דיווח מדדי סייבר

תחולה

1. הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א 1981 (להלן: "תאגיד בנקאי"):
   1.1. תאגיד בנקאי, למעט בנקי חוץ;
   1.2. תאגיד כאמור בסעיף 11(ב);
   1.3. נותן שירותי תשלום בעל חשיבות יציבותית כהגדרתו בסעיף 36ט.
2. על אף האמור בסעיף קודם, תאגידים בנקאיים שמנהל הגנת הסייבר שלהם הוא מנהל הגנת הסייבר של תאגיד בנקאי שולט, יהיו פטורים מהדיווח בכפוף לאישור הפיקוח על הבנקים.

בסיס הדיווח

3. הדיווח הינו על בסיס לא מאוחד.

תדירות הדיווח

4. הדיווח על לוח 01 יהיה בתדירות רבעונית.
5. הדיווח על לוחות 02 - 06 יהיה בתדירות שנתית.

מועד הגשת הדוח

6. הדיווח השנתי יוגש עד הראשון באפריל בכל שנה. הדיווח הרבעוני יוגש בתום חודש מסוף הרבעון.

הרכב הדוח

7. הדיווח כולל ששה לוחות כמפורט להלן:
   לוח 01 - מגמות השינוי במתקפות הסייבר (רבעוני);
   לוח 02 - מדדי סייבר תפעוליים (שנתי);
   לוח 03 - משאבים (שנתי);
   לוח 04 - ביקורות פנימיות בנושא הגנת הסייבר ואבטחת מידע (שנתי);
   לוח 05 - ביקורות פנימיות בנושא הגנת סייבר ואבטחת מידע כנושא ראשי/ מוביל שפורסמו בתקופת הדיווח (שנתי);
   לוח 06 - הגדרות התאגיד הבנקאי (שנתי).

דרך הדיווח

8. יש לדווח באמצעות תקשורת מחשבים באינטרנט, בטכנולוגיה המאובטחת, המשמשת את בנק ישראל. מתכונת הדיווח מצורפת בזה.

הגדרות

9. "**אירוע דלף מידע**" - אירוע שהתרחש בו "דלף מידע", כהגדרתו בהוראת נב"ת 364 "ניהול סיכוני טכנולוגיית המידע, אבטחת המידע והגנת הסייבר" (להלן: "הוראה 364"). "אירוע דלף מידע" בהוראה זו לא יכלול אירוע של מדיה שאינה אלקטרונית.
10. "**אירוע תודעה**" - מצג שווא של מתקפת סייבר, ללא תקיפה בפועל, באמצעות הטעיה או ניצול מצבי כשל שאינם קשורים למתקפה כלשהי, והצגתם כתקיפת סייבר שהצליחה.
11. "**דלף מידע**", "**השבה (Recovery)**", "**צד ג' / צדדים שלישיים**", "**קריטיות**" "**רגישות**" (בהקשר של המונח קריטיות בצמידות למונח רגישות), "**תשתית טכנולוגית**" - כהגדרתם בהוראה 364.
12. "**דרישת כופר**" - מתקפת סייבר או אירוע תודעה שבמסגרתם נכללה דרישת תשלום בכדי לעצור או למנוע את המשך המתקפה או בכדי להשיב נכסי מידע שנפגעו במהלך המתקפה.
13. "**מחשוב ענן**" - כהגדרתו בהוראת ניהול בנקאי 362 "מחשוב ענן".
14. "**מערכת**" - כהגדרתה בהוראה 364.
15. "**מערכת מהותית**" - מערכת התומכת ב"תהליך או שירות חיוני" כהגדרתו בהוראת ניהול בנקאי 355 "ניהול המשכיות עסקית".
16. "**משתמש פריווילגי**" - משתמש בעל הרשאות מוגברות או בעל הרשאות גישה למידע רגיש (לדוגמא: domain admin, מנהלי מערכות, אחראי גיבויים או מנהלי רשת).
17. "**מתקפת סייבר**" - כהגדרתה בהוראה 364. יש להבדיל מאירוע סייבר המחייב דיווח לפיקוח על הבנקים על פי הוראת נב"ת מס' 366 בנושא "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".
18. "**שירותי בנקאות בתקשורת**" - כהגדרתם בהוראת ניהול בנקאי 367 "בנקאות בתקשורת", אלא אם נאמר בהוראה זו אחרת.
19. "**תחנת עבודה**" - מחשב נייח או מחשב נייד שמסופק ומנוהל על ידי התאגיד הבנקאי ומתחבר לרשת הארגונית.
20. "**תרגול התאוששות רטוב**" - תרגיל מעשי בו נבדקת הלכה למעשה יכולת החזרה לפעולה של מערכות שנפגעו בהתאם לנוהל שהוגדר מראש.
21. "**BYOD**" - מכשירים ממוחשבים בבעלות עובדים, כגון: טלפונים חכמים ומחשבים ניידים, המשמשים לצרכי עבודה (Bring Your Own Device).

