בנק ישראל
הפיקוח על הבנקים
אגף מדיניות והסדרה

כ״ה באדר תשע״ה
16 במארס 2015
חוזר ח – 06 - 2457

לכבוד
התאגידים הבנקאיים וחברות כרטיסי אשראי

הנדון: **ניהול הגנת הסייבר**

(ניהול בנקאי תקין הוראה מס׳ 361)

כללי

1. לאחרונה חל גידול באיומי הסייבר, שחשופים להם מוסדות פיננסיים בעולם ובישראל. איומים אלו מתאפיינים, בין היתר, בתחכום גובר והולך של ההתקפות, בעוצמת הנזק הפוטנציאלי, בקושי לזהות התקפות וביכולות של היריבים. נוכח העובדה שישראל - ובפרט המגזר הפיננסי - מהווים יעד להתקפה מצד יריבים שונים, התאגידים הבנקאיים בישראל חשופים אף יותר, לאיומי הסייבר. מתוך הכרה במרכזיותם של איומי הסייבר במערך האיומים שבפניהם ניצב התאגיד הבנקאי, עלה הצורך לקבוע הוראה מיוחדת לנושא ניהול הגנת הסייבר.
2. פרסום הוראה מיוחדת לנושא ניהול הגנת הסייבר כאמור, בא להדגיש את גישת הפיקוח על הבנקים כי התמודדות עם סיכוני הסייבר מהווה נושא חוצה-ארגון, המחייב מעורבות פעילה של הדרגים הבכירים בתאגיד הבנקאי. על אף שסיכוני הסייבר נובעים משימוש בטכנולוגיות, הם אינם מהווים סוגיה טכנולוגית גרידא, אלא גם סוגיה עסקית-אסטרטגית.
3. ההוראה כוללת הסדרה של דרישות וציפיות של הפיקוח על הבנקים מהתאגידים הבנקאיים בנושא ניהול הגנת הסייבר. היא קובעת מסגרת מובנית, אך גמישה, לניהול סיכוני הסייבר, תוך מתן חופש לתאגיד הבנקאי במימושה. דרך הסדרה זו נועדה לאפשר לתאגיד הבנקאי להתאים באופן דינאמי את מערך ההגנה למפה העדכנית של איומי הסייבר.
4. לאור זאת, ההוראה אינה מפרטת ״רשימת בקרות״ סגורה, אלא מגדירה עקרונות להגנת הסייבר. הציפייה הינה שהתאגיד הבנקאי יאמץ עקרונות אלו בבניית מערך הגנת הסייבר בהתאם להיקף ומהות פעילותו ופרופיל הסיכון שלו. במידת הצורך, יפורסמו נספחים להוראה שיכילו הנחיות פרטניות בנושאים רלבנטיים. כך למשל, בנושא הסדרת העבודה מול

מרכז הגנת הסייבר המגזרי, לכשיוקם. בנוסף, מומלץ להתייחס לתקנים מקובלים בתחום הגנת הסייבר.

5. בהמשך לפרסום הוראה זו, בכוונת הפיקוח על הבנקים לפרסם הוראה להסדרת נושא אבטחת המידע. במסגרת זו, תבוצע לפי הצורך ההתאמה בין ההוראות.
6. לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגידה, קבעתי את הוראת הניהול התקין הבאה, כמפורט להלן.

מבנה ההוראה

7. ההוראה כוללת חמישה פרקים:

(א) **פרק א': כללי** –מבוא להוראה, פירוט עקרונות יסוד לניהול הגנת הסייבר, תחולה והגדרות.

(ב) **פרק ב': ממשל תאגידי** - מפרט את תפקידי הדירקטוריון וההנהלה הבכירה, מתאר את תפקיד מנהל הגנת הסייבר, ומערכי הניהול, תיאום ובקרה הנחוצים לצורך קיום הגנה אפקטיבית.

(ג) **פרק ג': אסטרטגיית הגנה ומסגרת לניהול סיכוני הסייבר** – עוסק בתפיסת הגנת הסייבר, הגדרת אסטרטגיית הגנת סייבר, קביעת מסגרת לניהול סיכוני הסייבר, הגדרת מדיניות הגנת סייבר וגיבוש תכניות עבודה.

(ד) **פרק ד': ניהול סיכוני הסייבר** - מפרט את הדרישה לקיום תהליך ניהול סיכוני סייבר מסודר, לרבות זיהוי הסיכונים, הערכת סיכונים, קביעה והערכה של בקרות הגנת הסייבר ודיווח על סיכונים.

(ה) **פרק ה' : יעדי בקרה ובקרות הגנת סייבר** – עוסק ביעדי הבקרות שעל התאגיד לבסס כדי לצמצם את החשיפה לאיומי הסייבר, לרבות: אבטחת סביבת הפעילות, הגנה פרואקטיבית, צמצום מעטפת התקיפה, הגנה לעומק, ראיה תהליכית, הגורם האנושי, שיתוף מידע ומודיעין, ניטור בקרה וזיהוי אירוע סייבר, תגובה וניהול אירוע סייבר, תרגולים ודיווח על אירוע סייבר.

מבוא (סעיפים 1 – 6 להוראה)

8. ההוראה קובעת כי על התאגידים הבנקאיים לתת דגש מיוחד ולנקוט בצעדים הדרושים לצורך ניהול אפקטיבי של סיכוני הסייבר. בפרט, נדרשים התאגידים הבנקאיים להרחיב ולהעמיק את היכולות הקיימות של מערך אבטחת המידע באופן אשר יאפשר להם להתמודד כנגד איומי הסייבר.
9. ההוראה רואה את ניהול סיכוני הסייבר כחלק מהמערך הכולל של ניהול הסיכונים בתאגיד הבנקאי. ככזו, ההוראה נועדה להשתלב במערך הקיים של הוראות ניהול בנקאי תקין, תוך

הוספת פירוט והעמקה בכל הנוגע להיבטי ניהול סיכוני הסייבר. הוראה זו אינה מחליפה הוראות אחרות, ובפרט את הוראת ניהול בנקאי תקין – "ניהול טכנולוגיית המידע" - מס' 357 (להלן: הוראה 357). בהקשר זה יודגש שמעבר לסיכון תפעולי, סיכון הסייבר מהווה גם סיכון אסטרטגי וסיסטמי לתאגיד הבנקאי.

