הפיקוח על הבנקים

י״ז בחשוון תשפ״ה

18 בנובמבר, 2024

חוזר מס׳ ח- 06 - 2799

לכבוד

התאגידים הבנקאיים

הנדון: ניהול סיכוני טכנולוגיית המידע, אבטחת המידע והגנת הסייבר

(ניהול בנקאי תקין הוראה מס׳ 364)

כללי

1. הסביבה הטכנולוגית בה פועלת המערכת הבנקאית משתנה בקצב מהיר וההסתמכות על מערך טכנולוגיית המידע בתאגיד הבנקאי כמו גם המורכבות של מערך זה, הולכות ומתגברות בשנים האחרונות. תאגידים בנקאיים רבים עוברים תהליך של טרנספורמציה דיגיטלית בכדי להגדיל את יעילותם ובכדי לספק שירותים טובים ומגוונים יותר ללקוחותיהם. תהליך זה מתאפיין באימוץ טכנולוגיות חדשות ובשימוש בטכנולוגיות קיימות בדרכים חדשניות בכדי להציע שירותים פיננסיים חדשים ללקוחותיהם ובכדי להמשיך ולמכן את פעילותם.
2. אולם בעוד שטרנספורמציה דיגיטלית מביאה איתה יתרונות רבים לאקוסיסטם הפיננסי, היא גם חושפת את התאגיד הבנקאי למגוון של סיכוני טכנולוגיית המידע שהינם חלק מהסיכונים התפעוליים העומדים בפני התאגיד הבנקאי, וכוללים בין היתר את סיכוני אבטחת המידע, שהעיקרי והחשוב בהם הוא סיכון הסייבר. בהתאם לכך, מסגרת ניהול סיכונים טכנולוגיים נאותה היא נדבך מרכזי בדרישות היציבותיות של הפיקוח על הבנקים.
3. על מנת להתאים את המסגרת הרגולטורית הנוכחית לניהול סיכונים טכנולוגיים לסביבה הטכנולוגית המשתנה, לאיומים המשתנים ולרגולציה המקובלת בעולם, ומאחר שלסיכוני טכנולוגיית המידע בכללותה קיימים אספקטים רבים משותפים, מחליפה הוראה זו את שלוש ההוראות הבאות המהוות את הבסיס הנוכחי עליו מושתת המסגרת לניהול סיכוני טכנולוגיית המידע: הוראת נ.ב.ת. מס׳ 357 בנושא: ״ניהול טכנולוגיית המידע״ (להלן: ״הוראה 357״), הוראת נ.ב.ת. מס׳ 361 בנושא: ״ניהול הגנת הסייבר״ (להלן: ״הוראה 361״) והוראת נ.ב.ת. מס׳ 363 בנושא: ״ניהול סיכוני סייבר בשרשרת אספקה״ (להלן: ״הוראה 363״).
4. עם זאת, לנוכח התגברות אירועי אבטחת מידע בכלל ומתקפות סייבר בפרט, והמאפיינים הייחודיים שלהם לרבות התחכום העולה שלהם והשפעתם, והמוטיבציה העולה של יריבים לפגוע, בין היתר, במערכות, ברשתות ובפעילות השוטפת של התאגיד הבנקאי, כוללת ההוראה חלקים ייעודיים לאופן ניהול סיכוני אבטחת מידע ובכלל זה סיכון הסייבר.
5. מטרת ההוראה היא ניהול נאות ואפקטיבי של טכנולוגיית המידע תוך צמצום למינימום של האירועים בהם מתממש סיכון טכנולוגי ומתקיימת פגיעה בסודיות, בשלמות או בזמינות של נכסי מידע. ההוראה משמשת כבסיס אחיד לניהול כלל הסיכונים הטכנולוגיים באופן שהוא

ניטרלי לטכנולוגיה, תוך מתן גמישות לתאגיד הבנקאי לנהל את הסיכון בהתאם לטכנולוגיה המתפתחת, לסיכונים המשתנים ובכלל זה בהתאם לאיום הייחוס הפרטני של התאגיד הבנקאי. אשר על כן, הוראה זו בנויה בעיקרה על עקרונות, אולם כוללת גם הנחיות ספציפיות היכן שהפיקוח על הבנקים סבר כי הן נדרשות. גישה מבוססת עקרונות מטילה על התאגידים הבנקאיים אחריות מוגברת ומחייבת אותם לנהוג בזהירות הנדרשת, ולשפר בכל עת את המסגרת הקיימת לניהול הסיכונים ולהתאים אותה לסביבה הטכנולוגית הדינאמית בה הם פועלים וכן אל מול מתאר האיומים המשתנה ללא הרף.

6. אבן הבניין המרכזית בה משתמשת ההוראה הינה נכס המידע של התאגיד הבנקאי. ההחלטה מה ייחשב כנכס מידע נתונה לשיקול דעתו של התאגיד הבנקאי ויישום העקרונות בהוראה מתבסס בעיקרו על קריטיות ורגישות נכס המידע. בהתאם לכך, התאגיד הבנקאי נדרש ליישם את הנחיות ההוראה גם לגבי נכסי מידע המנוהלים באמצעות צד ג', בין אם בחצרות התאגיד הבנקאי ובין אם מחוצה להן.

7. ההוראה תואמת את העקרונות הכלליים לניהול סיכונים המפורטים בהוראת נ.ב.ת. מס' 310 בנושא: "ניהול סיכונים" (להלן: "הוראה 310"), ואת העקרונות לניהול סיכונים תפעוליים המפורטים בהוראת נ.ב.ת. מס' 350 בנושא: "ניהול הסיכון התפעולי" (להלן: "הוראה 350"), וכתובה בהלימה עם הוראות נ.ב.ת. אחרות העוסקות ישירות בתחום הטכנולוגי כמו הוראת נ.ב.ת. מס' 362 בנושא: "מחשוב ענן" (להלן: "הוראה 362"), והוראת נ.ב.ת. מס' 355 בנושא: "המשכיות עסקית" (להלן: "הוראה 355") או נוגעות בו כמו הוראת נ.ב.ת. מס' 359A בנושא: "מיקור חוץ" (להלן: "הוראה 359A").

8. ההוראה תשמש בעתיד בסיס להוראות הפיקוח בנושאים ייעודיים בתחום טכנולוגיית המידע, ככל שתתפרסמנה. כמו כן, על מנת ליצור אחידות בשימוש במונחים שנקבעו בהוראה זו גם במסגרת הרגולטורית הנוכחית בתחום טכנולוגיית המידע, בכוונת הפיקוח על הבנקים לפרסם התאמות להוראות הרלבנטיות, כמו הוראת נ.ב.ת. מס' 366 בנושא: "דיווח על אירועי כשל טכנולוגי וסייבר" (להלן: "הוראה 366").

9. האסדרה לא לוותה בפרסום דו"ח לפי חוק עקרונות האסדרה, התשפ"ב – 2021 (להלן בסעיף זה - "החוק") וזאת לאור הפטור הקבוע בסעיף 34(ג)(4) בהיותה מבוססת בחלקה הגדול על כללים מקובלים במדינות עם שווקים משמעותיים, וכן לאור הקבוע בסעיף 34(ג)(2) לחוק בהיות החלק הנותר מחליף הוראות ניהול בנקאי תקין אחרות ללא שינויים מהותיים.
האסדרה תהיה נתונה לבחינה בדיעבד על פי סעיף 36 לחוק, בתום 10 שנים ממועד כניסתה לתוקף.

10. לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגיד, קבעתי את הוראת ניהול בנקאי תקין הבאה, כמפורט להלן.

מבנה ההוראה

11. ההוראה כוללת שישה עשר פרקים המקובצים תחת שישה חלקים:

11.1. **חלק א': פתיחה** – ובו **פרק א': כללי** – מבוא להוראה, תחולה והגדרות.

11.2. **חלק ב': ממשל תאגידי ומסגרת לניהול סיכונים** – ובו שלושה פרקים:

11.2.1. **פרק ב': ממשל תאגידי** – מפרט את תפקידי הדירקטוריון, ההנהלה הבכירה, מנהל טכנולוגיית המידע, מנהל הגנת הסייבר ואבטחת המידע, הפונקציה לניהול סיכונים, והביקורת הפנימית.

11.2.2. **פרק ג': מסגרת לניהול סיכוני טכנולוגיית המידע (כללי)** – עוסק במבנה ויעדי המסגרת לניהול כלל סיכוני טכנולוגיית המידע ובכלל זה גם סיכוני אבטחת מידע וסייבר, בתהליכים לזיהוי וסיווג של אבני הבניין המרכזיות הנדרשות לצורך ניהול מסגרת זו ובהערכת הסיכונים והפחתתם. זיהוי וסיווג אבני בניין אלו הינו תנאי יסוד ליכולת התאגיד הבנקאי לעמוד בדרישות ההוראה.

11.2.3. **פרק ד': הגורם האנושי** – הדרכה ומודעות משתמשים – עוסק בתוכניות הדרכה עבור טכנולוגיות ומוצרים חדשים, הדרכות לעובדים חדשים, הדרכות תקופתיות לריענון הידע של עובדים קיימים, ותוכניות להדרכה ולהגברת המודעות בנושאי אבטחת מידע.

11.3. **חלק ג': ניהול סיכוני טכנולוגיית המידע** - ובו שני פרקים:

11.3.1. **פרק ה': ניהול טכנולוגיית המידע** – עוסק בניהול נאות של טכנולוגיית המידע ובכלל זה עקרונות לתכנון, יישום, תפעול ובקרה של מערך טכנולוגיית המידע אשר יישומם באופן נאות יפחית את סיכוני טכנולוגיית מידע.

11.3.2. **פרק ו': ניהול פרויקטים וניהול שינויים** – עוסק במסגרת העבודה לניהול פרויקטי טכנולוגיית מידע, עקרונות לניהול רכישה ולניהול פיתוח של מערכת ובכלל זה יישום מערכת שנרכשה, עקרונות לניהול הפיתוח והשירות של ממשקי API ועקרונות לניהול שינויים.

11.4. **חלק ד': ניהול סיכוני אבטחת מידע והגנת הסייבר** - ובו שלושה פרקים:

11.4.1. **פרק ז': אבטחת מידע** – עוסק בהערכת יכולת אבטחת המידע של התאגיד הבנקאי והתאמתה להיקף נכסי המידע של התאגיד הבנקאי ולהיקף הסיכונים לנכסים אלו, בעקרונות העל שיש לבסס עליהם את המסגרת לניהול אבטחת מידע והגנת הסייבר, וכן בנושאים אליהם צריכה להתייחס מדיניות אבטחת המידע והגנת הסייבר.

11.4.2. **פרק ח': יישום בקרות אבטחת מידע** - מפרט את בקרות אבטחת המידע ובכלל זה בקרות הגנת הסייבר שעל התאגיד הבנקאי ליישם, תוך התייחסות להיבטים הבאים: קריטיות ורגישות נכס המידע, פגיעויות ואיומים על נכס המידע, השלב במחזור החיים בו נמצא נכס המידע, מזעור החשיפה לתרחישים חמורים אך סבירים של אירועי אבטחת מידע.

11.4.3. **פרק ט': הערכת אפקטיביות בקרות אבטחת המידע** – עוסק בדרישה להערכה על בסיס מתמשך את הבשלות, אפקטיביות התכנון, היישום והתפעול של אותן בקרות אבטחת מידע שהתאגיד הבנקאי מיישם.

11.5. **חלק ה': ניהול אירועים** - ובו שני פרקים:

11.5.1. **פרק י': ניטור מערך טכנולוגיית המידע** – עוסק במדיניות, בנהלים ובאמצעים שעל התאגיד הבנקאי לקבוע לצורך זיהוי בעיות מתהוות וחריגות (אנומאליות), וזאת במטרה למנוע מהן מלהתפתח לאירועי כשל טכנולוגי או לאירועי אבטחת מידע.

11.5.2. **פרק י"א: ניהול אירועים ובעיות** – עוסק בתהליכים לניהול אירועי כשל טכנולוגי ואירועי אבטחת מידע.

11.6. **חלק ו': שונות** - ובו חמישה פרקים:

11.6.1. **פרק י"ב: דיווח בנושא סיכוני טכנולוגיית המידע וסיכוני אבטחת מידע** – עוסק בדוחות הסדירים המוגשים להנהלה הבכירה ולדירקטוריון בנושאי סיכוני טכנולוגיית המידע וסיכוני אבטחת מידע בהתאם לנדרש בהוראה 350.

11.6.2. **פרק י"ג: ניהול סיכונים מול צדדים שלישיים** – מרכז את ההנחיות הספציפיות שניתנו בהוראה לעניין ניהול סיכונים מול צדדים שלישיים (נותני שירותים לתאגיד הבנקאי וספקים, וכן גורמים אחרים (שאינם לקוחות) שהתאגיד הבנקאי מעניק להם שירות או שהתאגיד הבנקאי משתף איתם את נכסי המידע שלו).

11.6.3. **פרק י"ד: ניהול המשכיות עסקית** – עוסק בעקרונות לבניית תוכנית התאוששות מאסון (DRP) בהתאמה לתוכנית המשכיות עסקית (BCP) של התאגיד הבנקאי, בבדיקה ובתרגול שלה.

11.6.4. **פרק ט"ו: בנק חוץ** – מפרט הנחיות ספציפיות עבור תאגיד שניתן לו רישיון בנק חוץ בהתאם לחוק הבנקאות (רישוי), התשמ"א 1981.

11.6.5. **פרק ט"ז: דיווחים לפיקוח על הבנקים** – מפרט את הדיווחים הנדרשים בנושא ניהול טכנולוגיית המידע אל הפיקוח על הבנקים.

ההוראה

<u>חלק א' – פתיחה</u>

<u>פרק א' – כללי</u>

ניהול נכסי מידע באמצעות צד ג' (סעיף 5 להוראה)

12. הגדרת "צד ג'" בהוראה זו, רחבה יותר מהגדרת "נותן שירות" בהוראה 359A. בהתאם לכך, צד ג' המוגדר גם כ"נותן שירות" בהוראה 359A נדרש לעמוד בדרישות הוראה זו ובדרישות הוראה 359A.

תחולה (סעיף 10 להוראה)

13. תחולת ההוראה תואמת לתחולת הוראת נ.ב.ת. מס' 367 בנושא: "בנקאות בתקשורת" (להלן: "הוראה 367") והוראה 366 (בשינוי מ"סולק" ל"נותן שירותי תשלום בעל חשיבות יציבותית").

הגדרות (סעיף 11 להוראה)

14. ההגדרות נועדו להבהיר את המסגרת ליישום ההוראה ולאפשר שפה אחידה והגדרת ציפיות. כך נקבעו הגדרות ל"סיכון טכנולוגיית המידע", ל"סיכון אבטחת מידע", ול"נכסי מידע" בהם נעשה שימוש לאורך כל ההוראה כמרכיב מרכזי במסגרת הבקרה.

15. "אבטחת מידע" – ההגנה על נכס מידע מפני פעולות בלתי מורשות, בין אם הן מבוצעות בזדון ובין אם בשוגג, במטרה לספק סודיות, שלמות וזמינות.

16. "אירוע כשל טכנולוגי" – הגדרת מונח זה הועברה מהוראה 366. יצויין כי גם פגיעה בסודיות או כשל בשלמות או חוסר התאמה או חוסר זמינות של נכס מידע (למעט פגיעה בסודיות, כשל בשלמות או חוסר זמינות של נכס מידע שסווגו כאירוע אבטחת מידע) מבלי שהפעילות השוטפת של מערך טכנולוגיית המידע או של השירותים הניתנים על ידו נפגעו, תחשב כ"השפעה משבשת על הפעילות התקינה של מערך טכנולוגיית המידע".

17. "הרשאה" – מתן גישה לנכסי מידע עבור המבקש בהתבסס על צרכיו של התאגיד הבנקאי ובכלל זה צרכיו העסקיים, קיום הוראות החוק ודרישות הלקוח, וכן בהתבסס על רמת אבטחת המידע הנדרשת.

18. "זיהוי (בהקשר של זיהוי ואימות גורם המבקש גישה – Identification)" – הגדרת המונח היא בהקשר של זיהוי ואימות גורם המבקש גישה, ולמען הסר ספק היא לא מגדירה זיהוי בהקשרים אחרים כגון הדרישה המופיעה בסעיף 43.2 להוראה בנוגע לזיהוי נכסי המידע.

19. "טכנולוגיית המידע, מערך טכנולוגיית המידע" – בהוראה זו המונח "טכנולוגיית המידע" והמונח "מערך טכנולוגיית המידע" משמשים כמושגים נרדפים.
יצויין כי, מערך טכנולוגיית המידע אינו כולל את עובדי המערך.

20. "מידע רגיש" – כל מידע שסווג כרגיש בהתאם לסיווג הרגישות של התאגיד הבנקאי, הנדרש על פי פרק ג' להוראה, בין אם מידע זה הינו של יחיד, תאגיד או של התאגיד הבנקאי עצמו (לדוגמא: מידע על הפעילות העסקית של התאגיד הבנקאי), ולרבות כל "מידע בעל רגישות מיוחדת" כהגדרתו בתיקון מס' 13 לחוק הגנת הפרטיות, תשמ"א – 1981 (להלן: "חוק הגנת הפרטיות").

21. "מערכת" - תאגיד בנקאי יקבע מה ייחשב על ידו כמערכת בהתאם להגדרה זו, לצורך מילוי דרישות ההוראה הרלבנטיות.

22. "נכסי מידע" – נכסי המידע הם אבני הבניין הבסיסיות בניהול מערך טכנולוגיית המידע של התאגיד הבנקאי לרבות ניהול סיכוני טכנולוגיית המידע.
הגדרת נכסי מידע כוללת גם נתונים שעל גבי תדפיסים, וסעיפי ההוראה יחולו גם על תדפיסים בהתאם לעניין.

23. "סודיות" **(Confidentiality)** – הן בהיבטי אבטחת מידע והן בהיבטי הגנה על פרטיות.

24. "סיכון אבטחת מידע" – הסיכון מורכב מהמונח "איום אבטחת מידע" ומהמונח "פגיעות אבטחת מידע". סיכון אבטחת מידע הינו חלק מסיכון טכנולוגיית המידע ומאופיין בכך שהוא נוצר כתוצאה מפעולות בלתי מורשות של גישה, שימוש, גילוי, שיבוש, שינוי או מחיקה שעלולות לפגוע בסודיות, שלמות או זמינות של נכס מידע.

25. "סיכון טכנולוגיית המידע" – בהתאם להגדרה סיכון זה כולל בתוכו את סיכון אבטחת מידע, וכן סיכונים לפגיעה בסודיות, שלמות וזמינות נכס מידע כתוצאה מאסונות טבע ומפעולות מורשות.

26. "פגיעות אבטחת מידע (Vulnerability)" – חולשה טכנולוגית, תהליכית או אנושית בנכס מידע או בבקרת אבטחת מידע אשר ניתן לנצלה לצורך פגיעה באבטחת המידע.

27. "פרויקט טכנולוגיית המידע" –השימוש במונח "פרויקט טכנולוגיית המידע" בהוראה הוא גנרי למשימות שינוי, החלפה, הוצאה משימוש וכו' בטכנולוגיית המידע. כל תאגיד בנקאי ימלא את דרישות ההוראה ל"פרויקט טכנולוגיית המידע" בהתאמה לטרמינולוגיית ביצוע המשימות הנ"ל הנהוגה אצלו.

חלק ב' – ממשל תאגידי ומסגרת לניהול סיכונים

פרק ב' – ממשל תאגידי

כללי (סעיף 12 להוראה)

28. ממשל תאגידי בתחום טכנולוגיית המידע הוא חלק בלתי נפרד מהממשל התאגידי הכולל של התאגיד הבנקאי ומורכב מתרבות ארגונית, מבנה ארגוני ותהליכים שנועדו להבטיח שמערך טכנולוגיית המידע מקיים את האסטרטגיה והיעדים הארגוניים שלו. היעדים של ממשל תאגידי בתחום טכנולוגיית המידע הינם לוודא כי מערך טכנולוגיית המידע יוצר ערך עסקי לתאגיד הבנקאי וממזער את הסיכונים הכרוכים בשימוש בטכנולוגיה.

29. סעיף זה נועד לוודא שכל הפעילויות הנחוצות לניהול טכנולוגיית המידע ולניהול סיכוני טכנולוגיית המידע (לרבות קבלת החלטות, אישורים, פיקוח ותפעול של אבטחת המידע והגנת הסייבר) הוגדרו והוקצו ליחידים הרלבנטיים, לרבות לדירקטוריון וועדותיו.

אחריות הדירקטוריון לניהול סיכוני טכנולוגיית המידע (סעיף 13 להוראה)

30. סעיף זה בא להדגיש את אחריותו של הדירקטוריון לוודא כי רמת טכנולוגיית המידע, אבטחת המידע של התאגיד הבנקאי והבקרות המיושמות כנגד סיכוני טכנולוגיית מידע אחרים, תואמים לא רק את השינויים המהירים בתחום הטכנולוגיה, אלא גם מתקשרים למטרה האסטרטגית הרחבה יותר והיא, המשך פעילותו הנאות של התאגיד הבנקאי. בנוסף, באמצעות דרישה זו מבקש הפיקוח על הבנקים להגביר את מעורבותו של הדירקטוריון בתחום טכנולוגיית המידע ובאבטחת המידע והגנת הסייבר של התאגיד הבנקאי, ולעודד אותו להשתמש, במידת הצורך, במומחים מתאימים לתחומים אלו.

התווית אסטרטגיית טכנולוגיית המידע (סעיף 14 להוראה)

31. אסטרטגיית טכנולוגיית המידע תגדיר מתווה מקיף המנחה את ניהול הטכנולוגיה בתאגיד הבנקאי ומכיל יעדים ותוכניות ברמת על עבור כל תחומי טכנולוגיית המידע המשפיעים על התאגיד הבנקאי, ולא רק עבור התשתיות. האסטרטגיה מתמקדת באופק של 3 עד 5 שנים ותסייע לוודא שהתכנון הטכנולוגי עקבי ומתואם עם התכנון העסקי של התאגיד הבנקאי.

32. האסטרטגיה נדרשת גם לשקף את הצורך בניהול דינמי של תחום טכנולוגיית המידע בתאגיד הבנקאי, והתאמתו ללא הרף למצב המתפתח. הטכנולוגיות המשתנות במהירות, עשויות להשפיע על פעילות התאגיד הבנקאי, ומה שהספיק והיה נכון בעבר, כבר אינו בהכרח מספיק ורלבנטי כיום.

33. אסטרטגיית טכנולוגיית מידע אפקטיבית תבטיח אספקת שירותים טכנולוגיים המאזנים בין עלויות לבין יעילות, כשבמקביל היא תאפשר לקווי העסקים לעמוד בדרישות התחרותיות של השוק.

34. בהתאם לסעיף 14(ה) להוראה 310, תיאבון הסיכון ינוסח בשפה ברורה ומובנת ויהווה בסיס לקביעת מדיניות ומגבלות הסיכון.

הבנת הדירקטוריון בפעילות ובסיכוני טכנולוגיית המידע וניטור היישום של אסטרטגיית טכנולוגיית המידע (סעיף 17 להוראה)

35. הדירקטוריון נדרש להבין את פעילות טכנולוגיית המידע ברמה מספקת שתאפשר לו למלא את חובותיו ובכלל זה לפקח על אופן ניהול הסיכונים.

36. לנוכח אחריותו בהתאם לסעיף 13 להוראה נדרש הדירקטוריון להחליט לדוגמא על אילו פרויקטי טכנולוגיית מידע מרכזיים הוא מעוניין לקבל דיווח, אילו מדדי ביצוע הוא מעוניין לקבל, ואילו תיעדופים נדרשים להיות מובאים לאישורו.

37. התאגיד הבנקאי נדרש לקשור בין יכולת אבטחת המידע (סעיפים 102-100 להוראה) לבין תפקיד הדירקטוריון לוודא שאבטחת המידע והגנת הסייבר תואמת את היקף האיומים, ושיכולת אבטחת המידע מאפשרת את המשך פעילותו הנאותה של התאגיד הבנקאי. בדרך זו מבקש הפיקוח על הבנקים לחזק את חשיבות אבטחת המידע והגנת הסייבר בתאגיד הבנקאי ואת הצורך לטפל בהשפעתה על התאגיד הבנקאי בצורה רחבה יותר.

מנהל טכנולוגיית המידע (סעיפים 26 – 23 להוראה)

38. מנהל טכנולוגיית המידע אחראי על מערך טכנולוגיית המידע, לרבות התפעול והניהול היומיומי של כלל הפעילויות הטכנולוגיות, אבטחת המידע של סביבת טכנולוגיית המידע וחוסנה התפעולי. מנהל טכנולוגיית המידע אחראי, בין היתר, על הזמינות של הרכיבים המרכיבים את תשתיות התאגיד הבנקאי לרבות חומרה, רשתות, תקשורת, תוכנה ואחסון.

39. מנהל טכנולוגיית המידע בתאגיד הבנקאי לא יוכל לשאת באחריות נוספת, הן בתאגיד הבנקאי והן מחוצה לו, שיש בה כדי להפריע לתפקודו מסיבות שונות לדוגמא: במקרה של ניגודי עניינים או משאבים מוגבלים.

40. אין בהוראה זו דרישה לדיווח על מינוי מנהל טכנולוגיית המידע, שכן מנהל טכנולוגיית המידע נכלל בין כה וכה ברשימת שבעת נושאי המשרה הנוספים בתאגיד הבנקאי שהמפקח על הבנקים נדרש לאשר בהתאם לסעיפים 11א ו – 15ג לפקודת הבנקאות. בהתאם לסעיפים אלו לא יכהן אדם כנושא משרה בתאגיד בנקאי ובסולק, אלא אם כן נמסרה למפקח הודעה, שישים ימים לפני תחילת כהונתו.

מנהלי קווי העסקים (סעיף 27 להוראה)

41. גם למנהלי קווי העסקים, בנוסף למנהל טכנולוגיית המידע ולמנהל הגנת הסייבר ואבטחת המידע קיימת אחריות בתחום טכנולוגיית המידע. לכל בעל תפקיד אחריות בתחומו. כך למשל, בבדיקות הנאותות על צד ג' יבצע מנהל קו העסקים (שלו בין היתר, חלק באפיון המערכות, בתיעדוף הפיתוחים, בווידוא קיום גיבויים ותיעוד תהליכים) בדיקות שהמערכת מספקת את צרכיו העסקיים, בעוד שמנהל אבטחת המידע והגנת הסייבר יבצע בדיקות לוודא שהמערכת עומדת במדיניות אבטחת המידע של התאגיד הבנקאי.

הסעיף מפרט דוגמאות לתחומי אחריות בתחום טכנולוגיית המידע בהם נדרשת חלוקה בין בעלי התפקידים כאמור. מכיוון שלכל תאגיד בנקאי מבנה ותרבות ארגונית ייחודיים, חלוקה זו תבוצע בהתאם למדיניות התאגיד הבנקאי ולתהליכים שייקבעו מכוחה.

42. הסעיף אינו מתייחס לאופן ולמידת העומק בה יבוצעו תפקידי מנהלי קווי העסקים, כך למשל, בביצוע בדיקות נאותות על צד ג' לא קבע הפיקוח על הבנקים מהי רמת הבדיקה שתבוצע, והיא יכולה להיקבע, בין היתר, בהתאם לקריטיות ולרגישות נכס המידע.
ככל שצד ג' הינו גם "נותן שירות" כהגדרתו בהוראה 359A, על התאגיד הבנקאי לבצע את בדיקת הנאותות גם בהתאם לנדרש בסעיפים 21-18 להוראה 359A.

43. ניטור פעילות של צד ג' על ידי מנהלי קווי העסקים יכול להתקיים לדוגמא באופן של קבלת דוח סטטוס פעילות תקופתי תוך השוואה להתחייבויות צד ג' במסגרת החוזה.

תפקידי מנהל הגנת הסייבר ואבטחת המידע (סעיפים 34-28 להוראה)

44. הסעיף מפרט את תפקידי מנהל הגנת הסייבר ואבטחת המידע ואין בו כדי להנחות לגבי אופן והיקף ביצוע תפקידים אלו. כך למשל הסעיף קובע כי, מנהל הגנת הסייבר ואבטחת המידע אחראי, בין היתר, על ביצוע בדיקות נאותות בהיבטי אבטחת מידע והגנת הסייבר על צדדים שלישיים. עם זאת, הסעיף אינו מתייחס לרמה בה תבוצע בדיקת הנאותות והיא יכולה להתבצע בהתאמה להשפעות האפשריות של אירוע אבטחת מידע על נכסי המידע אשר יש לו גישה אליהם (ראה סעיף 102.1 להוראה).
ככל שצד ג' הינו גם "נותן שירות" כהגדרתו בהוראה 359A, על התאגיד הבנקאי לבצע את בדיקת הנאותות גם בהתאם לנדרש בסעיפים 21-18 להוראה 359A.

45. מנהל הגנת הסייבר ואבטחת המידע נדרש להתעדכן ביוזמות עסקיות חדשות על מנת לזהות סיכוני אבטחת מידע ביוזמות אלו, וכן לקבוע דרכים להפחתתם. לצורך כך יכול מנהל הגנת הסייבר ואבטחת המידע לקיים דו שיח עם מנהלי קווי העסקים וכן ללמוד על סיכונים אלו ממקורות אחרים, לדוגמא, גופים אחרים שיישמו יוזמות אלו וגורמים אחרים בתעשייה.
בדומה לכך, על מנהל הגנת הסייבר ואבטחת המידע להתעדכן גם בתהליכי זרימת המידע, הסיכונים למידע בתהליכים אלו, ואמצעי אבטחת המידע והגנת הסייבר הנדרשים, וזאת באמצעות דו שיח עם מנהלי קווי העסקים, גורמים אחרים בארגון, ומקורות מחוצה לו.

46. דוגמא לתיאום וקישור מול גורמים חיצוניים בנושאי הגנת הסייבר - השתתפות בפורומים ובקבוצות שיתוף הידע של ה – CERT הלאומי ובתוכניות אחרות לשיתופי פעולה בהן איומי אבטחת מידע וסייבר ינוטרו, ישותפו, ויידונו.
שיתוף המידע ומודיעין לצורך הגנתי מול גורמים חיצוניים יתבצע בכפוף לדין ובכלל זה בהתאם להנחיות המפקח על הבנקים (ראה סעיף 111.4 להוראה).

47. קיים הבדל בין "תכלול ניהול אירוע" לבין "ניהול אירוע". תחת הדרישה "לתכלל את ניהול האירוע" נדרש מנהל הגנת הסייבר ואבטחת המידע לוודא שכל הגורמים הרלוונטיים נמצאים "סביב השולחן" ושהתאגיד הבנקאי פועל לפי תכניות המגירה הקיימות, ובנוסף הוא נדרש למלא את תפקידו כגורם מייעץ להנהלה ולדירקטוריון בסוגיות שונות שיעלו וכדו'. תאגיד בנקאי יכול להחליט, בהתאם למאפייני האירוע, לגבי זהות הגורם האחראי לניהול האירוע. עם זאת, את התכלול נדרש לבצע מנהל הגנת הסייבר ואבטחת המידע.

תוכנית העבודה של הביקורת הפנימית (סעיף 37 להוראה)

48. הביקורת הפנימית היא כלי חשוב באמצעותו יכול הדירקטוריון לוודא כי הבקרות הטכנולוגיות מיושמות כך שהן מפחיתות את הסיכון ופועלות באופן שבו הנהלת התאגיד הבנקאי תכננה. כך לדוגמא, יכול הדירקטוריון באמצעות כלי זה, לוודא כי אבטחת המידע נשמרת בתאגיד הבנקאי. לשם כך, על הביקורת הפנימית להתייחס להיבטי טכנולוגיית המידע השונים ובכלל זה היבטי אבטחת המידע במסגרת תוכנית העבודה שלה. כמובן שבמקרים מסוימים, למשל כאשר אין לביקורת הפנימית את הידע והמומחיות המתאימים או כאשר הנושא הנבדק מנוהל אצל צד ג', הרי שעל מנת להשלים את התמונה שמספקת הביקורת הפנימית, יכול הדירקטוריון לבחור להסתמך בנוסף, על חוות דעת מומחים או על אמצעים אחרים לפי בחירתו.

הביקורת הפנימית תמפה את כלל הפעילות של מערך טכנולוגיית המידע, הממשל התאגידי, הפונקציות והתהליכים בתחום טכנולוגיית המידע לרבות אלו שבתחום אבטחת המידע. מיפוי זה ישמש כבסיס ממנו תיגזר תוכנית העבודה של הביקורת הפנימית.

הסתמכות הביקורת הפנימית על עבודה המבוצעת על ידי גורם אחר (סעיף 38 להוראה)

49. הסעיף מתייחס למקרים בהם הביקורת הפנימית מסתמכת על גורמים מחוץ לביקורת הפנימית על מנת לבצע את מחויבויותיה. במקרים כאלו על הביקורת הפנימית להעריך את היקף ואיכות הבדיקה שנעשתה, על מנת לקבוע האם ובאיזו מידה ניתן להסתמך עליה. להלן מקרים אלו:

49.1. הסתמכות הביקורת הפנימית על עבודה המבוצעת על ידי גורמים אחרים בתאגיד הבנקאי. לדוגמא: סקירת התכנון והאפקטיביות של בקרות אבטחת מידע שיזם מנהל הגנת הסייבר ואבטחת המידע.

49.2. שימוש של הביקורת הפנימית במיקור חוץ לצורך ביצוע של הפעילויות המוטלות עליה.

49.3. הסתמכות של הביקורת הפנימית על בדיקות שמסופקות לה על ידי צד ג' המבצע פעילות עבור התאגיד הבנקאי .

<u>פרק ג' - מסגרת לניהול סיכוני טכנולוגיית המידע (כללי)</u>

כללי

50. בהמשך לסעיף 9 להוראה, המסגרת לניהול סיכוני טכנולוגיית המידע תהיה תואמת למסגרת ניהול הסיכונים הנדרשת בהוראה 310.

פרק זה משמש כמעטפת לניהול כלל הסיכון הטכנולוגי, ובכלל זה גם לסיכוני אבטחת המידע הניצבים בפני התאגיד הבנקאי. עיקרו של הפרק בחובת התאגיד הבנקאי לקבוע מתודולוגיה לזיהוי נכסי מידע, פעילויות עסקיות ותהליכים תומכים, ולאופן מדידת הסיכון והפחתתו. כמו כן עוסק הפרק בדרישה לחלוקת האחריות לניהול הסיכון, לרבות בחלוקה בין שלושת קווי ההגנה, תפקידי מפתח, וקווי דיווח.

ניהול סיכוני טכנולוגיית המידע (סעיף 41 להוראה)

51. הסעיף תואם את סדר הפעולות בניהול הסיכון: זיהוי, הערכה, בקרה, ניטור ודיווח, כאשר סעיף 41.7 להוראה מפרט את הגורמים להתחלת מחזור חדש לעדכון ניהול הסיכון.

52. ייתכנו אירועי כשל טכנולוגי או אירועי אבטחת מידע שיוגדרו על ידי התאגיד הבנקאי כמשמעותיים לצרכי זיהוי והערכה של סיכוני טכנולוגיית המידע חדשים, אולם הם לא יהיו

חייבים בדיווח לפיקוח על הבנקים על פי הקריטריונים לדיווח המפורטים בהוראה 366. כמו כן, אירוע כשל טכנולוגי משמעותי ואירוע אבטחת מידע משמעותי בסעיף זה, אינם בהכרח האירועים נשוא סעיף 146.6 להוראה זו.

זיהוי של פעילויות, תהליכים ונכסי מידע וסיווגם (סעיף 43 להוראה)

53. לעניין רמת פירוט המיפוי הנדרשת – ראה סעיף 44 להוראה.

54. למען הסר ספק, זיהוי כל הפעילויות העסקיות בהתאם לסעיף זה יכול לשמש גם לצורך מיפוי התהליכים והשירותים החיוניים על פי הוראה 355.

55. תאגיד בנקאי יכול לקבל ערך מוסף מבחינה של קשרים בין נכסי מידע, לרבות זיהוי נכסי מידע שאמנם אינם מסווגים ברמת קריטיות או רגישות גבוהה, אך ניתן להשתמש בהם לצורך פגיעה באבטחת המידע של נכסי מידע המסווגים ברמת קריטיות או רגישות גבוהה או שאירוע כשל טכנולוגי הפוגע בהם, יכול להשפיע על נכסי מידע המסווגים ברמת קריטיות או רגישות גבוהה.

56. למותר לציין כי כתנאי מקדים למיפוי של כל נכסי המידע המנוהלים באמצעות צד ג' כפי שנדרש בהוראה, על התאגיד הבנקאי למפות את כל "צד ג'" כהגדרתם בהוראה זו.

57. על מנת לנהל את סיכון טכנולוגיית המידע באופן אפקטיבי, נדרש התאגיד הבנקאי לזיהוי והבנה מלאים של נכסי המידע שלו, ושל השפעת פגיעה אפשרית באבטחת המידע שלהם או של כשל טכנולוגי בהם. בהתאם לכך, כל נכסי המידע של התאגיד הבנקאי, לרבות תשתיות, מערכות משניות כמו מערכות לבקרת גישה פיזית, כמו גם נכסי מידע המנוהלים באמצעות צד ג', נדרשים להיות מזוהים ומסווגים בהתאם לרמת קריטיות ורגישות.

58. על מנת לפשט את תהליך הזיהוי של נכסי המידע ומיפוי הקשרים ביניהם, יכול התאגיד הבנקאי לעשות שימוש במערכות ניהול מאגרים מתאימות דוגמת Configuration Management DataBase (CMDB) שהינן מערכות המנהלות מידע בנוגע לנכסי המידע של הארגון, לרבות הקשרים ביניהם.

59. קיימת חשיבות רבה לשמירה על עדכניות תוצר המיפוי והסיווג של הפעילויות העסקיות, התהליכים התומכים ונכסי המידע במונחים של קריטיות ורגישות. תוצר לא עדכני, עלול להקשות ואף לפגוע בתהליכי ניהול סיכוני טכנולוגיית המידע, ובכלל זה בתהליכי ניהול סיכוני אבטחת המידע של התאגיד הבנקאי. בהתאם לכך, התאגיד הבנקאי נדרש לבצע תהליך:

- לזיהוי המקרים בהם נדרש שינוי בסיווג של נכסי המידע, של הפעילויות העסקיות או של התהליכים התומכים.
- לסיווג נכסי מידע, פעילויות עסקיות או תהליכים תומכים חדשים.

תהליך זה נדרש להתבצע בכל אחד מהמקרים הבאים:

- לפחות אחת לשנה - התהליך השנתי ישמש כבקרה לעדכניות השוטפת של תוצרי המיפוי והסיווג כאמור לעיל, ולזיהוי טעויות וכשלים אחרים בתוצרים, ככל שיהיו כאלו.
- כאשר נעשים שינויים מהותיים בנכסי מידע, בפעילויות עסקיות ובתהליכים תומכים - לשינויים מהותיים כאמור יכולות להיות השפעות על סיווג נכסי מידע, פעילויות עסקיות, ותהליכים תומכים שאינם בהכרח אלה בהם בוצעו השינויים. תהליך כאמור, עשוי לזהות השפעות אלו.
- כאשר נעשים שינויים בסביבה העסקית בה התאגיד הבנקאי פועל.

