דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

דואר ישראל

# מערכות המידע בחברת דואר ישראל ובבנק הדואר

# מערכות המידע בחברת דואר ישראל ובבנק הדואר

## רקע

חברת דואר ישראל היא חברה ממשלתית בבעלות מלאה של מדינת ישראל, המספקת שירותי דואר וכן מפעילה שירותים בנקאיים באמצעות חברת הבת שלה - בנק הדואר. נכון לסוף שנת 2023, לחברת הדואר ולבנק הדואר 400 יחידות דואר, 650 מרכזי מסירה וכ-60 מרכזי דוורים אזוריים. כ-11.9 מיליון לקוחות החברה והבנק קיבלו שירות ביחידות הדואר בשנת 2023.

חברת הדואר מספקת ללקוחותיה מגוון שירותים, כגון שירותי דואר בישראל, משלוח מסמכים וסחורות בין ישראל לחו"ל והפעלת רשת מוקדי שליחים המספקת שירותי הפצה ללקוחות עסקיים ופרטיים בכל רחבי הארץ.

בנק הדואר מספק שירותים פיננסיים ללקוחות עסקיים, לגופי ממשלה ולכלל הציבור. בנק הדואר הוא בבעלות ממשלתית ונתון לפיקוח משרד התקשורת, כמו חברת דואר ישראל. שירותי בנק הדואר ניתנים באמצעות כ-400 סניפים של חברת הדואר והם כוללים שירותי אשנב בנקאיים. בבנק הדואר כ-510,000 חשבונות בנק, שיעור הפיקדונות הכולל בבנק זה הוא כ-4.7 מיליארד ש"ח, מתבצעות בו כ-22 מיליון פעולות של לקוחות מזדמנים בשנה ומספר לקוחותיו הכולל הוא כמיליון.

בחברת הדואר ובבנק הדואר יש מגוון רחב מאוד של מערכות מידע, ובכלל זה מערכות תפעוליות המשמשות לצרכים אלה: יצוא ומכס, שירותי דיגיטל, שירותי שליחים, בנק וקמעונאות, מטה, תשתיות ואבטחת מידע, הפעלה וטלפוניה.

באפריל 2023 התגלתה תקיפת סייבר במערכות המידע של הדואר. בבדיקה שביצעו צוותי אבטחת מידע וסייבר של אגף מערכות מידע בדואר ישראל ב-2.4.23 התגלתה פעילות חשודה במערכות המידע של הדואר. ב-5.4.23 הופעל צוות IR[1] של חברה חיצונית שנותנת שירותי הגנת סייבר לדואר ישראל. בחברה הוחלט כצעד מניעתי לנתק את מערכות הדואר מרשת האינטרנט. החברה החיצונית זיהתה עדות לפעילות התוקף במערכות החברה החל מיולי 2022. החברה החיצונית לא הצליחה לזהות את התוקף, והתוקף הצליח להוציא מהארגון את מאגר המשתמשים והסיסמאות. כתוצאה מכך הושבתו שירותים רבים של החברה. בין היתר, לא ניתן היה לבצע תשלומים מקוונים, העברת בעלות רכב, תשלומים להוצאה לפועל והעברות לקופות חולים. כמו כן, חלו עיכובים בשחרור פריטים המגיעים מחו"ל. עם התקדמות עבודת צוות החברה החיצונית הופעלו השירותים בהדרגה.

1 צוות תגובה לאירועי סייבר.