עקרונות לניהול הגנת הסייבר (סעיפים 7 – 11 להוראה)

10. ניהול הגנת הסייבר של תאגיד בנקאי יתבסס על עקרונות היסוד המפורטים בפרק ג' להוראה.
11. ניהול סיכוני הסייבר יתבצע במסגרת תהליך, בהתאם לעקרונות ניהול סיכונים הרלבנטיים לכל תהליכי ניהול הסיכונים, כמפורט בהוראות ניהול בנקאי תקין הרלבנטיות. ההוראה מפרטת את ההוראות הרלבנטיות ואת הדגשי היישום וההקשר לאותן הוראות.
12. ניהול נאות של סיכוני הסייבר מחייב הרחבה והתאמה של המסגרת הקיימת של ניהול סיכוני טכנולוגיית המידע בתאגיד הבנקאי בהיבטי תפיסת מרחב האיום ויכולות ההגנה הנדרשות. הוראה 357 מתייחסת לבקרות אבטחת מידע ובקרות טכניות לניהול סיכוני טכנולוגיית מידע. הוראת ניהול הגנת הסייבר מתמקדת במנגנונים ובתהליכים הנדרשים לניהול הסיכון, ביעדי הגנת הסייבר וההרחבות הנדרשות ביכולות ההגנה, ולבסוף – גם בבקרות הייעודיות הנדרשות לצורך השגת יעדי הגנה.

תחולה (סעיף 12 להוראה)

13. תחולת ההוראה לניהול הגנת הסייבר תואמת לתחולת הוראת ניהול בנקאי תקין מס' 357.

הגדרות (סעיף 13 להוראה)

14. ההגדרות נועדו ליצור "שפה" אחידה לצורך הוראה זו, תוך התמקדות בהגדרות להן נודעת משמעות מעשית לצורך יישום ההוראה.
15. לעניין הגדרת "ניהול אירוע סייבר", ההוראה מתייחסת ל- 5 שלבים בתהליך זה. עם זאת, התאגיד הבנקאי רשאי לאחד בין שלבים, כל עוד נשמר רצף הפעילות בין השלבים המאוחדים.
16. נוכח המאפיינים של איומי הסייבר ותרחישי התקיפה, תקלה תפעולית עלולה להתברר בהמשך כאירוע סייבר. לפיכך, הציפייה היא שבמקרה של תקלה תפעולית במערך טכנולוגיית המידע, תהיה מעורבות, לפי העניין, של מנהל הגנת הסייבר.

ממשל תאגידי (סעיפים 14 – 24 להוראה)

דירקטוריון והנהלה בכירה

17. ההוראה מפרטת את תחומי האחריות של הדירקטוריון ושל ההנהלה הבכירה. מעורבותם של גופים אלה מהווה גורם מפתח ביכולתו של התאגיד הבנקאי לנהל באופן אפקטיבי את הגנת

הסייבר. בהתאם, הציפייה היא שהתאגיד הבנקאי ייצור את מנגנוני הבקרה והדיווח הנדרשים לצורך כך.

18. לעניין קבלת דיווח תקופתי, כאמור בסעיף 16 (ו) יובהר כי ניתן לשלב את הדיווח הנדרש על פי סעיף זה בדיווח הנדרש לפי סעיפים 34-33 להוראת ניהול בנקאי תקין מס' 350.

מנהל הגנת הסייבר

19. כדי לספק הגנה אפקטיבית, בראייה חוצת ארגון, נדרש קיומה של פונקציה מתכללת ייעודית לנושא, אשר משלבת מגוון תחומים, גם אלו שאינם משתייכים לניהול טכנולוגיית המידע, כגון: זיהוי הונאות, המשכיות עסקית, הגנה פיזית, כוח אדם, ציות ועוד.
20. בהתאם לכך, ההוראה קובעת כי התאגיד הבנקאי ימנה עובד בכיר בעל ידע וניסיון מתאימים כמנהל הגנת הסייבר. ההוראה אינה מכתיבה מבנה ארגוני וחלוקת סמכויות בתחום הגנת הסייבר. עם זאת, על תאגיד בנקאי לוודא כי מיקומו הארגוני וסמכויותיו של מנהל הגנת הסייבר יתמכו בתפקידו כגורם מנחה, מפקח ומתכלל של הפעילויות והתהליכים הרלבנטיים, לרבות ברמה העסקית-אסטרטגית של כלל פעילות התאגיד, ולא רק של ניהול טכנולוגיית המידע.
21. האפקטיביות של מנהל הגנת הסייבר באה לידי ביטוי ביכולתו להשפיע על החלטות בתאגיד. הציפייה בהקשר זה היא שמנהל הגנת הסייבר יביע את דעתו באופן עצמאי אל מול המנהלים האחראים על קווי העסקים ועל ניהול טכנולוגיית המידע, ושלעמדותיו יינתן משקל מהותי בקבלת ההחלטות.
22. מנהל הגנת הסייבר יכול לשמש גם כמנהל אבטחת מידע, ובלבד שלא יווצרו ניגודי עניינים בין התפקידים השונים.

מערכי ניהול, תיאום ובקרה משיקים

23. תכלול היבטי סיכוני הסייבר בתאגיד הבנקאי משקף תפיסה הוליסטית של טיפול בסיכוני הסייבר בתאגיד הבנקאי, אשר באה לידי ביטוי, בין היתר, ביצירת קווי דיווח וכפיפות מקצועית וארגונית לגורמים הרלבנטיים, כמפורט בהוראה.

אסטרטגיית הגנה ומסגרת לניהול סיכוני הסייבר (סעיפים 25 – 33 להוראה)

24. ההוראה מתווה מסגרת מובנית לניהול סיכוני הסייבר, אשר מושתתת על תפיסת הגנת הסייבר כמפורט בהוראה. רשימת העקרונות לקיום מערך הגנת סייבר אפקטיבי ויעיל, המובאת בהוראה, אינה מהווה רשימה סגורה. היא נועדה לספק קווים מנחים באשר לתורת ההפעלה והיעדים האסטרטגיים של מערך הגנת הסייבר. בהמשך ההוראה, בפרק ה' מפורטים הדרכים והמנגנונים למימושם של אלה.

25. אסטרטגיית הגנת הסייבר מהווה מסמך יסוד אותו מתווה דירקטוריון התאגיד הבנקאי. האסטרטגיה מתמקדת במטרות העל ויעדי הגנת הסייבר. ההוראה מפרטת את הנושאים שיש לכלול במסמך האסטרטגיה. הציפיה היא כי מסמך האסטרטגיה יעודכן, על פי הצורך, בהתאם להתפתחות איומי הסייבר, ובכל מקרה לפחות אחת לשלוש שנים.