הנחיות כלליות

22. דיווח שדות המלל יהיה בעברית למעט מונחים מקצועיים שידווחו בלועזית כגון: שמות וסוגים של מערכות.
23. הדיווח באחוזים יהיה במספרים שלמים (לדוגמא: בדיווח על 24 אחוזים יש לדווח 24).
24. בסעיפים בהם קיימת אפשרות לפירוט נוסף, ניתן לפרט ולהסביר במלל חופשי. במקרים מסוימים, הפירוט הנוסף הינו חובה, כמפורט בהנחיות לדיווח על הלוחות.
25. מתקפת סייבר תכלול גם ניסיון תקיפה שלא צלח או שלא גרם נזק בפועל.

נחיות ללוח 01 - מגמות שינוי במתקפות הסייבר

26. בשורות 01 - 07, 12 יש לדווח בעמודה 02 "מגמת שינוי ביחס לרבעון קודם" על מגמות השינוי בניסיונות התקיפה השונים, במהלך הרבעון המדווח. יש לבחור ערך מתוך רשימת בחירה כלהלן:
    1 - ללא שינוי
    2 - ירידה
    3 - עליה
    4 - עליה משמעותית
27. בשורה 01 "מגמת שינוי כללית במתקפות הסייבר" תתאר את מגמת השינוי הכללית בכמות מתקפות הסייבר.
28. בשורות 03 - 08 "השינוי במגמה מאז הדיווח האחרון", יש לדווח בעמודה 01 על כמות מתקפות הסייבר השונות, במהלך הרבעון המדווח.
29. בשורה 08 יש לפרט מתקפות שלא נכללו בשורות 03 - 07. בסעיף "פירוט" נדרש לציין את סוגי מתקפות הסייבר, את כמותן ואת מגמת השינוי בכל אחד מהם.
30. בשורה 09 "כמות מתקפות הסייבר" - יש לדווח על מספר מתקפות הסייבר שהתרחשו במהלך הרבעון המדווח, בהם לפחות אחד ממנגנוני ההגנה כשל והמתקפה לא זוהתה או לא נעצרה על ידי מנגנון ההגנה, בהתאם לפונקציונליות המיועדת שלו, גם אם המתקפה נעצרה על ידי מנגנון הגנה אחר. יש לדווח גם על מתקפה אשר לא כשל בה אף מנגנון הגנה.
    דוגמא למתקפת סייבר בה נחדרו מספר שכבות הגנה והמתקפה נעצרה בשכבה הגנה אחרת - תוקף מחליף קובץ עדכון תוכנה ומצרף אליו קוד זדוני שמנצל פגיעות לא מוכרת (Day-0). הקוד הזדוני זוהה בתחנת העבודה על ידי EDR, כך שבסופו של דבר לא נגרם נזק, אבל הקוד הזדוני לא זוהה בסינון הדואר או ב-Sandbox וגם לא זוהה במערכות זיהוי אנומליה ברשת.
31. בשורה 10 "משך זמן ממוצע מזיהוי ועד להשבה" - משך זמן ממוצע (בשעות), מזיהוי מתקפת הסייבר ועד לחזרה לתקינות ופעילות מלאה של כל פעילות אצל התאגיד הבנקאי שנפגע מהמתקפה.
32. בשורות 11, 12 הדיווח על אירועים של צדדים שלישיים יהיה על בסיס מיטב ידיעתו של התאגיד הבנקאי נכון למועד הדיווח, ובהתאם לדיווח שמועבר אליו מהספק (צד ג') או מחברת מודיעין או מגורמים מדינתיים אחרים".
33. אין באמור בסעיף קודם מלגרוע מאחריותו של התאגיד הבנקאי לקיום מכלול הדינים וההוראות החלים עליו.
34. בשורה 13 "מספר הלקוחות שמידע בגינם דלף מתוך התאגיד הבנקאי" - יש לדווח את מספר הלקוחות שמידע בגינם דלף מתוך התאגיד הבנקאי, (ללא מחזור של מידע מתוך אירועי דלף מידע ישנים). הדיווח יהיה על אירועי דלף מידע המחויבים בדיווח לרשות להגנת הפרטיות.
35. בשורה 14 "מספר העובדים שמידע אודותיהם או אודות פעילותם כעובדים דלף מתוך התאגיד הבנקאי" - יש לדווח את מספר העובדים שמידע אודותיהם או אודות פעילותם כעובדים, דלף לראשונה מתוך התאגיד הבנקאי ללא מחזור של אירועי דלף ישנים.
36. בשורה 15 "מס' אירועי דלף מידע בהם דלף מידע עסקי / תפעולי רגיש" - יש לדווח על כל אירועי דלף מידע עסקי ולא רק אירועי דלף מידע המחויבים בדיווח לרשות להגנת הפרטיות.

