



מדינת ישראל
רשות שוק ההון, ביטוח וחסכון

יא' באלול התשפ"ג
28 באוגוסט 2023

חוזר נותני שירותים פיננסיים
2022-369
סיווג: כללי > טיוטה <

ניהול סיכונים סייבר בנותני שירותים פיננסיים (תיקון) - טיוטה

בתוקף סמכותי לפי סעיפים 4(א) ו-39(א) לחוק הפיקוח על שירותים פיננסיים (שירותים פיננסיים מוסדרים), תשע"ו-2016 (להלן – "חוק הפיקוח על שירותים פיננסיים"), ובתוקף סמכותי לפי סעיפים 29(ג), 35(ב), ו-62(ב) לחוק שירות מידע פיננסי, התשפ"ב-2021 (להלן – "חוק שירות מידע פיננסי"), ולאחר התייעצות עם הוועדה המייעצת, להלן הוראותיי:

1. כללי

ביום 29 במאי 2022 פורסם על ידי המפקח חוזר נותני שירותים פיננסיים מספר 2022-10-9 שעניינו ניהול סיכונים סייבר בנותני שירותים פיננסיים מוסדרים (להלן – חוזר ניהול סיכונים סייבר).

החוזר מגדיר עקרונות המחייבים כי ניהול סיכונים סייבר יתבצע באופן אפקטיבי, עדכני ושוטף, על בסיס עקרונות ממשל תאגידי נאותים הכוללים, בין השאר, התייחסות לשיטות, לתהליכים ולבקורות, ובאופן המאפשר להתמודד עם איומי סייבר וניהול אירועי סייבר.

במסגרת התיקון לחוזר זה מוצע להרחיב את תחולת הוראות החוזר כך שיחול גם על יוזם תשלומים המוגדר בסימן ב' ('שירות ייזום תשלומים') לחוזר בנקאות פתוחה זאת במסגרת התחברות למערכת הבנקאות הפתוחה שבה ניתן אישור לנותן שירותים פיננסיים לפעול כיוזם תשלומים ולאור סיכונים סייבר שיוזם התשלומים חשוף אליהם בפעילות זו.

2. תיקון החוזר המאוחד

בחוזר המאוחד לעניין שירותים פיננסיים מוסדרים, בחלק 5 ('ניהול סיכונים והלבנת הון'), בפרק 3 ('ניהול סיכונים סייבר') יבוא סימן א' ('ניהול סיכונים סייבר בנותני שירותים פיננסיים') וסעיפים 1-6, המצורפים כנספח לחוזר זה.

3. תחולה

הוראות חוזר זה יחולו על:

א. בעל אישור לפעול כיוזם תשלומים כהגדרתו בסימן ב' (שירות ייזום תשלומים) לחוזר המאוחד לעניין שירותים פיננסיים מוסדרים, בחלק 6 ('הוראות נוספות'), בפרק 1 ('בנקאות פתוחה').

4. תחילה

תחילתו של חוזר זה ביום 29 בנובמבר 2023.

עמית גל

המפקח על שירותים פיננסיים מוסדרים (בפועל)

הוראות ניהול סיכוני סייבר

1. הגדרות

בסימן זה –

“איום” – אפשרות פוטנציאלית לפגיעה בסודיות, שלמות או זמינות מערכות או מידע של נותן השירותים הפיננסיים;

“אירוע סייבר” – כל מקרה של תקיפת מערכות או אמצעי טכנולוגי אחר ששייכים לנותן השירותים הפיננסיים, העלולה לפגוע בסודיות, שלמות או זמינות מערכות או המידע של נותן השירותים הפיננסיים;

“אמצעי זיהוי” – אמצעי המאפשר אימות פרטים של אדם או מערכת, בעת ניסיון גישה או ביצוע פעולות מטעמים במערכת מידע. אמצעי זיהוי כולל אחד מאלה:

(א) Something You Are – תכונה פיזיולוגית ייחודית של המשתמש;

(ב) Something You Have – פריט הנמצא ברשות המשתמש;

(ג) Something You Know – פריט מידע הידוע למשתמש.

“גישה מרחוק” – התחברות גורם (חיצוני או פנימי) מחוץ לרשת של נותן השירותים הפיננסיים אל הרשת הפנימית של נותן השירותים הפיננסיים;

“הגנת סייבר” – פעילות הקשורה לכלל היבטי אבטחת המידע והמערכות במרחב הקיברנטי;

“הזדהות חזקה” – הזדהות המבוססת על שימוש בלפחות שני אמצעי זיהוי;

“הערכת סיכונים” – תהליך של הערכת רמת הסיכון של כלל המידע, מערכות המידע והתהליכים העסקיים והטכנולוגיים בנותן השירותים הפיננסיים. התהליך ממפה את הסיכונים השונים הנובעים מהפעילות והתהליכים בנותן השירותים הפיננסיים;

“הצפנה” – המרת מידע גלוי (Clear Text) למידע מוצפן (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים;

“הצפנה מקצה לקצה” – הצפנת תווד התקשורת או הנתונים בין התחנה או השרת היוזמת את השירות, לבין התחנה או השרת המספקת את השירות;

“טוקניזציה” – תהליך המרת נתונים רגישים בערכים חלופיים שאינם רגישים (“טוקנים”) אשר אין סכנה בחשיפתם. לרוב, תהליך זה מבוצע על ידי מערכת המחליפה את הערך המקורי בערך חלופי, ומאפשרת את שחזור הערך המקורי בעת הצורך, ובאופן מוגבל;

"יעד התאוששות" – יעד אותו קבע נותן השירותים הפיננסיים להחזרת פעילות עסקית ספציפית ומערכות התומכות בה לרמת שירות מוגדרת בפרק זמן מוגדר ;

"מידע רגיש" – כל אחד מאלה :

- (א) כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981 ;
- (ב) מידע אשר סווג על ידי נותן השירותים הפיננסיים כמידע רגיש ;
- (ג) מידע פיננסי כהגדרתו בחוק שירות מידע פיננסי, תשפ"ב-2021.

"מיסוך נתונים" – טכנולוגיה המבצעת הסתרה של נתונים או חלק מהם אשר הוגדרו סודיים, כך שבעת הצגת נתון, הוא מוחלף ברצף תווים אחר. שימוש בטכנולוגית מיסוך מאפשר לעבד נתונים כך שהצפייה בהם תהיה מוגבלת לגורמים מועטים בלבד ;

"מערכות ליבה" – כל אחת מאלה :

- (א) המערכות שהוגדרו על ידי נותן השירותים הפיננסיים כמערכות מרכזיות של הארגון ואושרו ככאלה על ידי הדירקטוריון ;
- (ב) מערכות שיש להן השפעה ישירה על הלקוחות, על הנכסים הפיננסיים שלהם או מערכות אשר שומרות מידע או נכסים הקיימים אצל נותן השירותים הפיננסיים ;
- (ג) כל המערכות שהמידע המנוהל או המעובד בהן עשוי להשפיע באופן מהותי על עסקי נותן השירותים הפיננסיים.

"מערכות מידע" – כל המערכות התומכות בפעילות העסקית של נותן השירותים הפיננסיים, לרבות ציוד ממוכן, תשתיות וטכנולוגיות התומכות בתפעולן ;

"מערכות OT (Operation Technology)" – מערכות (לרבות תוכנה וחומרה) המיועדות לשליטה ובקרה של מערכות תעשייתיות או אוטומציה (באמצעות בקרה ושליטה ישירה) של התקנים פיזיים ;

"מנהל כללי" – כל אחד מאלה :

- (א) בבעל רישיון בסיסי – המנכ"ל או מי שמנהל את פעילותו של בעל הרישיון ;
- (ב) בבעל רישיון מורחב – המנכ"ל.

"נותן שירותים פיננסיים" –

- (א) בעל רישיון למתן שירות פיקדון ואשראי ;
- (ב) בעל רישיון להפעלת מערכת לתיווך באשראי ;
- (ג) בעל רישיון למתן שירות בנקס פיננסי אשר נותן שירות שבו נשמר ומנוהל נכס פיננסי בחשבון ייעודי המנוהל עבור לקוח מסוים, ואשר מאפשר העברת נכס פיננסי לחשבון אחר. לעניין זה אין נפקא מינה אם מעביר הנכס ומקבל הנכס הוא אותו אדם.¹

(ד) כל בעל רישיון למתן שירותים פיננסיים שאינו מנוי לעיל, ואשר מתקיים בו אחד מאלה :

- (1) הוא שומר באופן מקוון הן את המידע על לקוחותיו וכן את הנכסים הפיננסיים של לקוחותיו² ;
- (2) הוא משמש מקור מידע או משתמש בנתוני אשראי כהגדרתם בחוק נתוני אשראי, התשע"ו-2016 ;

¹ סעיפים 103-108 בנוהל הרישוי לנותני שירותים פיננסיים.
² לדוגמה שירות בנקס פיננסי מסוג מטבע וירטואלי, ושירות בנקס פיננסי מסוג שמירה של פיקדונות.

(3) הוא פועל או מבקש לקבל אישור לפעול כנותן שירות כהגדרתו בחוק שירות מידע פיננסי, תשפ"ב-2021.

(4) בעל אישור לפעול כיוזם תשלומים כהגדרתו בסימן ב' (שירות ייזום תשלומים) לחוזר המאוחד לעניין שירותים פיננסיים מוסדרים, בחלק 6 ('הוראות נוספות'), בפרק 1 ('בנקאות פתוחה').