מתודולוגיה לזיהוי וסיווג הפעילויות העסקיות, התהליכים התומכים ונכסי המידע (סעיף 44 להוראה)

60. רמת פירוט המיפוי של נכסי המידע תקבע על ידי התאגיד הבנקאי באופן שהמיפוי יאפשר את קביעת אופי וחוזקת הבקרות הנדרשות על מנת להגן על נכסים אלו. כך למשל, ניתן לראות במערכת כאוסף של הרכיבים המרכיבים אותה (אפליקציות, בסיסי נתונים, מערכת הפעלה, תווכה, נתונים), ולהתייחס אליה כנכס מידע אחד לצרכי מיפוי, ולחילופין ניתן להתייחס אל כל רכיב מהרכיבים המרכיבים אותה כאל נכס מידע בפני עצמו.

61. סיווג במונחי קריטיות ורגישות יתחשב, בין היתר, בהשפעת פגיעה אפשרית באבטחת מידע על נכס המידע או בהשפעת כשל טכנולוגי על נכס המידע. מאחר והמונח קריטיות מוגדר בהוראה כ"ההשפעה הפוטנציאלית של העדר זמינות", הרי שסיווג נכס המידע מושפע גם ממידת חשיבותו לקיום התהליכים והשירותים החיוניים המוגדרים בתוכנית ההמשכיות העסקית של התאגיד הבנקאי.

רמת הקריטיות ורמת הרגישות בהן מסווג כל נכס מידע, אינן חייבות להיות זהות.

"בעל נכס המידע" (סעיף 45 להוראה)

62. בעל נכס המידע יהיה בדרך כלל עובד בפונקציה העסקית אשר נדרש לנכס המידע יותר משאר הגורמים העושים בו שימוש. תחומי האחריות של בעל נכס המידע יוגדרו, והוא יידרש לתת דיווח, בין היתר, לגבי אבטחת המידע של נכס המידע.

יובהר כי גם אם מאגר מידע כהגדרתו בחוק הגנת הפרטיות מוגדר על ידי התאגיד הבנקאי כנכס מידע, אין חובה על התאגיד הבנקאי לקבוע כי בעל נכס המידע ישמש גם כמנהל המאגר כהגדרתו בחוק הגנת הפרטיות, ולהיפך.

ביצוע הערכת סיכונים על בסיס מתמשך (סעיף 46 להוראה)

63. כאמור בסעיף 9 להוראה, תהליך ניהול סיכון טכנולוגיית המידע ובכלל זה שלב זיהוי והערכת הסיכון, נדרש להיות תואם לעקרונות לניהול הסיכון התפעולי המפורטים בהוראה 350 ולעקרונות ניהול סיכונים בכלל המפורטים בהוראה 310. בנוסף, בתהליך זיהוי והערכת סיכוני טכנולוגיית המידע, יינתנו דגשים נוספים המפורטים בסעיף זה.

<u>פרק ד' - הגורם האנושי</u>

הגדרת "עובדים" (סעיף 50 להוראה)

64. למען הסר ספק, המונח "עובדים" בפרק זה כולל עובדים חיצוניים המנוהלים על ידי התאגיד הבנקאי.

רציפות בתפקידי מפתח במערך טכנולוגיית המידע (סעיף 52 להוראה)

65. מטרת השמירה על רציפות בתפקידי מפתח היא לספק מעבר חלק במקרה של תחלופה בתפקידי ניהול או תפעול חיוניים.

תוכנית להדרכה ולהגברת המודעות בנושאי אבטחת מידע (סעיף 53 להוראה)

66. על מנת להפחית טעויות אנוש, גניבות, הונאות, שימוש לא ראוי בנכס מידע או הפסדים, יפתח התאגיד הבנקאי תוכנית להדרכה ולהגברת המודעות בנושאי אבטחת מידע והגנת הפרטיות אותה יעברו מידי תקופה ולפחות אחת לשנה, כל העובדים לרבות עובדים חיצוניים וזמניים.

תוכנית ההדרכה והגברת המודעות בנושאי אבטחת מידע והגנת הפרטיות יכולה לכלול, בין היתר, התייחסות לנושאים הבאים: שימוש בנכסי מידע למטרות אישיות לעומת מטרות עבודה; שימוש בדוא"ל ובאינטרנט (לרבות רשתות חברתיות) והגנה מפני נוזקה; אבטחה פיזית לרבות על תדפיסים בבית העובד; גישה מרחוק (ובפרט מסביבות שאינן מוגנות) ושימוש במכשירים ניידים; מודעות להתקפות נפוצות המכוונות לעובדי ומתקני התאגיד הבנקאי (לדוגמא: הנדסה חברתית (Social engineering, Tailgating); בקרות גישה לרבות כללים לסיסמאות ודרישות אימות אחרות; פיתוח על ידי משתמשי קצה; ציפיות מהעובדים כאשר מתאפשר שימוש במכשיר העובד (Bring Your Own Device); טיפול במידע ונתונים רגישים; דיווח על אירועי אבטחת מידע ועל חשד לאירוע אבטחת המידע.

חלק ג' - ניהול סיכוני טכנולוגיית המידע

כללי

67. חלק זה בהוראה עוסק בניהול טכנולוגיית המידע ובסיכונים הנלווים לכך (ראה הגדרת "סיכון טכנולוגיית המידע" בסעיף 11 להוראה). חלק ד' בהוראה עוסק בהיבטים הייחודיים לסיכוני אבטחת מידע ובכלל זה סיכוני סייבר.

פרק ה' - ניהול טכנולוגיית המידע

מדיניות ניהול טכנולוגיית המידע (סעיף 54 להוראה)

68. ניהול אפקטיבי של טכנולוגיית המידע הוא חלק מהותי מניהול סיכוני טכנולוגיית המידע. העקרונות והפרקטיקות המרכיבים את תהליכי התכנון, היישום והתפעול המפורטים בפרק זה להלן, ואשר יבואו לידי ביטוי במדיניות טכנולוגיית המידע, חשובים ליצירת סביבה טכנולוגית אפקטיבית. הם תומכים בקווי העסקים של התאגיד הבנקאי ובאספקת מוצרים ושירותים לצורך עמידה ביעדי האסטרטגיה העסקית. תיאום ופיקוח לא מספקים על תהליכי התכנון, היישום והתפעול, עלולים לגרום להתממשותם של מגוון סיכונים כמו: סיכון אשראי, סיכון נזילות, סיכון תפעולי וסיכון ציות.

מאפייני מערכות המידע (סעיף 55 להוראה)

69. מערכות מידע שונות מספקות להנהלה ולדירקטוריון מידע הנחוץ לניהול התאגיד הבנקאי באופן אפקטיבי. הנהלת התאגיד הבנקאי והדירקטוריון עושים שימוש במערכות מידע לצרכי הערכת הביצועים העסקיים של התאגיד הבנקאי, דיווח על הסיכונים והאתגרים העומדים בפניו, ובעיקר לצורך סיוע בניהול העסקי שלו.

70. מערכות המידע מספקות נתונים למקבלי ההחלטות בזמן שיאפשר להם לבצע את תפקידם, תומכות ומשפרות את תהליכי קבלת ההחלטות, ומשפרות את ביצועי העבודה בתאגיד הבנקאי.

71. בדירקטוריון ובדרגי ההנהלה הבכירים, דיווחי מערכות המידע מספקים נתונים ומידע המסייעים לקבלת החלטות אסטרטגיות. בשאר הדרגים, דיווחי מערכות המידע מאפשרות

להנהלה לנטר את פעילויות התאגיד הבנקאי ולהפיץ מידע לעובדים, ללקוחות, ולחברי ההנהלה.

72. השיפור בטכנולוגיה הביא עימו גידול בנפח הנתונים והמידע אשר זמינים להנהלה ולדירקטוריון לצורך תכנון וקבלת החלטות. מאחר והקלט של מערכות המידע יכול להיות מוזן ידנית או מתוך מידע המופק ממספר רב של מערכות פיננסיות, התאגיד הבנקאי נדרש ליישם נהלי בקרה מתאימים על מנת לוודא שהנתונים והמידע המופקים ממערכות המידע הינם נכונים ורלבנטיים.

73. מאחר ודיווחי מערכות המידע יכולים להגיע ממספר פלטפורמות טכנולוגיות, הבקרות צריכות להיות מתוכננות כך שהשלמות של המידע וסביבת העיבוד תשמר.
בהתאם לכך, על מנת שדיווחי מערכות המידע ישמשו ככלי אפקטיבי לדירקטוריון, להנהלה ולעובדים, עליהם לעמוד בחמישה אלמנטים חיוניים:

- מהירות – על מנת לבצע תהליך מהיר של קבלת החלטות, מערכות המידע של התאגיד הבנקאי צריכות להיות מסוגלות לספק ולהפיץ מידע עדכני לגורמים הרלבנטיים.
- דיוק – מערכות המידע צריכות לספק נתונים מדויקים, לשם כך יכול התאגיד הבנקאי להסתייע בבקרות פנימיות מיכוניות וידניות במערכות המידע על מנת לוודא את תקפות הנתונים.
- עקביות – על מנת שניתן יהיה להסתמך על המידע, הנתונים צריכים להיות מעובדים בצורה אחידה. שימוש במגוון שיטות איסוף מידע ובמגוון שיטות דיווח באופן שאינו עקבי, עלול לפגוע במידע ובניתוח המגמות.
- שלמות – הדיווחים צריכים לכלול את המידע הנחוץ למקבלי ההחלטות ללא פירוט יתר.
- רלבנטיות – מערכות המידע צריכות לספק מידע עדכני, ישים, ושניתן לפעול על פיו.

חוסן תפעולי (סעיף 56 להוראה)

74. מערך טכנולוגיית המידע מאובטח ובעל חוסן הכולל: תהליכי ארכיטקטורה, בניית תשתית טכנולוגית, ותפעול מתאימים, הינו חיוני לאספקה של הפעולות החיוניות על ידי התאגיד הבנקאי. בכדי לחזק את החוסן התפעולי של התאגיד הבנקאי, נדרש התאגיד הבנקאי לשלב תהליכים אלו בתוך תוכנית ההמשכיות העסקית שלו, כך שיסייעו בהפחתת איומים, במתן תגובה לשיבושים ובהתאוששות מהם, ובהפקת לקחים.

75. חוסנם התפעולי של התהליכים כאמור (תכנון ארכיטקטורה, בניית תשתית טכנולוגית ותפעול), הינו הרבה מעבר ליכולות התאוששות גרידא. חוסן תפעולי מושג על ידי נקיטת צעדים יזומים לצורך שמירה על סודיות, שלמות וזמינות והפחתת הסיכון לשיבוש, בעת תכנון מערך טכנולוגית מידע מתאים (לרבות מערכות לגיבוי והתאוששות), בחירה מתאימה של תשתית טכנולוגית, ופריסת המערך בפועל. תאגיד בנקאי נדרש לתכנן, ליישם ולתפעל את מערך טכנולוגיית המידע ואת התהליכים שהוא מפעיל, כך שיספקו חוסן תפעולי עבור פעילויות עסקיות חיוניות.

76. על מנת לשלב באופן נאות היבטים של חוסן תפעולי, בתהליכי תכנון הארכיטקטורה ועדכונה וביישום התשתית הטכנולוגית, ידאג התאגיד הבנקאי לשלב היבטים אלו בתהליך ניהול הפרויקטים שקבע לעצמו. שילוב היבטים אלו בתהליכים פורמליים המונהגים בתאגיד הבנקאי, יכול לסייע בתהליכי קבלת החלטות אסטרטגיות ובהפניית משאבים לחיזוק החוסן

התפעולי של קווי הליבה העסקיים (קווי העסקים של התאגיד הבנקאי, לרבות פעילויות, שירותים ופונקציות קשורים, שלפי הערכתו של התאגיד הבנקאי, כשל שיתרחש בהם יסתיים בהפסד משמעותי של הכנסה או רווח).

ארכיטקטורה (סעיף 57 להוראה)

77. תכנון ועיצוב של ארכיטקטורת טכנולוגיית מידע אפקטיבית יסייעו להנהלה בבניית תשתית טכנולוגית התואמת את המטרות, האסטרטגיות והיעדים העסקיים של התאגיד הבנקאי.

78. כאמור בסעיף 56 להוראה, תאגיד בנקאי נדרש להתייחס להיבטים של חוסן תפעולי (לדוגמא: יתירות, רב שכבתיות, ומערכות גיבוי איתנות) ובכלל זה היבטי אבטחת מידע והגנת הסייבר, כבר בתחילת תהליך תכנון הארכיטקטורה.

79. קיים מגוון של מתודולוגיות לצורך פיתוח תוכנית ארכיטקטורת טכנולוגיית מידע. העיקרון המנחה בכולן הוא שחלק גדול מהדרישות הטכנולוגיות הינן תוצאה של תהליך מתוכנן מראש שמתחיל בדרישות העסקיות ומסתיים בפתרונות טכנולוגיים אשר תואמים את המדיניות והנהלים שאושרו על ידי ההנהלה הבכירה והדירקטוריון. תוכנית ארכיטקטורת טכנולוגיית מידע אפקטיבית עשוייה לסייע, בין היתר, בתחומים הבאים:

- שיפור השימוש בטכנולוגיית מידע לצורך יצירת יכולת הסתגלות עסקית לתאגיד הבנקאי.
- יצירת שותפות קרובה בין קווי העסקים לבין היחידות הארגוניות האחראיות על טכנולוגיית המידע.
- מיקוד משופר במטרות התאגיד הבנקאי.
- הפחתת מספר מערכות מושבתות.
- הפחתת מורכבותן של מערכות.
- שיפור הזמישות (Agility) של טכנולוגיית המידע.
- התאמה טובה יותר בין מה שמספק מערך טכנולוגיית המידע לבין הדרישות העסקיות.
- וידוא שכל התוכנות, לרבות מערכות ההפעלה הינן עדכניות ושירותי התמיכה בהן אינם עתידים להסתיים.

80. נקודות עיקריות שמומלץ להתחשב בהן כאשר מפתחים תוכנית ארכיטקטורת טכנולוגיית מידע כוללות, בין היתר, אבטחת מידע והגנת הסייבר, עמידות עסקית, ניהול נתונים, קישוריות לגורמים מחוץ לתאגיד הבנקאי, והתאמה אל מטרות ויעדי התאגיד הבנקאי. על מנת ליישם באופן אפקטיבי את התוכנית, התאגיד הבנקאי צריך לנתח את הסיכונים ואת ההשפעה הפוטנציאלית של האיומים על כל פעילויות התאגיד הבנקאי. תוכנית מקיפה המבוססת על פרקטיקות נאותות יכולה לסייע לתאגיד הבנקאי לפתח תהליכים לניהול סוגיות שונות הקשורות לטכנולוגיית מידע, ולזהות, למדוד, וליישם בקרות כנגד סיכוני טכנולוגיית המידע השונים.

תשתית טכנולוגית (סעיף 58 להוראה)

81. להלן דוגמאות ליישום בקרות תשתית טכנולוגית:

81.1. חומרה –

81.1.1. ניהול מצבת עדכנית של כל רכיבי החומרה בתאגיד הבנקאי אשר תסייע לתאגיד הבנקאי להגן עליהם, לנהל סיכוני אבטחת מידע, להגיב על אירועים ולהתאושש מהם. לשם כך תאגיד בנקאי יכול להסתייע בכלים ממוכנים מתאימים.

81.1.2. תהליך לזיהוי נכסי מידע שאינם מורשים להתחבר לרשת והסדרת הטיפול בהם (הסרה, בידוד, או הוספה שלהם למצבת העדכנית).

81.2. רשתות ותקשורת –

81.2.1. תהליך המתעד ומתחזק מצבת עדכנית של חומרה ותוכנה המרכיבות את הרשתות והתקשורת של התאגיד הבנקאי וכן של הקונפיגורציה של הרשת, לרבות תהליך לסקירה ולניהול שינויים ברשתות ובתקשורת.

81.2.2. תהליך המוודא את קיומה של יתירות (redundancy) לתשתית התקשורת.

81.2.3. תהליך המוודא את עמידת תשתית התקשורת של התאגיד הבנקאי בנתוני תעבורת הרשת הנוכחית והצפויה.

81.2.4. אבטחה פיזית של ציוד התקשורת והגבלה וניטור של הגישה אליו באמצעות קביעת מדיניות ונהלים מתאימים.

81.3. תוכנה –

81.3.1. תהליך לאיתור ולניטור של התוכנות בתאגיד הבנקאי, בין אם הן מבוססות רשת ובין אם הן נמצאות בתחנת העבודה של העובד.

81.3.2. שימוש בכלים לניהול מצבת התוכנות בתאגיד הבנקאי.

81.3.3. ניידות (Portability) – תכונה המיוחסת לתוכנה אשר יכולה לפעול במינימום שינויים, על גבי מערכות הפעלה השונות ממערכת ההפעלה עבורה היא נוצרה.

82. התשתית הטכנולוגית תתמוך בחוסן תפעולי בהתאם לקריטיות של נכס המידע עבור הפעילויות החיוניות של התאגיד הבנקאי. כך לדוגמא, תאגיד בנקאי יבחר בין יתירות שרתים, אתר חלופי או שירות חלופי, על מנת לספק רמה נאותה של חוסן תפעולי בהתאם לקריטיות של נכס המידע.

עקרונות לניהול התפעול (סעיף 59 להוראה)

83. תהליך התפעול הוא ביצוע של פעילויות המורכבות משיטות, עקרונות, תהליכים, נהלים ושירותים התומכים בפעילותו העסקית של התאגיד הבנקאי. הסביבה התפעולית כוללת את המערכות והמתקנים שהתאגיד הבנקאי משתמש בהם כדי להפעיל את התהליכים העסקיים והתפעוליים שלו. הסביבה התפעולית מבצעת תהליכי עיבוד שוטפים ותומכת - בפונקציות שונות בתאגיד הבנקאי, באספקת שירותים ובניהולם, ובתהליכי בקרה - לצורך השגת יעדיו של התאגיד הבנקאי. כחלק ממסגרת העבודה לניהול התפעול של מערך טכנולוגיית המידע ובגלל הצורך להטמיע בה היבטי חוסן תפעולי, תאגיד בנקאי יישם בסביבה התפעולית תהליכים ובקרות מארבע קבוצות מרכזיות: בקרות תפעוליות, תהליכים טכנולוגיים תפעוליים, תהליכי שירות ותמיכה, תהליכי ניטור והערכה.

בקרות תפעוליות (סעיף 60 להוראה)

84. בקרות תפעול הן כל הנהלים והמנגנונים היומיומיים אשר נועדו להגן על המערכות והתוכנות התפעוליות של התאגיד הבנקאי. בקרות התפעול משפיעות על סביבת המערכות וסביבת התוכנה. מכיוון שסביבות המערכות והתוכנה הן היסודות עליהם מושתתים התהליכים העסקיים של התאגיד הבנקאי, הנהלת התאגיד הבנקאי צריכה להגדיר תהליכים וליישם בקרות כדי להגן על סביבות אלו. בקרות אלו כוללות, בין היתר, בקרות שימוש פיזיות ולוגיות במתקני התאגיד הבנקאי, בקרות לניהול זהויות וניהול גישה לנכסי מידע, בקרות על הגורם האנושי כמו: תהליכי מיון קפדניים שיוודאו את התאמת העובד לתפקיד, הגדרה מסודרת של תפקידים ותחומי אחריות, יישום רוטציה בתפקידים שונים, הפרדת תפקידים נאותה, יישום עיקרון ארבע עיניים ובקרות לשימוש בציוד פרטי של העובד. פירוט של חלק מהבקרות הנכללות תחת קבוצה זו מופיע בפרק ח' להוראה "יישום בקרות אבטחת מידע".

תהליכי תחזוקה (סעיף 61.1 להוראה)

85. תחזוקה מונעת מפחיתה את אירועי הכשל של ציוד ויכולה לאבחן בעיות לפני התרחשותן. תאגיד בנקאי נדרש ליישם תהליכי תחזוקה שונים למניעת כשל כאמור לדוגמא: סקירה של דוח תקופתי הכולל נתונים כמו: תדירות וסוג הבעיות שהתגלו מתוך ה - Activity Log של נכס המידע, יכולה לסייע בזיהוי בעיות פוטנציאליות שדורשות החלפת מערכת, או החלפת ספק, או הגדלה של קיבולת נכס המידע וכד'.

הפסקת תמיכה (סעיף 61.3 להוראה)

86. ניהול נאות של מחזור החיים של נכס המידע כולל, בין היתר, תמיכה שוטפת בו וצמצום הפגיעויות שלו. סיכונים טכנולוגיים שונים לרבות חשיפות אבטחת מידע יכולים לנבוע מחומרה או תוכנה מיושנת או מתמיכה מוגבלת או העדר תמיכה בכלל, בין אם מדובר בתמיכה של צד ג' ובין אם מדובר בתמיכה של גורם מתוך התאגיד הבנקאי עצמו (In-house). טכנולוגיה שקרובה לסיום מחזור החיים שלה (לא מבוצעות בה השקעות חדשות), שהתמיכה בה הופסקה או שנמצאת בתקופה שלפני סיום התמיכה בה, הינה בדרך כלל פחות מאובטחת, ולא ניתן לעדכנה מפני איומים חדשים בזמן סביר, אם בכלל.

כאשר קיימים הסדרי תמיכה לתקופה שמעבר למועד סוף התמיכה הרשמית בנכס המידע (להלן: "הסדרי תמיכה מורחבים"), חשוב שלתאגיד הבנקאי תהיה הבנה ברורה של אופי אותם ההסדרים והאפקטיביות שלהם. כמו כן, בעוד שהסדרי תמיכה מורחבים או כאלו אשר ייעודיים לתאגיד הבנקאי עצמו יכולים למזער סיכונים באופן חלקי, הרי שהם בדרך כלל יקרים, ויכולים לתת תחושה מוטעית של פתרון לרבות תחושה מוטעית של אבטחת מידע או חמור מכך לדחות את הטיפול בטכנולוגיה המתיישנת. יתרה מכך, הסכמי תמיכה מסוג זה בדרך כלל מספקים טלאים לפגיעויות קריטיות בלבד, ונותרים כבולים למגבלות הטכנולוגיה המתיישנת.

ניהול טלאים (Patches) (סעיף 61.4 להוראה)

87. ניהול טלאים הינו תהליך שבו מזוהים תיקונים נדרשים במערכות הפעלה ובקוד מערכת, התיקונים מאומתים ולבסוף מיושמים. תהליכים אלו הינם תהליכים הנמצאים באחריות משותפת של גורמי התפעול ופונקציית אבטחת המידע והגנת הסייבר. בהתאם לדרישה הכללית בסעיף 15(ג) בהוראה 310 לפיה יש לעגן בנהלים ברורים סביבת בקרה פנימית נאותה

עליה תושתת המסגרת לניהול הסיכון בתאגיד הבנקאי, נדרש התאגיד הבנקאי, בין היתר, לקבוע נהלים לצורך התעדכנות מתמדת בטלאים כנגד הפגיעויות השונות, נהלים לבדיקת הטלאים בסביבה נפרדת, ונהלים לצורך התקנתם.

למקרה שבו נדרשת העברת שינוי כתגובה בחירום שלא ניתן ליישם לגביו את תהליך ניהול הטלאים הרגיל - ראה סעיף 97 להוראה.

ניהול גיבויים (סעיף 61.5 להוראה)

88. גיבויים מאפשרים לתאגיד הבנקאי את היכולת לחזור ולפעול בפרק זמן מוגדר מראש, תוך שהם מאפשרים המשכיות עסקית עם הפרעה מוגבלת. ההחלטה ליישם שיטה ספציפית של גיבויים, תתבסס בין היתר, על הקריטיות והרגישות של הנתונים והמערכות המהווים את נכס המידע.

89. לעניין גיבויים – ראה גם התייחסות בהוראה 355.

ניהול קיבולת וביצועים (סעיף 61.6 להוראה)

90. תהליך של ניהול קיבולת הוא תהליך לתכנון ולניטור המשאבים הטכנולוגיים של התאגיד הבנקאי הנדרשים לצורך תמיכה ביעדיו האסטרטגיים הנוכחיים והצפויים. התהליך משתמש בנתוני הקיבולת הנוכחיים של מערך טכנולוגיית המידע, לצורך מידול וקביעת תחזית של צרכיו העתידיים של התאגיד הבנקאי. ניהול קיבולת צריך להיות משולב באופן הדוק עם תהליכי התקצוב והתכנון של מערך טכנולוגיית המידע – ראה סעיף 64 להוראה בנושא: "תהליך תכנון והשקעה בטכנולוגיית המידע".
האופן שבו יבוצע תהליך ניהול הקיבולת נתון לשיקול דעתו של התאגיד הבנקאי, אולם מומלץ כי התהליך יבוצע באמצעות כלים ממוכנים על מנת להקל על ההנהלה בניתוח המידע אותו היא מקבלת.

ניהול נתיב ביקורת (סעיף 61.7 להוראה)

91. קבצי נתיב ביקורת הינם בדרך כלל בעלי נפחים גדולים ומהווים אתגר לקריאה. הם נוצרים במגוון מערכות ולעיתים קשה לנהל אותם ולבצע ביניהם קורלציות. מערכות SIEM (Security Information and Event Management) לדוגמא, יכולות לספק אמצעי לאיסוף, ביצוע אגריגציה, ניתוח וקורלציה של מידע ממערכות ויישומים נפרדים.
ניתוח נתיב ביקורת מאפשר לתאגיד הבנקאי לאתר בעיות, לתחקר פעילות חשודה, להבין מהי הפעילות הרגילה של מערך טכנולוגיית המידע מבחינת ביצועים וקיבולת, ולשפר אותו.

האתגר העומד בפני כל תאגיד בנקאי הוא לאזן בין כל הרכיבים הבאים המרכיבים את נתיב הביקורת: כמות הנתונים שנאספת, הזמינות של מקום האחסון והקיבולת, היכולת לנתח נתונים, והיכולת להגיב למסקנות העולות מניתוח זה.

ככל שהערכת הסיכונים גבוהה יותר כך נדרש ניתוח מעמיק יותר של הלוג בתכיפות גבוהה יותר ובאמצעים מתוחכמים יותר.

מחיקת נתונים והשמדת מדיה (סעיף 61.8 להוראה)

92. תהליכים למחיקת נתונים והשמדת מדיה וציוד הינם תהליכים הנמצאים באחריות משותפת של מספר פונקציות בתאגיד הבנקאי לרבות התפעול, אבטחת מידע והגנת הסייבר והנהלת צד ג' אם קיים. הנהלים יגדירו את שיטת המחיקה או ההשמדה בהתאם לסוג הנתונים שיש

למחוק. לדוגמא, תאגיד בנקאי יכול לבחור בהשמדה פיזית של מדיה אשר מכילה נתונים רגישים של לקוחות על מנת למנוע שחזור של נתונים אלו ושימוש לא נאות בהם.
התהליך יקבע גם אילו נתונים לא נדרשים במחיקה.

93. למען הסר ספק, משמעותה של העברת מדיה וציוד בסעיף זה הינה מגורם א' לגורם ב', בין בתאגיד הבנקאי ובין מחוצה לו (לדוגמא מתן מדפסת כתרומה), ואין משמעותה הוצאה ושימוש במדיה ובציוד על ידי עובד התאגיד הבנקאי מחוץ לכותלי התאגיד הבנקאי, לדוגמא בביתו (לעניין הוצאה ושימוש במדיה פיזית מסוג תדפיסים מחוץ לכותלי התאגיד הבנקאי על ידי עובד התאגיד הבנקאי - ראה סעיף 134 להוראה).
94. תאגיד בנקאי ישקול שימוש בטכניקות למחיקת נתונים גם כאשר המדיה מועברת בין מחלקות שונות בתוך התאגיד הבנקאי, זאת מאחר שבדרך כלל לא כל המחלקות בתאגיד הבנקאי נדרשות לגישה למידע הרגיש או המסווג שעל גבי אותה מדיה. לדוגמא, לעיתים נעשה שימוש חוזר במחשב של עובד שעזב, ולכן אם לאותו עובד שעזב הוענקה גישה לנתוני לקוחות רגישים, הרי שיש למחוק אותם מהמחשב של אותו עובד לפני שמעבירים אותו לעובד אחר במחלקה אחרת של התאגיד הבנקאי.
95. תאגיד בנקאי המתקשר עם צד ג', ידאג לעדכן בחוזה ההתקשרות עימו הסדרים למחיקת נתונים של התאגיד הבנקאי המאוחסנים אצלו לרבות אצל גורם שמתקשר עם אותו צד ג' לצורך ביצוע תכולת ההתקשרות עבור התאגיד הבנקאי. ההסדרים ייקבעו בהתאם לקריטיות ולרגישות הנתונים.
סעיף 30(א) להוראה 362 מחייב מחיקת המידע של התאגיד הבנקאי רק ממערכות נותן שירות מחשוב ענן מהותי. לפיכך, ייתכנו מקרים בהם הסדרי המחיקה הנדרשים בכל אחת מההוראות יהיו שונים. במקרה כזה, הדרישה המחמירה מבין שתי ההוראות, היא זו שתחול. כך לדוגמא: ייתכן מצב בו נותן שירות מחשוב ענן מהותי יחוייב במחיקת כל הנתונים הנשמרים אצלו בהתאם להוראה 362 על אף שחלק מהנתונים מוגדרים כלא רגישים, בעוד שעל פי הוראה זו אין על התאגיד הבנקאי חובה למחוק נתונים שאינם מוגדרים כרגישים. במקרה כזה תחול חובת המחיקה.
יצויין כי בהתאם לסעיף 23(ז)(3) להוראה 359A, במקרה של צד ג' המוגדר גם כ"נותן שירות" בהתאם להוראה 359A, על התאגיד הבנקאי לשקול את הכללת נושא אופן השבת המידע לתאגיד הבנקאי במסגרת חוזה מיקור החוץ.

תהליכי שירות ותמיכה (סעיף 62 להוראה)

96. להלן דוגמאות לתהליכי שירות ותמיכה נוספים על תהליכי "ניהול אירועים ובעיות" שהובאו בסעיף כדוגמא:
96.1. שירותי Help-Desk – בתהליך זה מספק ה – Help-Desk - סיוע טכני, סיוע בפתרון בעיות הקשורות לתוכנה, חומרה או רשתות, וסיוע בעת התרחשות אירועים ובעיות - לעובדי התאגיד הבנקאי וללקוחותיו.
96.2. תמיכה תפעולית – עובדי מערך טכנולוגיית המידע מספקים תהליכים תפעוליים התומכים בקווי העסקים של התאגיד הבנקאי (לדוגמא: מריצים משימות (Job) במחשב המרכזי). מכיוון שלהנהלת קו העסקים אין את הידע המתאים לבחון תהליכים אלו, על הנהלת התאגיד הבנקאי להנהיג, לדוגמא:

96.2.1. תהליכים המוודאים שתהליכי קליטת הנתונים במערכות ועיבודם הינם שלמים ומדויקים.

96.2.2. בקרות המוודאות שתהליכי קליטת נתונים מגורמים מחוץ לתאגיד הבנקאי ועיבודם נעשים בהתאם למדיניות אבטחת המידע והגנת הסייבר של התאגיד הבנקאי.

96.2.3. בקרות המוודאות שנתונים לא נפגעו במהלך קליטתם או כתוצאה מכשלים בעיבודם.

96.2.4. מנגנונים לדיווח על תקלות בקליטה ובעיבוד.

תהליכי ניטור, הערכה ודיווח (סעיף 63 להוראה)

97. תהליכי ניטור, הערכה ודיווח תומכים בניהול פרואקטיבי של מערך טכנולוגיית המידע ומסייעים בהכוונת התאגיד הבנקאי להשגת יעדיו העכשוויים ותוכניותיו לעתיד כמו: צמיחה, מיזוגים או הרחבת קו עסקים.

להלן דוגמאות לסוגי דיווחים על פעילות מערך טכנולוגיית המידע:

97.1. דוח על ניצול קיבולת.

97.2. דוחות על זמינות מערכות, זמני תגובה של מערכות, וזמני עיבוד.

97.3. שלמות ודיוק טרנזקציות.

97.4. השוואת רמת שירות מוסכמת (SLA) אל מול הביצועים בפועל.

97.5. שימוש באינדיקטורים מרכזיים לביצועים (KPI) אשר מאפשרים לקבוע עד כמה התהליך המיושם מסייע בהשגת המטרות.

עקרונות ליישום נאות של תהליך תכנון והשקעה בטכנולוגיית המידע (סעיף 64.1.4)

98. המשאבים הטכנולוגיים כוללים, בין היתר, את הרכיבים הבאים, והתאגיד הבנקאי נדרש לוודא תאימותם לצרכים הנוכחיים והצפויים של התאגיד הבנקאי:

98.1. תשתית – לדוגמא: חשמל, תקשורת, ארכיטקטורת רשת ומתקנים מתאימים.

98.2. חומרה – לדוגמא: מחשב מרכזי, שרתים, רשתות, מחשבים שולחניים, מכשירים ניידים, התקני אחסון.

98.3. תוכנות הפעלה – לדוגמא: מערכות הפעלה, מהדרים (Compilers), רכיבים שנועדו לסייע לציוד ולתוכנות ההפעלה לתפקד באופן נאות.

98.4. אפליקציות לרבות, יישומים ומערכות.

98.5. עובדים מיומנים.

99. תכנון הינו תהליך בו התאגיד הבנקאי נערך לקראת פעילויות עתידיות באמצעות הגדרת היעדים והאסטרטגיה להשגתם. פעילויות עתידיות כוללות, בין היתר, הצעה של מוצר או שירות חדשים, מיזוגים ורכישות מתוכננים, או היערכות לקראת הפסקת תמיכה במערכת מידע. טכנולוגיית המידע הינה חלק בלתי נפרד מהפעילות העסקית של התאגיד הבנקאי. לפיכך, תאגיד בנקאי נדרש לשלב שיקולים של הקצאת משאבים והשקעות בטכנולוגיה, במסגרת תהליך התכנון העסקי הכולל. להשקעות משמעותיות בטכנולוגיה יש השלכות ארוכות טווח על הביצועים של מוצרים ושירותים שמציע התאגיד הבנקאי ועל הצעה של חדשים.

100. בתהליך תכנון נאות ישתתפו הדירקטוריון, ההנהלה הבכירה והעובדים. הדירקטוריון יאתגר את ההנהלה הבכירה באשר לאפקטיביות תהליך התכנון בעת אישור מדיניות טכנולוגיית המידע כמפורט בסעיף 15 להוראה, וההנהלה הבכירה תגבש את מדיניות טכנולוגיית המידע ותוכנית עבודה שנתית ורב שנתית בתחום טכנולוגיית המידע כאמור בסעיפים 19.3 ו- 19.4 להוראה.

101. תהליך התכנון יותאם באופן שוטף לסיכונים חדשים הניצבים בפני התאגיד הבנקאי ולהזדמנויות הנקרות בפניו, תוך שהוא ממקסם את התרומה של מערך טכנולוגיית המידע עבורו.

התקשרות עם צדדים שלישיים בתהליך התכנון (סעיף 64.2 להוראה)

102. כחלק מהבדיקות לצורך וידוא שצד ג' יכול להמשיך ולתמוך בתוכניותיו של התאגיד הבנקאי, יכול התאגיד הבנקאי לסקור את אתר צד ג', קטעי עיתונות רלבנטיים, ועדכונים תקופתיים של צד ג' או כל מקור מידע אחר, כדי להתעדכן בפעילויות של צד ג', בשינויים באסטרטגיה שלו ובשירותים שהוא מספק, בתוכניות עתידיות שלו, התחייבויות עתידיות נוספות שלו (קיימות או עתידיות), תכנון של צד ג' לשנות את אופי הפעילות שלו או את כוח האדם, ובסוגיות שונות הקשורות לאבטחת המידע או לשירות שהוא מספק.

<u>פרק ו' - ניהול פרויקטים וניהול שינויים</u>

כללי (סעיפים 99-65 להוראה)

103. ההוראה מגדירה את התוצרים הרצויים מתהליך ניהול פרויקטים וניהול שינויים ואת העקרונות שהתאגיד הבנקאי נדרש ליישם כדי להשיג תוצרים אלו. ההוראה אינה מגדירה שיטות ספציפיות שבאמצעותן ניתן להשיג את התוצרים, והדרך הטובה ביותר למימוש העקרונות המפורטים בהוראה נתונה להחלטתו של התאגיד הבנקאי. ההוראה מתאימה לתפיסות ושיטות ניהול פרויקטים ושינויים מקובלות והיא ניטרלית לטכנולוגיה.

מסגרת עבודה לניהול פרויקטי טכנולוגיית מידע (סעיף 65 להוראה)

104. תהליך נאות לניהול פרויקטי טכנולוגיית מידע הוא גורם מפתח בניהול נאות של מערך טכנולוגיית המידע וכולל ידע, מומחיות, כלים וטכניקות להשגת יעדי הפרויקט. המורכבות התפעולית של התאגיד הבנקאי מכתיבה את רמת הפורמליות של הפרקטיקות לניהול פרויקטים. היכולת של התאגיד הבנקאי לנהל פרויקטים משפיעה על יכולתו להסתגל לשינויים בסביבה העסקית ועל יכולתו לעמוד ביעדים האסטרטגיים שקבע לעצמו.

105. מסגרת העבודה לניהול פרויקטי טכנולוגיית המידע תגדיר, לכל הפחות, תפקידים, תחומי אחריות, סמכויות וקווי דיווח והיא תבחין בין סוגי פרויקטים שונים בהתאם לקריטיות ולרגישות נכס המידע הרלבנטי לפרויקט, ובהתאם למאפיינים נוספים המפורטים בסעיף. כך למשל, פרויקט חדשני מעצם טבעו יצריך תשומת לב ניהולית רבה יותר, והתאגיד הבנקאי יידרש לקבוע מסגרת עבודה מתאימה.

מדיניות לניהול פרויקטי טכנולוגיית המידע (סעיף 67 להוראה)

106. המדיניות לניהול פרויקטי טכנולוגיית המידע הינה חלק ממדיניות ניהול טכנולוגיית המידע של התאגיד הבנקאי.

107. הסעיף דורש שהמדיניות תתייחס לאופן היישום של הנושאים המפורטים בו בהתאמה לסוגי הפרויקטים השונים. כך למשל: המדיניות תקבע באיזה סוג פרויקט יידרש לקבוע אבני דרך מרכזיות.

זיהוי הסיכונים בפרויקטי טכנולוגיית המידע, הערכתם ומזעורם (סעיף 71 להוראה)

108. התממשות סיכונים בפרויקט יכולה להשפיע באופן שלילי על לוחות הזמנים למסירתו, על תקציבו ועל איכותו. בהתאם לכך, נדרש התאגיד הבנקאי לנטר את הסיכונים הנובעים מהפרויקט.

