דיווח על אירועי כשל טכנולוגי ואירועי סייבר

תחולה

1. הוראה זו חלה על התאגידים המנויים בסעיף 3(א) להוראת נוהל בנקאי תקין מס' 366 "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".
2. הדיווח יחול על כל ישות בנפרד, גם אם האירוע מתרחש בו זמנית במספר תאגידים בנקאיים השייכים לקבוצה בנקאית אחת.

הרכב הדוח

3. הרכב הדוח:
לוח 01 - "דיווח על אירועי כשל טכנולוגי ואירועי סייבר"

דרך הדיווח

4. הדיווח הטלפוני יהיה לממונה האגפי כמפורט בנב"ת 366 "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".
5. הדיווח על לוח 01 יהיה באמצעות תקשורת מקוונת, בטכנולוגיה המאובטחת, המשמשת את בנק ישראל לדיווחים.

הגדרות

6. משמעות כל מונח בהוראה זו יהיה כהגדרתו בהוראת ניהול בנקאי מס' 366 "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".

אופן ומועדי הדיווח

7. **תהליך הדיווח יהיה כמפורט בזאת:**

7.1 **דיווח טלפוני**

דיווח טלפוני בתוך שעתיים מזיהוי האירוע כאירוע המחייב דיווח כהגדרתו בנב"ת 366 סעיף 6. הדיווח הטלפוני יתבצע ללא תלות בשעות העבודה המקובלות.

7.2 **דיווח ראשוני**

בתוך 8 שעות ממועד הדיווח הטלפוני יישלח דיווח בהתאם לפורמט לוח 01, עם כל המידע הידוע נכון למועד הדיווח.

7.3 **עדכון הדיווח**

7.3.1 ככל שיחולו שינויים מהותיים בפרטי האירוע, ולכל הפחות אחת ביום, יועבר דיווח מעודכן. גם אם לא חל שינוי בפרטי האירוע יש לדווח את המידע המעודכן ביותר נכון לאותו מועד אחת ליום.

7.3.2 הדיווח יתבצע בשעות העבודה המקובלות.

7.4 **דיווח על סיום האירוע**

7.4.1 עם סיום האירוע כהגדרתו על ידי הבנק, יישלח דיווח מעודכן עם כל המידע הידוע לאותו מועד.

7.4.2 לאחר קבלת דיווח על סיום אירוע, אחראי הדיווח מהפיקוח על הבנקים ישלח אישור על קבלת דיווח על סיום אירוע.

הנחיות כלליות

8. חובת דיווח חלה על כל אחד מסוגי האירועים הבאים המפורטים בנב"ת 366 בסעיף 6.

9. הנתונים המדווחים בכל אחד מהדיווחים יהיו מעודכנים, ככל שניתן, למועד הדיווח.

10. בדיווח על סיום אירוע - נתונים שאינם ידועים נכון לסיום האירוע ידווחו כ"טרם ידוע", ונתונים שאינם רלוונטיים ידווחו כ"לא רלוונטי".

11. יש לדווח באופן מצטבר כך שבכל דיווח יופיע המידע המצטבר המעודכן ביותר למועד הדיווח.

הנחיות ללוח 01

12. בכל סעיף בו נדרש לדווח על תאריך, הפורמט יהיה: DD/MM/YYYY.

13. בכל סעיף בו נדרש לדווח על שעה, הפורמט יהיה: HH:MM

14. בשורה 08 בסעיף "מספר האירוע" - יש לדווח את המס' המזהה של האירוע כפי שניתן על ידי האחראי על הדיווח בפיקוח על הבנקים. הדיווח הראשוני ישלח ללא מספר מזהה של האירוע, ולאחר קבלת מספר מזהה יש לדווח עליו בכל הדיווחים הנוספים בגין אותו אירוע.

15. בשורה 10 בסעיף " סוג האירוע" - יש לבחור בערך אחד או יותר, מתוך רשימת הערכים הבאה:
1 - אירוע כשל טכנולוגי מהותי
2 - אירוע סייבר העונה לקריטריונים בסעיף 6.2 בהוראת נב"ת 366
3 - אירוע סייבר בעל השפעה רבה או מאפייני תקיפה חדשים
4 - אירוע דלף מידע מהותי
5 - אירוע אבטחה חמור בהתאם לסעיף 6.6 בהוראת נב"ת 366

16. בשורה 11 בסעיף "מס' סידורי של הדיווח" - יש לדווח את המס' הסידורי של הדיווח בגין אותו אירוע.