**נתוני מפתח**

**124**
**מיליוני ש"ח**
ממוצע שנתי של הוצאות התפעול וההשקעות של אגף מערכות מידע בשנים 2019 - 2022

**55**
מספר מערכות המידע בחברת דואר ישראל. בבנק הדואר יש 16 מערכות מידע נוספות

**48.75%**
שיעור הירידה של תקציב ההשקעות המתוכנן באגף מערכות מידע מ- 64.2 מיליוני ש"ח בשנת 2019 ל-32.9 מיליוני ש"ח בשנת 2022

**64%**
שיעור הפניות בנושא תקלות חומרה מסך הפניות הקשורות לתקלות שגרמו להשבתת תחנות קצה ביחידות הדואר

**683**
מחשבים בלבד הוחלפו או שודרגו מסך של 1,850 אשר נדרש להחליפם או לשדרגם ל-WIN 10

**85**
בעלי ההרשאות למערכת ג'[2] (ששיעורם 3% מכלל בעלי ההרשאות במערכת זו) אינם מוגדרים במערכת משאבי אנוש כעובדים פעילים בחברה, נכון לינואר 2024

**780**
מבעלי ההרשאות הפעילות במערכת הניהול המרכזי של הרשת[3] (המהווים כ-13% מכלל בעלי ההרשאות במערכת זו) הם עובדים שאינם נכללים ברשימת העובדים הפעילים במערכת משאבי אנוש בחברה

**449**
בעלי הרשאות פעילות מתוך 780 בעלי ההרשאות הפעילות אשר אינם מופיעים כ"פעילים" במערכת משאבי אנוש לא התחברו למערכת הניהול המרכזי של הרשת מתחילת שנת 2024

# פעולות הביקורת

בחודשים יוני 2023 עד מרץ 2024 בדק משרד מבקר המדינה את פעולותיה של חברת דואר ישראל ובנק הדואר בתחום מערכות המידע. הביקורת בוצעה בחברת הדואר ובבנק הדואר. בין יתר הבדיקות משרד מבקר המדינה ביצע בדיקה על אופן ניהול הרשאות המשתמשים בדואר והבקרה עליו. בדיקות השלמה נעשו במשרד התקשורת.

2 המערכת המרכזית לניהול תהליכי אשנב המשמשת גם קופה של דואר ישראל לצורך כל הפעולות הכספיות המבוצעות בסניפים ובסוכנויות.

3 מערכת כלים ייעודית המשמשת לניהול מרוכז של רשתות מחשבים בארגונים.

# תמונת המצב העולה מן הביקורת

- **חיבור ה-SOC של חברת הדואר ל-SOC המגזרי של משרד התקשורת -** כלי חשוב הנכלל במערך ההגנה על נתונים ומשאבים ארגוניים הוא SOC (SECURITY OPERATION CENTER). זהו מרכז פעולות אבטחה המדווח על פעולות חריגות, איומים פוטנציאליים, תובנות על בסיס ממצאי החקר שבוצע בעקבות אירוע ועוד. חברת הדואר מפעילה SOC באחריותו של אגף מערכות מידע בחברת הדואר. שירותי ה-SOC מושכרים מחברה פרטית. בביקורת עלה כי אף שבשנים 2022 - 2023 היחידה המגזרית במשרד התקשורת, המפעילה SOC מגזרי הממומן על ידי משרד התקשורת ומערך הסייבר הלאומי, פנתה כמה פעמים לחברת הדואר בבקשה לחבר את חברת הדואר ל-SOC של משרד התקשורת, במועד סיום הביקורת חברת הדואר טרם התחברה ל-SOC של משרד התקשורת. בכך החברה אינה מנצלת את היתרונות הגלומים בחיבור ל-SOC של משרד התקשורת, ובהם בקרה חיצונית נוספת בעת התרחשותן של תקיפות סייבר.

