ט' באייר תשע"ח
24 באפריל 2018
חוזר מס' ח- 06 -2560

לכבוד
התאגידים הבנקאיים וחברות כרטיסי אשראי

הנדון: ניהול סיכוני סייבר בשרשרת אספקה
(ניהול בנקאי תקין הוראה מס' 363)

כללי

1. בשנים האחרונות גדל מספר אירועי הסייבר המתרחשים בארגונים פיננסיים בעולם ובישראל. אירועים אלו מתאפיינים ברובם, בין היתר, בגרימה של נזק רב ובשיטות תקיפה מתוחכמות וחדשניות, שמקורן לעתים בגורמים חיצוניים המספקים שירותים שונים לתאגידים הבנקאיים. גורמים אלו נכללים בשרשרת האספקה (Supply Chain) של התאגידים הבנקאיים. לפיכך, נדרש התאגיד הבנקאי לקבוע את הפעולות הנחוצות לוודא שהספקים החיצוניים המהותיים נוקטים באמצעים הנדרשים להפחתת חשיפת התאגיד הבנקאי לסיכוני סייבר.
2. מטרת הוראת "ניהול סיכוני סייבר בשרשרת אספקה" הינה להבהיר את האחריות של התאגיד הבנקאי בנוגע לקיום תצורת עבודה מאובטחת מול הספקים החיצוניים המהותיים, ואת חובותיו לניהול סיכוני סייבר הולמים בפעילות ספקים אלו בחצרותיהם, בחצרי התאגיד הבנקאי ובממשקים שלהם עם התאגיד.
3. במקרה שהספק המהותי הינו תאגיד בקבוצה הבנקאית (לדוגמא: בנק, חברת כרטיס אשראי, וכד'), ההוראה מאפשרת ליישם דרישות המפורטות בה בהתאם להערכת הסיכונים של התאגיד הבנקאי.
4. הפיקוח על הבנקים מכין הוראה רחבה בנושא "מיקור חוץ". הוראה זו תשולב בהוראה החדשה.
5. לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגידה, קבעתי את הוראת הניהול התקין הבאה, כמפורט להלן.

מבנה ההוראה

6. ההוראה כוללת ארבעה פרקים:
   (א) **פרק א': רקע** – כולל מבוא להוראה ותחולה.
   (ב) **פרק ב': כללי** – מפרט הנחיות כלליות.
   (ג) **פרק ג': הסכם התקשרות** – עוסק במסגרת הסכם ההתקשרות של התאגיד הבנקאי עם הספק המהותי.
   (ד) **פרק ד': תמיכה ותחזוקה** – מתייחס לפעילויות שדורשות אמצעי זיהוי חזקים ולמנגנוני אבטחה ובקרה בגישה מרחוק של הספק המהותי.

מבוא, תחולה (סעיפים 1 – 7 להוראה)

7. ההוראה מתייחסת ל"ספקים מהותיים": גורמי חוץ הנכללים בשרשרת האספקה של התאגיד הבנקאי (כדוגמת חברות התומכות במתן שירותי מסחר בשוק ההון), שמהותיים לפעילותו ו/או חושפים אותו לסיכוני סייבר ואבטחת מידע פוטנציאליים גבוהים אשר בהתממשותם ניתן לתקוף את התאגיד הבנקאי או לפגוע בפעילותו. הכוונה לגורמי חוץ הנותנים שירותים לתאגיד בתחומים הקשורים לטכנולוגיית המידע, כגון: תמיכה ו/או תחזוקת מערכת מידע, אחסון נתונים רגישים מחוץ לחצרי התאגיד, שירותי מיקור חוץ טכנולוגיים, וכד'. אין הכוונה לספקים כגון: בתחום ההסעדה, שירותי ניקיון, אספקת אנרגיה, וכד'.

8. ההוראה נועדה להציג בפני התאגיד הבנקאי את הפעולות הנחוצות כדי לנהל את סיכוני הסייבר ואבטחת המידע הנגזרים מהשירותים הניתנים לו ע"י ספקים מהותיים.