הנחיות ללוח 02 - מדדי סייבר תפעוליים

37. בשורה 01 "היקף הנזק הכספי בפועל ממתקפות סייבר (ללא הונאות לקוחות)" - יש לדווח על היקף הנזק הכספי בפועל (באלפי ש"ח) של כלל מתקפות הסייבר (ללא אירועי הונאות כנגד לקוחות), כפי שדווח לדירקטוריון ברמה שנתית.
38. בשורה 03 "שיעור הסקרים והמבדקים שלא בוצעו במועד הנדרש" - הדיווח על סעיף זה יהיה בהתאם לעקרונות לקביעת היקף, תדירות וסוג הבדיקות כפי שגובשו ואושרו על ידי התאגיד הבנקאי. הדיווח יהיה באחוזים שלמים.
39. בשורה 04 "מספר חשיפות פתוחות חורגות ברמת חומרה גבוהה ומעלה" - יש לדווח על מספר החשיפות הפתוחות ברמת חומרה גבוהה ומעלה (בהתאם להגדרת התאגיד הבנקאי), במערכות בסיכון גבוה, שמופו בסקרים ומבדקים ושחרגו ממסגרת הזמן לתיקון הליקוי (בהתאם להגדרת התאגיד הבנקאי), נכון לתום התקופה המדווחת.
40. בשורה 05 "מספר חשיפות פתוחות חורגות ברמת חומרה בינונית ומטה" - יש לדווח על מספר הליקויים הפתוחים ברמת חומרה בינונית ומטה (בהתאם להגדרת התאגיד הבנקאי) במערכות בסיכון גבוה, שמופו בסקרים ומבדקים ושחרגו ממסגרת הזמן לתיקון הליקוי (בהתאם להגדרת התאגיד הבנקאי), נכון לתום התקופה המדווחת.
41. בשורה 06 "משך זמן ממוצע לטיפול בחולשה ברמה גבוהה ומעלה" - משך הזמן הממוצע בימים קלנדריים, שחלף מרגע פרסום טלאי אבטחה או התרעה קריטית, לחולשה גבוהה ומעלה (על פי הגדרת התאגיד הבנקאי, יכול להיות לפי CVSS או מדד אחר שהתאגיד הבנקאי אימץ), במערכות או בציוד שחשופות מחוץ לתאגיד הבנקאי עד לסגירת החולשה.
42. שורה 07 "מספר חשיפות פתוחות ברמת חומרה גבוהה ומעלה, במערכות מחשוב ענן" - מספר ליקויים פתוחים ברמת חומרה גבוהה ומעלה (סקרים ומבדקים) בהתאם להגדרת התאגיד הבנקאי.
43. שורה 08 "שימוש במודיעין טכני" - יש לדווח האם נעשה שימוש במודיעין טכני, לדוגמא: נתוני IOC (Indicator Of Compromise), נתוני HASH, חתימות, כתובות IP וכו'. רשימת ערכים לבחירה, כן / לא.
44. שורה 09 "שימוש במודיעין איכותני" - יש לדווח האם נעשה שימוש במודיעין איכותני, לדוגמא: מידע וניתוח כדוגמת אירועים, קבוצות תקיפה, יכולות וכוונות. רשימת ערכים לבחירה כן/ לא.
45. בשורות 10 - 12 יש לדווח על מערכות הגנה / תחנות עבודה/ שרתים, שלפחות אחד מהרכיבים שלהם נמצא ב- EOL (End Of Life) או EOS (End Of Support).
46. בשורה 14 "שיעור מערכות מהותיות שלא מחוברות ל-SIEM/SOC בתאגיד הבנקאי" - יש לדווח על שיעור המערכות המהותיות שלא מחוברות ל -SIEM/SOC מתוך כלל המערכות המהותיות.
47. בשורה 15 "שיעור התראות שהגיעו למערכת ה - SIEM ואובחנו כ- "False Positive", יש לדווח על שיעור המקרים בהם הייתה ההתראה במערכת ה - SIEM לאירוע שהתברר שאינו מתקפת סייבר.
48. בשורה 16 "שיעור השרתים החשופים לאינטרנט שהוקשחו לפי מפרט מקובל ועדכני" - יש לדווח על אחוז השרתים שהוקשחו לפי מפרט מקובל ועדכני (בהתאם להגדרת התאגיד הבנקאי) מתוך סך השרתים.

