דיווח על אירועי כשל טכנולוגי, אירועי אבטחת מידע ומתקפת סייבר

מבוא ומטרות

1. התאגידים הבנקאיים הינם נדבך מהותי הנחוץ לפעילותו התקינה של הסקטור הפיננסי בישראל. מאחר ומערך טכנולוגיות המידע של התאגידים הבנקאיים מהווה תשתית קריטית לפעילותם העסקית, נדרשים התאגידים הבנקאיים לזהות ולטפל מהר ככל הניתן ובאופן היעיל ביותר באירועי כשל טכנולוגי ואירועי אבטחת מידע, לרבות מתקפות סייבר, תוך שהם ממשיכים לנהל תהליכים ולספק שירותים חיוניים. בהתאם לכך, מדיניות התאגיד הבנקאי ונהליו לטיפול באירועים מסוג זה – ראה פרק י"א להוראת ניהול בנקאי תקין מס' 364 בנושא "ניהול סיכוני טכנולוגיית המידע, אבטחת מידע והגנת הסייבר" (להלן: "הוראה 364") - נדרשים להתייחס בין היתר לתהליך הדיווח לפיקוח על הבנקים המחוייב על פי סעיף 171.1 להוראה 364 ואשר הוראה זו קובעת כיצד ובאילו מקרים הוא יתבצע.
2. לדיווח על אירועי כשל טכנולוגי ואירועי אבטחת מידע לפיקוח על הבנקים יש מספר מטרות וביניהן:
   2.1. לוודא כי התאגיד הבנקאי בו מתרחש האירוע מנהל את האירוע בצורה תקינה ולסייע בהתמודדות עם האירוע במידת הצורך.
   2.2. לספק את היכולת להעריך תמונת מצב עדכנית על מנת לקבל החלטה מושכלת האם ואילו פעולות הפיקוח על הבנקים נדרש לנקוט.
   2.3. זיהוי פוטנציאל לאירוע מערכתי וצמצום השפעת האירוע ככל שניתן על תאגידים בנקאיים נוספים.
   2.4. זיהוי התחומים אשר התאגיד הבנקאי או המערכת הבנקאית בכללותה נדרשים לנקוט לגביהם צעדים למניעת הישנות אירועים מסוג זה או צעדים שישפרו את עמידות התאגידים הבנקאיים בעתיד בהתרחשות אירועים מסוג זה.
   2.5. היערכות הפיקוח על הבנקים לתרחישים דומים בעתיד בהתבסס על הערכת סיכונים מתאימה למערכת הבנקאית.
   2.6. ווידוא תהליך תחקור והפקת לקחים בעקבות האירוע.

תחולה

3. (א) הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א 1981 (להלן: "תאגיד בנקאי"):
   (1) תאגיד בנקאי;
   (2) תאגיד כאמור בסעיף 11 (ב)(1);
   (3) בעל רישיון נותן שירותי תשלום בעל חשיבות יציבותית כהגדרתו בסעיף 36ט;

   (ב) בטל.

4. חובת הדיווח תחול על כל תאגיד בנקאי בנפרד, גם אם האירוע מתרחש בו זמנית במספר תאגידים בנקאיים השייכים לקבוצה בנקאית אחת.

הגדרות

5. בהוראה זו למונחים הבאים תהיה המשמעות כמפורט להלן:

אירוע אבטחת מידע	כהגדרתו בהוראה 364.
אירוע כשל טכנולוגי	כהגדרתו בהוראה 364.
אירוע כשל טכנולוגי מהותי	אירוע כשל טכנולוגי הגורם לשיבוש פעילות עסקית, תהליך או פונקציה אשר יש להם השפעה חמורה ונרחבת על הפעילות של התאגיד הבנקאי (ובכלל זה השפעה חמורה ונרחבת על פעילות מערך טכנולוגיית המידע כשלעצמו), על השירותים שהוא מעניק ללקוחותיו או על המערכת הבנקאית.
דלף מידע	כהגדרתו בהוראה 364.
טכנולוגיית המידע, מערך טכנולוגיית המידע	כהגדרתם בהוראה 364.
מתקפת סייבר	כהגדרתה בהוראה 364.
נזק	כהגדרתו בהוראה 364.
סטטוס האירוע	תיאור השלב בו נמצא האירוע המדווח: זיהוי – זיהוי קיום אירוע. ניתוח – איתור מקור האירוע והיקפו. עצירת החמרה/ הכלה — עצירת החמרת האירוע. טיפול/ הכרעה - ביצוע פעולות תיקון/ נטרול רכיבי התקיפה שמצויים בתאגיד הבנקאי. תוקן/ השבה – חזרה לתקינות ולפעילות מלאה.
צד ג'	כהגדרתו בהוראה 364.
שעות עבודה מקובלות	שעות העבודה המקובלות לעניין הוראה זו בלבד הן: ימים א'-ה' שהינם ימי עסקים במערכת הבנקאית, בין השעות 8:00 ל- 18:00.

