדמת ומחייבים הבנה של העולם החדש, היכרות עם הסיכונים המתפתחים, והיערכות לבדיקות חדשניות באופן אחר.

ממחקר חדש שנערך לרגל 50 שנות פעילות של איגוד ISACA הבינלאומי, בנושא "עתיד ביקורת טכנולוגיית המידע", עלה שקיים גידול משמעותי בהסתמכות על כישורים טכנולוגיים לביקורת (64%).

המחקר מבוסס על תשאול של יותר מ-4,000 מבקרים, ועולה ממנו שב-3-5 השנים הקרובות מתוכננת הסתמכות גוברת על Artificial intelligence ועל 33%) Analytics) לצורך עבודת הביקורת.

כבר כיום ניתן לראות את הסנוניות הראשונות המבטאות יכולות ניתוח של כלל הנתונים בביקורת, בלי להגדיר מראש שאילתה ספציפית. קיימים כלים לניתוח כלל הנתונים וליצירת דשבורדים

ההתקדמות הטכנולוגית והכלים החדשניים אינם מחליפים את המבקר, אלא מאפשרים לו להתמקד בניתוח המידע ואבחון החריגים מתוך כלל האוכלוסייה. חלף התפקיד המסורתי של בחינת תהליכים על בסיס מדגם. מבקר פנימי שישקיע בהיכרות עם עולמות תוכן אלה ויפעל לקידום המודעות לטיפול בהיבטים חדשניים וטכנולוגיים בארגונו, המבוססים על ניתוח מידע, יבטיח שמירה על נכסי הארגון זיהוי סיכונים וחשיפות בזמן, וניצול היכולות החדשניות לצורך עבודת ביקורת איכותית ורלוונטית.

"הדבר היחיד שעומד בינך לבין המטרה שלך הוא הסיפור הזה שאתה ממשיך לספר לעצמך על למה אתה לא יכול לעשות את זה."

(ג'ורדן בלפורט)

תפקידו של המבקר הפנימי הוא לרוץ קדימה עם החדשנות, על סמך ההתקדמות הטכנולוגית, עולמות המידע הפרוסים לפניו, הכלים המתקדמים המשמשים אותו, והסיכונים המתגברים בעולמות הסייבר ובכלל. מי שישכיל לנצל את הכלים והמידע לביצוע ביקורות מתקדמות בתחום, יוכל להשיא ערך ולהוביל לביקורות מקצועיות ומשמעותיות לארגון.

בברכת שנה טובה וחג שמח,

גלית מור

משולחן האיגוד

כנס GRC: ממשל תאגידי, סיכונים וציות - שת"פ של IIA עם ISACA

מהעשה בעולם

אי ציות לתקנות הפרטיות הוא סיכון משמעותי

תקנות הפרטיות הגלובליות יוצרות מורכבות ואתגר עבור ארגונים.

לפי דוח של חברת המחקר העולמית גרטנר לרבעון הראשון של 2019, "דוח מעקב אחר סיכונים מתפתחים", הסיכון של "האצת הרגולציה הפרטית" הוא הסיכון המתפתח ברמה הגבוהה ביותר ועקף את הסיכון "מחסור בכישרונות" .

הסקר העולמי שנערך הצביע על כך שהסיכון באי עמידה בתקנות הפרטיות דורג על ידי 70% מהמשיבים כסיכון גבוה. רשימת המשיבים כללה מבקרים ראשיים, מנהלי ציות, חשבים ומנהלי סיכונים בארבעה מגזרים עיקריים: בנקאות, שירותים פיננסיים, טכנולוגיה וטלמרקטינג, וכן מוצרי מזון ומשקאות.

מר מאט שינקמאן, סגן הנשיא ומנהל סיכונים בגרטנר, מציין כי "עם כניסת תקנות הגנת המידע GDPR לתוקף, המנהלים מבינים כי עמידה וציות לתקנות הפרטיות מורכבת יותר ויקרה יותר ממה שהם צפו מראש". חוק הפרטיות לצרכנים של קליפורניה שייכנס לתוקף ב-2020 רק מוסיף עוד שכבה של מורכבות עבור חברות המתמודדות עם התקנות לפרטיות.

סיכון "האצת הרגולציה בתחום הפרטיות" נתפס גם כסיכון "מהיר ומואץ", שתהיה לו השפעה גבוהה על הארגון אם יתממש. מנהלים רואים בו איום קונקרטי על הארגונים שלהם, ומדרגים אותו כסיכון בעל ההסתברות הגבוהה ביותר להתרחשות מבין עשרת הסיכונים המובילים בדוח.

רוב החששות של מנהלים בנוגע לתקנות הגנת המידע נוגעים לנושא של הכרה רחבה יותר, כי "ארגונים נדרשים לתקן את האסטרטגיה בנוגע לממשל אבטחת המידע בכללותה".

בקנה אחד עם תוצאות "דוח מעקב אחר סיכונים מתפתחים" נמצא בסקר גרטנר לשנת 2019 בנושא סדר עדיפויות בתוכנית פרטיות כי העדיפות העליונה של מנהלי הפרטיות היא הסתגלות לסביבה הרגולטורית התנודתית.

רק ארבעה מתוך עשרה משיבים בטוחים ביכולתם הנוכחית לעמוד בקצב הדרישות החדשות.

קביעת אסטרטגיה לנושא פרטיות לתמיכה בשינוי הדיגיטלי, והטמעת תוכנית ניהול סיכוני צד שלישי בצורה אפקטיבית הן בסדר העדיפויות מס׳ 2 ומס׳ 3 בהתאמה.

חברות הגדילו את השימוש בבינה מלאכותית

כ-20% מהעסקים מקבלים תוספת ערך משמעותי מבינה מלאכותית מתקדמת, ולפי ההערכות, השימוש בטכנולוגיה זו צפויה לגדול פי שלושה עד לשנת 2021. מסקרים שנעשו עולה כי בשנתיים הקרובות הטכנולוגיה הזו תגדיל את ההכנסות, הפריון, הרווחיות והערך המניות עבור העסקים העושים שימוש בבינה מלאכותית.

סקר על תחרותיות בעידן הקוגניטיבי, שנוהל על ידי חברת פרוטיביטי Protiviti בשיתוף פעולה עם חברת המחקר ESI thoughtlab , איגד בתוכו כ-300 בכירים של חברות מכלל הגדלים. כמעט אחד מכל שלושה משיבים לסקר ציינו כי ארגונו מקדים את המתחרים בכל הקשור לשימוש בבינה מלאכותית מתקדמת. בקרב ציבור זה, 92% מצפים לראות ערך גבוה מהבינה המלאכותית ככל שהשימוש בטכנולוגיה זו תתקדם. יותר מ-40% מהמשיבים טוענים כי התחומים המובילים שבהם בינה מלאכותית מייצרת יותר ערך כוללים ניהול סיכונים ותהליכי ציות. 45% טוענים כי בינה מלאכותית מסייעת לשפר תכנון וקבלת החלטות, ו-42% ציינו את שיפור המהירות בהוצאת מוצריהם לשוק (Time to market). שיפורים אלה הם פועל יוצא של השקעות משמעותיות בטכנולוגית הבינה המלאכותית.

הסקר מצא כי חברות השקיעו בממוצע 36 מיליון דולר בבינה מלאכותית במהלך שנת הכספים שעברה, והמשיבים מצפים כי סכום השקעה זה יגדל ב-10% בשנים הקרובות.

באזל מודד את חוסן הסייבר

ועדה שהוקמה על פי דו"ח הפיקוח על הבנקים משווה בין שיטות הפיקוח על הבנקים, הרגולציה ופרקטיקות התאוששות בסייבר. בתחומי סמכותה של הוועדה, מגוון תחומי התמחות בחוסן הסייבר הנובעים מניתוח מענה של רשויות לסקרים קודמים וכן מחילופי מומחים בינלאומיים. הדוח נועד לסייע לבנקים ולמפקחים "לנווט את הסביבה הרגולטורית" וכן לזהות "תחומים בהם נדרש לרתום את הוועדה לבחינה נוספת של המדיניות".

ועדת באזל מסווגת את סקירתה בדבר חוסן הסייבר (התאוששות הסייבר) בארבע קטגוריות עיקריות: ממשל ותרבות, הערכת סיכוני סייבר וניהול, תקשורת וקשרי גומלין עם ספקי שירות חיצוניים. במסגרת תחומים אלה, המחקר מסכם את האתגרים הנוכחיים ואת היוזמות לאורך 10 ממצאי מפתח, המומחשים במקרי בוחן.

בין ממצאי הדוח, מדווחת הוועדה כי רוב המפקחים ממנפים סטנדרטים קיימים בחתירה לחוסן הסייבר, כולל ISO27000 והמכון הלאומי האמריקאי לתקנים ומסגרת טכנולוגית לאבטחת סייבר. בעוד שהדוחות מציינים שיטות פיקוח המכסות תחומים כגון ממשל ובדיקות, נבדלים המפרטים הטכניים ומומחי אבטחת הסייבר בין אזורי שיפוט.

בנוסף, הדוח מצא רמות גבוהות של בשלות בתחומי IT ושיטות ניהול סיכונים תפעוליים, אשר הדגישו כי הבנקים ממנפים שיטות אלה כדי להתמודד עם אבטחת סייבר ולפקח על התאוששות הסייבר. בפרט, הדוח מציין "בעלי סמכות מצפים שלבנקים תהיה אסטרטגיה ומסגרת כדי למפות בצורה מקיפה ולנהל באופן פעיל את ארכיטקטורת מערכות ה-IT שלהם". עדיין, מצא הדוח כי בדרך כלל לבנקים אין אסטרטגיה מאושרת על ידי מועצת המנהלים אשר מגדירה באופן ברור את התיאבון ועמידה לסיכוני הסייבר.

מישהו הזיז את הגבינה שלנו...

כמה פעמים בדקתם תהליך ו.... קפצתם ראש לתוך סכסוך מדמם?!

בוודאי נסכים כי נעים יותר לטפל בתהליכים "סטריליים" מאשר לגעת בעצבים החשופים של יחסים בינאישיים. אבל, בסופו של יום, רבים מהליקויים בארגון נובעים מתקלות ומ"קצרים" בממשקים הבינאישיים.

באמצעות טכנולוגיות חדשות המבוססות על ניתוח מתמטי של רשתות קשרים ארגוניות, ניתן ללמוד על איכות מערכות היחסים והתקשורת הבינאישית "ללא מגע יד אדם".

במדורנו היום אסקור שת"פ עם הסטארט-אפ הישראלי DNA7, לביקורת תהליכים לצד ניתוח רשתות קשרים ארגוניות, ללא התערבות אקטיבית או ישירה של הביקורת במערכות היחסים.

מאת

מרגלית שפרבר | רו"ח, CIA, MBA

מבקרת פנימית ראשית, תנובה

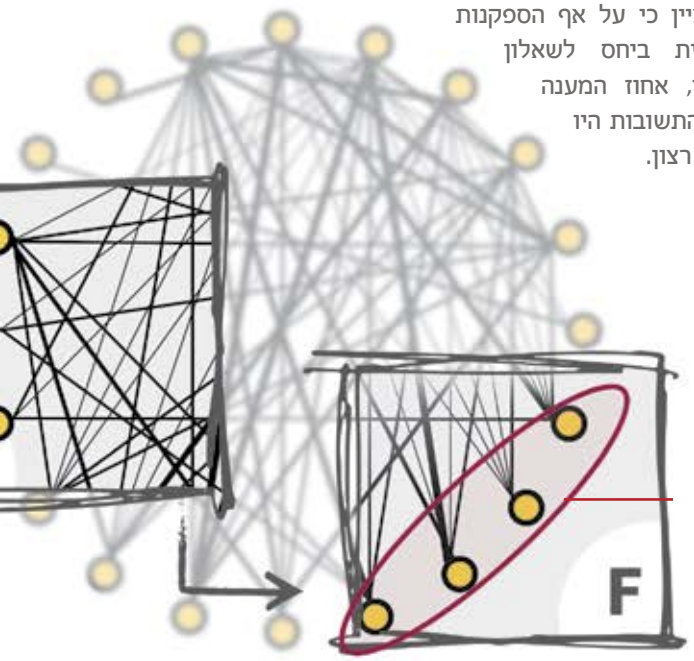
שיטת ביצוע הביקורת

העבודה בוצעה באזור ארגוני מרובה ממשקים המהווה "מרכז עצבים", שיש קושי לנתח את פעילותו ולאתר גורמי שורש. בבדיקה השתתפו כ-300 מנהלים ועובדים (מ"מרכז העצבים" עצמו והממשקים שלו) בשיטת self-assessment . ביצענו שני ניתוחים שונים בשני שלבים:

בשלב הראשון - ביקשנו התייחסותם של המשיבים במלל חופשי- שאלות פתוחות למספר מצומצם של תהליכים העוברים ב"מרכז העצבים" (לדוגמה: הערכות לחגים). רצינו לזהות חשיפות לסיכונים, ליקויים ונושאים לשיפור. את השלב הזה ערכנו באמצעות תוכנת הסקרים הארגונית.

בשלב השני - המשתתפים נתבקשו להשיב לשאלון סלולרי שכלל ארבע שאלות סגורות בנוגע לקשרי הניהול וקשרי העבודה שלהם (מי המנהל שלך? את מי אתה מנהל? עם מי אתה עובד? עם מי אתה רוצה לחזק את ממשקי העבודה? מה הסיבה לכך?). תקשורת פורמלית ולא פורמלית.

ראוי לציין כי על אף הספקנות הראשונית ביחס לשאלון הסלולרי, אחוז המענה ואיכות התשובות היו משביעי רצון.



עיבוד המידע שהתקבל

עיבוד המידע שנאסף בשני השלבים נערך בנפרד. בעיבוד השאלות הפתוחות (השלב הראשון) נדרשה עבודה רבה של ניתוח הערות המשיבים, לאיסוף המגמות והבעיות המהותיות לאורך התהליכים שנבדקו. הממצאים מוקמו על שרטוט של התהליכים, באופן שהבהיר בפשטות ובקלות היכן מצויים הממצאים ה'כבדים'.

התוכנה של DNA7 ניתחה את עוצמת הקשרים שעליהם דיווחו המשיבים (בשלב השני). קשר חזק הוגדר קשר צפוי ע"פ המבנה הארגוני ושני הצדדים דיווחו עליו. קשר חלש הוגדר כקשר חד-צדדי. המערכת איתרה גם קשרים חסרים. כמו כן נערכו ניתוחים לגבי הקשר בין יחידות ארגוניות.

המערכת המירה את הקשרים באמצעות נוסחאות לתופעות שונות המאפיינות רשתות של קשרים חברתיים: מרכזי עוצמה, צווארי בקבוק, סוכני שינוי, חוזק/חוסר שיתוף פעולה, עבודה בסילו, ליקויים בזרימת המידע ובתקשורת. המערכת יצרה מפה ארגונית להנגשת התופעות שנמצאו בשפה גרפית. בסיכום שלב זה הנחנו זו על גבי זו את המטריצה והמפה.

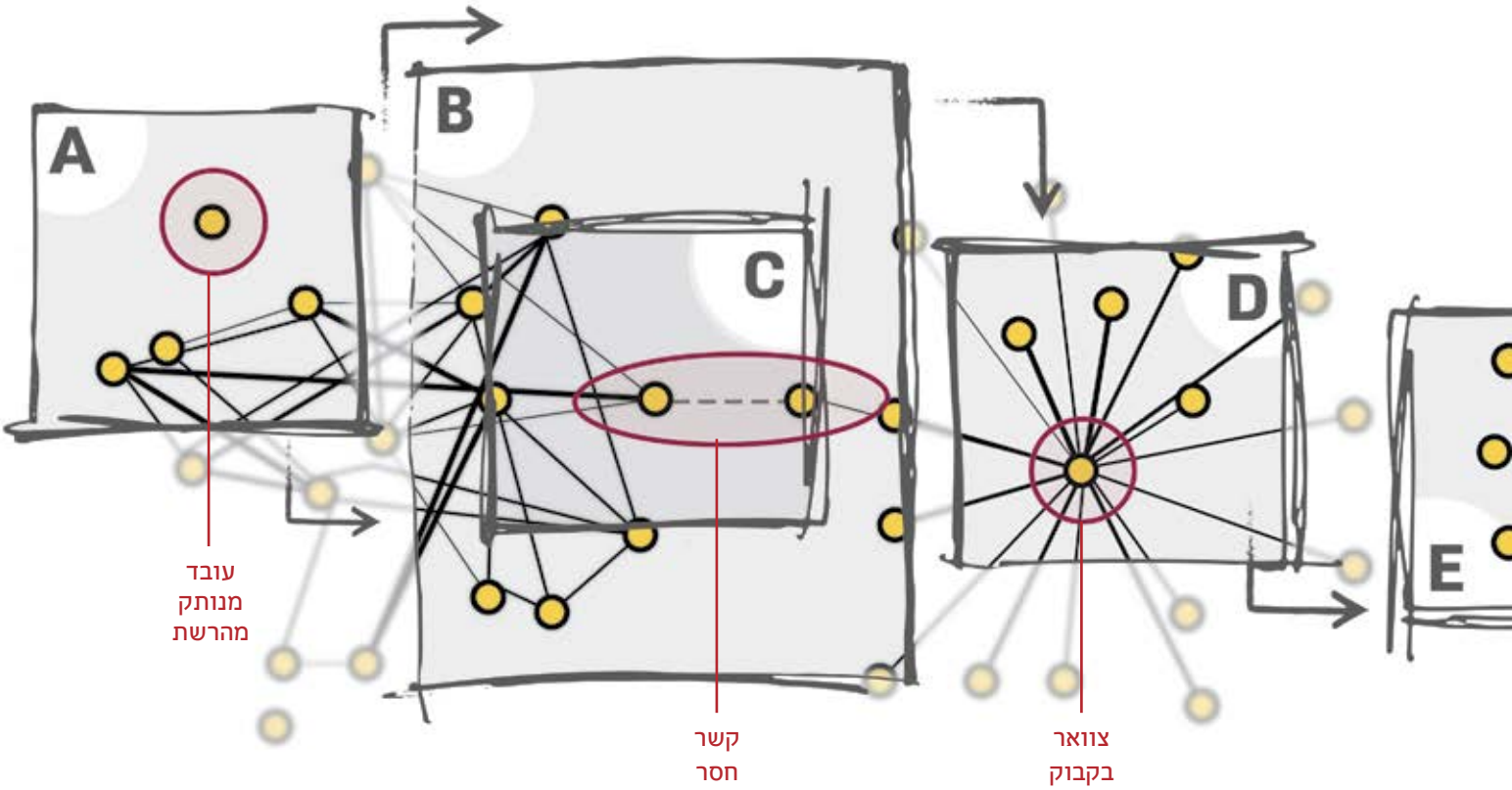
תוצאות הבדיקה

המפה המפה הציפה מגוון רחב של תובנות: עובדים שהם מנהיגים (אף על פי שלא הוגדרו כך במבנה הארגוני) לעומת עובדים מנותקים מהרשת, יחידות עם לכידות פנימית גבוהה לצד יחידות שבהן רמת הלכידות נמוכה, יחידות שעובדות בסילו - ושביניהן רמת קשרים נמוכה אף שנדרש קשר חזק, ועוד ועוד.

המפה עוררה עניין רב ותגובות מגוונות, בעוד שמטריצת התהליכים סיפקה דוגמאות טריות להשלכות וללקויים בתהליכים. החיבור בין המפה והמטריצה הצית דיון סוער בסוגיות של תרבות ארגונית ומשאבים אנושיים, ההשפעה שלהן על התהליכים והמשמעות הכלכלית שלהן. לדוגמה:

- כיצד משפיעה העבודה בסילו על התהליכים שנבחנו?
- יחידות שבהן הלכידות גבוהה או נמוכה וההשפעה על תפקוד היחידה והארגון כולו.
- קשרי עבודה חסרים בין יחידות וההשלכה שלהם על זרימת התהליך.

בסיכומה של העבודה נערכה על ידי ההנהלה והביקורת רשימה של שיפורים נדרשים הן בתהליכים והן בהיבטי המשאב האנושי.



סיכום

התובנה המשמעותית הייתה שמיפוי של רשת קשרים חברתית מספק לארגון תמונת מצב חדה ואף "עיניים חדשות" לראות בהן את המציאות. זהו מיפוי בועט שמעורר דיון סוער ושמשאיר חותם. כל זאת ביחס הפוך בין ההשקעה לבין האימפקט.

סקר התהליכים השלים את ניתוח הרשתות ותיעל את הדיון לשיפור ותיקון, אף על פי או אולי מכיוון שהחיבור בין שני השלבים לעיתים היה שנוי במחלוקת . החקר התנהגותי שימש זרז לתיקון שורשי של תהליכים.

לסיפורנו הפעם סוף עצוב. במהלך 2016 נגמר המימון ו-DNA7 הפסיקה את פעילותה (למעט שלוחה קטנה שנותרה באיטליה). נשארנו עם טעם של עוד ויצאנו לחפש סטארטאפים נוספים שיביאו ערך.

מדור מחקרים אקדמיים

החקר האקדמי של השפעת המהפכה הדיגיטלית וטכנולוגיית המידע על הביקורת הפנימית

מאת

ד"ר גבי סייג | מרצה וחוקר בית הספר למדעי המדינה - אוניברסיטת חיפה, מנהל אקדמי של תוכנית מבקרים פנימיים - היחידה ללימודי המשך, אוניברסיטת חיפה

להתפתחות בתחום טכנולוגיות הבינה המלאכותית ופלטפורמת הבלוקצ'יין יש השפעה משמעותית על הביקורת ועל התחום הפיננסי.

ברמה הגלובלית, מקצוע הביקורת, מוסדות הביקורת והרגולציה, כולם שמים דגש על השפעת טכנולוגיות אלה. ישנם יתרונות ברורים בשימוש בטכנולוגיות להגברת היעילות התפעולית והתובנות. הטכנולוגיה משנה את הדרך שבה העסק מנוהל והנתונים נבדקים. המיקוד הוא על ניהול הנתונים ופחות על הכר את הלקוח שלך. הטכנולוגיות הנ"ל הפכו לגורמים שמשנים את כללי המשחק בתחומי הסקטור הפיננסי והחשבונאי וכמובן במקצוע הביקורת הפנימית. הן משנות את תפקידיהם של המבקרים הפנימיים ושל אלה העוסקים בתחומי ראיית חשבון ופיננסים. הן מאפשרות למבקרים לזהות טוב יותר את המידע הנדרש להם, ולהגדיל את יכולתם לאתר את הסיכונים התפעוליים והפיננסיים המאיימים על הארגון. במקביל הן משפיעות על המיומנויות הנדרשות מהמבקרים בתחומים השונים ובהמשך גם על מדיניות הגיוס של כוח אדם וההכשרה הניתנת להם.

מתוך סקירה של המחקר האקדמי עולה שטכנולוגיית המידע וטכנולוגיות נוספות שמקורן במהפכה הדיגיטלית, משפיעות באופן מובהק על דרכי עבודתם של המבקרים הפנימיים ועל אפקטיביות עבודת הביקורת.

1. השפעת טכנולוגית המידע על הביקורת הפנימית

Krishma Moorthy M., & Al 2011. The Impact of Information Technology on Internal Auditing. .African Journal of Business Management Economic Sciences Series, 5(9): 3523-3539

המחקר דן בהערכת תפקידה של טכנולוגיית המידע (IT) ובדרכים שבהן היא משפיעה על תהליך עבודת הביקורת בארגון. המחקר מדגיש, בין היתר, את המגמה הכללית ההולכת וגוברת של השימוש בטכנולוגיית המידע (תוכנה וחומרה) על מנת לקיים סביבת בקרה מתאימה בעת יישום תהליך הביקורת. המחקר בודק איך טכנולוגיית המידע משפיעה על מערכת הבקרה הפנימית (בקרת הסביבה הארגונית, הערכת הסיכונים, פעילויות הבקרה, מידע ותקשורת וניטור הפעילויות) ומספק קווים מנחים להערכת הטכניקות הזמינות לביצוע באופן יעיל של מטלות הביקורת. המחקר מצביע על השפעת טכנולוגיית המידע על מנגנון הבקרה הפנימית בארגון.

אחת המסקנות החשובות של המחקר היא אחריות המבקר באבטחת ממשל תאגידי יעיל.

המסגרת התיאורטית עליה מתבסס המחקר:

2. השפעת טכנולוגיות המידע על אפקטיביות עבודת הביקורת הפנימית

Akinlete Gideon T., & Olanipekum Comfort. T.2019. Effects of Information Technology (IT) y on Internal Audit in Southwest Nigeria Universities Journal of Economics and Behavioral Studies ,11(1): 22-26

איסוף נתוני המחקר בוצע באמצעות 180 שאלונים שנתקבלו ממדגם מייצג של תשע אוניברסיטאות מתוך אוכלוסייה של 46 אוניברסיטאות הקיימות בדרום מערב מדינת ניגריה. שאלונים אלה שימשו לגזירת ערכי המשתנים המופיעים במשוואה האקונומטרית של מודל המחקר.

המסקנות וההמלצות של עבודת המחקר:

- באוניברסיטאות שנבדקו קיים קשר חיובי ומובהק בין טכנולוגיית המידע ועבודת ביקורת אפקטיבית.

- **הביקורת הפנימית אינה משתמשת במידה הנדרשת בטכנולוגיית המידע לגילוי מעילות והונאות ולהיערכות לשמירה על הרכוש.**

- השימוש של הביקורת החיצונית בטכנולוגיית המידע לא השפיע כנדרש.

- מחברי המחקר המליצו לאוניברסיטאות לקדם ולעודד שימוש מוגבר בטכנולוגיית המידע במחלקות הביקורת הפנימית ולהשתמש בטכנולוגיה זו בפעילות שמטרתה גילוי מעילות והונאות והיערכות לשמירה על הרכוש של הארגון.

3. באיזה מידה טכנולוגיית המידע משפיעה על פונקציית הביקורת הפנימית

Fengchun, T. et al. 2017. Exploring perceptions of Data Analytics in the Internal Audit Function. Behaviour & Information Technology 365(11): 1125-1136

ניתוח ותחקור נתונים מתאר את הגזירה של נתונים מתאימים מתוך ים הנתונים הקיים בארגון, על מנת לענות על שאלות ספציפיות וחשובות. כריית נתונים והטכניקות השייכות ליישומה הן תהליך המשתמש בסטטיסטיקה, מתמטיקה ובינה מלאכותית, שבסופו הארגון יוצר ידע מאוד חשוב למטרותיו העסקיות והאסטרטגיות. המחקרמנסה להבין, בין היתר, איך פונקציית הביקורת משלבת את הניתוח והתחקור של הנתונים בארגז הכלים שלה כדי לשפר את עבודת הביקורת הפנימית המתבצעת בארגון.

שאלות המחקר מובאות להלן:

- לדעת המבקרים הפנימיים הראשיים, איזה סוג של הסמכה ו/או תארים הם חשובים עבור עובדי הביקורת?

- האם המבקר הפנימי הראשי סבור שניתוח ותחקור נתונים (Data Analytics) נמצא בעדיפות בארגון פונקציית הביקורת הפנימית?

- האם הביקורת הפנימית (א) מבצעת הערכת סיכונים ובהמשך משתמשת בניתוח ותחקור נתונים לביצוע מטלות הביקורת, או (ב) עוסקת תחילה בניתוח ותחקור נתונים ובהמשך קובעת את רמת הסיכון במטלות ביקורת?

- על סמך הפעילות המתבצעת לגבי ניתוח ותחקור נתונים בארגון, איך עובדי הביקורת מקבלים את ההכשרה הנדרשת בתחום זה?

- על סמך הפעילות המתבצעת לגבי ניתוח ותחקור נתונים בארגון, באילו תוכנות וכלי תוכנה משתמשים הכי הרבה במחלקת הביקורת הפנימית כיום?

המחקר השתמש בשיטה של ניתוח מקרה ובטכניקה של ראיונות עם משתתפי המחקר. המחקר כלל שש חברות עסקיות ושש חברות לא עסקיות והדגש היה על ראיונות שנוהלו עם המבקרים הפנימיים הראשיים של אותן חברות.

ממצאי המחקר ממצביעים על כך שהביקוש למיומנויות בטיפול בניתוח ותחקור נתונים על ידי פונקציית הביקורת הפנימית ילך ויגבר בעתיד הקרוב. הצורך בעובדי ביקורת בעלי מיומנויות ויכולות בתחום הניתוח והתחקור של נתונים הוא תוצאה של הציפיות לשימוש מוגבר ב-Data Analytics, כדי לתמוך במטלות הביקורת ולסייע בהערכת הסיכונים ובמשימות נוספות של המבקר הפנימי. ממצאים אלה עולים בקנה אחד עם ממצאיו של Bond's (2014) שטען:

אחד השימושים החשובים של Data Analytics עבור הביקורת הפנימית הוא לשפר את יכולתה להעריך ולנהל את הסיכונים וכתוצאה מכך להפוך לגורם המספק תובנות נוספות לארגון.

4. הקשר בין גילוי מעילות והונאות לתחקור וניתוח נתונים

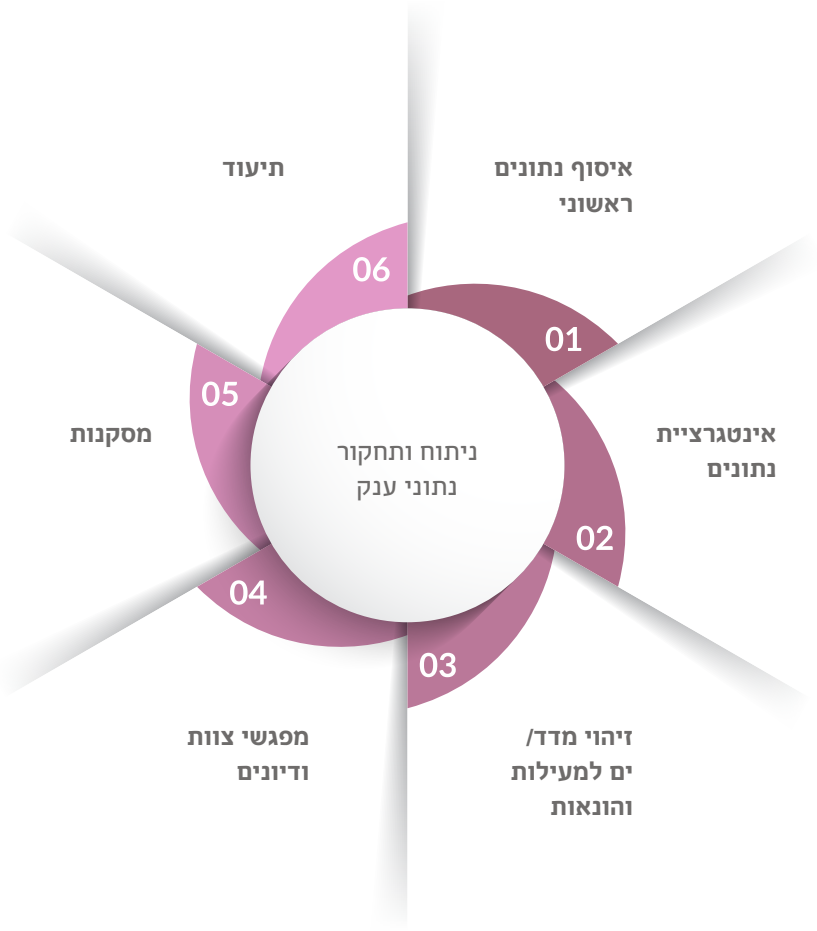
Jiali, T. & Khondar, E.K. 2019. Financial fraud detection and Big Data Analytics - Implications on auditor's use of fraud brainstorming session. Managerial Auditing Journal 34 (3): 324-337

מסקנת המחקר:

שילוב של ניתוח ותחקור נתוני ענק (Big Data Analytics) יחד עם מפגשי סיעור מוחות בעקבות ניתוח הנתונים מהווה פתרון לשיפור הביצועים:

המודל המוצע של המחקר כולל שישה שלבים שיישומם מאפשר לשפר את היכולת של המבקרים לעקוב ולגלות מעילות והונאות בארגון.

