

ז' חשון תשפ"ב
13 אוקטובר 2021

דוח ריכוז ממצאי ביקורת רוחב בנושא היבטים טכנולוגיים בפעילות זירות הסוחר מיועד לזירות הסוחר

במהלך שנת 2023, בחנה מחלקת ביקורת והערכה ברשות באמצעות שאלון את אופן יישום ההמלצות שפורטו במסגרת חוזר התובנות שלהלן, בקרב זירות הסוחר. בעקבות הבחינה הוחלט לעדכן את חוזר התובנות. העדכונים בוצעו ביחס לתובנות מס' 1, 3 ו-5 להלן, והם משקפים ליקויים רוחביים אשר עלו בבחינת יישום התובנות ועמדות הסגל לגביהם. העדכון נכון לפברואר 2024.

רקע

זירות הסוחר (להלן: "הזירות") הן פלטפורמות מסחר ממוחשבות, המאפשרות למשקיעים לסחור מול מפעילי הזירות באמצעות מכשירים פיננסיים שונים. הפעילות העסקית של זירות הסוחר עתירת טכנולוגיה, ונשענת ברובה על שירותי מיקור חוץ הניתנים בחלקם על ידי חברות הקשורות לזירה.

סעיף 44(א) לחוק ני"ע, התשכ"ח-1968 קובע כי "חברה בעלת רישיון זירה תנהל את זירת הסוחר באופן תקין והוגן". בנוסף, סעיף 44(ב)(4) לחוק קובע כי רשות ני"ע תיתן רישיון זירה לחברה אשר לה "מיומנות טכנית ואמצעים מתאימים לצורך הפעלת זירת הסוחר **באופן שיבטיח את יציבות הזירה, אמינותה, זמינותה ואבטחת המידע שבה**", כאשר חובה זו חלה על הזירה גם ביחס להתנהלותה השוטפת, כמוסדר בסעיף 44(ד) לחוק: "חברה בעלת רישיון זירה תעמוד, **בכל עת**, בתנאים הקבועים בסעיף 44(ב)(1), (2), (4) ו-(5)" (ההדגשות אינן במקור).

פעילות הזירות אף הוסדרה במסגרת תקנות ניירות ערך (זירת סוחר לחשבונו העצמי), התשע"ה-2014 (להלן: "התקנות"). תקנה 2(א)(8)(יט) לתקנות מחייבת את זירת הסוחר לצרף לבקשה לרישיון תיאור של המערכת הטכנולוגית שבאמצעותה תספק את שירותיה, ובכלל זה תיאור גורמים חיצוניים לזירה המתפעלים את המערכת הטכנולוגית או חלק ממנה ותחומי אחריותם, ממשקים של המערכת הטכנולוגית עם גורמים חיצוניים לזירה, מערך שמירת הנתונים, גיבוי, אבטחת מידע ומנגנוני בקרה, בצירוף חוות דעת מומחה המאשרת כי המערכת פועלת בהתאם לתקנים מקובלים. בנוסף, תקנה 34 לתקנות קובעת כי "חברה תסדיר בנהלים את אופן שמירת המסמכים כדי להבטיח את קיומם, הגנתם מפני נזקים, הגישה אליהם, סודיות כלפי הלקוח, אפשרות גיבוי המידע, אחזור המידע ואיתור מסמכים במידת הצורך".

מחלקת ביקורת והערכה

בחודשים פברואר-יולי 2021 נערכה על ידי סגל מחלקת ביקורת והערכה ברשות ני"ע ביקורת רוחב אצל זירות הסוחר, בנושא 'היבטים טכנולוגיים בפעילות הזירות'. מטרת הביקורת הייתה לוודא, בין היתר, כי ניהול הסיכונים הטכנולוגיים על ידי זירות הסוחר, מבוצע באופן נאות.

חוזר זה נועד לשקף את עמדת סגל הרשות במספר סוגיות אשר התגבשו במהלך הביקורת ויפורטו להלן. מצופה כי הזירות יפעלו ליישום התובנות המוצגות במסמך זה, ככל שהן רלוונטיות לגביהן.