"נכסי מידע" – חומרה, תוכנה או עותק קשיח המכילים מידע, לרבות מאגרי נתונים, התקנים ותשתיות התומכים בפעילויות הקשורות במידע;

"נתיב בקרה" – תיעוד פעולות המתבצעות במערכות מידע;

"המרחב הקיברנטי" – המרחב הפיזי והלא פיזי שנוצר או מורכב בין השאר מהגורמים הבאים: מערכות ממוכנות וממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה ולרבות הרובד האנושי;

"סיכון סייבר" – פוטנציאל לנזק הנובע מהתרחשות אירוע סייבר, בהתחשב ברמת סבירות התממשותו וחומרת השלכותיו;

"סיכון סייבר שורשי" – סיכון סייבר הנובע מאופי פעילות נותן השירותים הפיננסיים, ללא תלות באמצעי הגנת סייבר המיושמים אצל נותן השירותים הפיננסיים;

"סיכון סייבר שיווי" – סיכון סייבר שנוצר לאחר יישום בקרות ואמצעי הגנת סייבר אצל נותן השירותים הפיננסיים;

"סקר סיכונים סייבר" – תהליך שמטרתו זיהוי האיומים, הערכת הסיכון הנובע מהם (תוך התחשבות בסבירות התממשותם והנזק הפוטנציאלי כתוצאה מכך) וזיהוי הבקרות הנדרשות לצמצום סיכונים אלה;

"סריקת חשיפות אבטחת מידע" – סריקה לאיתור חולשה במערכות מידע שעלולה להוביל להתממשות איום;

"קוד עוין" – קוד המושתל על ידי משתמש זדוני ועשוי לגרום לביצוע פעולות לא רצויות, פגיעה במערכות נותן השירותים הפיננסיים וזליגת מידע רגיש לגורמים לא מורשים;

"רשת פנימית" – קבוצת מחשבים המקושרים זה לזה בעזרת ציוד תקשורת ונגישים למשאבים בתוך הארגון, ומופרדים מרשתות ציבוריות;

"תווך תקשורת ציבורי" – תשתיות תקשורת המשרתות או משתפות מספר רב של צרכנים ואינן שייכות לאחד מהם;

"תרחיש ייחוס" – איום אזרחי, ביטחוני, או כלכלי על נותן השירותים הפיננסיים שעלול לגרום נזק מלא או חלקי לתפקודו, או להשבתה, חלקית או מלאה, של תהליכים עסקיים.

(א) תפקידי הדירקטוריון

(1) מדיניות ניהול סיכונים סייבר

דירקטוריון של נותן שירותים פיננסיים יקבע מדיניות לניהול סיכונים סייבר ובכלל זה:

א. ידון ויאשר מדיניות כתובה לניהול סיכונים סייבר, כמפורט בסעיף 3(ה1);

ב. ידון בתכנית מעודכנת לניהול סיכונים סייבר כמפורט בסעיף 3, לרבות השינויים שבוצעו בה, ככל שבוצעו, לכל הפחות אחת לשנה;

יאשר את כתב מינוי ועדת ההיגוי בתחום סיכונים סייבר, שבמסגרתו יוגדרו תפקידי הוועדה, חבריה וסמכויותיה.

(2) פיקוח ובקרה

דירקטוריון של נותן שירותים פיננסיים יפקח על אופן ניהול סיכונים סייבר, בין היתר באמצעות כל אלה:

א. יקבע סוגי דיווחים אשר נדרשים לדירקטוריון, בנוסף לדיווחים הנדרשים בהתאם לסימן זה, בקשר

לניהול סיכונים סייבר, לרבות בקרות אירועי סייבר, וכן יקבע את מועדי הדיווחים ומתכונת העברתם;

ב. ידון בדוחות שהוגשו לו על ידי מנהל הגנת הסייבר, לפי סעיף 2(ד)3, סמוך למועד הגשתם, ויוודא

שסיכונים הסייבר אשר הוצגו בדוחות מטופלים באופן ראוי;

ג. יגדיר אירועי סייבר מהותיים, עליהם יש לדווח באופן מידי לדירקטוריון ולמפקח.

(3) בבעל רישיון שהוא יחיד, יחולו הוראות סעיף 2(א) ו-2(ב) על מי שמנהל את פעילות בעל הרישיון, והכל בשינויים המחויבים.

(ב) תפקידי המנהל הכללי

המנהל הכללי של נותן השירותים הפיננסיים יפעל ליישום ובקרה של ניהול סיכונים סייבר בנותן השירותים הפיננסיים ובכלל זה:

(1) יפעל להבטחת ניהול התקין של תחום סיכונים הסייבר בהתאם למדיניות לניהול סיכונים סייבר ולצרכי נותן השירותים הפיננסיים;

(2) יפעל ליישום מדיניות ניהול סיכונים סייבר ובכלל זה יקבע מנגנוני בקרה ופיקוח נאותים בתחום ניהול סיכונים סייבר;

(3) יוודא הקצאת משאבים נאותים לטובת ניהול סיכונים סייבר, ובכלל זה משאבים אשר יוקצו לתחום הגנת הסייבר לצורך הבטחת יכולתו של מנהל הגנת הסייבר למלא את תפקידו;

(4) יקיים מבנה ארגוני הולם לניהול סיכונים סייבר ויגדיר תחומי אחריות ברורים לעוסקים בתחום ואת הממשקים ביניהם, תוך שמירה על עקרונות של הפרדת תפקידים וסמכויות;

(5) יאשר את תכנית העבודה השנתית כאמור בסעיף 2(ה)3, יקצה משאבים נאותים ליישומה ויפקח על ביצועה;

(6) ידון בהמלצות ועדת ההיגוי, בעניין תוצאות הערכת סיכונים ובתכנית להפחתתם;

(7) יקבע סוגי דיווחים אשר נדרשים למנהל הכללי, בנוסף לדיווחים הנדרשים בחוזר זה, לרבות בקרות אירועי סייבר, וכן יקבע את מועדי הדיווחים ומתכונת העברתם;

(8) יבחן אפשרות לאמץ בנותן השירותים הפיננסיים תקן ת"י ISO 27001 של מכון התקנים הישראלי, תוך בחינת התאמתו לאופי הפעילות של נותן השירותים הפיננסיים.

(ג) ועדת היגוי לניהול סיכוני סייבר

(1) מינוי ועדת היגוי לניהול סיכוני סייבר

- א. נותן השירותים הפיננסיים ימנה ועדת היגוי אשר תמנה לפחות שלושה חברים. בראש ועדת ההיגוי יעמוד המנהל הכללי של נותן השירותים הפיננסיים, והיא תכלול את מנהל הגנת הסייבר, את מנהל הסיכונים, וכן את מנהל מערכות המידע ככל שמונה בנותן השירותים הפיננסיים.
- ב. על אף האמור בסעיף א' לעיל, נותן השירותים הפיננסיים יכול למנות חבר הנהלה אחר, בעל כישורים מתאימים, לעמוד בראש ועדת ההיגוי, ובלבד שהתקיים דיון בהנהלת נותן השירותים הפיננסיים בו הוצגו הנימוקים לבחירתו של חבר הנהלה אחר.
- ג. קבוצה של נותני שירותים פיננסיים שנשלטים על ידי אותו בעל שליטה יכולה למנות ועדת היגוי משותפת לקבוצה (להלן – "ועדת היגוי קבוצתית"), ובלבד שהגורמים המוסמכים לכך בהתאם לחוזר זה, בכל אחד מנותני השירותים הפיננסיים בקבוצה, יאשרו את מינוי ועדת ההיגוי הקבוצתית כוועדת ההיגוי של כל אחד מהם.
- ד. דיוני ועדת ההיגוי הקבוצתית יכולים להיות משותפים לכל חברות הקבוצה, ובלבד שכלל שקיים הצורך לדון באופן פרטני בנושאים הנוגעים לאחד הגופים החברים בקבוצה, יתקיימו בוועדת ההיגוי הקבוצתית דיונים כנדרש, בהתאם להוראות חוזר זה, ובהשתתפות כלל הגורמים הנדרשים בהתאם להוראות החוזר.
- ה. הוועדה תתכנס לכל הפחות אחת לרבעון ותערוך פרוטוקולים לכל ישיבותיה.
- ו. בבעל רישיון שהוא יחיד יכול שלא תוקם ועדת היגוי לניהול סיכוני סייבר ובלבד שכל תפקידי הוועדה המפורטים להלן יעברו לאחריות מנהל הפעילות של בעל הרישיון.

(2) תפקידי ועדת ההיגוי לניהול סיכוני סייבר

- א. סיוע למנהל הכללי לקבל החלטות ולבצע את תפקידיו בכל הקשור לניהול התקין של תחום ניהול סיכוני סייבר, מתוך ראיה אינטגרטיבית של התחום ברמה כלל ארגונית.
- ב. בחינת הצורך לעדכן את מדיניות לניהול סיכוני סייבר, לכל הפחות אחת לשנה, וכן בכל שינוי משמעותי המתבצע בתהליכים עסקיים, בסביבה הטכנולוגית או שינוי מהותי במתאר הסיכונים העסקי או הטכנולוגי בפעילות נותן השירותים הפיננסיים.
- ג. ביצוע מעקב אחר יישום תכניות העבודה, לרבות תכנית העבודה השנתית.
- ד. דיון בתוצאות הערכת הסיכונים ואישור התכנית לניהול סיכוני סייבר והתכנית להפחתתם בהתאם לאמור בסעיפים 3(א) ו-3(ב).
- ה. דיון בסיכונים אפשריים בהפעלת שימוש במערכות מבוססות ענן בהתאם לאמור בסעיף 4(ה)3(א).
- ו. תחקור והפקת לקחים לגבי כל אירוע סייבר משמעותי בהתאם לאמור בסעיף 4(א)2(ט).
- ז. ועדת היגוי שבראשה עומד חבר הנהלה שאינו המנהל הכללי, תדווח למנהל הכללי על סטטוס ביצוע תכנית העבודה השנתית אחת לרבעון, ותעביר לו את המלצותיה בעניין תוצאות הערכת הסיכונים והתכנית להפחתתם בהתאם לאמור בסעיף 4(ד) לעיל ולגבי כל אירוע סייבר משמעותי כאמור בסעיף 4(ו) לעיל.
- ח. דיווח לדירקטוריון, לכל הפחות אחת לשנה, על פעילותה, מסקנותיה והמלצותיה בנושאים שהוסמכה לעסוק בהם.

(ד) מנהל הגנת הסייבר

(1) מינוי מנהל הגנת הסייבר

- א. נותן שירותים פיננסיים ימנה מנהל הגנת הסייבר בעל מומחיות וניסיון מוכחים בתחום הגנת הסייבר.
- ב. למנהל הגנת הסייבר תהיה גישה ישירה למנהל הכללי וליושב ראש הדירקטוריון של נותן השירותים הפיננסיים.
- ג. מנהל הגנת הסייבר לא ימלא כל תפקיד אחר אשר עלול לפגוע ביכולתו לבצע כראוי את תפקידו או להגבילה.
- ד. קבוצה של נותני שירותים פיננסיים שנשלטים על ידי אותו בעל שליטה יכולה למנות מנהל הגנת הסייבר לכלל החברות בקבוצה, ובלבד שמנהל הגנת הסייבר ימלא את תפקידו כנדרש בהתאם להוראות חוזר זה ובהתאם להגדרת התפקיד עבור כל אחד מנותני השירותים הפיננסיים החברים בקבוצה.