- **תוכניות עבודה שנתיות ורב-שנתיות בתחום מערכות המידע -** אף שהיקף תקציב אגף מערכות מידע בחברת הדואר הוא מהותי ונע בין כ-102 מיליוני ש"ח לכ-136 מיליוני ש"ח ושיעור תקציב האגף מסך תקציב החברה נע בין 17.2% עד 19.6% (כ-102 מיליוני ש"ח מסך תקציב של כ-592 מיליוני ש"ח בשנת 2022 וכ-136 מיליוני ש"ח מסך תקציב של כ-693 מיליוני בשנת 2020), אין לחברה ולבנק הדואר נוהל להסדרת נושא תוכניות העבודה, ואף בשנים 2019 - 2023 לא הייתה תוכנית עבודה רב-שנתית בתחום מערכות המידע. תהליך גיבוש תוכנית העבודה עד לתום שנת 2023 אינו כולל בחינת חלופות בראייה אגפית, אלא מתבסס בעיקר על תקציב קבוע ומוגדר מראש. לא מתבצע מעקב אחר יישום תוכנית העבודה, ונבצר מהנהלת החברה לדעת בכל רגע נתון מה היא תוכנית העבודה ואילו שינויים בוצעו בה. כמו כן, לא ניתן לעקוב אחר תקציבים שהוסטו ממשימה למשימה, ואף הנהלת אגף מערכות מידע אינה יודעת להעריך כמה שעות עבודה הושקעו בכל משימה. יצוין כי בשנת 2024 החברה הטמיעה תוכנה ייעודית לניהול הצוותים והפרויקטים.

- **תקלות במערכות מידע בדואר ובבנק הדואר -** בשנת 2018 הציג אגף מערכות מידע במצגת את הצורך בהחלפת ציוד מחשוב מיושן ביחידות הקצה, וזאת בשל תקלות חומרה רבות. על פי נתוני החברה, מ-1.4.22 עד 21.7.23 הגישו משתמשי המערכות 46,349 פניות אשר סווגו כתקלות חומרה. מספר הפניות על תקלות בשל בעיות חומרה הוא הגדול ביותר ושיעורו כ-35% מסך הפניות בחברה. בתקופה זו כ-64% מהפניות הקשורות לתקלות שגרמו להשבתת תחנה בנקודת קצה עסקו בתקלות חומרה, שהן 3,306 פניות מתוך 5,178 פניות שנבחנו, וכ-32% מהתקלות שגרמו להשבתה מלאה של יחידות דואר בתקופה הנבדקת היו תקלות חומרה, שהן 525 תקלות מתוך 1,618 תקלות שנבחנו. כמו כן, כ-80% מכלל תקלות החומרה שבגינן הושבתו תחנות קצה וכ-92% מתקלות החומרה שגרמו להשבתה של יחידות דואר הן תקלות בציוד ממוחשב אשר בשנת 2018 חלקו כבר הוגדר כציוד שנדרש להחליפו. מנתונים אלה אפשר ללמוד על היקף הפגיעה של חומרה מיושנת בתפקוד של יחידות הדואר, וכפועל יוצא מכך על פגיעתן בשירות שניתן ללקוחות.

- **פרויקט החלפת ציוד ממוחשב מיושן בחברת הדואר ובבנק הדואר -** פרויקט החלפת הציוד[4] אושר בתוכניות העבודה לשנים 2019 - 2023. בד בבד עם החלפת המחשבים החל גם שדרוג מערכות ההפעלה למערכות הפעלה WIN-10. פרויקט החלפת הציוד הממוחשב הוגדר כפרויקט אסטרטגי כבר בשנת 2019. על אף האמור, רק בתחילת שנת 2022 החלו בחברת הדואר ברכישת ציוד מחשוב חדש. נכון למועד סיום הביקורת, יותר מארבע שנים לאחר שעלה הצורך בהחלפת ציוד מחשוב מיושן, תקלות רבות נגרמות בשל אי-החלפתו, והדבר מחזק את הצורך הדחוף בהחלפת הציוד. עד מרץ 2024 החברה החליפה ושדרגה רק 683 מחשבים (כ-37%) מכלל 1,850 המחשבים שיש לשדרגם ל-WIN-10 ולהחליפם; שדרגה רק 196 (כ-56%) מכלל 350 מחשבי הפלזמה שיש לשדרג ל-WIN-10; וכן שדרגה רק 136 (כ-68%) מכלל 200 המערכות לניהול תורים שיש לשדרג. כמו כן בביקורת נמצא כי הפחת השנתי על מחשבים וציוד נמוך במעט מרכישות של אלה ברוב השנים. סך רכישות המחשבים והציוד ההיקפי בשנים 2019 - 2022 הוא 39.8 מיליוני ש"ח, וסך הפחת השנתי לשנים אלה הוא 37.4 מיליוני ש"ח (כ-94%). מנתונים אלה עולה כי השקעות החברה ברכש תוכנה ומחשבים וציוד היקפי גבוהות רק במעט מהפחת על ההשקעות שנעשו בשנים קודמות, ובשנת 2022 ההשקעה ברכש תוכנה ומחשבים וציוד היקפי הייתה נמוכה מהפחת על ההשקעות שנעשו בשנים קודמות. ניתן להסיק כי החברה שומרת על המצב הקיים ולא דואגת לשיפור מתמיד בתחום מערכות המידע.