השלבים השונים של המודל ויישומם מוצגים בתרשים להלן:



להלן תמצים השלבים:

- תהליך סיעור מוחות מתחיל באיסוף ראשוני של נתונים המסייע לגזור מדדים פוטנציאליים למעילות והונאות שישמשו את המשתתפים במפגשים.
- המידע שנאסף בשלב הראשון מעובד במטרה לשלב ולאחד את כל המידע בעת הצגתו.
- על סמך מידע מאורגן זה ניתן לבצע עבודת ניתוח במטרה לזהות גורמי סיכון פוטנציאליים.
- עכשיו צוות הביקורת יכול לתאם מפגשי סיעור מוחות שבהם ניתן לדון בגורמי הסיכון שזוהו וליצור חשיבה ואתגרים בקרב חברי הצוות.
- רעיונות המועלים והמוצעים במהלך מפגשי סיעור מוחות מוערכים ומסוכמים.
- סיום התהליך: תיעוד של התכנים והתוצאות של מפגשי סיעור מוחות. תוצאות אלה מהוות את התוצר החשוב ביותר בתהליך.

מרחב הסייבר

אחד הסיכונים הצומחים והמשמעותיים ביותר

מאת

רפאל פרנקו | ראש מכלול עמידות, מערך הסייבר הלאומי

במרחב הסייבר מתרחשים כיום במהירות וביעילות דברים שרק לפני שנים ספורות היו חלק מסרטי מדע בדיוני. רובוטים, רחפנים, בינה מלאכותית ושלל טכנולוגיות נמצאות בליבה של המהפכה התעשייתית הרביעית. לצד ההזדמנויות הרבות הטמונות בטכנולוגיה, מרחב זה מציב יריעת איומים רחבה.

על פי דוח מיפוי האיומים הגדולים על העולם, שנערך השנה על ידי הפורום הכלכלי העולמי, מתקפת סייבר היא בין חמשת האיומים הקריטיים ביותר.

תחכומם ויכולותיהם של היריבים, ומאמצי הפגיעה במרחב העולמי בכלל והישראלי בפרט, משתנים בתדירות תכופה.

היריבים משנים את דרכי התקיפה ומתאימים אותן למטרות ייעודיות. בנוסף התוקפים עושים שימוש בכלים וביכולות מסחריות. לכן לא פלא שתעשיית הפשיעה בסייבר עקפה בהיקפה את תעשיית הסמים, ועל פי הערכות שוק הפשיעה ונזקי הסייבר מגלגל מעל 1.5 טריליון דולר בשנה.

מה בין הגנה על ארגון להגנה על מדינה?

כדי לגבש אסטרטגיית הגנת סייבר למדינה יש לשאול מספר שאלות יסוד: על מה רוצים להגן? מה חשוב למשק הישראלי? מה חשוב לאזרחי ישראל במרחב הסייבר והפרטיות? שאלת מפתח בסיסית נוספת היא קיומם או היעדרם של כשלי שוק שמותירים את הסיכון ברמה גבוהה מהמקובל.

ככלל, ארגונים נוטים לנהל את הסיכונים שלהם בכוחות עצמם.

לעיתים פערים בזמינות של ידע או מומחיות ייחודית חסרה עלולה להשליך על רמת ניהול הסיכון והאופן שלו.

בנוסף, ישנם סיכונים ששייכים לקטגוריה שבה "גורם אחר משלם על הנזקים שהארגון מייצר". תופעה זו נקראת בכלכלה "החצנה שלילית". לדוגמה, כאשר ספק תוכנה בעל רמת הגנה נמוכה בסייבר מספק שירות למאות לקוחות רגישים וחיוניים למשק, אם ספק התוכנה הזה לא פיתח את המוצר שלו בהתאם לכללי פיתוח מאובטח, גופים רבים וחיוניים עשויים להיות חשופים למתקפות סייבר רבות. זהו רק אחד מהתרחישים הנפוצים המכונים "התקפות דרך שרשרת האספקה".

כשל שוק נוסף שעימו מתמודדים גם בתחום הסייבר הוא מסוג "מוצר צריכה ציבורי". אנשים או ארגונים אינם מעוניינים לשלם על מוצר או שירות מאחר שלא משתלם להם "להקים אותו לבד". כשם שלא הגיוני שאזרח יסלול לעצמו כביש, ידאג לפינוי האשפה ברחוב או יקים מערכת חינוך - גם בעולם הסייבר נדרש לפעול לעיתים לאיגום משאבים לטובת התייעלות. אם את בית התוכנה מהדוגמה שלעיל יבדקו עשרים לקוחות שונים במשק מדי שנה, הרי שייצרנו בזבוז משאבים בראיית הכלכלה המשקית. נטייה זו מעודדת את תופעת "הטרמפיסט", שבה גופים סומכים על כך שמישהו אחר יבצע את העבודה במקומם.

ראייה רוחבית של כשלי שוק ושל השלכות חוצות משק דורשות מבט אינטגרטיבי/משולב מלמעלה, מבט מדינתי.

מענה לאומי לאתגרים אלו יביא למזעור כשלי שוק ויגביר את התחרותיות במשק ואת צריכת שירותי הסייבר, וזאת לצד תעדוף האתגרים והסיכונים בראייה כלל משקית.

כיצד המדינה מסייעת למשק להעלות את החוסן ולפתור בעיות וכשלי שוק?

המטרה המרכזית של מערך הסייבר הלאומי היא יצירת סביבה מוגנת המקשה על פעילות התקפית של יריבים במרחב הסייבר הישראלי האזרחי.

בהקבלה לעולם הרפואה, רמת עמידות גבוה משולה לרמת היגיינה טובה ואורח חיים בריא המונעים את מרבית המחלות.

במשק הישראלי פועלים ארגונים בעלי אופי וצרכים שונים: תשתיות קריטיות שמספקות שירותים חיוניים וקיומיים לאזרחי המדינה; ארגונים המספקים שירותים חיוניים למשק הישראלי ולציבור הרחב; וחברות פרטיות וארגונים פרטיים המספקים שירותים מגוונים למשק האזרחי. לכך מתווסף הציבור הרחב שגם לו יש תפקיד חשוב ברמת העמידות.

פעילות העמידות מבקשת להבטיח, ככל שניתן ובהתאם לרמת האיום והסיכון, את הרציפות התפקודית של המשק מול איומי סייבר ומתקפות סייבר.

הגנה מידתית - לתפור חליפת הגנה בהתאם לפוטנציאל הנזק המדינתי:

בניתוח הסיכונים על המשק הישראלי נקבעו תשעה תבחיני נזק וחמש רמות אפשריות של פגיעה המשמשות מצפן לפעולות ההגנה על המשק הישראלי.

בין התבחינים שנקבעו: אובדן חיי אדם כתוצאה מתקיפת סייבר, פגיעה בכספי הציבור (כלכלי), פגיעה בשירותים חיוניים לאזרחי המדינה, פגיעה בנכסי מידע חיוניים ועוד. בנוסף, המשק מאופיין ב-18 מגזרים שלהם מאסדרים ממשלתיים.

בכל אחת מהמאסדרים הוקמה יחידת סייבר מגזרית שתפקידה לפעול להעלאת העמידות והרציפות המשקית המגזרית. מתוך כלל המגזרים הוגדרו בראייה לאומית חמישה מגזרים בעלי פוטנציאל נזק מרבי למשק.

- **מגזרים אלו נדרשים למנוע את סיכוני הסייבר הבאים:**
- **מגזר האנרגיה**
  פוטנציאל לפגיעה ברציפות האנרגטית של מדינת ישראל.
- **המגזר הפיננסי**
  פוטנציאל לפגיעה ברציפות הפיננסית של המשק.
- **מגזר התחבורה**
  פוטנציאל לפגיעה בתחבורה הימית, היבשתית והאווירית.
- **מגזר הבריאות.**
- **מגזר התקשורת.**

ניתוח הסיכונים והגדרת "רמת סיכון בראייה לאומית", מאפשרים למערך הסייבר הלאומי למקד את המאמצים בבניין הכוח ובהפעלת הכוחות הלאומיים.

התפיסה האסטרטגית לעמידות בישראל שמה דגש על חיזוק המרחב הישראלי במגוון דרכים המותאמות לרמת האיום של החברות והארגונים במשק.

הפעילות המרכזית בתחום של בניין הכוח הלאומי היא הדגש על הון אנושי חזק.

מערך הסייבר מפעיל ושותף למגוון רחב של תוכניות לאומיות להכשרה וללימודי סייבר: "מגשימים", "אודיסאה", "מדעני העתיד", חרדים לסייבר, קידום נערות לסייבר, ותוכנית "סיכוי שווה" לנוער ולאנשים בעלי מוגבלויות. קידום ההון האנושי בישראל הוא הבסיס לכלל תהליכי ההגנה על המשק, והמנוע המרכזי ליצירת שירותים ומוצרים למרחב הכלכלי והמובילות של מדינת ישראל בסייבר.

עיצוב מרחב הסייבר הישראלי כמרחב בטוח

מערך הסייבר הלאומי פועל בשיתוף עם מגוון ארגונים, חברות ייעוץ, איגודים מקצועיים, עמותות ומלכ"רים על מנת לאמץ תרבות סייבר.

לשם כך נבנה מכלול כלים משקיים המאפשרים לכל ארגון ואזרח במשק להכיר את הסיכונים ולהבין כיצד על הארגון לבנות הגנה יעילה.

מערכת יוב"ל פותחה במערך הסייבר לשם ניהול כלל סיכוני הסייבר בארגון, והיא כלי מרכזי המאפשר ניהול וניתוח סיכונים לארגון בחתכים שונים ומגוונים. שימוש במערכת מביא למיקוד ולייעול מאמצי ההגנה הארגוניים. המערכת תהיה זמינה בקרוב באתר מערך הסייבר הלאומי ללא תשלום.

המערכת היא תולדה של בניית תורת הגנה לאומית לארגון וניסיון שהצטבר במערך הסייבר בלמידה וניתוח האיומים על המשק הישראלי.

לצד פעולות העלאת מודעות משקית לאיומי סייבר, פועל מכלול עמידות במערך הסייבר באמצעות מגוון רחב של כלי מדיניות הנגזרים מהאיום.

אחת הדרכים היא הכוונת המשק באמצעות מאסדרים מגזריים. כך למשל בתחום הגנה על איכות הסביבה מול איום של "הרעלה המונית ופגיעה בסביבה" כתוצאה מתקיפת סייבר, הקים מערך הסייבר בשיתוף המשרד לאיכות הסביבה "יחידה מגזרית" שפועלת לצמצום משטח התקיפה מסיכוני סייבר במפעלים מזהמים או כאלה בעלי סיכון לבריאות הציבור. היחידה משתלבת בפעילות "העסקית" של המשרד לאיכות הסביבה וקובעת הוראות ותקני סייבר למניעת פגיעה אזרחית.

כיום קיימות כ-18 יחידות מגזריות שהוקמו בשיתוף בין מערך הסייבר למאסדר ומונחות על ידי מרכז המגזרים במערך הסייבר הלאומי.

הנחיה זו כוללת בין היתר הטמעת תורת הגנה ייעודית, היערכות למצבי חירום ומשבר יחד עם המרכז להיערכות לאומית, וכן הכשרות מקצועיות לעובדי היחידה על ידי המרכז להכשרה, מודעות והון אנושי במערך.

רובד נוסף בהגנה הלאומית הוא התשתיות הקריטיות של מדינת ישראל, שפועל באמצעות הנחיה ייעודית וישירה המבוצעת על ידי אגף תשתיות מדינה קריטיות, תוך שימת דגש על השאת ערך חיוני וייחודי לארגונים.

תורת הגנה ייעודית ומסווגת היא רק חלק מסל הכלים והיכולות שמפעיל מערך הסייבר לטובת המשכיות ורציפות תפקודית בסייבר של שירותים חיוניים וקיומיים לאזרחי מדינת ישראל.

במערך הסייבר פועל מכלול נוסף שתפקידו לספק התראה על תקיפה ולסלק תקיפות ברמה הלאומית במקרה הצורך. בנוסף, המערך מפעיל מרכז מבצעי הפועל 24/7 בחיוג מקוצר חינם 119.

עיצוב המרחב מתממש גם באמצעות מגוון רחב של פרויקטים לאומיים כדוגמת

פרויקט הזדהות בטוחה לאומי לכלל אזרחי ישראלי. הפרויקט יאפשר לצרוך שירותים בצורה מאובטחת, ויסייע להקטנת הנטל הכלכלי לצד שיפור רמת השירות הדיגיטלי והגנה על פרטיות האזרחים.

שירותי ענן מקומיים יספקו רמת שירותי IT טובים לצד הגנה גבוהה לארגונים במשק הישראלי ויצמצמו את הנטל הכלכלי באחזקת מערכות.

שדרת התקשורת החדשה G5 תאפשר את קפיצת המדרגה הטכנולוגית ותעניק חוויית שירות דיגיטלית ומאובטחת לכלל צרכני המשק הישראלי.

תעופה אזרחית מוגנת - מדינת ישראל היא החלוצה בהגנת התעופה האזרחית בעולם. אנו רותמים שחקנים עולמיים ממשלתיים ופרטיים להגנה גלובאלית.

בית חולים חכם ומוגן - אנו רואים אתגר ממשי באספקת שירותי בריאות עתידיים. אנו בונים ביחד עם משרד הבריאות ובתי חולים מובילים תפיסת הגנה לשירותי הבריאות העתידיים.

תוכנית גלובאלית להגנה על שרשרת אספקה של ארגונים. התוכנית תעסוק ביכולת לשמר רציפות תפקודית וצמצום משטח התקיפה ברכש של ספקים באמצעות יצירת שותפויות ואמון בין שחקנים מקומיים לשחקנים גלובאליים.

לסיכום

לצד האיומים הרבים המציבים תוקפי הסייבר, ניתן לומר כי מדינת ישראל יחד עם שותפים רבים מחו"ל, בממשל הישראלי ובמשק הפרטי עושים מאמצים רבים על מנת למנוע הצלחה של תקיפות סייבר. רמת המוכנות של מדינת ישראל משתפרת ככל שהטכנולוגיה מתקדמת, אך יש להמשיך במאמצים רבים ונוספים לצמצום משטח התקיפה על המרחב הישראלי, לפעול לחיבורים ושותפויות נוספים בין מערך הסייבר לשוק הפרטי, להרחבת בריתות הגנה בין מדינתיות, ולהטמעת תרבות סייבר אזרחית.

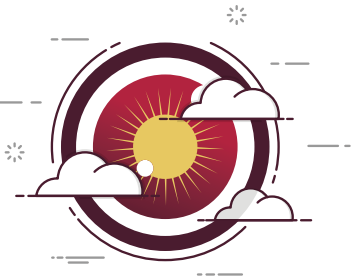
מוכנות הארגון לאירועי סייבר

מאת
דרור בר משה | רו"ח, LLM, CIA, CISA, CFE, CSX - F, CRISC, CRMA - סגן המבקר הפנימי, אמדוקס

מדור טכנולוגיות מידע וסייבר

גיליון זה של כתב העת עוסק בפן הטכנולוגי של עבודת המבקר הפנימי, וכעורך מדור טכנולוגיות מידע וסייבר אני מבקש לחזור על חלק מהדגשים שבהם עסקנו בגיליונות שפורסמו עד כה.

בחירת הנושאים לכתיבה במדור נשענה כמובן על הערכת הסיכון. זו מבוססת בין היתר על פרקטיקות ופרסומים מובילים בעולם, ונושאים אלו יכולים לשמש כחלק מתוכנית ביקורת מקיפה בנושא אבטחת מידע וסייבר.



"הנדסה חברתית" (Social Engineering) היא פעילות מרכזית לחדירה עוינת שבאמצעותה מושגת "דריסת רגל" במערכות וברשתות הארגוניות. מאמצים אלה נעשים למשל באמצעות פישינג (Phishing) - ניסיון להשיג מידע רגיש באמצעות התחזות, בדרך כלל בדואר אלקטרוני; באמצעות Spear Phishing - ניסיון להשיג מידע רגיש מאדם מסוים תוך שימוש במידע פרטי כדי להגביר את הסיכוי להצלחת המתקפה; או באמצעות מתקפות מתוחכמות יותר המכוונות לדרג ההנהלה בארגון ועושות שימוש בהודעות הכוללות נוזקה (Malware). בשנים האחרונות פעילות ההנדסה החברתית של התוקפים עברה לאינטרנט באמצעות אתרים, רשתות חברתיות ואפליקציות להתקנים ניידים (טלפונים חכמים, טאבלטים).

מומחים מסכימים כי הגורם האנושי הוא נקודת תורפה מהותית בניסיונות תקיפה של מערכות ורשתות בהנדסה חברתית. הבנה זו חיונית כדי לספק מידה רצויה של אבטחת מידע. פעולה, התעלמות, חוסר ידיעה או אי ציות של עובדים יכולים להוביל לאירוע אבטחת מידע - למשל על ידי גילוי מידע רגיש (סיסמאות וכדומה) לגורם שאינו מורשה, התעלמות מפעילות חריגה, או שימוש במידע רגיש על ידי עובד שלא לצורך ביצוע תפקידו תוך אי ציות לנהלים.

מודעות עובדים

לתוכנית מודעות והדרכת עובדים יש חשיבות רבה כחלק מאסטרטגיית אבטחת המידע הארגונית, והיא המפתח לטיפול באיומי הנדסה חברתית.

על העובדים להיות מודעים לאיומים הנפוצים, לאחריותם במניעת איומים אלה, לזיהויים ולדיווח עליהם.

דגשים בביקורת פנימית בנושא מודעות עובדים:

- הירתמות של ההנהלה היא חיונית להצלחתה. מומלץ לבחון את מידת המעורבות והאחריות של ההנהלה.
- יש לבדוק את מידת מעורבותם של גורמים מקצועיים בתהליך הבנייה והיישום של תוכנית המודעות וההדרכה.
- יש לבחון כיצד נבנתה התוכנית והאם קיים קשר מובהק למטרות הארגון, לתהליך ניהול הסיכונים, לתהליך ניהול אירועי אבטחת המידע (Incident Management) ולמגמות עולמיות.
- יש לבדוק את אופן תקשור התוכנית לעובדים - האם המסר הרלוונטי הועבר לגורם הרלוונטי? מהם ערוצי התקשורת שנבחרו לשם כך?
- מומלץ לבדוק את אפקטיביות התוכנית להשגת מטרותיה. ניתן לבדוק אפקטיביות באמצעות בדיקות פתע (שיחות טלפון המדמות תקיפה להשגת מידע רגיש, תרגילי התחזות ברשתות חברתיות, שליחת דוא"ל ממקור לא ידוע למייל הפנימי של העובדים כדי לבחון את ערנותם למיילים זדוניים ובדיקה האם יפתחו את הקישורים הללו, וכו'), קביעת יעדים מדידים ובחינת עמידה בהם (למשל הורדת כמות המשתמשים שהקליקו על דואר אלקטרוני זדוני שנשלח אליהם, בחינת כמות הדיווחים על אירוע חריג, וכו'), שימוש בסקרים, סריקת הרשת החיצונית לארגון והפנימית של הארגון כדי לבדוק האם דלף מידע רגיש מהארגון ומאיזה מקור בארגון, ועוד.
- יש לבחון האם פעילות המודעות וההדרכה תוקצבה בצורה מספקת. תקציב זה יכול להיקבע כאחוז מתקציב ההדרכה הכללי, אחוז מתוך תקציב ה-IT הכללי, הקצאה תקציבית לעובד, ועוד.
- יש לבדוק האם מופו קהלי יעד בקרב העובדים ולדרגם על פי סיכון. בהתאם לסיכון יש לתעדף ולהדגיש נושאים ספציפיים (דוגמאות לאוכלוסיות רגישות: אנשי מערכות מידע ורשתות, הנהלה, אנשי כספים, עוזרות אישיות, עובדי קבלן, עובדים חדשים או עובדים ששינו תפקיד בארגון, וכו').
- יש לבדוק האם ניתן דגש להגברת המודעות לדרכי הדיווח של העובדים בנוגע לחשד להתקפה. דיווח מיידי הוא קריטי לעצירת ההתקפה ולהפחתת הנזק.
- נושאי בדיקה נוספים מופיעים בתדריך שפרסם ה-NIST (המכון הלאומי לתקנים וטכנולוגיה בארה"ב). מומלץ לעיין בו בהרחבה.

איום הכופרה

תוכנת כופר או "כופרה" היא נוזקה שמגבילה גישה למערכות המחשב הנגוע, ומשמשת לסחיטת תשלום דמי כופר מהמותקף עבור הסרת מגבלת הגישה. לרוב, תוכנות הכופר מבצעות הצפנה או נעילה של הקבצים תוך שימוש בשיטות הצפנה מורכבות, כך שקשה מאוד להסיר את ההצפנה בלי לשלם כופר עבור מפתח ההצפנה. ישנו סוג נוסף של כופרה, החוסם שימוש במחשב או בהתקן נייד כלשהו.

קיימת נטייה לתקוף את אלה שיש ברשותם חומר רגיש או בעל ערך, מפני שהסיכוי לקבל כסף גבוה יותר.

בדרך כלל התוקפים דורשים תשלום שיבוצע באמצעות מערכת תשלומים שלא ניתנת למעקב (מטבעות דיגיטליים כדוגמת ביטקוין).

דגשים בביקורת פנימית בנושא מתקפות כופרה:

- האם מקפידים על התקנת עדכוני תוכנה (הכוללים עדכוני אבטחת מידע)?
- האם מופרדים רכיבים שאינם יכולים לעבור עדכוני תוכנה לאזורים נפרדים של הרשת הארגונית?
- האם הוכנה תוכנית פעולה למקרה של התקפה? בכלל זה, האם מיפו את המידע הקריטי של הארגון ואת הגישה למידע?
- האם הגנו על נקודות הממשק בין הרשת הארגונית ל"עולם החיצון"? ודאו כי הגדרות ברירת המחדל ברכיבים אלה שונו.
- האם בוצעו תרגילים כדי לוודא שהתוכנית אפקטיבית?
- האם הופעלו כלי "אנטי-ספאם" היעילים בדרך כלל במתקפות כופרה?
- יש לוודא כי הגיבויים תקינים ומתבצעים בצורה שוטפת.
- יש לבדוק סגמנטציה של הרשת הארגונית.

ניהול עדכוני תוכנה (PATCH MANAGEMENT)

את רוב התקפות הכופרה אפשר למנוע! חשוב לחזור לרגע אל היסודות. ניהול עדכוני תוכנה הוא תהליך של וידוא שכל פיסת תוכנה וקושחה (Firmware) שנמצאות בשימוש בחברה מעודכנות בגרסאות הרצויות (בדרך כלל העדכניות ביותר שפורסמו על ידי היצרן) ושכל טלאי האבטחה הרלוונטיים הותקנו. עדכון (ובמונחים המקצועיים "טלאי תוכנה") הוא למעשה תיקון פגיעויות מערכת (תיקוני קוד) המתגלות לאחר שתוכנה או רכיב שוחררו לשוק ודורשות תיקון מיידי. טלאי תוכנה חלים על חלקים שונים של מערכת מידע, בהם מערכות הפעלה, שרתים, נתבים, מחשבים אישיים, אפליקציות שונות (דואר אלקטרוני למשל), מכשירים ניידים, firewalls ורכיבים רבים אחרים הקיימים בתשתית הרשת.

ידוע כי אחד מווקטורי התקיפה הפשוטים ביותר עבור פצחנים המחפשים גישה לרשת הארגונית הוא מערכות שלא עברו עדכון תוכנה. פצחנים וחוקרי אבטחה מגלים כל הזמן פגיעויות חדשות, וחברות תוכנה מפרסמות בתדירות גבוהה עדכונים כדי לטפל בהן. אם עדכונים אלה אינם מוחלים, לפושעי הסייבר יש נקודת כניסה קלה לתוך הרשת הארגונית.

אם רכיב אחד ברשת לא עבר עדכון, הוא עלול לאיים על היציבות של הרשת כולה ואף למנוע את הפונקציונליות הנדרשת.

דגשים בביקורת הפנימית בנושא עדכוני תוכנה:

- שיקול המפתח העיקרי הוא סדר עדיפויות של עדכוני התוכנה. יש ליישם טלאי אבטחה קריטיים בהקדם האפשרי, אך מעבר לכך יש לקחת בחשבון גורמים נוספים. מנהלי IT צריכים לשקול באיזו תכיפות נעשה שימוש בתוכנה וכמה היא קריטית לארגון לפני ההחלטה להחיל עדכון.
- חשוב לוודא כי לפני ההתקנה בסביבת הייצור העדכונים נבדקים כיאות בסביבת המעבדה וכי נעשה גיבוי לתצורתה הנוכחית של המערכת. כמו כן חשוב להכין תוכנית נסיגה מפורטת למקרה של כשל.
- סימן ההיכר של ניהול עדכוני תוכנה יעיל הוא בחירת הזמן הטוב ביותר לתזמן אותם. יש לוודא כי עדכונים מותקנים מחוץ לשעות העבודה כדי למזער את ההפרעה לעובדים ולתהליכים האוטומטיים.
- ניהול עדכוני תוכנה הוא קריטי לפעולות העסקיות, אולם נוטים לחשוב כי תהליך זה הוא באחריות מחלקת ה-IT. קשה ליישם בהצלחה תהליך זה ללא הבנה ותמיכה של ההנהלה הבכירה.
- לבסוף, מנהלי עדכוני תוכנה יכולים לייעץ בנוגע להחלטות רכישה נבונות להשקעה עתידית. במקרה שספק מסוים מנפיק עדכוני תוכנה תכופים, ייתכן שמוצריו מהווים סיכון אבטחה וכי נרצה לבחון אפשרויות חלופיות.

בבואנו לבחון את התהליך, מומלץ לוודא כי הפעולות הבאות מבוצעות:

- האם הארגון יודע מהן הגרסאות המותקנות ומהן הגרסאות הזמינות להתקנה (הגרסאות החדשות ביותר)?
- האם הארגון יודע אילו עדכוני תוכנה מתאימים למערכות שונות?
- האם כל העדכונים מותקנים כראוי?
- האם קיימות בקרות לבדיקת התקנת העדכון לאחר התקנתו?
- האם קיימים נהלים לתיעוד פעולות ההתקנה, כולל קונפיגורציה שיושמה?
- האם מיושמת מערכת אוטומטית לניהול העדכונים? בהיעדר מערכת כזו נוודא האם קיימות בקרות מפצות.
- האם נעשים גיבויים ובדיקת עדכונים טרם ההתקנה על מערכות קריטיות?

מניעת דלף מידע

בעידן שבו המידע נדרש לנוע באופן דינמי בתוך הארגון ומחוצה לו בערוצים רבים ומגוונים, הסיכון שמידע רגיש יזלוג מתוך מערכות הארגון השונות למקורות שאינם מורשים גדל ומתעצם.

מידע רגיש עשוי לכלול מידע רפואי, מידע אישי ומידע עסקי ארגוני, נתוני כרטיסי אשראי, תשלומי לקוחות ועוד.

ישנן אינספור דוגמאות של זליגת מידע רגיש, הן מחברות ענק עוצמתיות והן מארגונים בסדר גודל בינוני, המדגישות את הצורך של כל ארגון לשמור על שלמות, סודיות וזמינות המידע שברשותו בכל זמן נתון. מידע הוא אחד הנכסים החשובים ביותר של כל ארגון, ולכן על הארגון לפעול במיטב האמצעים העומדים לרשותו על מנת למנוע אירועי דלף מידע, בין היתר כדי למזער את הסיכונים לפגיעה במוניטין ואי עמידה בהוראות החוק והרגולציה.

הסיכונים להתרחשות אירוע דלף מידע מושפעים ממספר רב של גורמים שניתן לחלקם לקטגוריות הבאות: גניבת מידע מהארגון על ידי גורם חיצוני, זליגת מידע מהארגון בשוגג, וזליגת מידע מהארגון בזדון - על ידי גורם פנימי. אירוע אבטחת מידע שבו מבוצעת פעולה כגון העתקה, העברה או צפייה במידע רגיש או מסווג ללא הרשאה או בשגגה, מכונה גם הוא אירוע דלף מידע.

על הארגון לענות על שורה של שאלות מהותיות ובהן:

- האם וכיצד הארגון מגדיר מידע רגיש ומהן רמות הרגישות השונות? על הארגון למפות ולהגדיר מהו הסיכון של מידע אישי לסוגיו; מהו הסיכון של מידע עסקי לסוגיו; מהו הסיכון של מידע פיננסי ומסחרי לסוגיו; מהו הסיכון של מידע טכנולוגי, כולל קניין רוחני, וכדומה.
- היכן המידע מאוחסן?
- מהם הערוצים שדרכם המידע עלול לדלוף?
- ולבסוף - כיצד למזער את הנזקים אם וכאשר יתרחש אירוע של דלף מידע?

דגשים ביקורת פנימית בנושא מניעת דלף מידע:

- **מדיניות ונהלים** - האם הוגדרו ומיושמים בארגון מדיניות ונוהלי אבטחת מידע בנושאי סיווג מידע, הפרדת סמכויות, זיהוי עובדים שחשופים למידע רגיש, גילוי וניהול אירועי דלף מידע, הדרכות, החלפת סיסמאות, בקרה שוטפת על הרשאות גישה תוך עדכונים עקב מעבר תפקיד או פרישה, נוהל בנוגע לעובדים העומדים בפני פיטורין, וכן נוהל בדבר אובדן/גניבת סלולרי או מחשב נייד המאפשר גישה.
- **סקר דלף מידע** - מומלץ לבצע סקר דלף מידע מקיף על ידי גורם מומחה חיצוני ובלתי תלוי, במטרה לסקור את כלי אבטחת המידע שבהם הארגון עושה שימוש ולבחון את התאמתם לצורכי האבטחה העסקיים בארגון ושיטת העבודה הנהוגה בו. הסקר יאפשר לזהות את רמת התאימות בין כלי אבטחת המידע השונים ואופן הפעלתם אל מול הסיכונים לדלף מידע.
- **מערך הרשאות** - יש לבחון כיצד מיושם מערך הרשאות וסמכויות במערכות המידע בארגון והאם הוא עומד בעקרון "הצורך לדעת" (Need to Know), תוך הגבלת הגישה למידע לבעלי התפקידים הזקוקים לו בלבד. כמו כן יש לבחון עמידה בעקרון הפרדת התפקידים. בנוסף, יש לבחון אילו בקרות מפצות יושמו על מערך ההרשאות, כגון הפצת דוחות חריגים על פעילות המשתמשים במערכות ובדיקתם.
- **טכנולוגיה** - יש לבחון את הכלים הטכנולוגיים שהוטמעו בארגון לשליטה ומניעת דלף מידע בכל פעילות הארגון. פתרונות DLP - Data Leakage Prevention מאפשרים לשלוט ולהגביל את הוצאת הנתונים בנקודות הקצה בארגון.
- **מודעות עובדים** - יש לבחון האם התוכנית להגברת המודעות של העובדים כוללת הסברה מספקת בנושאי אבטחת המידע הארגוני וחשיבות מניעת דלף המידע.
- **שילוב אבטחת מידע בתהליכי משאבי אנוש** - יש לבחון האם בקרות אבטחת מידע שולבו גם בתהליכי משאבי אנוש, למשל: החתמת עובד חדש על נספח שמירת סודיות והנחיות אבטחת מידע.

