האתגרים במעבר של מאגרי מידע ומערכות המאגר לענן

נוסח מעודכן בעקבות תיקון 13

1. כללי

הטכנולוגיות המתפתחות של השנים האחרונות, כגון טכנולוגיות להעברת מידע בצורה מהירה המאפשרת קישוריות גבוהה בין רכיבים באמצעות רשתות האינטרנט והסלולר, טכנולוגיית הבינה המלאכותית (AI) המאפשרת עיבוד מידע בהיקף עצום לרבות מידע מסוג נתוני עתק (Big Data) וטכנולוגיות מחשוב ענן (Computing Cloud) המאפשרות שימוש קל ונוח בפלטפורמות ענן לאחסון ולשיתוף מידע בהיקף כמעט בלתי מוגבל, הביא לעלייה משמעותית במספר מאגרי המידע המועברים לאחסון ענן.

לפיכך, ארגונים רבים נמצאים בשלבי מעבר של תשתיות המחשוב והיישומים השונים לשרתי ענן בהליך שקרוי גם מיגרציה לענן. מדובר בתהליך מורכב, במסגרתו על הארגון לתעד את השלבים השונים בהליך בו לוקחות חלק מרבית מחלקות הארגון, החל מהנהלת הארגון וכלה בצוותי המחשוב.

המעבר לשימוש בטכנולוגיית ענן טומן בחובו יתרונות משמעותיים לצד אתגרים רבים, בעיקר בכל הנוגע לביצוע המיגרציה באופן מאובטח, תוך שמירה על המידע הרגיש שנמצא במאגרי המידע המצויים במערכות המחשוב והיישומים השונים של הארגון.

להלן יפורטו האתגרים אותם יש לבחון בעת ביצוע מעבר לטכנולוגיית ענן

2. האתגרים במעבר לטכנולוגיית ענן

2.1. **הגדרות שגויות** – סיכון משמעותי בהליך המיגרציה לענן נובע מיצירת הגדרות שגויות אשר עשויות להוביל לכך שמידע ארגוני ייחשף לעיני גורמים שאינם מורשים. לצורך התמודדות עם אתגר זה, יש להקצות כוח אדם מיומן ובהיקף הנדרש לביצוע המיגרציה.

לצוותי ה-IT בארגון אמנם ישנו ניסיון רב בתחזוקת המערכות הפנימיות בארגון, אך קיים שוני מהותי בין סביבת המחשוב הארגונית לבין הסביבה העננית, ולכן הידע שנצבר בניהול והתחזוקה של סביבת המחשוב הארגוני לעיתים אינו רלוונטי לאתגרי המיגרציה והתחזוקה עצמה בתשתיות הענן. לכן, יש לוודא, כי צוותי ה-IT הארגוני הוכשרו לצורך מתן מענה ברמה הנדרשת, הן לתהליך המיגרציה והן לתחזוקת תשתיות הענן והמערכות השונות בסיום התהליך.

2.2. **ממשקי API שלא אובטחו כראוי** - לממשקים אלו גישה למידע הארגוני ברמות שונות. לכן, כשל בהגנה על ממשקי API עלול לאפשר שליפה של נתונים ומידע ע"י גורמים שאינם מורשים. לצורך אבטחת ממשקי ה-API יש לשלב מנגנוני בקרה ותיעוד עדכניים בתהליכי המיגרציה והעבודה השוטפת בתשתיות הענן. כמו כן, כחלק מתפיסת ההגנה הכוללת בענן, מומלץ להצפין את המידע במנוחה ובתנועה, ולוודא כי מפתחות ההצפנה שמורים בסביבה מוגנת, שאינה סביבת הענן בה הוצפן המידע.

2.3. **חוסר התאמה של הארכיטקטורה הנוכחית (Incompatibility of the Current Architecture)** – כאשר מועבר מידע מסביבה אחת לסביבת אחרת, חשוב לבחון האם הארכיטקטורה בסביבה החדשה בנויה בצורה המתאימה, שכן חוסר תאימות עלול לגרום להעברת נתונים איטית או שגויה.

על מנת להתאים את הארכיטקטורה למעבר לענן, על הארגון לבצע סקירה מעמיקה של הארכיטקטורה המקומית ולייצר תיעוד מקיף שלה. כך, שבמקרים בהם יש צורך לשלב בפתרון ענן פרטי וציבורי, יחד עם נכסים מקומיים ליצירת סביבה היברידית, ניתן יהיה לבחון מחדש את הארכיטקטורה הכללית, ובכלל זה את הארכיטקטורה של הסביבה המקומית, ולבצע את השינויים הנדרשים בארכיטקטורה לצורך הפחתת הסיכונים בסביבה ההיברידית.

2.4. **חוסר אסטרטגיה במעבר לענן**.