בדיקת נאותות בעת רכישת מערכת (סעיף 75 להוראה)

109. בהתאם לאמור בסעיף 5 להוראה, בצד ג' המוגדר גם כ"נותן שירות" בהתאם להוראה 359A, רמת בדיקת הנאותות שתבוצע תהיה בהתאם לקריטיות ולרגישות נכס המידע, ובנוסף היא תידרש לעמוד גם באמור בסעיפים 21-18 להוראה 359A.

פיתוח ויישום מערכת (סעיפים 83-79 להוראה)

110. למען הסר ספק, פרק זה מתייחס גם למקרה שבו התאגיד הבנקאי רכש מערכת והוא מבקש ליישם אותה או מבקש ליישם מערכת שאת חלקה הוא רכש וחלקה פותח על ידו.

צעדים למזעור הסיכון לשינוי (סעיף 79 להוראה)

111. תאגיד בנקאי נדרש לוודא שננקטו צעדים למניעת טעויות אנוש ולמניעת פעולות מכוונות לפגיעה במערכת, במהלך תהליך הפיתוח ויישום המערכת בסביבת הייצור.

גישה על פי צורך (סעיף 81 להוראה)

112. במתן גישה על בסיס צורך – ההרשאות ניתנות לזמן קצוב (Just in time access), בניגוד לתהליך בו הרשאות קבועות ניתנות בתהליך חד פעמי.

מחזור חיים של פיתוח ויישום מערכת (סעיף 82 להוראה)

113. System Development Life Cycle (SDLC) הינו מודל קונספטואלי אשר מתאר את השלבים המעורבים בפרויקט לפיתוח מערכת, משלב ההיתכנות הראשונית ועד לשלב התחזוקה. SDLC יכול להיות רלבנטי לנכסי מידע דוגמת חומרה ותוכנה. כל חומרה, תוכנה, מערכת יעברו דרך תהליך פיתוח, שניתן להתייחס אליו כאל סדרה של תהליכים שחוזרים על עצמם עם מספר רב של שלבים. SDLC משמש כמבנה וכמסגרת נוקשים לצורך הגדרת השלבים המעורבים בתהליך פיתוח מערכת. מתודולוגיות SDLC לדוגמא: Waterfall, Spiral, Agile. מתודולוגיית SDLC מתמקדת בשלבים הבאים: ייזום, איסוף הדרישות, תכנון, עיצוב, פיתוח התוכנה, בדיקה, יישום ותחזוקה.

פיתוח API (סעיפים 91-84 להוראה)

114. ממשקי API מאפשרים למגוון אפליקציות לתקשר אחת עם השנייה ולקבל ולהעביר נתונים. ממשקי API הינם ממשקים הזמינים לצדדים שלישיים ואשר מאפשרים למפתחים גישה פרוגרמטית לאפליקציות או לשירות ה – WEB. תאגיד בנקאי יכול לשתף פעולה עם חברות פינטק וכד' ולפתח ממשקי API אשר ישמשו להעברת מידע או נתונים אל ומצדדים שלישיים. מכאן שקיימת חשיבות רבה לתאגיד הבנקאי ליישם אמצעי בקרה נאותים לניהול מאובטח של הפיתוח והתפעול של ממשקי API.

למען הסר ספק יובהר כי פרק זה מפרט את עקרונות אבטחת מידע בנוגע לפיתוח וניהול Open API מאובטח מול צדדים שלישיים, הן אלו הנחשבים "ספק צד ג'" כהגדרתו בהוראת נ.ב.ת.

מס' 368 בנושא: "בנקאות פתוחה" (להלן: "הוראה 368"), והן אלו שאינם נחשבים "ספק צד ג'" כהגדרתו בהוראה 368 ואשר התאגיד הבנקאי בוחר מיוזמתו להתקשר עימו בממשק כאמור (על אף שאינו מחוייב לכך על פי חוק), במסגרת יוזמות עסקיות. עם זאת יודגש כי, סעיפים 87-85 להוראה לא יחולו במקרה שמדובר בצד ג' שהוראה 368 חלה עליו.

העברה לייצור של שינויי חירום (סעיף 97 להוראה)

115. ככלל, גם שינויי חירום צריכים להתבצע בהתאם לתהליך השינויים הרגיל הנהוג בתאגיד הבנקאי. יחד עם זאת, ייתכנו שינויים דחופים או שינויי חירום, כמו טלאי אבטחה (patch אבטחתי) בעל חשיבות גבוהה ובתעדוף גבוה, שהינם שינויים אשר צריכים להיות מיושמים במהירות ושלא ניתן ליישם לגביהם את תהליך ניהול השינויים הרגיל האמור בסעיף 61.4 להוראה ותחת נושא זה ("ניהול שינויים"). שינויים מסוג זה יבוצעו במקרים חריגים מאד.

<u>חלק ד' – ניהול סיכוני אבטחת מידע והגנת הסייבר</u>

<u>פרק ז' – אבטחת מידע</u>

הערכת נאותות יכולת אבטחת המידע (סעיף 100 להוראה)

116. הערכה שוטפת של נאותות יכולת אבטחת המידע של התאגיד הבנקאי יכולה להתבצע במגוון דרכים, לדוגמא בדיקה של אחד או יותר מהפרמטרים הבאים: נאותות התקציב והקצאת כוח האדם, יכולת גישה מהירה למיומנויות מתאימות, ושלמות סביבת הבקרה – מניעה, זיהוי ותגובה.

רכיבי יכולת אבטחת המידע (סעיף 101 להוראה)

117. מתאר האיומים הנוכחי עימו מתמודדים התאגידים הבנקאיים, לרבות איומי מתקפת סייבר, מחייב יכולות אבטחת מידע ייחודיות מעבר לבקרות אבטחת מידע כלליות. יכולות אבטחת מידע ייחודיות אלו יכללו בין היתר את הרכיבים המפורטים בסעיף.

הערכת נאותות יכולת אבטחת המידע של צד ג' (סעיף 102 להוראה)

118. תאגיד בנקאי יעריך את נאותות יכולת אבטחת המידע של צד ג', בין היתר בהיבטים של נאותות המשאבים, המיומנויות והבקרות המוקצים לה. הערכה זו יכולה להתבצע באמצעות שילוב של מגוון כלים דוגמת: ראיונות, דוחות שירות (service reporting), בדיקת בקרות, חוות דעת של גורמים בלתי תלויים.

מסגרת לניהול אבטחת המידע והגנת הסייבר (סעיף 103 להוראה)

119. הסעיף קובע כי מסגרת לניהול אבטחת המידע והגנת הסייבר של התאגיד הבנקאי תתאם את סיכוני אבטחת המידע שלו. דרישה זו נועדה להדגיש את הציפייה של הפיקוח על הבנקים שמסגרת אבטחת המידע והגנת הסייבר תתעדכן בהתאם לשינויים במתאר סיכוני אבטחת המידע העומדים בפני התאגיד הבנקאי.

120. הנחיות ללקוחות התאגיד הבנקאי הנוגעות לאבטחת מידע, כנדרש בסעיף, יכולות להינתן באמצעות מגבלות טכנולוגיות, לדוגמא, חיוב הלקוח בקביעת סיסמא בת X תווים.

עקרונות על מרכזיים בבסיס מסגרת לניהול אבטחת המידע והגנת הסייבר (סעיף 105 להוראה)

121. מסגרת לניהול אבטחת המידע והגנת הסייבר תתבסס על עקרונות אבטחת מידע שינחו את מקבלי ההחלטות בנוגע לאבטחת מידע. יישום העקרונות המינימליים המפורטים בסעיף,

ייצור בסיס נאות למסגרת אבטחת המידע והגנת הסייבר של התאגיד הבנקאי ויביא לצמצום מעטפת התקיפה (סך כל הפעולות ומשאבי המערכת שחשופים לסביבה).

הגנה לעומק (סעיף 105.1 להוראה)

122. מימוש הגנה לעומק על ידי יישום אבטחה רב שכבתית (Multi-Layer Defense) יכול לחזק באופן משמעותי את האבטחה הכוללת של תהליכים עסקיים, מערכות מידע, מוצרים ושירותים בנקאיים וכן להיות יעיל בהגנה על מידע רגיש ללקוח, מניעת גניבת זהות ומניעת הפסדים כתוצאה משימוש בלתי מורשה.

הרשאות מינימליות (סעיף 105.2 להוראה)

123. יישום עיקרון זה עשוי לצמצם את מספר וקטורי התקיפה (ממשקים חיצוניים של המערכת המהווים יחד את מעטפת התקיפה) שניתן לנצלם כדי לפגוע באבטחת המידע של התאגיד הבנקאי.

זיהוי אירועי אבטחת מידע בזמן (סעיף 105.3 להוראה)

124. זיהוי אירוע אבטחת מידע צריך להיות בזמן שיאפשר צמצום השפעת הפגיעה באבטחת המידע למינימום.

מניעת גישה בלתי מורשית או פגיעה אחרת באבטחת המידע בעת התרחשות שגיאה (סעיף 105.7)

125. על התאגיד הבנקאי למנוע מצב בו שגיאה, בין אם נגרמה בזדון ובין אם נגרמה שלא בזדון תגרום לפגיעה באבטחת המידע. כך לדוגמא: שרת קיבל פניה עם מידע לא צפוי (למשל, שם משתמש ריק), וכתוצאה מכך חשף פרטים שאינו אמור לחשוף.

אימות כל גורם בטרם הסתמכות עליו (סעיף 105.8 להוראה)

126. על התאגיד הבנקאי להתייחס באופן מיוחד לגורמים שאינם מוכרים בטרם הסתמכות עליהם ובכלל זה, נקיטת זהירות יתר בפעילות מול נכסי מידע פנימיים וחיצוניים שאינם מוכרים, משום שרמת בקרות אבטחת מידע בנכסים אלו אינה ידועה וייתכן שהיא אינה מספקת.

הפרדת תפקידים (סעיף 105.9 להוראה)

127. יישום עיקרון זה מפחית את הפוטנציאל לפגיעה באבטחת המידע של התאגיד על ידי עובד יחיד.

איסוף מידע (סעיף 105.13.2 להוראה)

128. עיקרון מודעות מצבית עוסק בתפיסת מצב הגנת הסייבר של התאגיד הבנקאי, בפרק הזמן הנוכחי, אל מול האיומים, ביצוע ניטור מקיף של הסביבה הפנימית והחיצונית לתאגיד הבנקאי לצורך זיהוי חולשות ו/או איומים ו/או אירועי אבטחת מידע ו/או סממנים לקיומם של אלה, תוך שימוש ביכולות זיהוי שונות - למשל: ניתוח דפוסים, זיהוי אנומאליות, ניתוח נתוני עתק (Big Data Analysis) - ותעדוף של האירועים בהתחשב ברמת הסיכון ופוטנציאל הנזק הגלום בהם, כבסיס לקבלת החלטות אופרטיביות.

מדיניות אבטחת המידע והגנת הסייבר (סעיפים 107-106 להוראה)

129. יובהר כי אין באמור בסעיפים אלו בכדי לגרוע מהחובה בדבר ניהול ועדכון מסמך הגדרות המאגר, הקבועה בתקנה 2 ל"תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017".

130. המדיניות צריכה להתייחס לנושאים המפורטים בסעיף 106 להוראה. ככל שנדרש, ניתן להרחיב לגבי נושאים אלו באמצעות הפנייה למסמך מתאים בו יוסדר הנושא באופן מפורט יותר.

<u>פרק ח': יישום בקרות אבטחת מידע</u>

כללי (סעיפים 110-108 להוראה)

131. כאמור בסעיף 9 להוראה, תהליך ניהול סיכון אבטחת המידע ובכלל זה שלב יישום והטמעת בקרות כנגד אותם סיכונים, נדרש להיות תואם לעקרונות לניהול הסיכון התפעולי המפורטים בהוראה 350 ולעקרונות ניהול סיכונים בכלל המפורטים בהוראה 310. בנוסף, בתהליך יישום והטמעת בקרות אבטחת מידע יינתנו דגשים נוספים המפורטים בפרק זה.

על מנת להגן על נכסי המידע ובהמשך לתהליך הערכת הסיכונים המפורט בפרק ג' להוראה, תאגיד בנקאי נדרש ליישם בקרות אבטחת מידע, אשר תואמות, בין היתר, את רמת הקריטיות והרגישות של נכס המידע, ואת שלב מחזור החיים בו נמצא נכס המידע. על התאגיד הבנקאי להבטיח כי בקרות אבטחת המידע יישארו אפקטיביות בכל שלב של מחזור החיים של נכס המידע.

132. מיפוי בקרות אבטחת המידע המיושמות או המתוכננות להיות מיושמות אצל צד ג' יכול להתבצע באמצעות שילוב של מגוון כלים דוגמת: ראיונות, סקרים, מבדקי בקרות, אישורים וחוות דעת של גורמים בלתי תלויים.

יישום בקרות אבטחת מידע אצל צד ג' (סעיפים 110-109 להוראה)

133. הדרישות בסעיפים אלו הינן דרישות ליישום בקרות אבטחת מידע על נכסי מידע המנוהלים באמצעות צד ג' וצריכות להתבצע בטרם או במהלך ההתקשרות עימו. לעניין הדרישה להערכת אפקטיביות הבקרות המיושמות על נכסי מידע המנוהלים באמצעות צד ג' – ראה פרק ט' להוראה "הערכת אפקטיביות בקרות אבטחת מידע".

זיהוי, הערכה והטמעת בקרות בהתייחס לפגיעויות ואיומי אבטחת מידע (סעיף 111 להוראה)

134. תהליך זיהוי, הערכה והטמעת בקרות אבטחת מידע צריך להיות מתמשך ולהתבצע בין היתר בהתאם לשינויים פנימיים וחיצוניים, ובכללם שינויים עסקיים, ארגוניים וטכנולוגיים.

135. תאגיד בנקאי נדרש להבנה מלאה באשר לנכסי המידע עליהם נשענת הפעילות העסקית שלו, ולהתמקד באותם נכסי מידע, אשר במקרה של אירוע אבטחת מידע תהיה להם ההשפעה הרבה ביותר עליו. יחד עם זאת, "חוזק השרשרת הוא כחוזק החוליה החלשה בה" ולפיכך קובע הסעיף כי, על התאגיד הבנקאי לזהות ולהעריך פגיעויות ואיומים גם לגבי נכסי מידע באמצעותם ניתן לסכן נכסי מידע קריטיים ורגישים.

136. פעילויות תיקון (remediation activities) הן פעילויות אקטיביות לזיהוי ומיגור האיום. פעילויות אלו הן מרכיב מרכזי באסטרטגיית אבטחת מידע והגנת הסייבר של התאגיד הבנקאי והן מסייעות לתאגיד הבנקאי להגיב על איומי אבטחת מידע, לדוגמא: במתקפות סייבר - להכיל את הנזק, ולסלק את האיום בכללותו.

137. תמונת האיום והחשיפה של התאגיד הבנקאי יכולה להיגזר, בין היתר לדוגמא, מהמידע הבא: מיפוי גורמי איום רלבנטיים בחתך מוטיבציה ויכולות; טכניקות, טקטיקות, תרחישים ואמצעי תקיפה; חולשות, הגדרות מערכת, או פגיעויות שעלולות לשמש כר להתקפות; פעולות שננקטו בעבר בתגובה להתקפה, התקפות שאירעו בעבר (בתאגיד הבנקאי ו/או בסביבת הפעילות); דרכים ואינדיקטורים לגילוי וזיהוי התקפות; דרכי התמודדות עם התקפות.

בקרות אבטחת מידע בשלבי מחזור החיים של נכס המידע (סעיפים 115-112)

138. הסעיפים עוסק במחזור החיים של נכס המידע שהוא רחב יותר ממחזור החיים של פיתוח תוכנה. שלבי מחזור החיים של נכס המידע כוללים: תכנון, עיצוב, רכישה, יישום, הוצאה משימוש והשמדה.

בקרות ניהול פגיעויות (סעיף 114.7 להוראה)

139. ניהול פגיעויות הוא תהליך מתמיד שבו התאגיד הבנקאי מקבל מידע על פגיעויות חדשות, מנתח אותו ונוקט בפעולה בעקבותיו, לרבות טיפול בהן תוך צמצום חלון הזמן לניצולן על ידי גורם עוין. ניהול הפגיעויות כולל גם תהליך לניהול טלאים.

בהתאם לדרישה הכללית בסעיף 15(ג) להוראה 310, לפיה יש לעגן בנהלים ברורים סביבת בקרה פנימית נאותה עליה תושתת המסגרת לניהול הסיכון בתאגיד הבנקאי, נדרש התאגיד הבנקאי, בין היתר, לקבוע נהלים לצורך התעדכנות מתמדת בפגיעויות לנכסי המידע.

בקרות ניהול קיבולת וביצועים (סעיף 114.11 להוראה)

140. תהליך לניהול קיבולת וביצועים מערב היבטים טכנולוגיים תפעוליים (ראה סעיף 61.6 להוראה - "ניהול קיבולת וביצועים") שמשפיעים על זמינות נכס המידע. יחד עם זאת, תהליך של ניהול קיבולת וביצועים יכול להיות חשוף גם לסיכוני אבטחת מידע גרידא. למשל: אירוע של מתקפת DDoS בה גורם עוין גורם לקריסת השרת באמצעות פניות מרובות אליו.

בקרות לניהול זהויות ולניהול גישה לוגית (סעיפים 120-116 להוראה)

141. למען הסר ספק, אין באמור בסעיפים 119-117 להוראה בכדי לגרוע מחובת התאגיד הבנקאי לעמוד בסעיף 14(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017, למעט הסיפא של סעיף 14(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 שלא תחול על גישה של הלקוחות למידע על אודותם.

קביעת בקרות לניהול זהויות ולניהול גישה לוגית (סעיף 116.1 להוראה)

142. הרשאות גישה ניתנות בדרך כלל ליחידים, חשבונות מערכת ייעודיים, ונכסי מידע דוגמת שירותי מערכת (Services) ותוכנה.

תאגיד בנקאי נדרש לקבוע בקרות לניהול זהויות ולניהול גישה לוגית עבור כל גורם בעל גישה לנכס המידע. למען הסר ספק מובהר כי הכוונה גם לצד ג' אשר יש לו גישה לנכס המידע.

חריגים (סעיף 116.2 להוראה)

143. דוגמא למקרה חריג שבו לא ניתן לקבוע אמצעי זיהוי ואימות אישיים, היא מפעילי מחשב המתחלפים תוך כדי פעולת המחשב, וזיהוי ואימות אישיים יחייבו יישום תהליך מורכב של החלפת משתמשים שעלול לשבש את תהליך העבודה.

חוזקם של אמצעי הזיהוי והאימות (סעיף 119 להוראה)

144. טכניקות מקובלות להגברת חוזקם של אמצעי הזיהוי והאימות כוללות, בין היתר, את השימוש בסיסמאות חזקות (פרמטרים לדוגמא המשפיעים על חוזק הסיסמא: אורך, מורכבות, מגבלות לשימוש חוזר ותדירות שינויים גבוהה), טכניקות הצפנה, הגדלת מספר גורמי האימות הנדרשים (Multi Factor Authentication) וכן שימוש בטכנולוגיה המשלבת זיהוי ואימות של המשתמש, סודיות ושלמות הנתונים ומניעת הכחשה, לדוגמא, התקני PKI (Public Key Infrastructure) (שימוש במפתח ציבורי ופרטי).

למען הסר ספק, אימות מוגבר אינו בהכרח כמשמעות המונח "פרט אימות מוגבר" בחוק שירותי תשלום, תשע"ט – 2019.

מזעור החשיפה לתרחישים חמורים אך סבירים (סעיף 121 להוראה)

145. בחינת תרחיש של חדירת תוכנה זדונית למערכת ולמידע המוצפן עליה, לרכיבי האחסון שלה, לרבות לרשתות התאגיד הבנקאי ולהסדרי האחסון בענן שברשותו, יכולה להוות דוגמא לבחינת תרחישים בסבירות נמוכה ובעלי השפעה חמורה מאוד הנדרשת בסעיף. סוג כזה של התקפה יכול למשל ללמד על החשיבות בהגנה על סביבת הגיבוי במקרה שבו אבטחת סביבת הייצור נפגעת. הגנה זו יכולה להתבצע, בין היתר, באמצעות הפרדת רשתות, בקרות גישה חזקות, ומגבלות על התעבורה ברשת.

בקרות גישה פיזית ובקרות סביבתיות (סעיף 122 להוראה)

146. העדר בקרות גישה פיזית ובקרות סביבתיות יכול לפגוע באפקטיביות של בקרות אבטחת מידע אחרות. תאגיד בנקאי נדרש ליישם בקרות אלו בחצרותיו, ובמתקני מיקור חוץ בהם הוא עושה שימוש.

בדיקות אבטחה (Security Testing) לזיהוי פגיעויות (סעיף 124.1 להוראה)

147. הסעיף קובע כי על התאגיד הבנקאי לקבוע נקודות בדיקה לאורך תהליך השינוי על מנת לוודא כי דרישות אבטחת מידע והגנת הסייבר מזוהות, מתוכננות, נבנות ונבחנות כך שרמת אבטחת המידע ממשיכה לתמוך ביעדים העסקיים של התאגיד הבנקאי. אופי הבדיקה ייקבע בהתאם לרמת הקריטיות והרגישות של נכס המידע שמושפע מהשינוי (ולא רק נכס המידע שבו מבוצע השינוי) ויכול לנוע בין בדיקות באמצעות השוואה לשינויים דומים שבוצעו לבין בדיקה בפני עצמה.

פיתוח ואישור השינויים בסביבה אחרת (סעיף 124.3 להוראה)

148. התאגיד הבנקאי נדרש לפיתוח שינויים ובדיקתם (לרבות שינויים מתוכננים, דחופים, ושינויי חירום לתוכנה, חומרה ונתונים) בסביבה נפרדת מסביבת הייצור. לצורך כך, יש לשקול הקמת מספר סביבות המשקפות את השלבים השונים בפיתוח ובדיקה של השינויים.

להעברת שינוי כתגובה בחירום שלא ניתן ליישם לגביו את תהליך ניהול השינויים הרגיל - ראה סעיף 97 להוראה.

שימוש בנתוני אמת לאחר הפיכתם ללא רגישים במסגרת הפיתוח והבדיקות (סעיף 124.5 להוראה)

149. הסעיף קובע כי במקרה שהדבר חיוני ניתן לעשות שימוש בנתוני אמת לאחר הפיכתם ללא רגישים.

צמצום למינימום של שינויים הכרוכים ביצירת פגיעויות אבטחת מידע שלא ניתן לטפל בהן (סעיף 124.6 להוראה)

150. לעיתים קיימת נחיצות לבצע שינוי כלשהו בייצור, אולם ידוע ששינוי זה טומן בחובו גם יצירת פגיעות אבטחת מידע עבור התאגיד הבנקאי שלא ניתן באותה עת לטפל בה. במצב כזה, במהלך הפעילות השוטפת, כמובן שלא ניתן להכניס את השינוי לייצור, עד אשר פגיעות אבטחת המידע לא טופלה. יחד עם זאת, ייתכנו מקרים בהם הערכת הסיכון מאי הכנסת השינוי תגבר על הערכת הסיכון מהכנסת השינוי תוך יישום בקרות מפצות. במקרים כאלו הכנסת השינוי לייצור אפשרית ובלבד שתתקבל לכך הסכמה מראש של הגורם המתאים ותוך יישום בקרות מפצות ככל שניתן.

מצב כזה שבו השינוי כולל פגיעויות אבטחת מידע ביודעין, מתרחש בדרך כלל במערכות או בטכנולוגיות ישנות שבשימוש התאגיד הבנקאי. הפיקוח על הבנקים סבור כי הצורך באישור מראש של שינויים שיוצרים ביודעין פגיעויות אבטחת מידע, יצמצם תופעות כאלו למינימום הנדרש, ויעודד יישום בקרות מפצות.

בקרות גישה לאמצעים המאפשרים חשיפה של מידע רגיש (סעיף 126)

151. סעיף זה עוסק בבקרות הגישה הנדרשות על-מנת למנוע מגורמים בעלי גישה להסיר, להעתיק, להפיץ או לחשוף באופן אחר מידע שהוגדר כרגיש, וזאת באותם המקומות בהם קיים חשש לדלף מידע.

להלן דוגמאות לאמצעים אשר בשימוש לא נאות עשויים לאפשר חשיפה בלתי מורשית של מידע רגיש: מכשירים ניידים (מחשבים נישאים, מחשבי לוח, טלפונים ניידים וכו'), התקני אחסון ניידים, אמצעים להעברה אלקטרונית (דוא"ל, תוכנות למשלוח מסרים מידיים וכו') ואמצעים להעברת מידע (מדפסות, טלפוניה, ציוד לשיחות ועידה חזותיות וכו').

עקרונות לשימוש בטכניקות קריפטוגרפיות (סעיף 127.4-127.1 להוראה)

152. טכניקות קריפטוגרפיות הן שיטות המשמשות להצפנת נתונים, אימות זהויות, והבטחת שלמות הנתונים.

תאגיד בנקאי נדרש להשתמש בטכניקות קריפטוגרפיות לצורך בקרת גישה לנתוניו שבתנועה ולנתוניו שבמנוחה ולתווך בו עוברת תעבורת הרשת, בהתאם להערכת סיכונים מתאימה שתתחשב, בין היתר, באופי הפעילות הנבחנת (לדוגמא, העברת נתונים על גבי תווך שאינו בשליטתו הבלעדית של התאגיד הבנקאי), ובמידת הקריטיות והרגישות של הנתונים.

למרות האמור לעיל, בכל מקרה של אחסון נתונים שהוגדרו על ידי התאגיד הבנקאי ברמת קריטיות גבוהה וגם ברמת רגישות גבוהה שלא ברשת הפנימית של התאגיד הבנקאי, ובכל מקרה של העברת נתונים בכלל ברשת ציבורית או ברשת שהתאגיד הבנקאי לא יכול לאכוף את מדיניות אבטחת המידע והגנת הסייבר שלו בה, נדרש התאגיד הבנקאי לעשות, לכל הפחות, שימוש בטכניקות הצפנה מקובלות.

יודגש כי הצפנת תווך תעבורת הרשת אינה מייתרת בהכרח את הצפנת הנתונים העוברים בו. ולהיפך, הצפנת הנתונים אינה מייתרת בהכרח את הצפנת תווך תעבורת הרשת. בהתאם לכך, ייתכנו מקרים בהם תידרש הצפנה הן של הנתונים והן של תווך התעבורה.

חוזק הטכניקה הקריפטוגרפית בה ייעשה שימוש, ייקבע בהתאם להערכת סיכונים שתתחשב, בין היתר, במידת הקריטיות והרגישות של הנתונים, באופי הפעילות, ובבקרות נוספות.

דרישות והחרגות לעניין הצפנה בהוראות נ.ב.ת 362 ו 367 (סעיף 127.5 להוראה)

153. על התאגיד הבנקאי ליישם את הוראות ס"ק 127.3 – 127.1 להוראה זו, לגבי כל נתוניו. יחד עם זאת, קיימים מקרים בהם הפיקוח על הבנקים מצא לנכון להנהיג הסדרים שונים מהדרישות המפורטות בהוראה זו, והסדרים אלו ימשיכו לחול על אף האמור בהוראה זו. כך לדוגמא:

153.1. סעיף 63 להוראה 367 - תאגיד בנקאי המעביר מידע על לקוחותיו ברשתות חיצוניות לרבות האינטרנט נדרש לעשות שימוש באלגוריתם הצפנה על מנת להגן על המידע של לקוחותיו העובר ברשתות חיצוניות לרבות האינטרנט.

153.2. סעיף 63 להוראה 367 - תאגיד בנקאי המעביר מידע על לקוחותיו ברשת הטלפוניה – אינו מחוייב בהצפנת מידע זה.

153.3. סעיף 33 להוראה 362 - תאגיד בנקאי המעביר מידע בתקשורת לנותן שירותי מחשוב ענן יצפין אותו בעת העברתו וכן בעת אחסונו אצל נותן שירותי מחשוב ענן. במקרים בהם יש קושי לתאגיד הבנקאי להצפין את כל המידע כאמור, יש להצפין לפחות את הנתונים שסווגו על ידו כמידע רגיש או שיש בחשיפתם כדי לפגוע בתאגיד הבנקאי ובלקוחותיו.

154. יודגש כי הדרישות וההחרגות לעניין הצפנה המפורטות במסגרת הוראה 367, רלבנטיות אך ורק למידע של לקוחות העובר במסגרת מתן שירותים בערוצי בנקאות בתקשורת כהגדרתם בסעיף 8 להוראה 367. בהתאם לכך, נתוני לקוחות שאינם עוברים במסגרת שירותים הניתנים בערוצי בנקאות בתקשורת כאמור ואינם נכנסים לגדר של תחולת סעיף 33 להוראה 362, נדרשים בהצפנה בהתאם להוראות ס"ק 127.3 – 127.1 להוראה זו.

בקרות לניהול נאות של מפתחות קריפטוגרפיים (סעיף 127.6 להוראה)

155. ניהול נאות של מפתחות קריפטוגרפיים מבטיח שמיושמות בקרות להפחתת הסיכון לחשיפתם. בקרות לדוגמא:

155.1. שימוש בהגנה פיזית ולוגית על התקנים וסביבות המשמשים לאחסון וליצירת מפתחות קריפטוגרפיים, ליצירת סיסמאות ללקוח, ולהצפנה ולפתיחת ההצפנה.

155.2. שימוש בשיטות קריפטוגרפיות לשמירה על סודיות המפתחות הקריפטוגרפיים.

155.3. החלפה תקופתית של המפתחות הקריפטוגרפיים בהתאם לסיכון.

155.4. הגדרת נהלים ברורים לתהליך ביטול של מפתחות קריפטוגרפיים.

155.5. יישום טכניקות לזיהוי כל ניסיון להחלפה לא מאושרת של המפתחות הקריפטוגרפיים.

בקרות מחזור חיים על פתרונות טכנולוגיים לאבטחת מידע (סעיף 129 להוראה)

156. הסעיף קובע כי רמת היישום של בקרות מחזור החיים על הפתרונות הטכנולוגיים תותאם לרמת ההסתמכות של התאגיד הבנקאי על הפתרון הטכנולוגי בהגנה על נכסי המידע שלו, כך שככל שההסתמכות גבוהה יותר, כך בקרות מחזור החיים לגבי אותו פתרון טכנולוגי תיושמנה באופן הדוק יותר.

157. הסעיף קובע כי בין בקרות מחזור החיים על פתרונות טכנולוגיים לאבטחת מידע ייכללו אמצעים המספקים התרעה במידה והפתרונות הטכנולוגיים לאבטחת מידע אינם פועלים כראוי, וזאת באופן עקבי לדרישת ההוראה בסעיף 114.13, לכלול בקרות המוודאות באופן רציף את פעילותן של בקרות אבטחת המידע המיושמות (Continuous Control Monitoring).

פיתוח על ידי משתמשי קצה - תהליכים לזיהוי ולהערכת חשיפה לסיכון (סעיף 130.1 להוראה)

158. הטכנולוגיות הקיימות כיום מאפשרות למשתמשי קצה לפתח ולקנפג (To Configure – להגדיר תצורה) תוכנה לצורך מיכון תהליכים עסקיים שוטפים או לצורך פישוט תהליכי קבלת החלטות (לדוגמא, באמצעות גיליונות אלקטרוניים, בסיסי נתונים מקומיים). מקרים כאלו בהם מערך טכנולוגיית המידע אינו מעורב נקראים גם טכנולוגיית מידע צללים (Shadow IT). הסיכון, בין היתר, הוא שבקרות מחזור החיים המיושמות בתאגיד הבנקאי לא תתאמנה למקרים כאלו, וכתוצאה מכך ניתן יהיה להגיע למידע רב המסווג כרגיש מסביבות שאינן מבוקרות.

מערכות מורשת (Legacy) (סעיף 131 להוראה)

159. נכסי מידע שהוטמעו בטרם החלת המסגרת לניהול אבטחת המידע והגנת הסייבר הנהוגה באותה עת, נדרשים לעמוד בעקרונות ובדרישות אבטחת המידע והגנת הסייבר של אותה המסגרת. אם לא ניתן ליישם לגבי אותם נכסי מידע את העקרונות והדרישות כאמור, על התאגיד הבנקאי לשקול להחליפם או לטפל בהם בהתאם למדיניות לחריגה ממסגרת לניהול אבטחת המידע והגנת הסייבר שקבע לעניין זה.

טכנולוגיות חדשות (סעיף 132 להוראה)

160. סעיף 132.1 להוראה עוסק בהכנסה לשימוש של טכנולוגיות חדשות בסביבת הייצור, בעוד שסעיף 132.2 להוראה עוסק בבחינת טכנולוגיות חדשות (שאינן עומדות בתנאים המפורטים בסעיף 132.1 להוראה) בסביבת ניסוי ייעודית או בסביבת ייצור ייעודית מגודרת ("ארגז חול"). בהקשר של בחינת טכנולוגיות חדשות בסביבת ניסוי ייעודית או בסביבת ייצור ייעודית (סעיף 132.2 להוראה) יש לשים לב למכתב הפיקוח על הבנקים מס' ח-390 מיום 23/6/19 בנושא: "עידוד חדשנות בבנקים ובסולקים".

עבודה מרחוק (סעיפים 134 – 133 להוראה)

161. כאמור, המונח "נכסי מידע" מתייחס גם לתדפיסים, בין אם התדפיס מצוי במשרדי התאגיד הבנקאי ובין אם התדפיס הוצא על ידי עובד לרבות עובד חיצוני וזמני, לצורך עבודתו בביתו או בכל מקום אחר מחוץ לכותלי התאגיד הבנקאי.

בנוסף, מאחר ותדפיס הינו סוג של מסמך, הרי שגם הנחיות הוראת ניהול בנקאי תקין מס' 356 בנושא: "הוצאת מסמכים ממשרדי התאגידים הבנקאיים" יחולו עליו בהתאם לעניין.

קישוריות התאגיד הבנקאי לרשתות ציבוריות (סעיף 135 להוראה)

162. למען הסר ספק, רשת האינטרנט הינה סוג של רשת ציבורית.

163. להלן דוגמא למנגנונים הנדרשים בסעיף לצורך הגנה על נוכחותו המקוונת של התאגיד הבנקאי: נקיטת אמצעים לאיתור התחזות לאתר האינטרנט שלו, ומתן כלים מתאימים ללקוח לצורך וידוא זהות האתר שלו.

164. בין הסיכונים הכרוכים בפעילותו של התאגיד הבנקאי ברשתות החברתיות ניתן למנות סיכונים בתחומים הבאים: זיהוי ואימות לקוח (התחזות באמצעות מידע שהושג מהרשת החברתית), פרסום מידע, הונאות, חדירת וירוסים מהרשתות וכד'.

<u>פרק ט' - הערכת אפקטיביות בקרות אבטחת מידע</u>

מיפוי בקרות אבטחת המידע ובדיקתן (סעיף 136 להוראה)

165. התאגיד הבנקאי נדרש למפות את כל בקרות אבטחת המידע המיושמות לרוחב הארגון, ולקבוע תוכנית בדיקות שתתקף את אפקטיביות התכנון, היישום והתפעול שלהן על בסיס מתמשך.

"תוכנית בדיקת שיטתית" – תוכנית המסודרת ומבוצעת על פי שיטה או סדר קבוע מראש שהוגדרו על ידי התאגיד הבנקאי.

תדירות והיקף הבדיקות (סעיף 137.1 להוראה)

166. תדירות והיקף הבדיקות יתוכננו כך שיוודאו שחלק מספק מתוך כלל בקרות אבטחת המידע בתאגיד הבנקאי ייבדק לפחות אחת לשנה, על מנת שהתאגיד הבנקאי יוכל להניח את דעתו שבקרות אלו נותרו אפקטיביות.

בנוסף, בעת קביעת התדירות וההיקף כאמור, יתחשב התאגיד הבנקאי, בין היתר, במידת הקריטיות והרגישות של נכס המידע עבורו נועדו הבקרות, וכן בהשלכות אפשריות של התממשות אירוע אבטחת מידע בנכס המידע עבורו נועדו הבקרות.

בכל מקרה, כל בקרת אבטחת מידע תיבדק לפחות אחת לשלוש שנים.

בדיקת אפקטיביות הבקרות (סעיף 137.2 להוראה)

167. בנוסף לביצוע בדיקות בהתאם לתוכנית הבדיקות, יבצע התאגיד הבנקאי בדיקות על אפקטיביות בקרות אבטחת המידע, בין היתר, בכל מקרה של שינויים מהותיים בנכס המידע, בסביבה הטכנולוגית בה התאגיד הבנקאי פועל, או בשל פגיעויות ואיומים חדשים שהתגלו, בין היתר, בשל אירועי אבטחת מידע שהתרחשו.

בקרות הקשורות לנכסי מידע החשופים לסביבות שבהן התאגיד הבנקאי לא יכול לאכוף את מדיניות אבטחת המידע והגנת הסייבר שלו (סעיף 137.3 להוראה)

168. סביבות שבהן התאגיד הבנקאי לא יכול לאכוף את מדיניות אבטחת המידע והגנת הסייבר שלו הן למשל סביבה החשופה לאינטרנט, ולמשל סביבה המספקת קישוריות לצד ג' וללקוחות.

קביעת סוגי הבדיקות (סעיף 138.1 להוראה)

169. בפני התאגיד הבנקאי עומד מגוון רחב של כלים לבדיקת בקרות אבטחת מידע ובכל בדיקה עליו להתאים את הכלי המתאים לבקרה הנבדקת, תוך התחשבות בפרקטיקה המקובלת באותה עת. להלן דוגמאות למטרות בקרה, לבקרות אבטחת מידע המתאימות למטרות אלו, ולכלים שבאמצעותם ניתן לבדוק ולהעריך את האפקטיביות שלהן:

מטרת הבקרה	דוגמאות לבקרות	דוגמאות לכלים באמצעותם ניתן לבדוק ולהעריך את הבקרה
הגבלת גישה לנכסי מידע בהתבסס על תפקיד המשתמש ועיקרון מתן מינימום הרשאות (Least Privileged)	ניהול זהויות וגישה (IAM- Identity and Access Management), זיהוי ואימות המשתמש, אבטחה פיזית, מודעות עובדים והדרכת עובדים	מבדקי הנדסה חברתית (social engineering)
אימות משתמש ברמה התואמת את רגישות נכס המידע אליו הוא מבקש לגשת	מדיניות סיסמאות, מערכות זיהוי ואימות	ביקורות על גישת משתמשים בהתאם לרגישות נכס המידע.