סימולציה המדמה תקיפת סייבר יעילה הן לארגון והן לביקורת הפנימית. סימולציית תקיפה מאפשרת למפות את הפערים בין המצוי לרצוי, בין התכנון לביצוע.

בשלב התכנון של התרגיל יש לקבוע מי ישתתף בו, מה התרחיש שייבדק, אילו הזרמות מידע (תת-תרחישים) יימסרו תוך כדי תרגיל ואת סדר האירועים בתרגיל.

מטרות ברורות לתרגיל הן אבן יסוד בביצוע תרגיל משמעותי ואפקטיבי. מטרות מוגדרות היטב מסייעות לתכנון מדויק וריאלי יותר של התרחיש במרחב האיומים.

דוגמאות לתרחישים:

- התקפת פישינג (Phishing/Spear Phishing) על עובד הארגון שבאמצעותה מוחדר וירוס לרשת הארגונית.
- הורדת תוכנה "מודבקת" מהאינטרנט על ידי עובד בארגון.
- התקפת Denial of Service (DoS) - הזרמת תנועה רבה לרשת הארגונית הגורמת לקריסתה.
- גניבה פיזית של מחשב ארגוני והשגת גישה למידע או למערכות.
- חדירה לרשת הארגונית על ידי חיבור פיזי של התקן לא מורשה.

דוגמאות לאירועים ופעולות שיש לתת עליהם את הדעת במהלך סימולציה המדמה התקפת סייבר:

- כוננות לאירוע סייבר (מאפייני מצב שגרה, קיום נהלים עדכניים ורלוונטיים).
- שלבים בזיהוי וחקירת האירוע.
- מתי וכיצד מכריזים על אירוע סייבר/מצב חירום סייבר.
- מתי מאיישים חדרי מצב.
- שלבים לבלימת האירוע.
- תדירות ביצוע הערכות מצב ודיווחים.
- תקשורת לגורמי פנים וחוץ (עובדים, הנהלה, לקוחות, תקשורת, מדיה חברתית וכו').
- מעורבות גופים שונים בארגון, כגון מחלקה משפטית, יחסי ציבור ודוברות, הנהלה וגורמים עסקיים, ושיתוף הפעולה ביניהם.
- שלבים בתהליך הערכת הנזק.
- הפעלת תוכנית המשכיות עסקית והתאוששות מאסון.

חשוב מאוד לתעד

בפירוט את מהלך התרגיל מפני שהתיעוד יעזור בהסקת מסקנות. מומלץ כי המתורגלים יתעדו את האירועים וההחלטות ביומן אירועים, כולל תזמון של כל אירוע, פעולה או החלטה. מרכיב הזמן בתרגיל חשוב מאוד ויכול בהחלט לשחק תפקיד מכריע בהתאוששות מאירוע סייבר.

בנוסף, מומלץ לקיים בסוף התרגיל דיון פתוח בהשתתפות המתורגלים והמתרגלים במטרה לשמוע את דעתם על התרגיל ומסקנות שעלו ממנו. דיון כזה מסייע לזהות הצלחות ונקודות לשיפור.

לסיכום

ביצוע תרגיל סייבר הוא הזדמנות לארגון לשפר את המענה לאיום סייבר או לאשרר את אפקטיביות הבקרות הקיימות. על המשתתפים בתרגיל (המתרגלים, המתורגלים והצופים בו) לעבוד בשיתוף פעולה על מנת להשיג את המרב - שיפור מוכנות הארגון להתקפת סייבר.

השרשרת חזקה כחוזק החוליה החלשה שלה

סיכוני סייבר בשרשרת אספקה

מאת

נועם הנדרוקר |
B.sc במדעי המחשב, MBA
מנהל יחידת ייעוץ סייבר
מרכז הגנת הסייבר של BDO

אם בעבר ארגונים לא נתנו את הדעת לאיומי הסייבר, היום סיכון הסייבר הפך לאחד הסיכונים העיקריים שאיתם מתמודדת הנהלת הארגון. לכן כל ארגון, בלי קשר לגודלו ולפעילותו העסקית, חייב לנהל את סיכון הסייבר ולהשקיע משאבים בהפחתתו.

כמעט מדי יום מפורסמות תקיפות סייבר שהתממשו, והנושא רלוונטי לקשת ארגונים רחבה,

כגון בנקים, רשתות קמעונאות, חברות היי-טק וטכנולוגיה, מוסדות רפואיים, חברות תעופה, חברות תעשייה, וכמובן תשתיות קריטיות מדינתיות.

טייוואן סמיקונדוקטור, החברה הגדולה בעולם לייצור צ׳יפים, חוותה באוגוסט האחרון התקפת סייבר רחבה, והדבר עלול לעכב ייצור מוצרים של חברות ענקיות כגון האייפון של אפל. זוהי רק דוגמה אחת בשורה ארוכה של דיווחים מטרידים מהתקופה האחרונה לגבי מפגעים באבטחת שרשרת האספקה העולמית.

מרחב הסייבר הארגוני שעליו יש להגן השתנה מאוד בשנים האחרונות. בעבר, רשתות ארגוניות היו סגורות וניתן היה לתחום אותן בצורה ברורה. כיום ההגדרה של ה-Perimeter (״הגבול ההיקפי״) הארגוני הולכת ומיטשטשת. חלק מהמערך התפעולי והעסקי נמצא בענן, חלק מהשירותים שהארגון צורך מתקבל במיקור חוץ, הארגון תלוי בספקי משנה שמספקים לו שירותים, והאפשרויות של עבודה מרחוק הולכות ומתרחבות.

נשאלת השאלה האם הקמת מערך סייבר ארגוני מסורתי מספיקה? כיצד מנהלים את הסיכונים באופן מושכל? על מה שמים את הדגש? כיצד נמנעים ממצב של בזבוז ועודף השקעה? איך מבקרים נכון כדי שביום הדין נמשיך לעמוד ולספק שירותים ברמה סבירה?

התשובה כמובן מורכבת ולכל ארגון יש את סדרי העדיפויות שלו, אך הבסיס הוא הבנת הסיכונים המהותיים להמשך הקיום העסקי של הארגון, ומשם יש לגזור את הערכת הסיכון והבקרות המפצות.

דוגמה טובה לכך היא שרשרת האספקה המשרתת את הארגון. סיכוני הסייבר הנובעים מתוך שרשרת האספקה הם רבים ומגוונים, ומערך ההגנה הארגוני חייב לקחת אותם בחשבון ולמצוא דרכים כדי לזהות, להעריך ולטפל בהם.

תקיפות דרך שרשרת האספקה

בעידן שבו התוקפים מחפשים דרכים לפגוע בארגון,

פגיעה בשרשרת האספקה הפכה לשיטה מועדפת במטרה למצוא את הדרך הקלה ביותר להיכנס לארגון.

תוקף יעדיף לכוון את משאביו לשרשרת האספקה, שלרוב אינה בעלת מערך הגנה מקצועי ורחב כמו הארגון שלו היא מספקת שירותים.

במהלך השנתיים האחרונות אנו עדים לעלייה במספר התקיפות שבוצעו דרך ניצול שרשרת האספקה בארגונים שונים. על פי נתוני חברת סימנטק, בשנת 2017 אחוז התקיפות משרשרת האספקה עלו בכ-200% (10 תקיפות גדולות שבוצעו דרך שרשרת האספקה לעומת 4 תקיפות בלבד שבוצעו בשנים 2015-2016).

ככל שלארגון יש יותר ספקים, הסבירות לתקיפה שמגיעה משרשרת האספקה עולה משמעותית.

ניהול סיכוני שרשרת האספקה הארגונית - הלכה למעשה

שלב מיפוי הספקים

לצורך הבנה של סיכוני הסייבר, ראשית עלינו למפות את כלל הספקים בארגון. נדרש להבין מיהם הספקים, אילו שירותים הם מספקים לארגון, מיהם אנשי הקשר בספק, מיהם האנשים בארגון שנמצאים בקשר עם הספק, והאם הספק חתום על הסכם סודיות והנחיות אבטחת מידע של הארגון (אם יש כאלה).

בשלב הבא יש למפות את רשימת הספקים לפי דרגות חשיבות. נדרש לבחון מיהם הספקים המהותיים לארגון ומי לא. ניתן לדרג את רשימת הספקים לפי רמת חשיבות גבוהה, בינונית, נמוכה, או במגוון פרמטרים אחרים כגון ספק קריטי, מהותי/לא מהותי, אסטרטגי וכו׳.

יש לבחון גם האם הספק נוטל חלק מהותי בשירות קריטי של הארגון. כלומר האם ללא השירות הניתן מהספק, הארגון אינו יכול לספק שירות מרכזי ללקוחותיו.

שלב הערכת הסיכונים

לאחר שלב המיפוי נדרש להבין מהם סיכוני הסייבר שאליהם חשוף הארגון מתוך שרשרת האספקה:

- האם הספק מחזיק במידע רגיש של הארגון?
- האם הספק חשוף למידע רגיש של הארגון?
- האם לספק יש גישה מרחוק לרשת הארגון?

כפי שצוין בתחילת המאמר, ספקים מהווים דלת כניסה לתוקפים לתוך הארגון, ולכן נדרש לבחון את רמת ההגנה של הספקים נותני שירות. בשלב הראשון יש לבחון את הספקים שהוגדרו כמהותיים. לאחר מכן ניתן להשלים את התהליך לכל שאר הספקים.

על מנת להבין את מערך הגנת הסייבר של ספקים, נדרש לבחון נושאים כגון בקרת גישה, אבטחה פיזית, הגנה על עמדות קצה ושרתים, רכיבי אבטחת מידע, תחזוקת והקשחות שרתים ומערכות, גישה מרחוק, ניהול וטיפול באירועי אבטחת מידע, גיבויים וכו'.

כל הפרמטרים האלה יעידו על חוזק מערך ההגנה של הספק מפני אירועי סייבר. ככל שהגנה של הספק מפני תקיפות חלשה יותר, כך הסבירות שתוקף יחדור לארגון באמצעות הספק היא גבוהה ויש לטפל בה בהקדם האפשרי.

ניהול סיכוני הסייבר של שרשרת האספקה

ארגון לא יכול להתמודד עם מה שהוא לא יודע, ולכן כדי להתמודד עם הסיכון אנחנו צריכים להבין את הסיכון. אם לא מתבצעת הערכת סיכונים לספקי הארגון, הארגון לא יוכל לדעת מהם הסיכונים שאליהם הוא חשוף ומה עליו לעשות כדי לצמצם את היקף החשיפה.

סקרי סיכונים ושאלונים הם מרכיב מהותי בשלב הערכת הסיכונים. בשלב זה על הארגון לבצע סקר סיכוני סייבר של הספק ולבחון את הנושאים לדוגמה שצוינו לעיל. ארגון יכול לבצע סריקות חיצוניות למשטח התקיפה של הספק ולבחון לאילו חולשות הספק חשוף. באמצעות סריקות אלה ניתן לבחון עד כמה הספק חשוף לתקיפות מבחוץ.

מתוך הסקרים השונים עולים ממצאים. מטרת הסקר היא להציף את הפערים השונים ולהציע דרכים ובקרות להפחתתם. הספק מקבל את הממצאים שעלו מתוך הסקר ומתחייב לתקנם תוך פרק זמן מסוים. הפקת תוכנית עבודה המכילה את הסיכונים, הממצאים וההמלצות הנדרשות היא מרכיב חיוני בתהליך ניהול הסיכונים ומאפשרת כלי מעקב נוח ליישום.

נושא ניהול הממצאים הוא מהותי לארגון. חשוב לעקוב אחר יישום ההמלצות ולוודא כי הספק אכן ביצע את מה שמוטל עליו מתוך תוכנית העבודה. אם הארגון מבצע סקר אצל ספק בשנה מסוימת ורק בסקר הבא (שמתקיים לרוב אחרי שנתיים) הוא בודק אם הממצאים תוקנו, מדובר בתהליך לא יעיל מפני שהרבה יכול להשתנות בשנתיים. המעקב אחר תוכניות העבודה לתיקון הליקויים צריך להיות עקבי ושוטף, אחרת הארגון נשאר חשוף לסיכונים מצד הספק ומסתכן בתקיפה שעלולה להגיע מתוך שרשרת האספקה הארגונית.

ראייה הוליסטית של ביקורות סייבר

לאור הסיכונים שהצגנו לעיל ולאור העובדה שהארגון לא מתנהל לבדו ויש שרשרת אספקה ענפה שמסייעת לו להגיע ליעדיו, תפיסת ביקורות הסייבר חייבת להשתנות.

ביצוע ביקורות סייבר לנושאים מקצועיים שונים היא חשובה מאוד ויש להמשיך בה. לדוגמה, ביצוע ביקורת דלף מידע, ביקורת על תהליך ניהול סיכוני הסייבר, ביקורת על תהליך ניהול ההרשאות והמשתמשים ועוד מגוון ביקורות אחרות.

כל נושא המבוקר על ידנו חשוב בפני עצמו, אולם האם בחנו את כל חלקי הפאזל? האם בחנו את כל הגורמים המהווים דלת כניסה לארגון?

ביקורת על תהליכי הניהול של שרשרת אספקה הפכה למהותית יותר ויותר בשנים האחרונות. אנחנו מבינים שארגונים לא נמצאים לבד במערכה. ארגון לא יכול להתנהל ללא שרשרת אספקה, והגנה על שרשרת האספקה חיונית בדיוק כמו ההגנה על משאבי הארגון.

נושאים לבדיקה בביצוע ביקורות על שרשרת האספקה:

תהליך מיפוי הספקים
האם כל הספקים הפעילים בארגון מופו וקוטלגו לפי רמת חשיבות?

תהליך הערכת סיכונים
האם בוצע סקר סיכוני סייבר לספק? האם הארגון מבין את החשיפות של הספק ואת השפעתן הפוטנציאלית על הארגון?

תהליך ניהול סקרי סיכוני סייבר
האם הארגון מנהל את הסקרים בכלי מרכזי אחד המאפשר קבלת תמונה של מגוון הסיכונים שאליהם הוא חשוף מתוך שרשרת האספקה? ניהול ידני באקסלים פחות יעיל ככל שלארגון מספר רב של ספקים.

תהליך ניהול הממצאים
האם קיים מקום מרכזי לניהול כלל הממצאים שעלו מתוך הסקרים? האם מתקיים מעקב שוטף אחר תיקון הממצאים?

יעילות ביצוע הסקרים
האם לספקים מהותיים בוצע סקר מעמיק? לעיתים מתבצעים סקרים במסגרת זמן של כמה שעות ספורות. לעיתים מסגרת הזמן הזאת אינה מספקת על מנת להבין את הסיכונים המהותיים של הספק. יש לוודא כי הסקר הוא מקצועי ומעמיק בהתאם לרמת הרגישות של הספק לארגון.

ביצוע תרגיל תקיפה על הספק
בחינה עד כמה הספק חשוף לתקיפות סייבר. יש לעגן חוזית מול הספק את נושא ביצוע תרגילי תקיפה עליו.

לאחר בדיקת הנושאים שצוינו לעיל ניתן לבצע ביקורת מעמיקה יותר שתבחן את רמת ההגנה של הארגון מפני תקיפות דרך שרשרת האספקה.

בסופו של דבר, מבחן התוצאה הוא המבחן הטוב ביותר על מנת לבחון את יעילות ואפקטיביות מערך הגנת הסייבר הארגוני.

ביצוע סימולציית תקיפה או תרגיל Red Team כאשר וקטור החדירה לארגון הוא שרשרת האספקה, יהווה ביקורת מעמיקה ומקיפה יותר על מערך ההגנה הארגוני מפני תקיפות דרך שרשרת האספקה.

תרגיל Red Team מקיף ובוחן את שכבות ההגנה השונות ללא מידע מקדים על הארגון, כך שתמונת הביקורת שתוצג לארגון תהיה יעילה יותר ובעצם תראה הלכה למעשה האם ניתן לתקוף את הארגון דרך שרשרת האספקה.

באמצעות הממצאים שעולים מסימולציית התקיפה או מתרגיל ה-Red Team ויישום ההמלצות שיעלו מתוך הביקורת, הארגון יוכל לשפר את מערך ההגנה שלו בצורה ממוקדת יותר ובזמן קצר יותר, דבר שיוביל לחיסכון רב של משאבי הארגון.

סיכום

מערך ההגנה הארגוני שלנו אינו מסתיים רק ב-Perimeter ("הגבול ההיקפי") הארגוני אלא כולל גורמים נוספים שמהווים דלת לתוך הארגון. שרשרת האספקה הפכה ליעד מרכזי של תוקפים כדי לקבל גישה לתוך הארגון בדרך קלה יחסית מאשר לפרוץ מערכי הגנה בשלים ומתקדמים.

הסיכונים הנובעים מתוך שרשרת האספקה עלולים להוביל לנזק פוטנציאלי משמעותי עבור הארגון ולעיתים אף לאיים על המשך קיומו.

לכן תהליך ניהול שרשרת האספקה הארגונית הוא תהליך חשוב ומהותי על מנת לבחון את סיכוני הסייבר שאליהם עלול הארגון להיות חשוף.

ביצוע ביקורות על תהליך ניהול שרשרת האספקה ככלל, וניהול סיכוני הסייבר של שרשרת האספקה בפרט, הוא מהותי על מנת להבין את כל חלקי הפאזל של נושא מורכב כמו הסייבר.

בבסיסו של עניין

צעדים ראשונים בביקורת בסיסי נתונים

מאת

ארטור יעקובוב
רו"ח, MBA,
מנהל ביקורת מערכות מידע,
דואר ישראל

בחודש מאי 2019 חברת Salesforce המעניקה שירותי ענן, חסמה גישה ללקוחותיה עקב תקלה בבסיס הנתונים של החברה. התקלה נגרמה כתוצאה מקיומן של הרשאות גישה עודפות לנתוני הלקוחות.

מידע הוא משאב מרכזי לכל ארגון, ולבסיסי נתונים יש בו תפקיד מרכזי מרגע שהמידע נוצר ועד לרגע שהוא הושמד.

חברות רואות חשיבות רבה בניתוח הנתונים הקיימים בהן, הפקת תובנות חדשות מתוך נתונים, זיהוי סיכונים והזדמנויות, גילוי הונאות ותרמיות ועוד. במהלך השנים חברות הבינו כי הגנה על בסיס הנתונים היא משימה חשובה לא פחות מהגנה על נכסים פיזיים.

קיימים מספר היבטים שיש לבחון בביקורת בסיסי נתונים, במיוחד כאשר מדובר בנתונים המכילים מידע אישי וכפופים לחקיקה בהיבטים של ניהול מאגרי מידע וחוק הגנת הפרטיות.

מאמר זה מתמקד בביקורת בסיסי הנתונים בתחום הרשאות גישה למשתמשים, ומסב את תשומת הלב של המבקר לדגשים שעליו לקחת בחשבון בעת בניית תוכנית ביקורת בתחום זה. מדובר ברשימה לא סגורה, אך כזו המפרטת את הנושאים המהותיים.

הענקת גישה לגורמים לא מורשים לבסיס הנתונים מהווה סיכון מהותי שעלול לגרום לנזקים כבדים בסביבת הייצור, למחיקה ולהוספת נתונים בהיקפים משתנים, בלי שניתן לגלות זאת בזמן אמת, ללא כלים ממוחשבים המנטרים פעילויות חריגות. זאת עוד לפני שנכנסים להיבטים של דליפת מידע ופגיעה בפרטיות.

לנוכח הסיכון, חברות פועלות באופן תמידי לצמצום כמות הגורמים המורשים לגשת לבסיסי הנתונים, ואף מנטרות את פעילויות בעלי ההרשאות השונים (מפתחים, מתכנתים, אנשי תשתיות, מנהלי מסד נתונים ועוד) כדי לדעת מהן הפעולות שבוצעו בפועל בבסיסי הנתונים.

תקן ISO 27001 לניהול מערכת אבטחת מידע מגדיר (בין היתר) את השלבים השונים בתכנון וניהול מערכת ניהול אבטחת מידע החלים על נכסי החברה ובהם בסיסי הנתונים.

להלן השלבים המרכזיים בביצוע הביקורת:

1 מיפוי בסיסי נתונים

יש לוודא שקיים מיפוי של כלל בסיסי הנתונים הקיימים בחברה, המערכות שהם משמשים והמאפיינים שלהם, לרבות:

- שמות בסיסי הנתונים;
- סוג בסיסי הנתונים (SQL, Oracle ועוד);
- גרסה;
- שרתים;
- סביבות;
- רמת הסיכון שמייחסת הנהלת הארגון לבסיסי הנתונים השונים.

בהיעדר מיפוי בסיסי נתונים כמפורט לעיל, לא קיימת ודאות כי ינותח כל המידע הנדרש במסגרת הביקורת. במצב כזה מומלץ לנסות למפות את בסיסי הנתונים עם גורמים רלוונטיים בחברה, על מנת לאפשר לביקורת לאמוד נכונה את תכולת הבדיקות הנדרשות.

2 קביעת מדגם

בחברות בינוניות וגדולות כמות בסיסי הנתונים יכולה להגיע לעשרות. בהיעדר יכולת לבדוק את כולם, על המבקר לבנות מדגם מייצג תוך התייחסות לשיקולים הבאים:

- סוג בסיסי הנתונים - העדפה לבחירת סוגים שונים על פני התמקדות בסוג אחד ייעודי (SQL, Oracle,DB2 וכו').
- תחום המערכות - מיקוד הן במערכות כספיות והן במערכות תפעוליות/מחשוביות.
- מהותיות המערכות בפעילות החברה.

3 מדיניות סיסמאות

חשוב מאוד שבגישה לבסיסי נתונים יוגדרו סיסמאות חזקות העומדות בסטנדרטים שהחברה קבעה. כמו כן חשוב שמשתמשים חזקים בעלי הרשאות מרובות, שיכולים לבצע פעילות בעלת סיכון גבוה (כגון DBA), יחליפו את הסיסמאות בתדירות גבוהה יותר ממשתמשים אחרים.

הסיכון גבוה משמעותית בחברות שמשתמשות בשירותים חיצוניים (outsource), לרבות בתמיכה ובפיתוח על ידי צד שלישי. במקרים של החלפת גורמי מיקור החוץ, אי החלפת סיסמאות של בעלי חשבונות חזקים חושפת את אמצעי הזיהוי לגורמים לא מאושרים. לשם המחשה, לא אחת נתקלים בעובד במיקור חוץ שעושה שימוש בשם משתמש וסיסמה של עובד שכבר עזב את החברה.

הגדרות סיסמה של חשבונות ברירת מחדל

בעת התקנת בסיס הנתונים, החברה משתמשת בחשבונות שכבר הוקמו, עם סיסמה ידועה מראש. בכל מסד הנתונים, יש להחליף את סיסמת ברירת המחדל מיד לאחר ביצוע ההתקנה, על מנת לא להיות חשופים להתקפות מצד גורמים זרים, היות שהחשבונות והסיסמאות הנ"ל מוכרים לכל גורם המתמחה בתחום. לדוגמה, בבסיס הנתונים של SQL, סיסמה ברירת מחדל עבור חשבון SYS היא Change_on_install וסיסמת ברירת מחדל עבור חשבון SYSTEM היא Manager.

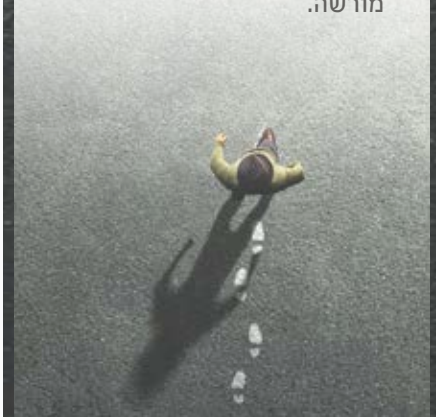
4 גישה לפעולות אדמיניסטרציה

משתמשים חזקים עלולים להשפיע ואף להזיק לנתונים באופן מהותי, בין אם בשוגג ובין אם במזיד. לכן ישנה חשיבות רבה לכך שרק גורמים מורשים יקבלו את ההרשאות החזקות לצורך מילוי תפקידם, ושכמות המשתמשים החזקים תהיה מצומצמת ביותר.

אחת ההמלצות היא למפות את כלל החשבונות הרשאים לגשת לבסיסי הנתונים, ולבדוק לעומק האם אכן קיים צורך ממשי בהרשאות שניתנו. מומלץ לסקור את הרשימה לפחות פעם בחצי שנה ולוודא כי השינויים שחלו בהרשאות בבסיס הנתונים אכן מתועדות.

להלן הפעולות הנדרשות לצורך בדיקת הנושא:

- מיפוי של כלל משתמשים/חשבונות הרשאים לגשת לבסיס הנתונים.
- בדיקת שיוך החשבון, לצורך מה הוא משמש וכמה גורמים משתמשים בחשבון.
- קבלת הסברים על חשבונות לא אישיים (כלליים).
- בחינה כיצד מתבצע ניטור של חשבונות המערכת (ממשקים, שרתים וכו').
- סקירת החשבונות ברמה חצי שנתית ואישורם על ידי גורם מורשה.



5 הקמת משתמש/חשבון או הסרתו

אחד התהליכים החשובים בבדיקה הוא תהליך הקמת משתמש/חשבון, מאחר שבתהליך זה מוענקות הרשאות למשתמשים חדשים שטרם היו רשאים לגשת לבסיס הנתונים. ניהול משתמשים נאות יקטין את סיכון חשיפת המידע לגורמים שאינם מורשים היכולים להיחשף למידע זה דרך הרשאותיהם.

ישנם מספר דגשים המשפיעים על כל התהליך עצמו:

- בקשה למתן הרשאה.
- אישור מגורם מוסמך.
- הענקת הרשאות כפי שהוגדרו ואושרו בבקשה.

יש לשים לב כי תהליך הענקת הרשאות מתבצע לפי הסדר הנ"ל ומתועד בהתאם.

בעת הקמת משתמש בבסיס הנתונים, מעורבים בדרך כלל גורמים מתחומים שונים (אנשי רשת, תשתיות, אבטחת מידע ועוד). לעיתים התיעוד המאשש את הקמת המשתמש נמצא במקומות שונים, כך שבעצם לא קיים ריכוז של כל הטפסים/אישורים בעת הקמת המשתמש במקום אחד. אי יכולת לרכז את התיעוד פוגע ביכולת לנטר את התהליך במהלך הקמת המשתמש ולבחון אותו בדיעבד.

הניסיון מראה כי בעת עזיבת משתמש, החברה לא ממהרת להסיר את ההרשאה מבסיסי הנתונים ובעצם מאפשרת גישה לגורמים לא מורשים באמצעות שם המשתמש שלא הוסר, בלי יכולת לאתר בדיעבד את הגורם שעשה שימוש בהרשאה. חשוב לבדוק את תהליך הסרת משתמשים כתהליך רוחבי, על מנת לוודא שהוא אכן מתקיים, מתועד ומבוקר לפי נוהלי החברה.

חשוב גם להתייחס לתהליך חסימה ו/או הסרת משתמשים שפרשו מהארגון, ולהדגיש את הסיכון של עיכובים בטיפול בכך.

6 חשבונות גנריים

ככלל, קיימים שני סוגי חשבונות בבסיס הנתונים:

- חשבונות אישיים המשויכים למשתמש ספציפי.
- חשבונות גנריים שאינם משויכים לגורם ספציפי, והם נדרשים לצורך עיבודים במערכת, תהליכים עסקיים וכו'. בחשבונות אלו הסיכון הוא בדליפת הסיסמה של החשבון ושימוש בחשבון על ידי גורמים לא מורשים.

מטרת הבדיקה היא לוודא כי כל החשבונות הגנריים שלא מזוהים עם אדם ספציפי אכן מזוהים עם עובד חברה/מערכת/תהליך אחד ייעודי. על מנת לבצע בדיקה זו יש למפות את כלל החשבונות ולבחון לגביהם את שייכות החשבון, לאיזה צורך הוא משמש, ומי חשוף לסיסמה עבורו.

7 ניטור

על החברה לבחור כלים המנטרים שימוש במסדי הנתונים. הניטור כולל בין היתר התרעה מפני פעילות חשודה וזיהוי ניסיונות הונאה או אירועים עוינים אחרים. בנוסף, על הכלי לנטר פעולות בבסיס הנתונים (מחיקה, רישום וכו'), גישה מחשבונות לא מורשים ומורשים, שליפה מרובה של נתונים, סריקות בבסיס הנתונים לחשיפת פגיעות, והגדרות נוספות בהתאם לצורך.

סוגי הניטורים העיקריים:

ניטור אחר פעולות של DBA

ניתן לנטר סוגים שונים של פעולות המתבצעות בבסיס הנתונים על ידי כלי הניטור, כגון פעולות המשפיעות על שינוי מסד נתונים או מבנה טבלה, תרשים, רמת ההרשאה של משתמשים ו/או שינוי רשומות בטבלה.

ניטור טבלאות רגישות

בבסיס נתונים המשפיע על דיווח כספי מומלץ להגדיר אילו טבלאות הן רגישות, ולהתריע על כל נגיעה בטבלאות לגורם העסקי. ישנן חברות שמגדירות בתור טבלאות רגישות גם נתוני עובד/לקוח/ספק בשל הפגיעה האפשרית בנושא של פרטיות המידע.

גישה לשרתים (server)

יש לבדוק מי הגורמים הרשאים לגשת לשרתי החברה והאם הגורמים הנ"ל אושרו ונסקרו בסקירה תקופתית. חשוב להפריד בין מתן הרשאות לבסיס הנתונים למתן הרשאות לשרתים, מפני שברוב המקרים אנשי DBA לא צריכים הרשאות חזקות על השרתים שמותקנים בבסיס הנתונים, וכן להיפך, אנשי תשתיות (אדמיניסטרטורים על השרתים) לא אמורים לקבל הרשאה לבסיסי הנתונים של החברה.

לסיכום

ביקורת על בסיס נתונים ככלל, וביקורת על הרשאות גישה לבסיס הנתונים בפרט, הן רק חלק קטן מעולם ביקורת אבטחת המידע ומערך ההגנה על נכסי החברה. השמירה על המידע וההגנה עליו מפני גישה לא מורשית הינו תהליך בעל מספר רבדים, שיש לקיימו בתדירות הראויה תוך מתן דגש למכלול הנושאים הראויים להיבדק.

ביקורת הרשאות גישה נועדה לוודא כי המידע נגיש רק לגורמים שהחברה הסמיכה לכך, תוך צמצום הסכנה לדלף מידע באמצעות גורמים לא מורשים, ניטור שוטף של הפעולות שהוגדרו כרגישות ו/או מהותיות לפעילות העסקית ועמידה ברגולציה ובהוראות סטטוטוריות.

חברות להוטות לחדש ולהיות מזוהות עם חדשנות

תאגיד דיגיטלי

על חדשנות דיגיטלית, IT, ניהול סיכונים ומה שביניהם

חדשנות דיגיטלית על שום מה?

חדשנות דיגיטלית מגיעה היום מכל כיוון ומקור אפשרי, ומשפיעה על שינויים רבים בארגון. חובה להבין את השינויים, לנהלם, לבקרם ולהתאימם לתרבות המקומית. בעבר חדשנות הייתה נחלה של יזמים ייחודיים, אולם כיום כל מי שיש לו גישה לאינטרנט יכול ליזום את הדבר הבא, תוך שימוש נכון ומושכל בטכנולוגית המידע.