(2) תפקידי מנהל הגנת הסייבר

- מנהל הגנת הסייבר יפעל ליישום מדיניות ניהול סיכוני סייבר של נותן השירותים הפיננסיים, כאמור בסעיף 2(ה)1, ותפקידיו יהיו, בין היתר:
- א. ייעוץ והנחיית נותן השירותים הפיננסיים בנושא ניהול סיכוני סייבר;
 - ב. קביעת נהלי עבודה ומסגרת דיווחים;
 - ג. גיבוש תכנית העבודה השנתית כמפורט בסעיף 2(ה)3(ה), הבאתה לאישור ועדת ההיגוי ויישומה בפועל;
 - ד. מעקב אחר אירועי סייבר משמעותיים בישראל ובעולם, הפקת לקחים ויישום המסקנות הרלוונטיות לנותן השירותים הפיננסיים;
 - ה. גיבוש תכנית להעלאת מודעות לסיכוני סייבר בקרב עובדי נותן השירותים הפיננסיים, ובהתאם לסעיפים 4(ז)3 ו-5(ד)2.

(3) דיווחים ודוחות

מנהל הגנת הסייבר יגיש דיווחים ודוחות כמפורט להלן:

- א. דיווחים לדירקטוריון ולמנהל הכללי, בהתאם לסעיפים 2(א)2 א ו-2(ב)7;
- ב. דוח מסכם לוועדת ההיגוי, לכל הפחות אחת לרבעון, אודות כלל ניסיונות התקיפה ואירועי סייבר שהתרחשו בנותן השירותים הפיננסיים וכן ההחלטות והפעולות שבוצעו בעקבותיהם.

(ה) מסגרת ניהול סיכוני סייבר (FRAMEWORK)

(1) מדיניות לניהול סיכוני סייבר

נותן שירותים פיננסיים יגדיר מדיניות לניהול סיכוני סייבר, אשר תקבע את העקרונות המנחים ליישום הגנת הסייבר בנותן השירותים הפיננסיים. המדיניות תכלול לכל הפחות התייחסות למסגרת הארגונית לניהול סיכוני סייבר אצל נותן השירותים הפיננסיים, לרבות תחומי אחריות, חובות דיווח, פיקוח ובקרה, וכן תתייחס ליישום ההוראות המפורטות בחוזר זה.

(2) נהלים

- א. נותן שירותים פיננסיים יגדיר נהלים שיתייחסו לאופן יישום הגנת סייבר בנותן השירותים הפיננסיים ואשר יבטיחו את קיום הוראות החוק והוראות חוזר זה, ויפעל להטמעתם.
- ב. הנהלים ייגזרו ממדיניות ניהול סיכונים הסייבר וכן מהוראות הדין והתחייבויות חוזיות החלות על נותן השירותים הפיננסיים.
- ג. נותן שירותים פיננסיים יבחן את הצורך בעדכון הנהלים, בהתאם לעדכון מדיניות ניהול סיכונים הסייבר, וכן בכל שינוי משמעותי המתבצע בתהליכים עסקיים, בסביבה הטכנולוגית או שינוי במתאר הסיכונים, ולכל הפחות אחת ל-24 חודשים, ויעדכן את הנהלים בהתאם.

(3) תכניות עבודה

נותן שירותים פיננסיים יקבע תכניות עבודה בתחום ניהול סיכונים הסייבר, ולכל הפחות יקבע את התוכניות כמפורט להלן. תכניות העבודה ייגזרו ממדיניות ניהול סיכונים הסייבר ומהנהלים של נותן השירותים הפיננסיים. התכניות יתייחסו לאופי המידע, לסוגי התהליכים, התשתיות והמערכות בנותן השירותים הפיננסיים.

- א. תכנית לניהול סיכונים הסייבר כאמור בסעיף 3 ;
- ב. תכנית התאוששות ויעדי התאוששות מאירוע הסייבר כאמור בסעיף 4(א)(3)(ד) ;
- ג. תכנית לביצוע סקרים בהתאם לאמור בסעיף 4(ב)(1)(ה) ;
- ד. תכנית להעלאת רמת מודעות העובדים בהתאם לאמור בסעיף 4(ז)(3) ;
- ה. תכנית עבודה שנתית אשר תתייחס בין היתר למדיניות וליישום יתר תכניות העבודה.

3. ניהול סיכונים סייבר

נותן שירותים פיננסיים יקבע תכנית עבודה לניהול סיכונים הסייבר, שתעסוק, בין היתר, בהערכת הסיכונים לתהליכים, למערכות מידע ולנכסי מידע. התכנית תאשר על ידי ועדת ההיגוי, תוצג לדירקטוריון ותנחה את נותן השירותים הפיננסיים בהקצאת משאבים להטמעת אמצעים לניהול סיכונים הסייבר ובקביעת תכנית העבודה השנתית.

הצגת התוכנית לדירקטוריון תכלול, לכל הפחות, פירוט של סיכונים הסייבר השוריים, תכנית להפחתת סיכונים ופירוט הסיכונים המשמעותיים אותם נותן השירותים הפיננסיים החליט שלא להפחית לרמה מזערית ככל שניתן.

התכנית כאמור תכלול התייחסות, לכל הפחות, לנושאים המפורטים להלן :

(א) הערכת סיכונים

- (1) נותן שירותים פיננסיים יכין הערכת סיכונים הסייבר בפעילותו במטרה לייצר תמונת מצב עדכנית של מכלול סיכונים הסייבר עמם הוא מתמודד.
- (2) נותן שירותים פיננסיים יבחן ויעדכן את הערכת הסיכונים בהתאם לצורך וכן בהתאם לעדכון מדיניות ניהול סיכונים הסייבר או בכל שינוי משמעותי המתבצע בתהליכים עסקיים וטכנולוגיים, בסביבה

הטכנולוגית או במתאר הסיכונים, ולכל הפחות אחת ל-36 חודשים.

(3) הערכת הסיכונים תתייחס לסיכונים הנוגעים לנכסי מידע, לתהליכים ולמערכות מידע (לרבות מערכות OT), ולסביבות פיתוח ובדיקות המכילות מידע רגיש או חשופות למערכות מידע אחרות של נותן השירותים הפיננסיים.

(4) הערכת הסיכונים תתייחס למכלול שרשרת האספקה וכן לסיכונים הנובעים מאופי הפעילות של נותן השירותים הפיננסיים אל מול צדדים שלישיים המעורבים בפעילות, דוגמת ספקי מיקור חוץ ולקוחות.

(5) נותן שירותים פיננסיים ינהל ויתחזק רשימה עדכנית של נכסי המידע, התהליכים ומערכות המידע הקיימים בו אשר בעניינם תתבצע הערכת סיכונים. הרשימה תעודכן לכל הפחות אחת לשנתיים.

(6) הערכת הסיכונים תכלול בין היתר, את השלבים הבאים:

א. זיהוי והגדרת מערכות מידע, נכסי מידע ותהליכים;

ב. מיפוי הסיכונים למערכות מידע, נכסי מידע ותהליכים שזוהו, כאמור בסעיף א';

ג. מיפוי סיכוני סייבר שורשיים;

ד. מיפוי והערכת הבקורות ואמצעי ההגנה למזעור הסיכונים שנמצאו, לרבות בחינה של מידת השפעת הבקורות עליהם;

ה. הערכת סיכון הסייבר השיורי שנותר לאחר יישום הבקורות ואמצעי הגנה כאמור בסעיף (ד) לעיל, והגדרת מערכות מידע ותהליכים כבעלי רמת חשיפה גבוהה לסיכוני סייבר המתבססות על תוצאות הערכת הסיכונים.

(7) בביצוע הערכת הסיכונים נותן שירותים פיננסיים יתבסס, בין היתר, על מידע מממצאי ביקורות וסקרים, על ניתוח אירועי סייבר שהתרחשו בנותן השירותים הפיננסיים או בגופים אחרים וכן על ניתוח תרחישים לזיהוי אירועים פוטנציאליים של התממשות הסיכון בנותן השירותים הפיננסיים.

(8) נותן שירותים פיננסיים יוכל להסתמך על הערכת סיכונים שביצע גוף אחר ובלבד שבחן את הערכת הסיכונים שנעשתה ואת תוצאותיה ואלו אושרו על ידו. הסתמכות על הערכת סיכונים כאמור תתאפשר רק במקרים הבאים:

א. הערכת הסיכונים נעשתה על ידי גוף מוסדי או תאגיד בנקאי;

ב. הערכת הסיכונים נעשתה על ידי נותן שירותים פיננסיים אחר אשר חלות עליו הוראות חוזר זה.

(9) לצורך עמידה בהוראות סעיף (4) לעיל, נותן שירותים פיננסיים יוכל להסתמך על הערכת סיכונים שנערכה לגבי ספק מיקור חוץ, ובלבד שבוצעה על ידי גורם בלתי תלוי בספק מיקור החוץ; נותן השירותים הפיננסיים בחן את הערכת הסיכונים שנעשתה ואת תוצאותיה ואלו אושרו על ידו, וכן בדק את רמת ההגנה שמיישם ספק מיקור החוץ, לרבות בחינת מידע לגבי תהליכי בקרה ותוצאות הבדיקות שנעשו, ומצא כי היא תואמת את הדרישות אשר חלות על נותן השירותים הפיננסיים.

(ב) הפחתת סיכוני סייבר

נותן שירותים פיננסיים יקבע תכנית להפחתת הסיכונים, על בסיס הערכת הסיכונים אשר בוצעה בהתאם לאמור בסעיף 3(א).

(ג) יישום בקורות

בהתאם להערכת הסיכונים כאמור בסעיף 3(א), וכחלק מהתכנית להפחתתם בהתאם לסעיף 3(ב), יגדיר נותן שירותים פיננסיים בקורות מתאימות ואפקטיביות להתמודדות עם סיכוני סייבר. על הבקורות להתייחס למערכות מידע ולתהליכים בנותן השירותים הפיננסיים וכן לצדדים שלישיים, דוגמת ספקי שירותים במיקור חוץ או לקוחות.