מטרת הבקרה	דוגמאות לבקרות	דוגמאות לכלים באמצעותם ניתן לבדוק ולהעריך את הבקרה
הגנה על הרשתות מפני תעבורה שאינה מורשית	Firewalls, נתבים, הפרדת רשתות	בדיקות חדירה
הגנה על מערכות מפני מתקפות זדוניות	שימוש בתוכנות לגילוי והסרה של תוכנות זדוניות (Anti-malware), תוכנות לסינון תכנים בדוא"ל ובאינטרנט	בדיקת התנהגות תוכנות לגילוי והסרה של תוכנות זדוניות מול מדגם של נוזקות דמי, בדיקות קונפיגורציה.
הגנה על תקשורת בין מערכות לרבות העברת מידע, מפני גישה ושימוש בלתי מורשים	הצפנה, ניהול מפתחות	בדיקת ניהול המפתחות.
זיהוי מהיר של גישה ושימוש בלתי מורשים	לוגים, מערכת SIEM (Security Information and Event management), מצלמות אבטחה, מערכת לאיתור ניסיונות חדירה IDS-Intrusion) Detection System), כלים לזיהוי פגיעה בשלמות נכס המידע (Integrity change detection solutions), ניתוח אירועים ונהלי אסקלציה	ניסיונות חדירה מבוקרים לרבות טכניקות מתקדמות יותר דוגמת מבדקי "צוות אדום".
יישום תוכנה מאובטחת	תהליך של פיתוח תוכנה מאובטחת, פרקטיקות מתאימות לרכישה ולהטמעת תוכנה	סקר תיכון (Design review), ניסיונות חדירה מבוקרים, סקר קוד (Code review), ניתוח תעבורת הרשת, בדיקת התנהגות המערכת ויכולת ההתאוששות שלה בעת תקלה (Fault testing), בדיקות תוכנה אוטומטיות

מטרת הבקרה	דוגמאות לבקרות	דוגמאות לכלים באמצעותם ניתן לבדוק ולהעריך את הבקרה
		בהן מוכנס ערך לא צפוי למערכת (fuzzing).
מענה שיטתי לאירועי אבטחת מידע	כתיבת מדריכים לצורך מתן מענה לאירועי אבטחת מידע, ניהול משברים, תוכנית המשכיות עסקית	קיום תרגילים מסוג Table top – משחקי תפקידים כהכנה לשעת חירום.
שרידות המערכות לאחר כשל באחד מהרכיבים	פתרונות גיבוי מסוג Active-Active או Active-Passive, פתרונות מסוג Sandbox (סביבה מגודרת שמאפשרת לתוכנית לגשת רק למשאבים מסוימים ואשר שומרת שהבעיות שקרו בסביבה הזו לא ישפיעו על שאר סביבות המערכת), יישום Zero trust architecture (ארכיטקטורה המבוססת על העיקרון לפיו לא ניתן לסמוך על אף גורם המבקש להתקשר עם הארכיטקטורה, גם לא מתוך הארגון)	ביצוע בדיקות Chaos monkey testing, סקירת ארכיטקטורת המערכת, בדיקת התנהגות המערכת ויכולת ההתאוששות שלה בעת תקלה (Fault Testing), בדיקת יכולת המערכת להקצות משאבים נוספים ולהעביר את המשך הפעילות למערכת גיבוי בזמן תקלה (Failover testing).
התאוששות תחת כל תרחיש סביר	תוכנית להתאוששות מאסון, הסדרים ובדיקות התאוששות מאסון. בקרות למניעת גישה בלתי מורשית לסביבת הגיבוי.	בדיקת התוכנית. ניסיונות חדירה מבוקרים לסביבת הגיבוי.
בקרות יישום המפחיתות את הסיכון לפגיעויות חדשות כתוצאה משינויים במערכת,	שימוש בפיתוח תוכנה מאובטחת, בקרות שינויים, הקשחת מערכות	בדיקת ניהול השינויים, סקירת קוד המערכת, בדיקת ארכיטקטורת המערכת,

מטרת הבקרה	דוגמאות לבקרות	דוגמאות לכלים באמצעותם ניתן לבדוק ולהעריך את הבקרה
המערכות מפותחות כך שעקרונות אבטחת המידע והגנת הסייבר משולבים בהן כבר בשלב תכנון המערכת (secure by design)		בדיקות תוכנה אוטומטיות בהן מוכנס ערך לא צפוי למערכת (fuzzing).
זיהוי וטיפול מהיר בפגיעויות חדשות	ניהול טלאים, ניהול תצורה	סריקה למציאת פגיעויות, ניסיונות חדירה מבוקרים.
זיהוי וטיפול מהיר באיומים חדשים	מודיעין, אסטרטגית אבטחת מידע והגנת הסייבר, מערכת SIEM	סקר בלתי תלוי של יכולת אבטחת מידע.

הסתמכות התאגיד הבנקאי על בדיקות להערכת אפקטיביות הבקרות של צד ג' על נכסי מידע המנוהלים באמצעותו (סעיף 140)

170. הערכת אפקטיביות הבקרות על נכסי מידע המנוהלים באמצעות צד ג' צריכה להתבצע בהתאם לעקרונות שלפיהם מתבצעת הערכת אפקטיביות הבקרות בתאגיד הבנקאי.

ככל שהתאגיד הבנקאי מעריך שקיימים פערים ביישום העקרונות כאמור אצל צד ג', עליו לבחון את המשך השימוש בשירותיו.

חלק ה' – ניהול אירועים

פרק י' – ניטור מערך טכנולוגיית המידע

כללי (סעיפים 143 – 141 להוראה)

171. חלק מאירועי הכשל הטכנולוגי ומאירועי אבטחת מידע (להלן: "אירועים") ניתן למנוע או לכל הפחות לאתר בשלבים מוקדמים, בין היתר, באמצעות זיהוי מוקדם של דפוסים חשודים ושל חריגות בפעילות הן של מערכות הבנק והן של הלקוחות.

כך למשל, זיהוי של שרת המגיע לניצול של 80% מהזיכרון שלו יכול למנוע קריסת המערכת באופן בלתי צפוי. וכך למשל, זיהוי של כמות גדולה מאוד של פניות לשרת בזמן נתון מעבר למקובל או זיהוי של פעילות חשודה של לקוח, יכול להצביע על תחילתה של מתקפת סייבר על הארגון.

בהתאם לכך, התאגיד הבנקאי נדרש לקבוע מדיניות ונהלים לזיהוי בעיות מתהוות או חריגות (אנומליות) על מנת למנוע מהן באופן פרואקטיבי מלהתפתח לאירועים כאמור. המדיניות והנהלים יגדירו תהליכי ניטור מתמשכים שיפעלו במהלך כל השבוע, 24 שעות ביממה, ואשר

ינטרו בין היתר, את פעילות וביצועי המערכות – בהיבט שליטה ובקרה, את הפעילות העסקית ובכלל זה את הטרנזקציות, את פעילותם של גורמים רלבנטיים פנימיים (כמו בעלי תפקידים בפונקציות העסקיות ובפונקציות האדמיניסטרטיביות של מערך טכנולוגיית המידע) וחיצוניים, וכן ינטרו איומים פנימיים וחיצוניים פוטנציאליים.

172. כחלק מאמצעי הניטור, נדרש התאגיד הבנקאי לקיים מערך ניטור ובקרה, שיהיה מאויש באופן רציף (24X7X365), יקבל דיווחים בזמן אמת מהמערכות השונות, לרבות מערכות תפעוליות ועסקיות (שו"ב) ומערכות אבטחת מידע והגנת הסייבר שונות (דוגמת SIEM/SOC). מערך זה יזהה אינדיקטורים להתרחשותם של אירועי כשל טכנולוגי ושל אירועי אבטחת מידע, וייזום פעילויות דיווח ותגובה במידת הצורך.

173. בקרות ניטור לדוגמא שהתאגיד הבנקאי יכול לשקול ליישמן כדי למלא אחר דרישות הפרק:

- יצירת פרופיל פעילות לרשתות ולמשתמשים בצירוף מנגנוני תיעוד לוגים ומנגנוני התרעה, לצורך זיהוי פעילות חריגה.
- סריקה לצורך זיהוי של הכנסת חומרה או תוכנה בלתי מורשים לרשת או שינויים בקונפיגורציה שלא אושרו.
- יישום חיישנים המזהים חריגה מסף שהוגדר מראש תוך מתן התרעות מתאימות.
- תיעוד לוג והתרעות על גישה למידע רגיש או ניסיונות גישה שלא צלחו.
- ניטור מוגבר של משתמשים בעלי הרשאות גישה מיוחדות (דוגמת: מנהלי מערכת).

<u>פרק י"א - ניהול אירועים ובעיות</u>

יישום תהליך לניהול אירועים (סעיף 144 להוראה)

174. אירוע מתרחש כאשר יש אירוע כשל טכנולוגי או אירוע אבטחת מידע כהגדרתם בסעיף 11 להוראה.

175. התהליך לניהול אירועים נועד להשיג שתי מטרות עיקריות:

175.1. ניטור האירוע במהלך התרחשותו על מנת לצמצם את השפעתו ולחדש את הפעילות של התאגיד הבנקאי במהירות.

175.2. תיעוד האירוע לצורך למידה והפקת לקחים.

המסגרת לניהול אירועים ובעיות (סעיף 146 להוראה)

נהלים לניהול בעיות (סעיף 146.5 להוראה)

176. ניהול בעיות (Problem Management) הינו תהליך שנועד להשיג פתרון שורש לבעיות חוזרות ובעיות מורכבות.

דיווח אירועים בעלי פוטנציאל להשפעה שלילית גבוהה על נכסי מידע קריטיים ורגישים (סעיף 146.6.1 להוראה)

177. לאירועים מסוימים קיים פוטנציאל להתפתח למשבר. תאגיד בנקאי יעדכן את ההנהלה הבכירה, הנהלת טכנולוגיית המידע, והגורמים הפנימיים הרלבנטיים האחרים, באשר לסטטוס של אירועים אלו על מנת שההחלטות בנוגע להפחתת ההשפעה של האירוע תוכלנה להתקבל במהירות, למשל החלטה על הפעלת התוכנית להתאוששות מאסון.

דיווח בעת התרחשות אירוע משמעותי (סעיף 146.6.2 להוראה)

178. בעוד שסעיף 146.6.1 להוראה עוסק באירועים משמעותיים שהתרחשו ושיש להם פוטנציאל להשפעה שלילית גבוהה על נכסי מידע קריטיים ורגישים של התאגיד הבנקאי, הרי שסעיף זה עוסק באירועים כאמור, שהפוטנציאל שיש להם להשפעה שלילית גבוהה על נכסי מידע קריטיים ורגישים התממש בפועל.

יובהר כי ייתכנו אירועי כשל טכנולוגי או אירועי אבטחת מידע שיוגדרו על ידי התאגיד הבנקאי כמשמעותיים ואשר בהתרחשותם החליט התאגיד הבנקאי שיש למסור בגינם דיווח מיידי לדירקטוריון, אולם הם לא יהיו חייבים בדיווח לפיקוח על הבנקים על פי הקריטריונים לדיווח המפורטים בהוראה 366.

למען הסר ספק, אירוע כשל טכנולוגי משמעותי ואירוע אבטחת מידע משמעותי בסעיף זה, אינם בהכרח האירועים נשוא סעיף 41.7 להוראה זו.

תוכניות תגובה (סעיף 146.7 להוראה)

179. ראוי כי רמת הפירוט של תוכניות התגובה תהיה כזו שתצמצם למינימום את הדרישות לקבלת החלטות במהלך אירוע ואשר תספק בהירות בנוגע לתפקידים ותחומי האחריות של כל גורם במהלך התרחשותו של אירוע.

שיתוף פעולה ותיאום מול צד ג' (סעיף 146.10 להוראה)

180. תוכניות תגובה נדרשות, בין היתר, לצורך הפחתת ההשפעות הקשורות לאירוע ועל מנת לוודא שהשירות חוזר להיות פעיל. תוכניות התגובה משתלבות בדרך כלל עם התוכנית להמשכיות עסקית. בהתאם לכך קובע הסעיף שבמקרה בו תאגיד בנקאי משתמש בצד ג', עליו לדאוג לתיאום בין תוכניות התגובה שלו לבין תוכניות התגובה של צד ג' וכן בין תוכניות התגובה שלו לבין תוכנית ההמשכיות העסקית של צד ג'.

אירועי אבטחת מידע (סעיפים 152 – 147 להוראה)

181. לאירועי אבטחת מידע בכלל, ולמתקפות סייבר בפרט קיימים מאפיינים ייחודיים הבאים לידי ביטוי בין היתר, בתוקף מתוחכם ובדינמיות של האירוע. לא תמיד אירועים אלו מזוהים בזמן, המידע על חלק מאירועים אלו מגיע ממקורות חיצוניים, ובדרך כלל הם דורשים תחקיר נוסף על מנת לזהות האם בוצעה בפועל פגיעה באבטחת המידע של התאגיד הבנקאי. בהתאם לכך, להלן דגשים נוספים על אילו שפורטו בסעיפים 146-144 להוראה, שיש ליישם לגבי אירועים מסוג זה.

<u>חלק ו' – שונות</u>

<u>פרק י"ג – ניהול סיכונים מול צדדים שלישיים</u>

סיכוני טכנולוגיית המידע להם חשוף התאגיד הבנקאי מצד ג' (סעיף 155 להוראה)

182. ניהול הסיכונים הקשורים למיקור חוץ יוצר היבט משמעותי נוסף במסגרת העבודה לניהול סיכוני טכנולוגיית המידע של התאגיד הבנקאי. בהתאם לכך, ובנוסף לדרישות היציבותיות הקשורות למיקור חוץ המפורטות בהוראת נ.ב.ת. מס' 359A בנושא: "מיקור חוץ" ובהוראה 362, הוראה זו מרחיבה ומוסיפה, במגוון נושאים.

ההנחיות בנושאים אלו שויכו לסעיפים הרלבנטיים בהוראה, כך למשל, חובתו של הדירקטוריון להתייחס בכל דיוניו גם להיבטים העולים משימוש התאגיד הבנקאי בצד ג' - מופיעה בסעיף 18 להוראה זו. בנספח להוראה מובא ריכוז של ההנחיות לצורך נוחות הקורא.

<u>פרק י"ד – ניהול המשכיות עסקית (BCM)</u>

כללי

183. פרק זה מתמקד בהיבטים הטכנולוגיים הרלבנטיים לתוכנית ההמשכיות העסקית.

הדרישה לבניית תוכנית המשכיות עסקית מופיעה בהוראה 355.

בהוראה זו ניתנו דגשים והרחבות לסוגיות טכנולוגיות הקשורות להמשכיות עסקית, ובפרט בנוגע לתוכנית ההתאוששות מאסון (DRP).

184. חלק מהמונחים בהם משתמש הפרק מופיעים גם בהוראה 355. סעיף 156 להוראה קובע כי משמעות מונחים אלו בהוראה דנן, תהיה בהתאם למשמעותם בהוראה 355. מונחים לדוגמא: "תהליך או שירות חיוני", "זמן התאוששות (RTO-Recovery Time)", "שיבוש תפעולי משמעותי", "תוכנית המשכיות עסקית (BCP)".

ניתוח השלכות עסקיות (BIA) (סעיף 158 להוראה)

185. דוגמא לתכנון מתאים: תכנון עם יתירות של רכיבים קריטיים מסוימים למניעת שיבושים הנגרמים על ידי אירועים המשפיעים על רכיבים אלה.

קביעת תוכנית ההמשכיות העסקית (סעיף 160 להוראה)

186. תיעדוף לדוגמא: ביצוע מעקף עבור טרנזקציה קריטית בזמן שמתבצעות פעולות תיקון.

187. תאגיד בנקאי יכול להשתמש גם בהערכת הסיכונים שנעשית בהתאם לסעיף 46 להוראה, ואינו חייב להשתמש בהערכת סיכונים ייעודית עבור סעיף זה.

מיקוד תוכנית ההתאוששות מאסון (סעיף 163.1 להוראה)

188. תוכנית ההתאוששות מאסון תתייחס הן להתאוששות התפקוד של התהליכים והשירותים החיוניים בהתאמה ליעדי השירות שקבע התאגיד הבנקאי (לרבות ביצוע מעקף לתהליך הטכנולוגי לצורך עמידה ביעדי השירות), והן להשבת התהליכים הטכנולוגיים ונכסי המידע למצבם בטרם אירע השיבוש התפעולי.

תיעוד וזמינות תוכנית ההתאוששות מאסון (סעיף 163.2 להוראה)

189. תאגיד בנקאי נדרש להיערך למצבים שונים בהם תידרש תוכנית תגובה והתאוששות זמינה ונגישה. כך למשל: ניתן לשקול שמירת עותק של התוכנית גם על גבי מסמכים, על מנת לשמור על זמינות ונגישות התוכנית במצב בו אירע כשל באמצעי הטכנולוגי עליו היא נשמרת.

<u>פרק ט"ו - בנק חוץ</u>

תחולת ההוראה על בנק חוץ (סעיף 170 להוראה)

190. "מערך טכנולוגיית המידע המקומי, לרבות הממשקים של מערך זה עם מערך הבנק בחו"ל" הינו כל מרכיב ממערך טכנולוגיית המידע כהגדרתו בסעיף 11 להוראה אשר נמצא בשליטתו של בנק החוץ, לרבות רכיבי ממשקים שבשליטתו של בנק החוץ.

191. ככל שבנק חוץ סבור כי סעיפים מסוימים בהוראה זו אינם ישימים לגביו, קיימת בפניו האפשרות לעשות שימוש בסעיף 5 להוראת נ.ב.ת. מס' 100 בנושא: "מבוא לקובץ הוראות ניהול בנקאי תקין" (להלן: "הוראה 100"), ולפנות לפיקוח על הבנקים על מנת לתאם את דרך יישומם לגביו. ציפיית הפיקוח על הבנקים היא כי השימוש בסעיף 5 להוראה 100 ייעשה במקרים חריגים בלבד.

<u>נושאים נוספים</u>

טיפול בהוראות ואישורים קיימים

192. החל ממועד תחילת הוראה זו יבוטלו הוראות ניהול בנקאי תקין מס' 357 בנושא: "ניהול טכנולוגיית המידע", מס' 361 בנושא" "ניהול הגנת הסייבר", מס' 363 בנושא: "ניהול סיכוני סייבר בשרשרת אספקה", וכן יבוטלו מכתבי הפיקוח בנושאים הבאים:

192.1. "ניהול נכסי טכנולוגיית המידע (IT)" מס' 09LM0643 מיום 24.8.09.

192.2. "ניהול תהליכים מרכזיים בתחום טכנולוגיית המידע" מס' 09LM0650 מיום 14.9.09.

193. האישורים שניתנו על ידי המפקח או מי מטעמו בהתאם להוראות ניהול בנקאי תקין שבוטלו כאמור לעיל, יוותרו בתוקפם. ככל שתאגיד בנקאי אוחז באישור המתיר פעילות שאינה עומדת בהנחיות הוראה זו, יודיע על כך למפקח על הבנקים עד למועד תחילת ההוראה כמפורט בסעיף 194 להלן, על מנת לברר את עניינו.

תחילה והוראות מעבר

194. תחילת האמור בהוראה זו הוא 18 חודשים מיום פרסומה.

195. לעניין חוזים שנכרתו לפני מועד פרסום ההוראה - במועד החידוש הקרוב של החוזה ולא יאוחר מ-3.5 שנים ממועד התחילה (ובסך הכל – 5 שנים), יתאים התאגיד הבנקאי את החוזים להוראה ככל שהדבר נדרש.

196. תאגיד בנקאי רשאי לפעול ע"פ הוראה זו במועד מוקדם יותר מהמועד הקבוע בסעיף 194 לעיל, ובלבד שיחולו עליו גם סעיפים 192 ו - 193 לעיל מאותו מועד.

197. בחר תאגיד בנקאי לעשות כאמור בסעיף 196 לעיל, יודיע למפקח על הבנקים 30 יום קודם למועד כאמור.

עדכון הקובץ

198. מצ"ב דפי עדכון לקובץ ניהול בנקאי תקין. להלן הוראות העדכון:

להוציא עמוד	להכניס עמוד
-----	364-1-57 [1] (11/24)

בכבוד רב,

דניאל חחיאשוילי

המפקח על הבנקים

ניהול סיכוני טכנולוגיית המידע, אבטחת המידע והגנת הסייבר

חלק א' - פתיחה

פרק א': כללי

מבוא

1. טכנולוגיית המידע מהווה כיום את התשתית המרכזית לפעילותו העסקית של התאגיד הבנקאי ומוגדרת כגורם מאפשר בסקטור הפיננסי. בהתאם לכך, ניהול נאות של טכנולוגיית המידע הינו קריטי לביצועי התאגיד הבנקאי ולהצלחתו, והתאגיד הבנקאי נדרש לנהל את סיכוני טכנולוגיית המידע כחלק בלתי נפרד מהפעילות העסקית שלו ומעבר להיבטים טכנולוגיים גרידא.
תאגידים בנקאיים נשענים באופן גובר והולך על טכנולוגיה על מנת לעמוד במגוון האתגרים הניצבים בפניהם בשוק התחרותי. מערכות התאגיד הבנקאי נותנות שירות לקווי העסקים בתוך התאגיד הבנקאי ולציבור הרחב, ומקושרות אל צדדים שלישיים, ובכלל זה לתאגידים פיננסיים אחרים (לדוגמא: חברות טכנולוגיה פיננסית). תפקיד טכנולוגיית המידע הוא, בין היתר, ליצור את הקישור המתאים בין התשתיות, המערכות ושאר הרכיבים הרלבנטיים, באופן שיתמוך בצורה המיטבית ביותר במתן מוצרים ושירותים קיימים ובהצעת מוצרים ושירותים חדשים. זאת ועוד, מידע מדויק, הניתן בזמן ובאופן מאובטח, הינו קריטי לעמידה בדרישות העסקיות של התאגיד הבנקאי ולקוחותיו.
קצב השינויים המהיר בתשתית הטכנולוגית, החדשנות המתמדת במתן שירותים בנקאיים ללקוחות, זמינותם של השירותים "בכל עת, בכל מקום", ההסתמכות על מגוון ערוצי תקשורת (אינטרנט, מובייל, וכד') גם לצורך קישוריות לתאגידים פיננסיים אחרים, הקישור של מערכות מידע ותיקות של התאגיד הבנקאי לתשתיות מחשוב מודרניות ו"פתוחות", כמו גם התלות הגוברת בשירותי מחשוב ותקשורת המסופקים על ידי צד שלישי – כל אלו ועוד מאתגרים את ניהול טכנולוגיית המידע של התאגידים הבנקאיים, יוצרים כר נרחב מאוד להתגברות סיכוני טכנולוגיית המידע הכוללים בתוכם פגיעויות ואיומי אבטחת מידע, לרבות סיכוני סייבר (להלן: "סיכוני אבטחת מידע"), מגבירים את הצורך בתהליך נאות של ניהול סיכונים המותאם לסיכונים מסוג זה, ומחייבים מומחיות, ידע וכישורים מתאימים לניהול של טכנולוגיית המידע ושל הסיכונים הכרוכים בה.

2. סיכוני טכנולוגיית המידע ובכללם סיכוני אבטחת מידע עלולים להוות סיכון יציבותי משמעותי לתאגיד הבנקאי, ולסכן את המשך קיומו. בהתאם לכך, הפיקוח על הבנקים סבור כי, ניהול נאות של סיכוני טכנולוגיית המידע הינו מרכיב בסיסי לצורך השגת היעדים האסטרטגיים, התאגידיים, והתפעוליים של התאגיד הבנקאי. לפיכך, מצופה מהתאגיד הבנקאי לשמור באופן נאות על נכסי המידע שלו, ולהטמיע תרבות ארגונית המקדמת את ניהול סיכוני טכנולוגיית המידע ובכלל זה אבטחת המידע. הוראה זו באה, בין היתר, להבטיח כי התאגיד הבנקאי ינקוט בצעדים לבניית עמידות מתאימה בפני התממשות סיכוני טכנולוגיית מידע, וזאת על ידי ניהול אפקטיבי של מערך טכנולוגיית המידע, ושמירה שוטפת של יכולת אבטחת מידע נאותה המתאימים להתמודדות עם סיכוני אבטחת מידע הניצבים בפניו. ניהול ושמירה נאותים כאמור, יסייעו לתאגיד הבנקאי לשמור

ככל הניתן על עמידתו בהתחיבויותיו הפיננסיות לכל בעלי העניין שלו בעת התרחשות אירועים בהם מתממש סיכון טכנולוגיית המידע.

3. ההוראה מתייחסת לניהול סיכוני הסייבר כחלק בלתי נפרד מניהול כלל סיכוני אבטחת המידע הניצבים בפני התאגיד הבנקאי, אולם יש להדגיש כי למתקפות סייבר קיימים מאפיינים ייחודיים שעל התאגיד הבנקאי להתחשב בהם, בבואו לוודא כי אמצעי הבקרה אותם הוא מיישם במטרה להפחית את סיכוני אבטחת המידע מתאימים גם לצורך הפחתת סיכוני הסייבר, וביניהם:

3.1. ההתפתחות הטכנולוגית והטרנספורמציה הדיגיטלית בשנים האחרונות מאפשרות כר נרחב יותר להיווצרות חולשות נוספות במערכי ההגנה של התאגיד הבנקאי אשר מרחיבות את משטחי התקיפה עליו וחושפות אותו לסיכוני סייבר משמעותיים. בד בבד, חל גידול משמעותי במתקפות סייבר בכלל ועל גופים פיננסיים בפרט, הן בהיקף המתקפות, הן בבחינת גורמי האיום והן בהיבטי תחכום וזמינות כלי התקיפה.

3.2. המניעים למתקפות סייבר הם שונים ויכולים לנבוע, בין היתר, מפשיעה כלכלית או מנסיבות גיאו-פוליטיות. לכן, קיימת חשיבות בהבנת תפיסת מרחב האיום, תרחישי הייחוס הרלוונטיים ויכולות ההגנה הנדרשות בהתאם.

3.3. קיימת חשיבות לייצר יכולת זיהוי מוקדם בזמן אמת של מתקפות סייבר, אולם קשה לזהות או לצפות אותן, וקשה גם לכמת את היקף הנזק לו הן גורמות, בעיקר ביחס לנזקים הלא ישירים. זאת ועוד, באירוע קיצון מתקפות סייבר עלולות אף לפגוע ביציבותו של התאגיד הבנקאי. לפיכך נדרש שימוש בטכנולוגיות מתקדמות והפעלה של צוותים מיומנים אשר ידעו כיצד להתמודד עם המתקפה ויוכלו להעריך את מידת הנזק אשר עלול להיגרם.

3.4. מעורבות יריב (חיצוני או פנימי לתאגיד הבנקאי) במתקפת סייבר, שיכול גם בזמן אירוע להגיב על פעולות הגנה שמבצע התאגיד הבנקאי. לכן, קיימת חשיבות להכרת יכולות היריבים הפוטנציאליים וכוונותיהם, ולהיערכות להתמודדות מולם.

3.5. מתקפות הסייבר יכולות לפגוע בתהליכי ניהול הסיכונים ובהסדרי ההמשכיות העסקית של התאגיד הבנקאי, ובמקרים מסוימים יכולות אף לגרום להתפשטות הנזק גם למערכות הגיבוי של התאגיד הבנקאי.

3.6. המקור של חלק ממתקפות הסייבר הינו בגורמים חיצוניים לתאגיד הבנקאי ובכלל זה צדדים שלישיים כהגדרתם בהוראה זו. לאור השוני שיש לעיתים בין יכולות ההגנה של תאגידים בנקאיים לבין יכולות ההגנה של חלק מהארגונים המקושרים לתאגיד, נדרש התאגיד הבנקאי ליישם תהליכי בקרה וניהול סיכונים מתאימים כנגד סוג זה של מתקפות.

3.7. במישור התודעתי, יכולים להתקיים מצגי שווא של מתקפות סייבר גם אם אין תקיפה בפועל. זאת באמצעות הטעיה או ניצול מצבי כשל שאינם קשורים למתקפה כלשהי והצגת המצב שנוצר כתקיפת סייבר שהצליחה. הנזק שנגרם לארגון בעקבות פרסומים מוטעים בדבר מתקפת סייבר עלול לפגוע במוניטין של הארגון אבל עלול גם לגרום לפגיעה בפעילות העסקית בעקבות הפעלת נהלי תגובה לטיפול בחשד לאירוע סייבר.

4. מטרתה המרכזית של ההוראה היא ניהול נאות ואפקטיבי של טכנולוגיית המידע תוך צמצום למינימום של האירועים בהם מתממש סיכון טכנולוגי ומתקיימת פגיעה בסודיות (הן בהיבטי

אבטחת מידע והן בהיבטי הגנת הפרטיות של לקוחות הבנק ועובדיו), בשלמות או בזמינות של נכסי מידע.

5. חלק מנכסי המידע של התאגיד הבנקאי מנוהלים באמצעות צד ג', בין אם בחצרות התאגיד הבנקאי ובין אם מחוצה להן. למען הסר ספק, אין הבדל בין נכסי מידע המנוהלים על ידי התאגיד הבנקאי עצמו לבין נכסי מידע של התאגיד הבנקאי המנוהלים באמצעות צד ג'. ההוראה חלה על כל נכסי המידע של התאגיד הבנקאי לרבות אלו המנוהלים באמצעות צד ג', בהתאם לקבוע בה ובכלל זה בהתאם לקריטיות ולרגישות של נכסי המידע, וללא תלות במהותיות צד ג' המנהל אותם או במהותיות הפעילות המבוצעת באמצעות צד ג'.
בכל מקרה של צד ג' שהוא גם "נותן שירות" לפי הוראת נ.ב.ת. מס' 359A בנושא: "מיקור חוץ" (להלן: "הוראה 359A"), תחולנה הנחיות הוראה זו בנוסף להנחיות הוראה 359A.

6. יישום (Implementation) נאות של נכסי מידע, שימוש נאות בהם, והגנה נאותה עליהם יכולים לסייע לתאגיד הבנקאי לזהות ולאתר סיכונים לחוסן התפעולי שלו, מגבירים את יכולתו של התאגיד הבנקאי לעמוד בשיבושים או כשלים, ומפשטים את תהליך זרימת המידע בתאגיד הבנקאי והדיווח לגורמים הרלבנטיים, כך שיתאפשר תהליך קבלת החלטות אפקטיבי במהלך שיבושים או כשלים אלו. הנחיות הוראה זו מקדמות את האבטחה והחוסן התפעולי של נכסי המידע בהתאמה להוראות נ.ב.ת. הקיימות של הפיקוח על הבנקים הרלבנטיות לניהול הסיכון התפעולי (ראה בעניין זה גם את סעיף 9 להלן).

7. הוראה זו תעסוק בשלושה נושאים מרכזיים:

7.1. ממשל תאגידי בתחום טכנולוגיית המידע כחלק מהממשל התאגידי הכולל של התאגיד הבנקאי.

7.2. תהליכי ניהול סיכוני טכנולוגיית המידע כחלק מתהליכי ניהול הסיכון התפעולי וההמשכיות העסקית בתאגיד הבנקאי.

7.3. תהליכי ניהול סיכוני אבטחת מידע.

8. ניהול סיכוני טכנולוגיית המידע ובכלל זה סיכוני אבטחת מידע בתאגיד בנקאי יתבסס על העקרונות המפורטים בהוראה זו. עקרונות אלו מקנים את הגמישות הנדרשת לאור קצב השינויים המהיר בתחום טכנולוגיית המידע, אבטחת מידע והגנת הסייבר, ומתוך הכרה שלכל תאגיד בנקאי פרופיל סיכונים ייחודי, הדורש התאמה של תוכנית ניהול הסיכונים ואופן יישום העקרונות למאפייני הפעילות ולצרכים העסקיים הפרטניים של כל תאגיד בנקאי.

9. ניהול סיכוני טכנולוגיית המידע ובכלל זה סיכוני אבטחת מידע בתאגיד הבנקאי, מהווה חלק מהמערך הכולל של ניהול סיכונים בכלל, וסיכונים תפעוליים בפרט. משכך הוראה זו תואמת את הוראת ניהול בנקאי תקין מס' 310 בנושא: "ניהול סיכונים" (להלן: "הוראה 310") הקובעת עקרונות יסוד לניהול ולבקרת הסיכונים בראייה משולבת וכלל תאגידית (Firm Wide Risk Management), את הוראת ניהול בנקאי תקין מס' 350 בנושא: "ניהול סיכונים תפעוליים" (להלן: "הוראה 350") הקובעת עקרונות כאמור בדגש על הסיכון התפעולי, ומשלימה את הוראת ניהול בנקאי תקין מס' 355 בנושא: "ניהול המשכיות עסקית" (להלן: "הוראה 355") בהיבטים הטכנולוגיים.

תחולה

10. לעניין תחולת ההוראה:

10.1. הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א 1981 (להלן: "תאגיד בנקאי"):

10.1.1. תאגיד בנקאי;

10.1.2. תאגיד כאמור בסעיפים 11 (א) (3א) ו-(3ב);

10.1.3. תאגיד כאמור בסעיף 11 (ב);

10.1.4. נותן שירותי תשלום בעל חשיבות יציבותית כהגדרתו בסעיף 36ט.

10.2. על אף האמור בהוראה זו, כאשר תאגיד בנקאי נותן גישה לנכסי המידע שלו לצד ג', שהינו תאגיד בקבוצה הבנקאית אליה משתייך התאגיד הבנקאי, יפעל התאגיד הבנקאי בהתאם להערכת הסיכונים שלו.

הגדרות

11. בהוראה זו למונחים הבאים תהיה המשמעות כמפורט להלן:

אבטחת מידע – ההגנה על נכס מידע מפני פעולות בלתי מורשות - לרבות גישה, שימוש, חשיפה, שיבוש פעילות, הוספה, מחיקה או העתקה - במטרה לספק סודיות, שלמות וזמינות (CIA - Confidentiality, Integrity, Availability).
בכלל פעולות בלתי מורשות תבואנה גם פעולות שיש למשתמש הרשאה מיכונית לבצען, אולם הדבר נאסר עליו באמצעות דין, נוהל, פרקטיקת עבודה, הגדרת תפקיד וכד'.

איום אבטחת מידע – נסיבות או אירוע שיש בהם פוטנציאל לניצול פגיעות באבטחת המידע.

אימות (Authentication) – אישור הזיהוי של הגורם המבקש גישה.

אירוע אבטחת מידע – אירוע שבו נפגעה אבטחת המידע או שהיה בו פוטנציאל לפגיעה (אירוע "כמעט ונפגע" - Potential Compromise) באבטחת המידע, ובכלל זה מתקפת סייבר.

אירוע כשל טכנולוגי – אירוע, התרחשות או תוצאה שאינם צפויים או שאינם מתוכננים כחלק מהפעילות התקינה של התאגיד הבנקאי ואשר יש להם או עלולה להיות להם השפעה משבשת על הפעילות התקינה של מערך טכנולוגיית המידע או של השירותים הניתנים על ידו. אירוע כשל טכנולוגי אינו כולל אירוע אבטחת מידע כהגדרתו בהוראה זו.

ארכיטקטורה – האופן שבו התכנון האסטרטגי של רכיבי התשתית הטכנולוגית מאורגנים ומשולבים לצורך השגת יעדי התאגיד הבנקאי ותמיכה שוטפת בהם.

בקרת אבטחת מידע אמצעי למניעה, לזיהוי או לתגובה לצורך הפחתת ההסתברות להתרחשות אירוע אבטחת מידע או לצורך הפחתת ההשפעה של אירוע כזה.

דלף מידע חשיפה בלתי מורשית של מידע רגיש, לרבות בשל טעות אנוש, שתוצאתה היא אובדן סודיות המידע.

הרשאה מתן גישה לנכסי מידע עבור המבקש בהתבסס על צרכיו של התאגיד הבנקאי ורמת אבטחת המידע הנדרשת.

זיהוי (בהקשר של זיהוי ואימות גורם המבקש גישה – Identification) קביעה מי או מה מבקש גישה.

זמינות (Availability) נגישות ואפשרות לשימוש במידת הצורך.

חוסן תפעולי יכולת התאגיד הבנקאי לספק פעולות חיוניות לאורך תקופה של שיבוש. יכולת זו מאפשרת לתאגיד הבנקאי לזהות ולהגן על עצמו מפני איומים וכשלים פוטנציאליים, להגיב ולהסתגל לאירועים משבשים, כמו גם להתאושש וללמוד מהם, על מנת למזער את השפעתם על אספקת פעילותו הקריטית בתקופה של שיבוש.

טכנולוגיית המידע, מערך טכנולוגיית המידע תשתית טכנולוגית או הארכיטקטורה הטכנולוגית של התאגיד הבנקאי או שירותים (וביניהם: שירותי מחשוב ענן, שירותי Help desk, שירותים מקצועיים אחרים התומכים בכל נקודה במחזור החיים של נכס המידע) או משאבים נלווים (משאבים שאינם נכללים תחת תשתית טכנולוגית והנדרשים לצורך התשתית הטכנולוגית, הארכיטקטורה והשירותים, דוגמת מבנה וחשמל).

יכולת אבטחת מידע כלל המשאבים, המיומנויות והבקרות הנדרשים לצורך קיום פעילות אבטחת מידע נאותה בסביבת סיכונים משתנה.

מודעות מצבית (Situational Awareness) היכולת לקלוט את המידע בנוגע לאיומים, למטרות, ולסביבה, לפרש אותו נכון ובזמן, כדי להחליט על פעולה המועילה להשגת המשימה, לפעול ולקלוט איך השתנתה תמונת המצב בעקבות הפעולה וחוזר חלילה.

מידע רגיש מידע שסווג כרגיש על-ידי התאגיד הבנקאי, לרבות "מידע בעל רגישות מיוחדת" כהגדרתו בחוק הגנת הפרטיות, תשמ"א – 1981 (להלן: "חוק הגנת הפרטיות").

מערכת אוסף של רכיבי מחשוב או תקשורת ומשאבים אחרים שמאורגנים יחד לצורך איסוף, עיבוד, תחזוקה, שימוש, שיתוף או הפצה של מידע, ואשר תומכים באחד או יותר מהיעדים הפונקציונליים של הארגון.

מתקפת סייבר אירוע אשר במהלכו מתבצעת מתקפה (גם אם לא נגרם נזק בפועל) על נכסי מידע דיגיטליים של התאגיד הבנקאי על ידי, או מטעם, יריבים (חיצוניים או פנימיים לתאגיד הבנקאי).