- **מערכת ניהול תורים ממוחשבת -** בשנת 2007 החלו חברת הדואר ובנק הדואר להפעיל מערכות לניהול תורים בחלק מיחידות הדואר על ידי שימוש ב"תוכנת מדף". בביקורת נמצא כי המערכת הקיימת אינה מאפשרת ללקוחות החברה להזין מידע על השירות שלשם קבלתו קבעו את התור[5], ואינה מקצה ללקוח זמן נדרש בהתאם לצרכיו. פרק הזמן שנדרש להקצות ללקוח המגיע לאשנב לצורך פתיחת חשבון בנק בבנק הדואר הוא לרוב ארוך בהרבה מפרק הזמן שנדרש להקצות ללקוח המגיע לאסוף חבילת דואר. עקב כך לעיתים עלול להיווצר בסניפי בנק הדואר תור ארוך, והשירות עלול להינתן ללקוחות זמן רב לאחר המועד שנקבע להם. המערכת אינה מאפשרת הזנה של מידע על השירות שלשם קבלתו נקבע התור ואינה מזהה את הפעולות שהלקוח רוצה לבצע. זיהוי מוקדם של הפעולות יכול היה לסייע לעדכון הלקוח מראש במסמכים הנדרשים או בהכנות הנדרשות לקבלת השירות. כמו כן, לקוח יכול לבטל תור ביוזמתו. עם זאת, המערכת אינה שולחת הודעות ללקוחות כדי לוודא שהם מגיעים לסניף לקבלת השירות בתור שנקבע או לחלופין לביטול התור שנקבע. חוסר התאמה של המערכת לניהול תורים לאופי פעילות החברה ולצורכי החברה מקשה את ניהול התורים באופן יעיל ואפקטיבי וגורם לפגיעה בשירות ללקוח.

- **ריבוי מערכות והיעדר ממשק ביניהן -** במועד סיום הביקורת מופעלות בחברת הדואר 55 מערכות מידע, שחלקן נחלקות לתתי-מערכות, ובבנק הדואר יש 16 מערכות נוספות שחלקן נחלקות לתתי-מערכות. למערכות אלו יש יותר מ-20 ספקים שונים, והן מבוססות על טכנולוגיות שונות. ריבוי המערכות והיעדר ממשק ביניהן מובילים לפגיעה באינטגרציה בין המערכות, בחוסר אחידות בנתונים ובקושי בניהול תהליכים. בשל היעדר האינטגרציה בין המערכות בחברה ובבנק נוצר קושי בסנכרון נתונים בין מערכות, והדבר עלול לגרום לטעויות. לפיכך, החברה משקיעה בתשומות כוח האדם או בפיתוח תהליכים ידניים מפצים,

4 מחשבים, מדפסות, עמדות ממוחשבות לניהול תורים, מסכי מחשב וציוד חומרה נוסף.

5 מלבד העברת בעלות רכב.

