

דיווח על אירועי כשל טכנולוגי ואירועי אבטחת מידע לרבות מתקפת סייבר

תחולה

1. הוראה זו חלה על התאגידים המנויים בסעיף 3(א) להוראת נוהל בנקאי תקין מס' 366 "דיווח על אירועי כשל טכנולוגי ואירועי אבטחת מידע" (להלן: "נב"ת 366"), המוגדרים בו כתאגידים בנקאיים.
2. הדיווח יחול על כל תאגיד בנקאי 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 אבטחת מידע לרבות מתקפת סייבר".

דרך הדיווח

4. דיווח הטלפוני לגורם האחראי באגף טכנולוגיה, חדשנות וסייבר" בפיקוח על הבנקים כמפורט בנב"ת 366.
5. דיווח על לוח 01 בפורמט Excel.

הגדרות

6. משמעות כל מונח בהוראה זו תהיה כהגדרתו בנב"ת 366.

אופן ומועדי הדיווח

7. תהליך הדיווח יהיה כמפורט בזאת:

7.1 דיווח טלפוני

דיווח טלפוני יהיה בתוך שעותיים מזיהוי האירוע כאירוע המחייב דיווח כהגדרתו בנב"ת 366 סעיף 6, ללא תלות בשעות העבודה המקובלות.

7.2 לוח 01 - דיווח ראשוני

בתוך שמונה שעות ממועד הדיווח הטלפוני, ישלח דיווח בהתבסס על המידע הידוע נכון למועד הדיווח.

7.3 לוח 01 - עדכון דיווח

7.3.1 ככל שיחולו שינויים מהותיים בפרטי האירוע, ולכל הפחות אחת ליום, יועבר

דיווח עדכני. 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 לוח 01 - 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 הגורם האחראי על הדיווח מאגף טכנולוגיה, חדשנות וסייבר בפיקוח על הבנקים, ישלח אישור על קבלת דיווח סיום אירוע.