כללי (סעיפים 8 – 11 להוראה)

9. תאגיד בנקאי נדרש, על פי ההוראה, לקבוע עקרונות להתחייבויותיהם של ספקים מהותיים בנושא ניהול סיכוני סייבר ולוודא עמידה בעקרונות אלו. בנוסף, בהסכם התקשרות עם הספק המהותי יש לכלול התייחסות פרטנית לנושא זה.

10. תאגיד בנקאי נדרש לערוך אחת לתקופה מיפוי של הספקים המהותיים של התאגיד הבנקאי, בחינת הסכם ההתקשרות, עמידתו של הספק המהותי בהתחייבויותיו והצורך לעדכן את ההסכם כתוצאה משינויים בשירותים הניתנים ע"י הספק ושינויים טכנולוגיים המשפיעים על הערכת הסיכונים. הבחינה נועדה לאפשר לתאגיד הבנקאי להעריך את הסיכונים הנגזרים מהשירותים הניתנים ע"י הספקים המהותיים. במקרה שגורמים רלוונטיים בתאגיד הבנקאי יגיעו למסקנה כי הספק המהותי חושף את התאגיד הבנקאי לסיכוני סייבר משמעותיים (לדוגמה, כאשר הספק אינו עומד בהתחייבויות מסוימות או מקיים אותן אך במידה לא מספקת), עליהם לדווח להנהלת התאגיד. ראוי כי בהערכת הסיכונים תשולב גם פונקציית ניהול הסיכונים של הבנק כדי שתיתן את חוות דעתה באשר לחומרת סיכונים אלו והשלכותיהם. על בסיס דיווח זה והערכת הסיכון, על ההנהלה יהיה לשקול ולהחליט בדבר המשך ההתקשרות עם הספק המהותי (לדוגמא, צמצום הפעילות, הטמעת בקרות מפצות בתאגיד הבנקאי, הפסקת ההתקשרות, וכד').

11. נציין כי סעיפים 10-11 חלים גם על ספקים מהותיים שהסכם ההתקשרות עימם נחתם קודם למועד תחילת ההוראה ובכל מקרה על התאגיד הבנקאי לבחון ולנהל את הסיכונים הגלומים בהתקשרויות הקיימות עם ספקים מהותיים ולבחון את אופן המשך ההתקשרות עימם בהתאם.

הסכם התקשרות (סעיף 12 להוראה)

12. במסגרת הסכם ההתקשרות של התאגיד הבנקאי עם הספק המהותי, התאגיד הבנקאי יקח בחשבון את הצורך בשילוב בהסכם של היבטים המפורטים בסעיף 12 להוראה, וזאת בהתאם להערכת הסיכונים הנגזרים מהשירות ו/או מהפעילות, ובדגשים הבאים:

(א) סעיף 12(א) בהוראה – נדגיש כי כוונת ההנחיה להקשחת מערכות הספק המהותי המותקנות בחצרי התאגיד הבנקאי (ולא בחצרי הספק).

(ב) סעיף 12(ה) בהוראה – ביצוע בדיקות מהימנות לעובדי הספק המהותי אשר מעורבים בפעילות ו/או השירות הניתנים לתאגיד הבנקאי על ידי הספק ובהתאם להערכת הסיכונים הנגזרים מהפעילות ו/או מהשירות.

(ג) סעיף 12(ו) בהוראה – מינוי נאמן אבטחת מידע וסייבר אצל הספק, יכול שיהיה גם מקרב עובדי הספק.

(ד) סעיף 12(ז) בהוראה – נדגיש כי אין כוונה להצגת רשימה של כל ספקי צד ג' (ספק משנה) של הספק המהותי, כי אם ספקי צד ג' אשר תומכים בשירותים הניתנים לתאגיד הבנקאי ע"י הספק המהותי. כמו כן, מצופה כי התאגיד הבנקאי יעדכן לפי הצורך את הערכת הסיכונים הגלומים בשירות הניתן על ידי הספק המהותי לאחר קבלת רשימת ספקי צד ג' של ספק זה. לדוגמא: כאשר ספק צד ג' מאחסן נתונים רגישים של התאגיד הבנקאי בענן ציבורי.