49. בשורה 17 "שיעור תשתית טכנולוגית אחרת שחשופה לאינטרנט שהוקשחה לפי מפרט מקובל ועדכני" - יש לדווח על שיעור האמצעים בתשתית טכנולוגית בעלי כתובת IP שניתנת לגישה מרשת האינטרנט, שהוקשחו לפי מפרט מקובל ועדכני (בהתאם להגדרת התאגיד הבנקאי), מתוך סך האמצעים בתשתית הטכנולוגית של התאגיד הבנקאי. אין לדווח בסעיף זה על שרתים שדווחו בשורה 16 "שיעור השרתים החשופים לאינטרנט שהוקשחו לפי מפרט מקובל ועדכני".
50. בשורה 18 "שיעור השרתים המוקשחים ברשתות הפנימיות לפי מפרט מקובל ועדכני" - יש לדווח על אחוז השרתים שאינם מחוברים לאינטרנט, שהוקשחו לפי מפרט מקובל ועדכני (בהתאם להגדרת התאגיד הבנקאי) מתוך סך השרתים.
51. בשורה 20 "תרגילי סייבר" - יש לדווח על מספר תרגילי סימולציית סייבר שהתקיימו ברבדים שונים (הנהלה, גורמים טכניים וכו') אשר מדמים התקפות סייבר על מערכות מחשוב ורשתות, כדי לבדוק את חוסנן ואת יכולת התגובה של התאגיד הבנקאי במטרה לשפר תהליכים קיימים.
52. בשורות 26 - 27 יש לציין בשדה "פירוט נוסף" את שם החברה עמה התקשר התאגיד הבנקאי בהסכם.
53. בשורה 28 " מספר ספקים פעילים" - מספר הגורמים מולם קיימת התקשרות רכש פעילה.
54. בשורה 29 "מזה: מספר הספקים שחושפים את התאגיד הבנקאי לסיכוני סייבר מהותיים" - יש לפרט בשדה "פירוט נוסף" את הקריטריונים לסיווג הספקים ככאלה שחושפים את התאגיד הבנקאי לסיכוני סייבר מהותיים.
55. בשורה 32 "מספר משתמשים אנושיים ברשת" - יש לדווח על מספר היוזרים המוגדרים ברשת למשתמשים אנושיים, כולל יוזרים הרשומים ב -domain controller או ב - active directory , יוזרים כפולים, יוזרים במצב גיבוי וכו'.
אם למשתמש אנושי יש יותר מיוזר אחד יש לדווח את מס' היוזרים, ואם יש יוזר שמשמש מספר משתמשים אנושיים, היוזר יספר פעם אחת.
56. בשורות 35 - 38 המונח MFA משמעותו "אימות רב גורמי".
57. בשורה 35 "שיעור משתמשים ברשת שמתחברים ב - MFA" - שיעור המשתמשים שנדרשים לחיבור MFA בכניסה לרשת באתרי התאגיד הבנקאי, מתוך סך המשתמשים ברשת.
58. בשורה 36 "שיעור משתמשים פריווילגים שנדרשים ל-MFA בכל חיבור מכל מקום" - יש לדווח על שיעור המשתמשים הפריווילגים שנדרשים ל-MFA בכל חיבור מכל מקום מתוך סך המשתמשים הפריווילגים.
59. בשורה 37 "שיעור המשתמשים המתחברים מרחוק שנדרשים ל-MFA בקרב צדדים שלישיים" - שיעור משתמשים המתחברים מרחוק שנדרשים ל - MFA בקרב כל צדי ג' מתוך סך המשתמשים המתחברים מרחוק בקרב כל צדי ג'.
60. בשורה 38 "שיעור המשתמשים המתחברים מרחוק שנדרשים ל-MFA בקרב עובדי התאגיד הבנקאי (לרבות עובדים במיקור חוץ)" - שיעור משתמשים המתחברים מרחוק שנדרשים ל - MFA בקרב עובדי התאגיד הבנקאי, מתוך סך המשתמשים המתחברים מרחוק בקרב עובדי התאגיד הבנקאי.
61. בשורה 43 "תדירות בקרת הרשאות למשתמשים פריווילגים בתאגיד הבנקאי" - יש לציין מהי תדירות בקרת ההרשאות למשתמשים פריווילגים בתאגיד הבנקאי בחודשים (מספר שלם).