ממצאי הביקורת ועמדות הסגל לגביהם

1. קבלת שירותים במיקור חוץ

זירות הסוחר מתבססות על קבלת שירותים במיקור חוץ ביחס לפלטפורמות המסחר המשמשות את הלקוחות. לרוב, שירותים אלו מתקבלים באמצעות חברות אחרות בקבוצה אליה משתייכת הזירה, בין אם מדובר בפלטפורמת מסחר שהיא פרי פיתוחה של הקבוצה או כזו שנרכשה מספק חיצוני על ידי אחת מחברות הקבוצה. מסגרת התקשרות דומה קיימת גם ביחס לשאר מערכות המחשוב התומכות בפעילות העסקית של זירות הסוחר.

מסקירת דפוסי הפעילות בזירות הסוחר ומעיון במסמכי ההתקשרות של הזירות מול ספקי המערכות עולה, כי חלק מהזירות אינן מבצעות בחינה עצמאית של נאותות הספק, קביעת רמת שירות נדרשת (SLA) וכן בקרה על עמידתו בתנאי החוזה והערכת טיב ההתקשרות עמו. לצורך כך, מסתמכות הזירות על בדיקת נאותות של הספק המבוצעת על ידי חברות אחרות בקבוצה, כאשר בדיקות אלו נערכות לרוב מנקודת ראות החברה המתקשרת בלבד, ועל כן אינן מבטיחות בהכרח את התאמת רמת השירות המתקבלת לצרכיה הפרטניים של הזירה ולדפוסי עיסוקה. נציין כי אמירה זו רלוונטית גם בכל הקשור לרמת המומחיות והניסיון של אנשי המקצוע המספקים שירותי מיקור חוץ לחברות בקבוצה, וכן ביחס לבחינת הלימת מדיניות ההמשכיות העסקית של ספקי החוץ למדיניות הזירה ולצרכיה בעניין זה.

בחלק מהמקרים אף נמצא כי קיימת לזירות תלות בספק מיקור חוץ יחיד, וכי יכולתן לצמצם את הסיכון הנובע מכך מוגבלת. יודגש כי הפסקת קבלת שירות מספק יחיד עלולה לפגוע ברציפות מתן השירות של הזירות.

לעמדת סגל הרשות, על זירות הסוחר לנקוט בגישה פרואקטיבית בכל הקשור לניהול הסיכונים הגלומים בקבלת שירותי מיקור חוץ, ולכלל הפחות לקבל עדכונים שוטפים ביחס לאופן הטיפול בסיכונים אלו על ידי חברות אחרות בקבוצה.

בכל הקשור לחוזי התקשרות עם ספקי מיקור חוץ, דרך המלך לעמדתנו היא התקשרות ישירה של הזירה מול ספקי החוץ, באופן בו תוכל הזירה לבצע בחינה עצמאית של נאותות הספקים וכן לבחון התאמה של רמת השירות לצרכיה הפרטניים ודפוסי עיסוקה. במקרים בהם חוזי מיקור החוץ נערכים מול חברות אחרות בקבוצה אליה משתייכת הזירה (להלן: "הקבוצה"), מומלץ להתקשר בחוזה מול הקבוצה אשר יכלול את פירוט השירותים שיסופקו, וכן פרטים בנוגע לטיבם ואיכותם. לחלופין, מומלץ לזירה לוודא כי תהליך בחינת הנאותות של ספק מיקור החוץ על ידי הקבוצה בוצע באופן מקיף תוך התייחסות להיבטים החשובים לזירה, וזאת טרם ההתקשרות עמו. כמו כן, יש לוודא, לכל הפחות, כי תנאי חוזי ההתקשרות מאפשרים לזירה להתנהל כחברה עצמאית, בין היתר בהיבטים של דרישות רגולציה.

בכל הקשור לשירותי מחשוב ואבטחת מידע, מומלץ לקבוע קריטריונים לגבי מומחיות וניסיון של אנשי מקצוע המספקים שירותים אלה בפועל, ולוודא עמידתם בקריטריונים אלה. כמו כן, על זירות הסוחר לוודא כי ספקי מערכות המחשוב הקריטיות מקיימים מדיניות המשכיות עסקית ומדיניות אבטחת מידע התואמות את מדיניות הזירה וצרכיה.