יש להחליט מיהו ספק הענן שבשירותיו מעוניין הארגון להשתמש ולקבוע מראש איזה מידע יישאר בסביבה מקומית ואיזה מידע יעבור לתשתיות הענן. לשם כך, יש לבצע כבר בשלבים הראשונים של ההליך מיפוי של מאגרי המידע, תוך תיעוד והבנה מעמיקה של מבנה תשתיות המחשוב הארגוני, היישומים ואופן זרימת המידע בהם.

במידה וקיים במערכות הארגון מידע רגיש, יש לשקול בהתאם לאופי המידע ותהליך בחינת הסיכונים האם לאחסן מידע רגיש זה בסביבה המקומית, ולהשתמש בפלטפורמת ענן ציבורית לגמישות, חוזק מחשוב, מדרגיות וקישוריות. כמו כן, חשוב לדעת מהם היתרונות והחסרונות בבחירת אסטרטגיה של עבודה מול מספר ספקי ענן שכן ריבוי ספקי ענן מצריך התייחסות רחבה יותר מצד הארגון ביחס לאופן בו נדרש להגן על נכסי הארגון ומעלה את רמת הסיכון.

2.5. **אובדן נתונים (Data Loss):** לפני המעבר לענן, יש להקפיד לגבות את כל הנתונים השמורים במערכות הארגון, ובמיוחד את הקבצים המיועדים לעבור לענן. זאת, שכן במהלך הליך העברת המידע לענן, ייתכנו בעיות הקשורות לאובדן נתונים כגון קבצים חסרים, קבצים לא שלמים או קבצים פגומים. לכן, יש להקפיד לגבות את הנתונים טרם העברתם לענן וכן בסיום המיגרציה, על מנת שיתאפשר לאתר כל קובץ פגום או חסר באופן מהיר, במידת הצורך.

2.6. **סיכוני אבטחה:** העברת נתונים לענן עלולה להביא לסיכוני אבטחה רבים, כגון איומים פנימיים, שגיאות מקריות, התקפות חיצוניות, תוכנות זדוניות, הגדרת תצורה שגויה ברשת, מתן הרשאות גישה באופן שגוי, בעיות בצד של ספק הענן, הפרות חוזיות, הפרות תאימות ועוד. לצורך ניהול סיכוני האבטחה והתמודדות עימם, יש לפעול במסגרת מודל חלוקת האחריות להגנה על המידע העסקי לפיו "ההגנה על המידע בתוך הענן חלה על הלקוח", אשר משמעותו היא שהאחריות להגנת המידע המצוי במערכות הארגון, חלה על הארגון עצמו, ולא על ספק הענן.

בהקשר זה חשוב להזכיר כי חובות אבטחת המידע הקבועות בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**התקנות**"), חלות על הארגון, בהתאם לרמת האבטחה החלה על מאגרי המידע של הארגון[1], גם בעת ביצוע מיגרציה לענן, לרבות החובה לקבוע מנגנוני אימות, הגבלת הרשאות, שימוש במנגנוני הצפנה, הדרכות עובדים, תיעוד ובקרה ועוד.

בנוסף, יצוין כי ארגונים נדרשים לבחון אחת לשנה, אם אין המידע שהם שומרים במאגר רב מן הנדרש[2]. חובה זו מקבלת משנה חשיבות בעת המעבר לענן. ועל כן, ארגונים נדרשים לבחון אם יש ברשותם מידע עודף טרם השלמת המעבר לענן.

הפרה של חובות אבטחת המידע, עשויה להוביל לקיום הליכי אכיפה ולהטלת עיצומים כספיים בסכומים משמעותיים על הארגון.

הליך המיגרציה לענן הינו הליך מורכב, ועל מנת ליהנות מיתרונותיו ולצמצם את סיכוני האבטחה הכרוכים בתהליך זה, חשוב למלא אחר ההמלצות לעיל.

[1] רמת אבטחת המידע נקבעת בהתאם להוראות התוספת הראשונה והשנייה לתקנות, ובכלל זה בשים לב לסוג המידע הקיים במאגר והאם הוא כולל מידע מסוגי המידע המפורטים בסעיף 1(3) לתוספת הראשונה, כמו גם כמות נושאי המידע במאגר. יובהר בעניין זה, כי ההגדרות של רמות האבטחה בתוספת השלישית לחוק הגנת הפרטיות, התשמ"א-1981, רלוונטיות אמנם לעניין גובה העיצום הכספי שניתן להטיל בגין הפרת התקנות, לפי הוראות התוספת השלישית, אולם הגדרות אלו אינן קובעות את רמת האבטחה שחלה על המאגר לעניין התקנות עצמן, ולעניין החובות החלות על המאגר לפי התקנות.

[2] תקנה 2(ג) לתקנות אבטחת מידע, התשע"ז-2017.