כגון תהליכים ליצירת התאמה בין המערכות או תהליכים לפיתוח מערכות נוספות. כך לדוגמה, למערכת מידע משאבי אנוש אין ממשק ממוחשב עם מערכת המחשב המרכזי[6] של הבנק. לצורך ביטול הרשאות של עובד[7] במערכת המחשב המרכזי נעשות פעולות ידניות מפצות: נשלח דוא"ל מאגף משאבי אנוש לבעלי תפקידים במערכת המחשב המרכזי בבקשה לבטל את הרשאות העובד במערכת. נדרשת פעולה של ביטול ההרשאות. נוסף על כך, פעם בחודש מתבצע תהליך של בקרה מפצה הכולל הפקת דוח חריגים בעניינם של כל העובדים שפרשו או עזבו וטרם נותקו ממערכת המחשב המרכזי, ובדיקה ידנית של המקרים החריגים. הערך החד-ערכי במערכת המידע של אגף משאבי אנוש שונה מהערך החד-ערכי במערכת המחשב המרכזי. כמו כן, בשל הבדלים ברישום העובדים בשתי המערכות, יצרה החברה טבלת המרה ידנית, וזאת כדי לקשר בין מספר הזהות של העובד לשם המשתמש במערכות הבנק. טבלת ההמרה אמורה להתעדכן ידנית כפתרון המפצה על חוסר ההתאמה בנתונים.

- **סקירת הרשאות תקופתית בחברת הדואר -** פעמיים בשנה, בינואר ובאוגוסט, החברה מבצעת סקירת הרשאות ידנית של 17 מערכות ליבה. עם זאת, ביתר המערכות בחברת הדואר לא מתבצעת סקירת הרשאות, כנדרש בנוהל משתמשים והרשאות. כמו כן, לא מתבצע תהליך המציג את החריגות שנמצאו במהלך הבדיקה, אף שהדבר היה יכול לסייע בזיהוי של מערכות או אגפים אשר יש בהם באופן קבוע מספר חריגות רב ולתת להם מענה בהתאם לכך. כמו כן, לא מתבצע תהליך בקרה ממוחשב נוסף הבוחן את מידת התאמתן של ההרשאות לבעלי ההרשאה. למשל, ייתכן שעובד יחליף תפקיד עם עובד אחר במחלקה ולצורך תפקידו החדש נדרש לבצע שינוי בהרשאות המוקצות לו, אך המנהל העסקי המבצע את הסקר לא יהיה ער לשינוי הנדרש.

- **בדיקת הרשאות במערכת ג' בחברת הדואר -** בבדיקת צוות הביקורת נמצא כי נכון לינואר 2024, 85 מבעלי ההרשאות למערכת ג' (ששיעורם 3% מכלל בעלי ההרשאות במערכת זו) אינם מוגדרים במערכת משאבי אנוש כ"פעילים". כלומר, הרשאתם של עובדים שעזבו או פרשו מהחברה לא נותקה, ולחלופין מעמדם לא עודכן במערכת משאבי אנוש. עוד נמצא כי למרות ביצוע בקרות אוטומטיות מפצות על ידי החברה, חלו שגיאות בתהליך הבקרה הממוחשבת האוטומטית. ממצאי הביקורת העלו כי לא אותרו בבקרה האוטומטית 79 עובדים שלהם הרשאות פעילות ומנגד אינם "פעילים" במערכות משאבי אנוש.

- **הרשאות במערכת הניהול המרכזי של הרשת בחברת הדואר -** ממצאי הביקורת העלו כי נכון לדצמבר 2023, 780 (כ-13%) מבעלי ההרשאות הפעילות במערכת הניהול המרכזי של הרשת הם עובדים שאינם נכללים ברשימת העובדים הפעילים במערכת משאבי אנוש בחברה. 449 (כ-58%) מתוך 780 עובדים בעלי הרשאות שאינם מוגדרים כ"פעילים" לא התחברו למערכת הניהול המרכזי של הרשת מתחילת שנת 2024 ואילך. אין מידע על תאריך ההתחברות האחרונה של 196 (כ-25%) מבעלי ההרשאות, וידוע כי מועד ההתחברות האחרונה של 135 (כ-17%) מהעובדים היה בשנת 2024. ניתן להסיק כי עובדים שלא התחברו לאחר שנת 2023 וכן עובדים שאין מידע לגבי מועד התחברותם האחרונה הם עובדים שעזבו את החברה אך לא בוטלו הרשאותיהם. עובדים אשר התחברו לאחרונה

6 מחשב מרכזי המשמש להפעלת יישומים רבים בעת ובעונה אחת, תוך שימוש בעיבוד נתונים בהיקף רחב.