26. התאגיד הבנקאי יקבע בכתב את המסגרת לניהול סיכוני הסייבר. המסגרת מסדירה את האופן שבו יממש התאגיד הבנקאי את תהליך ניהול סיכוני הסייבר, לרבות מנגנונים ארגוניים, כלים ומתודולוגיות, ותהליכים כמפורט בהוראה.

27. מדיניות הגנת הסייבר התאגידית קובעת את הבקרות ודרכי הפעולה לצמצום איומי הסייבר. ההוראה מפרטת את הנושאים שיש לכלול במסמך המדיניות. הציפייה היא כי מסמך המדיניות יעבור הערכה לפחות אחת לשנה.

28. מסמכי מדיניות ההגנה הפרטניים יכללו עקרונות הנוגעים לכל אחד מסוגי הבקרות שמיישם התאגיד הבנקאי.

29. ההוראה קובעת כי על בסיס ניתוח סיכוני הסייבר התאגיד הבנקאי יגבש ויאשר תכניות עבודה, כמפורט. הציפייה היא כי התאגיד הבנקאי יקצה משאבים הולמים, יעקוב ויוודא את מימוש התוכניות בהתאם ללוח הזמנים שנקבע.

30. תאגיד בנקאי רשאי לשלב את הנדרש בסעיפים 32-27 לעיל במסמכי אסטרטגיה ומדיניות הנדרשים בהוראות אחרות של המפקח על הבנקים.

ניהול סיכוני הסייבר (סעיפים 34 – 47 להוראה)

31. ההוראה מפרטת את הדרישות הנוגעות לקיום תהליך אפקטיבי לזיהוי והערכת סיכוני סייבר. בהתחשב בדינאמיות של מרחב הסייבר, הציפייה היא כי התאגיד הבנקאי יבצע זיהוי והערכה שוטפים של האיומים וסיכוני הסייבר.

32. במסגרת הערכת בקרות הגנת הסייבר, יש לבחון, באופן שוטף, את רמת האפקטיביות של בקרות ההגנה השונות שיושמו לצורך הפחתת סיכוני הסייבר. מנהל הגנת הסייבר ירכז את המידע הרלבנטי בחתכי הפעילות השונים בתאגיד. הציפייה היא כי מנגנוני הערכת בקרות הגנת הסייבר יתואמו וישולבו במנגנוני ההערכה הקיימים בתאגיד. לדוגמה: סקרי פגיעויות, מבדקי חדירה מבוקרים (כמפורט בהוראה 357) וכדומה. עם זאת, מנהל הגנת הסייבר יזום הפעלה של מנגנוני הערכה ובקרה (למשל: סקרי פגיעויות ובדיקות חוסן) היכן שנדרש.

33. ההוראה מדגישה כי הערכת בקרות הגנת הסייבר צריכה להתבצע בחתכי פעילות שונים ותהליכים בתוך התאגיד הבנקאי ובקשרים שלו עם גורמים חיצוניים, כגון: לקוחות, ספקים וכד'.

34. דוחות סדירים על תמונת סיכוני הסייבר יימסרו להנהלה והדירקטוריון. יודגש כי דיווח על אירועי סייבר מטופל בסעיפים 82-81 להוראה.

יעדי בקרה ובקרות הגנת סייבר (סעיפים 48 – 82 להוראה)

35. ביסוס מערך בקרות אפקטיבי אל מול סיכוני הסייבר, מחייב שילוב חוצה ארגון של אנשים, טכנולוגיות, תהליכים ונהלים. חלק זה של ההוראה מבוסס על עקרונות ותפיסות היסוד שהובאו בהוראה בעיקר בפרק ג', והוא כולל קווים מנחים ליישום מערך הגנת סייבר אפקטיבי. הפרק שם דגש, בין היתר, על פעולות שמאפיינות את בקרות הגנת הסייבר ובכללן אלו שנועדו לבסס הגנה פרואקטיבית, הגנה רב שכבתית, שיתוף מידע ומודיעין, ניטור, ניהול ותרגול אירוע סייבר.

36. ההוראה שמה דגש על הצורך לקיים הגנת סייבר פרואקטיבית, שכוללת בין היתר:

(א) מיפוי של כל סביבות התפעול בהן פועל התאגיד הבנקאי, לרבות הסביבה החיצונית, שבה יכולת השליטה והבקרה של התאגיד הבנקאי חלשה יותר בהשוואה לסביבה הפנימית (ראה סעיף 37 בהמשך). הסביבה החיצונית כוללת פעילות לקוחות, ספקי מוצרים, שירותים ואחרים בשרשרת האספקה, רשתות חברתיות וכדומה.

(ב) איסוף מידע ושיתוף מידע ומודיעין עם גורמים חיצוניים רלבנטיים החשופים לאיומי סייבר דומים, שיסייעו להיערך מבעוד מועד לאיומים ותרחישי תקיפה שונים ולחזק לפי הצורך את מערך הגנת הסייבר, לרבות היכולת לפעולה בזמן אמת.

(ג) יכולת להגיב מהר ובאופן אפקטיבי לסוגים שונים של איומים. היכולת לדעת אלו גורמים בתוך התאגיד הבנקאי אמורים להיות מעורבים בטיפול באירוע מסוים והכוונה לא רק לאנשים הטכנולוגיים אלא גם לגורמים כגון: עסקיים, דוברות וכד'. גורם המפתח בתגובה הוא המהירות, שחשיבותה היא ביכולת לזהות אירוע ככל שניתן בסמוך להתרחשותו כדי לצמצם את הנזק הפוטנציאלי.

(ד) ניטור שוטף ומקיף של סביבות התפעול השונות של התאגיד כדי לזהות אנומליות ואירועים חשודים. התרחישים והכלים של פעולות הניטור חייבים להיבחן באופן שוטף, ולהתעדכן לפי הצורך, כדי לבדוק את מידת האפקטיביות של פעולות אלו.

37. לא די בכך שהתאגיד הבנקאי יישם מנגנונים פנימיים להפחתת סיכוני הסייבר. תאגיד בנקאי עלול להיות חשוף למימוש איום סייבר באמצעות ניצול חולשה אצל גורם חיצוני שיש לו קשר עם התאגיד. לפיכך ניתן ביטוי בהוראה לחשיבות של הפעולות שהתאגיד הבנקאי ינקוט כדי לוודא שגם גורמים חיצוניים רלבנטיים מיישמים מנגנונים לצמצם חשיפתו של התאגיד לסיכוני סייבר. הכוונה בעיקר לגורמים מהותיים בשרשרת האספקה של התאגיד.