החדשנות הדיגיטלית מהווה נושא "חם". חברות להוטות לחדש ולהיות מזוהות עם חדשנות. חדשנות דיגיטלית אינה מוצר הניתן לרכישה או התקנה בדומה למערכת מחשוב, אלא מאופיינת יותר כתרבות שיש לאמץ ולטפח. עם זאת, חדשנות אמורה לאפשר לחברה להשיג יעד כלשהו ואינה מהווה מטרה לכשעצמה.

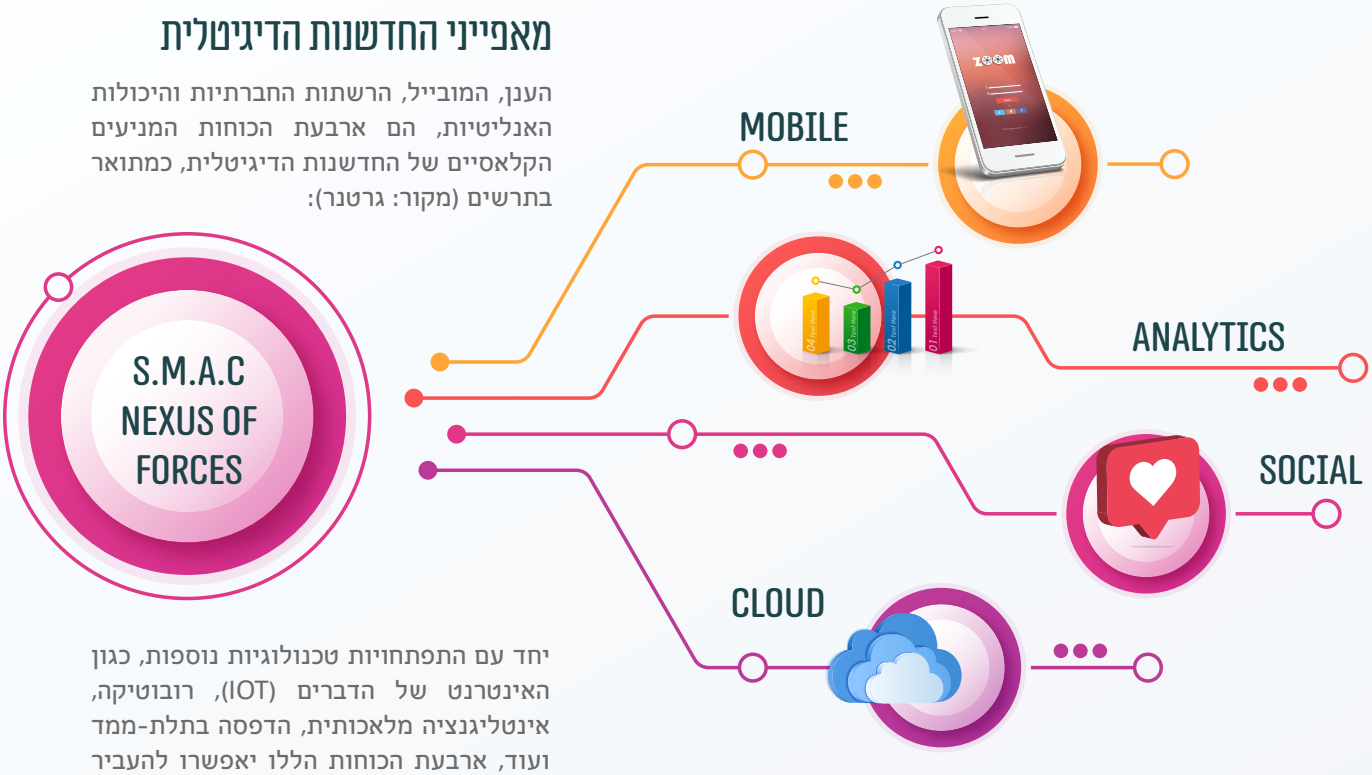
חדשנות דיגיטלית מייצרת את ההזדמנות הטובה ביותר לארגון להתקיים ולשרוד. היא עושה זאת על ידי חילוץ הערך מנכסיו הישנים והחדשים, על ידי גישות מהפכניות בתעשייה, בחברה ובעסקים, והשבחתו של הארגון. גם אם הדברים נשמעים כסיסמאות, ניתן להוכיח שחברות שאימצו חדשנות הצליחו בגדול.

מאת

אריה עמית | אלוף משנה (מיל'), בוגר ממר"ם ומפקד מרכז המיכון של אגף כוח האדם בצה"ל (ממכ"א), יועץ אסטרטגי וחבר הנהלת הלשכה לטכנולוגיות המידע בישראל

מאפייני החדשנות הדיגיטלית

הענן, המובייל, הרשתות החברתיות והיכולות האנליטיות, הם ארבעת הכוחות המניעים הקלאסיים של החדשנות הדיגיטלית, כמתואר בתרשים (מקור: גרטנר):



יחד עם התפתחויות טכנולוגיות נוספות, כגון האינטרנט של הדברים (IOT), רובוטיקה, אינטליגנציה מלאכותית, הדפסה בתלת-ממד ועוד, ארבעת הכוחות הללו יאפשרו להעביר את העסקים לעידן הדיגיטלי.

החדשנות הדיגיטלית תמשיך לדרוש יותר ויותר טכנולוגיה מתוחכמת, הארגון יידרש להיות רגיש לחידושים ולהתפתחויות טכנולוגיות, להתמצא בעולם המונחים החדש ולשלבו בעסקיו. בכך ייבדל הארגון הדיגיטלי בשוק החדש.

החדשנות הדיגיטלית ומערכות ה-IT הקיימות

בדרך כלל, לא מעשי ולא רצוי לבסס את התשתית הדיגיטלית על יסודות תשתית ה-IT הקיימים. במקום זאת, BCG וגרטנר דוגלים בהפרדה לשני מאמצים עיקריים:

המאמץ הראשון מתמקד במאמצים הדיגיטליים של החברה לפיתוחים מהירים לפי דרישות השוק, והמאמץ השני ממשיך לייצר תמיכה תפעולית לכלל העסק. שני המאמצים פועלים בקצב ובמהירויות שונים כמתחייב מאופי השינוי.

ישנם הבדלים משמעותיים בין פונקציות ה-IT התעשייתיות לדיגיטליות במונחים של נטייה, דרישות, יכולות והכישורים הנדרשים כדי למלא את המאפיינים השונים שלהם. פיתוח **IT** דיגיטלי נעשה תוך שיתוף פעולה מלא, משלב משתמשים ולקוחות (גם חיצוניים), אינטגרטיבי מאוד, ומשתמש בשיטות פיתוח ובכלים אג'יליים המאפשרים מחזורי פיתוח קצרים החוזרים על עצמם פעמים רבות.

מחלקות ה-IT הקיימות הן הבסיס של הארגון הדיגיטלי החדש. הן צריכות להיערך כדי להבטיח מבנה יציב וחדשני שבו ניתן לממש את התוכניות הדיגיטליות. המנמ"רים חייבים להתכונן לגל של טכנולוגיות חדשות שצריכות להשתלב בארגון, ומחלקות ה-IT תצטרכנה להתאים את תמיכתן במודלים החדשים ולהסתגל לשינויים אלה. בנוסף, המידע משתנה, וארכיטקטורות ותשתיות חדשות כמו עננים ציבוריים ופרטיים, וייצור ופיתוח יכולות לניצול Big Data, תופסות מקום מכובד.

אתגר גדול כרוך בזיהוי ומציאת בעלי הכישורים המתאימים להוביל ולתמוך ב-IT בארגון הדיגיטלי. מחקרים שונים בשוק מעידים שבעוד שכשני שלישים ממקבלי החלטות IT מאמינים בחשיבות המוביליות, הענן, האנליזה והרשתות החברתיות - כרבע מדווחים על פערים גדולים בכישורים העומדים לרשותם למימוש.

ניהול סיכוני IT

עולמות התוכן המקובלים והמוכרים בניהול סיכוני IT נחלקים בדרך כלל לארבע קבוצות:

- **ניהול ה-** IT **כ"בית חרושת"** המבטיח יעילות תפעולית ופיתוח שוטף ומתייחס למורכבות הטכנולוגית, לסביבת העבודה, לאינטגרציה בין המערכות, לתהליכי פיתוח, ניהול פרויקטים, ניהול שירות ותפעול השוטף.
- **משילות ה-** IT Governance המבטיחה הלימה בין האסטרטגיה העסקית והארגונית לאסטרטגיית ה-IT, ניהול תוכניות עבודה, ניהול תקציב, ניהול רכש, המשכיות עסקית, וציות לכללי החוק והרגולציה.
- **אבטחת המידע והגנה על תשתיות ונתונים** הכוללת את מדיניות אבטחת המידע, בקרת גישה, מניעת זליגת נתונים לגורמים לא מורשים, שמירת הפרטיות, בקרה ואבטחה פיזית.
- **ניהול המשאב האנושי ושימור הידע** הכולל ניהול משאבי האנוש והכשרה מקצועית לעובדים, פיתוח קריירה ותרבות ארגונית.

החדשנות הדיגיטלית על מאפייניה הייחודיים מדגישה גם מספר סיכונים חדשים המתוארים להלן:

השינוי התרבותי

חדשנות דיגיטלית כרוכה גם בשינוי תרבותי משמעותי, שינוי שאין להתעלם ממנו או לזלזל בו. ממוביל השינוי בארגון הדיגיטלי נדרשת הבנה עמוקה של אנשים ותרבות, הן בתוך הארגון והן מחוצה לו. נדרשת הבנה כיצד הארגונים פועלים עם טכנולוגיה, ואיך משתמשים בה כדי לתקשר אחד עם השני. עסקים דיגיטליים יכולים לאפשר צמיחה על ידי שילוב של טכנולוגיות דיגיטליות במאגרי מידע ובעסקים, כדי ליצור חוויות לקוח חדשניות שנועדו לענות לציפיות שלהם מהעולם הדיגיטלי.

תהליכי הפיתוח בארגון הדיגיטלי דורשים טיפוח של עבודת צוות, ועידוד כל הצוות (מעצבים, מפתחים, ויצרני התוכן) לגישות פיתוח חדשניות, ממוקדות בצרכן/לקוח, גמישות, זריזות ויעילות, הנותנות מענה מהיר לתגובות השוק. עם זאת, הגישות עדיין שיטתיות ורב תחומיות.

יעילות המנהיגות הדיגיטלית צריכה להילמד דרך השקיפות וטיפוח האיכויות, כגון יכולת הסתגלות, חוסן, פתיחות לדברים חדשים ולמידה מכישלונות/טעויות עבר. יותר מזה, למנהיגים דיגיטליים נדרש סט כישורים שיקדם את המיקוד בלקוחות ויבין את ההשלכות החברתיות.

השינויים הנדרשים יכולים להיות הרסניים וקיצוניים ולשבש את המערכת האקולוגית הרחבה יותר של לקוחות, שותפים וספקים. לכן יש להיערך להגנה על המערכות הארגוניות ועל הלקוחות. הדבר יחייב עמידה בדרישות רגולציה חדשות ובכללי דיווח שונים לדירקטוריון, הכוללים שילוב הערכות לסיכונים מסוג חדש.

תרבות ארגונית שמטפחת ומתגמלת, מעודדת שיתוף פעולה, היענות ופתיחות, היא הבסיס לבניית אסטרטגיה עסקית חדשנית ודיגיטלית חזקה.

ניהול הנתונים וניהול המידע

העולם הדיגיטלי החדש כולל נתונים ומידע בכמויות עצומות, ועל כן נדרש ניהול מידע אינטליגנטי. בעבר נהוג היה להתייחס בדיכוטומיה לניהול נתונים וניהול המידע, אולם עם הזמן התייחסות זו נעשית פחות ופחות הגיונית. בעולם של מיקוד בלקוח, נדרשות מיומנויות וטכנולוגיות משני העולמות יחד. נדרשת אסטרטגיה לניהול מידע אינטליגנטי ומשולב.

יש רמות רבות של מורכבות בחשיבה על האתגרים הניצבים בפני הארגונים. ולכן נדרש לנהל את המידע באופן מתקדם, באמצעות מגוון פתרונות המשלבים מידע מובנה המתקבל מתהליכי עבודה סדורים, מידע מודיעיני ומידע "פתוח" מרשת האינטרנט המתקבל מהרשתות החברתיות וממערכות המנטרות את פעילות הפרט והארגון ברשת.

ארגונים הממוקדים בלקוח ובחוויה שלו צריכים להבין את המסע שהלקוח עובר בתהליכי משנה רבים כמו רכישה ותשלום, או הצטרפות של לקוח חדש בעקבות קמפיין שיווקי. הבנת השלב שממנו הארגון מתחיל את ההערכות מסייעת לקבוע עד כמה רחוק יוכל להגיע בבניית תחזיות מציאותית לעתיד עסקיו.

ישנן פלטפורמות מעולם ה-Big Data לשיתוף מידע עבור "עובדי ידע", המנהלות נתונים מובנים ומידע "פתוח" באופן משולב וחדשני שהארגון יצטרך לאמץ.

שילוב גישות TOP DOWN ו-BOTTOM UP בטרנספורמציה דיגיטלית

ארגונים רבים נמצאים בעיצומו של מסע להפיכת העסק שלהם לדיגיטלי. המנהלים הבכירים מושפעים מהשיח הציבורי לגבי צורך במהלך נועז לשינוי דיגיטלי. אולם היוזמה לא תמיד מבוססת על הבנת כל המשמעויות הכרוכות בכך, לעיתים בשל חוסר במיומנויות הנדרשות לנושא, ולעיתים היא מתבססת על חוויות העבר לגבי ניהול תוכן וממשל הכרוך בניהול המידע.

כדי להבין את הפוטנציאל של יוזמות לשינוי דיגיטלי ולמנוע כישלון, נדרש עדכון לכישורים ולתפיסת העולם המיוחדת של עבודה עם כמות נתונים ותכנים מסדר גודל אחר.

טרנספורמציה דיגיטלית לא ב-BIG BANG

לא כל תהליך עסקי כולל טיפול בכמות מידע ענקית ובמיליוני מסמכים באופן ישיר בתהליך של ניהול תכנים מסורתי. תהליכי היום-יום הרבה יותר צנועים, אף שגם בהם יש כמות מידע אינטנסיבית. האוטומציה של תהליכי היום-יום האלה היא תנאי מקדים וקריטי לשינוי הדיגיטלי.

האתגר הוא לבנות חברה שיכולה להשתנות בקצב שבו קורים השינויים

לא "לשפוך את התינוק עם המים"

יש להחליט היכן נדרשת החלפה דרסטית והיכן אפשר לוותר תוך כדי התייחסות לשאלות מפתח כמו: כיצד למנף את ההשקעות הקיימות בניהול תכנים בארגון? איך משתלבות מערכות עתירות ידע קיימות (Legacy) יחד עם ההשקעה במערכות ממוקדות לקוח חדשות?

לרוב הארגונים יש מערכות ומאגרי מידע רבים יותר ממה שהם יודעים וחושבים, לכן חשוב להבין את המטרה של כל מערכת תוכן מרכזית, מידת הרלוונטיות שלה, העלות שלה, האם יש הזדמנויות לאחד ספקים, והאם יש פתרונות זמינים מודרניים וגמישים יותר. כל העת חשוב לזכור את דרישות הליבה הפונקציונליות.

חשיבותה של ה"מטה דטה"

Metadata היא המפתח למעבר מחשיבה הממוקדת באחסון לחשיבה הממוקדת ביישומים. היא גם המפתח לפעילות ישימה ושפויה סביב היכולת של עובדי הידע למצוא מידע ולהתמצא בתוך אוסף של מאגרי מידע רבים, וליכולת של הארגון לבנות מסגרת ניהולית לנכסי מידע. הימים שבהם אפשר היה להסתפק ב"מילון נתונים אחיד" כבר עברו מן העולם.

בקצה הפירמידה נמצא מדעני נתונים (Data Scientists), העוסקים לא רק בניתוחים ותחזיות, אלא גם בהסקת מסקנות על יד למידת מכונה ואינטליגנציה מלאכותית.

לסיכום

ניהול הסיכונים ביישום חדשנות טכנולוגית דיגיטלית אמור לאפשר לארגונים להתמודד עם שלושה אתגרים מהותיים:

התמודדות עם שינוי אקספוננציאלי מואץ המאפיין את תקופתנו ודורש מארגונים יכולת התאמה מהירה.

התמודדות עם תחרות הולכת וגוברת המכריחה את החברות להיאבק זו בזו כדי להגן על המיצוב והרווחיות שלהן. הדרך היחידה להתמודד היא באמצעות חדשנות.

התמודדות עם הפיכת הידע לקומודיטי המקשה על ארגונים לבדל עצמם לעומת המתחרה. כולם נמצאים באותן רשתות של שותפים עסקיים, לקוחות ויצרנים, המאפשרות זרימת ידע באופן חופשי. ההתמודדות היא ברמת היצירתיות - מהירות יצירת מידע וידע חדשים.

האתגר הוא לבנות חברה שיכולה להשתנות בקצב שבו קורים השינויים. החברות שיצליחו לשרוד את העשור הקרוב ואחריו, הן אלה שיצליחו להתקדם בשלושת האתגרים הללו.

השפעת טכנולוגיות משבשות על הביקורת הפנימית

מאת
אנה מילאג'

במפגש המליאה של חברי הנהלת ה-IIA שהתקיימה בדאלאס, טענו חברי הפאנל בדברי הפתיחה כי

טכנולוגיות חדשות יכולות להרחיב את יכולות הביקורת הפנימית

הפאנל התקיים בהנחיית מר הרולד סילברמן, מנכ"ל IIA דאלאס ובהשתתפות חברי פאנל נבחרים, כגון מר בריאן פוסטר, מנהל אגף ביקורת הפנימית בחברת מיקרוסופט; מר סטיבן מיילס, מנכ"ל בקבוצת פרומונטורי פיננסי; וכן גב' כריסטה סטייל, הבעלים של ChristaSteele.com.

מר פוסטר פירט את הכלים והטכנולוגיות שהביקורת הפנימית חייבת להיעזר בהם היום כדי להיערך לעתיד:

- כלים שיתופיים
- כלים לניתוח נתונים לרבות ניתוחי עומק
- אוטומציה
- כלים לחיזוי
- כלים לעיבוד שפה
- מסגרת ביקורת מוגדרת לבינה מלאכותית (AI)

הוא טען כי על הביקורת הפנימית לפתח יכולות כגון:

- הבנה העסקית
- יועץ מהימן
- שיתוף פעולה
- חשיבה מכוונת צמיחה
- תובנות טכניות - שימוש בטכנולוגיות לבצע ניתוח לחיזוי עתידי
- יכולת "לספר סיפור" באמצעות ניתוח נתונים; נקודת מבט - "אובססיביות" לצורכי הלקוח

לדעת פוסטר, "אם נוכל להתרחק ממשימתיות ולכוון לכיוון מתן תובנות, אנחנו נשתפר". הוא מציין כי

אם הביקורת הפנימית תתפתח היא לא רק תישאר רלוונטית אלא גם תהפוך לשותף אסטרטגי

מר מיילס הפנה את דבריו לקהל ואמר "היכולות הטכנולוגיות הפוטנציאליות מתפתחות במהירות גם ברגעים אלה, הן השימוש בהן והן היישומים". הוא התייחס לתהליך אוטומציה רובוטית, אוטומציה קוגניטיבית ובינה מלאכותית.

לדברי מיילס, "זהו אתגר אמיתי לניהול הביקורת". זוהי קריאה למנהלים בכירים להחליט במהירות על האופן שבו הם מתכוונים להשתמש בכלים אלה בארגונים שלהם. הוא הוסיף שאין מספיק מבקרים פנימיים בעלי מיומנות היודעים להפיק ערך נוסף מכלים אלה. מבקרים פנימיים ראשיים נדרשים לגייס את העובדים המתאימים.

מר מיילס אמר כי תעודת המבקר הפנימי המוסמך של ה-IIA היא ההסמכה המוכרת להכשרה של מקצוע הביקורת הפנימית. ככל שאנו מתקדמים קדימה, ההסמכה היא זאת המזהה אותנו כמומחים בתחומים אלה.

גברת סטייל אמרה לקהל שהגיע העת להתקדם ולא רק להיות בעל ידע ביישומים של טכנולוגיות חדשות. היא הוסיפה כי הקו המפריד בין פונקציות הביקורת לבין פונקציית הסיכון הולך ומיטשטש.

הביקורת הפנימית צריכה לבלוט מפני ש"אם אינך יוזם דיון בישיבת הדירקטוריון על מה מחוץ לנורמה, אתה מכשיל את הארגון"

גברת סטייל עודדה את הקהל להיות חשוף וכן בשיח על מה שהם מבקרים בפועל לעומת מה שרצוי שיבקרו. ואף דחקה: "לכו מעבר לדיווח הטיפוסי", כלומר "תנסו לפענח, לחזות ולמנוע". בדברי הסיכום אמרה לקהל: "אל לכם רק לאמץ את הכיוון, עליכם להתוות אותו."

אתר האיגוד
לשירותכם

WWW.THEIIA.ORG.IL

תוכלו למצוא באתר

- תקינה ומידע מקצועי ממוין לנושאים לפי קטגוריות -

- חדשות ועדכונים על חידושים במקצוע -

- בלוגים ודעות בנושאים שונים -

- כתבי עת קודמים לקריאה דיגיטלית -

- קורסים וערבי עיון -

- כנסים בארץ ובחו"ל -

איגוד מבקרים פנימיים בישראל
INSTITUTE OF INTERNAL AUDITORS IN ISRAEL

אני לא רובוט

תהליכי אוטומציה וביקורת פנימית

תארו לכם שהמושג "עובדים כמו רובוטים" היה מקבל משמעות אמיתית. עבודה הייתה מבוצעת במהירות, ללא הפסקות, ללא חופשות או מחלות. 24/7. ללא טעויות.

מסתבר שאנו כבר לא רחוקים מעולם כזה.

במצב שבו רובוטים משתלבים בעולמנו כמעט בכל תחום, אין סיבה שלא יגיעו גם לעולם התעסוקתי.

אז אמנם לא נראה רובוטים בדמות אדם מתהלכים ברחובות תל אביב (או אולי כן, אבל זה כבר נושא לדיון אחר) אך תוכנות ייעודיות המתוכנתות לביצוע פעולות ספציפיות ומוגדרות, בהחלט משתלבות בעולם העסקי. תהליכים אלו נקראים RPA (Robotic Process Automation).

במאמר זה ננסה לשפוך מעט אור על תהליכי האוטומציה ההולכים ומתרחבים במגוון תחומים ומגזרים שונים. ננסה להבין כיצד אלה יכולים לסייע לארגון, וכיצד מושפעת עבודת הביקורת הפנימית כתוצאה מתהליכי אוטומציה המוטמעים בארגון.

מאת

גלי גנה | רו"ח, CIA, CISA, CRISC, CRMA, שותף, רוזנבלום הולצמן ושות', רואי חשבון

מוריה צבעוני | רו"ח, CISA, רוזנבלום הולצמן ושות', רואי חשבון

מהם תהליכי רובוטיקה ואוטומציה?

בשנים האחרונות קיימת מגמה של מעבר לתהליכי רובוטיקה ואוטומציה (RPA) בעולם העסקי. מגמה זו צוברת תאוצה וניצנים ראשונים ניתן לראות גם בישראל. הצפי הוא כי המגמה תימשך ותבוא לידי ביטוי במגזרים שונים במשק.

חברת המחקר האמריקנית Forrester Research סבורה כי שוק ה-RPA יגיע לסך 2.9 מיליארד דולר עד לשנת 2021, ואילו עד לשנת 2029 כ-47% משוק העבודה האמריקאי יושפע בדרך כזו או אחרת מתהליכי RPA.

השפעה זו יכולה לבוא לידי ביטוי, בין היתר, ביצירת משרות חדשות או בתפיסת מקומם של עובדים על ידי RPA.

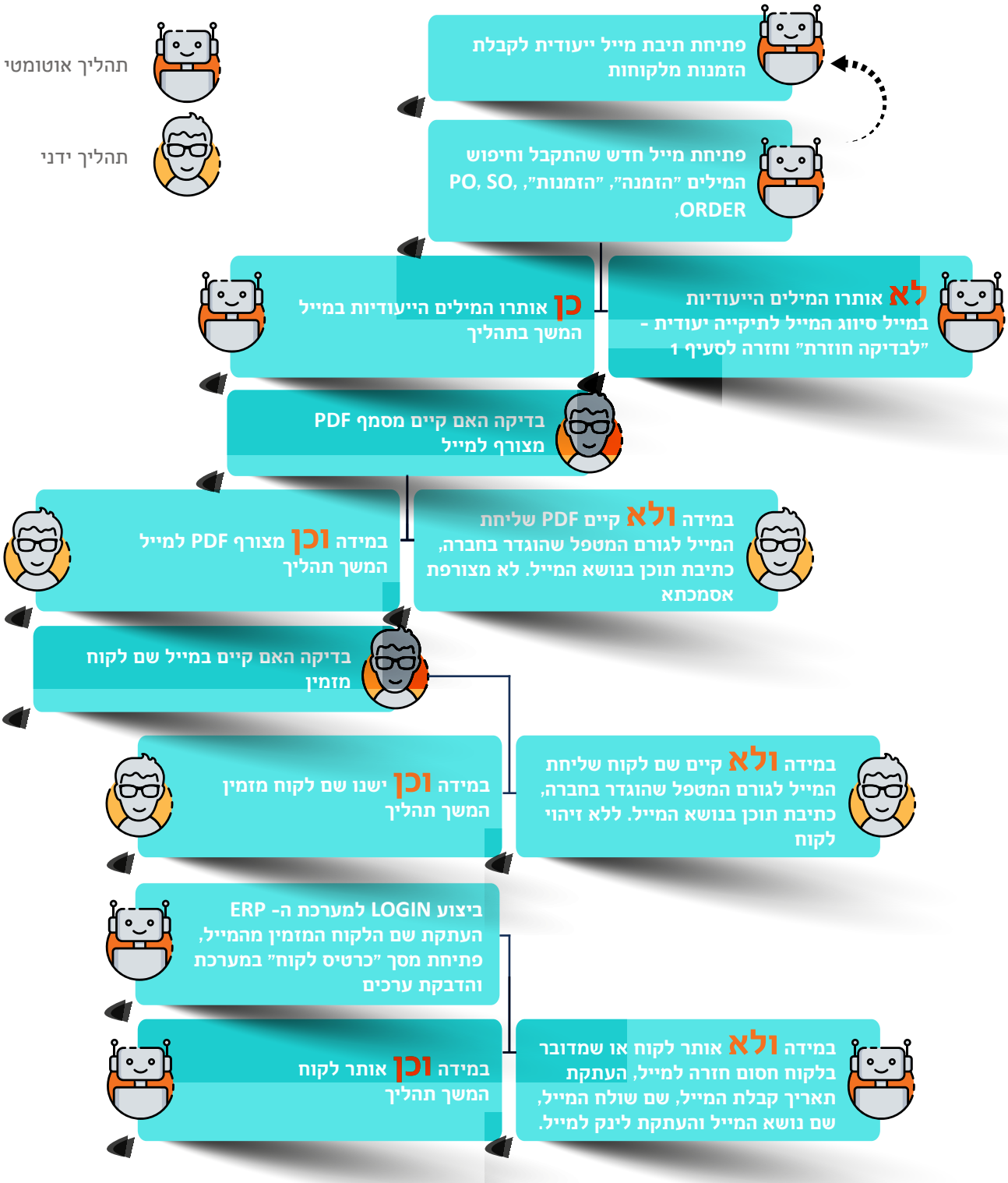
RPA הוא תהליך עסקי (במרבית המקרים) המבוצע על ידי "רובוט". יש המתייחסים לנושא כ"יצירת כוח אדם וירטואלי". במסגרת RPA ניתן לבצע פעולות מתוכנות ופלטפורמות טכנולוגיות שונות. דוגמאות לפעולות "קלאסיות" הניתנות לביצוע במסגרת תהליך RPA: שינוע קבצים ותיקיות, שליחת מיילים, קבלת טפסים ממוחשבים מלקוחות וקליטתם במערכות החברה.

נציג בפניכם דוגמה להמחשת תהליך עסקי בסיסי: תאגיד קמעונאי מעוניין להטמיע RPA לתהליך קליטת הזמנות מלקוחות. להלן תרשים המתאר מקטע מהליך הקליטה כפי שמבוצע טרום הטמעת RPA: אם נבקש להפוך את התהליך לאוטומטי (RPA), סביר שהשלב הראשון של תהליך פתיחת ההזמנות ייראה כך:

לפי ויקיפדיה, המילה "אוטומציה" מגיעה מיוונית עתיקה, ומשמעותה - "פועל מעצמו". משמעות המילה "רובוט", היא מכונה אוטומטית. המילה "רובוט" לקוחה מהמילה "רובוטה", שמשמעותה בשפה הצ'כית -"עבודת פרך".

Editorial credit: Ink Drop / Shutterstock.com

אם נבקש להפוך את התהליך לאוטומטי (RPA), סביר שהשלב הראשון של תהליך פתיחת ההזמנות ייראה כך:



הדוגמה לעיל ממחישה את הצורך לפרוט את התהליך למשימות פשוטות וקצרות, כמו גם הגדרת המסמכים הנדרשים בכל שלב על מנת שניתן לבצען באופן דיגיטלי, לדוגמה: מסמך שהתקבל בכתב יד נצטרך לקבלו מוקלד.

שלב העברה לאוטומציה מחייב הגדרת נקודות החלטה וברירת מחדל של "מה קורה אם לא"

שבמסגרתן התהליך האוטומטי ייעצר ותועבר הודעה לגורם האחראי.

יתרונות וחסרונות בתהליך

ארגון המעוניין לבחון העברת תהליך ידני ל-RPA צריך לבחון
את היתרונות והחסרונות. להלן נקודות מרכזיות:

יתרונות

חיסכון בעלויות לטווח הרחוק.

מניעת טעויות ידניות

מהירות תגובה.

זמינות - 24/7/365.

שביעת רצון עובדים - הפחתת "עבודה שחורה" ומעבר לעבודה תורמת.

שיפור הגנת הפרטיות - תהליכים המבוצעים אוטומטית פחות חשופים ליד אדם.

חסרונות

עלות ראשונית גבוהה.

בהיעדר בקרות הולמות והטמעה נכונה, קיימת חשיפה לתקלה רוחבית.

חשיפה לפגיעה בתהליכי העבודה אם לא בוצעה בחינה מחודשת לתהליך העבודה.

התנגדויות לצמצום כוח אדם.

אבטחת מידע - תהליכים המבוצעים באופן אוטומטי, חשופים יותר לאירועי סייבר ואירועי אבטחת מידע.

ביקורת פנימית לתהליכי RPA

עבודת הביקורת הפנימית לתהליכי RPA תבוצע בשני שלבים:

ביקורת פרויקט - כביקורת מלווה במהלך ההטמעה.

ביקורת פנימית על תהליך - ביקורת פנימית שוטפת לתהליך העבודה העסקי לאחר הטמעת RPA.