4. הגנת סייבר בנותן שירותים פיננסיים

נותן שירותים פיננסיים יקבע אמצעי הגנה מפני סיכוני סייבר, ויתאים אותם למכלול סיכוני הסייבר שלו בהתאם לתוצאות הערכת הסיכונים. נותן שירותים פיננסיים יקבע לכל הפחות את אמצעי ההגנה כמפורט להלן:

(א) איסוף מודיעין, ניטור ובקרה ומוכנות לאירועים

נותן שירותים פיננסיים יבסס תמונת מצב עדכנית אודות מצב הגנת הסייבר שלו תוך זיהוי חולשות ואיומים ויפעל לצמצום חשיפות לסיכונים אלו. תמונת המצב תשמש כבסיס לקבלת החלטות מושכלת, תיעודף דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת.

(1) איסוף מודיעין

- א. נותן שירותים פיננסיים יאסוף וינתח מידע רלוונטי ממקורות פנימיים וחיצוניים לצורך יצירת תפיסה כוללת ועדכנית של סיכוני סייבר וחשיפת נותן השירותים הפיננסיים למול האיום.
- ב. נותן שירותים פיננסיים יבחן אפשרות לעבודה מול המרכז הארצי לניהול אירועי סייבר (CERT-il) ומול מרכז הסייבר הפיננסי במשרד האוצר, ולשיתוף הדדי של מידע קיברנטי אופרטיבי עימם.

(2) ניטור ובקרת מערכות מידע

- א. נותן שירותים פיננסיים יקיים מערך ניטור ובקרה לקבלת דיווחים בזמן אמת ממערכות המידע השונות אודות חשש לאירוע סייבר.
- ב. נותן שירותים פיננסיים יישם נתיב בקרה של פעולות ושאליות המתבצעות במערכות המנהלות מידע רגיש על לקוחות וכן במערכות שרמת החשיפה שלהן לביצוע פעילות בלתי מורשה הינה גבוהה, בהתאם להערכת הסיכונים של נותן השירותים הפיננסיים. וזאת בין השאר במטרה לאפשר התחקות אחר פירוט הרישום לצורך ביקורת, זיהוי של פעילות בלתי מורשה, תחקור לאחר מעשה ומניעת התכחשות.
- ג. נתיב הבקרה כאמור יתייחס לפעולות ושינויים המבוצעים במערכות מידע כאמור וכן לשאליות וגישה לנתונים ולכל הפחות לגישה למידע רגיש. במסגרת נתיב הבקרה יתועדו גם ניסיונות לביצוע פעולות שלא צלחו, לרבות ניסיונות חיבור למערכות המידע, שאליות ועדכונים.
- ד. נתיב בקרה יכלול לכל הפחות מידע על מועד ביצוע הפעולה, מקור הפעולה, הגורם שביצע או ניסה לבצע ועל מי בוצעה הפעולה. במערכות ליבה יכלול נתיב הבקרה התייחסות גם לערך טרום ביצוע הפעולה ולאחריה.
- ה. נתיב הבקרה יהיה מוגן מפני מחיקה או שינוי בלתי מורשה.
- ו. פרק הזמן לשמירת נתיב בקרה יתאים למטרות נתיב הבקרה, ובכל מקרה לא יפחת מ-12 חודשים.
- ז. נותן שירותים פיננסיים ישתמש במערכות ותהליכים שיזוהו ויתריעו על פעולות חריגות או אסורות ואירועים חשודים בהתבסס על הערכת הסיכונים כאמור בסעיף 3 ועל ניתוח מודיעיני כאמור בסעיף 4(א)(1).
- ח. זיהוי והתרעה בגין פעולות חשודות או אסורות ואירועים חריגים יתייחס לפעולות שמקורן בנותן השירותים הפיננסיים או מחוצה לו, תוך שימת דגש על מערכות תשתית, מערכות אפליקטיביות ומערכות המנוהלות או מאוחסנות מחוץ לנותן השירותים הפיננסיים.

- ט. ככל שהזיהוי וההתרעה על פעולות חשודות ואירועים חריגים שמקורם מחוץ לנותן השירותים הפיננסיים מתבצעים על ידי ספק מיקור חוץ, נותן השירותים הפיננסיים יוודא שספק מיקור החוץ עומד בהוראות חוזר זה לעניין ביצוע ניטור כאמור, וכן כי ספק מיקור החוץ יתריע בפני נותן השירותים הפיננסיים בעת התגלותם של פעולות ואירועים כאמור.
- י. מנהל הגנת הסייבר יתחקר פעולות חשודות או אסורות ואירועים חריגים. ועדת ההיגוי תדון בממצאי כל אירוע משמעותי, תפיק ממנו לקחים ותעביר את המלצותיה למנכ"ל תוך פרק זמן סביר שלא יעלה על שלושה חודשים, כאמור בסעיף 2(ג)(2)(ו).
- יא. נותן שירותים פיננסיים יבחן מעת לעת, ולכל הפחות אחת לשנה, את חוקי הניטור והבקרה שהוגדרו, תקינותם ואיכות האירועים שמתקבלים.

(3) מוכנות לאירועים

- א. נותן שירותים פיננסיים יפעל להבטחת יכולת המוכנות, ההתגוננות והשרידות שלו מפני אירועי סייבר, בהתאם להערכת הסיכונים כאמור בסעיף 3 ובפרט בהתאם למיפוי גורמי האיום.
- ב. נותן שירותים פיננסיים יגדיר נוהל היערכות וניהול אירועי סייבר, בהתאם להערכת הסיכונים ולניתוח תרחישי ייחוס. עדכון הנוהל יבוצע לאחר כל עדכון של הערכת הסיכונים, והצורך לעדכן את הנוהל ייבחן לכל הפחות אחת לשנה. הנוהל יכלול התייחסות לכל השלבים הבאים:
1. גילוי – גילוי וזיהוי השלב בו נמצא האירוע תוך פירוט כל שלבי הפעולה לרבות: בידוד, חקירה, איסוף ראיות והסקת מסקנות.
 2. הערכת מצב – בירור וניתוח אירוע סייבר ובחינת דרכי פעולה להתמודדות עם האירוע;
 3. הכלה ובלימה – השגת שליטה על האירוע ועצירת החמרתו;
 4. התאוששות – הכרעת האירוע תוך מזעור הנזק שנגרם;
 5. השבה לשגרה – חזרה לפעילות חלקית או מלאה של נותן השירותים הפיננסיים תתבצע לאחר שנותן השירותים הפיננסיים וידא, בהתבסס על הערכת סיכונים עדכנית, שאין בחזרה לפעילות משום סיכון להישנות אירוע הסייבר או החמרתו, ולאחר אישור הדירקטוריון.
- ג. הנוהל כאמור בסעיף ב' לעיל יתייחס, לכל הפחות, לנושאים הבאים:
1. דרכי הפעולה והתגובה של נותן השירותים הפיננסיים באירוע סייבר, בהתייחס לתרחישים שונים וכן את אופן יישום הפעולות והתגובות ואת הגורמים האחראים על ביצוען.
 2. התקשרות עם גורמים פנימיים וחיצוניים, ובכללם לקוחות, בהתאם לתרחישים שונים.
 3. מועדי דיווח על אירועים ומתכונת הדיווח, לרבות גורם מדווח, נמען הדיווח וזמן התגובה הסביר לדיווח.
- ד. נותן שירותים פיננסיים יגדיר תכנית התאוששות ויעדי התאוששות מאירוע סייבר עד לתפקוד מלא בעת חזרה לשגרה, תוך התייחסות לתרחישי הייחוס, וליעדי השירות בחירום שקבע לעצמו.
- ה. נותן שירותים פיננסיים יבצע, לכל הפחות אחת לשנה, תרגול של כלל המערכים הרלוונטיים במטרה להכין אותם להפעלת התכניות כאמור ולשיפורן בהתאם ללקחים.
- ו. נותן שירותים פיננסיים יקים צוות תגובה להתמודדות עם אירועי סייבר, שיבצע תרגול אירוע אמת אחת לשנה, תוך שימוש במערכות המידע ותשתיות נותן השירותים הפיננסיים.
- ז. נותן שירותים פיננסיים יקבע מנגנון נגיש ופשוט לדיווח של עובדים על אירועי סייבר.
- ח. נותן שירותים פיננסיים ידווח בהקדם האפשרי לדירקטוריון ולמפקח על נותני שירותים פיננסיים על כל אירוע סייבר מהותי. אירוע יוגדר מהותי בהתאם לנהלים הפנימיים של נותן השירותים הפיננסיים, וכן בהתקיים לפחות אחד מהתבחינים הבאים:

1. אירוע סייבר בו נפגעו או הושבתו מערכות ייצור של נותן השירותים הפיננסיים המכילות מידע רגיש למשך של יותר משלוש שעות ;
2. כל אירוע סייבר בעל השפעה מהותית על לקוחות נותן השירותים הפיננסיים, בהתאם להערכת נותן השירותים הפיננסיים ;
3. אירוע סייבר המעיד על מתווה תקיפה חדש או המעיד על רמת מורכבות גבוהה, למיטב ידיעתו והבנתו של נותן השירותים הפיננסיים ;
4. קיימות אינדיקציות לכך שמידע של נותן השירותים הפיננסיים, או מידע רגיש אודות לקוחות או עובדים של נותן השירותים הפיננסיים, נחשף, דלף, שובש או נמחק ;
5. התקבלה דרישת כופר או סחיטה אצל נותן השירותים הפיננסיים מכל גורם שהוא, למעט מקרים בהם נותן השירותים הפיננסיים בדק את הדרישה ויודא כי לא מדובר באירוע סייבר ;
6. קבלת החלטה של נותן השירותים הפיננסיים לנקוט פעולות הגנה או מנע עקב אירוע או חשש לאירוע סייבר אצל ספק מיקור חוץ המחובר למערכות המידע של נותן השירותים הפיננסיים ;
7. קבלת דיווח או פניה לגבי אירוע סייבר מגורם חיצוני לנותן השירותים הפיננסיים, למעט דיווחים המגיעים בעקבות בדיקות או ביקורות שבוצעו ביוזמת נותן השירותים הפיננסיים או המפקח ולמעט דיווחים ופניות שנבדקו על נותן השירותים הפיננסיים, ונותן השירותים הפיננסיים וידא כי לא מדובר באירוע סייבר ;
8. אירוע סייבר החייב בדיווח לגופי ממשלה ואכיפה אחרים.