סוגי אירועים המחייבים דיווח

6. להלן סוגי אירועים אשר מחייבים דיווח לפיקוח על הבנקים:

6.1. אירוע כשל טכנולוגי מהותי.

6.2. אירוע החשוד כאירוע אבטחת מידע אשר מנוהל על ידי או במעורבות מנהל הגנת הסייבר ואבטחת המידע (כמשמעותו בהוראה 364) של התאגיד הבנקאי או גורם ניהולי אחר מטעמו, ואשר הטיפול בו לא הסתיים תוך ארבע שעות ממועד זיהויו הראשוני או תוך שעתיים במידה וכבר ידוע על נזק כלשהו בגינו.

6.3. אירוע אבטחת מידע המשפיע בפועל על מספר רב של לקוחות, או שהינו מתקפת סייבר בעלת מאפייני תקיפה חדשים.

6.4. כל אירוע דלף מידע מהותי שלא נכלל בסעיפים 6.1 – 6.3.

6.5. אירוע כאמור בסעיפים 6.1 – 6.4 לעיל, המתרחש בתאגיד שבשליטת תאגיד בנקאי שהוא עצמו אינו תאגיד בנקאי, ויש לו השפעה מהותית, בין היתר, בהיבטי טכנולוגיה, מוניטין ופיננסים, על התאגיד הבנקאי השולט בו, על הקבוצה הבנקאית או על המערכת הבנקאית.

6.6. אירוע אבטחה חמור כמשמעותו בסעיף 31 לחוק שירות מידע פיננסי, (התשפ"ב -2021), המתרחש אגב פעילותו של התאגיד הבנקאי כמקור מידע או כנותן שירות מידע פיננסי בהתאם לחוק זה.

6.א. מבלי לגרוע מהוראת סעיף 6, פנה המפקח אל תאגיד בנקאי ודרש דיווח בשל חשש לקרות אירוע אבטחת מידע בעל השפעה מערכתית, ימסור התאגיד הבנקאי דיווח בהתאם להוראה זו.

אחריות הדיווח

7. תאגיד בנקאי יקבע חבר הנהלה שבאחריותו קיום האמור בהוראת דיווח זו.

8. אחראי דיווחים:

8.1. תאגיד בנקאי יקבע אחראי דיווחי אירועי כשל טכנולוגי ואחראי דיווח אירועי אבטחת מידע.

8.2. כל אירוע כאמור בסעיף 6 לעיל ידווח ע"י האחראי לכך מטעם התאגיד הבנקאי אל הפיקוח על הבנקים.

8.3. יכולה להתקיים זהות בין שני האחראים המנויים בסעיף 8.1 לעיל, בהתאם להחלטת התאגיד הבנקאי.

8.4. ניתן למנות ממלא מקום קבוע לכל אחד מאחראי הדיווח.

9. תאגיד בנקאי יעביר את פרטי האחראים שימונו בהתאם לסעיפים 7 ו – 8 לעיל, לאגף טכנולוגיה, חדשנות וסייבר בפיקוח על הבנקים ויעדכן אותו בכל שינוי במינויים אלה, לרבות שינוי בפרטיהם.

אופן הדיווח

10. **דווח ראשון על האירוע** –

10.1. תאגיד בנקאי ידווח דיווח טלפוני עד שעתיים מזיהוי האירוע כאירוע המחייב דיווח בהתאם לסעיף 6 לעיל, ולאחר מכן ישלים דיווח ראשוני בכתב עד 8 שעות ממועד הדיווח הטלפוני. הפיקוח על הבנקים רשאי להאריך או לקצר את המועד האמור לדיווח בכתב בהתקיים נסיבות המצדיקות זאת.

10.2. הדיווח הטלפוני יתבצע בכל שעה ובכל יום, ללא תלות בשעות העבודה המקובלות.

10.3. הדיווח הטלפוני יועבר, לפי העניין, למנהל/ת יחידת טכנולוגיה בבנקאות או למנהל/ת יחידת הסייבר הפיקוחית באגף טכנולוגיה, חדשנות וסייבר בפיקוח על הבנקים (להלן: "הגורם האחראי באגף טכנולוגיה, חדשנות וסייבר").