(ה) סעיף 12(ח) בהוראה – נוגע לקביעת הסדרים למחיקת נתונים של התאגיד הבנקאי המאוחסנים בחצרי הספק המהותי בתום ההתקשרות בין הצדדים או בהתאם לבקשת התאגיד הבנקאי בכל מועד הקודם לסיום ההתקשרות; לדוגמה, בעת חשש לדליפת מידע ו/או אירוע סייבר אחר.

הכוונה בסעיף 12 בהוראה שהתאגיד יפעיל שיקול דעת על בסיס הערכת הסיכונים אם ראוי לעגן הנחיות אלו בהסכם עם הספק. מצב בו אין באפשרות התאגיד לשלב הנחיה מסוימת בהסכם למרות הסיכון הכרוך בכך, יילקח בחשבון לענין הערכת הסיכון כאמור בסעיף 10 בהוראה.

תמיכה ותחזוקה (סעיפים 13 – 14 להוראה)

13. בהתאם להערכת הסיכונים, על התאגיד הבנקאי להגדיר את הפעילויות עבורן נדרש הספק המהותי לעשות שימוש באמצעי זיהוי חזקים. הכוונה לפעילויות של הספק שעלולות לחשוף את התאגיד הבנקאי לסיכון גבוה כמו פעילות תחזוקה במערכות התאגיד הבנקאי או גישה מרחוק.

14. באשר לגישה מרחוק, נוכח הסיכונים הגלומים בפעילות זו, נדרש התאגיד הבנקאי, בהתאם להערכת הסיכונים, לקיים מנגנוני אבטחה ובקרה שיסייעו להפחתתם, כמפורט בפרק ד' בהוראה.

תחילה והוראות מעבר

15. תחילתה של הוראה זו לא יאוחר מ-6 חודשים ממועד פרסומה (להלן – מועד כניסת ההוראה לתוקף).

16. על אף האמור בסעיף 15 לעיל, התאגיד הבנקאי יחל בביצוע התהליכים המפורטים בסעיף 10 להוראה החל ממועד פרסום ההוראה.

17. הוראה זו תחול על הסכמי התקשרות עם ספקים שנכרתו (לרבות שחודשו) **לאחר** מועד כניסת ההוראה לתוקף.

18. לעניין הסכמי התקשרות עם ספקים שנכרתו (לרבות שחודשו) **לפני** מועד כניסת ההוראה לתוקף - במועד החידוש הקרוב של הסכם ההתקשרות ולא יאוחר מ-9 חודשים ממועד פרסום ההוראה, יפעל התאגיד הבנקאי בהתאם לקבוע בסעיף 10 להוראה והנהלת התאגיד הבנקאי תשקול ותחליט בדבר המשך ההתקשרות עם הספק המהותי, הצורך בעדכון ההסכם הקיים והמועד הנדרש לביצוע עדכון כאמור.

עדכון הקובץ

19. מצ"ב דפי עדכון לקובץ ניהול בנקאי תקין. להלן הוראות העדכון:

להוציא עמוד	**להכניס עמוד**
-----	363-1-5 [1] (04/18)