62. בשורה 44 "שיעור שרתים ברשתות החשופות לאינטרנט שמופעל בהם EDR" - יש לדווח על שיעור השרתים ברשתות החשופות לאינטרנט שמופעל בהם EDR, מתוך סך השרתים ברשתות החשופות לאינטרנט.
63. בשורה 45 "שיעור השרתים ברשת הפנימית שמופעל בהם EDR" - יש לדווח על שיעור השרתים ברשת הפנימית שמופעל בהם EDR, מתוך סך השרתים ברשת הפנימית.
64. בשורה 46 "שיעור תחנות העבודה שמופעל בהם EDR" - יש לדווח על שיעור תחנות העבודה שמופעל בהן EDR, מתוך סך תחנות העבודה.
65. בשורות 47, 48 - הביטוי "מחוץ לרשת" מתייחס לכל מקום שבו נמצא המידע שגובה, כך שבאם תוקף או קוד זדוני נמצאים בתוך הרשת, הם אינם יכולים לפגוע בגיבוי.
66. בשורות 49 - 52 "תרגיל התאוששות רטוב" כהגדרתו בהוראה זו. ככל שהתשובה היא "כן" - יש לפרט בסעיף "פירוט נוסף" מה נעשה במסגרת התרגיל המדובר .
67. בשורות 53 - 54 יש לדווח על תדירות הסריקות בימים קלנדריים. לדוגמא: כאשר התדירות היא אחת ליומיים, יש לדווח 2.
68. בשורה 55 "מספר ערוצי הגישה הלא מאובטחים" - יש לרשום את מספר הערוצים אשר מאפשרים גישה למשתמשים חיצוניים באמצעות פרוטוקולים לא מאובטחים, נכון לתום התקופה המדווחת. כגון: http, telnet, ftp.
69. בשורות 56 - 57 , בהתייחס לעובדי התאגיד הבנקאי כולל עובדים במיקור חוץ.

הנחיות ללוח 03 - משאבים

70. שורות 01 - 06 מתייחסות לכלל תקציב הגנת הסייבר ואבטחת המידע, באלפי ש"ח בכל החטיבות בתאגיד הבנקאי בתקופת הדיווח.
71. בשורות 07 - 19 יש לדווח על מספר משרות לנכון לתום התקופה המדווחת.
72. הנתונים אודות "משרות" יכללו גם עובדים במיקור חוץ ללא קשר למקור המימון.
73. בשורות 17 - 18, ממלא מקום הינו גורם שהוגדר על ידי התאגיד הבנקאי כממלא מקומו של מנהל הגנת הסייבר בהיעדרו.

הנחיות ללוח 04 - קווי הגנה ובקרות

74. בלוח זה יש לדווח על ביקורות שנושא הגנת הסייבר ואבטחת המידע הוא הנושא הראשי / המוביל.
75. בשורה 03 - 04 יש לדווח על מספר ימי העבודה כולל מיקור חוץ (במידת הצורך, יש להמיר את עלות הביקורת במיקור חוץ לימי עבודה).
76. בשורה 05 יש לכלול גם ממצאים בנושא הגנת הסייבר ואבטחת המידע שמקורם בביקורות שנושא הגנת הסייבר ואבטחת המידע אינו הנושא הראשי / מוביל בהן.

הנחיות ללוח 05 - ביקורות פנימיות בנושא הגנת הסייבר ואבטחת המידע (נושא ראשי / מוביל) שפורסמו בשנת הדיווח

77. בלוח זה יש לדווח על ביקורות שנושא הגנת הסייבר ואבטחת המידע הוא הנושא הראשי / המוביל.
78. בעמודה 01 "מספר הביקורת" יש לדווח את המספר המזהה כפי שנקבע ע"י התאגיד הבנקאי.
79. בעמודה 04 יש לבחור ערך מתוך רשימת בחירה כלהלן: ביקורת חדשה / השלמת ביקורת.

80. ביקורת חדשה תחשב כביקורת שהחלה במהלך התקופה המדווחת. השלמת ביקורת תחשב כביקורת שתוכננה להתבצע בשנה קודמת ומבוצעת בתקופת הדיווח.
81. בעמודה 05 "ציון הביקורת" - יש לדווח על ערך בין 1 - 5 , כאשר 1 הוא הציון הטוב ביותר, ו - 5 הוא הציון הגרוע ביותר. ביקורות בזמן אמת תדווחנה עם ציון "אפס".