נזק	תוצאה בלתי רצויה, לרבות שיבוש/הפרעה/השבתה של פעילות ; גניבת נכס ; איסוף מודיעין ; פגיעה במוניטין/אמון הציבור.
נכסי מידע	מידע ותשתית טכנולוגית, לרבות נתונים (גם על גבי עותק דיגיטלי וגם על גבי תדפיסים).
נקודת התאוששות רצויה (RPO-Recovery Point Objective)	מרכיב של יעד התאוששות. פרק הזמן המקסימלי שהוגדר בסיבולת הסיכון לאובדן מידע ונתונים עבור תהליך או שירות מסוים.
נתונים במנוחה	נתונים הנמצאים במערכות דוגמת קבצים המאוחסנים על גבי שרת, בסיסי נתונים, מדיות גיבוי ופלטפורמות אחסון כגון ענן, כמו גם נתונים הנמצאים במכשירי קצה דוגמת מחשבי מחברת (Notebook), מחשבים אישיים, מכשירי אחסון ניידים, ומכשירים ניידים.
נתונים בתנועה	נתונים המועברים על גבי רשת ציבורית או רשת שהתאגיד הבנקאי לא יכול לאכוף את מדיניות אבטחת המידע והגנת הסייבר שלו בה או רשת פרטית של התאגיד הבנקאי.
סודיות (Confidentiality)	גישה מוגבלת למורשים בלבד.
סיכון אבטחת מידע	איום אבטחת מידע או פגיעות אבטחת מידע. סיכון זה כולל בתוכו גם את סיכון הסייבר.
סיכון טכנולוגיית המידע	הסיכון להפסד כתוצאה מפגיעה בסודיות, כשל בשלמות של נכס מידע, חוסר התאמה או חוסר זמינות של נכס מידע או חוסר יכולת לשנות את מערך טכנולוגיית המידע בזמן ובעלויות סבירים כאשר הדרישות העסקיות והסביבתיות משתנות. סיכון זה כולל בתוכו גם את סיכון אבטחת המידע.
סיכון סייבר	אפשרות להתממשות סיכון אבטחת מידע באמצעות מתקפת סייבר.
פגיעות אבטחת מידע (Vulnerability)	חולשה בנכס מידע או בבקרת אבטחת מידע אשר ניתן לנצלה לצורך פגיעה באבטחת המידע.
פרויקט טכנולוגיית המידע	כל פרויקט או חלק ממנו, שבו מערכות ושירותי טכנולוגיית מידע עוברים שינוי, מוחלפים, מוצאים מכלל שימוש או מיושמים. פרויקט טכנולוגיית מידע יכול להיות חלק מתוכניות טכנולוגיית מידע רחבות יותר או חלק משינוי עסקי.
צד ג'	צד ג' שיש לו גישה לנכס מידע של התאגיד הבנקאי.
קבוצה בנקאית	תאגיד בנקאי, תאגיד בנקאי השולט בו ותאגידים בשליטת מי מהם.
קריטיות (בהקשר של המונח קריטיות בצמידות למונח רגישות)	ההשפעה הפוטנציאלית של העדר זמינות.
רגישות	ההשפעה הפוטנציאלית של אובדן סודיות או אובדן שלמות.
שלמות (Integrity)	דיוק, מהימנות והגנה מפני שינוי או מחיקה בלתי מורשים.

תפעול

הניהול הטקטי של נכסי מידע ואספקה שוטפת של שירותים לצורך תיעוד, העברה, עיבוד ואחסון של טרנזקציות ומידע התומכים בכלל התהליכים העסקיים של התאגיד הבנקאי.

תשתית טכנולוגית

חומרה, ציוד נלווה (כולל ציוד היקפי להדמיה, קלט, פלט, והתקני אחסון הדרושים לאבטחה ומעקב), ציוד היקפי הנשלט באמצעות מחשב (כולל בקרות סביבתיות (ראה סעיף 122 להלן) ובקרות גישה פיסית), רשתות ותקשורת, תוכנות, בסיסי נתונים, קושחה ואמצעים דומים, והתקנים (devices), אשר מאפשרים את התפעול והניהול של טכנולוגיית המידע.

חלק ב' - ממשל תאגידי ומסגרת לניהול סיכונים

פרק ב': ממשל תאגידי

12. תאגיד בנקאי יישם ממשל תאגידי נאות ואפקטיבי בתחום טכנולוגיית המידע הכולל מסגרת מתאימה לניהול סיכוני טכנולוגיית המידע ובכלל זה מסגרת לניהול סיכוני אבטחת מידע וסייבר, שיבטיחו בין היתר, את האמינות והחוסן התפעולי של מערך טכנולוגיית המידע ואת אבטחת המידע שלו. במסגרת זו יוקצו תפקידים ותחומי אחריות ברורים ונאותים לדירקטוריון וועדותיו, להנהלה הבכירה, לנושאי תפקידים רלבנטיים ולעובדים.

דירקטוריון

13. הדירקטוריון אחראי לניהול סיכוני טכנולוגיית המידע בתאגיד הבנקאי. בין היתר, עליו לוודא שאבטחת המידע ואמצעי הבקרה האחרים המיושמים בתאגיד הבנקאי תואמים את היקף הסיכונים לנכסי המידע שלו, בצורה המאפשרת את המשך פעילותו הנאות.

14. הדירקטוריון יתווה את אסטרטגיית טכנולוגיית המידע לרבות התיאבון לסיכון, תוך ייחוד דיון מעמיק לאסטרטגיית אבטחת המידע והגנת הסייבר הכלולה בה. מטרת האסטרטגיה בין היתר, להגן על התאגיד הבנקאי מפני סיכוני טכנולוגיית המידע קיימים ומתהווים, לרבות הסיכונים הקשורים לאבטחת מידע, והכל בהתאם לקבוע בהוראת נ.ב.ת. מס' 301 בנושא: "דירקטוריון" (להלן: "הוראה 301"), הוראה 310, ובהוראה 350. אסטרטגיית טכנולוגיית המידע תהיה בהלימה לאסטרטגיה העסקית הכוללת של התאגיד הבנקאי ותגדיר מתווה מקיף המנחה את ניהול הטכנולוגיה, וניהול אבטחת מידע והגנת הסייבר בתאגיד הבנקאי. המתווה יכיל יעדים ותוכניות ברמת על עבור כל תחומי טכנולוגיית המידע המשפיעים על התאגיד הבנקאי, ובכלל זה ניהול עלויות, ניהול הון אנושי, ניהול חומרה ותוכנה, ניהול צד שלישי, ניהול סיכונים, זיהוי איום הייחוס הרלבנטי לתאגיד הבנקאי וכל שאר השיקולים במערך טכנולוגיית המידע הארגוני.
בין היתר, תתייחס האסטרטגיה לאופן שבו מערך טכנולוגיית המידע יתאים את עצמו לצורך תמיכה והשתתפות ביישום האסטרטגיה העסקית של התאגיד הבנקאי, לרבות בעקבות שינויים במבנה הארגוני, שינויים בטכנולוגיית המידע, ותחומי מפתח בהם מתקיימים קשרים עם צדדים שלישיים. האסטרטגיה תעודכן על פי הצורך ובכל מקרה לפחות פעם בשלוש שנים.

15. הדירקטוריון ידון, יחליט ויאשר את מדיניות ניהול טכנולוגיית המידע ואת המסגרת לניהול סיכוני טכנולוגיית המידע, הנגזרות מהאסטרטגיה שקבע, ויוודא כי ההנהלה הבכירה של התאגיד הבנקאי תנקוט בצעדים הנדרשים ליישומן, והכל בהתאם למפורט בהוראה זו, וכן בהוראות 301, 310, ו-350. בדיוניו כאמור לעיל, ייחד הדירקטוריון דיון מעמיק עבור המסגרת לניהול אבטחת מידע והגנת הסייבר ובכלל זה עבור המדיניות לניהול אבטחת מידע והגנת הסייבר.

16. הדירקטוריון יוודא כי:

16.1. היקף ומיומנות כוח האדם בכל שלושת קווי ההגנה בתאגיד הבנקאי מספיקים בכדי לתמוך על בסיס מתמשך בצרכי מערך טכנולוגיית המידע, בתהליכי ניהול סיכוני טכנולוגיית המידע, ובכדי ליישם את אסטרטגיית טכנולוגיית המידע של התאגיד הבנקאי.

16.2. התקציב המוקצה להשגת מטרות אלו עבור כל שלושת קווי ההגנה הינו מספק.

17. לצורך מילוי חובותיו בהתאם לסעיפים 15-13 לעיל, על הדירקטוריון להבין את פעילות טכנולוגיית המידע בתאגיד הבנקאי ואת הסיכונים הכרוכים בה, ולהנהיג תהליכים לניטור ולמדידת אפקטיביות היישום של אסטרטגיית טכנולוגיית המידע. בין היתר יפעל הדירקטוריון:

17.1. לקדם ממשל תאגידי אפקטיבי בתחום טכנולוגיית המידע ובכלל זה בהיבטי ניהול סיכוני טכנולוגיית המידע.

17.2. להגדיר להנהלה את האופן בו הוא מבקש להיות מעורב בהתייחס לנושאי טכנולוגיית המידע השונים ובכלל זה סיכוני טכנולוגיית המידע בתאגיד הבנקאי, לרבות העקרונות להאצלת תחומי אחריות, אסקלציה של סיכונים, וסוגיות הדורשות דיווח לרבות אופן, היקף, תוכן ותדירות הדיווח.

17.3. לוודא את נאותות יכולת אבטחת המידע של התאגיד הבנקאי ואת נאותות ההשקעה בה, בהתייחס לסיכוני אבטחת המידע העומדים בפני התאגיד הבנקאי ובהתייחס למימוש האסטרטגיה שנקבעה.

17.4. לוודא קיומם של תהליכים שנועדו להבטיח את ציות התאגיד הבנקאי לדרישות חוקיות ורגולטוריות בתחום טכנולוגיית המידע, אבטחת המידע והגנת הסייבר, ולמסגרת לניהול סיכוני טכנולוגיית המידע שנקבעה, תוך שהוא מתבסס, בין היתר, על בדיקות של פונקציית הציות וסקירות של ההנהלה הבכירה לרבות מנהל הסיכונים הראשי והמבקר הפנימי.

17.5. לקיים דיון לפחות אחת לשנה, ובמידת הצורך לאתגר את ההנהלה בנוגע לאפקטיביות מדיניות ניהול טכנולוגיית המידע, אפקטיביות המסגרת לניהול סיכוני טכנולוגיית המידע ובכלל זה אפקטיביות סביבת הבקרה ושלמות נכסי המידע. לצורך כך על הדירקטוריון, בין היתר, לבדוק את נאותות כיסוי הבדיקות (ראה פרק ט' להלן: "הערכת אפקטיביות בקרות אבטחת מידע") הנעשות על סביבת הבקרה, חריגות מהותיות מהמסגרת והטיפול שניתן להן, ניתוח אירועים בהם התממש סיכון טכנולוגיית המידע ובכלל זה אירועי אבטחת מידע, והשוואה לפרקטיקות מקובלות. בהתרחש אירוע המחייב את ההנהלה הבכירה בדיווח מיידי לדירקטוריון, יתקיים דיון בנושא בהקדם (ראה סעיף 19.9 להלן).

17.6. לוודא כי תוכנית העבודה של הביקורת הפנימית לפי הוראת נ.ב.ת. מס' 307 בנושא: "פונקציית ביקורת פנימית" (להלן: "הוראה 307") ולפי הוראה זו, כוללת גם תוכנית עבודה מתאימה באשר לבחינת נאותות מערך טכנולוגיית המידע ונאותות המסגרת לניהול סיכוני טכנולוגיית המידע, וכי יש לביקורת הפנימית את המיומנויות, הקיבולת והיכולות המתאימות כדי לספק חוות דעת עצמאית באשר לבחינות נאותות כאמור.
הדירקטוריון יגבש את עמדתו באשר לאפקטיביות הבקרות בהתבסס על ממצאי הביקורת הפנימית, וישקול במידת הצורך שימוש בחוות דעת מומחה נוספות או באמצעים אחרים.

17.7. לדון, להחליט, ולאשר אחת לשנה את תוכנית העבודה השנתית והרב שנתית בתחום טכנולוגיית המידע, ובכלל זה תוכנית העבודה לטיפול בסיכוני טכנולוגיית המידע.

17.8. לקיים פגישה עם מנהל טכנולוגיית המידע ופגישה עם מנהל הגנת הסייבר ואבטחת המידע, לפחות אחת לשנה, כדי לסייע לדירקטוריון בביצוע הערכת האפקטיביות של המסגרת לניהול טכנולוגיית המידע והמסגרת לניהול סיכוני טכנולוגיית המידע בתאגיד הבנקאי.

18. בכל דיוניו בהתאם לסעיף 17 לעיל, יתייחס הדירקטוריון גם להיבטים העולים משימוש התאגיד הבנקאי בצד ג' לצורך ניהול נכסי המידע שלו.

הנהלה בכירה

19. ההנהלה הבכירה של התאגיד הבנקאי אחראית ליישום ותחזוקה של סביבת פעילות מאובטחת ונאותה התומכת ביעדי התאגיד הבנקאי ובמטרותיו, והעומדת בחוק וברגולציה הרלבנטיים. בכלל זה תהיה ההנהלה הבכירה אחראית לביצועי מערך טכנולוגיית המידע ולתפעול השוטף שלו. לשם כך על הנהלת התאגיד הבנקאי:
19.1. ליישם ממשל תאגידי אפקטיבי בתחום טכנולוגיית המידע, ובכלל זה להקצות תחומי אחריות וסמכות בהתאם לעקרונות שהתווה הדירקטוריון, לרבות הסדרת אופן הפיקוח והתיאום בין מנהל טכנולוגיית המידע ומנהל הגנת הסייבר ואבטחת המידע לבין הגורמים השונים המרכיבים את התחום והממשקים המשותפים של הגורמים השונים עמם ועם גורמים חיצוניים;
19.2. לתכנן וליישם מסגרת לניהול סיכוני טכנולוגיית המידע;
19.3. לגבש מדיניות ניהול טכנולוגיית מידע ומדיניות ניהול סיכוני טכנולוגיית המידע;
19.4. לגבש תוכנית עבודה שנתית ורב שנתית בתחום טכנולוגיית המידע ולניהול הסיכונים הקשורים בה, ולהקצות משאבים מתאימים ליישומה;
19.5. לשמור על יכולת אבטחת מידע ועדכונה לצורך המשך פעילותו הנאותה של התאגיד הבנקאי.
19.6. לתעדף ולתאם בין הפונקציה האחראית על טכנולוגיית המידע לבין קווי העסקים;
19.7. להתוות ולבצע מעקב אחר תיאום פעילות אבטחת המידע מול גורמי ניהול סיכון פנימיים (ראה סעיף 30 להלן) וגורמים חיצוניים (ראה סעיף 28.14 להלן), ולוודא קיום תהליך לקבלה, ניתוח ותגובה של מידע מודיעיני על איומים ופגיעויות, כגון באמצעות השתתפות בתוכניות לשיתופי פעולה בנושא;
19.8. לקבל ולספק דיווח תקופתי לדירקטוריון בנוגע לנושאים הבאים:
19.8.1. סיכוני טכנולוגיית המידע ודרכי ההתמודדות איתם.
19.8.2. אירועי אבטחת מידע רלבנטיים (פנימיים וחיצוניים) וניתוח המשמעויות הנגזרות מהם.
19.8.3. מימוש אסטרטגיית טכנולוגיית המידע.
19.8.4. שינויים מהותיים בתחום טכנולוגיית המידע;
19.9. לספק דיווח מיידי לדירקטוריון באשר לחריגה מהותית ממדיניות ניהול טכנולוגיית המידע ומהמסגרת לניהול סיכוני טכנולוגיית המידע (ראה סעיף 22 להלן), התפתחויות שליליות מהותיות בסיכוני טכנולוגיית המידע, שינוי מהותי בנכסי המידע או בסביבה העסקית, ובאשר לאירועי כשל טכנולוגי ואירועי אבטחת מידע שיש להם פוטנציאל להשפעה משמעותית על התאגיד הבנקאי;
19.10. ליישם תהליכים לצורך ווידוא ציות לדרישות חוקיות ורגולטוריות בתחום טכנולוגיית המידע ובכלל זה למסגרת לניהול אבטחת המידע;

19.11. לקבוע תהליך למיפוי נכסי המידע וליישום אמצעים להפחתת סיכונים כמפורט בפרק ג': "מסגרת לניהול סיכוני טכנולוגיית המידע (כללי)";

19.12. לוודא קיומם של נהלים ותהליכים מתאימים להעסקת עובדים ולהדרכתם על מנת לשמור על כשירות העובדים והתאמתם לתפקידיהם כמפורט בפרק ד': "הגורם האנושי – הדרכה ומודעות משתמשים";

19.13. להסדיר את תהליך הערכת אפקטיביות בקרות אבטחת מידע כמפורט בפרק ט': "הערכת אפקטיביות בקרות אבטחת מידע";

19.14. לקבוע עקרונות לניהול אירועים ובעיות כמפורט בפרק י"א: "ניהול אירועים ובעיות";

20. ההנהלה הבכירה תוודא אפקטיביות של המדיניות לניהול טכנולוגיית המידע ושל המסגרת לניהול סיכוני טכנולוגיית המידע לאורך זמן, ובכלל זה:

20.1. ההנהלה הבכירה של התאגיד הבנקאי תקיים דיונים תקופתיים לווידוא המשך הרלבנטיות והנאותות של הצעדים שננקטו למימוש אסטרטגיית טכנולוגיית המידע לרבות האסטרטגיה לניהול סיכוני טכנולוגיית המידע כמפורט להלן:

20.1.1. דיון שנתי במדיניות ניהול טכנולוגיית המידע ובתוכנית העבודה, ביכולת אבטחת המידע, במדיניות אבטחת המידע והגנת הסייבר, ובתוכנית העבודה.

20.1.2. דיונים תקופתיים בעמידה ביעדי תוכנית העבודה.

20.1.3. לפחות דיון אחד בשנה בנוגע לתהליך למיפוי נכסי המידע וליישום בקרות טכנולוגיות לרבות בקרות אבטחת מידע.

20.1.4. דיונים נוספים במקרים הבאים: כאשר עולים ממצאים מהותיים מתהליך הניטור של המסגרת לניהול טכנולוגיית המידע, שינויים מהותיים במסגרת ניהול סיכוני טכנולוגיית המידע ונושאים נוספים מהותיים כגון: התקשרויות משמעותיות.

20.2. במידת הצורך, תעדכן ההנהלה הבכירה את מדיניות ניהול טכנולוגיית המידע ואת המסגרת לניהול סיכוני טכנולוגיית המידע לרבות הנהלים, הבקרות ותהליך הערכת הסיכונים, תוך הקצאת המשאבים הנדרשים לביצוע החלטותיה ותוך שמירה על יכולת אבטחת המידע בהתאם להחלטות הדירקטוריון.

21. ההנהלה הבכירה של התאגיד הבנקאי תמנה מנהל טכנולוגיית המידע, מנהל הגנת הסייבר ואבטחת המידע כמפורט בסעיפים 23 ו - 28 להלן, ותדאג כי יהיו להם המשאבים הנדרשים לביצוע תפקידיהם.

22. בהתאם למדיניות שתיקבע, ההנהלה הבכירה של התאגיד הבנקאי תקבע נהלים למצבים מיוחדים בהם צפויה או התרחשה חריגה ממדיניות ניהול טכנולוגיית המידע ומהמסגרת לניהול סיכוני טכנולוגיית המידע שיכללו התייחסות, בין היתר, להיבטים הבאים: תיעוד החריגות, סמכויות לאישור חריגות, תוקף האישור לחריגה, ובקרה על החריגות שאושרו. כאשר מאושרת חריגה ידאג התאגיד הבנקאי לקיומן של בקרות מפצות.

מנהל טכנולוגיית המידע

23. תאגיד בנקאי ימנה מנהל שיהיה חבר הנהלה אשר יישא באחריות מפורשת למכלול הנושאים הקשורים לטכנולוגיית המידע (להלן: "מנהל טכנולוגיית המידע"). מנהל זה יהיה בעל הכשרה מקצועית מתאימה וניסיון מוכח בתחום טכנולוגיית המידע וניהולו.

24. במסגרת אחריותו למכלול הנושאים הקשורים לטכנולוגיית המידע, יהיה מנהל טכנולוגיית המידע אחראי על מערך טכנולוגיית המידע ובכלל זה תפעולו וניהולו השוטף, אבטחת המידע שלו וחוסנו התפעולי, לרבות:

24.1. פיתוח ויישום של אסטרטגיית טכנולוגיית המידע בשים לב להנחיות הדירקטוריון וההנהלה הבכירה.

24.2. גיבוש ויישום מדיניות ניהול טכנולוגיית המידע (ראו סעיף 54 להלן) בשים לב להנחיות הדירקטוריון וההנהלה הבכירה.

24.3. גיבוש ויישום תוכנית עבודה שנתית ורב שנתית של מערך טכנולוגיית המידע – ראה בעניין זה גם את סעיף 64 להלן בנושא: "תהליך תכנון והשקעה בטכנולוגיית המידע".

24.4. ניהול תקציב טכנולוגיית המידע;

24.5. ניהול ביצועים של המשאבים בתחום טכנולוגיית המידע;

24.6. ניהול קיבולת - ראה סעיף 61.6 להלן;

24.7. ניהול רכישות והשקעות בתחום טכנולוגיית המידע;

24.8. פיתוח מקצועי והדרכות מתאימות;

24.9. יישום ארכיטקטורת טכנולוגיית המידע - ראה סעיף 57 להלן;

24.10. תמיכה בפעילותם של קווי העסקים, בין היתר בהיבטים של אבטחת מידע, חוסן תפעולי, ודיווח על סיכוני טכנולוגיית המידע, והכל תוך התאמת מערך טכנולוגיית המידע לדרישות העסקיות;

24.11. קיום תהליכים ובקרות נאותים בכדי לוודא שכל סיכוני טכנולוגיית המידע מזוהים, מנותחים, נמדדים, מנוטרים, מנוהלים, מדווחים ונשמרים בתוך מגבלות התיאבון לסיכון של התאגיד הבנקאי ובכדי לוודא שהפרויקטים והמערכות אותם הוא מספק והפעילויות אותן הוא מבצע תואמים לדרישות מגורמים חיצוניים ופנימיים;

24.12. תכלול ובקרה של אירועי כשל טכנולוגי בתאגיד הבנקאי.

25. מנהל טכנולוגיית המידע לא יישא באחריות נוספת שיש בה כדי להפריע לתפקודו.

26. על תאגיד בנקאי להודיע 30 יום מראש למפקח על הבנקים על עזיבתו הצפויה של מנהל טכנולוגיית המידע, ובנוסף בעת מינוי ממלא מקום בפועל לתקופה של למעלה מחודש ימים, 30 יום קודם לתחילת כהונתו של ממלא המקום או עם ההחלטה על כך, כמאוחר מביניהם.

מנהלי קווי העסקים

27. למנהלי קווי העסקים, בנוסף למנהל טכנולוגיית המידע ולמנהל הגנת הסייבר ואבטחת מידע, ישנה אחריות בתחום טכנולוגיית המידע. חלוקת האחריות בין מנהלי קווי העסקים לבין מנהל טכנולוגיית המידע לבין מנהל הגנת הסייבר ואבטחת המידע, תקבע בהתאם למדיניות התאגיד הבנקאי ולתהליכים שייקבעו. נושאים לדוגמא לחלוקת אחריות:

27.1. קביעת תהליכים ליידוע של מערך טכנולוגיית המידע בצרכים העסקיים, בדוחות הנדרשים ממערכות המידע, ובתוכניות להשקת מוצרים חדשים;

27.2. וידוא כי תוכניות הפיתוח של מערך טכנולוגיית המידע מתועדפות, מתוקצבות ותואמות את האסטרטגיה העסקית של קו העסקים;

27.3. וידוא שקיים גיבוי מתאים למערכות ולתהליכים הטכנולוגיים התומכים בפעילות קו העסקים;

27.4. שמירת תיעוד של התהליכים בקו העסקים והודעה למנהל הגנת הסייבר ואבטחת המידע על כל שינוי בתהליכים אלו;

27.5. ביצוע בדיקות נאותות על צד ג' שהתאגיד הבנקאי מעוניין להשתמש בשירותיו, וניטור פעילותם של צדדים שלישיים קיימים;

27.6. דיון עם מנהל הגנת הסייבר ואבטחת המידע על סיכוני אבטחת מידע המובנים ביוזמות העסקיות החדשות של קו העסקים.

מנהל הגנת הסייבר ואבטחת המידע

28. תאגיד בנקאי ימנה עובד בכיר כמנהל הגנת הסייבר ואבטחת המידע שיהיה כפוף לחבר הנהלה ואחראי לניטור ולעמידת התאגיד הבנקאי במסגרת לניהול אבטחת המידע, ובכלל זה יהיה אחראי לפיקוח ולדיווח בנוגע לניהול ולהפחתת סיכוני אבטחת מידע, ותחום פעילותו יקיף את כל קווי העסקים של התאגיד הבנקאי והיבטים עסקיים-אסטרטגיים חוצי-ארגון. בין יתר תפקידיו:

28.1. תכלול היבטי ניהול אבטחת מידע והגנת הסייבר בתאגיד הבנקאי;

28.2. ייעוץ להנהלה הבכירה בתחום ניהול אבטחת המידע והגנת הסייבר;

28.3. סיוע להנהלה בגיבוש ויישום מדיניות אבטחת המידע והגנת הסייבר (ראו סעיף 106 להלן);

28.4. גיבוש מתודולוגיה תאגידית לניהול סיכוני אבטחת מידע;

28.5. פיתוח, מעקב אחר יישום, וניטור של תוכנית מקיפה ופרטנית להתמודדות התאגיד הבנקאי עם סיכוני אבטחת המידע כאמור בהוראה זו;

28.6. הגדרת עקרונות ונהלי עבודה למימוש בקרות אבטחת המידע והגנת הסייבר;

28.7. ייזום, קידום והטמעת תהליכים להגברת מודעות המשתמשים לאבטחת מידע והגנת הסייבר ובכלל זה תוכניות הדרכה מתאימות בנושאי סיכוני אבטחת מידע, לדירקטוריון, להנהלה הבכירה, לעובדים, לצדדים שלישיים וללקוחות (ראו פרק ד' להלן: "הגורם האנושי – הדרכה ומודעות משתמשים");

28.8. קביעת מסגרת הדיווחים שיקבל מגורמים שונים בתאגיד הבנקאי;

28.9. ייזום בדיקות להערכת אפקטיביות בקרות אבטחת המידע כמפורט בפרק ט' להלן: "הערכת אפקטיביות בקרות אבטחת מידע";

28.10. ביצוע בדיקות נאותות בהיבטי אבטחת מידע והגנת הסייבר על צדדים שלישיים, וניטור פעילותם של צדדים שלישיים קיימים בהיבטים כאמור;

28.11. התעדכנות בסיכוני אבטחת המידע ביוזמות עסקיות חדשות וקביעת דרכים להפחתתם, באמצעות דו שיח עם הנהלות קווי העסקים, ובאמצעים אחרים;

28.12. התעדכנות בתהליכי זרימת המידע, הסיכונים למידע בתהליכים אלו, ואמצעי אבטחת המידע והגנת הסייבר הנדרשים, באמצעות דו שיח עם הנהלות קווי העסקים, ובאמצעים אחרים;

28.13. פיתוח מדדים רלבנטיים, הכנת דוחות ומתן דיווחים בהתאם לנדרש בהוראה 350;

28.14. תיאום וקישור בנושאי אבטחת המידע והגנת הסייבר, לרבות שיתוף מידע ומודיעין לצורך הגנתי מול גורמים חיצוניים בהתאם לדין. גורמים חיצוניים לדוגמא: גורמי רגולציה, גורמי חקירה ואכיפה, מערך הסייבר הלאומי, המרכז לסייבר ורציפות פיננסית במשרד האוצר, גורמי ניהול סיכוני אבטחת מידע מקבילים במגזר הפיננסי, גורמי ניהול סיכונים אצל צדדים שלישיים;

28.15. תכלול ובקרה של ניהול אירועי אבטחת מידע בתאגיד הבנקאי לרבות דיווח על אירועי אבטחת מידע מהותיים לדירקטוריון, להנהלה ולרשויות הרלבנטיות, כמפורט בפרק י"א להלן: "ניהול אירועים ובעיות";

28.16. ייזום וביצוע תרגילים כמפורט בפרק י"א להלן: "ניהול אירועים ובעיות";

28.17. הובלה ותיאום של תהליכים הנוגעים לניהול אבטחת המידע והגנת הסייבר;

28.18. ניתוח אירועי אבטחת מידע משמעותיים בישראל ובעולם, הפקת לקחים ויישום המסקנות הרלבנטיות לתאגיד הבנקאי.

29. למנהל הגנת הסייבר ואבטחת המידע יינתנו מעמד ראוי וסמכויות.

30. מנהל הגנת הסייבר ואבטחת המידע ידאג להקמת ממשקים עם הגורמים השונים המרכיבים את המסגרת לניהול סיכון אבטחת מידע, כגון: יחידות טכנולוגיות, יחידות עסקיות, מנהל סיכונים ראשי, פונקציית ציות, מנהל המשכיות עסקית, הייעוץ המשפטי, הדרכה, משאבי אנוש ובטחון. מנהל הגנת הסייבר ואבטחת המידע יהיה אחראי על תיאום ואינטגרציה בין כל אותם גורמים המרכיבים את המסגרת.

31. מנהל הגנת הסייבר ואבטחת המידע יהיה בעל כישורים מתאימים לביצוע תפקידו, הכשרה מקצועית רלוונטית וניסיון מספק.

32. מנהל הגנת הסייבר ואבטחת המידע ידאג להתעדכן באופן שוטף במתודולוגיות ובטכנולוגיות חדשות לניהול אבטחת המידע, ובכלל זה יקיים קשרים עם גורמים מקצועיים בתחום בתוך ומחוץ למערכת הבנקאית.

33. מנהל הגנת הסייבר ואבטחת המידע לא יישא באחריות נוספת שיש בה כדי להפריע לתפקודו, ותפקידיו ותחומי אחריותו לא יעמידו אותו בניגודי עניינים, ובפרט בכל הקשור לתפקידים ביצועיים בתחום טכנולוגיית המידע.

34. על תאגיד בנקאי להודיע 30 יום מראש למפקח על הבנקים על מינוי מנהל הגנת הסייבר ואבטחת המידע ועל עזיבתו הצפויה, ובנוסף בעת מינוי ממלא מקום בפועל לתקופה של למעלה מחודש ימים, 30 יום קודם לתחילת כהונתו של ממלא המקום או עם ההחלטה על כך, כמאוחר מביניהם.

הפונקציה לניהול סיכונים

35. הפונקציה לניהול סיכונים:

35.1. תפקח ותוודא כי סיכוני טכנולוגיית המידע מנוהלים באופן נאות, בהתאם לעקרונות שהותוו בהוראה 310 והוראה 350.

35.2. מבלי לגרוע מהאמור בסעיף 11(ב) להוראה 310, הפונקציה תהיה עצמאית ובלתי תלויה בקו ההגנה הראשון ובקו ההגנה השלישי, ותפעל בנפרד מתהליכי התפעול של מערך טכנולוגיית המידע.

35.3. מבלי לגרוע מהאמור בסעיף 11(א) להוראה 310, הפונקציה תהיה אחראית, בין היתר:

35.3.1. לסיוע למנכ"ל בגיבוש ותחזוקה של מדיניות, נהלים והנחיות, תוך שיתוף כל הגורמים הרלבנטיים.

35.3.2. לפיתוח ולתחזוקה של מתודולוגיה לניהול סיכון טכנולוגיית המידע ולמדידתו.

35.3.3. לניטור ולבקרה של ציות התאגיד הבנקאי למסגרת העבודה לניהול סיכון טכנולוגיית המידע. הפונקציה תוודא שסיכוני טכנולוגיית המידע, יזוהו, ימדדו, יוערכו, ינוהלו, ינוטרו וידווחו.

תפקיד מרכזי של הפונקציה בתחום סיכוני טכנולוגיית המידע הוא לאתגר את נאותות התשומות של קווי העסקים לניהול סיכוני טכנולוגיית המידע, למדידת הסיכון ולמערכות הדיווח של התאגיד הבנקאי, ואת נאותות התפוקות המתקבלות.

ביקורת פנימית

36. תאגיד בנקאי יכלול, במסגרת פונקציית הביקורת הפנימית, יחידה ארגונית לביקורת טכנולוגיית המידע שלו. האחראי על הביקורת הפנימית בתחום טכנולוגיית המידע יהיה בעל הכשרה מקצועית וניסיון רלבנטיים לביצוע הביקורת בתחום זה.

37. בבניית תוכנית העבודה של הביקורת הפנימית הנדרשת בהתאם להוראה 307, יילקחו בחשבון כלל הפעילות של מערך טכנולוגיית המידע, הממשל התאגידי, הפונקציות והתהליכים בתחום טכנולוגיית המידע לרבות אלו שבתחום אבטחת המידע. התוכנית תכלול בדיקה של התכנון והאפקטיביות של הבקרות הטכנולוגיות לרבות בקרות אבטחת המידע ובכלל זה אלו המיושמות על ידי צד ג' עבור נכסי המידע של התאגיד הבנקאי, באופן בו כל ההיבטים של סביבת הבקרה בתחום טכנולוגיית המידע ייבדקו אחת לתקופה. התדירות בה תבוצע הבדיקה והיקפה, יושפעו מהתוצאה של פגיעה אפשרית בבקרות הטכנולוגיות לרבות באבטחת המידע בהתאם לשיקול דעתה של הביקורת הפנימית, מהיכולת של הביקורת הפנימית להסתמך על בדיקות אחרות שנערכו לגבי אותן בקרות, ומשינויים בפגיעויות ובאיומים או משינויים מהותיים בנכסי המידע.

38. בכל אחד מהמקרים הבאים על הביקורת הפנימית להעריך את היקף ואיכות העבודה שנעשתה על מנת לקבוע את מידת ההסתמכות עליה:

38.1. הסתמכות על עבודה המבוצעת על ידי גורמים אחרים בתאגיד הבנקאי.

38.2. שימוש במיקור חוץ לצורך ביצוע פעילות של הביקורת הפנימית כמפורט בהוראה 307.

38.3. הסתמכות על בדיקות שנערכו על ידי צד ג' לפעילות שהוא מבצע עבור התאגיד הבנקאי.

39. לצורך ביצוע ביקורות בזמן אמת (Objective Assurance) בתחום טכנולוגיית המידע, אבטחת המידע והגנת הסייבר, על הביקורת הפנימית לקבוע מתודולוגיה שתתייחס בין היתר:

39.1. להגדרת פרויקטים טכנולוגיים אסטרטגיים המחייבים ביצוע משימת ביקורת בזמן אמת ולהגדרת אופן מעורבותה לאורך השלבים השונים של מחזור חיי נכס המידע אליו מתייחס פרויקט כאמור.

39.2. להגדרת אופן מעורבותה בזמן אמת בתהליך לניהול אירועים ובעיות שקבע התאגיד הבנקאי – ראה פרק י"א להלן: "ניהול אירועים ובעיות".

פרק ג': מסגרת לניהול סיכוני טכנולוגיית המידע (כללי)

מבנה ויעדים

40. תאגיד בנקאי יקבע מסגרת לניהול סיכוני טכנולוגיית המידע שלו ולצורך כך יגדיר ויקצה תפקידי מפתח ותחומי אחריות, וכן קווי דיווח מתאימים על מנת שהמסגרת תהיה אפקטיבית. מסגרת זו תשולב במלואה בתהליכים הכוללים לניהול סיכונים בתאגיד הבנקאי ותהיה מתואמת עימם.

41. תאגיד בנקאי ינהל את סיכוני טכנולוגיית המידע בשלושת קווי ההגנה הנדרשים לפי הוראה 310 תוך הטמעה ויישום, בין היתר, של המסמכים והתהליכים הבאים:

41.1. אסטרטגיית טכנולוגיית המידע ובכלל זה התיאבון לסיכון עבור סיכוני טכנולוגיית המידע;

41.2. מדיניות ניהול סיכוני טכנולוגיית המידע הנגזרת מהאסטרטגיה;

41.3. זיהוי והערכה של סיכוני טכנולוגיית המידע אליהם חשוף התאגיד הבנקאי;

41.4. הגדרת אמצעים למזעור הסיכון, לרבות בקרות;

41.5. ניטור האפקטיביות של האמצעים למזעור הסיכון וכן ניטור של אירועי כשל טכנולוגי ואירועי אבטחת מידע (ראה פרק י"א להלן: "ניהול אירועים ובעיות"), ונקיטת צעדים לתיקונם של האמצעים לרבות יישום בקרות מתאימות במידת הצורך;

41.6. דיווח להנהלה הבכירה ולדירקטוריון בנוגע לסיכוני טכנולוגיית המידע והבקרות המיושמות;

41.7. זיהוי והערכה של סיכוני טכנולוגיית המידע שנוצרו כתוצאה משינויים מהותיים במערך טכנולוגיית המידע, בתהליכים ובנהלים, או כתוצאה מאירועי כשל טכנולוגי משמעותיים או אירועי אבטחת מידע משמעותיים.

תחומי האחריות ותחומי הפעילות של כל קו הגנה יהיו בהתאם לאמור בהוראות 310 ו – 350.

42. תאגיד בנקאי יוודא שהמסגרת לניהול סיכוני טכנולוגיית המידע הינה מתועדת, ומתעדכנת באופן שוטף בהתאם ללקחים שנלמדו בעת יישומה ובעת הניטור שלה.

זיהוי של פעילויות, תהליכים ונכסי מידע וסיווגם

43. תהליך הזיהוי והסיווג של פעילויות, תהליכים ונכסי מידע יתבצע כדלקמן:

43.1. תאגיד בנקאי יישם תהליך לזיהוי של כל הפעילויות העסקיות, התפקידים והתהליכים התומכים בהם, ליצירת מיפוי שלהם ולשמירה על עדכניותו, לצורך קביעת חשיבותם וקביעת הקשרים ביניהם, וזאת ביחס לסיכון טכנולוגיית המידע.

43.2. על סמך תהליך המיפוי בסעיף 43.1 לעיל, תאגיד בנקאי יישם תהליך לזיהוי (Identification) של כל נכסי המידע שלו, ליצירת מיפוי שלהם ולשמירה על עדכניותו, לרבות אלו המנוהלים באמצעות צד ג'. תהליך המיפוי יכלול גם זיהוי ותיעוד של הקשרים בין נכסי המידע על מנת לסייע, בין היתר, בתגובה לאירועי כשל טכנולוגי ואירועי אבטחת מידע.

43.3. תאגיד בנקאי יסווג את הפעילויות העסקיות, התהליכים התומכים ואת נכסי המידע במונחים של קריטיות ורגישות. סיווג זה ישקף את ההשפעה האפשרית, פיננסית או אחרת, על התאגיד

הבנקאי או על בעלי העניין בו בשל התממשות אירוע כשל טכנולוגי או אירוע אבטחת מידע המשפיע על הפעילות העסקית, התהליך התומך או נכס המידע.

43.4. על התאגיד הבנקאי ליישם תהליך לזיהוי המקרים בהם נדרש שינוי בסיווג של נכסי המידע, של הפעילויות העסקיות, או של התהליכים התומכים, וכן לסיווג נכסי מידע, פעילויות עסקיות ותהליכים תומכים חדשים. תהליך זה יתבצע לפחות אחת לשנה או כאשר נעשים שינויים מהותיים בנכסי מידע, בפעילויות עסקיות ובתהליכים תומכים או בסביבה העסקית בה התאגיד הבנקאי פועל.

מתודולוגיה לזיהוי וסיווג הפעילויות העסקיות, התהליכים התומכים ונכסי המידע

44. התאגיד הבנקאי יקבע מתודולוגיה לזיהוי וסיווג הקובעת עקרונות, בין היתר, באשר למה נחשב נכס מידע, פעילות עסקית ותהליך תומך, רמת פירוט המיפוי הנדרשת, ועקרונות לדירוג קריטיות ורגישות, ויתעד אותה.