בכבוד רב

ד"ר חדוה בר

המפקח על הבנקים

ניהול סיכוני סייבר בשרשרת אספקה

פרק א': רקע

מבוא

1. בשנים האחרונות גדל מספר אירועי הסייבר המתרחשים בארגונים פיננסיים בעולם ובישראל. אירועים אלו מתאפיינים ברובם, בין היתר, בגרימה של נזק רב ובשיטות תקיפה מתוחכמות וחדשניות, שמקורן לעתים בגורמים חיצוניים המספקים שירותים שונים לתאגידים הבנקאיים. גורמים אלו נכללים בשרשרת האספקה (Supply Chain) של התאגידים הבנקאיים.
2. הוראת ניהול בנקאי תקין מס' 361 בנושא "ניהול הגנת הסייבר", נותנת ביטוי לצורך לקיים תהליך אפקטיבי לזיהוי והערכת הסיכונים, בין היתר, בהתייחס לסביבות הפעילות החיצוניות של התאגיד הבנקאי ולעבודה עם ספקי שירות חיצוניים, וכן קובעת כי יש לכלול את תהליכי ניהול שרשרת האספקה ותלות בגורמי חוץ במערך הגנת הסייבר. בנוסף, התאגיד הבנקאי נדרש לקבוע את הפעולות הנחוצות לוודא שהגורמים החיצוניים נוקטים באמצעים הנדרשים להפחתת חשיפת התאגיד הבנקאי לסיכוני סייבר.
3. יודגש כי חלק מגורמי החוץ הנכללים בשרשרת האספקה של התאגיד הבנקאי (כדוגמת חברות התומכות במתן שירותי מסחר בשוק ההון), הינם מהותיים לפעילותו ו/או חושפים אותו לסיכוני סייבר ואבטחת מידע פוטנציאליים גבוהים אשר בהתממשותם ניתן לתקוף את התאגיד הבנקאי או לפגוע בפעילותו (להלן: ספקים מהותיים).
4. מטרת הוראה זו הינה להבהיר את האחריות של התאגיד הבנקאי בנוגע לקיום תצורת עבודה מאובטחת מול הספקים המהותיים, ואת חובותיו לניהול סיכוני סייבר הולמים בפעילות ספקים אלו בחצרותיהם, בחצרי התאגיד הבנקאי ובממשקים שלהם עם התאגיד.
5. למרות האמור בסעיף 3 לעיל, יישום דרישות בהוראה זו כאשר הספק המהותי הינו תאגיד בקבוצה הבנקאית, יהיה בהתאם להערכת הסיכונים של התאגיד הבנקאי. לעניין סעיף זה, "קבוצה בנקאית" – התאגיד הבנקאי, תאגיד בנקאי השולט בו ותאגידים בשליטת מי מהם.
6. הפיקוח על הבנקים מכין הוראה רחבה בנושא "מיקור חוץ". הוראה זו תשולב בהוראה החדשה.

תחולה

7. (א) הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א-1981 (להלן בהוראה זו – "תאגיד בנקאי"):
   1) תאגיד בנקאי;
   2) תאגיד בנקאי כאמור בסעיפים 11(א) (3א) ו-(3ב);
   3) תאגיד בנקאי כאמור בסעיף 11 (ב);

4) סולק כהגדרתו בסעף 36ט.

(ב) המפקח רשאי לקבוע הוראות מסוימות שונות מאלו המפורטות להלן שיחולו על תאגיד בנקאי מסוים או לפטור במקרים חריגים תאגיד בנקאי מסוים מהוראה מסוימת המפורטת להלן.

פרק ב': כללי

8. תאגיד בנקאי יקבע עקרונות להתחייבויותיהם של ספקים מהותיים כלפי התאגיד הבנקאי בהתייחס לניהול סיכוני סייבר.

9. תאגיד בנקאי יגדיר בהסכם ההתקשרות עם הספק המהותי התייחסות פרטנית לנושא ניהול סיכוני סייבר (ראה פרק ג' להלן) ויוודא כי הספק עומד בעקרונות שהגדיר התאגיד הבנקאי (סעיף 8 לעיל).

10. תאגיד בנקאי יערוך אחת לתקופה:

(א) מיפוי של הספקים המהותיים של התאגיד הבנקאי; בחינה של הסכם ההתקשרות עימם; עמידתם בהתחייבויותיהם החוזיות; זאת, תוך התייחסות לצורך בשינויים הנדרשים מהספק כתוצאה מהתפתחויות ושינויים טכנולוגיים ושינויים בשירותים הניתנים.