(ב) ביצוע סקרי סיכונים

(1) סקרים ומבחני חדירה

- א. נותן שירותים פיננסיים יישם סקרים, מבחני חדירה וסריקות חשיפות אבטחת מידע, עבור מערכות המידע והתהליכים הארגוניים בו.
- ב. הסקרים, מבחני החדירה וסריקות חשיפות אבטחת המידע, כפי שיפורטו להלן, יבוצעו על ידי גורם מקצועי, חיצוני ובלתי תלוי, שאינו מעורב בפיתוח ובהטמעת מערכות המידע בנותן השירותים הפיננסיים.
- ג. הסקרים, מבחני החדירה וסריקות חשיפות אבטחת המידע יבחנו לכל הפחות את התאמתם של מערכות המידע והתהליכים בנותן השירותים הפיננסיים למדיניות ניהול סיכונים הסייבר ולנהלי נותן השירותים הפיננסיים, ויבחנו קיום בקורות הגנת סייבר והתאמתן לסוג הפעילות של נותן השירותים הפיננסיים ואת אפקטיביות הבקורות כאמור.
- ד. הסקרים, מבחני החדירה וסריקות חשיפות אבטחת המידע יכללו ממצאים והמלצות, אשר יוצגו בדיון ועדת ההיגוי העוקב למועד השלמתם.
- ה. נותן שירותים פיננסיים יקבע תכנית לביצוע סקרים ומבחני חדירה אשר תכלול את הנושאים הבאים :
 1. בחינה של כל רמות האבטחה של התהליכים ומערכות המידע, ולכל הפחות התייחסות למפורט להלן : הגנות פיסיקות וסביבתיות ; הגנות תשתיות הכוללות אחסון ; מערכות הפעלה ; רשתות ; בסיסי נתונים ; רכיבי Middleware ; הגנות אפליקטיביות ; הגנות ברמת הלוגיקה העסקית המיושמת במערכת, וכן התייחסות לתהליכים הסובבים את המערכת כגון ניהול משתמשים והרשאות, תהליכי גיבוי, ניטור וכדומה.

2. ביצוע מבחני חדירה הכוללים: מבחן המדמה ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים), בדיקות הנדסה חברתית, התחזות ופשינג, באופן תקופתי ולכל הפחות אחת לשנה.

3. ביצוע סריקת חשיפות אבטחת מידע (Vulnerability Scan), לכל הפחות אחת לרבעון, במערכות מידע של נותן השירותים הפיננסיים. הסריקות תתייחסנה, בין היתר, לחשיפות הנובעות מחיבור מערכות נותן השירותים הפיננסיים לרשתות חיצוניות ("סריקה חיצונית") ולחשיפות הנובעות מניסיונות תקיפה מתוך הרשת של נותן השירותים הפיננסיים ("סריקה פנימית").

4. תדירות ביצוע הסקרים תיקבע בהתאם למידת החשיפה של המערכת לאיומים, רגישות המידע המנוהל במערכות המידע ושינויים שבוצעו במערכת או בסביבתה, ותעמוד לכל הפחות על תדירות כמפורט להלן:

א) עבור מערכות מידע אשר יש אליהן גישה מרשת ציבורית, תדירות ביצוע הסקרים לא תפחת מאחת ל-18 חודשים;

ב) עבור מערכות מידע שאין אליהן גישה מרשת ציבורית, תדירות ביצוע הסקרים לא תפחת מאחת ל-36 חודשים;

ג) עבור מערכות מידע שאין אליהן גישה מרשת ציבורית ורמת הסיכון שלהן כפי שנקבעה בהערכת הסיכונים היא נמוכה, תדירות ביצוע הסקרים לא תפחת מאחת ל-48 חודשים.

ו. בנוסף לאמור לעיל, טרם הטמעת שינוי משמעותי במערכת מידע שנקבעה כבעלת סיכון גבוה בהערכת הסיכונים, או שינוי בסביבה הטכנולוגית של מערכת כאמור, יבוצע סקר לבחינת תאימותה למדיניות לניהול סיכונים סייבר ולנהלים של נותן השירותים הפיננסיים.

ז. נותן שירותים פיננסיים אשר משתמש בספקי מיקור חוץ המאחסנים או מעבדים מידע של נותן השירותים הפיננסיים, יגדיר תכנית לביצוע סקרים אצל ספקי מיקור חוץ בהתאם לתכנית כאמור בסעיף (ה) לעיל. רמת הכיסוי של הסקרים תותאם לרגישות המידע ולרמת הסיכון, ותכלול בדיקות שמטרתן לוודא את עמידת הספקים בדרישות הגנת הסייבר כאמור בהוראות סעיף 4(ה)1 לסמך זה. סקרים אלו יבוצעו בתדירות המותאמת לרמת הסיכון ולקצב עדכון התהליכים ומערכות המידע אצל הספק, ולכל הפחות אחת ל-36 חודשים. לעניין זה יתאפשר שימוש גם בסקרים שנעשו ביוזמת הספק ובלבד שהספק עומד בדרישות חוזר זה לעניין ביצוע סקרים.

(2) טיפול בממצאי סקרים ומבחני חדירה

א. נותן שירותים פיננסיים יקבע נוהל לטיפול בחשיפות לסיכונים סייבר וכשלי אבטחת מערכות מידע מתגלות במהלך סקרים ומבחנים, וליישום ההמלצות לטיפול בחשיפות אלו.

ב. מנהל הגנת הסייבר יציג בוועדת ההיגוי את סטטוס הטיפול בחשיפות לסיכונים סייבר וכשלי אבטחת מערכות מידע בסיכון גבוה אשר התגלו בעקבות סקרים ומבחני חדירה אשר בוצעו מאז הדיון הקודם של ועדת ההיגוי. ככל שחשיפות אלו או חשיפות שהתגלו בסקרים קודמים עדיין לא טופלו, יוצגו הסיבות לאי הטיפול ומשמעויותיהן להערכת הסיכונים של נותן השירותים הפיננסיים.

(ג) יישום אמצעי הגנה במערכות מידע, תשתיות תקשורת ותפעול.

נותן שירותים פיננסיים יקבע ויתפעל אמצעי הגנת סייבר בתהליכים ובמערכות מידע, ולכל הפחות יישם אמצעים כמפורט להלן:

(1) אבטחת רשת וגישה מרחוק

- א. נותן שירותים פיננסיים ישתמש באמצעי הגנת סייבר לצורך הפחתת סיכוני גישה מרחוק לרשת של נותן השירותים הפיננסיים. האמצעים כאמור יקבעו בהתאם להערכת הסיכונים ויותאמו לסיכונים ייחודיים של שירותי הרשת השונים כגון דואר אלקטרוני, DNS, שירותי העברת קבצים ושירותי Web.
- ב. נותן שירותים פיננסיים יישם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיסית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרגישות המידע המנוהל במערכות השונות.
- ג. נותן שירותים פיננסיים יגדיר ויישם אמצעי אבטחה מיוחדים כגון שימוש בהזדהות חזקה, הצפנה מקצה לקצה וניטור מוגבר בגישה מרחוק לרשת של נותן השירותים הפיננסיים, על גבי רשת ציבורית או מנקודות קצה שאינן מאובטחות דיין, ובפרט גישה מרחוק המאפשרת קריאה וביצוע פעולות במידע רגיש.
- ד. נותן שירותים פיננסיים יישם מנגנונים שינטרו ויצמצמו את הסיכונים הנובעים מחיבור התקן זר או התקן בלתי-מאובטח לרשת נותן השירותים הפיננסיים.

(2) קישוריות נותן שירותים פיננסיים לרשת האינטרנט

- א. נותן שירותים פיננסיים יצמצם את רמת הגישה של העובדים לרשת האינטרנט למינימום הנדרש לצורך עבודתם.
- ב. קישור מערכות מידע בנותן שירותים פיננסיים לרשת האינטרנט יבוצע תוך יישום אמצעי הפרדה מתאימים, שמטרתם למנוע הפעלה של קוד עוין, הכנסה בלתי מבוקרת של קבצים לרשת נותן השירותים הפיננסיים או יצירה של ערוצים חשאיים אל מחוץ לנותן השירותים הפיננסיים.
- ג. נותן שירותים פיננסיים יבצע הפרדה מוחלטת של רשתות אלחוטיות מרשת הייצור שלו. לחילופין וככל שלא מדובר ברשת אלחוטית לשירות אורחיו, נותן שירותים פיננסיים יישם מנגנונים מספקים לאבטחת רשתות אלחוטיות, לרבות הצפנה, הזדהות חזקה, מניעת התקפות על הרשת ומניעה של התחברות גורמים או ציודים בלתי מורשים לרשת האלחוטית.

(3) הוצאת נתונים אל מחוץ לחצרותיו של נותן שירותים פיננסיים

- א. נותן שירותים פיננסיים יקבע בנוהל את האופן שבו תאושר הוצאת מידע אל מחוץ לחצרותיו, בהתאם לרמת רגישות המידע.
- ב. נותן שירותים פיננסיים יגדיר ויישם את אמצעי הגנת הסייבר הנדרשים בתהליך העברת המידע מחוץ לחצרותיו (כגון הצפנת נתונים ווידוא הגעת נתונים ליעדם), וזאת בהתאם לרמת רגישות המידע.

(4) הצפנה

- א. נותן שירותים פיננסיים יישם הצפנה, תוך שימוש בטכניקות הצפנה מוכרות שהוכחו כיעילות על מידע רגיש, על מנת להגן ולהבטיח את חיסיון המידע בתווך התקשורת מחוץ לחצרותיו. נותן שירותים פיננסיים יבחן את האפקטיביות של מנגנוני וטכניקות ההצפנה באופן תקופתי.
- ב. נותן שירותים פיננסיים יגדיר נהלים מתאימים ליצירה, עדכון, חידוש, התקנה וביטול של מפתחות הצפנה ככל שרלוונטי לפעילותו.