במקרים בהם קיימת תלות בספק מיקור חוץ יחיד, מומלץ על ביצוע הפעולות דלהלן:

- **קיום דיונים על הסיכון הנגזר ממצב דברים זה בדירקטוריון ובהנהלה;**
- **איתור אפשרויות לצמצום הסיכון ובחינתן באופן מעשי;**
- **מתן ביטוי בתכנית ההמשכיות העסקית של הזירה לאופן התמודדותה עם סיכון של ספק יחיד, שכן היעדר טיפול בסיכון זה עלול לשבש את יכולתה להפעיל את תכנית ההמשכיות העסקית שלה במקרה הצורך;**
- **מתן התייחסות לסיכון זה בדוחות התקופתיים במסגרת פרק "חשיפה לסיכונים ודרכי ניהולם"¹.**

2. שמירת מידע על אודות לקוחות הזירה

כאמור, תקנה 34 לתקנות קובעת כי "חברה תסדיר בנהלים את אופן שמירת המסמכים על מנת להבטיח את קיומם, הגנתם מפני נזקים, הגישה אליהם, סודיות כלפי הלקוח, אפשרות גיבוי המידע, אחזור המידע ואיתור מסמכים במידת הצורך". גישת הלקוחות לפלטפורמת המסחר ולכלל המידע הפיננסי האישי הנלווה לפעילותם, נערכת באופן מאובטח באמצעות אתרי האינטרנט של הזירות. עם זאת, חלק מממשקי הזירות מול לקוחותיהן מנוהלים באמצעות דואר אלקטרוני, בפרט במקרים בהם נשלחים לבקשת הלקוחות דוחות הכוללים מידע פיננסי רגיש. דוחות אלו מועברים באופן לא מאובטח וללא הצפנה באמצעות סיסמה, דבר המעלה את הסיכון לדליפת מידע וחשיפתו לגורם בלתי מורשה.

לעמדת סגל הרשות, על זירות הסוחר לוודא כי העברת קבצים המכילים מידע רגיש הנוגע ללקוחותיהן מחוץ לכותלי הארגון, לרבות ללקוח עצמו, תעשה באופן מוצפן בלבד. בנוסף, יש לעגן את אופן העברת המידע כאמור בנוהל אבטחת מידע.

3. עריכת סקר סיכוני סייבר

ממענה לשאלון הביקורת ומשיחות שהתקיימו עם הנהלת הזירות עולה, כי במרביתן לא נערכה הערכת סיכוני סייבר בשנתיים האחרונות. עניין זה מקבל משנה תוקף נוכח מעבר גורף של עובדי הזירות לעבודה מהבית באמצעות חיבור מרחוק למערכות הארגוניות, אשר התבצע ללא הערכה מקדימה של סיכוני סייבר הכרוכים בהליך זה². היעדר הערכה כאמור, עלול להקשות על הזירות לנהל את סיכון הסייבר באופן נאות ולמזער ככל הניתן את מידת התממשותו בפועל, ובכך עלול להפוך את הזירות לפגיעות יותר לאיומים מסוג זה.

עוד יצוין כי במסגרת בחינת יישום ההמלצות נמצא כי רוב זירות הסוחר לא קבעו כלל תדירות מחייבת לביצוע הערכת סיכוני סייבר.

לעמדת סגל הרשות, על זירות הסוחר לבצע בהקדם האפשרי הערכת סיכוני סייבר אשר תכלול, בין היתר, התייחסות לסיכונים הגלומים במעבר עובדים לעבודה מרחוק. עוד יודגש, כי היעדר

¹ לעניין זה ראו סעיף הנוגע לתלות בספקי חוץ במסגרת עמדת סגל משפטית בנושא 'תיאור המערכת הטכנולוגית בדוח פרטים נוספים, המוגש לרשות כחלק מבקשת הרישיון לניהול זירת סוחר', אשר פורסמה בתאריך 08/01/2015.

² לעניין זה ראו [חוזר תבנות](#) בנושא 'סיכוני סייבר בחיבור מרחוק למערכות הארגוניות', אשר פורסם ב-14/06/2021.

קביעת תדירות לביצוע הערכת סיכוני סייבר, אינו עולה בקנה אחד עם הפרקטיקה המקובלת בתחום³. לפיכך, ובשל הדינאמיות המאפיינת את עולם הסיכונים הסייבר ואבטחת המידע ותכיפות השינויים בו, מומלץ לבחון ולקבוע תדירות סבירה לביצוע הערכת סיכוני סייבר.