תחילה

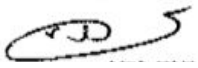
38. תחילת האמור בחוזר זה היא מיום 1/9/2015.

עדכון הקובץ

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

להוציא עמוד	**להכניס עמוד**
-----	361-1-19 [1] (3/15)

בכבוד רב,



דוד זקן

המפקח על הבנקים

ניהול הגנת הסייבר

פרק א': כללי

מבוא

1. להתפתחות המתמשכת ולחדשנות הטכנולוגית נודעת השפעה מרחיקת לכת על האופן שבו תאגידים בנקאיים מנהלים את עסקיהם ועל האופן שבו הם מתקשרים עם לקוחות, ספקים ושותפים.

2. קצב השינויים המהיר בתשתית הטכנולוגית, החדשנות המתמדת במתן שירותים בנקאיים ללקוחות, זמינותם של השירותים "בכל עת, בכל מקום", 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, יוצרים כר נרחב מאוד להיווצרות חולשות במערכי ההגנה של התאגיד הבנקאי אשר עלולות לחשוף אותו לסיכוני סייבר משמעותיים.

3. בד בבד, חל גידול משמעותי בעצמת איומי הסייבר, הן מבחינת היקפם, הן בבחינת גורמי האיום והן בהיבטי תחכום וזמינות כלי התקיפה.

4. התממשותם של סיכוני סייבר עלולה לשבש את פעילתו התקינה והמאובטחת של התאגיד, ולגרום בין היתר, למניעת שירות מלקוחותיו, לחשיפת מידע פרטי, למחיקה ושיבוש נתונים של התאגיד הבנקאי ושל לקוחותיו, לירידה באמון הציבור, לפגיעה בתדמית התאגיד הבנקאי וביכולתו לנהל את נכסיו ואת נכסי לקוחותיו באופן נאות. בתרחיש קיצון התממשותם של סיכונים אלו עלולה לפגוע ביציבותו של התאגיד הבנקאי.

5. אשר על כן, על התאגידים הבנקאיים לתת דגש מיוחד ולנקוט בצעדים הדרושים לצורך ניהול אפקטיבי של הגנת הסייבר. בפרט, נדרשים התאגידים הבנקאיים להרחיב ולהעמיק את יכולות ההתמודדות הקיימות של אבטחת המידע באופן אשר יאפשר להם להתמודד כנגד איומי הסייבר.

6. ניהול סיכוני סייבר מהווה חלק מהמערך הכולל של ניהול סיכונים בתאגיד הבנקאי. הוראה זו נועדה להוסיף ולהרחיב על ההוראות המפורטות בסעיף 8 בהמשך, בכל הנוגע לניהול תקין של סיכוני הסייבר.

עקרונות יסוד לניהול הגנת הסייבר

7. ניהול הגנת הסייבר של תאגיד בנקאי יתבסס על עקרונות היסוד המפורטים בהוראה זו. עקרונות אלו מהווים קווים מנחים, אשר מקנים את הגמישות הנדרשת לאור קצב השינויים המהיר בתחום הסייבר, ומתוך הכרה שלכל תאגיד פרופיל סיכונים ייחודי, הדורש התאמה של תכנית הגנת הסייבר למאפייני הפעילות ולצרכים העסקיים הפרטניים של כל תאגיד.

8. התאגיד הבנקאי ינהל את סיכוני הסייבר בראייה משולבת כלל תאגידית במסגרת ובהתאם לכללים לניהול ולבקרת סיכונים כאמור בהוראות ניהול בנקאי תקין, ובפרט בהוראות הבאות:

(א) הוראה מספר 310 - "ניהול סיכונים";

(ב) הוראה מספר 350 – "ניהול סיכונים תפעוליים";

(ג) הוראה מספר 355 – "ניהול המשכיות עסקית";

(ד) הוראה מספר 357 – "ניהול טכנולוגיית המידע".

9. במסגרת תהליך ניהול הסיכונים התפעוליים, כאמור בהוראת ניהול בנקאי תקין מס' 350, תאגיד בנקאי יביא בחשבון, באופן מתועד, את סיכוני הסייבר הרלוונטיים.

10. בכל הנוגע לניהול המשכיות עסקית, בהתאם להוראת ניהול בנקאי תקין מס' 355, יתייחס התאגיד הבנקאי גם לתרחישי אירועי סייבר שיש בהם כדי להשפיע על פעילות התאגיד, ספקים ונותני שירותים, זמינות תשתיות תומכות וכיו"ב, כל זאת בכדי לשפר את עמידותו של התאגיד בעת התרחשות שיבושים תפעוליים, הנגרמים מהתממשות סיכוני סייבר, וכן להקטין את ההשפעה ששיבושים מסוג זה עלולים לגרום לרציפות הפעילות העסקית בתאגיד ובמשק.

11. ניהול נאות של סיכוני הסייבר מחייב הרחבה והתאמה של המסגרת הקיימת של ניהול סיכוני טכנולוגיית המידע בתאגיד הבנקאי בהיבטי תפיסת מרחב האיום ויכולות ההגנה הנדרשות, כמפורט בהוראה זו.

תחולה

12. הוראה זו תחול על:

(א) תאגיד בנקאי, כהגדרתו בחוק הבנקאות (רישוי), התשמ"א-1981 (להלן – חוק הבנקאות (רישוי));

(ב) תאגיד כאמור בסעיפים 11(א)(3א), 11(א)(3ב) ו- 11(ב) לחוק הבנקאות (רישוי), שהינו בשליטה, במישרין או בעקיפין, של התאגיד הבנקאי, כאילו היה תאגיד בנקאי.

(ג) המפקח רשאי לקבוע הוראות נוספות על אלה המפורטות להלן, שיחולו על תאגידים בנקאיים מסוימים.