10.4. היה ומועד הדיווח הראשוני בכתב הינו בשעות שאינן שעות העבודה המקובלות - הדיווח הראשוני בכתב יועבר עם תחילת שעות העבודה המקובלות של היום העוקב.

11. אירוע כשל טכנולוגי מהותי ואירוע אבטחת מידע ידווחו כאירוע שקיים בו חשד למתקפת סייבר (בשדה המתאים בטופס הדיווח) כל עוד לא הוכח שאין חשד כאמור.

12. **דיווחים נוספים במהלך האירוע -**

12.1. תאגיד בנקאי נדרש לשלוח בכתב, על גבי טופס הדיווח האחרון שנשלח ככתוב לעיל, נתונים מעודכנים על פרטי האירוע לכל הפחות אחת ליום או ככל שיחולו שינויים מהותיים בפרטי האירוע ו/או בהשלכותיו, לרבות הקריטריונים לדיווח המפורטים בסעיף 6. הפיקוח על הבנקים רשאי לאשר בקשת תאגיד בנקאי להפחית את תדירות הדיווח באירוע מסוים, בהתקיים נסיבות המצדיקות זאת. האישור כאמור יעמוד בתוקף כל זמן שלא חל שינוי מהותי בפרטי האירוע או בהשלכותיו.

12.2. מבלי לגרוע מהאמור בסעיף 12.1 לעיל, יובהר כי אירוע שדווח על בסיס אחד הקריטריונים המפורטים בסעיף 6 ובהמשך מתברר שעונה על קריטריונים נוספים אינו מחייב דיווח חדש נוסף בגינו, אלא שנדרש לעדכן אודות הקריטריון הנוסף במסגרת הדיווחים השוטפים.

12.3. במקרה בו חלה התפתחות משמעותית באירוע שכבר מצוי בתהליכי דיווח, בשעות שמעבר לשעות העבודה המקובלות, יש לעדכן טלפונית את הגורם האחראי באגף טכנולוגיה, חדשנות וסייבר בפיקוח על הבנקים (כאמור בסעיף 10.3 לעיל), ולאחר מכן להעביר דיווח בכתב, כנדרש.

13. **דווח על סיום האירוע -**

13.1. תאגיד בנקאי נדרש לדווח על סיום האירוע.

13.2. התאגיד הבנקאי יוודא כי הטופס מלא ומכיל את כל הפרטים העדכניים ביותר למועד דיווח סיום האירוע.

תחקור אירוע ודיווח אודותיו

14. תאגיד בנקאי יקבע נוהל תחקיר אירוע, בו ייקבעו בין היתר שיטת התחקיר והגורמים המשתתפים בו. התחקיר יתבצע על ידי או במעורבותו של גורם בלתי תלוי באירוע. הנוהל יתייחס גם למקרה בו התרחש אירוע בתאגיד שבשליטת תאגיד בנקאי שהוא עצמו אינו תאגיד בנקאי.

15. תאגיד בנקאי יבצע תחקיר בסיום אירוע כאמור בסעיף 6 בהתאם לנוהל שקבע. התחקיר יכלול לכל הפחות את הנושאים הבאים:

15.1. פרטים סופיים ומעודכנים אודות האירוע ונסיבות התרחשותו (תוך התייחסות לכלל הפרטים שדווחו לפיקוח על הבנקים).

15.2. דו"ח הפקת לקחים, לרבות המלצות, יישום בקרות פנימיות, לו"ז לביצוע, פירוט הגורמים המעורבים בתחקיר ומאשר התחקיר.

16. התחקיר יאושר על ידי חבר ההנהלה האחראי על קיום ההוראה, כאמור בסעיף 7 לעיל, ויועבר לפיקוח על הבנקים בתוך עד 45 יום ממועד סיום האירוע או בתוך עד 60 יום ממועד זיהוי האירוע כאירוע המחויב בדיווח לפי סעיף 6 לעיל, לפי המוקדם מביניהם.

תיעוד אירועים שלא דווחו

17. בחן תאגיד בנקאי את הצורך לדווח על אירוע בהתאם להוראה זו והחליט שלא לדווח על האירוע לפיקוח על הבנקים, יתעד את ההחלטה, את הגורם שקיבל אותה, ואת הנימוקים לה. על אף האמור לעיל, סעיף זה לא יחול על אירועים אשר באופן מובהק אינם עונים על ההגדרות בסעיף 6 לעיל.

עדכונים

חוזר 06 מס'	גרסה	פרטים	תאריך
2643	1	חוזר מקורי	29/12/20
2669	2	עדכון	30/09/21
2680	3	עדכון	24/11/21
2736	4	עדכון	22/01/23
2848	5	עדכון	17/06/26