ביקורת בנושא הטמעת פרויקט

בדומה לביקורת פנימית בנושא ניהול וביצוע פרויקטים, ניתן לבצע ביקורת על תהליך הטמעת RPA בתאגיד הן ב"ראיית-על" (מדיניות, השלכות בנושא יחסי עבודה, שירות לקוחות/ספקים וכו') והן בראייה ממוקדת עבור תהליך נקודתי. ניתן לבצע אף כביקורת מלווה.

כאמור, ביקורת ניהול פרויקט כוללת נושאים גנריים שסביר שנמצא בכל פרויקט בכל תחום (תכנון מול ביצוע והשגת היעד, עמידה בלוח זמנים, תקציב מול עלויות בפועל). במאמר זה נשים דגש על נושאים ייחודיים בתהליך RPA.

להלן דגשים לביקורת פנימית בנושא ניהול פרויקט RPA :

- **Proof of Concept (POC)** - בחינת תהליך בדיקת היתכנות טרם יציאה לפרויקט. האם אוטומציה היא אכן פתרון ראוי או שניתן לייעל את התהליך בחלופה אחרת. בבדיקת ההיתכנות רצוי לבחון גם האם קיימים היבטי רגולציה בתחום הנבדק. לדוגמה: בתהליך שבו נדרש הליך זיהוי פיזי, ייתכן שהפעלת ה-RPA תחל לאחר הליך הזיהוי הידני.
- **Return of Investment (ROI)** - יש לוודא כי הארגון ביצע תהליך בחינת כדאיות כלכלית וקבלת אישור מוסדות התאגיד הנדרשים.
- **מסמך אפיון** - יש לוודא כבר בשלב זה כי במסמך האפיון הוגדרו: דוחות שגויים ותהליכי Fallback - (חזרה למצב מקור טרם שינוי) בגין שגויים בתהליך, תהליך העבודה בסביבת RPA, בקרות לאיתור תקלות בזמן סביר.
- **בחינת תהליכי ניהול שינויים**, ובכללם:
  - קיום סביבות נפרדות לפיתוח ולייצור.
  - תסריטי בדיקות.
  - בדיקות קבלה.
  - אישור העברה לייצור.
- **תוכנית לביצוע הדרכות לעובדים.**
- **היערכות לחירום -** בחינת החברה לצורך בעדכון תוכנית היערכות לשעת חירום בעקבות מעבר ל-RPA.

ככל שמדובר בביקורת מלווה, מומלץ כי המבקר הפנימי יעמוד מקרוב על הסיכונים הרלוונטיים לפרויקט.

להלן מספר דוגמאות לסיכונים הכרוכים בהטמעת RPA והצעות למענה:

- **בחינת שינוי תהליך העבודה השוטף -** על הארגון לבחון האם כתוצאה מהטמעת RPA נדרש לבצע שינוי בתהליך העבודה השוטף. לדוגמה: אם במצב הנתון מתקבלות הזמנות הן באמצעות טלפון, הן באמצעות פקס והן באמצעות מייל, הרי שהחברה תצטרך להגדיר הליך אחיד וסדור לקבלת הזמנות מלקוח. למשל, הזמנות יתקבלו באמצעות מייל ובצירוף PO (הזמנת רכישה) בפורמט אחיד מהלקוח. אם יישאר מענה טלפוני הוא צריך להיות במערכת IP חכמה שתוכל לייצא נתונים על ההזמנה, ואם יועברו פקסים יש להגדיר מנגנון Fax to mail.
- **אבטחת מידע -** הנושא יכול לבוא לידי ביטוי בניהול הרשאות גישה עבור ה-USER המשמש את הרובוט (לדוגמה: מי מנהל את סיסמאות הרובוט?), בחינת מוצר התוכנה והספק בהיבטי אבטחת המידע. לצורך כך ישנה חשיבות שישולבו בתהליך האפיון אנשי אבטחת המידע בארגון.
- **שגויים בתהליך העבודה -** שגויים בתהליך ייתכנו ממספר סיבות:
- שרתים ו/או מערכות הנדרשים לתהליך מושבתים. כמענה לנושא זה יש לוודא כי החברה הגדירה מנגנוני ניטור קבועים לשרתים למערכות הקריטיות לתהליך. כך שאם שרת אחד או יותר אינם פעילים, תהליך RPA לא יבוצע ותתקבל התראה לגורמים הרלוונטיים.
- RPA מבצע הליך סדור וקבוע המוגדר מראש, ובהיעדר תהליכי בינה מלאכותית (IA) מדובר בהליך ללא שיקול דעת. לכן בעת אפיון RPA יש להגדיר מראש פתרונות למקרים אלו. לדוגמה: בתהליך יצירת SO (הזמנת מכירה), מסמך חובה יהיה ה-PO של הלקוח. אם לא יצורף PO, לא ניתן יהיה להמשיך בתהליך האוטומטי והאירוע יועבר לטיפול ידני.
- **היערכות החברה להשבתת RPA -** כתיבת נוהלי עבודה סדורים המפרטים את תהליך העבודה במקרה של השבתת הרובוט והדרכת העובדים הרלוונטיים.
- **שילוב כלי בקרה כחלק מהפיתוח -** מומלץ כי בחודשי העבודה הראשונים תבוצע בדיקה מדגמית ידנית במקביל לעבודת הרובוט השוטפת, במטרה לוודא את תקינות התהליך.

ביקורת פנימית על תהליך (כנושא ביקורת שוטף)

עבודת הביקורת הפנימית תשתנה ככל שתהליכים ידניים יהפכו ל-RPA. במקום לדגום מסמכים, הביקורת נדרשת לבקר תהליכי בקרה ממוחשבים.

המבקרים הפנימיים יידרשו להשתמש בכלים טכנולוגיים כגון: כלי ניתוח ממוחשבים, אפליקציות לביצוע סימולציה וכו'. ביצוע הביקורת ידרוש שילוב של ידע במערכות מידע ותהליכים עסקיים.

ייתכן שאף מבנה דוח הביקורת יעבור שינויי מסוים. הדיווחים יהיו קצרים יותר, תוצרי הביקורת יהיו לא פעם ניתוחי אוכלוסיות שגויים בתהליך, ולא מן הנמנע כי ממצא ביקורת שיימצא יהיה בעל השפעה רוחבית. דוחות הביקורת יכללו פחות ממצאים אך לכל ממצא יהיה משקל מהותי.

לאחר הטמעת התהליך, במסגרת הביקורות השוטפות ייבחנו הנושאים שלהלן:

- הרשאות גישה בתהליך - מורשים לביצוע פעולות ידניות, מורשים לשינוי הגדרות הרובוט.
- בקרת שלמות התהליך - בדיקה אפשרית לתהליך זה היא באמצעות סימולציה (לרבות בחינת צומתי ההחלטות ובדיקה כי במקרים שבהם הוגדר מעבר לתהליך ידני אכן בוצעה העברה לתהליך ידני ולא חזרה ל"תחילת" הפעולה).
- ביצוע בדיקות על אוכלוסיות שגויים ודרך הטיפול בהן.
- ניתוח אירועי כשל וצמתים של קבלת החלטות.
- מוכנות הארגון להשבתת RPA.
- בדיקות ועדכון שוטף של RPA (תחזוקה, ניהול גרסאות).
- בדיקות סבירות שוטפות. לדוגמה: סבירות כמות המיילים שהתקבלו ביחס לכמות ההזמנות שנפתחו.
- בדיקות איכות התהליך וכדאיות שוטפת - בחינה האם המעבר לעבודה באמצעות רובוט אכן יעיל, או שכמות ההעברה לתהליך ידני היא משמעותית ומעמידה בספק את כדאיות התהליך.
- שינויים בהגדרות פעילות הרובוט לאחר הפעלה ראשונית - תקינות התהליך, אישורים נדרשים.
- השפעתם של שינויים בפעילות העסקית על עבודת הרובוט. לדוגמה, אם החברה פתחה או סגרה מחסן מלאי, האם ישנה השפעה על ניהול הזמנות הלקוח?

לסיכום

מגמת המעבר ל-RPA בעולם ובישראל, יחייבו את המבקר הפנימי להכיר את העולם החדש הזה ולהיות קשוב ופתוח לאפשרויות חדשות העומדות בפניו בניצול יכולות RPA לשם קידום, ייעול ושיפור עבודת המבקר הפנימי, וכפועל יוצא להגברת תרומתו לארגון.

הקבוצה פתוחה
לכל המבקרים הפוטנציאלים

הצטרפו אלינו!

מפגשי נטוורקינג
Meetups -ו

יש לכם שאלה
שאלו אותנו ברשת

הזדמנות להכיר את
החברים **הבכירים**
והצעירים מקרוב

הצטרפו
לקבוצות
דיון
בפייסבוק
ובלינקדאין

שאלות לדיון
שיגרמו לכם
לחשוב

הזדמנות להתייעץ
עם קולגות
מארגונים אחרים

מאת

חן-דיאנה כץ | מבקרת פנימית
ראשית בשירותי בנק אוטומטיים
(שב״א) ובמרכז סליקה בנקאי
(מס״ב)

לילך זילבר-טל | מנהלת מחלקת
ביקורת פנימית ב-Cal חברת
כרטיסי אשראי

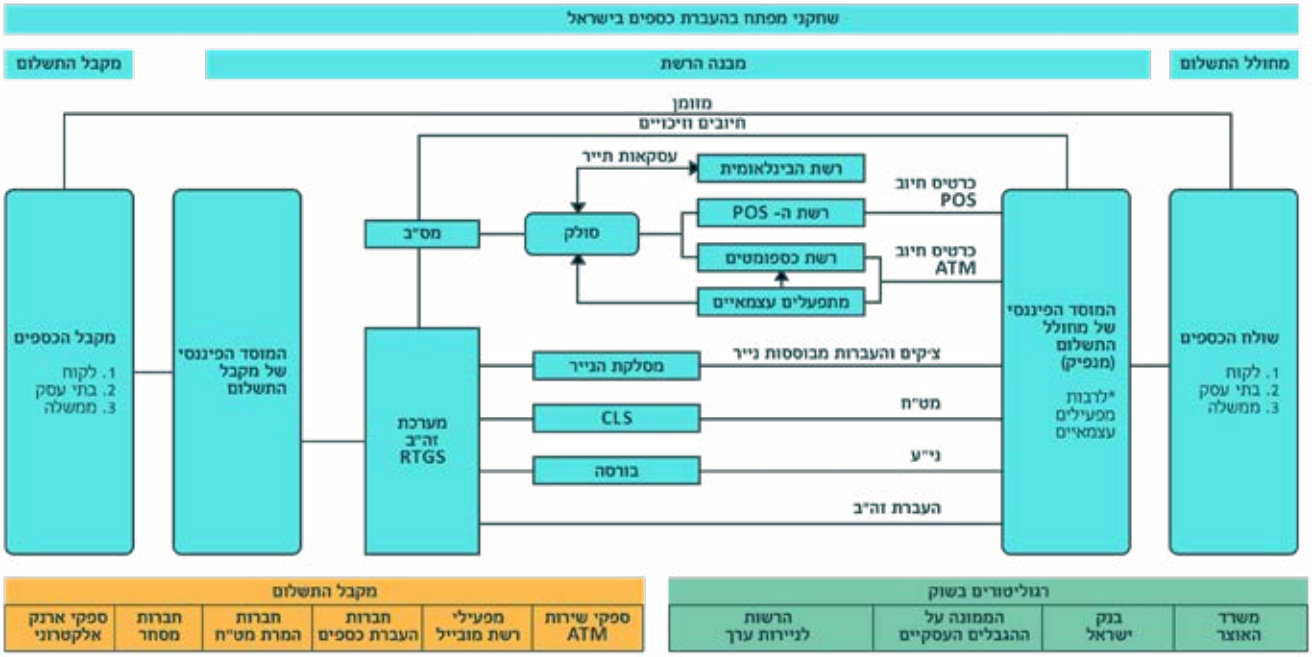
לבקר את תחום התשלומים בעידן של שינויים טכנולוגיים

בשנים האחרונות אנו עדים למהפכה כלל עולמית בתחום התשלומים. המהפכה מונעת על ידי שינויים רבים בשרשרת ביצוע תשלום, המשפיעים ומושפעים זה מזה בתאוצה הולכת וגוברת. בין היתר, שינויים טכנולוגיים, שינויים בצרכים ובציפיות של הצרכנים ושינויים רגולטוריים. מבקרים פנימיים בארגונים כאלה נדרשים להתאים עצמם למציאות החדשה, לרבות קיום מעקב מתמיד אחר השינויים ובחינת השפעתם על הארגון, עדכון יעדי הביקורת ושדרוג האמצעים לביצועה.

מאמר זה מנתח ממעוף הציפור את התפקיד של פונקציית הביקורת הפנימית בארגונים המעורבים בשרשרת ביצוע תשלומים ואת האתגרים העומדים בפניה בעת הזו.

כיום, עדיין קיימים מספר אמצעי תשלום מסורתיים מקובלים: מזומן, צ׳קים, תשלומים ישירים אלקטרוניים וכרטיסי חיוב (כרטיסי אשראי, כרטיס דביט וכרטיסים נטענים). בנוסף, קיימת מגמה של התפתחות באמצעי תשלום אלקטרוניים מתקדמים.

בתרשים להלן, מתוך דוח ״שרשרת ביצוע עסקה בכרטיסי חיוב״ של בנק ישראל (יולי 2016), מוצגים שחקני מפתח בשרשרת ביצוע תשלומים בישראל.



התקדמות טכנולוגית ושינויים בצרכים ובציפיות של הצרכנים - איפה הביצה ואיפה התרנגולת?

ההתקדמות הטכנולוגית מרגילה אותנו לגישה מיידית לדברים שאנחנו רוצים, והציפיות בנוגע לתהליכי תשלומים אינם יוצאי דופן. בעולם שבו הכול מתרחש בלחיצת כפתור - אנשים לא מסתפקים עוד רק בעצם העברת התשלום משולח לנמען באופן בטוח, אלא מהירות זה שם המשחק החדש. ואכן, בשנים האחרונות אנו עדים למהפכה בתחום התשלומים, מהפכה שמשפיעה על כל אחד מהשחקנים בשרשרת ביצוע העסקה (צרכנים, סוחרים ומגוון ארגונים התומכים בשלבים שונים של תהליכי התשלום (מנפיקים של כרטיסי חיוב, סולקים, מאגדים, מעבדים, חברות ניכיון, ספקי נזילות, מפעילי מערכות תשלומים וכו׳).

לשם הדיון על צורכי השוק, חשוב להבחין בין פעולת התשלום המתבצעת במעמד ביצוע העסקה לבין התהליך של הסליקה הכספית בפועל בין הגופים הפיננסיים התומכים בתהליכי התשלום. צרכנים וסוחרים רוצים מהירות תשלום (כלומר היכולת לראות עסקאות המשתקפות בחשבונותיהם תוך מספר שניות וגישה מיידית לכסף). עם זאת, הגישה המיידית של הצרכנים לכסף לא בהכרח מחייבת שגם הסדרת הפירעון בפועל בין השחקנים בשרשרת ביצוע העסקה תהיה מיידית. הארגונים התומכים בתהליכי ביצוע העסקה רוצים נתוני תשלום עשירים יותר ומערכות מתקדמות כדי להבטיח גם את הסדרת הפירעון ביעילות ובמהירות האפשרית. כולם רוצים אבטחה ופרטיות. בהתאם, כל השחקנים בתעשייה חייבים לפעול להתקדמות טכנולוגית כדי להישאר רלוונטיים.

יד ביד עם הרגולטורים וגורמי הפיקוח

לגורמי הרגולציה והפיקוח יש תפקיד משמעותי במהפכת התשלומים העולמית. בתגובה לשינויים של השוק, יותר מ-30 מדינות ברחבי העולם השיקו יוזמות גדולות למודרניזציה של תשתיות התשלומים הלאומיות שלהן. בו-בזמן הרגולטורים רצו להבטיח כי שירותי התשלום המתפתחים מציעים לא רק מהירות ביצוע אלא גם שקיפות וסיכון מופחת לצרכנים ולעסקים. כתוצאה מכך הם החילו על השחקנים בשרשרת ביצוע התשלום תקני ניהול סיכונים מחמירים יותר.

המעורבות הרגולטורית בתחום התשלומים ניכרת גם בישראל. להלן מספר דוגמאות מרכזיות מהשנים האחרונות כפי שעולה מאתרי האינטרנט של גורמי הרגולציה השונים (משרד האוצר, רשות החדשנות, בנק ישראל וכו׳):

- חוק אמצעי תשלום
- דוח של הוועדה לקידום השימוש באמצעי תשלומים מתקדמים בישראל
- צעדים להרחבת התשתית של אמצעי התשלום האלקטרוניים
- חוק סליקה אלקטרונית
- חוק שירותי התשלום
- חוק הפיקוח על שירותים פיננסיים
- החוק להגברת התחרות ולצמצום הריכוזיות בשוק הבנקאות

דוגמאות למונחים מקצועיים מתחום התשלומים שצריכים כבר להיות חלק מהשפה היומיומית של הביקורת ולקבל ביטוי בתוכנית העבודה שלה - **ממש על קצה המזלג:**

ארנקים דיגיטליים (Apple pay, PayPal, Google wallet, Samsung pay)

אפליקציות תשלום (BIT, Paybox, פייפר)

אבטחה ואימות צרכנים (הזדהות ביומטרית, זיהוי באמצעות קול ופנים, סורק של טביעת אצבע וכו')

מאפשרי תשלום (NFC, Tokenization, מודלים מבוססי ענן וכו')

סטנדרט הבנקאות הפתוחה - API

P2P

EMV

תפקיד הביקורת הפנימית

ארגון המהווה חוליה בתהליך זרימת תשלומים, חשוף במהות לסיכונים רבים. כמו כן, בעת התממשות סיכון משמעותי קיימת חשיפה מוגברת לאפקט דומינו אל השחקנים האחרים המעורבים בתהליך זה, עד כדי גרימת נזק רוחבי למערכת הפיננסית (המקומית ואף הבינלאומית).

לפיכך, בארגונים כאלה יש חשיבות רבה לאתגור מתמשך של מנגנוני ניהול הסיכונים וקווי העסקים על ידי הביקורת הפנימית. עם זאת, קיימת שונות בהגדרת תפקידי הביקורת הפנימית והאתגרים העומדים בפניה, בהתאם למגוון פרמטרים המאפיינים את הארגון המסוים ואת אופי פעילותו.

כך לדוגמה:

- שוני במיקום של הארגון על פני שרשרת ביצוע העסקה, שבא לידי ביטוי בין היתר בשוני בסל השירותים שהארגון נותן, שוני בתיחום גאוגרפי של הפעילות, ושוני בהגדרת לקוחות הארגון (צרכנים פרטיים, בתי עסק, גופים פיננסיים אחרים וכו').
- שוני בסוגי הסיכונים הגלומים בפעילות של הארגון: ארגונים שפעילות הליבה שלהם יוצרת סיכונים פיננסיים מגוונים לעומת ארגונים המהווים תשתית טכנולוגית וחשופים בעיקר לסיכונים תפעוליים.
- שוני במערכות המידע עליהן מתבססת הפעילות: ארגונים ותיקים עם מארג מערכות מידע מדורות שונים אל מול ארגונים צעירים עם מערכות מידע חדשות ומסונכרנות היטב אחת עם השנייה.
- גורמי פיקוח ורגולציה: ארגונים הכפופים לרגולציה פיקוחית שונה בהיקפה ו/או במהותה.

בישראל, שחקני המפתח בתחום התשלומים (התאגידים הבנקאיים, חברות כרטיסי האשראי וחברות שירותים משותפים) פועלים על פי הוראות המפקח על הבנקים, לרבות בנושא הביקורת הפנימית. ואכן, תפקידי הביקורת בארגונים אלו הוגדרו בהרחבה במסגרת הוראות ניהול בנקאי תקין של בנק ישראל. זאת החל מהוראה ייעודית בנושא "פונקציית ביקורת פנימית" ודרך הדגשת תפקידי הביקורת בהתייחס למגוון נושאים המטופלים בהוראות נוספות (ניהול טכנולוגיות המידע, ניהול המשכיות עסקית, ניהול הגנת הסייבר, ניהול סיכונים מחשוב ענן).

בנוסף, ארגונים המוגדרים כמערכת תשלומים על פי חוק מערכות תשלומים, נדרשים לפעול על פי הוראות יחידת הפיקוח על מערכות תשלומים של בנק ישראל, ומסמך עקרונות למערכות תשלומים המהוות תשתיות של השוק פיננסי. במסמך העקרונות מוצגת הגדרה מורחבת של תפקיד הביקורת הפנימית, תוך מתן דגש רב לביקורת על מנגנוני ניהול הסיכונים.

השפעת ההנחיות על תוכנית הביקורת
(ולמעשה – איך הביקורת צריכה/יכולה לסייע ולתת ערך מוסף לארגון)

על פי הוראת בנק ישראל באשר לתפקידי הביקורת הפנימית: "ההנהלה הבכירה תבטיח כי פונקציית הביקורת הפנימית תעודכן באופן מלא בהתפתחויות חדשות, יוזמות, מוצרים ושינויים תפעוליים כדי להבטיח שכל הסיכונים הנלווים יזוהו בשלב מוקדם".

על פי מסמך העקרונות למערכות תשלומים המהוות תשתית שוק פיננסי: בעת ביצוע שינויים בארגון רצוי שתהיה מעורבות פרואקטיבית של הביקורת. סקירה של הביקורת טרם הטמעת השינויים בדרך כלל תפחית את הצורך בבזבוז משאבים עודף לשיפור רטרואקטיבי של תהליכים ומערכות, ותאפשר שילוב בקרות קריטיות כחלק מתהליך התכנון הראשוני.

בדומה לנדרש מקברניטי הארגון,

גם הביקורת הפנימית צריכה לשלוט בשפה החדשה בתחום התשלומים, לעקוב בזמן אמת אחר השינויים המהירים, ולהבין את ההשלכות המיידיות ו/או העתידיות שלהם.

תוכנית העבודה של הביקורת הפנימית צריכה להתייחס לשינויים החלים בארגון ולבדיקת נושאים שבליבת התוכנית האסטרטגית של החברה.

כך לדוגמה:

1. הביקורת צריכה להעריך האם היעדים והתוכניות העסקיות של הארגון נותנים מענה הולם לתהליכים המואצים של טרנספורמציה דיגיטלית (כלומר, שימוש בכלים טכנולוגיים במקום בכלים פיזיים מסורתיים) הן אצל הלקוחות והן אצל המתחרים, לסייע לארגון בעיצוב ובהטמעה של מסגרת שליטה ובקרה על תהליכים ומערכות דיגיטליים (כגון ליווי פרויקטים אסטרטגיים, עריכת ביקורת בזמן אמת) ולזהות הזדמנויות של הארגון במיכון תהליכי עבודה.
2. הסתכלות הביקורת צריכה להיות גם בראייה צופה פני עתיד. כך לדוגמה: קול קורא מטעם בנק ישראל ציין במפורש את האפשרות להקמת תשתית תשלומים מיידית מבוזרת (DLT). אמנם כרגע נראה שהשוק עדיין לא בשל אליה, אך לא מן הנמנע כי עם הזמן טכנולוגיות אלו יתפתחו וישתלבו גם במערכות התשתית הפיננסיות בישראל.
3. הביקורת צריכה להיות ערה ולתת תשומת לב ומשאבים לנושאים המתאפיינים בזיקה מוגברת להתפתחות הטכנולוגית בעולם התשלומים, ובכלל זה: סייבר ואבטחת מידע, שימוש בפלטפורמות ענן, בנקאות בתקשורת, חדשנות בתהליכי שירות לקוחות (תוך מיקוד בחוויית לקוח) והתמודדות עם מערכות "LEGACY".

לסיכום,

באופן כללי, ובעולם התשלומים בפרט,

הביקורת צריכה לנצל את זמינות המידע בעידן הטכנולוגי כדי לשדרג את תהליכי הביקורת והערך המוסף הנגזר מהם.

חשוב להבין כי ניתוח נתונים צריך להיות בסיס לכל מטלת ביקורת ולא רק למטלות שהוגדרו כביקורת מערכות מידע. זאת לרבות התייחסות לכל הנתונים הקיימים בתהליכים המבוקרים, איכותם ואופן ניהולם.

נתונים מעצימים ביקורת

שימוש בניתוח נתונים ו-Big Data בביקורת פנימית

מאת

יוסי אליאס | רו"ח Data Analyst ומבקר IT
בחטיבת הביקורת הפנימית בבנק דיסקונט.

שימוש בתחקור נתונים בביקורת הפנימית מאפשר למבקר להסביר מגמות המתרחשות בארגון (Descriptive Analysis), אך אימוץ של כלים מתקדמים מעולם ה-Big Data יאפשר למבקר הפנימי לעבור למודל של חיזוי ואופטימיזציה (Predictive Analysis) ולזהות מגמות בארגונו שלא ניתן לאתר על ידי שאלות מוגדרות מראש.

ההתפתחות המואצת של הטכנולוגיה בשנים האחרונות כללה גידול ניכר בכמויות המידע הנאגר בחברות ובארגונים וכן ריבוי של מקורות המידע. כתוצאה מכך חברות רבות עושות שימוש בנתונים הרבים שברשותן במסגרת תהליכי קבלת ההחלטות. נוסף על כך, השיפורים הטכנולוגיים העצימו את יכולות הכלים לניתוח נתונים, והם מאפשרים לחברות להפיק תועלת מהנתונים המאוחסנים במאגרי המידע שלהן, ללא צורך בהגדרה מקדמית של מטרות הניתוח.

אימוץ של כלים מתקדמים לניתוח נתונים על ידי יחידות ביקורת פנימית, יאפשר להן להעצים את היכולות שלהן לבקר את התהליכים המתקיימים בחברות ובארגונים שבהם הן פועלות.

כיום, במרבית הארגונים והחברות השימוש בניתוח נתונים בביקורת הפנימית נועד לתת מענה לשאלות שהוגדרו מראש על ידי המבקר. שימוש בכלי ניתוח נתונים במסגרת עבודת הביקורת מאפשר למבקר לאתר פעילות חריגה ביחידה המבוקרת ולבחון את מידת העמידה של המבוקרים בהוראות החוק, נוהלי עבודה או רגולציה. הנתונים הנשלפים ממערכות המידע מהווים כלי עזר עבור המבקר לאיתור יעיל של מדגמים מוטי סיכון, ולביסוס הבדיקות שהוא עורך במסגרת עבודת הביקורת. למעשה, שימוש בכלי ניתוח הנתונים בא לתת מענה לשאלות "כמה" ו"מתי" בהתייחס לתהליך המבוקר.

היכולות הטמונות בכלים לתחקור נתונים, כגון כלי Data Analysis (DA) וכלי BI (Business Intelligence), מאפשרות למבקר הפנימי לעבד כמות עצומה של נתונים בזמן קצר - כולל ניתוח של כלל הפריטים הקיימים באוכלוסייה המבוקרת (לעומת שימוש במדגמים), להצליב נתונים מתהליכים עסקיים שונים וממערכות שונות, וכפועל יוצא מכך להגדיל את הסיכוי לאיתור פעולות חריגות בתהליך המבוקר. שימוש בכלים אלה במסגרת היערכות לביצוע עבודת ביקורת פנימית מאפשר למבקר לקבל תמונת מצב על התהליך המבוקר עוד לפני שהחלה עבודת הביקורת.

תהליכי עבודה בביקורת הפנימית

עבודת הביקורת הפנימית מתבססת על הערכת סיכונים בתהליך המבוקר, שממנה נגזרים תוכנית הביקורת וכן אופן ניתוח הנתונים שיבוצע. קביעת הנושאים לתחקור מאפשרת למבקר הפנימי להגדיר את היקף העבודה שיש לבצע ולהקצות משאבים כגון כוח אדם, זמן וכלים באופן יעיל ואפקטיבי. בנוסף, הגדרת המטרות מסייעת בביצוע יתר השלבים בניתוח הנתונים, ובהם: אפיון שאילתות לשליפת נתונים, מיפוי אזורי הסיכון בתהליך המבוקר, וכן איתור ממצאים.

לאחר הגדרת המטרות לניתוח הנתונים, על המבקר הפנימי לערוך מיפוי של אזורי הסיכון הקיימים בתהליך המבוקר ולהפנות אליהם את המשאבים שהוקצו. שימוש בתחקור נתונים בשלב מקדים זה ימקד את המבקר בתתי-התהליכים שנמצאים בסיכון גבוה ביחס לשאר, ויאפשר לו להעמיק את בדיקותיו במסגרת עבודת הביקורת. קיימת חשיבות רבה לידע, לניסיון ולהיכרות של המבקר הפנימי עם הארגון והתהליכים העסקיים המתקיימים בו. תחקור הנתונים יאפשר לו לזהות פעילות חריגה בתהליך, ובהמשך להפעיל שיקול דעת במתן המענה לאותם סיכונים שזוהו.

ביקורת מונעת-נתונים – DATA DRIVEN AUDIT

עד כה תוצרים של ניתוח הנתונים נתנו מענה לשאלות שהוגדרו מראש על ידי המבקר, אך בשיטת ניתוח נתונים המבוססת על Big Data, הנתונים עצמם מגדירים את שאלת הביקורת. כלומר, שימוש אפקטיבי ויעיל בכלים מתקדמים לניתוח נתונים במסגרת עבודת הביקורת הפנימית, יאפשר למבקר להעלות תובנות עסקיות, לזהות מגמות בפעילות יחידות הארגון, ולאתר קשרים בין נתונים שלכאורה לא קיימת ביניהם קורלציה. שימוש בכלי ניתוח מתקדמים, כגון שפת R, שפת Python ושילוב עם מתודולוגיות חדשניות כגון Machine Learning ו-Data Science, עשויים לאפשר למבקר הפנימי לקבל מענה לשאלה "למה", בנוסף על השאלות "כמה" ו"מתי".

מה זה BIG DATA?

המונח Big Data ("נתוני עתק") משמש לתיאור כמות גדולה של מידע המגיע ממקורות שונים ומגוונים. ההיקף העצום של המידע וקצב עדכונו דורשים שימוש במתודולוגיות מתקדמות, השונות מהשיטות המסורתיות, לעיבוד הנתונים ולחילוץ משמעות מהם. את המידע הרב יש לשמור, לנהל, לתחזק ולעשות בו שימוש בקלות וביעילות, תוך השקעה של מינימום משאבים.

ניתן לאפיין Big Data לפי חמישה קריטריונים עיקריים:

- **נפח** (volume)

  נפח הנתונים. בעולם ה-Big Data על הארגון לעבד כמויות גדולות של נתונים בלתי מובנים (unstructured). אלה יכולים להיות נתונים של ערך לא ידוע, כגון הזנת נתונים של Twitter, זרימת קליקים בדף אינטרנט או באפליקציה לנייד, או חיישנים. עבור ארגונים מסוימים, נפח הנתונים עשוי להגיע לעשרות טרה-בייט עד מאות פטה-בייט של נתונים.

- **מהירות** (velocity)

  הקצב שבו הנתונים מתקבלים. בדרך כלל, כאשר קצב העברת הנתונים אל מערכות הארגון הוא גבוה, העיבוד נעשה בזמן אמת. לדוגמה, בעת קליטת פעולות משתמשים מאפליקציות או מרשתות חברתיות, קצב זרימת הנתונים אל הארגון הוא קריטי ודורש תגובה בזמן אמת.

- **גיוון** (variety)

  סוגים רבים ומגוונים של נתונים זמינים. סוגי הנתונים המסורתיים הם מובנים (Structured), ומתאימים בצורה מסודרת למסדי נתונים יחסיים (רלציוניים). עידן ה-Big Data הביא עימו סוגי נתונים חדשים במודל לא מובנה (Unstructured). נתונים אלה, העשויים להיות קטעי טקסט, וידאו וקול, דורשים עיבוד מקדים לשם הפקת משמעות מהם ותמיכה במטא-דאטה.