הגדרות

13. בהוראה זו למונחים הבאים תהיה המשמעות כמפורט להלן:

"**איום סייבר**" -	איום להתרחשות אירוע סייבר.
"**אירוע סייבר**" –	אירוע סייבר הינו אירוע אשר במהלכו מתבצעת תקיפת מערכות מחשוב ו/או מערכות ותשתיות משובצות מחשב על ידי, או מטעם, יריבים (חיצוניים או פנימיים לתאגיד הבנקאי) אשר עלולה לגרום להתממשות סיכון סייבר. יצוין, כי בהגדרה זו נכללים גם ניסיון לביצוע תקיפה כאמור גם אם לא נגרם נזק בפועל.
"**הערכת בקרות הגנה**"	פעולות שנועדו לבחון את תקינות יישומן בפועל של בקרות ההגנה (ניהוליות, תפעוליות וטכניות), התפעול השוטף שלהן, ואת האפקטיביות שלהן אל מול דרישות ההגנה הרלבנטיות.
"**התרעה על אירוע סייבר**" -	ידיעה המתייחסת לאירוע סייבר מתוכנן, או אירוע שכבר התרחש, או עודו מתרחש, אך טרם זוהה על ידי הגורם המותקף.
"**יריב**" (adversary) –	בהקשר הוראה זו: יחיד, קבוצה, ארגון, או גורמים מדינתיים שבכוונתם להסב נזק לתאגיד בנקאי.

"**ניהול אירוע סייבר**" - תהליך מובנה, אשר מתייחס לשלבים הבאים:

(א) **זיהוי (Detection) -** ביצוע בירור ראשוני בדבר קיומו של אירוע סייבר וגיבוש מהיר ככל האפשר של דפוס הפעילות הדרוש לשלב הבא אחריו.

(ב) **ניתוח (Analysis) -** ביצוע בירור מקיף ומעמיק ככל האפשר לגבי אירוע הסייבר, לצורך קבלת החלטות ברמה האופרטיבית, גיבוש רשימת חלופות של דפוסי פעולה אפשריים לבלימת התקיפה והחלטה על דרך הפעולה העיקרית לשלב ההכלה.

(ג) **הכלה (Containment) -** השגת שליטה ראשונית באירוע לצורך הכלתו ועצירת החמרתו והשגת יעדיו. ביצוע תהליך השתלטות על מערך התקיפה, בתוך התאגיד הבנקאי המותקף, ועצירה מלאה של ווקטור הנזק.

(ד) **הכרעה (Eradication) -** נטרול רכיבי התקיפה שמצויים במערכות התאגיד הבנקאי, תוך שאיפה לבטל או למזער, ככל שניתן, את הנזק שכבר נגרם.

(ה) **השבה** (Recovery) **-** חזרה לתקינות ופעילות מלאה של כל פעילות אצל התאגיד הבנקאי המותקף שהושבת, הוגבל או הופרע תפקודו.

כל שלב כולל דיווח לגורמים הפנימיים והחיצוניים הרלוונטיים.

"**נזק**" - תוצאה בלתי רצויה, לרבות שיבוש/הפרעה/השבתה של פעילות; גניבת נכס; איסוף מודיעין; פגיעה במוניטין/אמון הציבור.

"**סיום אירוע סייבר**" (Post-Incident Activity)- תהליך מובנה, אשר מתייחס לשלבים הבאים:

(א) **תחקור והפקת לקחים** - תהליך בחינה וניתוח מתודולוגי של ניהול אירוע הסייבר מראשיתו לסופו בהיבטי אנשים, תהליכים וטכנולוגיה. התהליך מבוצע בסמוך ככל שניתן למועד הטיפול האופרטיבי באירוע, במטרה לספק לקחים ותובנות אשר יאפשרו טיפול יעיל ומהיר יותר באירוע סייבר עתידי.

(ב) **מעקב אחר יישום הלקחים ותובנות** - תהליך בחינה הבא לוודא כי כל הלקחים והתובנות שעלו באירוע יומשו בפועל.

"**סיכון סייבר**" - פוטנציאל לנזק שנובע מהתרחשות אירוע סייבר, בהתחשב ברמת סבירותו וחומרת השלכותיו.

פרק ב': ממשל תאגידי

דירקטוריון והנהלה בכירה

14. התאגיד הבנקאי ינהל את סיכוני הסייבר בהתאם לעקרונות האמורים בהוראת ניהול בנקאי תקין מס' 350. הדירקטוריון וההנהלה הבכירה של תאגיד בנקאי ייצרו מסגרת אפקטיבית לניהול סיכוני הסייבר.

15. הדירקטוריון של התאגיד הבנקאי יהיה אחראי על הנושאים הבאים:

(א) התוויית אסטרטגיית הגנת סייבר כלל תאגידית ואישורה;

(ב) אישור מסגרת לניהול סיכוני הסייבר ומדיניות הגנת הסייבר התאגידית;

(ג) קביעת אופן המעקב והפיקוח על ההנהלה הבכירה, ביישום מסגרת ניהול סיכוני הסייבר;

(ד) קבלת דיווח על אירועי סייבר משמעותיים.

16. ההנהלה הבכירה של התאגיד הבנקאי תהיה אחראית על הנושאים הבאים:

(א) יצירת מסגרת כוללת לניהול סיכוני הסייבר וקיום פיקוח נאות עליה;

(ב) גיבוש מדיניות הגנת הסייבר התאגידית;

(ג) יישום עקבי ותחזוקה של מסגרת העבודה לניהול סיכוני סייבר בכל חלקי התאגיד הבנקאי, לרבות הקצאת משאבים נאותים;

(ד) מעקב אחר האפקטיביות של מערך הגנת הסייבר ותיאום פעילותו מול גורמי ניהול סיכון פנימיים וחיצוניים, כאמור בהוראה זו;

(ה) קבלת דיווח על תמונת מצב עדכנית של איומי הסייבר ודרכי ההתמודדות מולם, בהתאם לתוצאות הערכת הסיכונים כאמור בהוראה זו;

(ו) קבלת דיווח תקופתי על אירועי סייבר רלבנטיים (פנימיים וחיצוניים) וניתוח המשמעויות הנגזרות מהם;

(ז) דיון בהשלכות האופרטיביות, חוצות ארגון, של סיכוני סייבר והנחיה ובקרה על ביצוע שינויים או התאמות במערך ההגנה ו/או בפעילות העסקית, לפי הצורך.

מנהל הגנת הסייבר

17. התאגיד הבנקאי ימנה עובד בכיר בעל ידע וניסיון מתאימים כמנהל הגנת הסייבר ויגדיר את תחומי אחריותו וסמכויותיו.

(א) מנהל הגנת הסייבר יהיה כפוף לחבר הנהלה של התאגיד הבנקאי, ויהיה בעל מעמד וסמכות להשפיע על החלטות המשליכות על החשיפה של התאגיד הבנקאי לסיכוני סייבר.

(ב) מיקומו הארגוני של מנהל הגנת הסייבר יקבע באופן בו ימנעו, ככל הניתן, ניגודי עניינים.