17. בשורה 12 בסעיף "סטטוס האירוע" - יש לבחור בערך אחד או יותר, מתוך רשימת הערכים הבאה:
1 - זיהוי
2 - ניתוח

3 - עצירת החמרה/ הכלה

4 - טיפול/ הכרעה

5 - תוקן/ השבה

18. בשורה 20 בסעיף "האם האירוע חשוד כאירוע סייבר?" - רשימת בחירה עם הערכים: כן/לא. יש לבחור "לא" כאשר קיימת וודאות כי אין מדובר באירוע סייבר.

19. בשורה 21 בסעיף "האם האירוע דווח לרגולטורים אחרים" - רשימת בחירה עם הערכים כן/ לא.

20. בשורה 23 בסעיף "מס' אירוע קודם" - אם מדובר בהמשך של אירוע שהתרחש בעבר יש לציין מספר אירוע קודם.

21. בשורה 24 בסעיף "האם האירוע פורסם?" - רשימת בחירה עם הערכים: כן/לא.

22. בשורה 25 בסעיף "פרסום האירוע - פירוט" - יש לתת מידע נוסף כגון: מועד הפרסום, אמצעי הפרסום וכו'.

23. בשורה 26 בסעיף "תיאור האירוע" - יש לתת תיאור כללי של האירוע, ככל שידוע נכון למועד הדיווח.

24. בשורה 27 בסעיף "הערכת חומרת האירוע" - רשימת בחירה עם הערכים:1 - 4. יש להעריך את חומרת האירוע נכון למועד הדיווח, כאשר 1 - רמת חומרה נמוכה , ו- 4 - רמת חומרה גבוהה מאוד.

25. בשורה 28 בסעיף "תפקודים שנפגעו" - יש לפרט את הפונקציונליות / תהליכים עסקיים, לרבות מערכות מעורבות, שנפגעו כתוצאה מהאירוע. אם קיים חשש לפגיעה נוספת יש לפרט גם אותו.

26. בשורה 30 בסעיף "הגורם המזהה" - יש לציין את הגורם שזיהה את האירוע לראשונה, כגון: לקוח, התרעת מערכת וכו'.

27. בשורה 31 בסעיף "מקור האירוע" יש לתת מידע על הגורם שבגינו נגרם האירוע.

28. שורות 32 - 39 ידווחו רק בגין אירוע סייבר.

29. בשורה 32 בסעיף "סוג התוקף" - יש לבחור מתוך רשימה בחירה אחד או יותר מהערכים הבאים:

1 - עובד פנימי

2 - ספק

3 - גורמי פשע

4 - גורמי טרור

5 - ארגוני אקטיביזם

6 - מדינה

7 - לא ידוע

8 - אחר

30. בשורה 34 בסעיף "תיאור תרחיש התקיפה" - יש לתאר את תרחיש התקיפה, לרבות שיטת החדירה (וקטור התקיפה), ערוץ התקיפה ופרטים נוספים לגבי התקיפה.

31. בשורה 35 "מאפייני תקיפה חדשים" יש לפרט במידה ונעשה שימוש במאפייני תקיפה חדשים מנקודת ראות הבנק.