(5) אבטחת תשתיות ומערכות מידע ועדכון

- א. נותן שירותים פיננסיים ישמור רשימה עדכנית של תשתיות ומערכות מידע לצורך הגנת סייבר, ויגדיר תהליכים לשמירת עדכניות רישום זה.
- ב. נותן שירותים פיננסיים יגדיר בנוהל תהליכי עדכון מבוקרים למערכות ולתשתיות, תוך התייחסות למקוריות קבצי העדכון, בדיקת עדכונים בטרם יישומם, ושמירה על יציבות מערכות בתהליך העדכון.
- ג. ככל שנותן השירותים הפיננסיים קבע כי קיימות נסיבות אשר בגינן אין צורך לבצע תהליכי עדכון של מערכת מידע מסוימת בהתאם להוראות הנוהל, על ועדת ההיגוי לדון בסיכונים הנובעים מחוסר עדכניות או היעדר תמיכה של מערכת המידע, וליישם אמצעי הגנה אשר מעניקים מענה נאות לסיכונים אלה.
- ד. נותן שירותים פיננסיים יישם עדכוני אבטחת מידע שוטפים למערכות המידע ולתשתיות באופן תקופתי.
- ה. נותן שירותים פיננסיים יעקוב באופן תדיר אחר פרסום עדכוני אבטחת מידע למערכותיו ולתשתיותיו, ויישם עדכונים קריטיים בהקדם האפשרי, בהתייחס לרמת חשיפת מערכותיו לסיכונים הקשורים לעדכונים אלה.

(6) אבטחת מערכות קצה

- א. נותן שירותים פיננסיים יישם אמצעי הגנה על מערכות קצה, תוך התחשבות בסיכוני הפעלת קוד עויין וסיכוני חדירה למערכות תוך ניצול התקנים המחוברים למערכות קצה.
- ב. נותן שירותים פיננסיים יישם הצפנת מידע רגיש במערכות קצה ניידות, לרבות, מידע הנמצא על מחשבים ניידים, טאבלטים, התקני אחסון ניידים וטלפונים ניידים.
- ג. נותן שירותים פיננסיים ישתמש במערכות בקרה, במטרה לצמצם זליגת מידע רגיש ממערכות קצה ויגביל את היכולת לשמור מידע רגיש על מערכות קצה.

(7) מניעת קוד עויין

- א. נותן שירותים פיננסיים יטמיע אמצעי הגנה, למניעת חדירה והתפשטות קוד עויין במערכותיו. אמצעי ההגנה כאמור יכללו מספר שכבות הגנה, דוגמת סינון תקשורת וקבצים נכנסים, סריקת מערכות קבצים, הגנה בזמן אמת על שרתים ועל תחנות קצה, וכן מערכות ניטור ומניעה ייעודיות.
- ב. נותן שירותים פיננסיים יעדכן בתדירות גבוהה את אמצעי ההגנה כאמור, ויגדיר תהליכים לוודוא אפקטיביות אמצעי האבטחה כאמור (כגון: קבלת התרעות על כשל בעדכון קבצי חתימות).
- ג. בעת חיבור מדיה נתיקה למערכות מידע נותן השירותים הפיננסיים יעשה שימוש במנגנוני הגנה אפקטיביים המונעים חדירת קוד עויין, כגון שימוש במערכות "הלבנת קבצים".

- א. נותן שירותים פיננסיים יגדיר בנוהל דרישות לאמצעי הגנת סייבר בכל תהליך רכש או פיתוח של מערכות מידע חדשות וכן בעת שדרוג מהותי של מערכות מידע קיימות. הגדרת הדרישות כאמור תכלול לכל הפחות, את השלבים הבאים:
1. ייזום ואפיון מערכת – הערכת סיכוני סייבר רלוונטיים והגדרת דרישות הגנה מתאימות בעת ייזום ותכנון מערכת.
 2. פיתוח מערכת – מימוש הדרישות המוגדרות באפיון המערכת.
 3. בדיקת מערכת – בדיקות במהלך פיתוח ומבחני חדירה, תוך יישום היבטי הגנת סייבר ולרבות ביצוע סקר אבטחת מידע כאמור בסעיף 4(ב)(1).
 4. קליטת מערכת – קבלה והתקנה מאובטחת ומאושרת של המערכת על ידי גורמים מוסמכים לכך, תוך וידוא יישום דרישות הגנת סייבר.
 5. שינויים במערכת – מנהל הגנת הסייבר יקבל דיווח טרם ביצוע שינוי במערכות המידע, ויקבע את רמת המעורבות הנדרשת בהתאם לאופי השינוי, לרגישות נתונים ולהשפעה אפשרית של השינוי על סיכונים וחשיפות המערכת.
- ב. אמצעי הגנת סייבר יוטמעו בכל רכיבי המערכת, לרבות, בתשתיות, באפליקציה וברמת הלוגיקה העסקית המיושמת במערכת.
- ג. נותן שירותים פיננסיים יבצע מבחני חדירה בטרם הטמעת מערכות בנותן השירותים הפיננסיים.
- ד. מבחני חדירה יכללו, לכל הפחות, את הנדרש בעת ביצוע סקרים, בהתאם לסעיף 4(1)(ה) לסימן זה.
- ה. כחלק מההתקשרות לרכישת ופיתוח מערכת מידע מגורם חיצוני, נותן שירותים פיננסיים יבטיח כי קוד המקור עבר בדיקה נגד חשיפות אבטחת מידע ואי קיום קוד עוין.

(9) הפרדה בין סביבות ואבטחתן

- א. סביבת יצור תופרד מסביבות אחרות, כגון פיתוח ובדיקות.
- ב. רשת המשתמשים תופרד מסביבות אחרות וכל גישה מרשת המשתמשים לסביבה אחרת תאושר על ידי מערכת להגנה מפני התקשרויות בלתי רצויות.
- ג. הרשאות משתמשים לסביבות ייצור תוגדרנה בנפרד מההרשאות לסביבות האחרות.
- ד. סביבות פיתוח ובדיקות לא יכילו נתוני אמת, אלא אם רמת ההגנה מפני סיכון הסייבר המיושמת בסביבות אלו הינה בהתאם לרמת ההגנה המיושמת בסביבת הייצור.
- ה. מנהל הגנת הסייבר יקבע נהלים להעברת נתונים מסביבת ייצור לסביבה אחרת, ולהעברת נתונים מסביבת פיתוח ובדיקות לסביבת ייצור.
- ו. העברת נתונים מסביבת ייצור לסביבה אחרת ומסביבת פיתוח ובדיקות לסביבת ייצור תיערך בצורה מבוקרת, בהתאם לנהלים כאמור ולהנחיות מנהל הגנת הסייבר.

(ד) ניהול משתמשים והרשאות

(1) ניהול משתמשים

- א. נותן שירותים פיננסיים יישם אמצעי הגנה נאותים בכל הנוגע לניהול משתמשים במערכות מידע ובכלל זה:
1. חשבון משתמש של עובד ישויך לעובד מסוים, ותוגדר אחריותו של העובד על חשבון זה ועל הפעולות המבוצעות במערכות נותן שירותים פיננסיים באמצעות חשבון זה.
 2. חשבון משתמש יהיה חשבון אישי.

3. על אף האמור בסעיף 2 לעיל, במקרים בהם יש צורך בקיום חשבונות שאינם אישיים, כגון כאלה המיועדים לשימוש על ידי תהליך ממוכן, יוגדרו אמצעים מיוחדים לשמירה על סודיות אמצעי ההזדהות של החשבון, להגבלת השימוש בו ככל הניתן ויוגדר גורם האחראי על החשבון. בנוסף, תוגדר מדיניות ניהול סיסמאות סדירה במשתמשים אפליקטיביים.
- ב. נותן שירותים פיננסיים יקבע נהלים המגדירים את תהליכי הגנת הסייבר המתייחסים לניהול המשתמשים בנותן השירותים הפיננסיים. הנהלים יתייחסו לתהליכים שונים במחזור החיים של ניהול חשבונות משתמש במערכות מידע של נותן השירותים הפיננסיים, החל מיצירת חשבון משתמש ואופן אישורו, דרך ניהולו השוטף, ועד לאופן נעילת החשבון בתום ההעסקה או ההתקשרות. הנהלים כאמור יתייחסו לכל הפחות לנושאים הבאים:
 1. חשבונות משתמשים של ספקי מיקור חוץ ועובדיהם וכן של עובדים זמניים, לרבות הגדרת אופן אישור חשבונות אלה, הגבלת השימוש בהם והמעקב אחר ביטולם בתום תקופת ההתקשרות או בתום הפרויקט.
 2. תהליכי סקירה תקופתיים ומתועדים שמטרתם לוודא את הצורך בקיום חשבונות המשתמשים. תהליכי הסקירה לכלל החשבונות, יבוצעו לכל הפחות אחת לשנה.
 3. אופן נעילת חשבון משתמש במקרה של אי שימוש בחשבון במשך תקופה ממושכת, ואת תהליך אישור שחרור נעילה זו.

(2) סיסמאות ואמצעי הזדהות

- א. נותן שירותים פיננסיים יישם אמצעי הגנה נאותים בכל הנוגע להזדהות של משתמש ובכלל זה:
 1. יאמת את זהות המשתמש כאשר נמסרת למשתמש סיסמה ראשונית למערכת. תוקף הסיסמה הראשונית ייקבע למינימום אפשרי, בהתאם לאופי השימוש בחשבון ולא יעלה על 14 ימים. המשתמש יחויב לשנות סיסמא זו בהתחברות הראשונה למערכת.
 2. סיסמאות או אמצעי זיהוי אחרים לא יישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע של נותן השירותים הפיננסיים.
- ב. נותן שירותים פיננסיים יגדיר נהלים המתייחסים לאמצעי הזדהות. הנהלים כאמור יתייחסו לכל הפחות לנושאים הבאים:
 1. אופן הזדהות למערכות מידע, באופן המתאים לרמת רגישות המידע המנוהל במערכת ולסיכונים השונים בתהליך ההזדהות.
 2. מסירת אמצעי זיהוי, כגון מסירת אמצעי זיהוי באופן מאובטח למשתמש לאחר זיהוי, שמירה על סודיות הסיסמה והחלפת סיסמה ראשונית על ידי המשתמש.
 3. חוזק אמצעי הזיהוי, כגון הצורך בסיסמה חד-פעמית או מורכבות הסיסמה בהתאם להערכת הסיכונים.
 4. אמצעי בקרה על מערך ההזדהות, לדוגמת נעילת חשבון משתמש לאחר ניסיונות גישה כושלים או אי שימוש ממושך בחשבון, החלפה תקופתית של סיסמה ובקרה על מורכבותה.