(ג) מנהל הגנת הסייבר לא יישא באחריות נוספת שיש בה כדי להפריע לתפקודו;

(ד) ממשקי העבודה והדיווח הנדרשים בין מנהל הגנת הסייבר לבין בעלי התפקידים הרלבנטיים בארגון ייקבעו ויאושרו על ידי ההנהלה.

18. מנהל הגנת הסייבר יעמוד בראש מערך הגנת הסייבר ויהיה אחראי בין היתר על הנושאים הבאים:

(א) תכלול היבטי ניהול הגנת הסייבר בתאגיד הבנקאי;

(ב) ייעוץ להנהלה הבכירה בתחום ניהול הגנת הסייבר;

(ג) סיוע להנהלה בגיבוש ויישום מדיניות הגנת הסייבר;

(ד) גיבוש מתודולוגיה תאגידית לניהול סיכוני סייבר;

(ה) פיתוח, מעקב אחר יישום, וניטור של תכנית מקיפה ופרטנית להתמודדות התאגיד הבנקאי עם סיכוני הסייבר כאמור בהוראה זו;

(ו) הגדרת מדיניות פרטנית ונוהלי עבודה למימוש בקרות הגנת סייבר;

(ז) יצירת מודעות לאיומי הסייבר והדרכה לעניין דרכי ההתמודדות מולם, בקרב עובדים, ספקים, שותפים ולקוחות התאגיד הבנקאי;

(ח) עבודה עם הגורמים הרלבנטיים בתאגיד הבנקאי (טכנולוגיים ועסקיים) בכדי לנתח ולהעריך את רמות הסיכון המובנה בפעילות, את הבקרות הנדרשות ובהתאם, את רמות הסיכון השיורי והחשיפות לאיומי סייבר;

(ט) קביעת מסגרת הדיווחים שיקבל מגורמים שונים בתאגיד הבנקאי;

(י) תיאום וקישור מול גורמים חיצוניים בנושאי הגנת סייבר;

(יא) פיתוח מדדים רלבנטיים, הכנת דוחות ומתן דיווחים שוטפים כאמור בהוראה זו;

(יב) תכלול ובקרה של ניהול אירועי סייבר בתאגיד הבנקאי;

(יג) ייזום וביצוע תרגולים;

(יד) הובלה ותיאום של תהליכים הנוגעים לניהול הגנת הסייבר;

(טו) הערכת בקרות הגנת הסייבר;

(טז) ניתוח אירועי סייבר משמעותיים בישראל ובעולם, הפקת לקחים ויישום המסקנות הרלוונטיות לתאגיד הבנקאי.

19. המפקח על הבנקים ראשי להתיר למנהל הגנת הסייבר בתאגיד הבנקאי לשמש מנהל הגנת הסייבר גם בתאגידים בנקאיים הנשלטים על ידי אותו תאגיד בנקאי או בתאגידים כמפורט בסעיפים 11(א)(3א), 11(א)(3ב) ו- 11(ב) לחוק הבנקאות (רישוי).

ביקורת פנימית

20. ניהול הגנת הסייבר ואופן יישומה יבוקרו באופן תקופתי ע"י הביקורת הפנימית.

מערכי ניהול, תיאום ובקרה משיקים

21. כחלק מניהול סיכוני הסייבר בראייה משולבת כלל תאגידית, מערך הגנת הסייבר יפעל באופן מתואם עם מערכי ניהול, תיאום ובקרות משיקים בתוך התאגיד הבנקאי ומחוץ לו.

22. יחסי הגומלין וזרימת המידע בין המערכים שבתוך התאגיד הבנקאי יוגדרו בכתב. מערכי ניהול, תיאום ובקרה משיקים בתאגיד הבנקאי כוללים, בין היתר: אבטחת מידע, אבטחה פיזית, ממשל מערכות מידע, תפעול מערכות מידע, ניהול סיכונים, הונאות, ניהול כח אדם, המשכיות עסקית, ניהול יחסי לקוחות, דוברות, וייעוץ משפטי.

23. בפרט, מנהל הגנת הסייבר יקיים ממשקי עבודה מול מנהל הסיכונים הראשי והביקורת הפנימית תוך התאמה להוראות הרלבנטיות.

24. יחסי הגומלין וזרימת המידע בין המערכים שבתוך התאגיד הבנקאי לבין מערכים חיצוניים לתאגיד יוגדרו בכתב. מערכים חיצוניים לתאגיד הבנקאי כוללים, בין היתר: גורמי רגולציה, גורמי חקירה ואכיפה, מטה הסייבר הלאומי, גורמי ניהול סיכוני סייבר מקבילים במגזר הפיננסי, גורמי ניהול סיכונים אצל ספקים ושותפים עסקיים ומערכי שיתוף מידע בנוגע לסייבר.

פרק ג': אסטרטגיית הגנה ומסגרת לניהול סיכוני הסייבר

תפיסת הגנת הסייבר

25. התאגיד הבנקאי ירחיב ויעמיק את יכולות ההתמודדות הקיימות של אבטחת המידע (דהיינו: מניעה - Prevention, גילוי - Detection, תגובה- Response), באופן אשר יאפשר לו להתמודד כנגד איומי הסייבר. בפרט, התאגיד הבנקאי יפתח וירחיב יכולותיו בתחומים הבאים: חיזוי – Prediction, זיהוי והטעיה, ושרידות – Resilience.

26. התאגיד הבנקאי יקיים מערך הגנת סייבר אפקטיבי ויעיל, הפועל מתוך ראיה תהליכית ומביא לידי ביטוי, בין היתר, את העקרונות הבאים:

(א) תפיסה כוללת של מרחב הפעילות - מערך הגנת הסייבר יתחשב במקומו של התאגיד הבנקאי במכלול שרשרת האספקה של שירותי בנקאות, בשימוש בתשתיות ושירותים כלליים (כגון רשתות חברתיות), ובסיכונים הנובעים מאופי הפעילות אל מול הגורמים השונים במרחב, לרבות בחו"ל, חברות בנות (בישראל ובחו"ל), ספקים, נותני שירותים ולקוחות;

(ב) שיתוף מכלול הגורמים הרלבנטיים בתאגיד הבנקאי בגיבוש ויישום אסטרטגיית ומדיניות הגנת הסייבר;

(ג) פרואקטיביות – יכולות מודיעין, ניטור ותגובה בזמן אמת של מערך ההגנה, אל מול האיומים ושיתוף מידע ומודיעין;