(ב) הערכת סיכונים הנגזרים מהשירותים הניתנים ע"י הספקים המהותיים בהתבסס גם על הבחינה כאמור בסעיף 10 (א) לעיל ותוצאות הסקרים (סעיף 12 (ג) בהמשך).

11. במקרה שגורמים רלוונטיים בתאגיד הבנקאי יגיעו למסקנה לאחר הבחינה כאמור בסעיף 10 לעיל, כי הספק המהותי אינו עומד בהתחייבותיו, באופן שחושף את התאגיד הבנקאי לסיכוני סייבר משמעותיים, עליהם לדווח להנהלת התאגיד, תוך הצגת סיכונים אלו והשלכותיהם על התאגיד ולקוחותיו. במקרה זה, על ההנהלה יהיה לשקול ולהחליט בדבר המשך ההתקשרות עם הספק.

פרק ג': הסכם התקשרות

12. במסגרת הסכם ההתקשרות של התאגיד הבנקאי עם הספק המהותי, התאגיד הבנקאי יקח בחשבון את הצורך בשילוב ההיבטים הבאים בהסכם, בהתאם להערכת הסיכונים:

(א) הקשחת מערכות הספק המהותי המותקנות ברשת התאגיד הבנקאי בהתאמה לנהלי אבטחת המידע וניהול הסיכונים של התאגיד הבנקאי.

(ב) העברת קבצי Log ממערכות הספק, לפי בקשת התאגיד הבנקאי.

(ג) עריכת סקר פגיעויות ומבדקי חדירה מבוקרים אחת לתקופה לפי דרישת התאגיד הבנקאי גם לעניין תסריטי הבדיקות, ובהתאם לניהול הסיכונים.

(ד) טיפול בממצאים שזוהו בסקר ובמבדקי החדירה תוך פרק זמן סביר לאחר גילויים.

(ה) ביצוע בדיקת מהימנות לעובדי הספק המהותי הקשורים לשירות הניתן לתאגיד הבנקאי.

(ו) מינוי נאמן אבטחת מידע וסייבר אצל הספק המהותי והגדרת סמכויותיו ותפקידיו.

(ז) הצגת רשימה של ספקי משנה אשר תומכים בשירותים הניתנים לתאגיד הבנקאי ע"י הספק המהותי מידי תקופה שתיקבע ע"י התאגיד הבנקאי.

(ח) קביעת הסדרים למחיקת נתונים של התאגיד הבנקאי המאחוסנים בחצרי הספק, לאחר סיום ההתקשרות ו/או לפי דרישת התאגיד הבנקאי.

(ט) ביצוע הפרדה בחצרי הספק המהותי בין סביבות העבודה (פיתוח, ייצור, וכד').

(י) דיווח לתאגיד הבנקאי על אירועי סייבר אשר יתרחשו אצל הספק המהותי או אצל ספקי משנה שלו.

פרק ד': תמיכה ותחזוקה

13. התאגיד הבנקאי יגדיר פעילויות בהתאם להערכת הסיכונים, עבורן נדרש הספק המהותי לאמצעי זיהוי חזקים (2FA) בפעילויות, כגון: גישה מרחוק למערכות התאגיד הבנקאי, פעילות תחזוקה במערכות התאגיד הבנקאי, וכד'.
14. התאגיד הבנקאי יקבע מנגנוני אבטחה ובקרה בגישה מרחוק של הספק המהותי, בהתאם להערכת הסיכונים, כגון: מניעת גישה אלא אם אושרה על ידו; גישה מאובטחת ומסביבת פעילות נפרדת מיתר סביבות העבודה של הספק המהותי; הפעלת מנגנון ניתוק התקשורת (Time-out) לאחר פרק זמן שבו לא בוצעה פעילות מצד הספק המהותי; הקלטת וניטור פעילות תחזוקה; וכד'. כמו כן, גישה לסביבת הייצור של התאגיד הבנקאי לא תתאפשר, אלא אם אושרה על ידו.

עדכונים

חוזר מס'	גרסה	פרטים	תאריך
2560	1	חוזר מקורי	24/04/18