הנחיות ללוח 06 - הגדרות התאגיד הבנקאי

82. יש לציין את הגדרת התאגיד הבנקאי לכל אחד מהמונחים המפורטים.
83. בסעיפים 06 - 08, יש לדווח על מסגרת הזמן בימים קלנדריים.
84. בשורה 10 "שם מפרט הקשחה מקובל ועדכני" יש לציין את שם התקן או שם המפרט המקובל והעדכני, ואת רמת העדכניות שבה בחר התאגיד הבנקאי לאמץ.

דיווח מדדי סייבר

לוח 01 - מגמות השינוי במתקפות הסייבר (רבעוני)

			כמות	מגמת שינוי ביחס לרבעון קודם	פירוט נוסף
			01	02	03
01	מגמת שינוי כללית במתקפות הסייבר				
02	מגמת שינוי כללית - רמת תחכום מתקפות הסייבר				
03	מגמת שינוי במתקפות הסייבר	מניעת שירות (DDOS)			
04		דלף מידע			
05		חדירת קוד עוין			
06		אירועי תודעה			
07		דרישות כופר			
08		אחר			
09	מתקפות סייבר שבמסגרתן לפחות שכבת הגנה אחת לא עצרה את המתקפה	כמות מתקפות הסייבר			
10		משך זמן ממוצע מזיהוי ועד להשבה			
11	צדדים שלישיים	מס' מתקפות הסייבר או אירועי דלף מידע שהתרחשו בתאגיד הבנקאי שמקורם בצד ג'			
12		מס' מתקפות הסייבר שהתרחשו בחצרות גופי צד ג' והשפיעו על התאגיד הבנקאי			
13	דלף מידע	מס' הלקוחות שמידע שלהם דלף מתוך התאגיד הבנקאי			
14		מס' העובדים שמידע אודותיהם או אודות פעילותם כעובדים דלף מתוך התאגיד הבנקאי			
15		מס' אירועי דלף מידע בהם דלף מידע עסקי / תפעולי רגיש			

דיווח מדדי סייבר

לוח 02 מדדי סייבר תפעוליים (שנתי)