הנחיות כלליות

8. חובת דיווח חלה על כל אחד מסוגי האירועים הבאים המפורטים בנב"ת 366.
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 לדיווח - לוח 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 03 "שם התאגיד בו אירע האירוע" - יש לדווח את שם התאגיד הבנקאי בו אירע האירוע או את שם התאגיד הנשלט שאינו תאגיד בנקאי בו אירע האירוע.
15. בשורה 10 "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.
16. בשורה 12 בסעיף "סוג האירוע" - יש לבחור בערך אחד או יותר, מתוך רשימת הערכים הבאה:
 - 1 - אירוע כשל טכנולוגי מהותי;
 - 2 - אירוע אבטחת מידע העונה לקריטריונים בסעיף 6.2 בהוראה 366;
 - 3 - אירוע אבטחת מידע המשפיע בפועל על מספר רב של לקוחות, או שהינו מתקפת סייבר בעלת מאפייני תקיפה חדשים;
 - 4 - אירוע דלף מידע מהותי;
 - 5 - אירוע אבטחה חמור בהתאם לסעיף 6.6 בהוראה 366.
 - 6 - אירוע אבטחת מידע המחויב בדיווח על פי דרישת הפיקוח על הבנקים בשל חשש להשפעה מערכתית שלו.
17. בשורה 13 בסעיף "סיבת סיווג האירוע ככזה המחייב דיווח לפיקוח על הבנקים" - יש לתאר בקצרה את הסיבה לסיווג האירוע כאירוע המחייב דיווח לפיקוח על הבנקים.
18. בשורה 14 בסעיף "מס' סידורי של הדיווח" - יש לדווח את המס' הסידורי של הדיווח בגין אותו אירוע.
19. בשורה 15 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
20. בשורה 25 בסעיף "האם האירוע חשוד כמתקפת סייבר?" - רשימת בחירה עם הערכים: כן/לא. יש לבחור "לא" כאשר קיימת וודאות כי אין מדובר במתקפת סייבר.
21. בשורה 26 בסעיף "האם האירוע דווח לרגולטורים אחרים" - רשימת בחירה עם הערכים כן/ לא.
22. בשורה 28 בסעיף "מס' אירוע קודם" - אם מדובר בהמשך של אירוע שהתרחש בעבר יש לציין את מספר האירוע הקודם.
23. בשורה 29 בסעיף "האם האירוע פורסם?" - רשימת בחירה עם הערכים: כן/לא.
24. בשורה 30 בסעיף "פרסום האירוע - פירוט" - יש לתת מידע נוסף כגון: מועד הפרסום, אמצעי הפרסום וכו'.
25. בשורה 31 בסעיף "תיאור האירוע" - יש לתת תיאור כללי של האירוע, ככל שידוע נכון למועד הדיווח.
26. בשורה 32 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.
27. בשורה 33 בסעיף "תפקודים שנפגעו" - יש לפרט את הפונקציונליות / תהליכים עסקיים, לרבות מערכות מעורבות, שנפגעו כתוצאה מהאירוע. אם קיים חשש לפגיעה נוספת יש לפרט גם אותו.
28. בשורה 35 בסעיף "הגורם המזהה" - יש לציין את הגורם שזיהה את האירוע לראשונה, כגון: לקוח, התרעת מערכת וכו'.
29. בשורה 36 בסעיף "מקור האירוע" יש לתת מידע על הגורם שבגיניו נגרם האירוע.
30. בשורה 37 בסעיף "מעורבות שרשרת אספקה" - רשימת בחירה עם הערכים: כן/לא. ככל שהתשובה לסעיף זה היא "לא" סעיפים 38 - 40 לא ימולאו. המונח שרשרת אספקה כמשמעותו בהוראה 364.
31. בשורה 40 בסעיף "האם מדובר בצד ג' מהותי?" - רשימת בחירה עם הערכים כן/לא.
32. שורות 41 - 44 ידווחו רק בגין מתקפת סייבר.
33. בשורה 41 בסעיף "סוג התוקף" - יש לבחור מתוך רשימה בחירה אחד או יותר מהערכים הבאים:
- 1 - עובד פנימי
 - 2 - צד ג' נותן שירות
 - 3 - צד ג' מקבל שירות
 - 4 - גורמי פשע
 - 5 - גורמי טרור
 - 6 - ארגוני אקטיביזם
 - 7 - מדינה
 - 8 - לא ידוע
 - 9 - אחר

34. בשורה 43 בסעיף "תיאור תרחיש התקיפה" - יש לתאר את תרחיש התקיפה, לרבות שיטת החדירה (וקטור התקיפה), ערוץ התקיפה ופרטים נוספים לגבי התקיפה.
35. בשורה 44 בסעיף "מאפייני תקיפה חדשים" יש לפרט האם נעשה שימוש במאפייני תקיפה חדשים, מנקודת ראות התאגיד הבנקאי.
36. בשורה 45 בסעיף "סוג הנזק" - יש לבחור מתוך רשימה סגורה את סוג הנזק (ניתן לבחור יותר מערך אחד):
- 1 - שירות
 - 2 - כספי/ פגיעה בנכסים (לרבות נכסי מידע)
 - 3 - מידע/ איסוף מודיעין
 - 4 - מוניטין/ אמון הציבור
 - 5 - ציות
 - 6 - משפטי
 - 7 - אחר
37. בשורה 46 בסעיף "תיאור הנזק" - יש לפרט את כלל הנזקים שאירעו כתוצאה מהאירוע, כולל נזק כספי.
38. בשורה 47 בסעיף "אומדן נזק פוטנציאלי" - יש לפרט את כלל הנזקים הפוטנציאליים כולל אומדן נזק כספי פוטנציאלי.
39. בשורה 49 "האם ניתן שיפוי מלא ללקוחות?" - רשימת בחירה עם הערכים: כן/לא.
40. בשורה 50 בסעיף "פירוט פעולות שבוצעו" - יש לפרט את הפעולות שננקטו ע"י התאגיד הבנקאי, או התאגיד הנשלט שאירע בו האירוע ושאינו התאגיד הבנקאי המדווח, במסגרת האירוע (כולל workaround) לפי סדר כרונולוגי.
41. בשורה 53 בסעיף "גורמים פנימיים אליהם דווח האירוע" ובשורה 54 בסעיף "גורמים פנימיים מעורבים בטיפול באירוע" 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 הסייבר ואבטחת המידע
 - 7 - מנהל תפעול
 - 8 - מנהל המשכיות עסקית
 - 9 - דוברות
 - 10 - מנהל תשתיות
 - 11 - אחראי ביטחון פיזי
 - 12 - מחלקה משפטית
 - 13 - סמנכ"ל היחידה העסקית הרלוונטית
 - 14 - אחר.
42. בשורה 55 בסעיף "גורמים חיצוניים אליהם דווח האירוע" ובשורה 56 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 אבטחת מידע לרבות מתקפת סייבר