(3) ניהול הרשאות ובקרת גישה

- א. מתן הרשאות גישה למערכות המידע של נותן השירותים הפיננסיים יתבצע על בסיס מינימום הרשאות נדרשות בהתאם ל"צורך לדעת" ו"לצורך לבצע".
- ב. נותן שירותים פיננסיים יגדיר בנוהל תהליכים מתועדים לאישור מתן הרשאות גישה למערכות מידע ושירותים, לרבות: אחריות גורמים עסקיים על אישור הרשאות למערכות עסקיות, התאמת

הרשאות לצרכי תפקיד, רמת הסיכון מהרשאות, שינוי הרשאות בעת שינוי תפקיד וביטול הרשאות בעת סיום העסקה.

ג. נותן שירותים פיננסיים יגדיר תהליכי סקירה תקופתיים, שמטרתם לוודא את הצורך בקיום הרשאות משתמשים.

ד. תהליכי הסקירה לכלל ההרשאות יבוצעו לכל הפחות אחת לשנה, ולחשבונות ספקי מיקור חוץ ועובדיהם וכן עובדים זמניים יבוצעו בתדירות גבוהה יותר.

(ה) מיקור חוץ (OUTSOURCING)

נותן שירותים פיננסיים יישם את ההוראות הבאות הנוגעות להגנת סייבר בעת התקשרות עם גוף אחר לביצוע פעולות בשמו או עבורו (לעיל ולהלן: "ספק מיקור חוץ"):

(1) דרישות הגנת סייבר בהסכמי מיקור חוץ

א. נותן שירותים פיננסיים יגדיר נוהל לדרישות הגנת סייבר בהסכמים עם ספקי מיקור חוץ, ביחס לסיכוני מיקור חוץ וביחס לאבטחת שרשרת האספקה. נוהל זה ייושם בעת התקשרות לראשונה עם נותן שירות במיקור חוץ.

ב. במסגרת הסכם התקשרות עם ספק מיקור חוץ, נותן שירותים פיננסיים יפעל כמפורט להלן:

1. ספק מיקור חוץ לא יעביר לאחר מידע שקיבל מנותן השירותים הפיננסיים במסגרת ההתקשרות ולא ישתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.

2. בעת הצורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים לצורך מתן השירות, ולא ישוכפל כלל בסיס הנתונים.

3. תיבחן דרישה מספק מיקור החוץ לעמידה בתקן ת"י ISO 27001, של מכון התקנים הישראלי.

(2) שירות למערכות נותן שירותים פיננסיים על ידי ספק מיקור חוץ

אספקה של שירותי תחזוקה למערכות נותן השירותים הפיננסיים מרחוק (מידע, תוכנה או ציוד תקשורת) על ידי ספק מיקור חוץ, תתבצע בתנאים הבאים:

א. ספק מיקור חוץ יקבל אישור פוזיטיבי להתחברות, בכל התחברות למערכות נותן השירותים הפיננסיים. מנהל הגנת הסייבר יקבע מי בעל הסמכות לאשר התחברות מסוג זה.

ב. גישה מרחוק תתאפשר באמצעות משתמש ייעודי לכל ספק במיקור חוץ ובתיאום מראש עם נותן השירותים הפיננסיים לאופן ההתקשרות ותדירותה.

ג. גישה מרחוק תתאפשר לזמן מוגבל בהתאם לסוג הפעילות אותה יבצע נותן שירות במיקור החוץ.

ד. נותן שירותים פיננסיים יישם הזדהות חזקה בכל גישה מרחוק של נותן שירות במיקור חוץ.

ה. נותן שירותים פיננסיים יישם הצפנה מקצה לקצה לכל אורך נתיב ההתקשרות מרחוק.

ו. נותן שירותים פיננסיים ינטר כל פעילות שבוצעה בגישה מרחוק;

ז. חשיפת ספק מיקור חוץ למידע אודות לקוחות נותן השירותים הפיננסיים תצומצם עד למינימום הכרחי, ובמידת האפשר תחסם במלואה.

שימוש בשירותי מחשוב ענן על ידי נותן שירותים פיננסיים יתבצע בהתאם להוראות סעיפים (1) ו-(2) לעיל, ובנוסף בהתאם להוראות הבאות:

- א. בטרם הפעלת שימוש במערכות מבוססות ענן, על נותן שירותים פיננסיים לבצע הערכת סיכונים ייעודית, בהתאם לקבוע בסעיף 3, ולקיים דיון בנושא בוועדת ההיגוי.
- ב. נותן שירותים פיננסיים לא יאחסן מידע רגיש או מידע של לקוחות בענן מחוץ לגבולות מדינת ישראל, אלא אם רמת ההגנה של ספק שירותי מחשוב הענן הממוקם מחוץ לישראל עומדת בהוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001, ובהוראות הדירקטיבה על הגנת המידע במדינות האיחוד האירופי (EU, GDPR, EUR-Lex).
- ג. בכל שימוש בשירותי מחשוב ענן מחוץ לגבולות מדינת ישראל מידע רגיש יוצפן, גם אם התשתית הינה ייעודית.
- ד. גישה לנתונים בענן תבוצע דרך כתובות מורשות בלבד.
- ה. במקרים בהם נתונים של נותן השירותים הפיננסיים מאוחסנים במערכת שאינה לשימוש הבלעדי של נותן השירותים הפיננסיים (Multi-tenant), ייעשה שימוש בטכנולוגיות כגון הצפנה, מיסוך נתונים או טוקניזציה.
- ו. הסכם ההתקשרות בין נותן שירותים פיננסיים לספק מחשוב הענן יכלול, בין היתר, את כל אלה:
 1. יכולת שליטה ובקרה של נותן השירותים הפיננסיים על כל המידע בענן;
 2. אפשרות חד צדדית של נותן השירותים הפיננסיים להפסקת השימוש בשירותי ספק מחשוב הענן תוך מחיקת המידע ממערכותיו;
 3. התחייבות של ספק מחשוב הענן לכך שלא יהיה ניתן לאחזר מידע השייך לנותן השירותים הפיננסיים במערכותיו של ספק מחשוב הענן לאחר שמידע זה נמחק ממנו על ידי נותן השירותים הפיננסיים.

(ו) אבטחה פיסית וסביבתית

(1) אזורים מאובטחים

- א. בקרות אבטחה פיסיות יתייחסו למכלול הסיכונים הפיסיים והסביבתיים.
- ב. נותן שירותים פיננסיים יחלק את סביבת העבודה לאזורים מאובטחים לפי רמת רגישות המידע אליו ניתן לגשת מאזורים אלו.
- ג. נותן שירותים פיננסיים יישם אמצעי הגנה לגישה פיסית. אמצעים אלו יכללו אמצעים למניעת גישה, כגון דלתות נעולות ושערים אלקטרוניים וכן אמצעים להתרעה וגילוי, כגון מצלמות ומערכות אזעקה. רמת הבקרה הנדרשת תותאם לרמת רגישות המידע אליו ניתן לגשת מאזורים אלה בהתאם להערכת הסיכונים.
- ד. נותן שירותים פיננסיים יאפשר גישה לאזורי העבודה בהתאם לצורך, וימנע בהקדם האפשרי את הגישה לאזורים אלה כאשר אין עוד צורך בגישה זו, לרבות בעת שינוי תפקיד או סיום ההעסקה.
- ה. על בקרת הגישה באזורים המוגדרים ברגישות גבוהה לכלול לפחות שער כניסה אחד הנפתח על ידי אמצעי זיהוי חזק, כגון אמצעי ביומטרי או כרטיס חכם.
- ו. נותן שירותים פיננסיים המעניק שירותי קבלת קהל במשרדיו, יפריד בין האזור בו ניתנים שירותים אלו, לבין אזורי העבודה השוטפים בנותן השירותים הפיננסיים. לא יתאפשר לגורם שאינו מורשה להסתובב במשרדי נותן שירותים פיננסיים ללא פיקוח.
- ז. אזורי ציבוריים המכילים מידע רגיש ימודרו בפני גישה של אנשים שאינם בעלי הרשאה למידע.

(2) אבטחת ציוד וניירת

- א. הוצאת ציוד המכיל מידע רגיש מאחד מהאזורים המאובטחים תיעשה בהתאם לרמת הסיכון כפי שנקבעה בהערכת הסיכונים.
- ב. ציוד המיועד להשמדה או תחזוקה או ציוד הנמסר לגורם מחוץ לנותן השירותים הפיננסיים, לא יכיל מידע רגיש הניתן לשחזור שאינו מוצפן. בטרם הוצאה של מערכות מידע מחוץ לנותן השירותים הפיננסיים לצורך תחזוקה, תבוצע מחיקת נתונים באופן המונע אפשרות שחזור מידע.
- ג. נותן שירותים פיננסיים יבצע השמדה של ציוד רגיש (פיסי או דיגיטלי) שאין בו שימוש ויגדיר בנוהל את אופן הטיפול והשמירה עד להשמדתו של ציוד כאמור.

(ז) הגנת סייבר במשאבי אנוש וגיוס עובדים

(1) הגנת סייבר בתהליך גיוס עובדים

- א. עבור תפקידים שיוגדרו כרגישים על ידי מנהל הגנת הסייבר (כגון כאלה המאפשרים גישה למידע רגיש או שיש להם הרשאות העלולות לסכן את נותן השירותים הפיננסיים), יבוצעו בדיקות לבחינת אמינות המועמדים.
- ב. חוזה העסקה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי סיכוני סייבר, וילווה בהצהרת סודיות.
- ג. חוזה של נותן שירותים פיננסיים עם חברות כוח אדם או השמה או עם ספקי מיקור חוץ יכלול התייחסות לסעיפים לעיל.

(2) הגנת סייבר בעת מעבר תפקיד או סיום העסקת עובדים

- א. בעת מעבר עובדים (לרבות עובדים של ספקי מיקור חוץ ועובדי קבלן) מתפקיד אחד לאחר, ייחסמו הרשאות הגישה שלהם למידע שכבר איננו נחוץ לביצוע תפקידם הנוכחי. עם סיום העסקתו של עובד, לא יישארו בידיו נכסי מידע של נותן השירותים הפיננסיים.
- ב. נותן שירותים פיננסיים יגדיר בקורות הגנת סייבר נוספות המתייחסות לתקופת הזמן שבין ההחלטה על מעבר תפקיד או סיום העסקה של עובד לבין ביטול הרשאות הגישה שלו, כגון מעקב מוגבר של מנהל הגנת הסייבר אחר בקשות של העובד להרשאות או פעולות חריגות שמבוצעות על ידו.