7 בשל עזיבה או פרישה.

בשנת 2024, שהם ככל הנראה עובדים פעילים בחברה, עדיין הופיעו במערכת כוח האדם כעובדים שאינם "פעילים". 70 מ-80 העובדים בעלי ההרשאות הפעילות שנכללו במדגם שדגם צוות הביקורת[8] כלל אינם עובדים בדואר. הרשאותיהם של שישה מהעובדים, שעזבו את חברת הדואר כבר בשנת 2020, עדיין לא בוטלו במועד המדגם, יותר משלוש שנים לאחר עזיבתם. כמו כן לא בוטלו ההרשאות של עובד אחר, שעזב את החברה כבר בשנת 2021, ושל שלושה עובדים שעזבו בשנת 2023. אי-ביטול הרשאות לעובדים שאינם "פעילים" עלול לגרום למצב שבו בלתי מורשים עושים שימוש בהרשאותיהם התקפות לצרכים זדוניים ולפגיעה בחברה.

**בדיקת ההרשאות במחשב המרכזי בבנק הדואר -** נמצא כי 35 (כ-2%) מתוך 1,794 ההרשאות הפעילות במחשב המרכזי של בנק הדואר שייכות לעובדים שאינם מוגדרים כפעילים במערכות כוח האדם. אומנם לרוב המשתמשים נדרשים תחילה להיכנס למערכת הניהול המרכזי של רשת הבנק כדי להתחבר למחשב המרכזי, אולם ממצאים אלה חמורים בשל חשיבות רמת אבטחת המידע הגבוהה בבנק. הותרת הרשאות פעילות למערכות הבנק לעובדים שאינם מועסקים בחברה עלולה לאפשר פגיעה באבטחת המידע.

**בדיקת ההרשאות במערכת הניהול המרכזי של רשת בנק הדואר -** נמצא כי 67 משתמשים בעלי הרשאות פעילות אינם מוגדרים כ"פעילים" במערכות משאבי אנוש או שלא ניתן לאתרם. לאחר בחינת כלל העובדים נמצא כי 58 מהם הם אנשי מערכות מידע שהם עובדים פעילים חיצוניים. בדיקת תשעת המשתמשים הנוספים העלתה כלהלן: הרשאותיהן של שלוש עובדות ששהו בחופשת לידה לא בוטלו אף שעל פי נוהל ניהול הרשאות עובדים יש לבטל הרשאות לעובדים הנעדרים מהעבודה למשך יותר מחודש ימים קלנדרי. עובד נוסף פרש מהבנק כבר ב-30.6.23 ולאחר מכן חזר לעבוד אך אינו מוגדר כעובד פעיל באגף משאבי אנוש. עובדת נוספת פרשה מהבנק אך עדיין יש לה הרשאות, ושלושה עובדים נוספים הם עובדים פעילים אך אינם מוגדרים ככאלה במערכות משאבי אנוש, אף ששמותיהם ומספר הזהות שלהם נכללים בטבלת ההמרה. כמו כן, נמצא כי שם המשתמש של עובד אחר שעזב עדיין משמש עובדים אחרים. עקב אי-ביטול הרשאותיהם של עובדים שאינם פעילים למערכות בנקאיות רגישות נפגעת אבטחת המידע של הבנק, ונשקף סיכון לחדירת גורמים לא מורשים למערכותיו.