32. בשורה 36 בסעיף "מעורבות שרשרת אספקה" - רשימת בחירה עם הערכים: כן/לא. כאשר התשובה בסעיף 36 היא "לא" סעיפים 37 - 39 לא ימולאו. המונח שרשרת אספקה כמשמעותו בהוראת ניהול בנקאי תקין מס' 363.
33. בשורה 39 בסעיף "האם מדובר בספק מהותי?" - רשימת בחירה עם הערכים כן/לא.
34. בשורה 40 בסעיף "סוג הנזק" - יש לבחור מתוך רשימה סגורה את סוג הנזק (ניתן לבחור יותר מערך אחד
1 - שירות
2 - כספי/ פגיעה בנכסים
3 - מידע/ איסוף מודיעין
4 - מוניטין/ אמון הציבור
5 - ציות
6 - משפטי
7 - אחר
35. בשורה 41 בסעיף "תיאור הנזק" - יש לפרט את הנזקים כולל נזק כספי.
36. בשורה 42 בסעיף "אומדן נזק פוטנציאלי" - יש לפרט את כל הנזקים הפוטנציאלים כולל אומדן נזק כספי פוטנציאלי.
37. בשורה 44 "האם ניתן שיפוי מלא ללקוחות?" - רשימת בחירה עם הערכים: כן/לא.
38. בשורה 45 בסעיף "פירוט פעולות שבוצעו" - יש לפרט את הפעולות שננקטו ע"י הישות במסגרת האירוע (כולל workaround) לפי סדר כרונולוגי.
39. בשורה 48 בסעיף "גורמים פנימיים אליהם דווח האירוע" יש לבחור ערך אחד או יותר מתוך רשימת הערכים הבאים:
1 - יו"ר דירקטוריון
2 - דירקטוריון
3 - מנכ"ל
4 - CRO
5 - CIO
6 - מנהל הגנת סייבר
7 - מנהל אבטחת מידע
8 - מנהל תפעול
9 - מנהל המשכיות עסקית
10 - דוברות
11 - מנהל תשתיות
12 - אחראי ביטחון פיזי
13 - מחלקה משפטית
14 - סמנכ"ל היחידה העסקית הרלוונטית
15 - אחר.

40. בשורה 49 בסעיף "גורמים חיצוניים אליהם דווח האירוע" ובשורה 50 בסעיף "גורמים חיצוניים מעורבים בטיפול באירוע" יש לבחור מתוך רשימה בחירה, אחד או יותר מהערכים הבאים:

1 - משטרה

2 - Cert לאומי

3 - הרשות להגנת הפרטיות (רל"פ)

4 - בורסה

5 - אחר

דיווח על אירועי כשל טכנולוגי ואירועי סייבר

לוח 01

01	**פרטי התאגיד המדווח**	שם הישות המדווחת
02		מס' הישות המדווחת
03		תאריך הדיווח
04		שעת הדיווח
05		שם פרטי ושם משפחה של ממלא הדיווח
06		מס' טלפון נייד
07		מס' טלפון נוסף
08	**פרטי האירוע**	מס' האירוע
09		שם האירוע
10		סוג האירוע
11		מס' סידורי של הדיווח
12		סטטוס האירוע
13		תאריך האירוע
14		שעת האירוע
15		תאריך זיהוי האירוע
16		שעת זיהוי האירוע
17		שם פרטי ושם משפחה של מקבל הדיווח הטלפוני (בפיקוח על הבנקים)
18		תאריך דיווח ראשוני
19		שעת דיווח ראשוני
20		האם האירוע חשוד כאירוע סייבר?
21		האם האירוע דווח לרגולטורים אחרים?
22		פירוט רגולטורים אחרים אליהם דווח האירוע
23		מס' אירוע קודם
24		האם האירוע פורסם ?
25		פרסום האירוע - פירוט
26	**תיאור האירוע**	תיאור האירוע
27		הערכת חומרת האירוע
28		תפקודים שנפגעו
29		השפעת האירוע על משתמשים/ תחום/שירות
30		הגורם המזהה
31		מקור האירוע
32	**הרחבת מידע – אירוע סייבר**	סוג התוקף
33		סוג התוקף - פירוט
34		תיאור תרחיש התקיפה
35		מאפייני תקיפה חדשים
36		מעורבות שרשרת אספקה
37		פרוט מעורבות שרשרת אספקה

38		שם הספק
39		האם מדובר בספק מהותי?
40	**הערכת הנזק**	סוג הנזק
41		תיאור הנזק
42		אומדן נזק פוטנציאלי
43		מספר לקוחות וחשבונות שנפגעו
44		האם ניתן שיפוי מלא ללקוחות?
45	**ניהול האירוע**	פירוט פעולות שבוצעו
46		פירוט פעולות מתוכננות, כולל לו"ז מתוכנן
47		האם הופעל נוהל חרום ? (לפרט)
48		גורמים פנימיים אליהם דווח האירוע
49		גורמים חיצוניים אליהם דווח האירוע
50		גורמים חיצוניים מעורבים בטיפול באירוע
51		הערכת זמן לסיום האירוע
52	**פרטי סיום האירוע**	תאריך סיום האירוע
53		שעת סיום האירוע