44.1. רמת פירוט המיפוי הנדרשת תהיה כזו אשר מאפשרת זיהוי מהיר של נכס המידע, מיקומו, והגורם שהוא בעל הנכס כמשמעותו בסעיף 45 להלן, ומספיקה לקביעת אופי וחוזקת הבקרות הנדרשות על מנת להגן על נכסי המידע, הפעילויות העסקיות והתהליכים התומכים.

44.2. במקרה בו תאגיד בנקאי בחר לכלול מספר רכיבים תחת נכס מידע אחד או תחת פעילות עסקית אחת, או תחת תהליך תומך אחד, רמת הקריטיות והרגישות של נכס המידע, הפעילות העסקית או התהליך התומך, תקבע על פי הרכיב בעל רמת הקריטיות והרגישות הגבוהה ביותר.

45. לכל נכס מידע יקבע "בעל נכס המידע" שיוגדר כאחראי לניהולו ולמתן דיווחים לגביו.

הערכת סיכונים

46. תאגיד בנקאי יבצע הערכת סיכונים על בסיס מתמשך במסגרתה יזהה ויעריך את סיכוני טכנולוגיית המידע המשפיעים על הפעילויות העסקיות, התהליכים התומכים, ונכסי המידע שזוהו, בהתאם לרמת הקריטיות והרגישות שלהם. הערכת הסיכונים תתועד, ותעודכן בפרט כאשר מתרחש שינוי מהותי בתשתיות, בתהליכים או בנהלים המשפיעים על הפעילויות העסקיות, התהליכים התומכים או נכסי המידע.

הפחתת סיכונים

47. תאגיד בנקאי יגדיר ויישם את האמצעים הנדרשים, ובכלל זה, יישום בקרות מתאימות או שינוי תהליכים, בכדי להפחית את סיכוני טכנולוגיית המידע שזוהו בהתאם לסעיף 46 לעיל, כך שיתאמו את תיאבון הסיכון שלו; ובכלל זה יקבע האם נדרשים שינויים בתהליכים העסקיים הקיימים, בבקרות, או במערך טכנולוגיית המידע.

48. הגדרת הבקרות ויישומן לצורך הגנה על נכסי המידע תעשה, בין היתר, בהתאם לסיווג רמת הקריטיות והרגישות שנקבעה להם ובהתאם לעקרונות המפורטים בפרק ח' להלן: "יישום בקרות אבטחת מידע".

דיווח

49. תאגיד בנקאי ידווח את תוצאות הערכת הסיכונים להנהלה הבכירה באופן בהיר ובזמן.

פרק ד': הגורם האנושי - הדרכה ומודעות משתמשים

50. בפרק זה, "עובדים" – לרבות עובדים חיצוניים, המנוהלים על ידי התאגיד הבנקאי.
51. תאגיד בנקאי יפתח ויישם תוכניות הדרכה לעובדים קיימים, עבור טכנולוגיות ומוצרים חדשים בטרם הטמעתם וכן תוכניות להדרכת עובדים חדשים עם כניסתם לתפקיד. בנוסף, ידאג התאגיד הבנקאי להדרכות תקופתיות לריענון הידע של אותם עובדים בהתאם לצורך.
52. תאגיד בנקאי ידאג לרציפות בתפקידי מפתח במערך טכנולוגיית המידע לרבות מערך אבטחת המידע באמצעות הסכמים מתאימים, תוכניות פיתוח מקצועיות, תוכניות הדרכה והכשרה של עובדים נוספים, ותוכניות גיבוי לצורך מילוי תפקידים אלו באופן זמני.
53. תאגיד בנקאי יפתח תוכנית להדרכה ולהגברת המודעות בנושאי אבטחת מידע והגנת הסייבר וכן בנושאי הגנת הפרטיות, אותה יעברו מידי תקופה ולפחות אחת לשנה, כל העובדים. התוכנית תכשיר את העובדים לבצע את תפקידם באופן התואם את המדיניות ונהלי אבטחת המידע של התאגיד הבנקאי, וכן תדריך את העובדים כיצד להתמודד עם סיכונים הקשורים לאבטחת מידע.
תאגיד בנקאי יוודא שגם עובדי צד ג' שאינם מנוהלים על ידי התאגיד הבנקאי יעברו תוכנית להדרכה ולהגברת המודעות בנושאי אבטחת מידע והגנת הסייבר וכן בנושאי הגנת הפרטיות כאמור לעיל, בהתאם לקריטיות ולרגישות של נכס המידע אליו יש להם גישה.

חלק ג' - ניהול סיכוני טכנולוגיית המידע

פרק ה': ניהול טכנולוגיית המידע

מדיניות ניהול טכנולוגיית המידע

54. מדיניות ניהול טכנולוגיית המידע תתועד ותתייחס לאופן ניהול מערך טכנולוגיית המידע ובכלל זה התפעול, הניטור והבקרה שלו, ותפרט תהליכים ברמת התאגיד הבנקאי הקשורים לעיצוב ולתכנון הטכנולוגיה לצורך מתן מענה לצרכיו העסקיים (ראה הרחבה בסעיף 57 להלן בנושא: "ארכיטקטורה"), ליישום תשתיות טכנולוגיות מתאימות (ראה הרחבה בסעיף 58 להלן בנושא: "תשתית טכנולוגית"), ולאספקת שירותים ומוצרים פיננסיים ללקוחותיו (ראה הרחבה בסעיפים 59-63 להלן בנושא: "ניהול התפעול"). המדיניות תיתן דגש, בין היתר, להיבטים הקשורים לניהול הסיכון הטכנולוגי, נאותות אבטחת המידע של טכנולוגיית המידע, הגנה על לקוחות, וציות להוראות הדין והרגולציה הרלבנטיות.

55. תאגיד בנקאי יוודא שמערכות המידע תאפשרנה לדירקטוריון ולהנהלה להעריך את ביצועיו העסקיים, לזהות את הסיכונים והאתגרים העומדים בפניו, ולסייע בתפעולו. לצורך כך, על מערכות המידע של התאגיד הבנקאי לענות על המאפיינים הבאים תוך יישום בקרות מתאימות:

55.1. לספק מידע מדויק, עקבי, שלם, רלבנטי ובזמן;

55.2. להיות אמינות כך שניתן יהיה להסתמך עליהן לצורך תיעוד ואיסוף מידע;

55.3. לספק מידע על מגמות ואינדיקטורים לסיכוני מפתח (Key Risk Indicators);

55.4. לתמוך באסטרטגיה העסקית של התאגיד הבנקאי;

55.5. לשמור על הסודיות, השלמות והזמינות של הנתונים;

55.6. להפחית ככל הניתן את אותן פעילויות מוטות עבודה ידנית.

56. בעת קביעת מדיניות כאמור בסעיף 54 לעיל, ידאג התאגיד הבנקאי לשלב היבטי חוסן תפעולי בתהליכי התכנון, היישום והתפעול כדלקמן:

56.1. התאגיד הבנקאי יוודא כי תהליכי התכנון, היישום והתפעול של מערך טכנולוגיית המידע מספקים חוסן תפעולי שיאפשר לו להמשיך באספקת פעולות חיוניות ללקוחותיו גם בעת שיבוש. לשם כך ידאג תאגיד בנקאי לשלב בתהליכים כאמור, אמצעים יזומים לשמירה על סודיות, שלמות וזמינות מערך טכנולוגיית המידע ולהפחתת הסיכון לאירוע כאמור, וכן לשלב את התהליכים כאמור בתהליך ניהול פרויקטים ובתוכנית להמשכיות עסקית.

56.2. בעת שימוש בסביבת מחשוב ענן לצורך אספקת פעולות חיוניות ללקוחותיו או בעת תכנון מעבר לסביבה כאמור, יוודא התאגיד הבנקאי את החוסן התפעולי של סביבה זו ואת עיגון הדרישה לכך בחוזה עם צד ג' הנותן שירותי מחשוב ענן.

ארכיטקטורה

57. תאגיד בנקאי יישם עקרונות לתכנון ולעיצוב של ארכיטקטורת טכנולוגיית מידע אפקטיבית, ובכלל זה:

57.1. תאגיד בנקאי יתכנן, יישם ויתאים את ארכיטקטורת טכנולוגיית המידע שלו ליעדים האסטרטגיים והעסקיים שקבע לעצמו, ויקבע תוכנית מתאימה לצורך כך, שתענה על הדרישה לשמירה על סודיות, שלמות וזמינות של מערך טכנולוגיית המידע במטרה למזער את הסיכונים התפעוליים והסיכון התדמיתי הנובעים ממערכות שאינן מתוכננות כיאות.

57.2. תוכנית הארכיטקטורה תפרט את התכנון הכולל של מערך טכנולוגיית המידע והעקרונות המתארים את מסגרת העבודה התפעולית של התאגיד הבנקאי, לרבות תיאור של המשימות העומדות בפניו, העסקים והלקוחות, תרשימי זרימה של הפעילות ותהליכים, תהליכי עיבוד נתונים, ממשקים למערך טכנולוגיית המידע, אבטחת מידע וזמינות. רמת הפירוט תהיה בהתאם לרמת הקריטיות והרגישות של נכסי המידע.

57.3. תוכנית הארכיטקטורה תיבנה כך שתסייע לתאגיד הבנקאי, בין היתר:

57.3.1. בעיצוב התפיסה ובתחזוקה השוטפת של מבנה מערך טכנולוגיית המידע, ושל בקרות טכנולוגיית המידע, המדיניות והנהלים הקשורים.

57.3.2. בשמירה על עדכניות רשימת נכסי טכנולוגיית המידע, הפעילויות העסקיות והתהליכים התומכים בהם – ראה סעיף 43 לעיל.

תשתית טכנולוגית

58. תאגיד בנקאי יישם עקרונות ליישום תשתית טכנולוגית נאותה, ובכלל זה:

58.1. ביישום תשתית טכנולוגית, בין אם היא מנוהלת על ידי התאגיד הבנקאי ובין אם על ידי צד ג', יוודא התאגיד הבנקאי כי היא מקיימת ומקדמת היבטים של סודיות, שלמות וזמינות, ואת יעדיו העסקיים. לצורך כך, תאגיד בנקאי יפתח, יתעד ויישם, בהתאם לקריטיות ולרגישות של נכס המידע, מדיניות ונהלים מתאימים להטמעת בקרות תשתית שתגנה על המתקנים, הטכנולוגיה, והנתונים. בקרות אלו תכלולנה היבטי יתירות וחוסן עבור רכיבי תשתית טכנולוגית ועבור מוצרים, שירותים ותקשורת נלווים. המדיניות והנהלים יסדירו, בין היתר, את הנושאים הבאים:

58.1.1. תהליכים לזיהוי, איתור, וניטור של רכיבי תשתית טכנולוגית;

58.1.2. הקצאה נאותה של משאבים לתחום התשתית הטכנולוגית לרבות ידע, ומומחיות מתאימים;

58.1.3. תהליכי ניהול קונפיגורציה של רשתות וניהול שינויים – ראה פרק ו' להלן בנושא: "ניהול פרויקטים וניהול שינויים";

58.1.4. תהליכי אבטחה וניטור לניתוח תעבורת נתונים וזיהוי פעילויות חריגות;

58.1.5. תהליכי פיתוח מערכת המתייחסים להיבטים של: מדרגיות (Scalability), יכולת העברת מידע בין מערכות ושימוש בו (Interoperability), ניידות (Portability), בקרות תוכנה נאותות, שימוש ובקרה בתוכנות קוד פתוח;

58.1.6. בקרות המטפלות בסיכונים הייחודיים למחשב מרכזי;

58.1.7. בקרות גישה פיזית ובקרות סביבתיות – ראה סעיף 122 להלן "בקרות גישה פיזית ובקרות סביבתיות".

58.2. התשתית הטכנולוגית של התאגיד הבנקאי תתמוך בחוסן תפעולי בהתאם לקריטיות של נכס המידע עבור התהליכים והשירותים החיוניים של התאגיד הבנקאי.

ניהול התפעול

59. תאגיד בנקאי יישם עקרונות לניהול התפעול, ובכלל זה:

59.1. תאגיד בנקאי יקבע מסגרת לניהול התפעול של מערך טכנולוגיית המידע שתתמוך בפעילויות ובשירותים אותם מערך זה מספק, תנהל את נכסי המידע, תנהל שינויים, תיתן מענה הולם לאירועים, ותבטיח את יציבות סביבת הייצור.

59.2. תאגיד בנקאי יוודא באופן תקופתי שניהול התפעול של מערך טכנולוגיית המידע תואם את הדרישות והיעדים העסקיים שקבע לעצמו.

59.3. תאגיד בנקאי ידאג להטמעת היבטי חוסן תפעולי במסגרת לניהול התפעול אשר יסייעו במניעת הפסדים, בהגנה על מידע רגיש של לקוחות, ובצמצום שיבושים באספקת השירותים.

59.4. תאגיד בנקאי ידאג לשמור על היעילות של הפעילויות והשירותים אותם מספק מערך טכנולוגיית המידע וישפרה ככל שניתן.

59.5. המסגרת לניהול התפעול תכלול, בין היתר, פיתוח ויישום של הבקרות והתהליכים המפורטים בסעיפים 63 - 60 להלן.

בקרות תפעוליות

60. תאגיד בנקאי יפתח ויישם בקרות תפעוליות לצורך שמירה על כלל הסביבה התפעולית שלו ובכלל זה: מתקנים פיזיים, תשתיות התומכות בתפעול, מערכות, תוכנות וכן בקרות על הגורם האנושי. בקרות לדוגמא: בקרות גישה פיזית ולוגית במתקני התאגיד הבנקאי, בקרות לניהול זהויות, תהליכי מיון קפדניים שיוודאו את התאמת העובד לתפקיד, הפרדת תפקידים נאותה, ויישום עיקרון ארבע עיניים (ראה פירוט לגבי חלק מהבקרות בפרק ח' – "יישום בקרות אבטחת מידע").

תהליכים טכנולוגיים תפעוליים

61. תאגיד בנקאי יפתח תהליכים טכנולוגיים תפעוליים במטרה להפחית כשלים תפעוליים פוטנציאליים לרבות מביצוע פעולות ידניות, ולמזער את השפעתם במידה ויתרחשו. תהליכים אלו יכללו בין היתר:

61.1. **תחזוקה** – תאגיד בנקאי יישם, בהתאם לקריטיות ולרגישות נכס המידע, תהליך למניעת כשל בתפקוד של נכס מידע או תהליך המחזיר את היכולות התפעוליות לקדמותן לאחר התרחשותו של כשל כזה.

61.2. **ניהול תצורה** – תאגיד בנקאי יישם תהליך לשמירה של מידע חיוני (כמו: מודל, גרסה, מפרט) על תצורת החומרה והתוכנה שמרכיבות את נכס המידע בהתאם לקריטיות ולרגישות שלו, ויסקור ויאמת את המידע על בסיס שוטף כדי לוודא שהוא מדוייק ועדכני.

61.3. **הפסקת תמיכה (End of Life/End of Support) -** תאגיד בנקאי יישם תהליך לזיהוי חומרה או תוכנה, שהתמיכה בהם, בין אם מדובר בתמיכה של צד ג' ובין אם מדובר בתמיכה של גורם מתוך התאגיד הבנקאי עצמו (In-house), הינה חלקית, עומדת להיפסק או שהופסקה. כחלק מהתהליך, תבוצע הערכת סיכונים על מנת להעריך את הסיכונים ובכלל זה חשיפות אבטחת המידע העלולים לנבוע מהמשך השימוש בחומרה או בתוכנה שזוהו כאמור, ותונהגנה בקרות מתאימות למזעור סיכונים אלו. לדוגמא, הפרדה מנכסי מידע אחרים. במידת הצורך יוציא התאגיד הבנקאי את החומרה או התוכנה מכלל שימוש.

61.4. **ניהול טלאים** (Patches) – תאגיד בנקאי יטמיע תהליך שיבטיח יישום של טלאים פונקציונליים ושאינם פונקציונליים (לדוגמא: תיקונים לפגיעויות אבטחה או לבאגים בתוכנה) בתוך פרק זמן שתואם את הקריטיות והרגישות של הטלאי ושל נכס המידע. הטלאים ייבדקו בסביבה נפרדת בטרם הטמעתם בסביבת הייצור, על מנת לוודא שהם מתאימים לנכסי המידע הקיימים ואינם גורמים לכשלים במערך טכנולוגיית המידע.
לעניין טלאי חירום שלא ניתן ליישם לגביו את תהליך ניהול הטלאים הרגיל – ראה סעיף 97 להלן.

61.5. **ניהול גיבויים -**

61.5.1. תאגיד בנקאי יגדיר תהליך לגיבוי ולשחזור נכסי מידע על מנת להבטיח כי ניתן יהיה לאחזרם בעת הצורך. היקף ותדירות הגיבויים יתאמו לדרישות ההתאוששות העסקיות ומידת הקריטיות והרגישות של נכס המידע, ויעודכנו בהתאם לשינויים בהערכת הסיכונים. התאגיד הבנקאי יוודא כי הגיבויים נשמרים באופן מאובטח ובאופן מרוחק מספיק מהאתר הראשי כך שהם לא יהיו חשופים לאותם סיכונים כמוהו. בדיקה של תהליך הגיבוי והשחזור תבוצע על בסיס תקופתי.

61.5.2. התהליך לגיבוי ולשחזור נכסי מידע יתוכנן להתאים גם לתרחיש של ניסיונות לפגיעה באמינות הגיבויים, לרבות באופן שיאפשר שחזור והתאוששות מגיבוי גם במקרה של פגיעה בתהליך הגיבויים עצמו.

61.5.3. תאגיד בנקאי העושה שימוש בצד ג' לצורך ניהול תהליך הגיבויים, יוודא כי צד ג' מבצע תהליך כאמור.

61.6. **ניהול קיבולת וביצועים -**

61.6.1. תאגיד בנקאי יקבע תהליכים לניהול קיבולת אשר מתחשבים בגורמים פנימיים צפויים דוגמת: גידול בהיקף העסקים של התאגיד הבנקאי, מיזוגים, רכישות, מוצרים חדשים ויישום טכנולוגיות חדשות, ובגורמים חיצוניים צפויים דוגמת: שינויים בדרישות הצרכנים, ובדרישות השוק.

61.6.2. תאגיד בנקאי יעריך באופן שוטף את הקיבולת של מערך טכנולוגיית המידע על מנת להבטיח קיומם של ביצועים נאותים, בין היתר, בהיבטים הבאים: מהירות העבודה של הפלטפורמה, זיכרון עבודה זמני ב – CPU (Primary working memory for each platform's CPU), מקום אחסון נוסף (additional data storage capacity), רוחב הפס להעברת נתונים.

61.6.3. תאגיד בנקאי ינתח מגמות בקיבולת על מנת להבטיח את המשך העמידה בדרישות העסקיות.

61.6.4. תאגיד בנקאי ינתח באופן תקופתי את צרכי הקיבולת שנחזו אל מול הקיבולת שבפועל על מנת לקבוע האם התהליכים לניהול ולתכנון קיבולת הינם נאותים ובמידת הצורך יעדכנם.

61.6.5. בעת פיתוח או רכישת טכנולוגיות חדשות, ישקול התאגיד הבנקאי, בין היתר, את הגמישות של המערכות המבוססות על טכנולוגיות אלו, בהתייחס לדרישות הקיבולת הצפויות.

61.6.6. בעת התקשרות עם צד ג', יעריך התאגיד הבנקאי את ביצועי צד ג' בשילוב עם הביצועים שלו, על מנת לקבוע האם הדרישות העסקיות הנוכחיות והעתידיות מקבלות מענה בהיבטי קיבולת.

61.7. ניהול נתיב ביקורת מבוסס קבצי LOG -

61.7.1. תאגיד בנקאי יקבע תהליך ליצירה, העברה, אחסון, ניתוח ומחיקה של נתיב ביקורת מבוסס קבצי Log אשר ישמש לצרכי זיהוי, מעקב, ניתוח ופתרון של אירועים שונים המתרחשים בפעילות מערך טכנולוגיית המידע לרבות אירועי אבטחת מידע. נתיב הביקורת יכיל מידע לגבי עצם הגישה, פעולות ושאילתות המבוצעות על ידי המשתמשים במערכות המידע של התאגיד הבנקאי. המידע שיישמר יכלול, בין היתר, את זיהוי הגורם הניגש, המקור (Source), הזמן וכן פרטים על נשוא הגישה.

61.7.2. על אף האמור בסעיף 61.7.1 לעיל, לגבי שאילתות של עובדי התאגיד הבנקאי יקיים התאגיד הבנקאי נתיב ביקורת על פי שיקול דעתו, תוך התבססות על הערכת הסיכונים.

61.7.3. הגישה לנתיב הביקורת תאובטח לצורך מניעת שינוי או מחיקה בלתי מורשים או שימוש לרעה בנתונים הנאספים באמצעותו, והוא יישמר לפרק זמן הולם והכל בהתאם לקריטיות ולרגישות של הפעילויות העסקיות, התהליכים התומכים ונכסי המידע, ולדרישות הרגולטוריות והמשפטיות החלות על התאגיד הבנקאי.

61.7.4. תאגיד בנקאי ישתמש, בהתאם להערכת סיכונים מתאימה, בכלים לצורך ניתוח ממוכן של נתיב הביקורת שיסייעו בין היתר בזיהוי אנומליות, ואירועים חשובים או דפוסי פעילות.

61.7.5. בעת התקשרות עם צד ג', יבחן התאגיד הבנקאי, בין היתר בהתאם להערכת הסיכונים, את הצורך בחיוב אותו צד ג' במסגרת חוזה ההתקשרות עימו, בהעברת קבצי Log ממערכותיו בהתאם לבקשת התאגיד הבנקאי.

61.8. **מחיקת נתונים והשמדת מדיה** -

61.8.1. תאגיד בנקאי יקבע תהליך למחיקת נתונים ולהשמדתה או העברתה של מדיה פיזית (לדוגמא: תדפיסים) ודיגיטלית (לדוגמא: דיסק קשיח, התקן אחסון), המותאם לקריטיות ולרגישות של נכס המידע ולסוג המדיה בה נעשה שימוש. שיטת המחיקה או ההשמדה תקבע על פי סוג הנתונים שיש למחוק. תאגיד בנקאי ישקול את מחיקת הנתונים מעל גבי מדיה גם כאשר היא מועברת בין מחלקותיו.

61.8.2. תאגיד בנקאי יקבע תהליך להעברה או להשמדת ציוד (לדוגמא: מדפסות) אשר עלול להכיל שאריות של נתונים. התהליך יתייחס גם לצורך בסקירה תקופתית של מערך טכנולוגיית המידע במטרה להבטיח השמדה מהירה של ציוד מושבת.

61.8.3. תאגיד בנקאי המתקשר עם צד ג', ידאג לעגן בחוזה ההתקשרות עימו הסדרים למחיקת נתונים של התאגיד הבנקאי המאוחסנים אצלו לרבות אצל גורם שמתקשר עם אותו צד ג' לצורך ביצוע תכולת ההתקשרות עבור התאגיד הבנקאי, לאחר סיום ההתקשרות עימו או לפי דרישת התאגיד הבנקאי. ההסדר למחיקת הנתונים ייקבע בהתאם לתהליך מחיקת הנתונים והשמדתם בתאגיד הבנקאי – ראה סעיף 61.8.1 לעיל.

בכל מקרה של אי תאימות בין דרישה זו לבין הדרישה המופיעה בסעיף 30(א) להוראת ניהול בנקאי תקין מס' 362 בנושא: "מחשוב ענן" (להלן: "הוראה 362") תחול הדרישה המחמירה מבין שתיהן.

תהליכי שירות ותמיכה

62. תאגיד בנקאי יפתח ויישם תהליכי שירות ותמיכה למערך טכנולוגיית המידע שיבטיחו את השגת היעדים והמטרות האסטרטגיים שקבע לעצמו, באמצעות הבטחת אמינות ועמידות מתמשכים של מערך טכנולוגיית המידע, תמיכה בקווי העסקים, העובדים והלקוחות, ומניעת כשלים במערך טכנולוגיית המידע. תהליכים אלו יכללו, בין היתר, את תהליכי "ניהול אירועים ובעיות" – פרק י"א להלן.

תהליכי ניטור, הערכה ודיווח

63. תאגיד בנקאי יפתח תהליכים:

63.1. לניטור שוטף של פעילות מערך טכנולוגיית המידע - ראה פרק י' – "ניטור מערך טכנולוגיית המידע".

63.2. להערכת אפקטיביות הבקרות המיושמות ולדיווח אודותיה באופן תקופתי להנהלה הבכירה. הערכת אפקטיביות הבקרות תסייע להנהלה הבכירה לזהות מגמות בהתפתחות סיכונים בפעילות המערך, לדוגמא: בקרות לא אפקטיביות, תהליכים לא יעילים, שימוש לקוי במשאבים או מחסור במשאבים, ושירותים טכנולוגיים שאינם ניתנים בסטנדרט המקובל.

התאגיד הבנקאי יקבע תהליך תקופתי לבחינה של תהליכי הניטור, ההערכה והדיווח ויתאים אותם בהתאם לדרישות והיעדים המתחדשים.

תהליך תכנון והשקעה בטכנולוגיית המידע

64. תאגיד בנקאי יישם עקרונות ליישום נאות של תהליך תכנון והשקעה בטכנולוגיית המידע:

64.1. תאגיד בנקאי יישם תהליך נאות לתכנון ולהשקעה במערך טכנולוגיית המידע הכולל היערכות לקראת פעילויות עתידיות באמצעות הגדרת יעדים והאסטרטגיה להשגתם. בתהליך ישתתפו הדירקטוריון, ההנהלה הבכירה והעובדים. התהליך ישולב במסגרת תהליך התכנון העסקי הכולל ויותאם באופן שוטף לסיכונים חדשים ולהזדמנויות העסקיות. תוצרי התהליך יהיו מסמכי האסטרטגיה, המדיניות ותוכניות העבודה. התהליך יתייחס בין היתר להיבטים הבאים:

64.1.1. יעדי התאגיד הבנקאי לטווח הקצר ולטווח הארוך והמשאבים המוקצים להשגתם;

64.1.2. התאמת אסטרטגיית טכנולוגיית המידע לאסטרטגיה העסקית של התאגיד הבנקאי;

64.1.3. זיהוי ומדידה של הסיכון בטרם נערכים שינויים או השקעות חדשות בטכנולוגיה;

64.1.4. קיומם של משאבים טכנולוגיים מתאימים (לדוגמא: תשתית, חומרה, תוכנות הפעלה, אפליקציות ועובדים) לתמיכה בפעילות העסקית הנוכחית והצפויה.

64.2. במסגרת תהליך התכנון, תאגיד בנקאי המתקשר עם צדדים שלישיים יוודא שהתוכניות והפעולות של צד ג' תומכות בתוכניות של התאגיד הבנקאי ולא משפיעות עליו לרעה.

פרק ו': ניהול פרויקטים וניהול שינויים

ניהול פרויקטי טכנולוגיית מידע

65. תאגיד בנקאי יישם מסגרת עבודה לניהול פרויקטי טכנולוגיית מידע שתבטיח עקביות בפרקטיקה הנהוגה בתחום זה, ובנוסף תבטיח שתוצאות הפרויקט תעמודנה בדרישות וביעדים שנקבעו לו. מסגרת העבודה תגדיר, לכל הפחות, תפקידים, תחומי אחריות, סמכויות וקווי דיווח כך שתתמוך ביישום אפקטיבי של אסטרטגיית טכנולוגיית המידע, תוך שהיא מבחינה בין סוגי פרויקטים בהתאם לקריטיות ולרגישות של נכס המידע הרלבנטי לפרויקט, ובהתאם למאפייני הפרויקט הרלבנטיים לתאגיד הבנקאי, כגון: גודל ומורכבות, חשיבות ליישום האסטרטגיה של התאגיד הבנקאי, וחדשנות.

66. תאגיד בנקאי יקיים תהליך לזיהוי והערכה נאותים של הסיכונים הנובעים מתיק פרויקטי טכנולוגיית המידע שלו ויפעל למזעורם. במסגרת זו יתייחס התאגיד הבנקאי גם לסיכונים היכולים לנבוע כתוצאה מתלויות בין פרויקטים שונים, וכן לסיכונים היכולים לנבוע מהתלות של מספר פרויקטים באותם משאבים או באותה מומחיות.

67. תאגיד בנקאי יקבע מדיניות לניהול פרויקטי טכנולוגיית מידע שתכלול, בין היתר, התייחסות לאופן היישום של הנושאים הבאים בהתאמה לסוגי הפרויקטים השונים:

67.1. יעדי הפרויקט;

67.2. תפקידים ותחומי אחריות, לרבות סמכויות לאישור הפרויקטים;

67.3. הערכת סיכוני הפרויקט והאמצעים למזעורם;

67.4. תוכנית הפרויקט, לוחות זמנים ושלבים;

67.5. אבני דרך מרכזיות;

67.6. דרישות ניהול השינויים.

68. מדיניות ניהול פרויקטי טכנולוגיית מידע תוודא שדרישות אבטחת המידע תנותחנה ותאושרנה על ידי פונקציה בלתי תלויה בפונקציית הפיתוח שאושרה על ידי מנהל הגנת הסייבר ואבטחת המידע.

69. תאגיד בנקאי יוודא כי לטובת מימוש פרויקט טכנולוגיית מידע, יהיו חברים בצוות הפרויקט נציגים מכל התחומים המושפעים ממנו, וכי קיים בו הידע הנדרש כדי להבטיח את השלמתו בצורה נאותה.

70. תאגיד בנקאי ידווח לדירקטוריון, בהתאם למדיניות שתיקבע, על ביצוע פרויקטי טכנולוגיית מידע וכן על ההתקדמות בהשלמתם לרבות הסיכונים הכרוכים בהם, בנפרד או במרוכז, בהתאם לחשיבותם ולהיקפם של הפרויקטים, הן באופן שוטף והן על פי דרישה, בהתאם לנדרש.

71. תאגיד בנקאי יכלול במסגרת לניהול הסיכונים שלו התייחסות לסיכוני הפרויקטים.

<u>רכישה, פיתוח ויישום מערכות</u>

כללי

72. תאגיד בנקאי יקבע תהליך מבוסס סיכון לניהול רכישה ולניהול פיתוח של מערכת ובכלל זה יישום מערכת שנרכשה.

73. תאגיד בנקאי יוודא לפני כל רכישה או פיתוח של מערכת, כי הדרישות הפונקציונליות והלא פונקציונליות לרבות דרישות בנושא אבטחת מידע מוגדרות בבהירות ומאושרות על ידי הנהלת הגורם העסקי הרלבנטי.

74. תאגיד בנקאי יישם מתודולוגיה לבדיקה ולאישור המערכת בטרם השימוש הראשוני בה. מתודולוגיה זו תתחשב בין היתר בקריטיות וברגישות של נכס המידע. הבדיקה תוודא כי המערכת החדשה מתפקדת כיאות, ותתבצע בסביבת בדיקות המדמה ככל הניתן את סביבת הייצור.

רכישת מערכת

75. תהליך ניהול הרכישה של מערכת יתייחס, בין היתר, להערכה ולבחירת צד ג' על מנת להבטיח כי הינו בעל יכולת מתאימה לעמוד בדרישות ולספק את המערכת. רמת ההערכה ובדיקת הנאותות שתבוצענה תהיה תואמת את הקריטיות והרגישות של נכס המידע.

76. בהתאם להערכת סיכונים מתאימה, יעריך תאגיד בנקאי את רמת החוסן (Robustness) של פיתוח התוכנה אצל צד ג' ואת פרקטיקות בקרת האיכות שלו, וכן יוודא יישום של אמצעי בקרה ובכלל זה אבטחת מידע מתאימים על כל מידע רגיש שלצד ג' יש גישה אליו במהלך הפרויקט. כל גישה של צד ג' במסגרת הפרויקט לנכס מידע תנוטר ותבוקר, בין היתר, בהתאם לקבוע בסעיף 61.7 לעיל "ניהול נתיב ביקורת מבוסס קבצי LOG".

77. במקרה שבפרויקט נעשה שימוש בפתרונות מדף או בפתרונות מבוססי קוד פתוח, שאינם עומדים בדרישות המסגרת לניהול אבטחת מידע של התאגיד הבנקאי, יעריך התאגיד הבנקאי את הסיכונים ויוודא קיומם של בקרות מפצות בטרם הטמעת הפרויקט.
78. תאגיד בנקאי יעריך את נחיצותו של הסכם נאמנות לשמירת קוד המקור, בהתאם לקריטיות ורגישות נכס המידע, ויקבע חלופות למקרה בו הסכם נאמנות נחוץ, אך לא ניתן ליישמו.

פיתוח ויישום מערכת

79. תאגיד בנקאי יוודא כי ננקטו צעדים למזעור הסיכון לשינוי לא מכוון או לביצוע מניפולציות מכוונות במערכת במהלך תהליך הפיתוח או היישום בסביבת הייצור.
80. תאגיד בנקאי יתעד באופן מקיף את הפיתוח, היישום, התפעול או הקינפוג של מערכות, על מנת לצמצם כל תלות מיותרת במומחים חיצוניים לנושא. התיעוד יכלול לכל הפחות, וככל שהדבר ישים, הדרכה למשתמש, מידע טכני, ונהלי הפעלה.
81. תאגיד בנקאי יישם הפרדה פיזית או לוגית בין סביבת הייצור לבין סביבות הפיתוח, הבדיקות וסביבות נוספות שאינן סביבות ייצור, וזאת על מנת להבטיח הפרדת תפקידים נאותה וכדי למנוע הכנסת שינויים שלא אושרו לסביבת הייצור. בנוסף, ישקול התאגיד הבנקאי הפרדה כאמור, לכל הפחות, עבור כל אחד מסוגי הבדיקות הבאים: יחידה, אינטגרציה ובדיקות משתמש. הגישה לכל סביבה תינתן למשתמשים מורשים בלבד על בסיס צורך.
82. תאגיד בנקאי יקבע תהליך לניהול מחזור החיים של פיתוח מערכת (SDLC), ובכלל זה עבור יישום מערכת שנרכשה. בהתאמה לתהליך יגדיר התאגיד הבנקאי נהלים ובקרות עבור כל שלב ממחזור החיים, וישמור על עדכניותם.
83. פונקציית אבטחת מידע והגנת הסייבר תהיה מעורבת לפי העניין, בכל שלב משלבי מחזור החיים של פיתוח מערכת ושל יישום מערכת.

פיתוח API

סעיפים 84-91 להלן יחולו על כל צד ג' שהתאגיד הבנקאי התקשר עימו בממשק API למעט סעיפים 85-87 שיחולו רק על צד ג' שהוראת נ.ב.ת. מס' 368 בנושא: "בנקאות פתוחה" אינה חלה עליו.

84. תאגיד בנקאי יקבע אמצעי בקרה נאותים לניהול הפיתוח והשירות של ממשקי API לצורך אספקה מאובטחת של שירותים אלו.
85. תאגיד בנקאי יישם תהליך במסגרתו תוערך התאמתו של צד ג' להתחברות לממשק ה - API של התאגיד הבנקאי, וכן ייבדק אופן הגישה שלו. תהליך זה יתייחס, בין היתר, לגורמים כמו: אופי הפעילות העסקית של צד ג', מצב אבטחת המידע שלו, והמוניטין שלו.
86. תאגיד בנקאי יבצע הערכת סיכונים בטרם יאפשר לצד ג' להתחבר אליו באמצעות ממשקי API, ויוודא כי יישום הממשק תואם את הקריטיות והרגישות של המידע העובר ביניהם.
87. תאגיד בנקאי יקבע עקרונות אבטחת מידע לעיצוב ופיתוח API. העקרונות יתייחסו, בין היתר, לאמצעים להגן על אמצעי הגישה לממשק ה – API אשר נעשה בהם שימוש לצורך החלפת מידע

סודי כגון: מפתחות או אסימוני גישה (Tokens), ולצורך בהגבלת תוקפו של אמצעי הגישה על מנת להפחית את הסיכון לגישה בלתי מורשית.

88. תאגיד בנקאי יישם סטנדרטים חזקים של הצפנה ובקרת ניהול אמצעי הגישה על מנת להעביר מידע רגיש באופן מאובטח באמצעות ממשקי API.

89. תאגיד בנקאי יבדוק את ממשק ה – API שבינו לבין צד ג', בין היתר, בהיבטי אבטחת מידע, בטרם העברתו לייצור, ויתעד את כניסתו של צד ג' לממשק לרבות זהות הגורם שיצר את הקשר, תאריך ושעת הקשר, והמידע שאליו ניגש.

90. תאגיד בנקאי יטמיע במהלך הפיתוח אמצעי ניטור בזמן אמת על ממשק ה – API שינטרו את השימוש והביצועים בממשק, ויזהו פעילות חשודה. זאת במטרה שבעת התרחשות אירוע של פגיעה בתאגיד הבנקאי או בלקוחותיו באמצעות הממשק, אמצעי הניטור יגרמו לביטול מהיר של אמצעי הגישה לממשק.

91. תאגיד בנקאי יוודא כי המערכות שלו מסוגלות לטפל בנפחים גדולים של בקשות API, ויישם אמצעים למזעור איומי אבטחת מידע ובכלל זה סייבר, דוגמת התקפות DDoS.

ניהול שינויים

92. תאגיד בנקאי יקבע תהליך לניהול שינויים שיבטיח כי שינויים הנעשים בנכס המידע מתועדים, נבדקים, מוערכים, נסקרים ומאושרים בטרם יישומם.

93. תאגיד בנקאי יפעל לבצע הערכת סיכונים וניתוח של השפעת השינוי על נכס המידע בטרם יישום השינוי. הערכת הסיכונים והניתוח כאמור, יתייחסו בין היתר להיבטים הבאים: אבטחת מידע וההשלכות של השינוי על נכסי מידע אחרים.

94. תאגיד בנקאי יוודא כי כל השינויים נבדקים באופן נאות בסביבת בדיקות. תוכנית הבדיקות תפותח ותאושר על ידי גורם ניהולי עסקי וגורם ניהולי טכנולוגי מתאימים. תוצאות הבדיקות יתקבלו ויאושרו בטרם יועבר השינוי לסביבת הייצור.

95. תאגיד בנקאי יקים ועדה ייעודית שתכלול באופן קבוע נציגים מטעם כל גורמי המפתח בתהליך ניהול שינויים, ובכלל זה גורם ניהול עסקי וגורם ניהול טכנולוגי, שתאשר ותתעדף שינויים, לאחר שתבחן, בין היתר, היבטים של יציבות והשלכות אבטחת מידע של השינויים על סביבת הייצור.

96. תאגיד בנקאי יגבה את נכס המידע בטרם יועבר השינוי לייצור, ויכין תוכנית "חזרה לאחור" (Roll Back) לנכס המידע, למקרה שתתרחש בעיה במהלך העברת השינוי לייצור או לאחריו.

