

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) (א3) ו-1(ב3) ;

(3) תאגיד בנקאי כאמור בסעיף 11(ב) ;

4) סולק כהגדרתו בסעיף 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.

טיוטה

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 המאוחסנים 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.

תאריך	פרטים	גרסה	חוזר XX מס'	עדכונים
03/2018	חוזר מקורי	1	XXX	