4. מודעות עובדים לסיכונים אבטחת מידע

הגורם האנושי מהווה אחד מסיכונים אבטחת המידע הגדולים ביותר. משיחות עם נציגי זירות הסוחר ומעיון במסמכים הרלוונטיים שהועברו במסגרת הביקורת עלה, כי כל זירות הסוחר משקיעות משאבים בהעלאת מודעות עובדיהן לסיכונים סייבר, בין היתר באמצעות עריכת הדרכות מתאימות ושליחת עדכוני אבטחת מידע בדואר אלקטרוני. יחד עם זאת, שני אירועי סייבר שהתרחשו בשנה האחרונה בשתי זירות סוחר (בכל זירה אירוע אחד), וגרמו לשיבוש בתהליכים עסקיים באותן זירות, מעלים שאלות בדבר אפקטיביות תכניות העלאת מודעות העובדים הקיימות בזירות, כמפורט לעיל.

מומלץ לזירות הסוחר לפעול לבנייתה של תכנית מקיפה המשלבת הדרכות, עדכוני מידע ותרגולים להעלאת מודעות עובדיהן לסיכונים אבטחת מידע. בנוסף, מומלץ כי יעילות התכנית תיבחן בתדירות תקופתית על בסיס קריטריונים שייקבעו מראש.

5. המשכיות עסקית, גיבויים ושחזורים

קיימת חשיבות גדולה בקיום הלימה בין תכנית המשכיות העסקית ובין השינויים שמתרחשים בחברה בפן העסקי ובפן הטכנולוגי, וזאת על מנת לשמור על האפקטיביות שלה. במסגרת בחינת יישום ההמלצות נמצא כי חלק מזירות הסוחר לא ערכו שינויים בתכניות המשכיות העסקית שלהן, ממועד פרסום דוח ריכוז ממצאי ביקורת זה, זאת חרף השינויים הדינמיים והתדירים בתחום הטכנולוגי והעסקי.

כמו כן, בשיחות שהתקיימו עם הנהלת הזירות התברר, כי תחזוקת תכנית המשכיות העסקית ותפעול מערך הגיבויים והשחזורים, לרבות ביצוע תרגולים של התכנית ובדיקות תקינות הגיבויים, נערכות על ידי חברות אחרות בקבוצה, כאשר עובדי הזירות כמעט ולא נוטלים בהם חלק ולעיתים אף אינם מודעים על קיומם (וכך גם הנהלות הזירות). יודגש, כי מעורבות עובדים בתרגילי הערכות לחירום מהווה נדבך מהותי בתחזוקת תכנית המשכיות העסקית והצלחתה, ומאפשרת רכישה ותרגול של המיומנות הנדרשת לצורך תפקודם בעת חירום. כמו כן, קיום מערך גיבויים תקין המותאם לצרכיה העסקיים של הזירה, מהווה תנאי מתלה לרציפות פעילות הזירות הן בקרות אירוע חירום והן כחלק מתפקודן השוטף.

לעמדת סגל הרשות, קיימת חשיבות רבה בביצוע בחינה תקופתית של תכנית המשכיות העסקית ועדכונה בהתאם להתפתחויות בתחום, על מנת לשמור על יעילותה והאפקטיביות שלה.

כמו כן, על זירות הסוחר ליטול חלק פעיל בתרגולי המשכיות עסקית המבוצעים ברמת הקבוצה. בהקשר זה נדגיש, כי מעבר לעבודה מרחוק בשגרה אינו מהווה תחליף לתרגול תכנית המשכיות

³ בהתאם לפרקטיקה המקובלת בתחום, אשר גם מיושמת על ידי חלק מזירות הסוחר, הערכת סיכונים סייבר מבוצעת

בתדירות שנתית, ככלל, בין שנה לשלוש שנים.

העסקית, היות שתרגול זה אמור לבחון את כלל היבטי היערכות הזירה לתפקוד בעת חירום, ולא רק בהתבסס על יכולתם של עובדיה להתחבר לשרתיה מרחוק.

בכל הקשור לגיבויים, על זירות הסוחר לוודא כי בדיקות תקינות הגיבויים כוללות גם גיבויים של כלל מאגרי הנתונים הרלוונטיים לפעילותן. עוד מומלץ כי הזירה תקבל מספקי השירות, לכל הפחות, דיווחים תקופתיים על תקינות הגיבויים ותקלות שאירעו בתהליך.

* * *