					פירוט נוסף
				01	02
01	**נזקים כספיים**		היקף הנזק הכספי בפועל ממתקפות הסייבר (ללא הונאות לקוחות)		
02			מגמת שינוי ביחס לשנה קודמת		
03	**טיפול בחשיפות**	סקרים ומבדקים במערכות בסיכון גבוה	שיעור הסקרים והמבדקים שלא בוצעו במועד הנדרש		
04			מספר חשיפות פתוחות חורגות ברמת חומרה גבוהה ומעלה		
05			מספר חשיפות פתוחות חורגות ברמת חומרה בינונית ומטה		
06			משך זמן ממוצע לטיפול בחולשה ברמה גבוהה ומעלה		
07			מספר חשיפות פתוחות ברמת חומרה גבוהה ומעלה, במערכות מחשוב ענן		
08			שימוש במודיעין טכני		
09	**שירותי מודיעין בתשלום**		שימוש במודיעין איכותני		
10	**מערכות**	EOL / EOS	מספר מערכות הגנה ב - EOS/EOL		
11			שיעור תחנות עבודה ב- EOS מסך תחנות העבודה		
12			שיעור השרתים ב-EOS מתוך סך השרתים		
13		SIEM / SOC	שיעור המערכות שלא מחוברות ל-SIEM / SOC בתאגיד הבנקאי		
14			מזה: שיעור מערכות מהותיות שלא מחוברות ל-SIEM / SOC בתאגיד הבנקאי		
15			שיעור התראות שהגיעו למערכת ה- SIEM ואובחנו כ- False Positive		
16		תשתית טכנולוגית	שיעור השרתים החשופים לאינטרנט שהוקשחו לפי מפרט מקובל ועדכני		
17			שיעור תשתית טכנולוגית אחרת שחשופה לאינטרנט שהוקשחה לפי מפרט מקובל ועדכני		
18			שיעור השרתים המוקשחים ברשתות הפנימיות לפי מפרט מקובל ועדכני		
19			שיעור המחשבים הניידים והניידים המשמשים לעבודה מרחוק בתצורת BYOD מכלל המחשבים הניידים והניידים המשמשים לגישה מרחוק		
20	**היערכות לאירועים, תירגולים ותרחישי קיצון**	תירגולים	תרגילי סייבר		
21			מזה: תרגילי Red Team (סימולצית תקיפה) שנערכו במהלך השנה		
22			מזה: תרגילי Table Top שנערכו במהלך השנה		
23			האם תורגל תרחיש קיצון סייבר במהלך השנה?		
24			האם תורגל אירוע סייבר כחלק מאירוע המשכיות עסקית (מלחמה, רעידת אדמה וכדו') במהלך השנה?		
25		ניהול משברי סייבר	האם קיים צוות IR (Incident Response) פנימי?		
26			האם יש הסכם לשירות עם חברת IR טכני חיצונית שכולל SLA מחייב לשגרה וחירום?		
27			האם יש הסכם לשירות עם חברה לניהול משברים שכולל SLA מחייב לשגרה וחירום?		
28	**ניהול שרשרת אספקה ומיקור חוץ**		מספר ספקים פעילים		
29			מזה: מספר הספקים שחושפים את התאגיד הבנקאי לסיכוני סייבר מהותיים		
30	**ניהול והרשאות משתמשים**	משתמשים פריבילגיים	שיעור המשתמשים שניגשים באמצעות מערכות Privileged Access Management מתוך סך המשתמשים הפריווילגיים האנושיים		
31			שיעור המשתמשים שניגשים באמצעות מערכות Privileged Access Management מתוך סך המשתמשים הפריווילגיים האפליקטיביים		
32		הרשאות משתמשים	מספר משתמשים האנושיים המוגדרים ברשת		
33			מזה: מספר משתמשים בעלי הרשאת אדמין ברשת (Domain Admin)		
34			מזה: מספר משתמשים בעלי הרשאת Local Admin		
35		MFA (Multi-Factor Authentication)	שיעור משתמשים ברשת שמתחברים ב - MFA		
36			שיעור משתמשים פריבילגיים שנדרשים ל-MFA בכל חיבור מכל מקום		
37			שיעור המשתמשים המתחברים מרחוק שנדרשים ל-MFA בקרב צדדים שלישיים		
38			שיעור המשתמשים המתחברים מרחוק שנדרשים ל-MFA בקרב עובדי התאגיד הבנקאי (לרבות עובדים במיקור חוץ)		
39		בקרות משתמשים	האם קיים תהליך אוטומטי לחסימת משתמש שסיים את עבודתו?		
40			האם קיים תהליך אוטומטי לעידכון הרשאות משתמשים בעת מעבר תפקיד ?		
41			האם קיימות בקרות במקרה של פיטורי עובד או עזיבת עובד במיקור חוץ, מעבר לבקרות השגרתיות על המשתמשים בתאגיד הבנקאי ?		
42			האם קיימות בקרות מיוחדות עבור משתמשים פריווילגיים בתאגיד הבנקאי		
43			תדירות בקרת הרשאות למשתמשים פריווילגיים בתאגיד הבנקאי		
44	**אבטחת רשת**	EDR (Endpoint Detection & Response)	שיעור שרתים ברשתות החשופות לאינטרנט שמופעל בהם EDR		
45			שיעור השרתים ברשת הפנימית שמופעל בהם EDR		
46			שיעור תחנות העבודה שמופעל בהם EDR		
47		גיבויים	האם קיים גיבוי למערכות המהותיות והגיבוי נשמר מחוץ לרשת התאגיד הבנקאי או במערכת שאינה ניתנת לשינוי (Immutable)?		
48			האם קיים גיבוי לכל המידע הקריטי והרגיש והגיבוי נשמר מחוץ לרשת התאגיד הבנקאי או במערכת שאינה ניתנת לשינוי (Immutable) ?		
49		תרגול התאוששות רטוב	האם בוצע תרגול התאוששות רטוב מתרחיש אירוע הכולל הצפנת/מחיקת/שיבוש תחנות קצה ?		
50			האם בוצע תרגול התאוששות רטוב מתרחיש אירוע הכולל הצפנת/מחיקת/שיבוש שרתים ?		
51			האם בוצע תרגול התאוששות רטוב מתרחיש אירוע הכולל הצפנת/מחיקת/שיבוש DB ?		
52			האם בוצע תרגול התאוששות רטוב מתרחיש אירוע הכולל הצפנת/מחיקת/שיבוש גיבויים ?		
53		סריקות	באיזו תדירות מבצע התאגיד הבנקאי סבב סריקות אבטחה פנימי של המערכות ?		
54			באיזו תדירות מבצע התאגיד הבנקאי סריקת פגיעויות חיצונית על כלל כתובות ה-IP החיצוניות שלו ?		
55	**ערוצי גישה**		מספר ערוצי הגישה הלא מאובטחים		
56	**מודעות עובדים**		מספר ממוצע של תרגילי Phishing לעובד		
57			מספר מתקפות Phishing שכוונו כנגד עובדי התאגיד הבנקאי במסגרתם עובד פתח צרופה זדונית או לחץ על קישור זדוני		