97. תאגיד בנקאי יגדיר נהלים להערכה, אישור והעברה לייצור של שינויי חירום שלא ניתן ליישם לגביהם את תהליך ניהול השינויים הרגיל ואת הגורם המוסמך לאשר שינויים מסוג זה, על מנת להפחית את הסיכון לאבטחת המידע וליציבות סביבת הייצור.

98. תאגיד בנקאי ידאג לשמירת נתיב ביקורת עבור הפעילויות המבוצעות במהלך הטמעת השינוי על מנת שיסייע לו בחקירה ופתרון בעיות במהלך יישום השינוי או לאחריו.

דגשי אבטחת מידע בתהליכי ניהול פרויקטי טכנולוגיית מידע וניהול שינויים

99. לדגשי אבטחת מידע בתהליכי ניהול פרויקטי טכנולוגיית מידע וניהול שינויים – ראה סעיפים 123-124 להלן בנושא: "אבטחת מידע בתהליך ניהול השינויים" וסעיפים 125 להלן בנושא: "רכישה ופיתוח מערכת מאובטחת".

חלק ד' - ניהול סיכוני אבטחת מידע והגנת הסייבר

פרק ז': אבטחת מידע

יכולת אבטחת מידע

100. תאגיד בנקאי יעריך באופן שוטף את נאותות יכולת אבטחת המידע שלו וישמור על יכולת אבטחת מידע התואמת את היקף נכסי המידע שלו ואת היקף הסיכונים לנכסים אלו, בצורה המאפשרת את המשך פעילותו הנאות. יכולת אבטחת מידע תתעדכן בעקבות שינויים בסיכוני אבטחת מידע, לרבות כאלו הנובעים משינוי בנכסי מידע או בסביבה העסקית. לשם כך, על התאגיד הבנקאי לאמץ גישה סתגלנית וצופה פני עתיד, לרבות מיפוי וחקר הסביבה, חיזוי וחקר איומים, והשקעה מתמשכת במשאבים (תקציב והקצאת כוח אדם), במיומנויות מתאימות ובבקרות (מניעה, זיהוי, ותגובה).

101. יכולת אבטחת מידע תכלול בין היתר את הרכיבים הבאים:

101.1. ניהול פגיעויות ואיומי אבטחת מידע;

101.2. מודעות מצבית, שיתוף מידע ומודיעין;

101.3. תפעול וניהול מערך אבטחת המידע;

101.4. פיתוח, ותכנון ארכיטקטורה מאובטחים;

101.5. בדיקות אבטחה (Security testing) לרבות בדיקות חדירה;

101.6. מערך הדיווחים בתחום סיכוני אבטחת המידע ויכולת הניתוח של סיכונים אלו;

101.7. זיהוי ותגובה לאירועים, לרבות התאוששות, דיווח ותקשורת עם גורמים רלבנטיים לגבי אותם אירועים;

101.8. תחקיר, שימור ראיות וניתוח מעמיק של אירועי אבטחת מידע;

101.9. הערכת אפקטיביות בקרות אבטחת מידע (Information security assurance).

102. תאגיד בנקאי המתקשר עם צד ג' יפעל בהתאם לעקרונות הבאים:

102.1. בהתקשרות עם צד ג', תאגיד בנקאי יעריך את נאותות יכולת אבטחת המידע שלו בין היתר בהיבטים של נאותות המשאבים, המיומנויות והבקרות. ההערכה תתבצע בהתאמה להשפעות האפשריות של אירוע אבטחת מידע על נכסי המידע אשר יש לו גישה אליהם. כל פער שזוהה יטופל תוך פרק זמן סביר בהתאם להשפעתו האפשרית.

102.2. בהתקשרות עם צד ג', שמתקשר עם גורם אחר לצורך ביצוע תכולת ההתקשרות עבור התאגיד הבנקאי, יבדוק התאגיד הבנקאי להנחת דעתו כי לאותו צד ג' קיימת יכולת אבטחת מידע נאותה לצורך ניהול סיכוני אבטחת מידע המתווספים כתוצאה מהסדרים אלו.

102.3. תאגיד בנקאי המסתמך על בדיקת יכולת אבטחת המידע של צד ג' המסופקת לו על ידי אותו צד ג', יוודא את היקף, איכות ומידת אי התלות של הבדיקה, ובמידת הצורך ינקוט בצעדים לטיפול במגבלות הבדיקה שנתגלו.

מסגרת לניהול אבטחת מידע והגנת הסייבר

103. מסגרת לניהול אבטחת מידע והגנת הסייבר תתאם את סיכוני אבטחת המידע הניצבים בפני התאגיד הבנקאי. המסגרת תכלול את כלל המדיניות, הנהלים וההנחיות הנוגעים לאבטחת המידע, ובהתאם להם יפעלו הדירקטוריון, ההנהלה הבכירה, הוועדות הייעודיות, בעלי תפקידים, עובדים לרבות עובדים חיצוניים וזמניים, צד ג' ולקוחות התאגיד הבנקאי.

104. המסגרת לניהול אבטחת המידע והגנת הסייבר תהיה עקבית עם מסגרות עבודה אחרות בתאגיד הבנקאי כגון: מסגרת לניהול הסיכונים, מסגרת לניהול מיקור חוץ, תתחשב בדרישות משפטיות רלוונטיות, ותאפשר את התכנון והיישום של בקרות אבטחת מידע.

105. תאגיד בנקאי יבסס מסגרת נאותה לניהול אבטחת מידע והגנת הסייבר על עקרונות - על מרכזיים, וביניהם:

105.1. הגנה לעומק (Defense in Depth) – יישום מספר רב של שכבות הגנה וסוגי בקרות תוך יצירת מערכי הגנה המשלבים תשתיות ארגוניות ואנושיות, נהלים ותהליכי עבודה, וטכנולוגיות (People, Processes, Technologies) כך שהשפעת התממשות חולשה בבקרה אחת, תוגבל באמצעות בקרות אחרות. בפריסת ההגנה לעומק התאגיד הבנקאי יתחשב בניתוח סיכוני אבטחת המידע, מצב הבקרות והחשיפות למול הפגיעויות והאיומים;

105.2. הרשאות מינימליות (Least Privileged) והצורך לדעת (Need to Know) – נכסי המידע יוקשחו ותוגבל הגישה אליהם ושלהם למינימום הנדרש לצורך השגת היעדים העסקיים;

105.3. זיהוי של אירועי אבטחת מידע בזמן שיאפשר לצמצם את ההשפעה של פגיעה באבטחת המידע;

105.4. שילוב של עקרונות אבטחת מידע כבר בשלב התכנון של מערכות המידע (Secure by Design);

105.5. צמצום איסוף המידע ועיבודו למינימום ההכרחי, כבר משלב התכנון המוקדם ולאורך כל מחזור החיים של איסוף המידע והשימוש בו (Privacy by Design);

105.6. השימוש בנכסי המידע והגישה אליהם ייוחסו לאדם, חומרה או תוכנה, והפעילות תתועד ותנוטר בכפוף לסעיף 61.7 לעיל "ניהול נתיב ביקורת מבוסס קבצי LOG" (ראה גם פרק י': "ניטור מערך טכנולוגיית המידע");

105.7. לא תתאפשר גישה בלתי מורשית לנכסי מידע או פגיעה אחרת באבטחת המידע גם בעת התרחשות שגיאה, בין אם נגרמה בזדון ובין אם נגרמה בשוגג (Error Handling);

105.8. אימות כל גורם בטרם הסתמכות עליו (Never trust always verify) כגון במודל Zero Trust;

105.9. הפרדת תפקידים הנאכפת באמצעות הקצאה נאותה של תפקידים ותחומי אחריות;

105.10. תכנון בקרות שאוכפות תאימות למדיניות אבטחת המידע והגנת הסייבר והפחתת ההסתמכות על הגורם האנושי;

105.11. תכנון בקרות זיהוי ותגובה המבוססות על ההנחה כי בקרות המניעה כשלו (Assumed Breach);

105.12. תפיסה כוללת של מרחב הפעילות, לפיה מערך אבטחת מידע והגנת הסייבר יתחשב בגורמים כמו: מקומו של התאגיד הבנקאי במכלול שרשרת האספקה של המערכת הפיננסית, בשימוש בתשתיות ושירותים כלליים (כגון רשתות חברתיות), ובסיכונים הנובעים מאופי הפעילות אל מול הגורמים השונים במרחב, לרבות בחו"ל, חברות בנות (בישראל ובחו"ל), צדדים שלישיים ולקוחות;

105.13. תפיסת הגנה פרואקטיבית – ביסוס מערך דינאמי של אבטחת מידע, בעל יכולות פרואקטיביות. בין היתר, באמצעות נקיטת הצעדים הבאים:

105.13.1. ביצוע מיפוי וניתוח עדכניים של הסביבה בה התאגיד הבנקאי פועל על מנת לזהות פגיעויות בנכסי המידע;

105.13.2. איסוף מידע תוך זיהוי וניתוח שוטפים של שיטות ודרכי תקיפה, כוונות ופעילות של גורמי איום במרחב הסייבר, תוך יישום עקרונות של מודעות מצבית ושיתוף מידע עם גורמים רלוונטיים אחרים לצורך הפקת מידע אופרטיבי, ניתוח תרחישים ו"חשיבה מחוץ לקופסה", אשר יסייעו לחיזוק מערך אבטחת מידע והגנת הסייבר, והסביבה התפעולית כנגד מתקפות פוטנציאליות;

105.13.3. פיתוח יכולת תגובה מהירה ואפקטיבית לאירוע אבטחת מידע וניהולו, על מכלול היבטיו ולאורך כל שלביו;

105.13.4. פיתוח יכולות הטעיה, הסטה ועיכוב לאירוע אבטחת מידע באמצעות שימוש בטכניקות ובטכנולוגיות ייעודיות (כדוגמת "מלכודות דבש" (Honeypots));

105.13.5. פיתוח עמידות תפעולית ויכולת התאוששות ובכלל זה יכולת לספוג את השלכותיו של שיבוש תפעולי משמעותי כתוצאה מאירוע אבטחת מידע, תוך המשך ניהול תהליכים ושירותים חיוניים, ושיקום הפעולות העסקיות לאחר שחל שיבוש כאמור עד לרמה מספקת לצורך מילוי התחייבויות העסקיות;

105.13.6. פיתוח יכולות חקירה, תחקיר, הפקת לקחים ושימור ידע בנוגע לאירועים, תוך שימוש במנגנונים חוקיים ושיתוף פעולה עם גורמי אכיפה, במידת הצורך, לצורך מיצוי הדין עם האחראים.

<u>מדיניות אבטחת המידע והגנת הסייבר</u>

106. תאגיד בנקאי יתייחס במדיניות אבטחת המידע והגנת הסייבר (ראה סעיף 15 לעיל), בין היתר, לנושאים הבאים:

106.1. מחוייבות וציפיות הדירקטוריון וההנהלה הבכירה;

106.2. מטרות ויעדי מדיניות אבטחת המידע והגנת הסייבר;

106.3. התאמת המדיניות לסביבה החוקית והרגולטורית, לרבות הצורך בעמידה בתקנים וסטנדרטים מקובלים;

106.4. תיאור הכלים והמתודולוגיות להערכת סיכוני אבטחת מידע ואופן השימוש בהם בהתאם למתואר בפרק ג' "מסגרת לניהול סיכוני טכנולוגיית המידע (כללי)";

106.5. הקצאת משאבים לצורך יישום המסגרת לניהול אבטחת מידע;

106.6. בקרות לניהול זהויות ולניהול גישה לוגית - ראה סעיפים 116-120 להלן;

106.7. בקרות אבטחת מידע בשלבי מחזור החיים של נכס המידע – ראה סעיפים 112-115 להלן;

106.8. ניהול של פתרונות טכנולוגיים לאבטחת מידע – ראה סעיפים 128-129 להלן;

106.9. ארכיטקטורת אבטחת מידע כוללת, המפרטת הנחיות לעיצוב סביבת טכנולוגיית המידע בהיבט האבטחה, והכוללת את כל נכסי המידע, ובכלל זה: סגמנטציה של הרשת, בקרות על נקודות קצה (end point controls), תכנון נקודות כניסה (Gateway) לרשת, אימות, ניהול זהויות, בקרות בממשק (interface controls), תוכנות, תכנון ומיקום של פתרונות אבטחת מידע ובקרות;

106.10. היבטי אבטחת מידע בעבודה מרחוק;

106.11. ניטור וניהול אירועי אבטחת מידע, לרבות זיהוי וסיווג אירועי אבטחת מידע, הנחיות דיווח ואסקלציה, שימור ראיות ותחקור האירוע;

106.12. שמירה על אבטחת מידע בעת התקשרות עם צד ג';

106.13. הגדרה מהו שימוש מקובל בנכסי מידע בהיבטי אבטחת מידע, בנוגע לשימוש בנכסים אלו על ידי עובדים, עובדים חיצוניים וזמניים וצד ג';

106.14. היבטי אבטחת מידע בתהליכי גיוס ומיון עובדים לרבות עובדים חיצוניים (contractors) וזמניים;

106.15. פירוט תפקידים ותחומי אחריות בתחום אבטחת מידע, וביניהם:

106.15.1. תפקידים במסגרת לניהול סיכון אבטחת מידע: תחזוקה, ניטור, ציות (מדיניות ונהלים), הדרכה ומודעות;

106.15.2. תפקידי אבטחת מידע ספציפיים: מנהל הגנת הסייבר ואבטחת המידע, מנהלי מערכת;

106.15.3. אחריותם של בעלי נכסי מידע ומשתמשי הקצה;

106.15.4. תפקידים הקשורים בניהול סיכונים, בקרות ועמידה במסגרת לניהול אבטחת מידע והגנת הסייבר;

106.15.5. אחריות על דיווחים להערכת אפקטיביות המסגרת לניהול אבטחת המידע;

106.15.6. תפקידי היחידות העסקיות.

106.16. בקרות גישה פיזית ובקרות סביבתיות – ראה סעיף 122 להלן;

106.17. שימוש בטכניקות קריפטוגרפיות ובפרט הצפנת נתונים – ראה סעיף 127 להלן.

106.18. פיתוח או קינפוג על ידי משתמשי קצה – ראה סעיף 130.3 להלן.

106.19. קישוריות התאגיד הבנקאי לרשת ציבורית – ראה סעיף 135.2 להלן.

106.20. מנגנונים להערכת העמידה במסגרת אבטחת המידע ולהערכת האפקטיביות שלה.

107. מדיניות אבטחת המידע והגנת הסייבר תתועד ותמציתה תתוקשר לכל העובדים ולכל צד ג', בהיבטים הרלבנטיים לפעילותם.

פרק ח': יישום בקרות אבטחת מידע

108. על מנת להגן על נכסי המידע, תאגיד בנקאי יישם בקרות אבטחת מידע תוך התייחסות להיבטים הבאים:

108.1. פגיעויות ואיומים על נכס המידע;

108.2. רמת הקריטיות ורמת הרגישות של נכס המידע;

108.3. השלב במחזור החיים בו נמצא נכס המידע;

108.4. מזעור החשיפה לתרחישים חמורים אך סבירים של אירועי אבטחת מידע.

109. במידה ונכסי המידע מנוהלים באמצעות צד ג', נדרש התאגיד הבנקאי לבחון האם בקרות אבטחת המידע המיושמות או המתוכננות ליישום על ידי אותו צד ג' לצורך הגנה על נכסי המידע של התאגיד הבנקאי, הינן בהתאם למקובל בתחום הפעילות של צד ג', בהתאם לבקרות אבטחת המידע המקובלות בתאגיד הבנקאי עצמו, ובהתאם לאופי נכסי המידע המעורבים. כל פער שזוהה, יטופל בהתאם להערכת סיכונים.

110. במסגרת הבחינה בסעיף 109 לעיל, יתחשב התאגיד הבנקאי גם ביכולתו במסגרת החוזה עם צד ג' לבחון את בקרות אבטחת המידע המיושמות אצל גורם אחר שבו אותו צד ג' עושה שימוש לצורך ביצוע תכולת ההתקשרות עבור התאגיד הבנקאי.

זיהוי, הערכה והטמעת בקרות בהתייחס לפגיעויות ואיומי אבטחת מידע

111. תאגיד בנקאי יבצע תהליך שוטף לזיהוי, ולהערכה של פגיעויות ואיומים קיימים ומתגבשים, עבור נכסי מידע קריטיים ורגישים ובכלל זה נכסי מידע שבאמצעותם ניתן לסכן נכסי מידע קריטיים ורגישים, ויישם בקרות מתאימות להפחתתם. לצורך כך, תאגיד בנקאי נדרש, בין היתר:

111.1. לבצע תהליך כאמור בהתאם לשינויים פנימיים וחיצוניים, ובכללם שינויים עסקיים, ארגוניים, טכנולוגיים ושינויים במערך הפגיעויות והאיומים;

111.2. לפתח פעילויות תיקון (Remediation activities) לסביבת הבקרה (מניעה, זיהוי ותגובה) התואמות את מתאר הסיכון;

111.3. ליישם מנגנונים המאפשרים גישה מהירה למידע מודיעיני ממקורות פנימיים וחיצוניים, וניתוח מהיר של המידע בהתייחס לפגיעויות, איומים, שיטות תקיפה, ואמצעי התגוננות. תמונת האיום והחשיפה לסיכון אבטחת מידע תיגזר, בין היתר, מהמידע הבא: מיפוי גורמי איום רלבנטיים, בחתך מוטיבציה ויכולות; טכניקות, טקטיקות, תרחישים ואמצעי תקיפה; חולשות, הגדרות מערכת, או פגיעויות שעלולות לשמש כר להתקפות; פעולות שננקטו בעבר בתגובה להתקפה, התקפות שאירעו בעבר (בתאגיד הבנקאי או בסביבת הפעילות); דרכים ואינדיקטורים לגילוי וזיהוי התקפות; דרכי התמודדות עם התקפות.
מידע זה ישמש כבסיס לקבלת החלטות מושכלת, תעדוף של דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת;

111.4. לשתף מידע במידת הצורך וככל שניתן, עם מחזיקי העניין בתאגיד הבנקאי, לרבות גופים ממשלתיים, גורמים במערכת הפיננסית ולקוחות, בנוגע לאיומים ולאמצעי התגוננות

בפניהם. איסוף ושיתוף המידע יתבצע בכפוף לדין ובכלל זה בהתאם להנחיות המפקח על הבנקים;

111.5. ליישם מנגנונים לשיבוש השלבים השונים של התקפה על נכסי המידע (שלבי התקפה לדוגמא, פעולה מקדימה להכרת השטח, ניצול פגיעות, השתלת נוזקה, שימוש בחולשה להשגת הרשאות (privilege escalation), וגישה בלתי מורשית).

בקרות אבטחת מידע בשלבי מחזור החיים של נכס המידע

112. תאגיד בנקאי יישם בקרות אבטחת מידע בכדי להגן על נכסי המידע, באופן התואם, בין היתר, את שלב מחזור החיים בו נמצא נכס המידע, יוודא באופן שוטף את האפקטיביות שלהן עבור כל שלב במחזור החיים ויעריך את שלמותן. מחזור החיים כולל את השלבים הבאים לפחות: תכנון ועיצוב, רכישה ויישום, תמיכה ותחזוקה, הוצאה משימוש והשמדה.

113. תאגיד בנקאי יישם בקרות תכנון ועיצוב בשלבים הראשונים של מחזור החיים על מנת לוודא שאבטחת המידע משולבת בתוך נכסי המידע. הפתרונות שייושמו יתאמו לדרישות אבטחת מידע כפי שמופיעות במסגרת לניהול אבטחת המידע.

114. תאגיד בנקאי יישם בקרות רכישה ויישום על מנת לוודא שאבטחת המידע לא נפגעת בעת הוספת נכס מידע חדש, בין אם באמצעות רכישה ובין אם באמצעות פיתוח, וכן בקרות תמיכה ותחזוקה שוטפות על מנת לוודא כי נכסי המידע ימשיכו לעמוד בדרישות אבטחת המידע של התאגיד הבנקאי. בקרות אלו יכללו בין היתר התייחסות לתחומים הבאים:

114.1. ניהול שינויים – בקרות המטפלות באבטחת המידע כחלק מתהליך ניהול השינויים ומעדכנות באופן שוטף את רשימת המצאי של נכסי המידע - ראה הרחבה בסעיפים 123-124 להלן: "אבטחת מידע בתהליך ניהול השינויים" וכן בסעיף 125 להלן "רכישה ופיתוח תוכנה מאובטחת";

114.2. ניהול תצורה (Configuration) – בקרות המוודאות שתצורת נכסי המידע ממזערת פגיעויות, ושהיא מוגדרת, מוערכת, מתועדת, ומתוחזקת גם כאשר מתגלים ומטופלים פגיעויות ואיומים חדשים (ראה גם סעיף 61.2 לעיל "ניהול תצורה");

114.3. ניהול יישום וסביבות - בקרות המוודאות שסביבות הפיתוח, הבדיקות והייצור מופרדות בצורה נאותה, מאובטחות ומסייעות לאכיפת הפרדת תפקידים - ראה הרחבה בפרק ו' לעיל: "ניהול פרויקטים וניהול שינויים";

114.4. בקרות גישה המוודאות שרק משתמשים, תוכנות וחומרות מורשים, יכולים לגשת לנכסי המידע - ראה הרחבה בסעיפים 116-120 להלן: "בקרות לניהול זהויות ולניהול גישה לוגית";

114.5. בקרות המונעות פרצות אבטחה הנגרמות מנכסי חומרה ותוכנה שהוכנסו למערך טכנולוגיית המידע של התאגיד הבנקאי באופן בלתי מורשה;

114.6. תכנון רשתות - בקרות המוודאות שרק תעבורת רשת מורשית עוברת, ואשר מפחיתות את השפעתן של פרצות אבטחה;

114.7. בקרות ניהול פגיעויות המוודאות זיהוי וטיפול בפגיעויות אבטחת מידע באופן מהיר ובהתאם להערכת סיכונים;

114.8. בקרות ניהול טלאים להערכה של טלאים ועדכונים אחרים עבור פגיעויות שהתגלו, וליישום שלהם בזמן הולם (ראה פירוט בסעיף 61.4 לעיל בנושא: "ניהול טלאים");

114.9. בקרות ניטור המזהות במהירות פגיעה באבטחת המידע;

114.10. בקרות תגובה לניהול אירועי אבטחת מידע (ראה הרחבה בפרק י"א "ניהול אירועים ובעיות" להלן) ומנגנונים לטיפול בליקויים שהתגלו בבקרות;

114.11. בקרות ניהול קיבולת וביצועים המוודאות כי הזמינות אינה נפגעת בעקבות הפעילות העסקית הנוכחית או הצפויה - ראה פירוט בסעיף 61.6 לעיל "ניהול קיבולת וביצועים";

114.12. בקרות ניהול שירותי צד שלישי המוודאות עמידה בדרישות אבטחת המידע של התאגיד הבנקאי;

114.13. בקרות המוודאות באופן רציף את פעילותן התקינה של בקרות אבטחת המידע המיושמות (Continuous Control Monitoring).

115. תאגיד בנקאי יישם בקרות הוצאה משימוש והשמדה ייעודיות כדי לוודא כי אבטחת המידע לא תיפגע כשנכסי המידע מגיעים לסוף מחזור חייהם. הבקרות כוללות, בין היתר, שיטות ארכוב ומחיקת מידע רגיש לפני השמדת נכס המידע - ראה פירוט בסעיף 61.8 לעיל "מחיקת נתונים והשמדת מדיה".

<u>בקרות לניהול זהויות ולניהול גישה לוגית</u>

116. להלן עקרונות לקביעת בקרות לניהול זהויות ולניהול גישה לוגית:

116.1. תאגיד בנקאי יקבע בקרות לניהול זהויות ולניהול גישה לוגית, ובכלל זה יקבע אמצעי זיהוי ואימות אישיים לכל גורם בעל גישה לנכס מידע כתנאי מוקדם למתן הגישה.

116.2. במקרים חריגים בהם לא ניתן לקבוע אמצעי זיהוי ואימות אישיים, למשל כאשר קיימות מגבלות טכנולוגיות המונעות זאת, יישם תאגיד בנקאי בקרות מפצות מתאימות.

116.3. בקרות ניהול הזהויות וניהול הגישה הלוגית תאפשרנה גישה לנכסי מידע רק כאשר קיים צורך עסקי ברור, וכל עוד הצורך קיים.

117. במתן הרשאות גישה לנכס מידע יתחשב התאגיד הבנקאי בין היתר בהיבטים שונים של הערכת סיכונים וביניהם: התפקיד העסקי של המשתמש, מיקומו הפיזי, גישה מרחוק, זמן ומשך הגישה, מצב הטלאים והתוכנות נגד נוזקות, התוכנה, מערכת ההפעלה, המכשיר, אופן ההתחברות ומידת הקריטיות והרגישות של נכס המידע.

118. תאגיד בנקאי יישם תהליכים כך שאמצעי הזיהוי והאימות האישיים:

118.1. יונפקו, ינוהלו, יאומתו, יבוטלו ויבוקרו עבור רכיבים, משתמשים, תהליכים ותוכנות מורשים.

118.2. יונפקו, ימסרו, יופעלו ויוחלפו באופן שיאפשר לוודא, בין היתר, כי מידע רגיש לא ייחשף בתהליך ההנפקה והמסירה.

119. חוזקם של אמצעי הזיהוי והאימות ייקבע בהתאם להשלכותיהם האפשריות של זיהוי ואימות שגויים על התאגיד הבנקאי ועל לקוחותיו. מבלי לפגוע בכלליות האמור, במקרים הבאים ייעשה

שימוש באימות מוגבר (כגון: אימות רב גורמי (Multi Factor Authentication)) התואם את הערכת הסיכונים הרלבנטית:

119.1. גישת מנהל מערכת או גישה של משתמש אחר בעל הרשאות מוגברות לנכס מידע קריטי או רגיש;

119.2. גישה מרחוק באמצעות רשת ציבורית לנכס מידע קריטי או רגיש;

119.3. פעילויות שהוגדרו בסיכון גבוה בהתאם לעקרונות שאושרו על ידי הדירקטוריון.

120. על אף האמור בסעיף 119 לעיל, על לקוחות המשתמשים בשירותי בנקאות בתקשורת כהגדרתם בהוראת נ.ב.ת. מספר 367 בנושא: "בנקאות בתקשורת" יחולו הסעיפים הרלבנטיים בהוראה האמורה ולא בהוראה דנן.

מזעור החשיפה לתרחישים חמורים אך סבירים

121. תאגיד בנקאי יבחן תרחישים חמורים אך סבירים של אירועי אבטחת מידע העלולים להשפיע עליו, מבחינה פיננסית או אחרת לדוגמא, פגיעה במוניטין או אי עמידה בדרישות הרגולציה, ולסכן את פעילותו העסקית. בחינה זו תסייע לו בזיהוי ויישום בקרות נוספות למניעת או הפחתת השפעתם של תרחישים אלו. בין היתר ייבחנו התרחישים הבאים:

121.1. פעולות זדוניות המבוצעות על ידי תוקף בעל הרשאות מיוחדות מתוך התאגיד הבנקאי, המסתייע בגורם פנימי או חיצוני;

121.2. מחיקה או השחתה של נתונים בסביבת הייצור ובסביבת הגיבוי, באופן מכוון, בעקבות טעות אנוש או בעקבות תקלה במערכת;

121.3. אובדן או גישה בלתי מורשית למפתחות הצפנה השומרים על נכסי מידע קריטיים או רגישים מאוד.

בקרות גישה פיזית ובקרות סביבתיות

122. תאגיד בנקאי ידאג להגדיר, לתעד וליישם בקרות גישה פיזית ובקרות סביבתיות על מנת להגן על מתקניו לרבות סניפיו ומרכזי הנתונים (Data Center) שלו, גם אלו המנוהלים על ידי צד ג', מגישה בלתי מורשית ומסיכונים סביבתיים. בין היתר, תתייחסנה הבקרות לנושאים הבאים:

122.1. קביעת מיקום ומבנה שיספק הגנה מפני איומים הנובעים מאיתני הטבע ומגורמים אנושיים. בקרות אלו יכללו התייחסות גם לגיוון הגישה לגורמים (sources) הנותנים שירותים חיוניים למתקנים כמו: חשמל ותקשורת, כמו גם התייחסות למנגנוני גיבוי לשירותים אלו שייכנסו לפעולה באופן מיידי (לדוגמא: גנרטור, UPS (Uninterrupted Power Supply);

122.2. הגבלת גישה לאזורים השונים כמו: המתקן, חדר המחשב, מארזי שרתים, וזאת הן לעובדים לרבות עובדים חיצוניים וזמניים, הן לצדדים שלישיים והן לאורחים בהתאם לתפקידיהם ותחומי אחריותם. הרשאות הגישה תסקרנה באופן תקופתי על מנת לוודא ביטול מהיר של הרשאות שאין בהן צורך;

122.3. שמירה על מצב הסביבה בתוך טווח ערכים מוגדר מראש, לדוגמא: מערכות איוורור, מערכות מיזוג אוויר, מערכות לכיבוי אש (בקרות סביבתיות). בקרות אלו תיושמנה בהתאם לחשיבות המתקן ומידת הקריטיות והרגישות של הפעילויות ומערכות המידע הממוקמות בו;

122.4. התקנת מערכות לגילוי והתרעה של אירועי אבטחת מידע במקרה בו בקרות הגישה הפיזית והבקרות הסביבתיות כשלו. בקרות לדוגמא: גלאים וחיישנים של נפח, טמפרטורה, מים, לחות, עשן, זמינות שירותים (כגון: הפסקת חשמל ובעיות בתקשורת).

אבטחת מידע בתהליך ניהול השינויים

123. תאגיד בנקאי יישם בקרות בתהליך ניהול השינויים בנכסי המידע לרבות שינויים בחומרה, תוכנה, בנתונים ובתצורה, בין אם מתוכננים ובין אם כתגובה בחירום, במטרה לוודא כי אבטחת המידע נשמרת.

124. בקרות אלו יכללו, בין היתר:

124.1. בדיקות אבטחה (Security Testing) לזיהוי פגיעויות ולווידוא כי דרישות אבטחת מידע יושמו. אופי הבדיקות יהיה תואם את היקף השינוי שבוצע ואת הקריטיות והרגישות של נכס המידע המושפע מהשינוי;

124.2. הפרדת תפקידים במטרה למנוע מהעובדים להטמיע שינויים עצמאיים בסביבת הייצור;

124.3. פיתוח ואישור השינויים בסביבה אחרת, המופרדת באופן נאות מסביבת הייצור, על מנת להימנע מפגיעה באבטחת המידע.
לעניין שינוי חירום שלא ניתן ליישם לגביו את תהליך ניהול השינויים הרגיל – ראה סעיף 97 לעיל;

124.4. תיקוף יישומן של דרישות אבטחת המידע לפני העברת השינוי לייצור בהתאם להערכת סיכונים;

124.5. שימוש בנתוני דמה במסגרת הפיתוח והבדיקות וככל שהדבר חיוני, שימוש בנתוני אמת לאחר הפיכתם ללא רגישים (לדוגמא: מחיקת שמות ומספרי ת.ז./ח.פ.) וזאת לאחר קבלת אישור מהגורמים המתאימים בתאגיד הבנקאי;

124.6. צמצום למינימום, יישום בקרות מפצות ככל שניתן, וקבלת הסכמה מראש של הגורם המתאים, במקרה של שינויים הכרוכים ביצירת פגיעויות אבטחת מידע שלא ניתן לטפל בהן.

רכישה ופיתוח מערכת מאובטחת

125. תאגיד בנקאי יישם תהליכים לפיתוח ולרכישת מערכת מאובטחת שיסייעו בשמירה על היבטי סודיות, שלמות וזמינות, באמצעות שיפור איכות התוכנה ומזעור פרופיל הפגיעות שלה. התהליכים יבדקו, בין היתר, כי המערכת:

125.1. ממשיכה לפעול כמתוכנן גם בעת התרחשות אירועים בלתי צפויים, לרבות כאשר מוכנס קלט שגוי;

125.2. נבנתה כך שתקשה על שימוש לא נכון, בין במזיד, ובין בשוגג;

125.3. עומדת בדרישות המסגרת לניהול אבטחת המידע של התאגיד הבנקאי.

בקרות גישה לאמצעים המאפשרים חשיפה של מידע רגיש

126. תאגיד בנקאי יישם בקרות גישה לאמצעים המאפשרים חשיפה בלתי מורשית של מידע רגיש, לרבות בשל טעות אנוש, שתוצאתה היא אובדן סודיות המידע (להלן: "בקרות דלף מידע") כדלקמן:

126.1. תאגיד בנקאי יעניק גישה לאמצעים המאפשרים הסרה, העתקה, הפצה או חשיפה אחרת של מידע רגיש, על בסיס הערכת סיכונים ורק כאשר קיים צורך עסקי או צורך תפעולי לכך.

126.2. תאגיד בנקאי יישם בקרות דלף מידע, תהליכיות וטכנולוגיות, התואמות את רמת הקריטיות והרגישות של המידע, באותם מקומות בהם קיים חשש לדלף של מידע רגיש. בקרות אלו יכללו בין היתר:

126.2.1. קיום תהליך של מתן הרשאת גישה לאמצעים והתקנים להעברת מידע, הכולל רישום ובחינה תקופתית של המשתמשים. משתמשים בעלי הרשאות גישה למידע רגיש יהיו נתונים לבקרה מוגברת;

126.2.2. חסימה, סינון וניטור נאותים של אמצעים אלקטרוניים להעברת מידע, של אתרים ושל אמצעים להדפסה;

126.2.3. הצפנה נאותה (ראה סעיף 127 להלן בנושא: "שימוש בטכניקות קריפטוגרפיות"), קיום תהליך לריקון אמצעים והתקנים להעברת מידע לאחר גמר השימוש בהם, וקיום נתיב ביקורת על התקנים;

126.2.4. הפרדה נאותה של מידע המבוססת על רגישות וצרכי גישה;

126.2.5. קיום תהליך של ניטור לצורך זיהוי תוכנות וחומרות שאינן מורשות לפעול בארגון (לדוגמא, תוכנה לרישום הקלדות (key loggers), תוכנה לפיצוח סיסמאות, נקודות גישה אלחוטיות).

שימוש בטכניקות קריפטוגרפיות

127. תאגיד בנקאי יישם טכניקות קריפטוגרפיות (שיטות המשמשות להצפנת נתונים, אימות זהויות והבטחת שלמות הנתונים) בהתאם לעקרונות הבאים:

127.1. תאגיד בנקאי ישתמש בטכניקות קריפטוגרפיות לצורך בקרת גישה לנתוניו שבתנועה ושבמנוחה ושהוגדרו ברמת קריטיות ורגישות גבוהה, וזאת הן ברשת הפרטית והן ברשת ציבורית או ברשת שהוא לא יכול לאכוף את מדיניות אבטחת המידע והגנת הסייבר שלו בה. הטכניקה הקריפטוגרפית וחוזקה ייקבעו, בין היתר, בהתאם למידת הקריטיות והרגישות של הנתונים, לאופי הפעילות, ולבקרות הנוספות הקיימות, ובלבד שיעשה שימוש בטכניקה להצפנת נתונים. על אף האמור לעיל, לגבי נתונים במנוחה הנמצאים ברשת הפנימית של התאגיד הבנקאי, ייעשה שימוש בטכניקה להצפנת נתונים באותם מקרים בהם מדיניות אבטחת מידע בנושא הצפנת נתונים מחייבת זאת.

127.2. לעניין נתונים (בתנועה או במנוחה) שלא הוגדרו ברמת קריטיות ורגישות גבוהה:

127.2.1. ברשת ציבורית או ברשת שהתאגיד הבנקאי לא יכול לאכוף את מדיניות אבטחת המידע והגנת הסייבר שלו בה - העברת נתונים, תיעשה, לכל הפחות, תוך שימוש בטכניקות הצפנה מקובלות כאמור בסעיף 127.4 להלן.

127.2.2. ברשת פרטית – השימוש בטכניקות קריפטוגרפיות לצורך הגבלת גישה אל נתונים אלו יקבע בהתאם להערכת סיכונים שתתחשב, בין היתר, במידת הקריטיות והרגישות של הנתונים, באופי הפעילות, ובבקרות נוספות .

127.3. תאגיד בנקאי יצפין את תווך תעבורת הרשת (פרטית או ציבורית או ברשת שאין לו יכולת לאכוף את מדיניות אבטחת המידע והגנת הסייבר שלו בה) בהתאם להערכת סיכונים שתתחשב, בין היתר, במידת הקריטיות והרגישות של הנתונים העוברים בה, באופי הפעילות, ובבקרות נוספות.

127.4. טכניקות הקריפטוגרפיה תבחרנה מתוך סטנדרטים בינלאומיים מקובלים, ותיבחנה באופן תקופתי על מנת לוודא את המשך התאמתן לפגיעויות ולאיומים הרלבנטיים.

127.5. האמור בסעיפים 127.1-127.3 לעיל לא יחול במקרים הבאים, ובמקומו תחולנה ההנחיות הרלבנטיות באותה הוראה:

127.5.1. הדרישות וההחרגות לעניין הצפנה שבמסגרת הוראת נ.ב.ת. מס' 367 בנושא: "בנקאות בתקשורת".

127.5.2. ההסדר המפורט בסעיף 33 להוראה 362.

127.6. תאגיד בנקאי יקבע בקרות לניהול נאות של המפתחות הקריפטוגרפיים, ובכלל זה חילול, הפצה, אחסון, חידוש, ביטול תוקף, שחזור, ארכוב והשמדה, במטרה להפחית את הסיכון לפגיעה באבטחת המידע שלהם.

127.7. תאגיד בנקאי יקבע בקרות להגבלת גישה למפתחות הקריפטוגרפיים.

<u>פתרונות טכנולוגיים לאבטחת מידע</u>

128. תאגיד בנקאי יישם פתרונות טכנולוגיים על מנת לשמור על אבטחת המידע של נכסי המידע השונים. פתרונות אלו כוללים, בין היתר, Firewalls, בקרות גישה לרשת, מערכות לאיתור ולמניעת ניסיונות חדירה (IDS/IPS), תוכנות נגד נוזקות, מסנני תוכן (Content Filtering), כלי הצפנה, כלי ניטור וכלי ניתוח של רישום ממוכן (Log).

129. רמת היישום של בקרות מחזור החיים על הפתרונות הטכנולוגיים תהיה בהתאמה לרמת ההסתמכות על פתרונות אלו לצורך אבטחת מידע. בין בקרות מחזור החיים תכללנה הבקרות הבאות:

129.1. הנחיות המפרטות באילו מקרים ומצבים יש להשתמש בכל פתרון טכנולוגי;

129.2. מסמכים המתעדים את היעדים והדרישות מכל פתרון טכנולוגי;

129.3. הסמכת גורמים שרשאים לעשות שינויים בפתרונות הטכנולוגיים תוך התחשבות בעקרון הפרדת תפקידים;

129.4. הערכה שוטפת של תצורת הפתרונות הטכנולוגיים (Configuration) לצורך בחינת האפקטיביות שלה ולגילוי שינויים בלתי מורשים בה;

129.5. סקירה תקופתית של הפרקטיקה המקובלת בעולם;

129.6. יישום אמצעים המספקים התרעה במידה והפתרונות הטכנולוגיים אינם פועלים כראוי.