**תהליך איסוף המאזנים מסניפי הדואר -** מדי יום נהגי החברה אוספים את האסמכתאות הפיזיות לפעולות הבנקאיות ביחידות הקצה לשקים (מאזנים[9]) ומעבירים אותם למטה בנק הדואר שבמרכז המיון במודיעין. נמצא כי החברה אינה עומדת ביעדים שקבעה לעצמה (85% מהמאזנים מגיעים ביום למוחרת) ורק 70% מהמאזנים מגיעים למטה הבנק בתוך יומיים. הבקרה והמעקב בנוגע להגעת המאזנים למטה בנק הדואר אינה מלאה, והמעקב היומי אינו מתבצע אחר מאזנים שאינם מיום העסקים הקודם, כך שלא ניתן לדעת אם מאזן כאמור הגיע לדואר אלא רק בבדיקה החודשית. כמו כן, לא מתבצע מעקב המשך לאחר בדיקה זו. עוד נמצא כי המאזנים הושארו במשך שעות ממושכות באולם המיון ללא השגחה

8 80 מסך 780 בעלי הרשאות פעילות במערכת הניהול המרכזי של הרשת שאינם נכללים ברשימת העובדים הפעילים במערכת משאבי אנוש בחברה.

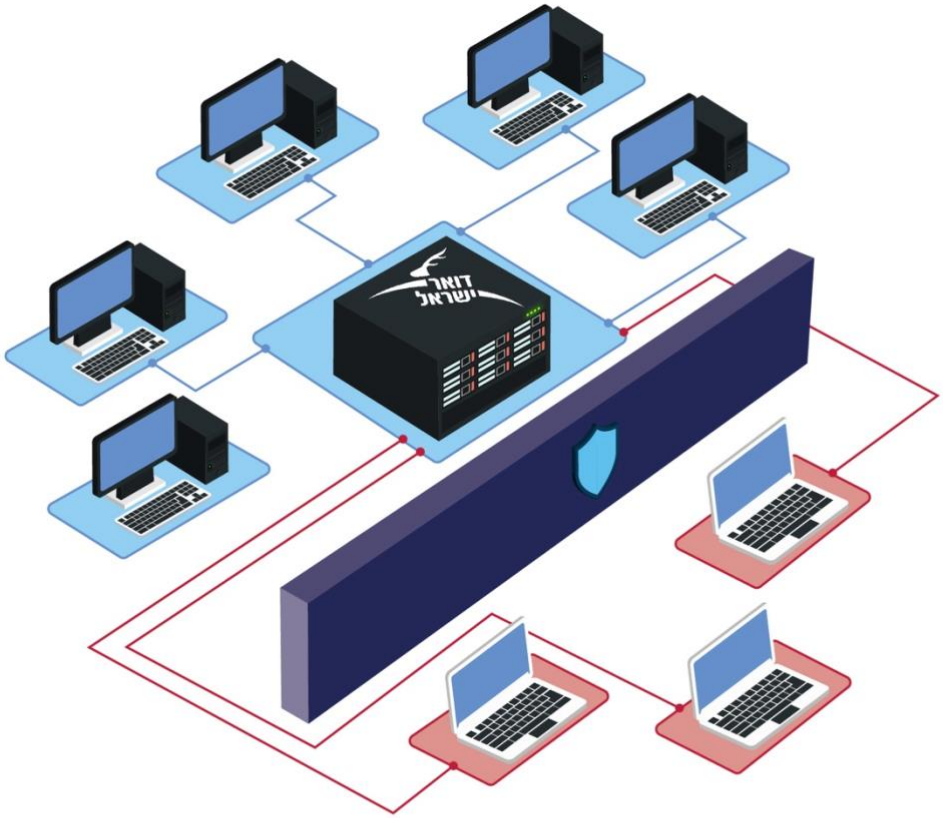
9 מאזנים אלו כוללים בין היתר, המחאות, שוברים, טפסים בנקאיים והמחאות למשמרת.

ותוך סיכון ממשי לגניבתם או לחשיפתם בפני גורמים שאינם מורשים לכך. תופעה זו נמשכה שנים.