- **ערך** (Value)

  מציאת ערך בנתוני Big Data אינה באה לידי ביטוי בניתוח נתונים בלבד. מדובר בתהליך שלם של חקר נתונים, הדורש חשיבה אנליטית מתקדמת ויכולות טכנולוגיות חדשניות ממשתמשים עסקיים וממנהלים. עליהם לדעת לשאול את השאלות הנכונות, לזהות דפוסי התנהגות בנתונים, להניח הנחות מושכלות ולחזות התנהגות או התרחשות של אירועים.

- **אמינות** (Veracity)

  מידת האמינות של הנתונים. עד כמה ניתן לסמוך על הנתונים שהתקבלו.

אחד מבסיסי הנתונים המרכזיים הקיימים בחברות ובארגונים הוא מחסן הנתונים (Data Warehouse), המאפשר לגורמים שונים בארגון לקבל החלטות על בסיס המידע האגור בו. הנתונים הקיימים במחסן הנתונים נשאבים ממערכות שונות של הארגון, וכוללים מידע רב על פעילותו. הנתונים מאוכסנים בטבלאות, במבנה נתונים יחסי (רלציוני) המאפשר לאתר מידע רלוונטי באמצעות נתוני זיהוי ייחודיים, כגון שדות מפתח וכדומה.

עם זאת, בחברות ובארגונים בעלי היקפי פעילות גדולים, כגון גופים פיננסיים, יש צורך בטכנולוגיות לניהול Big Data שיאפשרו להם לפעול בעולם המייצר וצורך מידע בהיקפים עצומים ביחס לעבר. אחת השיטות להתמודדות עם היקפי מידע עצומים היא שימוש במבנה נתונים המכונה NoSQL, בנוסף על מבנה נתונים יחסי. בסיסי נתונים אלו מכילים מידע בנפח גדול שאינו מאורגן במבנה מוגדר של טבלאות (Unstructured), ויש צורך בכלים ייעודים, כגון Hadoop של חברת Apache, שיאפשרו לעבד ולנתח כמות עצומה של נתונים המגיעים ממקורות רבים, בתצורות שונות ובאיכויות משתנות.

השימוש במודל ה-Unstructured, במקביל למודל הנתונים היחסי, הוא חלק משינוי בתפיסה של מטרות השימוש בניתוח נתונים בביקורת פנימית. אם עד עתה הייעוד העיקרי של ניתוח נתונים היה להסביר מגמות המתרחשות בארגון (Descriptive Analysis) - באמצעות מדידה של ביצועים או בחינה של אופן עמידה ביעדים ובמטרות, אז כעת המגמה היא מעבר למודל של חיזוי ואופטימיזציה (Predictive Analysis). מודל זה בא לידי ביטוי באיתור קשרים בין נתונים שונים, המצביעים על מגמות עתידיות.

סיכום

לסיכום, שימוש בכלי תחקור מתקדמים מאפשר לביקורת הפנימית לבחון בצורה רחבה, יעילה ואפקטיבית את כלל הנתונים העומדים לביקורת, ובכך להשיא ערך רב לארגון. ניתוח Big Data הנמצא במאגרי הארגון יאפשר לביקורת הפנימית להשיא ערך רב אף יותר, תוך הפניית תשומת הלב הארגונית לאזורי סיכון שלא ניתן היה לאתרם קודם לכן. תוצרי ביקורת מן הסוג הזה מעצימים את מעמד הביקורת הפנימית בארגון, ועשויים לבסס את מעמדה כ"יועץ נאמן" (Trusted Advisor) להנהלת ארגון.

ASSURANCE VS RESEARCH

יועץ נאמן? אולי עדיף חוקר נאמן

מאת

יוסי נטוביץ | רו"ח, מנכ"ל טיוב יועצי מערכות בע"מ

האומנם "יועץ נאמן"?

זה למעלה מעשור, במטרה להעלות את ערך הביקורת הפנימית, ראשי המקצוע מעודדים את המבקרים לאמץ את מודל "היועץ הנאמן" ("trusted advisor") - מבקר פנימי "אידיאלי" שבעיקר בזכות יחסי אמון קרובים שהוא משכיל לרקום עם ההנהלה יש לו הרבה השפעה והוא בעל ערך לארגון. לשם כך נדרש המבקר לפתח כישורים "רכים" במישור האישי והבינאישי.

אלא שבמציאות פני הדברים שונים. בסקר שערכה לאחרונה PWC נמצא כי רק 9% מבעלי העניין רואים במבקרים הפנימיים יועץ נאמן. חלק מהסיבה לכך נעוץ בקונפליקט המובנה הקיים בין "מבקר" לבין "יועץ", שכן הצורך לשמור על עצמאות ואובייקטיביות אינו עולה תמיד בקנה אחד עם יחסי הנאמנות הנדרשים מיועץ נאמן. בנוסף, מחקר עכשווי גילה שמרבית המבקרים הפנימיים נדרשים להתמודד באופן יומיומי עם לחצים פוליטיים כבדים. בהתחשב בכך, קצת קשה לצפות מהם לרקום יחסי אמון עם ההנהלה.

יצוין כי תפיסת "היועץ הנאמן" פותחה עוד בשנת 2000 על ידי Galford, Green& Maister בתחום הייעוץ הארגוני כאסטרטגיה שמעניקה ליועץ יתרון כלכלי-תחרותי, ומאז הוצעה גם לבעלי מקצועות נוספים כגון אנשי שיווק וסוכני ביטוח. ספק אם ראוי שגם הביקורת הפנימית תאמץ אסטרטגיה מסחרית כזו.

ההתקדמות הטכנולוגית מאפשרת כיום להציע מודל חלופי מלהיב למבקר הפנימי - מודל "החוקר הנאמן",

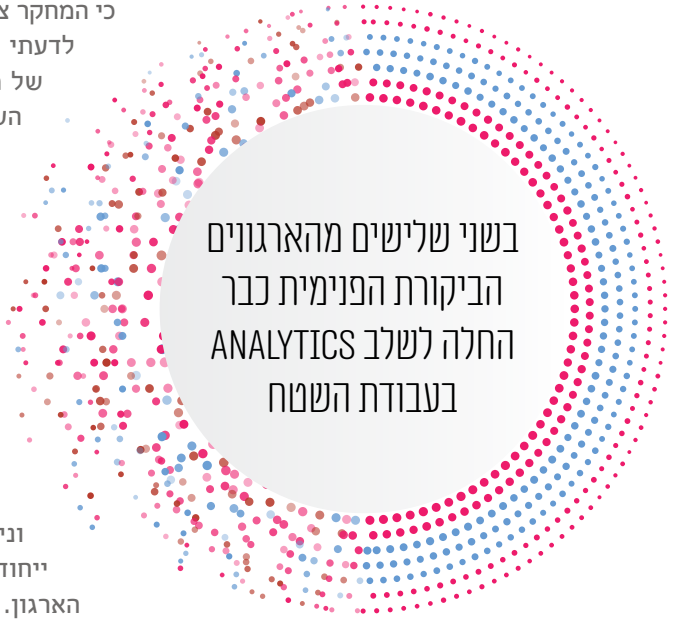
שלדעתי תואם יותר למעמדו ולכישוריו ומעניק לו הזדמנות להתקדם לעידן חדש ומבטיח.

מחקר נתונים

הפריצה של טכנולוגיית המידע בעשור האחרון אפשרה להגדיל את היקף הנתונים הנאגר במערכות הארגוניות, ולפתח שיטות מתקדמות לניתוח נתונים. כתוצאה מכך הביקוש למומחים בתחום ניתוח ומחקר של נתונים מרקיע שחקים. Harvard Business Review וגם Forbes זיהו את תחום מחקר הנתונים Data Science כ"מקצוע הסקסי והחם" ביותר כיום. אתר השמת כוח אדם glassdoor דירג אותו כמקצוע המבוקש ביותר בארה"ב לשנת 2019. אלא שכיום התחום עדיין בהתגבשות - אפילו שם מקצועי מקובל לעוסקים בתחום טרם נקבע, ובמודעות הדרושים פונים אליהם כסטטיסטיקאים, מנתחי נתונים, מדעני נתונים, כורי נתונים וכדומה. כעיסוק רב-תחומי אין עדיין מסלולי הכשרה מסודרים, ותוכניות לימוד שונות מוקמות אד-הוק עבור אוכלוסיות שונות. הביקוש לחוקרי נתונים בארגונים קיים כיום בעיקר בחברות טכנולוגיות מובילות כמו גוגל ופייסבוק, אך צפוי להתחזק גם במגזרים מסורתיים יותר כגון בתעשייה ובקמעונאות, ולחדור גם למגזר הציבורי. לסיכום, התחום אמנם צעיר יחסית, אך יש עדויות שככל שישוכללו כלי הניתוח הממוחשבים ויורחב מעגל העוסקים בו, ילך ויגדל פוטנציאל הערך שלו לארגונים.

המבקר הפנימי כ"חוקר נאמן"

מחקר נתונים מהווה הזדמנות מצוינת לביקורת הפנימית לבסס באמצעותו את הערך שלה לארגון. בשלב זה עוד לא נקבעו מסמרות בנוגע לאיזו יחידה ארגונית אחראית לעריכת מחקר נתונים - האם יחידת ה-IT שהיא בעלת הידע הטכנולוגי, חטיבת הכספים שאמונה על הדיווח הכספי, או גוף עצמאי חדש שבראשו סמנכ"ל? יש גם שטוענים כי המחקר צריך להשתלב כחלק בלתי נפרד מהפעילות בכל יחידות הארגון. לדעתי הביקורת הפנימית עשויה להתאים מאד כגוף הביצועי המרכזי של מחקר הנתונים בארגון, וזאת כפועל יוצא מהייחוד של כישורי העובדים בשילוב מעמד היחידה, בשל הסיבות הבאות:



סיבה ראשונה: מתודולוגיית המחקר אינה זרה למבקר, תהליך הביקורת דומה באופן מפתיע לתהליך מחקרי - גם הוא מבוסס על תהליך שיטתי של איסוף נתונים במטרה לבסס ממצאים שיתנו תשובה לשאלה. כמו במחקר גם ביקורת אוספת נתונים אמפיריים מתוך מאגרי המידע של הארגון ו/או על בסיס תצפיות, בחינת מסמכים, סימולציה של חישובים וכדומה. אמנם הביקורת הפנימית עוסקת בדרך כלל בשאלות מתחום ההבטחה, אך עדיין אותה מתודולוגיה תתאים גם לגבי בחינת שאלות בכלל תחומי ניהול.

סיבה שנייה: לרוב המבקרים הפנימיים יש הכשרה כלכלית וניהולית, והעיסוק בביקורת הפנימית מעניק גם הזדמנות ייחודית להיכרות מעמיקה עם ההיבטים העסקיים השונים של הארגון. היכרות זו מקנה למבקרים יכולת לספק תובנות, מסקנות והמלצות קונקרטיות ומעשיות על סמך ממצאי הניתוח.

סיבה שלישית: בשנים האחרונות מתרחבת המודעות של הביקורת הפנימית לצורך בכלים אנליטיים ממוחשבים מתקדמים, סטטיסטיים ולוגיים, להגברת אפקטיביות הביקורת. יותר מבקרים פנימיים רוכשים ידע בכלים אלה והשימוש בהם הולך וגובר. ניתוח נתונים בביקורת אינו חדש אבל כעת המבקרים נחשפים גם לכלים מתקדמים יותר של אנליטיקה - המאפשרים ויזואליזציה, לימוד מכונה, וכריית מידע. על פי סקר מ-2018, בשני שלישים מהארגונים הביקורת הפנימית כבר החלה לשלב analytics בעבודת השטח, אם כי רובם המכריע בשלב ראשוני.

סיבה רביעית: הגישה לנתונים ארגוניים ממקורות רחבים ככל האפשר מכל זרועות הארגון מקנה יתרון חשוב בעריכת המחקרים. גם כאן המבקר הפנימי במעמד מוביל - אין עוד גורם אחר בארגון הנהנה מגישה כה רחבה לנתונים.

סיבה חמישית ואחרונה: מעמדו של המבקר הפנימי כבלתי תלוי ואובייקטיבי, רלוונטי גם למחקר נתונים. על פי כללי האתיקה המחקרית, חוקר צריך לפעול באובייקטיביות מרבית ואסור לו להימצא בפוזיציה ביחס לנשוא המחקר - דעות קדומות, תלות פיננסית או אג'נדה רעיונית, שכן אלה עלולות באופן טבעי להטות את התוצאות. לדוגמה, החשדנות הקיימת בעולם הרפואה ביחס לאמינות מחקרים הבוחנים אפקטיביות של תרופות, שנערכים במימון חברות הפארמה שמייצרות את התרופות. אי תלות המבקר הפנימי מקנה יתר אמינות ואובייקטיביות לדוחות המחקר שלו, לעומת יחידות אופרטיביות שחוקרות את נתוניהן הן. המבקר הפנימי יכול בהחלט להיחשב ל"חוקר נאמן".

כ"חוקר נאמן" המבקר הפנימי ימשיך לספק שירותי הבטחה, אבל באמצעות אותם כלים וכישורים יוכל להעלות את ערך עבודתו בשירותי מחקר.

לשם כך לא יהיה עליו להתפשר בנושא אי התלות והאובייקטיביות, להיפך - הן מהוות ערך בסיסי גם בביצוע עבודות מחקר.

דוגמאות ליישומי מחקר נתונים בביקורת

מובאות כאן דוגמאות בולטות מתוך עבודות חוקרים באקדמיה שפורסמו בציבור בנושא גילוי הונאות בתחום העסקי. דוגמאות אלה ממחישות את הפוטנציאל העצום של מחקר נתונים להגדלת ערך הביקורת הפנימית לארגונים.

דוגמה 1: BACKDATING בהכרזת אופציות לעובדים

בשנת 2005 פרסם ד"ר דיוויד לי (Lie) מאוניברסיטת איווה מאמר שחשף שערוריית ענק. הוא גילה כי חברות בורסאיות נוהגות לקבוע רטרואקטיבית ובאופן לא חוקי את מועד הכרזת האופציות לעובדים ליום שישיא להם את הרווחים הגבוהים ביותר (Backdating). החברות ניצלו פרצה שהייתה קיימת בחוקי רשות ני"ע האמריקאית (SEC) עד שנת 2002, פרצה שאפשרה להם להודיע לבורסה על חלוקת האופציות בתוך 45 יום, כך שהם יכלו לבחור לעצמם בדיעבד את היום המתאים ביותר מבחינתם בתוך חלון הזמן הנ"ל, כלומר היום שבו ערך המניות הוא הנמוך ביותר.

במחקרו ניתח ד"ר לי שערי המניות של אלפי חברות 30 יום לפני ואחרי מועד ה-0 (יום ההכרזה), וגילה כי מבחינה סטטיסטית יום ההכרזה הוא אכן היום שבו השער היה הנמוך ביותר. התופעה מחריפה עם הזמן ובולטת ביותר בשנים 1999-2002 (תרשים 1).

בעקבות המחקר פיתחה ה- SEC בחקירה שהובילה לתשלום קנסות ענק של חברות שנתפסו בביצוע Backdating, ובין היתר גם לבריחתו הממושכת של הישראלי מייסד קומברס, קובי אלכסנדר, לנמיביה. לאחר שחזר לארה"ב הורשע אלכסנדר והוטל עליו עונש של שנתיים וחצי מאסר וקנס של עשרות מיליוני דולרים.

תרשים 1 - תשואות מניות לפני ואחרי יום הכרזת האופציות

דוגמה 2 – רמאויות במבחני המיצ"ב האמריקאיים

מערכת מבחני המיצ"ב הנהוגה בארה"ב מודדת את הישגי תלמידי בתי הספר היסודי, ובהתאם לכך מעריכה את תפקוד בית הספר ומתגמלת או מענישה אותו בתקציבי השנים הבאות. בשנת 2003 פרסמו חוקרי הכלכלה Jacob and Levitt מחקר שהראה כי בכ-5% מן הכיתות המורים מרמים ומתקנים באופן שיטתי את תשובות התלמידים כדי שהערכת בית הספר שלהם לא תיפגע.

החוקרים הניחו כי מורים שמרמים יתקנו באופן חוזר ונשנה את התשובות כך שתהיינה תשובות זהות לתלמידים בכיתה לכל השאלות או לחלקן. לכן הם הפעילו אלגוריתם ממוחשב לזיהוי תבניות קבועות בגיליונות התשובות של התלמידים בכל כיתה.

בתרשים 2 מוצגים גיליונות תשובות של כיתה לדוגמה שבה יש חשד לתרמית. כל שורה מציגה גיליון תשובות של תלמיד אחד. המבחן נערך בשיטת רב ברירה - ספרות מייצגות תשובות נכונות לשאלה, ואותיות מייצגות תשובות שגויות. בתרשים ניתן להיווכח כי קיימות בגיליונות תבניות חוזרות ונשנות של תשובות שאינן מתקבלות כאקראיות (מוקפות בקו), ומכאן עולה חשד של זיוף התשובות על ידי המורה האחראי.

כדי לאושש את המסקנה נערכו במקרים החשודים בדיקות נוספות, בין היתר השוואה לציונים בשנה העוקבת ובשנה הקודמת. בדוגמה בתרשים 2 ניתן לראות כי הציונים היו נמוכים יותר ביחס למבחן. בנוסף נערכו מבחנים חוזרים, הפעם בנוכחות מורה שלא מבית הספר הנבדק, ואז נמצא פער משמעותי מול המבחן החשוד. תוצאות המחקר הובילו, מלבד ענישה של המורים שסרחו, גם לשינוי מהותי בתהליך הערכת בתי הספר בארה"ב.

Student Answer Strings (each row represents one student's answers)	Student Test Scores		
	Year t-1	Year t	Year t+1
Suspected Cheating Classroom			
112A4A342CB214D0012ACD24A3A12DADBCB4A0000000	1.9	5.3	4.4
1B2A34D4AC42D23B141ACD24A3A12DADBCB4A2134141	4.3	5.6	4.3
DB2A3AD1ACBDDA212B1ACD24A3A12DADBCB400000000	3.0	6.5	5.1
1142340C2CBDDADB4B1ACD24A3A12DADBCB43D133BC4	3.6	6.3	4.9
D43A3A24ACB1D32B412ACD24A3A12DADBCB422143BC0	5.2	5.9	4.9
D43AB4D1AC3DD43421240D24A3A12DADBCB400000000	4.8	5.3	3.6
DBA2BA21AC3D2AD3C4C4CD40A3A12DADBCB400000000	1.9	6.1	3.6
D0AA4ADC4CBD24DBCB2A1110A3A12DADBCB400000000	3.3	6.3	6.2
144A3ADC4CBDDADBCBC2C2CC43A12DADBCB4211AB343	3.0	6.8	4.9
D43ABA3CACBDDADBCBCA42C2A3A12DADBCB42344B3CB	4.8	7.1	6.6
214AB4DC4CBDD31B1B2213C4AD412DADBCB4ADB00000	3.6	6.1	4.3
313A3AD1AC3D2A23431223C000C12DADBCB400000000	3.8	4.7	5.1
D4AAB2124CBDDADBCB1A42CCA3412DADBCB423134BC1	5.5	6.6	7.7
3B3AB4D14C3D2AD4CBCAC1C003A12DADBCB4ADB40000	3.0	6.5	6.6
DBAAB3DCACB1DADBC42AC2CC31C12DADBCB4ADB40000	3.8	7.1	5.6
DB223A24ACB11A3B24CACD12A2412DADBCB4ADB4B300	4.9	6.5	5.8
D122BA2CACBD1A13211A2D02A3A12D0DBCB4ADB4B3C0	3.6	6.1	6.2
1423B4D4A23D2413141323412 3A243A2413A21441343	4.9	2.5	5.6
DB4ABADCACB1DAD3141AC212A3A1C3A144BA2DB41B43	5.9	6.5	7.7
D82A33DCACBD32D313C21142323CC3000000000000000	3.8	4.4	5.6
1B33B4D4A2B1DADBC3CA22C0000000000000000000000	5.0	4.4	7.2
D12443D43232D3233C213C22D2C23234C332DB4B300	3.3	3.8	3.6
D4A2341CACBDDAD3142A2344A2AC23421C00ADB4B3CB	6.4	5.9	6.2
	4.1	5.8	5.5

תרשים 2 - גיליון תשובות עם תרמית

גישור על פערי ידע

למרות כל האמור לעיל, איני סבור שהכשרת המבקר הפנימי המקובלת ונהוגה כיום מספקת גם לביצוע עבודת המחקר. לשם כך הביקורת הפנימית תידרש להשלים את פערי הידע ולחזק את המיומנות בתחום טכנולוגיות המידע. עליה להגביר את שיתוף הפעולה עם אנשי ה-IT בארגון, ולהתמחות בשימוש מושכל בכלי אנליטיקה מתקדמים, כריית נתונים, ויזואליזציה ולימוד מכונה. כאמור, כבר כיום הביקורת הפנימית צועדת בכיוון זה גם בשירותי ההבטחה, אבל כניסה לשירות המחקר תדרוש מאמץ מרוכז ומהיר יותר.

בנוסף, רמת המיומנות הסטטיסטית בקרב מבקרים פנימיים תידרש להשתדרג. על המבקרים יהיה להעמיק את הידע בשיטות לבניית מודלים סטטיסטיים ולניתוח נתונים, ובכלל זה הרצת רגרסיות, קורלציות וניתוחי מובהקות.

לבסוף, המבקרים יידרשו להרחיב את הפריזמה שדרכה הם מביטים בארגון, ובין היתר:

- להתייחס בעבודה למכלול היבטים עסקיים, להיות ממוקדי ערך ולא רק ממוקדי סיכונים.
- לבצע הערכות, תחזיות ומגמות לעתיד ולא רק לדווח על העבר.
- לספק תובנות והמלצות ברמה העסקית-האסטרטגית ולא רק ברמה התפעולית-בקרתית.

סיכום

הביקורת הפנימית, שמנסה זה שנים לחזק את מעמדה ולהשיא ערך לארגון, ניצבת לפני הזדמנות להשתלב במחקר נתונים ארגוני - תחום חדש ומוערך המתפתח במהירות.

המבקרים הפנימיים מצוידים לשם כך במרב הכישורים, ככל הנראה יותר מכל גורם אחר בארגון, אבל אם לא ייערכו במועד הם יגלו עד מהרה כי גורמים אחרים בארגון שיבצעו מחקר נתונים יספקו ערך להנהלה במקומם ויותירו את עבודתם המסורתית נטולת ערך ממשי. לכן על ראשי המקצוע להיערך בתוכניות מתאימות להגברת המודעות ולהכשרת המבקרים הפנימיים במחקר נתונים, ובכך לשפר באופן דרמטי את מעמדה וערכה של יחידת הביקורת הפנימית העתידית.

שימוש בכלים טכנולוגיים וחדשניים בביקורת הפנימית

IT'S A MUST

מאת

אנה רוזנברג שפירו | רו"ח, מוסמכת בפיתוח תוכנה, סגן המבקר הפנימי של קבוצת כלל ביטוח

החברות העסקיות הגדולות, ובמיוחד אלו הפועלות במגזר הפיננסי ומנהלות כספים של אחרים, פועלות בסביבה עסקית ורגולטורית של שינויים משמעותיים שמקורם בשלוש מגמות מרכזיות:

מיכון תהליכים;

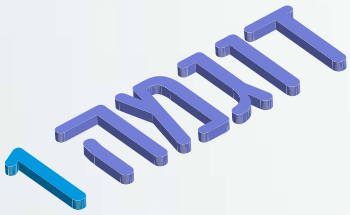
דיגיטציה;

קבלת החלטות על סמך ניתוח נתונים בכלים סטטיסטיים מתקדמים.

לצד השינויים האמורים והסביבה הדינמית שבה פועלות החברות, תפקיד הביקורת הפנימית נותר קבוע: לבדוק את כל התהליכים בחברה לפי תוכנית רב-שנתית מבוססת סיכונים, תוך שימוש בכלי ביקורת מתאימים שיאפשרו מתן חוות דעת על כל תהליך, ובמידת הצורך מתן המלצות אפקטיביות לשיפור התהליך. לפיכך, כדי שהביקורת הפנימית תוכל לבצע את תפקידה באופן אפקטיבי בתוך סביבה עסקית ורגולטורית משתנה, היא נדרשת להפעיל כלי ביקורת מתקדמים מגוונים, לרבות הפעלת כלים טכנולוגיים וסטטיסטיים חדשניים.

במאמר זה יוצגו שתי דוגמאות הממחישות את הצורך של יחידות ביקורת פנימית להפעיל כלי ביקורת מתקדמים וחדשניים לצורך בדיקת תהליכים בחברה, וכן יובאו דגשים מסוימים בדבר אופן השימוש באותם כלי ביקורת.

בדיקה טכנולוגית של נאותות מנגנון חישוב במערכת מידע תפעולית:



הדוגמה הראשונה, תתייחס לבדיקה של תהליך תפעולי המבוסס על מנגנון חישוב במערכת: תהליך גביית ריבית על הלוואה המבוסס על מנגנון לחישוב הסכום לגבייה במערכת. לצורך הדוגמה, נניח כי במסגרת הסקר המקדים שביצעה הביקורת עלו הפרטים הבאים: חישוב הסכום לגבייה מבוצע באמצעות מנגנון מיכוני שפותח בשנה האחרונה; החישוב מבוצע עבור כ-800,000 הלוואות; אופן חישוב הריבית משתנה בין סוגי הלוואות שונים; החברה מבצעת בקרת סבירות חודשית של סך ההכנסה מריבית ביחס לחודש קודם.

להלן טבלה הממחישה את ההבדלים בביצוע הבדיקה בין יחידת ביקורת פנימית שעושה שימוש בכלי ביקורת מוגבלים לבין יחידת ביקורת פנימית שמבצעת את הבדיקה תוך הפעלת כלי ביקורת טכנולוגיים מתקדמים.

	ביקורת עם כלים מוגבלים	ביקורת עם כלים טכנולוגיים
סוג הבדיקה	בדיקת נאותות חישוב הריבית לגבי מדגם אקראי של 100 הלוואות מסוגים שונים.	בדיקה ממוכנת של שלמות ודיוק מנגנון חישוב הריבית לכל אוכלוסיית ההלוואות.
ממצאים אפשריים	חמישה מקרים שבהם בוצע חישוב שגוי, מתוך 100 המקרים שנכללו בבדיקה.	ל-30% מההלוואות כלל לא מבוצעת גביית ריבית - בעיית שלמות הנתונים. ל-20% מההלוואות הריבית חושבה בצורה שגויה - בעיית דיוק הנתונים. בקרת הסבירות שביצעה החברה לא העלתה את הממצאים האמורים לגבי בעיות השלמות והדיוק.
המלצות רלוונטיות	לתקן את התקלות במנגנון שגרמו לחישוב השגוי במקרים שאותרו.	לבצע תיקון של המנגנון הממוכן. להטמיע בדיקות ממוכנות תקופתיות להבטחת נאותות מנגנון חישוב סכום הריבית לגבייה. להטמיע בדיקות ממוכנות לגבי מנגנוני חישוב מרכזיים נוספים במערכות התפעוליות שבהן לא קיימות בדיקות מסוג זה (ככל שנדרש, יש לבצע מיפוי של החישובים המרכזיים ולקבוע תוכנית רב-שנתית להטמעת הבדיקות הממוכנות).

בדיקה שבה נעשה שימוש בכלי ביקורת מוגבלים אינה מאפשרת מתן חוות דעת על התהליך

מהדוגמה לעיל ניתן לראות כי בדיקה שבה נעשה שימוש בכלי ביקורת מוגבלים אינה מאפשרת מתן חוות דעת על התהליך, שכן ממצא שלפיו קיימים חמישה מקרים שגויים מתוך 100 לא ניתן לגבש מסקנה לגבי התקינות של המנגנון לחישוב הריבית שעליו מבוסס התהליך - האם מדובר במנגנון "נאות" עם תקלות נקודתיות או שמדובר במנגנון שאינו תקין? יצוין כי מדגם ידני של כ-0.01% מהאוכלוסייה לא יכול ללמד באופן מיטבי על האוכלוסייה ולכן הבדיקה הידנית הראתה תוצאה של 5% שגויים, בעוד שהבדיקה הממוכנת שמלמדת על כל האוכלוסייה הראתה תוצאה של 20% שגויים בדיוק. כמו כן, המלצה לתקן את התקלות שאותרו משפרת את התהליך רק באופן חלקי, מאחר שיישום ההמלצה יביא רק לתיקון התקלות הנקודתיות שאותרו. לעומת זאת,

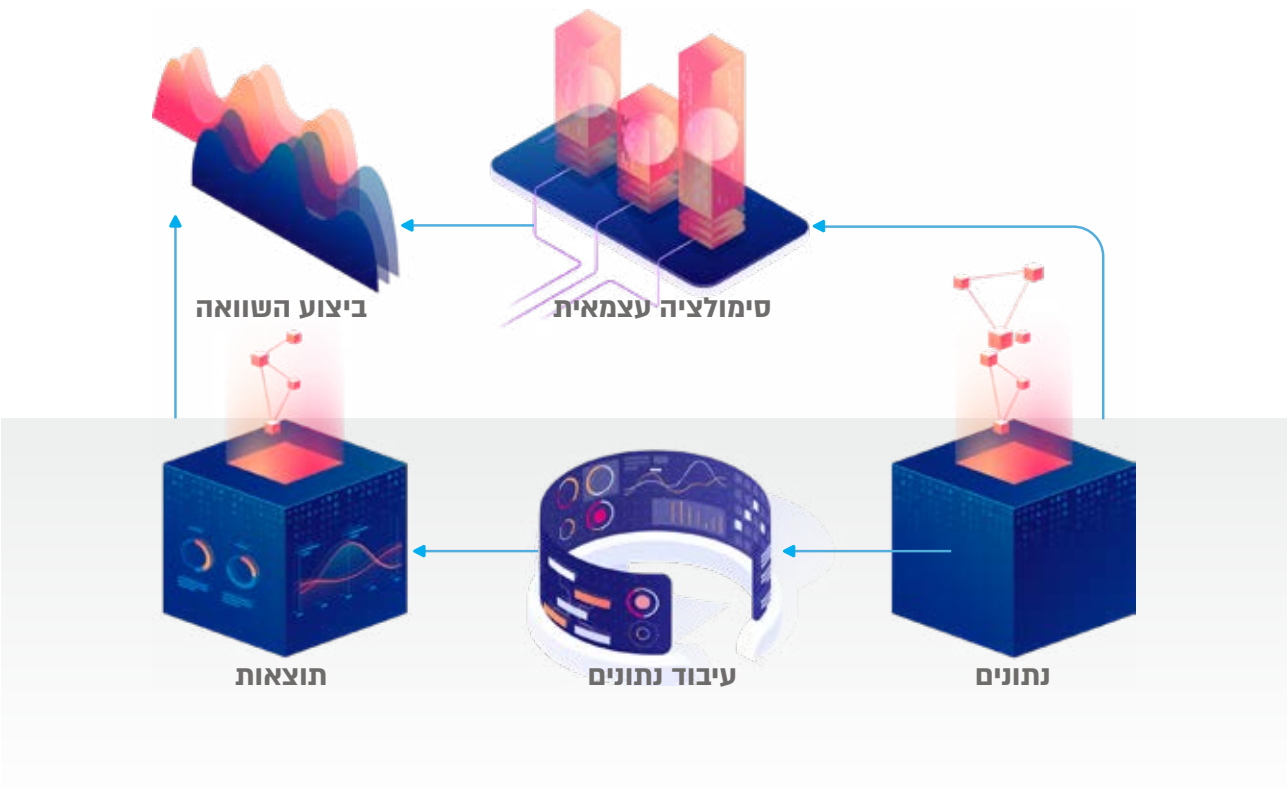
בבדיקה ממוכנת תוך שימוש בכלים טכנולוגיים, ניתן לתת חוות דעת שלפיה התהליך אינו נאות מאחר שהוא מבוסס על מנגנון מיכוני שאינו תקין,

כאשר גם הבקרה המבוצעת בתהליך כלל אינה אפקטיבית. כמו כן, יישום ההמלצות לתיקון המנגנון ולהטמעת בדיקות ממוכנות בתהליך הנבדק ובתהליכים רלוונטיים אחרים נוספים, יוביל לשיפור התהליך הנבדק ולבחינת הצורך בביצוע שיפור בתהליכים רלוונטיים נוספים בחברה.