(ד) העמקת יכולות ההתמודדות כנגד איום ממוקד, באמצעות יצירת מערכי הגנת סייבר המשלבים תשתיות ארגוניות ואנושיות, נהלים ותהליכי עבודה, וטכנולוגיות (People, Processes, Technologies) ופריסתם בשכבות בתצורת הגנה לעומק (Defense in Depth) בכדי למזער את החשיפה לאיום ולהשלכותיו;

(ה) שילוב יכולות מתקדמות במערך ההגנה (לרבות הונאת התוקף, פריסת מלכודות וזיהוי דפוסים חשודים ואנומאליות) גם ברמת תשתיות המחשוב והתקשורת וגם ברמת הפעילות העסקית (למשל: זיהוי הונאות);

(ו) מתן דגש למערכי הגילוי, החקירה והתגובה, מתוך הכרה במורכבות האיום ויכולות היריב, בהתבסס על ההנחה שמניעה מוחלטת של התממשות הסיכון היא בלתי אפשרית, ובהתייחס גם לאיומים שהסבירות להתממשותם היא נמוכה, אולם פוטנציאל הנזק שלהם הוא גבוה.

(ז) עמידות – מיפוי וחקר הסביבה, חיזוי וחקר איומים, מערך הגנה ממוקד משימה שיאפשר לתאגיד הבנקאי לספוג את השלכותיו של שיבוש תפעולי משמעותי (ישיר או עקיף) עקב התקפת סייבר ולהמשיך לנהל תהליכים ולספק שירותים חיוניים.

(ח) מתן דגש להגנה על פרטיות לקוחות התאגיד הבנקאי ונכסיהם, ושמירה על רמות אמינות, נאותות וזמינות גבוהות של השירותים המסופקים על ידי התאגידים הבנקאיים.

אסטרטגיית הגנת סייבר

27. אסטרטגיית הגנת סייבר כלל תאגידית תעוגן במסמך שיכלול, בין היתר, את הנושאים הבאים:

(א) מקומה וחשיבותה של הגנה הסייבר בתאגיד הבנקאי;

(ב) תפיסת איום הסייבר והאתגרים מולם עומד התאגיד הבנקאי;

(ג) גישת התאגיד הבנקאי לניהול סיכוני סייבר, קביעה וניטור של רמת חשיפה לאיומי סייבר;

(ד) עיקרי אסטרטגיית הגנת הסייבר: יעדים, עקרונות הפעלה ויישום.

28. האסטרטגיה תעודכן על פי הצורך ובכל מקרה לפחות פעם בשלוש שנים.

מסגרת לניהול סיכוני הסייבר

29. המסגרת לניהול סיכוני הסייבר תעוגן במסמך שיכלול, בין היתר, את הנושאים הבאים:

(א) זיהוי מבני הממשל התאגידי המשמשים לניהול סיכוני הסייבר, לרבות תחומי אחריות וקווי דיווח;

(ב) תיאור הכלים והמתודולוגיות להערכת הסיכונים ואופן השימוש בהם;

(ג) תיאור תהליכי ואמצעי הגנה עיקריים ואופן בקרתם והערכתם.

מדיניות הגנת סייבר

30. התאגיד הבנקאי יגדיר מדיניות הגנת סייבר כלל תאגידית, אשר תתייחס למכלול הבקרות ודרכי הפעולה להשגת יעדי ההגנה בהתאם לאסטרטגיה. המדיניות תעבור הערכה מדי שנה ותעודכן במידת הצורך.

31. המדיניות תתייחס, בין היתר, לנושאים הבאים: יעדי הגנת הסייבר; הגדרת תחומי אחריות, בעלי תפקיד וגורמים מעורבים (לרבות ממשקי עבודה); מבנים ארגוניים; מבנה וממשל תהליך ניהול סיכוני הסייבר בתאגיד הבנקאי; המסגרת הנוהלית הפנימית של התאגיד הבנקאי; פירוט הבקרות הנדרשות והמסגרת ליישומן; מערכי ניטור ותגובה; קידום מודעות; איסוף, מחקר ושיתוף מידע; שימוש במדדי יישום, בשלות ואפקטיביות; הערכה, בקרה ודיווח.

32. בהתאם למדיניות הגנת הסייבר, התאגיד הבנקאי ייקבע מדיניות פרטנית עבור בקרות ההגנה המיושמות. מסמכי המדיניות הפרטניים יעודכנו על פי הצורך.

תכניות עבודה

33. על בסיס האסטרטגיה והמדיניות, וכנגזרת מניתוח הסיכונים וחשיפות הסייבר, יגבש התאגיד הבנקאי תכנית עבודה רב-שנתית, אשר תתווה ותתעדף את דרכי ישום הבקרות השונות לצמצום סיכוני הסייבר. התכנית תאושר בידי הנהלת התאגיד הבנקאי אשר תקצה משאבים הולמים להשגת יעדי התכנית.

פרק ד': ניהול סיכוני הסייבר

ניהול סיכוני הסייבר: זיהוי סיכונים, הערכת סיכונים

34. תהליך אפקטיבי לזיהוי והערכת סיכוני סייבר מתייחס, בנוסף לאמור בסעיף 26 להוראת ניהול בנקאי תקין מס' 350, לגורמי האיום השונים, לסביבות הפעילות השונות של התאגיד (הפנימיות והחיצוניות) ולמגוון תרחישים, לרבות התייחסות לסיכונים הנובעים מפשיעת סייבר, תלות בתשתיות תומכות ועבודה עם ספקי שירות חיצוניים.

35. התאגיד הבנקאי יבצע, אחת לשנה לכל הפחות, הערכה של סיכונים ובקרות סייבר, אשר מזהה את הסיכון המובנה, את האפקטיביות של סביבת הבקרה, ואת הסיכון השיורי.

36. תהליך זיהוי והערכת סיכוני הסייבר צריך להיות מתמשך ולהתבצע בהתאם לשינויים פנימיים וחיצוניים, ובכללם שינויים עסקיים, ארגוניים וטכנולוגיים.

37. התאגיד הבנקאי יוודא כי הערכת סיכוני הסייבר ותשתית הבקרות לניהולם מתעדכנות בהתאם לשינויים והמגמות במערך האיומים ובהתאם לקצב הגידול או השינויים במוצרים, פעילויות, תהליכים ומערכות.