פיתוח על ידי משתמשי קצה

130. תאגיד בנקאי יישם עקרונות לפיתוח על ידי משתמשי קצה בתאגיד הבנקאי, ובכלל זה:

130.1. תאגיד בנקאי יגדיר תהליכים לזיהוי מקרים של פיתוח או קינפוג תוכנה על ידי משתמשי קצה ולהערכת החשיפה לסיכון במקרים אלו.

130.2. פיתוח או קינפוג על ידי משתמשי קצה, של תוכנה המהווה נכס מידע שהינו קריטי להשגת היעדים העסקיים או המעבד מידע או נתונים רגישים, נדרש לעמוד בבקרות הרלוונטיות לאורך מחזור חיי הנכס. על התאגיד הבנקאי לנהל תיעוד מתאים של נכסי מידע כאמור.

130.3. תאגיד בנקאי יקבע מדיניות לפיתוח או קינפוג על ידי משתמשי קצה. המדיניות תפרט בין היתר, באילו מקרים מותר פיתוח או קינפוג תוכנה על ידי משתמשי קצה, כמו גם את ציפיות התאגיד הבנקאי בנוגע לבקרות הנדרשות לאורך מחזור חיי הנכס, ובכלל זה בקרות בנושאי אבטחת מידע, פיתוח, ניהול שינויים וגיבויים.

מערכות מורשת (Legacy)

131. נכס מידע שהוטמע לפני החלת המסגרת הקיימת לניהול אבטחת המידע ואשר אינו עומד בדרישותיה, יוחלף או שיטופל בהתאם למדיניות לחריגה ממסגרת לניהול אבטחת המידע שקבע התאגיד הבנקאי.

טכנולוגיות חדשות

132. תאגיד בנקאי יישם עקרונות לשימוש בטכנולוגיות חדשות בתאגיד הבנקאי, ובכלל זה:

132.1. השימוש בטכנולוגיות חדשות בסביבת הייצור ייעשה בהתאם להנחיות לעניין מוצר חדש בהוראה 310, ובתנאי שמתקיים אחד מהתנאים הבאים:

132.1.1. הטכנולוגיה הגיעה למצב בשלות שבו קיימת מוסכמה באשר לבקרות אבטחת מידע שיש ליישם בקשר אליה.

132.1.2. קיומן של בקרות מפצות המפחיתות את הסיכון השיורי לרמת התיאבון לסיכון של התאגיד הבנקאי (לדוגמה: הפרדת רשתות).

132.2. על אף האמור לעיל, תאגיד בנקאי המבקש לבחון טכנולוגיה חדשה שאינה עומדת בתנאים המפורטים בסעיף 132.1 לעיל, רשאי לעשות כן בכפוף לתנאים הבאים:

132.2.1. גיבוש גישה אסטרטגית ברורה והוליסטית מתאימה לגבי אימוץ חדשנות בפעילותו.

132.2.2. זיהוי והערכה של הסיכונים הנובעים מהטכנולוגיה החדשה, תוך וידוא כי קיימים תהליכי בקרה נאותים לניהול מותאם של סיכונים אלו.

132.2.3. שימוש בסביבה מבוקרת לצורך בחינת הטכנולוגיה, לרבות הגבלת היקף הפעילות, הגבלת מספר הלקוחות ויידועם בדבר הבחינה של הטכנולוגיה החדשה וההשלכות האפשריות עליהם.

עבודה מרחוק

133. תאגיד בנקאי יוודא כי גישת עובדים מרחוק לנכסי המידע תתאפשר רק ממכשירים העומדים בעקרונות ובדרישות שנקבעו במסגרת לניהול אבטחת המידע לרבות לעניין הצפנה, בקרות גישה, דלף מידע, ובכפוף להדרכה מתאימה.

134. הוצאה ושימוש של תדפיסים מחוץ לכותלי התאגיד הבנקאי על ידי עובד לרבות עובד חיצוני וזמני תעשה בכפוף לאמור בהוראת ניהול בנקאי תקין מס' 356 בנושא: "הוצאת מסמכים ממשרדי התאגידים הבנקאיים", ותוך שמירה על כל העקרונות והדרישות שנקבעו במסגרת לניהול אבטחת המידע והגנת הסייבר לעניין זה, לרבות לעניין מניעת דלף מידע.

קישוריות התאגיד הבנקאי לרשתות ציבוריות

135. קישוריות התאגיד הבנקאי לרשתות ציבוריות תתבצע לפי העקרונות הבאים:

135.1. תאגיד בנקאי יקבע מנגנונים נאותים להגנה על נוכחותו המקוונת (Online Presence), ובפרט, למול הסיכונים הכרוכים בפעילותו ברשתות החברתיות.

135.2. הנהלת תאגיד בנקאי תקבע את מדיניות התאגיד הבנקאי לקישוריות לרשת ציבורית, בהתבסס על הערכת סיכונים מתאימה תוך נקיטת אמצעי בקרה נאותים כמפורט בסעיפים 128-129 לעיל.

פרק ט': הערכת אפקטיביות בקרות אבטחת מידע

136. תאגיד בנקאי ימפה את בקרות אבטחת המידע המיושמות ויעריך על בסיס מתמשך את רמת הבשלות, אפקטיביות התכנון, היישום והתפעול של אותן בקרות, באמצעות תוכנית בדיקות שיטתית.

137. תאגיד בנקאי יגבש עקרונות לקביעת היקף ותדירות הבדיקות, ובכלל זה:

137.1. היקף ותדירות הבדיקות יבטיחו כי חלק מספק מבקרות אבטחת המידע של התאגיד הבנקאי ייבדק לפחות אחת לשנה וכל הבקרות לפחות אחת לשלוש שנים, על מנת לוודא כי בקרות אבטחת המידע נותרו אפקטיביות. בנוסף, על תוכנית הבדיקות להתחשב, בין היתר, במידת הקריטיות והרגישות של נכס המידע, ובהשלכות אפשריות של אירוע אבטחת מידע על נכס המידע.

137.2. מבלי לגרוע מהאמור בסעיף 137.1 לעיל, תאגיד בנקאי יבצע בדיקה להערכת אפקטיביות התכנון, היישום והתפעול של הבקרות, בכל מקרה של שינוי מהותי בפגיעויות ובאיומים על נכס המידע, בנכס המידע או בסביבה הטכנולוגית בה הוא פועל, וכן לקראת הכנסתו לשימוש של נכס מידע חדש.

137.3. על אף האמור בסעיף 137.1 לעיל, בקרות הקשורות לנכסי מידע החשופים לסביבות שבהן התאגיד הבנקאי לא יכול לאכוף את מדיניות אבטחת המידע והגנת הסייבר שלו, תיבדקנה במשך השנה.

138. תאגיד בנקאי יגבש עקרונות לקביעת סוג הבדיקות ולטיפול בממצאיהן:

138.1. תאגיד בנקאי יקבע את סוגי הבדיקות הנדרשות בהתאם לסוג הבקרה הנבדקת, מתוך מגוון הכלים המקובלים בתחום ותוך התחשבות, בין היתר, בשיקולים הבאים: קצב השינויים בפגיעויות ובאיומים, מידת הקריטיות והרגישות של נכס המידע, ההשלכות של התממשות אירוע אבטחת מידע, המהותיות והתדירות של השינויים בנכס המידע. בדיקות לדוגמא: סקר פערים מול תקנים מקובלים של אבטחת מידע, סקר ציות, סקירת קוד מקור, סקר פגיעויות, ניסיונות חדירה מבוקרים ומבדקי "צוות אדום".

138.2. תאגיד בנקאי יקבע מראש את קריטריוני ההצלחה לבדיקה, לרבות הנסיבות שבהן תידרש בדיקה חוזרת.

138.3. תוצאות הבדיקות תדווחנה להנהלה הבכירה, יחד עם המלצות לפעולות מתקנות. ההנהלה הבכירה תשלים את דיוניה בממצאי הבדיקות והשלכותיהם, ותקבל את ההחלטות המתחייבות, לרבות קביעת לוח זמנים ליישומן. ההנהלה הבכירה תעקוב באופן מסודר אחר יישום החלטות אלו. כל התהליך יבוצע תוך פרק זמן סביר לאחר מועד תחילת ביצוע הבדיקות.

138.4. ממצאים מהותיים שעלו בבדיקות וכן כל ממצא המצביע על ליקויים בבקרות אבטחת מידע ואשר לא ניתן לתקנו בזמן סביר, יובא לידיעת הדירקטוריון או ועדה דירקטוריונית מתאימה. הזמן הסביר לתיקון ממצא ייקבע בין היתר, בהתאם למהות הממצא, ומידת הקריטיות והרגישות של נכס המידע אשר בקרת אבטחת המידע מיושמת לגביו.

139. הבדיקות תבוצענה באמצעות גורמים בעלי ידע, מומחיות ומיומנות המתאימים לביצוע הבדיקות, עצמאיים ובלתי תלויים בפעילותן ובתפעולן של הבקרות הנבדקות, וזאת על מנת למנוע ניגודי עניינים. מידת העצמאות ואי התלות תקבע, בין היתר, בהתאם לסוג ולחשיבות הבדיקה המתבצעת.

140. כאשר נכסי המידע של התאגיד הבנקאי מנוהלים באמצעות צד ג', והתאגיד הבנקאי נסמך על בדיקות להערכת אפקטיביות הבקרות של אותו צד ג', על התאגיד הבנקאי להעריך האם תדירות וסוג הבדיקות הנערכות לגבי אותם נכסי מידע, נקבעים על סמך העקרונות המפורטים בסעיפים 138.1-137 ו – 139 לעיל. תאגיד בנקאי יעריך את ההשפעה של כל פער שיימצא על יכולתו להמשיך ולהשתמש בשירותי צד ג'.

חלק ה' - ניהול אירועים

פרק י': ניטור מערך טכנולוגיית המידע

141. תאגיד בנקאי יקבע מדיניות ונהלים לזיהוי בעיות מתהוות או חריגות (אנומאליות) על מנת למנוע מהן באופן פרואקטיבי מלהתפתח לאירועי כשל טכנולוגי או לאירועי אבטחת מידע (להלן בחלק זה: "אירועים"), להבין את אופי האירועים, להתמודד איתם, להפחית את השפעתם, ולתמוך בתחקיר האירוע (ראה גם פרק י"א – "ניהול אירועים ובעיות"). כחלק מפעילות הניטור המתמשכת, תאגיד בנקאי יישם יכולות אפקטיביות ונאותות לזיהוי ולדיווח על פגיעה בסודיות, שלמות וזמינות של נכס מידע, וכן לזיהוי חדירה פיזית או לוגית. תהליכי הניטור והזיהוי המתמשכים יכללו גם את ההיבטים הבאים:

141.1. חריגות (אנומאליות) ברמה הטכנולוגית (פעילות וביצועי המערכות – שליטה ובקרה) וברמת הפעילות העסקית;

141.2. טרנזקציות - לצורך זיהוי שימוש לרעה בהרשאה על ידי צד ג' או גורמים אחרים מחוץ ומתוך התאגיד הבנקאי;

141.3. גורמים רלבנטיים פנימיים וחיצוניים, לרבות בעלי תפקידים בפונקציות העסקיות ובפונקציות האדמיניסטרטיביות של מערך טכנולוגיית המידע;

141.4. איומים פנימיים וחיצוניים פוטנציאליים.

142. תאגיד בנקאי יקבע תהליכים ומבנה ארגוני לצורך זיהוי ולצורך ניטור מתמיד של סיכוני טכנולוגיית המידע שיכולים להשפיע באופן משמעותי על היכולת שלו לספק שירותים. בכלל זה, תאגיד בנקאי:

142.1. יקיים מערך ניטור ובקרה אפקטיבי, אשר יהיה מאויש באופן רציף (7X24X365), יקבל דיווחים בזמן אמת מהמערכות השונות, לרבות מערכות תפעוליות ועסקיות, יזהה אינדיקטורים להתרחשות אירוע, וייזום פעילויות דיווח ותגובה במידת הצורך.

142.2. יבחן באופן שוטף את האופי המתפתח של מתאר האיומים והפרקטיקות המקובלות לניטור ולזיהוי שלהם, ומעת לעת תרחישי אירועי אבטחת המידע לצורך הערכת יכולתו לזהותם, ויעדכן בהתאם את תהליכי וכלי הניטור והזיהוי.

142.3. יישם אמצעים לזיהוי התממשות או פוטנציאל להתממשות סיכוני טכנולוגיית המידע, לדוגמא: דלף מידע אפשרי, קוד עוין ואיומי אבטחת מידע אחרים, וכן פגיעויות בתוכנה ובחומרה, ויבדוק מתן מענה מתאים, לדוגמא: באמצעות עדכוני אבטחת מידע חדשים.

143. מערכות הניטור תשולבנה עם מערכות אחרות בתאגיד הבנקאי בכדי לאפשר תהליך אפקטיבי של זיהוי וטיפול באירועים, לרבות: זיהוי אינדיקטורים לפעילות חריגה ומגמות, אחזור והעשרת מידע, חקירה ותיעוד, ניהול ידע וקבלת החלטות, יצירה וניהול התראות ודיווחים, תקשורת עם גורמים רלבנטיים וביצוע שינויים במערכות בזמן אמת.

פרק י"א: ניהול אירועים ובעיות

כללי

144. תאגיד בנקאי יישם תהליך לניהול אירועים שינטר אירועי כשל טכנולוגי ואירועי אבטחת מידע ויתעד אותם. התהליך לניהול אירועים יאפשר לתאגיד הבנקאי להמשיך או לחדש במהירות המירבית את פעילותם המאובטחת והיציבה של הפונקציות והתהליכים שנפגעו, כך שהשפעת האירוע על הפעילות העסקית של התאגיד הבנקאי ועל לקוחותיו תהיה מינימלית.

145. לצורך צמצום ההשפעה של אירועים שליליים ולצורך התאוששות מהירה, תאגיד בנקאי יקבע תהליכים ומבנים ארגוניים מתאימים (להלן: "המסגרת לניהול אירועים") שיבטיחו כי:

145.1. הטיפול, הניטור והצעדים שננקטים יהיו עקביים ומשולבים.

145.2. הגורם לאירוע יזוהה ויטופל כדי למנוע התרחשות חוזרת של האירוע.

146. המסגרת לניהול אירועים ולניהול בעיות (problem management) תתייחס, בין היתר, לנושאים הבאים:

146.1. נהלים לזיהוי, אבחון, תיעוד, ודירוג האירוע בהתאם לקריטיות ולרגישות התהליך העסקי שנפגע;

146.2. תחזוקה ושמירה של מידע הקשור לאירוע לצורך ביצוע תחקיר של האירוע ואבחון הגורם לו;

146.3. תפקידיהם ותחומי אחריותם של העובדים וגורמים חיצוניים בניטור, ניתוח, אסקלציה, קבלת החלטות, פתרון, ותיעוד, בתרחישי אירוע שונים דוגמת: טעויות, תקלות, מתקפות סייבר;

146.4. הקצאת משאבים מתאימים לעובדים לצורך מילוי תפקידם ותחומי אחריותם;

146.5. נהלים לניהול בעיות שמטרתם זיהוי, ניתוח, ופתרון של הגורם (root cause) לאירוע או למספר אירועים – תאגיד בנקאי יתעד אירועים שהשפיעו או שהיה להם פוטנציאל להשפיע על התאגיד הבנקאי ואשר זוהו או התרחשו בתוך או מחוץ לתאגיד הבנקאי, ינתח מגמות בהתרחשותם, יפיק מהם לקחים ויקבע אם נדרשים צעדי מניעה או תיקון בהתאם;

146.6. מערך דיווח פנימי נאות לגורמים בתוך התאגיד הבנקאי, לרבות נהלי דיווח על אירועים וקריטריונים להעלאת הדיווחים כלפי מעלה (אסקלציה) שמתייחסים גם לתלונות של לקוחות הקשורות לאבטחת מידע, שיבטיח כי:

146.6.1. אירועים בעלי פוטנציאל להשפעה שלילית גבוהה על נכסי מידע קריטיים ורגישים ידווחו להנהלה הבכירה, להנהלת טכנולוגיית המידע, ולגורמים הפנימיים הרלבנטיים האחרים.

146.6.2. בכל התרחשות של אירוע משמעותי יימסר דיווח מיידי לדירקטוריון אשר יכלול לכל הפחות את ההיבטים הבאים: השפעת האירוע, התגובה שננקטה, והבקרות הנוספות שתיושמנה לצורך טיפול באירוע.

146.7. תוכניות תגובה לצורך הפחתת ההשפעות הקשורות לאירוע ועל מנת לוודא שהשירות חוזר להיות פעיל ומאובטח בהקדם, וכן שילוב של תוכניות אלו עם תהליכי המשכיות עסקית לרבות התוכנית להמשכיות עסקית;

146.8. תוכנית לסקירה ולתרגול תוכניות התגובה של התאגיד הבנקאי לאירוע אבטחת מידע ולאירוע כשל טכנולוגי, אשר תבוצע בתדירות שלא תפחת מאחת לשנה לכל אחד מסוגי האירועים. על מנת לוודא את האפקטיביות של תוכניות התגובה ומידת התאמתן למטרה:

146.8.1. תוכנית הסקירה והתרגול, תכלול בין היתר, ביצוע תרגולים של מערכי התגובה השונים בתאגיד הבנקאי, תוך התחשבות בסוגי תרגול שונים (דימוי סוגים שונים של כשלים טכנולוגיים, התקפות, "משחקי מלחמה", וכיו"ב) ובהתייחס לגורמים המעורבים (למשל: גורמים טכניים, צוותי ניהול משבר, דרגי מקבלי החלטות, דוברות וכיו"ב).

146.8.2. תאגיד בנקאי יקבע מראש קריטריונים להצלחת התרגיל לרבות הנסיבות בהן יידרש תרגיל חוזר.

146.8.3. תוצאות התרגיל, יחד עם לוח זמנים ליישום ההחלטות שהתקבלו לתיקון הממצאים שעלו ממנו, ידווחו לגורמים המתאימים שיעקבו אחר יישומן.

146.9. תוכניות תקשור לגורמים חיצוניים בנוגע לפונקציות ולתהליכים עסקיים קריטיים שתתייחסנה בין היתר, לנושאים הבאים:

146.9.1. שיתוף הפעולה עם בעלי עניין בתאגיד הבנקאי וגורמים רלבנטיים אחרים לצורך מתן תגובה אפקטיבית לאירוע והתאוששות ממנו;

146.9.2. עדכון גורמים חיצוניים (לדוגמא: לקוחות, משתתפי שוק אחרים, רשויות רגולטוריות שונות) כפי שנדרש ובהתאם לרגולציה הרלבנטית;

146.9.3. ניהול ההיבטים התקשורתיים של האירוע.

146.10. שיתוף פעולה ותיאום מול צד ג' בנושאים הבאים, בהתאם לקריטיות ולרגישות של נכס המידע:

146.10.1. ביצוע תרגול תקופתי על ידי צד ג' לתוכניות התגובה שלו לאירועים הנוגעים בנכסי המידע של התאגיד הבנקאי המנוהלים על ידו.

146.10.2. הסכמה לגבי התפקידים ותחומי האחריות של כל צד במקרה של תגובה לאירוע הדורשת שיתוף פעולה ותיאום בין הצדדים, לרבות לעניין הממשק של תוכניות התגובה של התאגיד הבנקאי עם תוכניות התגובה של צד ג', ומעורבותו בתרגולים התקופתיים של התאגיד הבנקאי.

146.10.3. תיאום בין תוכניות התגובה של התאגיד הבנקאי לבין תהליכי ההמשכיות העסקית לרבות התוכנית להמשכיות עסקית הנהוגים אצל צד ג';

<u>אירועי אבטחת מידע</u>

להלן דגשים נוספים על אילו שפורטו בסעיפים 146-144 לעיל, שיש ליישם לגבי אירועי אבטחת מידע:

תגובה וניהול אירועי אבטחת מידע

147. בניהול אירוע אבטחת מידע יזהה התאגיד הבנקאי את השלב בו אירוע אבטחת המידע נמצא, וינהלו בהתאם למאפייניו כדלקמן:

147.1. זיהוי (Detection) - ביצוע בירור ראשוני בדבר קיומו של אירוע אבטחת מידע וגיבוש מהיר ככל האפשר של דפוס הפעילות הדרוש לשלב הבא אחריו.

147.2. ניתוח (Analysis) - ביצוע בירור מקיף ומעמיק ככל האפשר לגבי אירוע אבטחת המידע, לצורך קבלת החלטות ברמה האופרטיבית, גיבוש רשימת חלופות של דפוסי פעולה אפשריים לעצירת האירוע והחלטה על דרך הפעולה העיקרית לשלב ההכלה.

147.3. הכלה (Containment) - השגת שליטה ראשונית באירוע אבטחת המידע לצורך הכלתו ועצירת החמרתו והשגת יעדיו. ביצוע תהליך השתלטות על הגורם לאירוע לרבות על מערך התקיפה, בתוך התאגיד הבנקאי, ועצירה מלאה של ווקטור הנזק.

147.4. הכרעה (Eradication) - נטרול הגורמים לאירוע אבטחת המידע, לרבות רכיבי התקיפה שמצויים במערכות התאגיד הבנקאי, תוך שאיפה לבטל או למזער, ככל שניתן, את הנזק שכבר נגרם.

147.5. השבה (Recovery) - חזרה לתקינות ופעילות מלאה של כל פעילות אצל התאגיד הבנקאי בו התרחש אירוע אבטחת המידע אשר פגע באבטחת המידע שלו, תוך כדי גרימה להשבתתו, הגבלתו או הפרעה בתפקודו.

148. התאגיד הבנקאי יקבע נוהלי דיווח, ניהול, תגובה וסיום של אירוע אבטחת מידע ושל התרעה ממקור מהימן על אירוע אבטחת מידע, בין אם אמור להתרחש, ובין אם כבר התרחש או מתרחש, אך טרם זוהה על ידי התאגיד הבנקאי, בהתאם לחומרתו ובהתאם לשלבי הטיפול באירוע.

149. לצורך ניהול אירוע אבטחת מידע יקים התאגיד הבנקאי חדר מצב, ויגדיר בראיה משולבת כלל-תאגידית, את קבוצת העובדים אשר יאיישו אותו, את תפקידיהם, סמכויותיהם, גורמי דיווח פנימיים וחיצוניים, דרכי תקשורת, כלי עבודה וכן נוהלי עבודה פרטניים.

150. תאגיד בנקאי יבצע רישום ומעקב מסודר של אירועי אבטחת מידע שטופלו והפעולות שננקטו בידי הגורמים הרלבנטיים. בפרט, התאגיד הבנקאי ינהל "יומן אירועים" בו יתועדו, בסמוך ככל הניתן למועד ההתרחשות, מכלול הידיעות, ההחלטות והפעולות שבוצעו בקשר לאירוע אבטחת מידע.

151. תאגיד בנקאי יגדיר מאגר של פעילויות תגובה (כדוגמת שינויי קונפיגורציה, הגבלה או הסטה של תקשורת, פריסה של תוכנות וכיו"ב) בהתאם לתרחישים השונים, והגדרה של התנאים שבהם יינקטו פעילויות התגובה, את אופן יישומן הפרטני, את בעלי הסמכות להורות על הפעלתן, את ערוצי היידוע והאישורים הנדרשים, ואת אופן הערכת יעילות התגובה באירוע אבטחת המידע המסוים שבמסגרתו הופעלה.

152. תאגיד בנקאי יגדיר סולם של רמות כוננות ופעילויות נדרשות, בהתאם להתראות ולתרחישים השונים, כגון: צפי לביצוע התקפה מאורגנת; כמות וחומרת התקפות שזוהו בתאגיד הבנקאי, במגזר, או במדינה; גילוי חולשה מהותית או זיהוי כלי תקיפה המהווה איום ישיר על התאגיד הבנקאי.

חלק ו' - שונות

פרק י"ב: דיווח בנושא סיכוני טכנולוגיית המידע וסיכוני אבטחת מידע

153. הדוחות הסדירים המוגשים להנהלה ולדירקטוריון בנושאי סיכונים תפעוליים כנדרש בהוראה 350, יכללו התייחסות פרטנית לסיכוני טכנולוגיית המידע ולסיכוני אבטחת מידע.

154. דוחות סיכוני טכנולוגיית המידע וסיכוני אבטחת מידע יכללו, בין היתר:

154.1. שימוש במדדים תפעוליים לזיהוי סיכוני טכנולוגיית המידע בפעילות מערך טכנולוגיית המידע;

154.2. שימוש במדדי הערכה איכותיים וכמותיים לצורך כימות החשיפה לסיכוני אבטחת מידע, באופן אשר יאפשר מעקב אחרי שינויים בערכים אלו מעת לעת;

154.3. הפרות של התיאבון לסיכון ושל ספים, הגבלות או דרישות איכותיות שנקבעו עבור סיכוני טכנולוגיית המידע;

154.4. פירוט של אירועי אבטחת מידע ואירועי כשל טכנולוגי בהתאם לקריטריונים שקבע התאגיד הבנקאי, כולל ניתוח הגורמים לאירועים אלו;

154.5. אירועים ונתונים חיצוניים רלבנטיים, שיש להם השפעה פוטנציאלית על התאגיד הבנקאי, לרבות שינויים רגולטוריים.

פרק י"ג: ניהול סיכונים מול צדדים שלישיים

155. מקורם של חלק מסיכוני טכנולוגיית המידע להם חשוף התאגיד הבנקאי הינו בצד ג' (כדוגמת סיכוני טכנולוגיית המידע בשרשרת האספקה (Supply Chain)). בהתאם לכך, ובנוסף לדרישות היציבותיות הקשורות למיקור חוץ המפורטות בהוראה 359A ובהוראה 362, בהוראה זו שזורות הנחיות ספציפיות לניהול סיכונים אלו במגוון נושאים - ראה נספח: "הנחיות לניהול סיכונים מול צדדים שלישיים".

פרק י"ד: ניהול המשכיות עסקית (BCM)

156. משמעות המונחים בפרק זה, המופיעים גם בהוראה 355, תהיה כמשמעותם בהוראה 355 בנושא: "ניהול המשכיות עסקית".

157. תאגיד בנקאי יקבע תהליכים טכנולוגיים מתאימים בהתאם למפורט בפרק זה, לצורך תמיכה בתהליך לניהול המשכיות עסקית שייקבע על פי הוראה 355.

ניתוח השלכות עסקיות (BIA)

158. תאגיד בנקאי יוודא כי מערכות המידע והשירותים הטכנולוגיים מתוכננים בהלימה לניתוח ההשלכות העסקיות שבהוראה 355, ומותאמים אליו.

תכנון המשכיות עסקית (BCP)

159. תוכנית ההמשכיות העסקית תביא בחשבון סיכונים שיכולים לפגוע במערכות המידע או בשירותים הטכנולוגיים. התוכנית תתמוך בהגנה על סודיות, שלמות וזמינות של הפעילויות העסקיות, התהליכים התומכים ונכסי המידע, ובמידת הצורך בהשבתם לאחר שנפגעו. תאגיד בנקאי יקבע תוכנית זו בתיאום עם בעלי עניין פנימיים וחיצוניים רלוונטיים, בהתאם לצורך.

160. תאגיד בנקאי יקבע את תוכנית ההמשכיות העסקית כך שתבטיח שיוכל להגיב בצורה נאותה לתרחישי כשל פוטנציאליים ויוכל לאושש את התהליכים והשירותים החיוניים שלו במקרה של שיבושים, בתוך זמן התאוששות (RTO) ונקודת שחזור רצויה (RPO) שנקבעו מראש. במקרים של שיבוש תפעולי משמעותי שמפעיל תוכניות המשכיות עסקית ספציפיות, תאגיד בנקאי יתעדף פעילויות המשכיות עסקית תוך שימוש בגישה מבוססת סיכונים, אשר יכולה להתבסס, בין היתר, על הערכת הסיכונים בהתאם לסעיף 46 לעיל.

161. תאגיד בנקאי יתייחס בתוכנית ההמשכיות העסקית למגוון תרחישים שונים אליהם הוא עלול להיחשף, לרבות תרחישים חמורים אך סבירים ולרבות תרחישי מתקפת סייבר, ויעריך את ההשפעה הפוטנציאלית שעלולה להיות לתרחישים אלה על התהליכים והשירותים החיוניים. בהתבסס על תרחישים אלה, התוכנית תתאר כיצד תובטח הרציפות התפקודית של מערכות המידע והשירותים הטכנולוגיים, כמו גם אבטחת המידע של התאגיד הבנקאי.

תוכנית התאוששות מאסון (DRP)

162. בהתבסס על ניתוח ההשלכות העסקיות ותרחישים חמורים אך סבירים כאמור, תאגיד בנקאי יכין תוכנית התאוששות מאסון. תוכנית זו צריכה להגדיר באילו תנאים תופעל התוכנית, ואילו פעולות נדרש לבצע על מנת להבטיח את הזמינות, ההמשכיות וההתאוששות של מערכות מידע ושירותים טכנולוגיים התומכים בתהליכים ובשירותים החיוניים לתאגיד הבנקאי. תוכנית ההתאוששות מאסון תתאם את יעדי ההתאוששות של פעילויות התאגיד הבנקאי.

163. תוכנית ההתאוששות מאסון תיתן מענה לאפשרויות התאוששות הן לטווח הקצר והן לטווח הארוך. התוכנית צריכה להיות:

163.1. ממוקדת בהתאוששות תפקודים של תהליכים ושירותים חיוניים ובתהליכים טכנולוגיים ונכסי מידע תומכים והתלויות ביניהם, למניעת פגיעה בתפקוד התאגיד הבנקאי ובמערכת הבנקאית.

163.2. מתועדת וזמינה ליחידות העסקיות וליחידות הטכנולוגיות, ונגישה בעת חירום.

163.3. מעודכנת ומתחשבת בהפקות לקחים שנלמדו מאירועים, בדיקות ותרגולים, סיכונים חדשים שזוהו ושינויים שבוצעו בניתוח ההשלכות העסקיות, ביעדי ההתאוששות ובתעדוף יעדי ההתאוששות.

164. התוכנית תכלול התייחסות לאופציות אלטרנטיביות למקרה שההתאוששות בטווח הקצר לא תהיה ברת ביצוע בגלל עלויות, סיכונים, לוגיסטיקה או נסיבות בלתי צפויות מראש.

165. התוכנית תכלול אמצעים לשמירה על המשכיות שיישמו לצורך מזעור כשלים אצל צדדים שלישיים אשר להם השפעה מרכזית על תפקוד מערך טכנולוגיית המידע של התאגיד הבנקאי (בהתאם להנחיות בעניין ספקים ונותני שירות חיוניים בהוראה 355, הוראה 359A והוראה 362, ככל שהוראות אלו רלבנטיות לצד ג' הנדון).

בדיקת ותרגול תוכנית התאוששות מאסון (DRP)

166. תוכנית ההתאוששות מאסון עבור תהליכים טכנולוגיים ונכסי מידע התומכים בתהליכים ובשירותים חיוניים, והתלויות ההדדיות ביניהם (לרבות אלה הניתנים באמצעות צדדים שלישיים) תיבדק לפחות אחת לשנה.

167. תוכנית ההתאוששות מאסון תתעדכן לכל הפחות אחת לשנה, בהתבסס על תוצאות הבדיקות, מידע עדכני על איומים, ולקחים שהופקו מאירועים קודמים. יש להתייחס לכל שינוי ביעדי ההתאוששות וזמן ההתאוששות או שינוי בתהליכים ובשירותים החיוניים, התהליכים הטכנולוגיים ונכסי מידע התומכים, במידת הצורך.

168. בדיקת תוכנית ההתאוששות מאסון של התאגיד הבנקאי תוודא את יכולתו להמשיך בפעילותו עד אשר התהליכים והשירותים החיוניים שנפגעו יחזרו לתפקוד. לצורך כך הבדיקות יכללו, לכל הפחות, את המאפיינים הבאים:

168.1. מערך בדיקות נאות של תרחישים חמורים אך סבירים, לרבות אלו אשר נלקחו בחשבון בעת הפיתוח של תוכנית ההמשכיות העסקית (לרבות בדיקת שירותים המסופקים באמצעות צדדים שלישיים כאשר הדבר ישים). מערך הבדיקות יכלול, בין היתר, בדיקה של יכולת העברת התהליכים הטכנולוגיים ונכסי המידע התומכים בתהליכים ובשירותים חיוניים, לפתרון חלופי שיאפשר את הרציפות התפקודית של התאגיד הבנקאי (לדוגמא, בדיקה של יכולת העברת הפעילות מאתר המחשב המרכזי לפתרון חלופי במקרה של כשל בו), ובדיקה כי התאגיד הבנקאי מסוגל לתפקד בדרך זו למשך תקופת זמן מתאימה, ולאחר מכן לשוב לפעילות רגילה.

168.2. אתגור ההנחות עליהן מבוססת תוכנית ההתאוששות מאסון.

168.3. תהליכים לווידוא יכולתם של העובדים, עובדים חיצוניים, ושל מערכות המידע והשירותים הטכנולוגיים להגיב באופן נאות לתרחישים שהוגדרו בסעיף 168.1 לעיל.

169. על תוצאות הבדיקה להיות מתועדות. יש לנתח ולתת מענה לכל הליקויים שזוהו כתוצאה מהבדיקה ולדווח אותם להנהלה הבכירה ולדירקטוריון.

פרק ט"ו: בנק חוץ

170. ההוראה תחול על בנק חוץ, למעט השינויים המפורטים להלן:

170.1. בכל מקום בהוראה, הביטוי "טכנולוגיית המידע/מערך טכנולוגיית מידע" יוחלף בביטוי "מערך טכנולוגיית המידע המקומי, לרבות הממשקים של מערך זה עם מערך הבנק בחו"ל".

170.2. לסעיף 61.5 תתווסף הפסקה הבאה: "בנק חוץ ישמור בכל עת, במערכות המידע המקומיות בסניפיו בישראל, נתונים מלאים המכילים את כל הפרטים האישיים והמנהליים לגבי בעלי החשבונות, מיופי הכח וזכויות החתימה, וכן את כל היתרות העדכניות של החשבונות המנוהלים בסניפיו בישראל".

170.3. לסעיף 138.4 להוראה יתווסף הסעיף הבא: "תמצית ניהולית של תוצאות הבדיקות יחד עם המלצות לפעולות מתקנות, תועברנה לממונה על הגנת הסייבר ואבטחת המידע בבנק האם".

פרק ט"ז: דיווחים לפיקוח על הבנקים

171. תאגיד בנקאי ידווח למפקח על הבנקים על הנושאים והאירועים הבאים:

171.1. אירועי כשל טכנולוגי ואירוע אבטחת מידע בהתאם לנדרש בהוראת ניהול בנקאי תקין מס' 366 בנושא "דיווח על אירועי כשל טכנולוגי ואירועי סייבר";

171.2. מינוי מנהל טכנולוגיית המידע ועזיבתו הצפויה כמפורט בסעיף 26 לעיל או מינוי מנהל הגנת הסייבר ואבטחת המידע ועזיבתו הצפויה כמפורט בסעיף 34 לעיל.

171.3. מינוי ממלא מקום בפועל לתקופה של למעלה מחודש של מנהל טכנולוגיית המידע כמפורט בסעיף 26 לעיל, ושל מנהל הגנת הסייבר ואבטחת המידע כמפורט בסעיף 34 לעיל.

171.4. החלטה על שינויים מהותיים צפויים באסטרטגיה או במדיניות ניהול טכנולוגיית המידע, הסבה מהותית של מערכות המחשוב או מחשוב מחדש של מערכות מרכזיות ודומיהם.

עדכונים

מס' חוזר	פרטים	גרסה	תאריך
2799	חוזר מקורי	1	18/11/24

נספח – הנחיות לניהול סיכונים מול צדדים שלישיים

בהוראה זו שזורות הנחיות לניהול סיכונים מול צדדים שלישיים במגוון נושאים, וביניהן :

1. חובת הדירקטוריון להתייחס בכל דיוניו גם להיבטים העולים משימוש התאגיד הבנקאי בצד ג' לצורך ניהול נכסי המידע שלו – ראה סעיף 18 לעיל.
2. יישום תהליך לזיהוי (Identification) של כל נכסי המידע של התאגיד הבנקאי לרבות אלו המנוהלים באמצעות צד ג' ומיפויים – ראה סעיף 43.2 לעיל ;
3. תוכנית להדרכה ולהגברת המודעות בנושאי אבטחת מידע– ראה סעיף 53 לעיל ;
4. החוסן התפעולי של סביבת מחשוב ענן המשמשת לצורך אספקת פעולות חיוניות ללקוחות התאגיד הבנקאי – ראה סעיף 56.2 לעיל.
5. התשתית הטכנולוגית של התאגיד הבנקאי המנוהלת על ידי צד ג' – ראה סעיף 58.1 לעיל.
6. תהליך הגיבויים – ראה סעיף 61.5.3 לעיל.
7. היבטי קיבולת – ראה סעיף 61.6.6 לעיל.
8. העברת קבצי Log – ראה סעיף 61.7.5 לעיל.
9. הסדרים למחיקת נתונים של התאגיד הבנקאי המאוחסנים אצל צד ג' – ראה סעיף 61.8.3 לעיל.
10. תהליך התכנון וההשקעה בטכנולוגיית המידע – ראה סעיף 64.2 לעיל.
11. תהליך ניהול הרכישה של מערכת – ראה סעיף 78-75 לעיל.
12. פיתוח API – ראה סעיפים 91-84 לעיל.
13. הערכת יכולת אבטחת מידע - ראה סעיף 102 לעיל.
14. מסגרת לניהול אבטחת מידע והגנת הסייבר – ראה סעיף 103 לעיל.
15. מדיניות אבטחת המידע והגנת הסייבר – ראה סעיפים 106.12-106.13 ו – 107.
16. יישום בקרות אבטחת מידע על נכסי מידע המנוהלים באמצעות צד ג' – ראה סעיפים 110-109 לעיל.
17. בקרות ניהול שירותי צד שלישי המוודאות עמידה בדרישות אבטחת מידע של התאגיד הבנקאי – ראה סעיף 114.12 לעיל.
18. בקרות גישה פיזית ובקרות סביבתיות – ראה סעיף 122 לעיל.
19. הערכת אפקטיביות הבקרות של נכסי מידע המנוהלים באמצעות צד ג' – ראה סעיף 140 לעיל.
20. שיתוף פעולה ותיאום מול צד ג' במקרה של התרחשות אירוע – ראה סעיף 146.10 לעיל.
21. תוכנית התאוששות מאסון (DRP) – ראה סעיף 165 להלן.
22. בדיקת ותרגול תוכניות התאוששות מאסון (DRP) – ראה סעיף 168.1 לעיל.

יצויין כי ריכוז זה מובא לצורך נוחות הקורא, וכי בכל מקרה של סתירה בין האמור בנספח זה לבין האמור בגוף ההוראה, האמור בגוף ההוראה הוא זה הקובע.