(3) מודעות והדרכה

- א. מנהל הגנת הסייבר יגדיר תכנית להעלאת רמת המודעות של עובדים לסיכוני סייבר.
- ב. התכנית תשולב במערך ההדרכה של נותן השירותים הפיננסיים ותכלול התייחסות לאוכלוסיות העובדים השונות, לרבות ספקי מיקור חוץ.
- ג. התכנית תגדיר הדרכות תקופתיות לעובדים לפי סוג התפקיד, וכן תגדיר הדרכות נדרשות בעת קליטת עובדים או בעת מעבר לתפקיד חדש.
- ד. התכנית תפעל להשגת המטרות הבאות:
 1. העלאת רמת הידע והניסיון לגבי סיכוני סייבר שנותן השירותים הפיננסיים חשוף אליהם והנגזרים מאופי התפקיד.
 2. העלאת המודעות הארגונית הנדרשת כדי לזהות ולהגיב לסיכונים הנובעים מאופי תפקיד העובדים, כגון סיכוני "הנדסה חברתית".

3. הטמעת נהלי הגנת סייבר של נותן שירותים פיננסיים תוך הדרכת עובדים באשר לנהלים הרלוונטיים להגנת סייבר במסגרת תפקידם.

5. אבטחת ערוצי קשר עם לקוחות

(א) אבטחת ערוצי תקשורת מבוססי אינטרנט

(1) נותן שירותים פיננסיים ימפה את ערוצי התקשורת מבוססי אינטרנט שלו עם לקוחותיו, ויישם מערך בקורות הגנת סייבר אשר יכלול, לכל הפחות:

א. הצפנת ערוצי התקשורת למניעת האזנה או התערבות.

ב. אמצעי הגנה למזעור סיכונים הנובעים מרמת אבטחה לקויה של ציוד הקצה של לקוחות.

ג. ניטור ייעודי לזיהוי התקפות על ערוצי תקשורת עם לקוחות, כגון: ניסיונות התחזות, התקפות שונות על מנגנוני אימות זהות לקוח (אותנטיקציה), התקפות "הנדסה חברתית", התקפות על מנגנוני שחזור סיסמה וכדומה.

ד. אמצעים למניעת התקפות על ערוצי התקשורת כאמור כגון, ניחוש שמות משתמשים (user harvesting), ניחוש סיסמאות (Brute force), מניעת שירות באמצעות נעילת חשבונות וכדומה.

(2) נותן שירותים פיננסיים יוודא כי סיכונים שעלולים להיווצר בעת שינויים במערכות מקוונות בתהליכי הזדהות של לקוחות לשירותים מקוונים, יטופלו באופן מספק, טרם ביצוע השינוי.

(ב) רישום לקוחות לשירות

(1) נותן שירותים פיננסיים יוודא זהות לקוח בטרם השלמת רישום לשירותים מקוונים.

א. וידוא זהות לקוח ייעשה באמצעות שימוש בערוץ תקשורת המבוסס על מידע מוקדם שיש לנותן השירותים הפיננסיים על הלקוח.

ב. במקרים בהם לא קיים ערוץ תקשורת המבוסס על מידע מוקדם, ניתן לוודא זהות לקוח באמצעות אוסף פרטי מידע שיש לנותן השירותים הפיננסיים על הלקוח, ושאינם ידועים לגורם אחר מלבד הלקוח, ובלבד שייבחנו הסיכונים רלוונטיים ויישמו מנגנוני אבטחה לצמצום.

(2) על אף האמור בסעיף (1) לעיל, נותן שירותים פיננסיים אשר מזהה את לקוחותיו בהתאם להוראות חוזר נותני שירותים פיננסיים 2020-10-5 "התקשרות מרחוק עם מקבל שירות באופן מקוון" (8.12.2020), יראו אותו כמיישם את הוראות סעיף (1) לעיל.

(3) רישום לקוח לשירותים בערוצים מקוונים יחייב קבלת הסכמה מתועדת של הלקוח באמצעות טופס ידני, טופס מקוון, הקלטה, או באמצעות חשבונו המקוון של הלקוח.

(4) ללקוח תינתן הזכות לבטל את הסכמתו כאמור בסעיף (3) לעיל.

(ג) הזדהות לקוחות בערוצי שירות

(1) נותן שירותים פיננסיים יגדיר את אופן הזדהות הלקוחות לערוצי שירות שונים. אופן ההזדהות יתאים לאופי ערוץ השירות, לרמת הרגישות של המידע, לסוג הפעולות המבוצעות באמצעות הערוץ, ולסיכונים השונים לתהליך ההזדהות, כגון התחזות, הכחשה, האזנה לתווד התקשורת וכדומה.

(2) נותן שירותים פיננסיים יגדיר נהלים המתייחסים לאופן ההזדהות כאמור, ולכל הפחות לנושאים המפורטים להלן:

א. אופן מסירת אמצעי זיהוי ללקוח, כגון משלוח סיסמה ראשונית באמצעות דואר לכתובת לקוח, מסרון לנייד הלקוח או באמצעות ערוץ אחר המאפשר מסירת אמצעי הזיהוי ללקוח, וצמצום הסיכון לגניבת או העתקת אמצעי זה בדרך אל הלקוח.

ב. בעת שימוש באמצעי זיהוי קבועים, יתייחס נותן השירותים גם לאופן מסירת אמצעי זיהוי כאמור לעיל בעת איפוס סיסמה.

ג. אבטחת אמצעי ההזדהות באמצעות דרישות שונות כגון חוזק סיסמה, שמירה על סודיותה, החלפת סיסמה ראשונית על ידי המשתמש ותוקף הסיסמה הראשונית.

(3) נותן שירותים פיננסיים יוודא כי לעובדיו אין גישה לאמצעי זיהוי של לקוחות, העלולה לאפשר ניצול לרעה של חשבון לקוח, למעט עובדים מורשים.

(ד) שליחת מידע באמצעים דיגיטליים

(1) נותן שירותים פיננסיים ישלח מידע רגיש ללקוחות באמצעים דיגיטליים, בכפוף לתנאים הבאים:

א. נותן שירותים פיננסיים יצפין את המידע, על מנת למנוע את חשיפתו לגורם זר או את שיבושו.
ב. נותן שירותים פיננסיים יוודא כי המידע נשלח באופן תקין וכי לא התקבלה אינדיקציה לכך שהמידע לא הגיע ליעדו.

(2) נותן שירותים פיננסיים יעדכן את לקוחותיו על קיומם של סיכוני סייבר ומשמעותם, ויספק ללקוחותיו מידע אודות אמצעי הזהירות הנדרשים לשמירה על פרטיות המידע, וכן הנחיות כיצד לנהוג במקרה של חשד לאירוע סייבר.

(ה) שיווק מוצרים באמצעים דיגיטליים (ומסחר דיגיטלי)

שיווק מוצרים באמצעים דיגיטליים יתבצע בכפוף לתנאים הבאים:

1. ערוץ התקשורת המשמש את תהליך הרכישה יוצפן באמצעות הצפנה חזקה בהתאם לתקנים המקובלים בשוק, שתבטיח את שלמות המידע וסודיותו, תוך שימוש בתעודת הצפנה (SSL Certificate).
2. פרטי אמצעי התשלום של הלקוחות הנשמרים בשרתי נותן השירותים הפיננסיים יישמרו בהתאם לתקנים המקובלים בשוק.
3. נותן שירותים פיננסיים יישם אמצעים למניעת הכחשה, כגון תיעוד בלתי ניתן לעדכון של פרטי ההסכם עם הלקוח, וכן יבקר וינטר את אמצעי המסחר הדיגיטלי במטרה למנוע התחזות ללקוח, הונאה או ניצול לרעה של תהליכי המכירה.

6. אבטחת ערוצי העברת מידע בין נותן שירותים פיננסיים לאחר

בערוצי העברת מידע בין נותני שירותים פיננסיים ובין נותן שירותים פיננסיים לאחר, בהתאם להוראות הדין, לרבות העברת מידע בין נותן שירותים פיננסיים למקור מידע ולנותן שירותי מידע כהגדרתם בחוק שירותי מידע פיננסי, התשפ"ב-2021 או לאחר, כמשמעות בסעיף 29 לחוק האמור, תיושמנה בקרות הגנת סייבר הכוללות הצפנת תווך התקשורת והנתונים מקצה לקצה, אפשרות מעקב אחר הגעת הנתונים ליעדם והגבלת הגישה לנתונים על בסיס "הצורך לדעת".

ד"ר משה ברקת

המפקח על שירותים פיננסיים מוסדרים

חוזר ניהול סיכוני סייבר שפורסם ב- 29 למאי 2022 קובע עקרונות לניהול סיכוני הסייבר של נותן שירותים פיננסיים ודרישות שונות בהם נדרש בעל הרישיון לעמוד בין היתר, בהיבטי ממשל תאגידי, ניהול הסיכון, אמצעי הגנת סייבר, ניטור ובקרה, וכן דרישות הגנת סייבר הנוגעות לממשקים עם גורמים חיצוניים ופנימיים, לרבות ספקי מיקור חוץ, גופים פיננסיים אחרים, עובדיו של נותן השירותים הפיננסיים ולקוחותיו. במסגרת התיקון לחוזר זה מוצע להרחיב את תחולת הוראות החוזר כך שיחול גם על יוזם תשלומים על פי הגדרתו בחוזר בנקאות פתוחה לאור סיכוני סייבר שיוזם התשלומים חשוף אליהם בפעילותו.

לסעיף התחולה

הוראות סימן זה חלות על נותני שירותים פיננסיים אשר חשופים בפעילותם לסיכוני סייבר ולפיכך מוצע להחיל אותן גם על פעילות יוזם תשלומים אשר כחלק מפעילותו מחזיק במידע רגיש על לקוחותיו או על הנכסים הפיננסיים שלהם.

לסעיף התחילה

מוצע לקבוע כי לגבי בעל אישור לפעול כיוזם תשלומים, ייכנסו הוראות החוזר לתוקף ביום 29 בנובמבר 2023, מועד תחילת חוזר נותני שירותים פיננסיים מספר 7-10-2022 שעניינו ניהול סיכונים אצל נותן שירותים פיננסיים מוסדרים (להלן – **חוזר ניהול סיכונים**), משום שעמידה בהוראות החוזר והוראות חוזר ניהול סיכונים היא תנאי לקבלת אישור לפעול כיוזם תשלומים.