לוח 01

שם התאגיד הבנקאי המדווח	01	פרטי התאגיד הבנקאי המדווח
קוד זיהוי התאגיד הבנקאי המדווח	02	
שם התאגיד בו אירע האירוע	03	
תאריך הדיווח	04	
שעת הדיווח	05	
שם פרטי ושם משפחה של ממלא הדיווח	06	
תפקיד ממלא הדיווח	07	
מס' טלפון נייד	08	
מס' טלפון נוסף	09	
מס' האירוע	10	פרטי האירוע
שם האירוע	11	
סוג האירוע	12	
סיבת סיווג האירוע ככזה המחייב דיווח לפיקוח על הבנקים	13	
מס' סידורי של הדיווח	14	
סטטוס האירוע	15	
תאריך האירוע	16	
שעת האירוע	17	
תאריך זיהוי האירוע	18	
שעת זיהוי האירוע	19	
תאריך זיהוי האירוע כאירוע המחייב דיווח לפיקוח על הבנקים	20	
שעת זיהוי האירוע כאירוע המחייב דיווח לפיקוח על הבנקים	21	
שם פרטי ושם משפחה של מקבל הדיווח הטלפוני (בפיקוח על הבנקים)	22	
תאריך דיווח ראשוני	23	
שעת דיווח ראשוני	24	
האם האירוע חשוד כמתקפת סייבר?	25	
האם האירוע דווח לרגולטורים אחרים?	26	
פירוט רגולטורים אחרים אליהם דווח האירוע	27	
מס' אירוע קודם	28	
האם האירוע פורסם ?	29	
פרסום האירוע - פירוט	30	
תיאור האירוע	31	תיאור האירוע
הערכת חומרת האירוע	32	
תפקודים שנפגעו	33	
השפעת האירוע על משתמשים/ תחום/ שירות	34	
הגורם המזהה	35	
מקור האירוע	36	
מעורבות שרשרת אספקה	37	
פרוט מעורבות שרשרת אספקה	38	
שם צד ג'	39	

האם מדובר בצד ג' מהותי?		40
סוג התוקף	הרחבת מידע – מתקפת סייבר	41
סוג התוקף - פירוט		42
תיאור תרחיש התקיפה		43
מאפייני תקיפה חדשים		44
סוג הנזק	הערכת הנזק	45
תיאור הנזק		46
אומדן נזק פוטנציאלי		47
מספר לקוחות וחשבוניות שנפגעו		48
האם ניתן שיפוי מלא ללקוחות?		49
פירוט פעולות שבוצעו	ניהול האירוע	50
פירוט פעולות מתוכננות, כולל לו"ז מתוכנן		51
האם הופעל נוהל חרום ? (לפרט)		52
גורמים פנימיים אליהם דווח האירוע		53
גורמים פנימיים מעורבים בטיפול באירוע		54
גורמים חיצוניים אליהם דווח האירוע		55
גורמים חיצוניים מעורבים בטיפול באירוע		56
הערכת זמן לסיום האירוע		57
תאריך סיום האירוע	פרטי סיום האירוע	58
שעת סיום האירוע		59