דיווח מדדי סייבר

לוח 03 - משאבים (שנתי)

					פירוט נוסף	
					01	02
01	תקציב		תקציב הגנת הסייבר ואבטחת המידע	תכנון		
02				ביצוע		
03		מזה:	תקציב השקעות מתוך תקציב הגנת הסייבר ואבטחת המידע	תכנון		
04				ביצוע		
05			תקציב שוטף/ תחזוקה מתוך תקציב הגנת הסייבר ואבטחת המידע	תכנון		
06				ביצוע		
07	כח אדם		מספר משרות מאוישות **בכפיפות** למנהל הגנת הסייבר			
08			מספר משרות מאוישות שעיסוקן ניטור סייבר במוקד הניטור הפנימי			
09			מזה: Tier 1			
10			מזה: Tier 2			
11			מספר משרות מאוישות **בקו ראשון** בתפקידים שעיסוקן בהגנת הסייבר או אבטחת מידע ואינם כפופים למנהל הגנת הסייבר			
12			מספר משרות מאוישות ב**קו שני** בתפקידים שעיסוקן בניהול סיכוני סייבר ואבטחת המידע			
13			מספר משרות מאוישות **בקו שלישי** שעיסוקן בביקורת סייבר ואבטחת המידע			
14			מספר משרות שאינן מאוישות למעלה משלושה חודשים שעיסוקן בהגנת הסייבר ואבטחת המידע			
15			מספר משרות שאינן מאוישות למעלה משלושה חודשים שעיסוקן בניהול סיכוני סייבר ואבטחת מידע בקו שני			
16			מספר משרות שאינן מאוישות למעלה משלושה חודשים שעיסוקן בביקורת סייבר ואבטחת מידע בקו שלישי			
17			האם הוסמך ממלא מקום למנהל הגנת הסייבר?			
18			האם הוסמך ממלא מקום למנהל סיכוני הסייבר?			
19			האם קיימת יתירות כח אדם לפונקציות תפעוליות קריטיות בתחום הגנת הסייבר?			

דיווח מדדי סייבר

לוח 04 - ביקורות פנימיות בנושא הגנת הסייבר ואבטחת המידע (שנתי)

			פירוט נוסף
		01	02
01	מספר ביקורות שתוכננו להתבצע במהלך התקופה המדווחת		
02	מספר ביקורות שתוכננו להתבצע במהלך התקופה המדווחת כהשלמות לשנה קודמת		
03	מספר ימי עבודה שהושקעו לטובת ביקורות חדשות העוסקות בסיכון הסייבר ואבטחת מידע		
04	מספר ימי עבודה שהושקעו לטובת השלמת ביקורות משנה קודמת העוסקות בסיכון הסייבר ואבטחת מידע		
05	מספר הממצאים הפתוחים ברמת חומרה גבוהה ומעלה שחרגו ממסגרת הזמן לתיקון הליקוי		

דיווח מדדי סייבר

לוח 05 - ביקורות פנימיות בנושא הגנת הסייבר ואבטחת מידע כנושא ראשי/ מוביל שפורסמו בתקופת הדיווח (שנתי)

מס' ביקורת	נושא הביקורת	נושאים משניים/ נוספים מבוקרים	ביקורת חדשה/ השלמת ביקורת	ציון הביקורת
01	02	03	04	05

דיווח מדדי סייבר

לוח 06 - הגדרות התאגיד הבנקאי (שנתי)

		הגדרה
		01
01	מניעת שירות (DDOS)	
02	חדירת קוד עוין	
03	ליקוי ברמת חומרה גבוהה (סקרים ומבדקים)	
04	ליקוי ברמת חומרה בינונית (סקרים ומבדקים)	
05	ליקוי ברמת חומרה גבוהה (ביקורת פנימית)	
06	מסגרת הזמן לתיקון ליקוי ברמת חומרה גבוהה (סקרים ומבדקים)	
07	מסגרת הזמן לתיקון ליקוי ברמת חומרה בינונית (סקרים ומבדקים)	
08	מסגרת הזמן לתיקון ליקוי ברמת חומרה גבוהה (ביקורת פנימית)	
09	חולשה גבוהה (טלאי אבטחה או התראה קריטית)	
10	שם מפרט הקשחה מקובל ועדכני	
11	תרגיל Red Team	
12	הגדרת תפקיד Tier1 במוקד הניטור הפנימי	
13	הגדרת תפקיד Tier2 במוקד הניטור הפנימי	
14	ימי עבודה	
15	משרה	
16	מערכות בסיכון גבוה	