## עיקרי הביקורת

- על החברה לגבש נוהל להסדרת נושא תוכניות העבודה השנתיות והרב-שנתיות ולוודא את יישום הנוהל תוך הקפדה על בחינת חלופות, מעקב אחר יישום תוכנית העבודה וניהול תוכנית העבודה בצורה המאפשרת להנהלת אגף מערכות מידע ראייה כוללת בכל רגע נתון על המשימות המתבצעות, עלותן והיקפן.
- על החברה לפעול להשלמה של פרויקט החלפת הציוד המיושן ביחידות החברה בהקדם, וזאת כדי לצמצם סיכונים ולשפר את השירות הניתן ללקוחות.
- על החברה לפעול למימוש ההמלצה שבתוכנית האב משנת 2021 למניעת כפילויות ופעילויות מיותרות באמצעות תכלול, גיבוש והבניה של פעולות ותהליכי עבודה לפיתוח מסגרות משותפות ואחודות באמצעות טכנולוגיות דיגיטליות ומידע.
- על החברה לבצע בדיקת הרשאות שגרתית במערכת הניהול המרכזי של הרשת כדי למזער את הסיכון הכרוך במתן הרשאות לעובדים שאינם זכאים לכך וכדי שיתאפשר ניהול ההרשאות של מערכות רבות. כמו כן, על החברה לבחון את תהליך בדיקת ההרשאות במערכת ג' ובכלל המערכות הנבדקות כדי לאתר כשלים בתהליך איתור העובדים שאינם "פעילים", בין היתר במסגרת סקירת ההרשאות הידניות. נוסף על כך, על החברה לאתר את כלל העובדים שמוגדרים כמשתמשים לא פעילים ויש להם הרשאות במערכות השונות ולבחון לעומק את מנגנון הבקרה על הרשאות המשתמשים ולשפרו בהתאם לממצאים.
- על החברה לעבות את הבקרות הנערכות בבנק הדואר ולהשוות באופן שוטף את נתוני בעלי ההרשאות התקפות אל מול נתוני אגף משאבי אנוש. כמו כן, עליה לפתח תהליכים אוטומטיים לניתוק הרשאות ממערכות הבנק ולבצע בקרות על הרשאות אלה.

## ממצאי הביקורת בבדיקת הרשאות במערכת הניהול המרכזי של הרשת בחברת הדואר




**780**

**מבעלי ההרשאות הפעילות במערכת הניהול המרכזי של הרשת אינם נכללים ברשימת העובדים הפעילים בחברה.**

# סיכום

בחברת הדואר 55 מערכות מידע שחלקן נחלקות לתתי-מערכות, ובבנק הדואר יש 16 מערכות נוספות שחלקן נחלקות לתתי-מערכות. למערכות אלו יש יותר מ-20 ספקים שונים, והן מבוססות על טכנולוגיות שונות.

דוח זה מעלה ליקויים בתחומי מערכות המידע ואבטחת המידע בחברת הדואר ובבנק הדואר, ובהם ניהול לקוי של תהליך ביטול הרשאות לעובדים וליקויים בבקרה על תהליך זה; שימוש בציוד ממוחשב מיושן הפוגע הן בשירות ללקוחות החברה והבנק והן באבטחת המידע; היעדר תוכנית עבודה רב-שנתית לאגף מערכות מידע; היעדר מעקב אחר ביצוע תוכניות העבודה; ריבוי מערכות שמקשה את העברת המידע בין המערכות ועקב כך מעורר צורך בביצוע הליכים ידניים ובהשקעת משאבים בחברה כדי לפצות על כך.

על אגף מערכות המידע בחברת הדואר לקבוע תוכנית פעולה מוסדרת הכוללת פיתוח מערכות מידע בראייה עתידנית, שדרוג מערכות ישנות ומיטוב של המערכות הקיימות ושל האינטגרציה ביניהן, כל זאת תוך הקפדה על הגנת הסייבר וצמצום החשיפה לסיכונים שמקורם בהיבטים שונים של שימוש שאינו מורשה.

על החברה לפעול, במסגרת שיפור אבטחת המידע, ובייחוד - לנוכח אירוע סייבר שהתרחש בה באפריל 2023 - לשיפור הבקרה על ניהול ההרשאות בחברה. על החברה לבחון את הליקויים שהועלו בביקורת בנושא זה ולגבש דרכים לתיקונם המיידי.