בדיקה ממוכנת של מנגנון חישובי במערכת כפי שמובאת בדוגמה לעיל, מורכבת משני חלקים: בדיקת שלמות הנתונים ובדיקת דיוק הנתונים. בדיקת שלמות משמעה בדיקה כי החישוב מבוצע על כל האוכלוסייה הרלוונטית ועל האוכלוסייה הרלוונטית בלבד. בדיקת השלמות מבוצעת על ידי הביקורת באמצעות גיבוש עצמאי ובלתי תלוי של האוכלוסייה שעליה יש לבצע את החישוב במנגנון לפי ההגדרה העסקית/הרגולטורית והשוואת האוכלוסייה שגובשה על ידי הביקורת לאוכלוסייה שעליה מבוצע החישוב בפועל במערכת.

בדיקת דיוק משמעה בדיקה כי ביחס לכל מופע הכלול באוכלוסייה הרלוונטית, החישוב עצמו מבוצע במערכת באופן מדויק בהתאם להגדרה העסקית/הרגולטורית שנקבעה לצורך ביצוע החישוב. בדיקת הדיוק מבוצעת על ידי הביקורת בדרך של ביצוע חישוב עצמאי ובלתי תלוי (מחוץ למנגנון שבמערכת) של הנתון שמחשב המנגנון, והשוואת תוצאת החישוב העצמאי של הביקורת לתוצאה של החישוב כפי שבוצעה במנגנון של המערכת, זאת לגבי כל האוכלוסייה הרלוונטית שעליה מבוצע החישוב במנגנון.

להלן תרשים המתאר את האופן שבו מבוצעת בדיקה טכנולוגית מתקדמת של נאותות מנגנון חישוב מערכת:



לצורך ביצוע בדיקה טכנולוגית מתקדמת של מנגנון חישוב במערכת יש לבצע שליפה עצמאית ובלתי תלויה של נתונים מהמערכת, אולם בהתאם לנסיבות ובמקרים המתאימים, הביקורת יכולה להסתפק בשיטות אחרות לשליפת הנתונים כדי לבצע את הבדיקה באופן ממוכן.

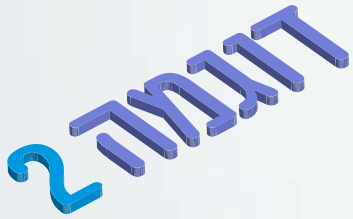
להלן תיאור שלוש שיטות מרכזיות שבהן ניתן לבצע שליפה של נתונים, ופירוט בדבר היתרונות והחסרונות של כל שיטה:

1. שליפה עצמאית ובלתי תלויה מבסיס הנתונים של המערכת באמצעות כלים טכנולוגיים. היתרונות בשיטה זו הם אי התלות של המבקר בביצוע הבדיקה, מאחר שהוא אינו נסמך על הגורם המבוקר לצורך קבלת המידע, וכן האפשרות של המבקר לקבל את כל הנתונים הנדרשים לו לצורך ביצוע הבדיקה, זאת מכיוון שהשליפה מבוצעת ישירות מהמערכת שבה מבוצע החישוב. החיסרון בשיטה זו הוא הצורך במשאבים ייחודיים - מבקר בעל יכולות טכנולוגיות, ופרק זמן ניכר שנדרש ללימוד הטבלאות הקיימות בבסיס הנתונים של המערכת, לרבות המיקום של כל נתון שנדרש לבדיקה בכל טבלה.

2. שליפה ממערכת BI (בינה עסקית) ארגונית - היתרון בשיטה זו הוא שלהבדיל משליפה מבסיס הנתונים של המערכת, שליפה מ-BI היא פעולה פשוטה יחסית שיכולה להתבצע על ידי כל מבקר ומשך זמן הלימוד הנדרש לביצוע השליפה קצר יחסית. החיסרון בשיטה זו הוא שכלי ה-BI בחברה מיועדים לשליפה של דוחות ניהוליים ואינם מותאמים לשליפות המיועדות לביצוע בדיקות, ועל כן גם המידע שניתן לשליפה באמצעות כלי ה-BI הוא בדרך כלל מידע מוגבל. חיסרון נוסף: המידע הקיים ב-BI מהימן פחות מאשר המידע הקיים בבסיס הנתונים במערכת, מאחר שהשליפות מה-BI אינן מבוצעות מבסיס הנתונים של המערכת אלא מבסיס נתונים אחר וייעודי ל-BI. לבסיס הזה מועברים הנתונים הרלוונטיים באמצעות ממשק מבסיס הנתונים של המערכת, ויש סיכון שהנתונים לא יעברו במלואם בממשק או שלא יעברו בצורה מדויקת.

3. קבלת שליפה מהגורם המבוקר. החיסרון המרכזי בשיטה זו הוא ההסתמכות על הגורם המבוקר, שמקשה על האפשרות לאתגר את שלמות המנגנון המיכוני, זאת מכיוון שקיים חשש שהשליפה שהועברה אל הביקורת אינה כוללת את כל הנתונים. לדוגמה, ייתכן מצב שבו הביקורת לא תוכל לאתר תקלה במנגנון החישוב, שכן אותו גורם ששלף את הנתונים עבור הביקורת התבסס על אותה שליפה שמשמשת להעברת הנתונים אל המנגנון - שליפה שיש בה תקלה לעניין שלמות הנתונים. במקרה כזה, במטרה לאתגר בכל זאת את שלמות הנתונים המועברים למנגנון, ניתן במקרים מסוימים לבצע הצלבה בין הנתונים ששימשו לצורך החישוב במנגנון שנבדק לבין נתונים שנשלפו ממערכת אחרת שגם היא ניזונה מאותם נתונים (לדוגמא: מערכת דיווח כספי, מערכת תשלומים וכו'). ההנחה העומדת בבסיס בדיקה זו היא שלא סביר שתהיה תקלה דומה הן בשליפת הנתונים המבוצעת כחלק ממנגנון החישובי הנבדק והן בשליפה המבוצעת כחלק ממנגנון נפרד המשמש להעברת נתונים למערכת אחרת.

בדיקה של תהליך קבלת החלטה תוך שימוש בכלי ניתוח נתונים מבוססי מודלים סטטיסטיים מתקדמים:



דוגמה שנייה, תתייחס לבדיקה של נאותות תהליך קבלת ההחלטה של חברת ביטוח להגדיל מכירת פוליסות ביטוח חיים למבוטחים שגילם עולה על 40 שנה.

לצורך הדוגמה, נניח כי במסגרת הסקר המקדים שביצעה הביקורת עלו הפרטים הבאים: ההחלטה של החברה התקבלה על סמך מודל חיזוי סטטיסטי מבוסס Machine Learning שהראה כי גידול במכירת פוליסות ביטוח חיים למבוטחים שגילם עולה על 40 יביא לגידול של 20% ברווח. המודל של החברה התייחס לשני פרמטרים: גיל המבוטח וגובה הכיסוי הביטוחי.

להלן טבלה הממחישה את ההבדלים בביצוע הבדיקה בין יחידת ביקורת פנימית שעושה שימוש בכלי ביקורת מוגבלים לבין יחידת ביקורת פנימית שמבצעת את הבדיקה תוך הפעלת כלי ביקורת מתקדמים.

	ביקורת עם כלים מוגבלים	ביקורת עם כלים טכנולוגיים
סוג הבדיקה	סקירת הגדרות המודל שנעשה בו שימוש. סקירת תוצאות המודל, לרבות דיוק המודל.	בדיקה עצמאית של דיוק תוצאות המודל, על בסיס מדדים לבחינת רמת מובהקות סטטיסטית אחרים מאלו שהשתמשה בהם החברה. פיתוח מודל סטטיסטי עצמאי מבוסס Machine Leraning המתייחס גם לפרמטרים נוספים שהחברה לא כללה במודל (לדוגמה: סכום הפרמיה לתשלום ומין המבוטח).
ממצאים אפשריים	הגדרות המודל סבירות ותוצאות המודל תומכות בהחלטה שהתקבלה. שיעור הדיוק של המודל 50% בלבד. במודל לא הוכללו פרמטרים נוספים רלוונטיים כדוגמת מין וגובה פרמיה.	שיעור הדיוק של המודל לפי מדד דיוק שבו השתמשה הביקורת הוא 30% בלבד, ולפי המדד של החברה 50%. לכן עולה השאלה האם תוצאות המודל יכולות להוות בסיס מספק לקבלת החלטה. הוספת שני הפרמטרים למודל (סכום הפרמיה לתשלום ומין המבוטח) הביאה לשיפור משמעותי בשיעור דיוק המודל והעמידה אותו על 70%. מניתוחים שבוצעו על פי המודל שפיתחה הביקורת, עולה למשל כי מכירה של פוליסות ביטוח חיים לנשים שגילן עולה על 40 תביא לעלייה של 50% ברווח (בעוד שהחברה כאמור לא עשתה הבחנה בין המינים והעריכה שיעור גידול של 30% בלבד ברווח).
המלצות רלוונטיות	לשקול הכללת פרמטרים נוספים במודל, שייתכן שישפרו גם את דיוק המודל	לשקול פיתוח מודל עדכני שיתבסס על פרמטרים נוספים ושהיה לו שיעור דיוק גבוה יותר. לשקול ביצוע בחינה מחודשת של החלטת החברה על סמך תוצאות מודל עדכני.

מהדוגמה לעיל ניתן לראות כי בדיקה עצמאית של המודל ואף פיתוח מודל עצמאי, מאפשרים לביקורת לתת חוות דעת שלפיה יש לבצע שיפורים בתהליך - פיתוח מודל מקיף ומדויק יותר ובחינה מחדש של ההחלטה שהתקבלה. לעומת זאת, סקירה בלבד של המודל אינה מאפשרת לתת חוות דעת של ממש בדבר נאותות המודל, ולפיכך גם אינה מאפשרת לאתגר בצורה משמעותית את תהליך קבלת ההחלטה של החברה.

להלן תרשים המתאר תהליך של ניתוח מידע באמצעות מודלים סטטיסטיים מתקדמים שניתן לשלב גם בעבודת הביקורת:

הדוגמה שהובאה לעיל מראה

ששימוש של הביקורת הפנימית בכלים של ניתוח מידע באמצעות מודלים סטטיסטיים מתקדמים, עשוי לשמש את הביקורת הפנימית לצורך אתגור תהליך קבלת החלטות של החברה

המבוססות על מודלים מסוג זה שמופעלים על ידי החברה עצמה. עם זאת, הביקורת הפנימית יכולה אף לשלב כלי ניתוח מתקדמים כאלה (כגון Machine Learning) גם ככלי ביקורת תומכים בביצוע בדיקות על תהליכים עסקיים ולצורך תמיכה בחוות דעת של הביקורת הפנימית לביצוע שיפורים באותם תהליכים עסקיים. למשל, בדרך של איתור מגמות שליליות או אנומליות בנתונים שעשויות להצביע על בעיה בתהליך או איתור מגמות חיוביות שדווקא עשויות להצביע על כך שהתהליך מבוצע באופן נאות.

לסיכום

תפקידה של הביקורת הפנימית הוא לבצע בדיקות לצורך מתן חוות דעת בדבר נאותות כל אחד מהתהליכים המבוצעים על ידי החברה, ובמידת הצורך מתן המלצות אפקטיביות לשיפור התהליכים. אף שתפקידה של הביקורת הפנימית לא השתנה עם השנים, בשל שינויים משמעותיים שחלו בסביבה העסקית והרגולטורית שבה פועלות החברות העסקיות, ובמיוחד מיכון תהליכים, דיגיטציה וקבלת החלטות על בסיס ניתוחים סטטיסטיים מתקדמים, הביקורת הפנימית חייבת להתאים עצמה ולהפעיל כלי ביקורת חדשניים כדי להישאר רלוונטית וכדי להיות אפקטיבית. במקרים מסוימים הביקורת הפנימית אף צריכה לשקול אם להשתמש בניתוחי נתונים מבוססי מודלים סטטיסטיים מתקדמים.

מי הזיז את המשרה שלי

האם ידע במערכות מידע הכרחי בארגז הכלים של המבקר הפנימי?

מאת

אלון עמית | MA, CIA, CISA, QAR - נשיא ISACA ישראל, מנכ"ל רווה רביד שירותי ביקורת פנימית בע"מ

רמי ניסן | CISA, CRISC, MBA - משנה לנשיא ISACA ישראל, מנהל תחום ממשל IT ודיגיטל ב- BDO ישראל

בשנים האחרונות מנקרות בראשנו השאלות הבאות: האם ידע במערכות מידע הכרחי בארגז הכלים של המבקר הפנימי? האם ידע במערכות מידע באמת מסייע לביקורת הפנימית בארגון להיות מועילה יותר, רלוונטית יותר, כזו שתדע להתייחס לתהליך העסקי ולטכנולוגיה ביחד, כמקשה אחת?

לדעתנו התשובה היא כן. ידע במערכות מידע חייב להיות בארגז הכלים של כל מבקר פנימי, ללא קשר לארגון שהוא מבקר, לידע ולניסיון שרכש עד כה, ולנושאים שיידרש לבקר מהיום והלאה.

אז איך ומדוע הגענו למסקנה זו?

העידן הדיגיטלי שאנו חווים כיום - המהפכה התעשייתית הרביעית - מאופיין בשילוב מואץ של טכנולוגיות בתהליכים העסקיים, עד כדי טשטוש הגבולות שבין העולם הפיזי לעולם הדיגיטלי. בין הטכנולוגיות שהתפתחו באופן מואץ בעשור האחרון: הסלולר, הענן ויכולות האחסון, הרשתות החברתיות, ה-IOT, האנליטיקה, האוטומציה וה- AI. כל אחת מהן בנפרד, ובמיוחד השילוב ביניהן, הביאו לכך שאין תהליכים עסקיים שאינם מבוססי IT.

בה-בעת, ותוך ניצול אותן טכנולוגיות בדיוק, איום הסייבר גדל ומתעצם, עד שכמעט שאין ארגון שלא חווה התקפת סייבר כלשהי בשנים האחרונות.

לכן יש לשאול:

האם הכלים הקיימים כיום בארגז הכלים של המבקר הפנימי מספיקים על מנת להתמודד עם הצונאמי הטכנולוגי שכולנו חווים?

האם ניתן בכלל לבקר תהליך או שירות עסקי כלשהו בלי להתייחס לטכנולוגיה הסובבת אותו? האם הרקע הטכנולוגי שיש לרוב המבקרים הפנימיים כיום הוא מספק?

האם ההחלטות של המבקר הפנימי הראשי, הן ביחס לנושאי הביקורת והן ביחס לממצאים/מסקנות/המלצות היו שונות אם היו לו רקע והבנה ברמה גבוהה יותר?

בהתאם, ועל מנת שהביקורת הפנימית תישאר רלוונטית, חשוב ואף נדרש לעשות את ההתאמות הנדרשות לארגז הכלים של המבקר הפנימי. סקר שבוצע על ידי IIA העולמי כבר בשנת 2012, הראה שמתוך חמש המיומנויות הנדרשות למבקר פנימי, שתיים הן: ידע כללי במערכות מידע וניתוח נתונים.

העולם משתנה, ומשתנה באופן מהיר יותר מהרגיל. בארגז הכלים של המבקר הפנימי נרצה למצוא כלים רבים שבעבר לא היינו מצפים למצוא.

על כן, כל מבקר נדרש לשאול את עצמו את השאלות הבאות:

האם קיים תהליך עסקי שיכול לפעול ללא מערכות מידע?

האם אני, כמבקר פנימי, יכול לבצע ביקורת על תהליך עסקי ללא היכרות מעמיקה עם מערכות המידע המאפשרות או המשולבות בתהליך העסקי?

האם בארגז הכלים שלי יש את הכלים הנדרשים (ידע, מתודולוגיה, ניסיון וכו') כדי לבצע ביקורת על התהליך העסקי, כולל על מערכות המידע המאפשרות אותו? אם לא, האם הגבינה שלי, סליחה, המשרה שלי, נמצאת בסכנה?

סקר שבוצע על ידי IIA העולמי, הראה שמתוך חמש המיומנויות הנדרשות למבקר פנימי, שתיים הן: ידע כללי במערכות מידע וניתוח נתונים.

להלן כמה דוגמאות לשאלות בסיסיות, שידע במערכות מידע עשוי לתת להן פתרון:

האם מערכות המידע הקיימות מספקות את צורכי הארגון ותומכות בתהליכים העסקיים בהיבטים של יעילות ומועילות?

מהי איכות המידע המשמש את התהליכים העסקיים?

האם הארגון מציית כראוי לחוק הגנת הפרטיות ולתקנות הנלוות?

האם הארגון מציית לחוקים, לתקנות ולסטנדרטים המתייחסים לאופן מתן השירות ללקוחות, לתקשורת עם עסקים אחרים וכדומה?

האם הארגון שלי מוגן מפני מתקפות סייבר חיצוניות ואירועי אבטחת מידע פנימיים?

האם הבקרות הקיימות במערכות המידע נאותות?

האם אני בודק במהלך הביקורת רק מדגם ולא את כל האוכלוסייה?

האם אני משתמש בכלי CAAT שיאפשרו להגיע לתובנות שאינן אפשריות ללא שימוש בכלים כאלה? מהם בכלל כלי CAAT? אם אתם לא יודעים את התשובה לשאלה הזאת, הרי שבוודאי חסר לכם ידע במערכות מידע ובביקורת מערכות מידע.

האם לארגון שלי יש יכולת המשכיות עסקית במקרה של תקלה/אסון?

האם הארגון שלי נסמך על מערכות מידע הנמצאות בענן? אם כן, מה המשמעות לכך? האם יש לכך השלכה על אופן ביצוע הביקורת? איזה ידע נדרש על מנת לבצע ביקורת בתחום הזה?

האם קיימות חשיפות כתוצאה משימוש באתרי אינטרנט, אפליקציות, רשתות חברתיות וכדומה?

האם הארגון ממצה כראוי את היכולות הטכנולוגיות העכשוויות כדי לתת מענה הולם לתהליכים העסקיים הקיימים? האם ניתן לשפר את התהליכים העסקיים הקיימים או לייצר תהליכים חדשים תוך שימוש בטכנולוגיות חדשות?

התעלמות מנושאים אלה או מחלקם במהלך ביצוע ביקורת בשל חוסר ידע של המבקר בעולמות הללו, עלולה לגרום לכך שסיכונים מתהווים משמעותיים בפעילות החברה לא יכוסו על ידי הביקורת פנימית. הדבר בולט לא פחות בתחום ההונאות והמעילות.

לצערנו, נראה שעולם ההונאות והמעילות לא נעלם. להיפך -

ההתקדמות בתחום מערכות המידע מאפשרת תסריטים חדשים של הונאות ומעילות שלא היו קיימים עד כה.

מתודולוגיות ניהול סיכונים מתקדמות שמות את הדגש על איתור הסיכונים הקיימים בעולם ההונאות והמעילות ועל הבקרות הממוחשבות שניתן להפעיל בתהליכי העבודה הרלוונטיים.

על סמך ניסיוננו (כולל מקרים שבהם טיפלנו באופן אישי במהלך השנים), מקרים רבים של הונאות ומעילות לא היו מתגלים ללא ידע והבנה של המבקרים הפנימיים במערכות המידע של הארגון. במקרים רבים לא ניתן היה לכמת את היקף ההונאות/מעילות ללא היכולת להשתמש בכלי ביקורת ממוחשבים.

האם יש לנו את הידע המתאים במערכות מידע כדי לאתר ולכמת הונאות ומעילות?

מקרים רבים של הונאות נובעים מניצול חשיפות בהגנת הסייבר בארגון. במסמך שפרסמה רשות ניירות הערך האמריקאית באוקטובר 2018 דווח כי חברות וארגונים הפסידו למעלה מ-5 מיליארד דולר מאז שנת 2013 (כ-675 מיליון דולר בשנת 2017 בלבד) כתוצאה מהונאות במרחב הסייבר. אנחנו כמבקרים נדרשים להכיר את הסיכונים הללו - סיכונים שכבר התממשו בפועל ואינם תיאורטיים בלבד, ולהמליץ על בקרות בסיסיות שהארגון צריך להפעיל בעולמות הללו.

שאלות קריירה – שאלו את עצמכם

האם אוכל להתקדם לשלבים הבאים בקריירה כמבקר ללא יכולת לבצע ביקורת במערכות מידע?

האם אוכל לשמור על אזור הנוחות שלי ועל המשרה הנוכחית שלי ללא ידע וכלים בסיסיים לביצוע ביקורת במערכות מידע? לעניות דעתנו, מבקר שלא יתאים את עצמו למציאות המשתנה עלול לגלות כי נותר לא רלוונטי.

נשאלת השאלה: **מה** המבקרים הפנימיים צריכים לעשות כדי להדביק את הפער שהולך וגדל בקצב מואץ, ובפרט לאור רוחב היריעה והנושאים שעל הפרק?

שואלים אותנו לא מעט **מדוע** צריך הסמכה בביקורת מערכות מידע/סייבר, מה נותנת ההסמכה והאם ניתן להצליח בתחום ללא הסמכה?

האם הייתם מוכנים שאת הדוחות הכספיים של הארגון שלכם יערוך אדם שלא הוסמך כרואה חשבון?

האם הייתם מוכנים שאדם שלא הוסמך כרופא ינתח את הילדים שלכם?

ודאי הייתם מעדיפים שהביקורת הפנימית בארגון שלכם ובגופים רלוונטיים נוספים (כמו הגוף המוסדי המנהל את כספי הפנסיה שלכם) תבוצע על ידי מבקרים פנימיים בעלי הסמכת CIA.

ודאי הייתם מעדיפים שמנהלי רשת המחשוב בארגון שלכם יחזיקו הסמכות מקצועיות מתאימות - MCSA, CCNA וכו'.

לימודי הסמכה בביקורת מערכות מידע יאפשרו למבקר ללמוד ולהשלים פערים בתחום, תוך התמקדות בעולמות הרלוונטיים לביקורת, בצורה יעילה ומתודית. נוסף על כך, ההסמכה מספקת אישור בלתי תלוי לידע ולניסיון של המבקר, משקפת מחויבות שלו למקצוע ומהווה עבורו יתרון תחרותי.

נקודה נוספת למחשבה

יעילות ומועילות ארגונית - ככלל, ככל שבעלי התפקידים בארגון מוסמכים בתפקידיהם השונים - אנשי כספים, רכש, אבטחת מידע, תשתיות מחשוב וכדומה, אנו מצפים לביצוע תהליכים יעילים יותר, אפקטיביים יותר ומדויקים יותר, ולאיכות גבוהה יותר בתוצרי הפעילות שלהם. ניתן להקביל זאת גם לאיכות המבקרים הפנימיים בארגון. ככל שבארגון יש מבקרים פנימיים המחזיקים הסמכות מקצועיות מתאימות, הרי שרמת הוודאות לגבי איכות התוצרים, עמידה בתקנים מקצועיים ורמה מקצועית הולמת - גדלה.

לסיכום

לדעתנו ראוי שמבקר פנימי יהיה בעל ידע בביקורת מערכות מידע. העולם כפי שהכרנו אותו משתנה ממש לנגד עינינו. הטכנולוגיות החדשות כבר משבשות כל חלקה טובה בתהליכים העסקיים הישנים, והדברים נמצאים רק בראשיתם. העשור הקרוב יהיה בוודאות מרתק יותר, מאתגר יותר ומשבש הרבה יותר מאשר העשור האחרון. הגבינה זזה ממש מול עינינו,

האם אנחנו מוכנים לחשב מסלול מחדש

ביקורת מערכות מידע לא רק למבקרי מערכות מידע

מאת

בר וויס סלהוב | CISA,CRISC, ראש ענף ביקורת תשתיות, תהליכי IT ודיגיטל, חטיבת הביקורת הפנימית, בנק לאומי

אילנה שחורי | רו"ח, CIA, CISA, CRMA, מנכ"ל משותף בחברת IA-IS, חברה לביקורת וייעוץ

ההתפתחות הטכנולוגית המואצת מובילה לשינויים רבים בתהליכי העבודה של ארגונים המשלבים יכולות טכנולוגיות שונות בתהליכי העבודה. למעשה,

כיום אין כמעט תהליך עסקי או תפעולי שאינו נתמך במערכת מידע או בתשתית טכנולוגית.

כתוצאה מכך מתגברים בארגונים סיכונים שונים כגון סיכוני אבטחת מידע וסייבר, סיכוני זמינות והמשכיות עסקית.

בספרו "מי הזיז את הגבינה שלי" כתב ספנסר ג'ונסון כך: "אם תבחין בשינויים הקטנים בשלב מוקדם, יהיה לך קל יותר להסתגל לשינויים הגדולים יותר שעומדים לקרות". התגברותם של סיכונים טכנולוגיים שונים במסגרת פעילות הארגון מחייבת ביצוע התאמות בתהליכי הביקורת שנדרשת לבחון היבטים טכנולוגיים גם במסגרת ביקורות עסקיות ולא רק בביקורות מערכות מידע ייעודיות.

לשינויים אלו חשיבות רבה בשמירה על רלוונטיות הביקורת הפנימית וביכולת של פונקציית הביקורת לבצע את תפקידה בזיהוי הסיכונים המשמעותיים לארגון.

שינוי יחסי הגומלין בין ביקורת פנימית עסקית וביקורת מערכות מידע

אם עד לאחרונה הייתה קיימת הבחנה ברורה בין תחומי הבדיקה של מבקרים פנימיים קלאסיים לבין תחומי הבדיקה של מחלקות ביקורת מערכות המידע בארגון, הרי שאנו מציעים הגדרה מחודשת של תחומי האחריות ושיתופי הפעולה.

על מנת לשמר את אפקטיביות הביקורת ולהגביר את התועלת ממנה, רצוי שמבקר פנימי ישלב במסגרת ביקורת תהליך עסקי כמה נושאי ליבה שבמקור היו נחלתם של מבקרי מערכות המידע.

חשוב להדגיש כי אין הכוונה ששילוב נושאים אלה במסגרת ביקורת הבוחנת תהליך עסקי יחליף ביקורת סדורה של בדיקת מערכת, דבר המחייב היכרות עם עולם ה-IT ומומחיות של מבקר מערכות מידע. ביקורת ייעודית של מערכות ליבה ותהליכי ניהול התשתיות יבוצע על ידי מבקרי מערכות מידע מקצועיים. המודל המוצע הוא שדרוג של הביקורת הקלאסית, שיאפשר שילוב של היבטים טכניים במסגרת הביקורות העסקיות

במטרה לתת התייחסות גם לסיכונים הטכנולוגיים ולשקף תמונה רחבה יותר בנוגע לסיכונים הקיימים בנושא הנבדק.

היבטים טכניים מרכזיים שמומלץ לשלב במסגרת ביקורת תהליך עסקי:

1

בחינת מידת התאמת המערכת לצורכי הארגון

אחד הפרמטרים המשמעותיים בהצלחת יישום מערכת הוא מידת המענה שלה לצרכים העסקיים ומידת השימוש של המשתמשים במערכת. ארגונים משקיעים סכומים אדירים ביישום מערכות מתקדמות שנכשלות כאשר הן אינן תואמות לצרכים ולדרישות המשתמשים. בהקשר הזה נבדוק: האם המערכת ידידותית וקלה לשימוש? האם היא מספקת למשתמש את כל המידע הנדרש לביצוע הפעילות העסקית? האם המשתמשים שותפים בהגדרת הדרישות והמבדקים? כמו כן נבקש לוודא כי הוגדרה ויושמה תוכנית הדרכה והטמעה מקיפה ואפקטיבית.

חשוב לזכור כי מערכת שאינה נותנת מענה לצורך של המשתמש העסקי עלולה להוביל לרמת שימוש נמוכה במערכת וליצירת תהליכי עבודה מקביליים באופן שייצור סיכון תפעולי לפעילות הארגון.

איך זה בא לביטוי בשטח?

במסגרת ביקורת בנושא שכר, נמצא כי חשבי השכר מבצעים חישובים ידניים בנושא שעות הנוכחות והזנת נתונים ידניים למערכות הנוכחות והשכר, מקום שמקובל שהערכים יהיו תוצאה של תהליכי עיבוד במערכות כגון יישום סוגי הסכמים וזכויות עובדים. מלבד חוסר יעילות ובזבוז משאבים, משמעות ההזנה הידנית היא חשיפה לטעויות ולהטעיות. ההתערבות הידנית נבעה מיישום לא מיטבי של מערכת הנוכחות בארגון. זיהוי הפערים הביא להמלצה על מיכון היבטים אלו במערכת.

2

בחינת נקודות בסיסיות בתחום אבטחת מידע

סיכוני אבטחת מידע הם נושאים משמעותיים בבדיקת תהליך עסקי/תפעולי בשל ההשלכה שעשויה להיות להם על הארגון.

בדיקת הנושא מצריכה לרוב מומחיות ומקצועיות, אך קיימים נושאים שגם המבקר הפנימי הקלאסי יכול לכסות בשלב ראשון של הבדיקה:

ניהול ההרשאות במערכת - חשוב לראות שתהליך מתן ההרשאות מבוסס על עקרון "הצורך לדעת" (עיקרון אבטחתי הדורש מתן הרשאות מינימליות למשתמש לצורך מילוי תפקידו) ומאפשר הפרדת תפקידים. בנוסף יש לבדוק האם מתקיים תהליך מובנה ותקופתי של סקירת ההרשאות, במטרה לוודא שאין הרשאות עודפות כתוצאה משינויים ארגוניים (ניוד ועזיבה של עובדים). תהליך זה יכלול התייחסות גם לספקים חיצוניים.

הרשאות גישה עודפות חושפות את הארגון לפעילות שאינה מורשית, ואף קיים חשש כי הרשאות עודפות ישמשו למעילות והונאות.

איך זה בא לידי ביטוי בשטח?

במסגרת סקירת ההרשאות במערכת תשלומים, התגלה כי עובדים מסוימים הוגדרו במערכת בהרשאה המאפשרת הזנת תשלום ובהרשאה נוספת כמאשרי תשלום. התוצאה - אופן יישום ההרשאות במערכת המידע אינו עומד בעקרונות מקובלים של הפרדת תפקידים ובנוהלי הארגון המחייבים אישור התשלום על ידי גורם אחר ממזין התשלום.

סיכוני אבטחה פיזית - נסתכל על יישום מדיניות "שולחן נקי" במטרה לוודא כי מידע רגיש מאוחסן בצורה מאובטחת וכי קיימת מודעות עובדים לנושא. כמו כן נבחן את הגישה למתחמים רגישים ונראה כי זו מותרת רק למורשים וכי מיושמים אמצעי הגנה פיזיים כגון בקרת כניסה ומצלמות. גישה מתירנית לאזורים רגישים כגון חדרי שרתים, יכולה להוביל לסיכוני דלף מידע ולחשיפת מידע רגיש של הארגון.

3

בחינת קיום בקרות מיכוניות הולמות

קיימים שלושה סוגי בקרות מיכוניות מרכזיות:

בקרות קלט - בקרות מונעת שתפקידן להבטיח את התאמתם של הנתונים המוקלדים או המוזנים למערכת ללוגיקה העסקית המוגדרת לאותו שדה במערכת. לדוגמה: מגבלת קליטת ספרות בלבד בשדות המייצגים סכום, בדיקת תקינות חוקיות תאריך בשדה תאריך.

בקרות עיבוד - בקרות אוטומטיות שתפקידן לוודא שלמות ודיוק עיבוד הנתונים. לדוגמה: חישוב שגוי של מערכת החיוב (מערכת Billing) יוביל להפקת חשבונות חיוב בעודף או בחוסר, חישוב שגוי של שיעורי הצמדה יגרור טעויות בתשלומים או ברישומים החשבונאיים ועוד.

בקרות פלט - בקרות שתפקידן להבטיח שנתוני המערכת יועברו ליעדן בצורה המיטבית תוך שמירה על אמינות הנתונים. לדוגמה: בקרות ביחס לתהליכי הפקת דוחות למשתמשי הקצה.

בקרות מיכוניות חסרות עלולות לפגוע באיכות הנתונים הקיימים במערכת ובמערכות אחרות שניזונות ממנה ובכך ליצור סיכון תפעולי משמעותי לארגון.

4

בחינת היבטי זמינות ותפעול המערכת

זמינות מערכות המידע מהווה יעד מרכזי בפעילותם של ארגונים על מנת להבטיח רציפות עסקית ומניעת פגיעה בהשגת היעדים העסקיים ובלקוחות הארגון. לפיכך, רצוי לשלב בביקורת בחינה של היקף התקלות במערכת, משך הזמן לטיפול בתקלות, והאם קיימת התחייבות ל- SLA (הסכם רמת שירות). כמו כן האם מתקיים תהליך הפקת לקחים לאיתור גורמי השורש וכן תהליך לאיתור תקלות חוזרות.

בעיות בזמינות המערכת פוגעות בפעילות העסקית שמבוצעת במערכת וביכולת של הארגון לעמוד ביעדיו העסקיים ובמתן שירות ללקוחותיו.

5

בחינת היבטי המשכיות עסקית

היבט נוסף שמומלץ להתייחס אליו הוא מידת קריטיות המערכת לפעילות העסקית של הארגון. חשוב לבדוק האם המערכת שתומכת בתהליך העסקי שאנו בודקים הוגדרה כמערכת קריטית לארגון, ולפיכך משולבת בתוכנית ההתאוששות מאסון של הארגון (כולל ביצוע תרגולי התאוששות מאסון למערכת). בנוסף יש לבדוק האם עובדי היחידות השונות מודעים לתוכנית ההמשכיות העסקית ולפעילות הנדרשת מהם בשעת חירום. היעדר תכנון והכנה להתמודדות עם מצבי חירום תוך שמירה על המשכיות עסקית, עלולים להוביל ארגונים לנזקים גדולים ולאבדון.

בחינת היבטים טכנולוגיים אלה בפעילות המערכת שתומכת בפעילות העסקית הנבדקת, מאפשרת מתן התייחסות לסיכון הטכנולוגי הקיים בנוסף על הסיכונים העסקיים הרלוונטיים לנושא הנבדק, ובכך לשקף תמונה רוחבית לגבי מכלול הסיכונים בנושא הנבדק.

כיצד ניישם את השינוי?

קיימת חשיבות רבה להגדרת תהליך עבודה ותהליך ניהול השינוי במטרה כדי ליישם באופן מיטבי מתודולוגיה זו. התהליך יכלול ביצוע מיפוי והבחנה בין מערכות הליבה/התשתית שיבוקרו על ידי מבקרי מערכות מידע לבין מערכות התומכות בפעילות עסקית נישתית/ממוקדת ("מערכות קצה") שהן ברמת מורכבות טכנולוגית נמוכה יותר, וכן שיוך "מערכות הקצה" לישויות הביקורת בתוכנית העבודה הרב-שנתית.

על מנת שהשינוי יצליח, הנהלת הארגון והביקורת צריכות להיות מחויבות לתהליך, לאור הצורך בהשקעת משאבים בהטמעתו. מומלץ להגדיר גורם ייעודי ביחידה שיהיה אחראי להטמעת התהליך וביצוע מעקב, בקרה ומתן סיוע מקצועי, וכן עוגנים מקצועיים בצוותי הביקורת שיסייעו בהטמעת המתודולוגיה. בנוסף, נדרש תהליך הדרכה שוטף לאור השינויים המתפתחים בעולם ה- IT ולאור השינוי במיומנויות המבקר ומקצועיותו.

לסיכום

עולם הביקורת משתנה לנגד עינינו לאור השינויים המהירים בעולם הטכנולוגי. שינויים אלו ושילובו של עולם הטכנולוגיה כמעט בכל הפעילויות העסקיות/התפעוליות של הארגונים, מחייבים ביצוע שינויים גם ביחידת הביקורת הפנימית ובחלוקת האחריות בין הביקורת הפנימית הקלאסית וביקורת מערכות המידע.

דגשים מרכזיים בבדיקת מערכות מידע התומכות בתהליך עסקי

אבטחת מידע

הנחיות

בדקו את סוג ההרשאה הקיימת לכל עובד/ספק (קריאה/עדכון). האם ההרשאות ניתנו בהתאם לעקרון "הצורך לדעת" ועקרון הפרדת תפקידים?

האם אין הרשאות עודפות לגורמים שאינם עובדים עם המערכת כגון עובדים שנוידו/עזבו?

האם מיושם תהליך בקרה מובנה ותקופתי אחר ההרשאות במערכת?

בקרות קלט

הנחיות

האם קיימות במערכת כל הבקרות הנדרשות בהתאם להגדרות העסקיות/ תפעוליות/ רגולטוריות?

האם בקרות הקלט מתבצעות מוקדם ככל האפשר, סמוך למועד יצירת הנתונים?

האם הוגדרו התראות מספקות למשתמשים על קלט לא חוקי?

בדקו את הנתונים שניתן להקיש בשדות השונים: האם בחירה מתוך רשימה סגורה או מלל חופשי?

בדקו את פורמט השדה, האם נקבעו גבולות ערכים שניתן להקיש לשדה?

בדקו אם קיימת תלות לוגית בין שדות שונים

הערות

בדיקות אלו ניתן לעשות על ידי צפייה בפעילות המשתמש ובקשה כי יקליד נתונים שגויים במטרה לבחון את בקרות הקלט במערכת ואת הודעות השגיאה או ביצוע מבדקים אם קיימת סביבת ניסוי למערכת.

בקרות עיבוד

הנחיות

סקירת דוחות פלט ובחינת שגויים ביחס לתהליך העיבוד.

סקירת תקלות המערכת: האם קיימות תקלות הנוגעות לחישובי המערכת? האם תקלות שתועדו לגבי המערכת יכולים להצביע על שיבוש בחישובי המערכת?

בחינת תחשיבי העיבוד באמצעות חישוב בלתי תלוי של המבקר

הערות

כאשר המערכת מבצעת חישובים ניתן לבחון את בקרות העיבוד באמצעות סימולציה של אופן ביצוע החישוב על ידי המערכת

בקרות פלט

הנחיות

בחנו את שלמות ואפקטיביות הפלט הקיים מהמערכת.

האם קיים במערכת מידע תפעולי וניהולי התומך בקבלת החלטות לרמות ההנהלה השונות? האם נעשה בו שימוש תקין ואפקטיבי לצורכי בקרה?

האם קיימים אמצעי זיהוי מספקים לדוחות/שאילתות? דוגמאות: שם דוח/שאילתה, מס׳, תאריך הפקה, מס׳ עמודים, סיכומי ביניים, תאריך נכונות.

בהתייחס לדוחות נייר המופקים אוטומטית מהמערכת - האם יש צורך בהפקתם אוטומטית באופן פיזי או שכדאי להפיקם בהתאם לדרישה/שאילתה?

התאמה לצורכי המשתמשים

הנחיות

האם ממשק המערכת הוא ידידותי ונוח לשימוש? האם המידע הנדרש לשם ביצוע הפעילות העסקית נמצא במערכת וכולל דוחות בקרה ודוחות מעקב?

האם המשתמשים השונים היו שותפים בתהליך הגדרת הדרישות?

האם המערכת עונה על צורכי המשתמשים? האם חסרים נתונים במערכת? האם הנתונים הקיימים במערכת נכונים?

האם מיושמים תהליכי עבודה ידניים מחוץ למערכת? אם כן, מדוע?

האם תדירות העדכון של הנתונים במערכת מתאימה לצורכי המשתמשים?

האם המשתמשים שבעי רצון מהמערכת? בחנו את היקף ואופי התלונות של משתמשים על המערכת, ראיינו מדגם של משתמשים או ערכו סקר שביעות רצון.

הערות

תשאול של משתמשי המערכת השונים.

התרשמות ממסכי המערכת וקלות העבודה במערכת: ידידותיות מסכים ותהליכי עבודה.

זמינות ותפעול

הנחיות

בדקו כי זמן הטיפול בתקלות נמדד למול חומרת התקלה.

האם מבוצע תהליך של הפקת לקחים לאיתור גורם השורש?

האם מבוצע תהליך לאיתור תקלות חוזרות?

הערות

סקירת דוחות של תקלות.

תשאול משתמשים לגבי שביעות רצונם מזמינות המערכת והשלכת התקלות על הפעילות העסקית.

המשכיות עסקית

הנחיות

האם הוגדרה רמת הקריטיות של המערכת? אם היא מוגדרת כקריטית, האם היא שולבה בתוכנית ההתאוששות מאסון (BCP/DRP) של הארגון ובתוכנית התרגולים?

האם הצוותים העסקיים מודעים לפעילות הנדרשת מהם בשעת חירום?

הערות

סקירת דוחות של תקלות.

תשאול משתמשים לגבי שביעות רצונם מזמינות המערכת והשלכת התקלות על הפעילות העסקית.

סדנת בקרה וביקורת פנימית - גישה מערכתית

מרכז אקדמי ומרצה
בעז ענר

מועד נובמבר 2019

קורס לימודי תעודה ביקורת פנימית 12 מפגשים

מרכז אקדמי יוסי גינוסר

מועד 11-12/2019

בין השעות 16:00 – 19:00

הקורס מקנה 36 שעות CPE

COMING SOON

סדנת כתיבה והשבחת דוחות ביקורת

מרכז אקדמי ומרצה
בעז ענר

מועד דצמבר 2019

סדנת תקנים מקצועיים

מרכז אקדמי ומרצה דורון רונן
משנה לנשיא ויו"ר הועדה המקצועית
IIA ישראל

מועדים 08/09/19 | 12/09/19 | 15/09/19

פרטים והרשמה
אינה גולדרביטר
מנהלת לשכת נשיא האיגוד טלפון
03-5116617
OFFICE@THEIIA.ORG.IL

השגת אמון בזכות הטכנולוגיה

מבקרים פנימיים הביאו לגידול באמון בעלי העניין על ידי שימוש בנתונים לתמיכה בממצאי הביקורת

מאת

מאת פול סליי וכריס וולטר

הטכנולוגיה היא מפתח המאפשר ערך עסקי. מבקרים פנימיים צריכים להיות מסוגלים לאמת שתהליך מסוים מספק החזר על השקעה מצופה וכי הופק המיטב מהחלטות על סיכוני טכנולוגיה ומשאבים. ללא הכישורים הנדרשים, מבקרים פנימיים עלולים שלא לספק את הערך שהארגון מצפה מהם.

מרבית מבקרי מערכות המידע בנורדסטרום הם בעלי השכלה המשלבת מומחיות טכנולוגית ותארים במינהל עסקים לצד שנים של ניסיון עסקי. הם עובדים יחד עבור שלושה יעדים בלתי רשמיים של הביקורת: תפעול, מודיעין עסקי וציות.

נורדסטרום משתמשת בשני מדדים על מנת לקבוע האם מבקרי מערכות המידע הם יועצים מהימנים. הראשון: האם לקוחות חוזרים ומבקשים שירותי ביקורת פנימית? השני: האם המלצות הביקורת מביאות לערך עסקי?

כדי לספק ייעוץ בעל ערך, מבקרי מערכות מידע צריכים להבין את הטכנולוגיות החדשות שעימן עובדים השותפים העסקיים, לרבות חידושים כגון DevOps, IOT וארכיטקטורה של מערכות ללא שרת.

מומחי ביקורת מערכות מידע בנורסטרום מצביעים על חמישה תחומים לחיזוק ערכם כיועצים:

1 אבטחת סייבר ופרטיות

רוב התעשיות מתייחסות לסיכוני סייבר ופרטיות כסיכונים מובנים וגבוהים. כחברה הנשענת על טכנולוגיה, נורדסטרום שכרה מומחים בעלי הסמכה בתחום אבטחת סייבר כדי לייעץ ולבקר כיצד לייצב באופן אופטימלי את הסיכון. כתוצאה מכך מבקרי מערכות מידע בנורדסטרום פירשו ויישמו בקרות אבטחה בשיטות עבודה על הסביבה החדשה, המבוססת על סביבת ענן.

שתי מסגרות המשמשות ארגונים בינלאומיים הן הארגון הבינלאומי לתקני ISO 27002 טכנולוגיות מידע - טכניקות אבטחה הקוד ליישום בקרות על אבטחת מידע, והמסגרת של המוסד הבינלאומי לסטנדרטים בטכנולוגיית אבטחת סייבר.

מבקרים פנימיים מתרגמים את דרישות האבטחה של המסגרות הללו לשפה של לקוחות הביקורת.

כך למשל, צוות של יישום אימץ לעצמו תהליכי עבודה שבהם כל חבר בצוות יכול לבצע שינויים בקוד היישום בסביבת הייצור. מבקרים פנימיים הסבירו לצוות את הפוטנציאל לשינוי לא מורשה של הקוד ואת הדרישות הנדרשות לפי תקני האבטחה. בכך הם סייעו לחברי הצוות להבין שעליהם ליישם בקרה מפצה באמצעות ניטור כניסות ליישום ורישום שינויים על מנת להבטיח ששינויים שאינם מורשים יאותרו באופן מיידי.

ככל שצוותים לומדים יותר על סיכוני אבטחה ועל בקרות, כך הם מקבלים את ההחלטות הטובות ביותר בנוגע לסיכון.

2 טכנולוגיות ממשל תאגידי

מבקרי מערכות מידע בנורדסטרום מסתמכים על תקני ISACA COBIT 5 כדי להעריך בשלות של טכנולוגיות משילות על בסיס חוזר ונשנה. מבקרים ממזגים בין תקני COBIT ותקני ISO ליצירת תקן ספציפי לנורדסטרום כבסיס לביקורת. תקן זה מאפשר למבקרים פנימיים וללקוחות הביקורת לראות היכן פעילותם משתלבת בתמונה הגדולה.

תקן זה גם מאפשר למחלקות לשתף פעולה עם המבקרים הפנימיים כדי לערוך ביקורת המשלבת היבטים שאינם טכנולוגיים של ממשל תאגידי. באחד הדוחות המבקרים סיפקו הבטחה כי הפרויקטים הטכנולוגיים מספקים את הערך המובטח בהיבט העסקי. מבקרים פנימיים בביקורת משולבת מרחיבים את הידע שלהם בכיסוי אסטרטגיית הטכנולוגיה, ארכיטקטורה משולבת, ומדידת ביצועי הארגון.

3 תחקור נתונים

מבקרים פנימיים של נורדסטרום ערכו יותר דוחות ביקורת משכנעים שבמסגרתן נבדקו 100% מהאוכלוסייה באמצעות טכנולוגיית תחקור נתונים. כדי לכתוב דוחות שכאלה, מצופה שלכל המבקרים הפנימיים יהיה ידע בסיסי באקסל, סטטיסטיקה ותיקוף נתונים. בצורה כזאת המבקרים הפנימיים ממנפים כלים לתחקור נתונים כדי להשיג מידע שישמש אותם בהכנת דוחות בנושאים משמעותיים.

כלים לתחקור נתונים הם שימושיים ביותר כאשר משלבים שתי מערכות נתונים או יותר. בפרויקט מסוים, מבקרים פנימיים חילצו אירוע במערכת המעקב והטיפול באירועים ותקלות, וקישרו אותו למידע על הבעיה בתיק באמצעות ניתוח סיבות שורש וזיהוי יישומים מתיעוד הנשמר במערכות משולבות.

כדי לחלץ מידע ממערכות מידע ייחודיות, מבקרים פנימיים משתמשים בכלי הדמיה של נתונים כדי לתת את המידע על מידת השליטה של החברה בבקרות ניהול השינוי והאם התהליך לווה בלמידה הנדרשת הלקוח מנצל את הניתוח הנ"ל כדי לעקוב אחר ההתקדמות מאז הדוח.

4 תהליכי רובוטיקה ואוטומציה

ההתקדמות האחרונה של מבקרים פנימיים בנורדסטרום עוסקת בשימוש של תהליכי אוטומציה רובוטית. ייעוץ פרויקטים תואם למטרות הביקורת הפנימית בזיהוי דרכים לצמצום הוצאות או מאמץ בתהליכי העבודה. בשותפות עם חטיבות החברה ומחלקות המס, המבקרים יצרו רובוטים כדי להפוך את ההליך הידני של רישוי מזון ומשקאות והקלדת חשבוניות להליך אוטומטי. באמצעות האוטומציה של התהליך המבקרים הפחיתו את הוצאות השכר של הלקוח.

דוגמה נוספת היא בבחינה של הרשאות המשתמשים של החברה ותהליכי האימות. המבקרים שילבו את תיעוד הבקרה של האחראי עליה במערך הבדיקות שביצעו, תוך שימוש בכלי אוטומציה לביצוע בדיקה זו. אחת הבדיקות שבוצעו אימתה שגישה שניתנה בוטלה במועד. אם כן, שימוש ברובוטיקה ואוטומציה מאפשר למבקרים לבצע יותר מבחנים באותה מסגרת זמן.

5 תקשורת

מבקרי מערכות מידע בנורדסטרום התמקדו בשיפור המיומנויות בתחום התקשורת המילולית הכתובה. כדי לתקשר ביעילות עם גופי הטכנולוגיה בארגון, מנהל מחלקת ביקורת מערכות מידע מבלה שישה חודשים בעבודה ישירה מול מנהלים ביחידות הטכנולוגיה טרם כניסתו לתפקיד בביקורת הפנימית. במהלך תקופה זאת הוא לומד את המנהלים וסגנון התקשורת שלהם, וישלב זאת בדוחות הביקורת כדי להגביר את השפעתם.

מבקרים פנימיים הפכו לבעלי תקשורת משכנעת, מנהלי משא ומתן יעילים ומאזינים גדולים. הם הביאו לגידול באמון בעלי העניין על ידי שימוש בנתונים לתמיכה בממצאי הביקורת ותוכניות פעולה של הארגון. כיום יש ציפייה שממצאי הביקורת ייתמכו על ידי נתונים אפילו בנושאים קשים לכימות ומדידה, אך צריך לזכור שהצגת נתונים חזותית אינה נדרשת בכל דוחות הביקורת. לעיתים הצגה חזותית עלולה לגרום ללקוח לקפוץ למסקנות בלי לקרוא את כל הפרטים, ולכן חלק מהלקוחות מעדיפים לקרוא את הטקסט. בעוד שדוחות הביקורת צריכים להתמקד תמיד בסיכונים החשובים ביותר, מבקרים מתאימים את סגנון דוחות הביקורת לפורמט המועדף על בעלי העניין.

לסיכום

יצירת אמון באמצעות הטכנולוגיה

הביקורת הפנימית צריכה באופן תמידי לפתח את אנשי הצוות, להפוך אותם ליועצים אמינים ולשמר אותם.

מאמציה של נורדסטרום בעניין כוללים: הגברת היקף שיחות ממוקדות סיכונים שעורכת ההנהלה כדי להביא להגדלת אפקטיביות הבקרות. והובלת שינוי תרבותי והקדשת זמן לבניית אסטרטגיות להפחתת סיכוני טכנולוגיה.

בתהליכים אלה מבקרי מערכות מידע הגדילו את שיעור שביעות הרצון של הלקוחות וקיבלו יותר דרישות לביצוע עבודות מצד ההנהלה. יותר מזה, ההנהלה יותר פרואקטיבית בקידום שינויים בנושאים שזוהו בביקורת פנימית, זאת עוד לפני קבלת דוח הביקורת.

כשהלקוחות מבינים שדוח הביקורת יכול להניע אותם מהר יותר להשגת יעדיהם, הם נוטים להפוך ללקוחות חוזרים ולשתף את עמיתיהם בארגון

מדור היתולי

מיומנה של מבקרת פנימית

מאת: רונית שוורץ, MBA - בנק הפועלים

שנת 2030 - יום בחיי מבקרת פנימית

היום היה יום שגרתי.

כדרכי מדי בוקר, פקחתי את עיניי ומיד הושטתי יד לעבר השידה שלצד המיטה, שם מונחות משקפי הג'ימייל שלי להטענה הלילית שלהן. הרכבתי את המשקפיים כדי לבדוק האם הגיע דואר אלקטרוני בלילה.

לאחר סידורי הבוקר הרגילים ובליעת כמוסת ארוחת הבוקר, התחברתי לאלקטרודות השידור על מנת להעביר למשרד את סיכום הממצאים שלי מיום האתמול. עצמתי את עיניי וניסחתי במוחי את הממצאים (בעלי טוען שתוך כדי אני גם ממלמלת ומזיזה את השפתיים). עם סיום השידור פתחתי את אפליקציית 'איזי דרייב' והזמנתי את הרכב האוטונומי לפתח הבית.

הנסיעה עברה באיטיות (לא ייאמן שגם בשנת 2030 טרם נפתרה בעיית הפקקים) והמכונית עצרה בפתח המפעל שבו אני מבצעת ביקורת בימים אלה.

את כל התשדורות לגבי מכונות הייצור כבר קיבלתי אתמול - החיישנים הרבים המפוזרים במפעל ובין קווי הייצור שידרו נתונים לגבי חומרי הגלם שהוכנסו לכל מכונה, קצב פעולת המכונות, נתוני עצירות בייצור או תקלות ביחס לכל מכונה (כולל משך זמן העצירה עד הפעלתה מחדש), כמות הפסולת שנותרה בכל מכונה ותוצרים תקולים. התעמקתי בנתונים באמצעות משקפי הג'ימייל במהלך הנסיעה בבוקר.

מיד זיהיתי שיש בעיה במכונה מס' 3.

את הבוקר ביליתי בשיחות עם מנהל המפעל, עם מנהל קו מס' 3, ועם הרובוט שמנהל את המחסן.

בעקבות ממצאיי הוחלט להפעיל במכונה מס' 3 תוכנה לבדיקה עצמית.

עד שזו תיתן תוצאות הרכבתי שוב את משקפי הג'ימייל, ובפניי הוקרנו ההערות לממצאי יום האתמול (אותם שידרתי כזכור בבוקר).

העברתי את המשקפיים למצב 'הפעלה קולית', הוריתי לקבל את כל התיקונים ולהעביר את הממצאים למבוקרים לקבלת תגובה. בסוד אספר שעל אף כל הטכנולוגיה המתקדמת, לדבר אחד לא הצלחתי להתרגל - לקרוא מסמכי ביקורת בלי להחזיק עט ביד...

מסרון מבעלי הזכיר לי שהיום תורי לאסוף את הילדה מבית הספר. בעזרת 'איזי דרייב' שלחתי את המכונית לאסוף את הילדה, ושיגרתי פקודה לטוסטר החכם להתחיל לחמם את ארוחת הצהריים בטמפרטורה נמוכה.

לפתע נזכרתי שמתוכננת ישיבה של ועדת הביקורת בעוד שבוע, ואני אמורה להציג בה דוח ביקורת שהגשתי לאחרונה. מיד שידרתי הוראה קולית למערכת הממוחשבת שבמשרד כדי שתייצר מצגת מן הממצאים הרלוונטיים.

כמו כן, לאחרונה הוחלט לשלוח את דוח הביקורת כקובץ קולי לא רק לחברי ועדת הביקורת, אלא גם למבוקרים. אני צריכה רק לזכור לצרף בכל

משלוח את קובץ ההנחיות לגבי פקודות קוליות - פקודות המאפשרות מיון הממצאים בקובץ הקולי לפי ציוני הסיכון, לפי הגורם המטפל, לפי סטטוס הטיפול וכדומה.

אגב כך, סוגיית מתן ציוני סיכון לממצאים גוזלת ממני זמן רב מדי לאחרונה. לפני מספר שבועות רכשנו במשרד מערכת חדשה לדירוג אוטומטי של סיכון הממצאים. המערכת מדרגת באופן עצמאי רמות סיכון בטווח של 1-10, ובתקופת ההטמעה אני נאלצת לבצע בקרה על קבלת ההחלטות של המערכת.

נחזור לענייננו, תוכנת הבדיקה סיימה לנתח את פעולות מכונה מס׳ 3, מקור התקלה אותר וכעת יפעלו לתיקונו. עוד (חצי) יום עבודה של הביקורת הביא ערך לארגון. הפעלתי את ׳איזי דרייב׳ והזמנתי את המכונית לאסוף אותי.

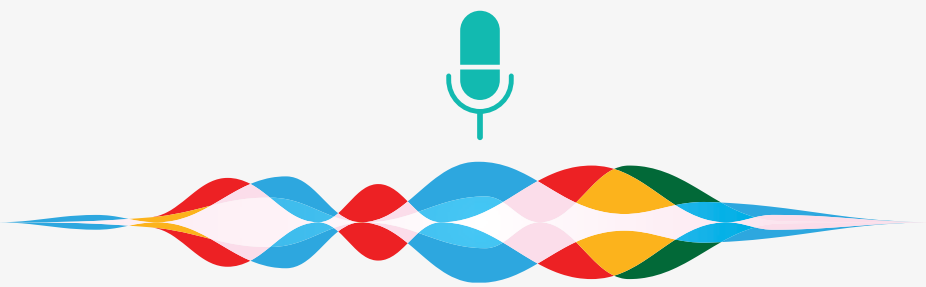
השאלה המתבקשת כעת היא מדוע בכלל נסעתי למפעל? הרי כל הנתונים היו בידי עוד לפני שהגעתי למקום. התשובה היא שאינספור רובוטים, מערכות וטכנולוגיה מתקדמת לא יחליפו "מידע רך" שניתן לאסוף רק בשיחה שמתקיימת פנים מול פנים, תוך קריאת שפת הגוף של בן השיח.

בדרך הביתה התחברתי לאלקטרודות השידור, והעברתי למשרד את עיקרי הממצאים שלי מהיום. בהמשך הדרך הרשיתי לעצמי לנוח קלות ולהאזין למוזיקה. נתתי הוראה קולית להשכיב את המושב לאחור, והרכבתי לעצמי רשימה מוזיקלית להאזנה.

מי היה מאמין שרק לפני עשור נהגתי לחזור הביתה מדי יום עם ערימות של ניירות וקלסרים, שנהגתי לקרוא עשרות עמודים של דוחות ביקורת, לשכתב ללא הרף ניסוחים וטיוטות, ולהשקיע שעות ארוכות בעיצוב מצגות בתוכנת ה-Power Point ה"מתקדמת".

לחזור לתקופה ההיא נראה לפתע

כמו חלום בלהות



Editor's Note

Sharon Witkowski Tabib, CPA, CIA, CRMA
Vice President of IIA Israel - Institute of Internal Auditors

This digital age is characterized by the accelerating integration of technologies in business processes, leading to changes in the risk landscape and threats for which the organization must prepare. Accordingly, audit processes are also evolving, as well as the tools used by auditors and the focus of the audits.

This issue focuses on four influential aspects of the audit work in the digital world:

Cyber risks: new technologies become available on daily basis, and with them new security exposures and cyber risks arise, with the potential of causing damage to individual customers or bringing down a whole organization and even a country. According to Fortinet's recent Threat Landscape Report, cyber-attacks are one of five most critical threats organizations are facing these days. As such, cyber-risks must be addressed in audit plans on a regular basis.

Innovation and technology: cloud, mobile, social networks, analytics, IoT, robotics and automation – all of these and more are the catalysts of digital innovation. Organizations need to be aware of innovations and technological developments and to incorporate them into their business. The auditor's job is to take advantage of these new capabilities in the audit process on the one hand, and on the other – to be familiar with tools and methodologies for examining processes managed in innovative ways.

Data analytics: leaning on science in any activity creates a significant advantage for auditors with analytical abilities. The tools available today for data analysis enable auditors to draw conclusions and identify trends even before risks are realized.

Training internal auditors for IT audits: business processes are supported by information systems, and the internal auditor is required to acquire skills that involve using technological audit tools to enable auditing these systems.

The world as we know it is changing right in front of us, technologies are evolving and IT-based solutions are becoming the center of our world.

The famous astrophysicist Steven Hawking used to express his opinion on various aspects of life, and said that "integration is the ability to adapt to changes". We, as auditors, need to be aware of the changes occurring around us, and must learn to adapt to them and bring value in our changing world.

In this issue, we set as our main objective to expand the set of tools available to auditors who wish to add value to their organizations through internal audits that are relevant to the digital age.

With wishes for a "Shana Tova" and pleasant reading,
Sharon Witkowski Tabib

President's Note

Doron Cohen
CPA, President IIA Israel - Institute of Internal Auditors

In my opening remark to the joint conference that was recently held by our institute together with the Information Systems Audit and Control Association (ISACA), I addressed various aspects that are changing in the internal audit world, including technology. Internal auditors cannot bury their head in the sand and ignore it. They must keep up to date with technological changes and understand the threats and opportunities entailed in them, both in relation to the organizations they serve and generally speaking. The auditor must have the ability to assess the organization's control framework and technological controls to help improve them. In addition, in a world where one must "do more with less", the internal auditor does not have a choice but to take advantage of technology to improve the internal audit processes and make them more efficient.

The objective of this issue, alike the conference mentioned above, is to raise internal auditors' awareness to the challenges of technology and to equip them with practical tools to improve their skills. I am thankful for the fruitful cooperation with ISACA. Hundreds of audit professionals filled the conference halls to capacity and enjoyed fascinating lectures as well as the opportunity to meet their peers. This corresponds with the need for integrated audits that examine both business processes and information systems in parallel.

I would like to congratulate the new State Comptroller, CPA Matanyahu Englman, and his Director-General Yishay Vaknin, and to wish them a successful term in office. In the conference we bade farewell to the former State Comptroller, Honorable Judge Yosef Zvi Shapira, and thanked him for his work. We thank him for his efforts to reinforce the internal audit profession in general and especially for his contribution to unifying the internal audit institutes in Israel. The task was assigned to his Director-General, Mr. Eli Marzel, who orchestrated the unification successfully.

The unification of the internal audit institutes is in high gear. I believe that by the end of this year this initiative will come to completion and we will be able to establish one strong, unified institute for the benefit of all internal auditors in Israel, that will operate in full cooperation with the global IIA according to international internal auditing standards.

"Shana Tova" (Happy new Jewish Year) to all,

Doron Cohen

נתראה בגיליון הבא

שצפוי להתפרסם לקראת חג הפסח תש"פ

אפריל 2020

Until the next issue, which is expected
to be released on April 2020