38. לצורך ניתוח והערכת איומי הסייבר יתחשב התאגיד הבנקאי בנתונים האמורים בסעיף 28 להוראת ניהול בנקאי תקין מס' 350, בדגשים ובשינויים כמפורט להלן:

(א) ממצאי ביקורות וסקרים וכל מידע שוטף אשר יש בהם כדי להצביע על חולשות בבקרות הרלבנטיות;

(ב) איסוף וניתוח נתונים חיצוניים שביכולתם להצביע על נקודות תורפה אפשריות או להוביל לגילוי חשיפות לסיכונים שלא זוהו בעבר;

(ג) איסוף וניתוח נתונים של אירועי סייבר בתאגיד;

(ד) מיפוי תהליכים עסקיים, לצורך חשיפת סיכונים ספציפיים, קשרי תלות הדדית בין סיכונים, ותחומי חולשה בבקרות או בניהול הסיכונים;

(ה) שימוש במדדים לצורך כימות החשיפה לסיכוני סייבר תוך שימוש במדדי הערכה איכותיים ו/או כמותיים, באופן אשר יאפשר מעקב אחרי שינויים בערכים אלו מעת לעת.

(ו) שימוש במדדי בשלות תהליכים (Process Maturity), אינדיקטורים עיקריים לסיכון (KRI) ולביצוע (KPI) וכיו"ב, בכדי לספק תובנות על סטטוס מנגנוני הבקרה ותכנית הגנת הסייבר;

(ז) ניתוח תרחישים בשיתוף עם מנהלי קווי העסקים ומנהלי הסיכונים במטרה לזהות אירועים פוטנציאליים של התממשות הסיכון, להעריך את תוצאותיהם האפשריות, ולשפר את יכולת הזיהוי והתגובה לאותם אירועים;

(ח) ניתוח השוואתי של תוצאות של כלי הערכה שונים, בכדי לספק מבט מקיף יותר על פרופיל סיכון הסייבר של התאגיד הבנקאי.

39. מתודולוגיות זיהוי, מדידה והערכת סיכוני הסייבר בתאגיד הבנקאי תהיינה מתועדות ומאושרות בידי ההנהלה הבכירה.

הערכת בקרות הגנת הסייבר

40. מנהל הגנת הסייבר יוודא קיום מנגנונים ניהוליים, תפעוליים וטכניים לביצוע הערכת בקרות הגנת הסייבר ויזום הפעלת מנגנוני הערכה ובקרה כאמור, לפי הצורך.

41. תכנון מערך הערכת בקרות הגנת הסייבר ייגזר מתפיסת מכלול מערך איומי הסייבר על התאגיד הבנקאי, ובהתחשב בסוגי הסיכונים, תרחישי אירוע סייבר שונים, הסתברות התממשותם ובתוצאות סקרים קודמים.

42. מנגנוני הערכת בקרות הגנת הסייבר יתואמו וישולבו במנגנוני הערכה קיימים בתאגיד, בין היתר, בסקרי פגיעויות (Vulnerability Assessments) ובדיקות חוסן/מבדקי חדירה מבוקרים (Penetration Tests) בהתאם להוראת ניהול בנקאי תקין מס' 357, תהליכי ביקורת פנימית על פי הוראת ניהול בנקאי תקין מס' 307, תהליכי ציות לחקיקה/תקנים וכיו"ב.

43. המדדים להערכת סיכוני הסייבר יעודכנו, מעת לעת, בהתאם לתוצאות הערכת בקרות ההגנה.

44. הערכת בקרות הגנת הסייבר תכלול ניתוח מצב הבקרות בהתייחס לאיומי הסייבר, לחולשות ולסיכונים הרלבנטיים, בחתכי הפעילות השונים לרבות: גישה פיזית; מנהל וארגון; ניהול מחזור חיי מערכות מידע (Information System Lifecycle) בסביבות השונות; ניהול תשתיות תקשורת ומחשוב בסביבות השונות, לרבות מערכות תומכות קריטיות; פעילות מול לקוחות, לרבות התקנים שבשימוש הלקוחות; גישה מרחוק; שירותי העברת הודעות; ניהול הרשאות וזהויות; עבודה עם שותפים עסקיים וספקי שירותים, לרבות ערוצי העברת מידע ונתונים; תרבות ארגונית ומודעות עובדים; נוכחות מקוונת (Online Presence) לרבות בנקאות ישירה/בתקשורת ושימוש ברשתות חברתיות, והמשכיות עסקית.

45. ממצאים מהותיים שנתגלו בעקבות או במהלך פעולות הערכת בקרות הגנת הסייבר ידווחו להנהלה והדירקטוריון, יחד עם הפקת הלקחים ותכנית לתיקון הממצאים, כאמור בהוראה זו.

דיווח על סיכונים

46. הדוחות הסדירים המוגשים להנהלה והדירקטוריון בנושאי סיכונים תפעוליים כאמור בהוראת ניהול בנקאי תקין מס' 350, יכללו התייחסות פרטנית לסיכוני הסייבר.

47. דוחות סיכוני סייבר יכללו:

(א) מצב עדכני ומנומק של מדדי סיכוני הסייבר;

(ב) פירוט של אירועי סיכון/נזק משמעותיים בתאגיד;

(ג) אירועים ונתונים חיצוניים רלבנטיים שיש בהם השפעה פוטנציאלית על התאגיד הבנקאי.

פרק ה': יעדי בקרה ובקרות הגנת סייבר

כללי

48. כחלק מניהול הגנת הסייבר, התאגיד הבנקאי יבסס מערך בקרות אפקטיבי להפחתת רמת סיכוני הסייבר.

49. מערך הבקרות יהיה מושתת על שילוב חוצה ארגון של טכנולוגיות, תהליכים, נהלים, ואנשים אשר יאפשרו לתאגיד הבנקאי לצמצם את החשיפה לאיומי הסייבר לרמה הנדרשת.

50. התאגיד הבנקאי ינקוט בצעדים הנדרשים להשגת יעדי הבקרות ולמימוש הבקרות כמפורט בפרק זה.

אבטחת סביבת הפעילות

51. התאגיד הבנקאי ימפה את סביבת הפעילות שבה הוא פועל, יזהה את סיכוני הסייבר הכרוכים בפעילותו, ויגדיר מדיניות להתמודדות עם סיכונים אלו, בהתאם לרמת הסיכון ואופי הקשר.

52. במסגרת זו, התאגיד הבנקאי יבחן את מכלול השירותים העסקיים והתפעוליים, לרבות: ספקים, תאגידים קשורים, לקוחות, ספקי תשתית מחשוב ותקשורת, מיקור חוץ, ספקי שירותים (למשל: עו"ד, רו"ח, משרדי פרסום, בתי דפוס וכיו"ב), וגורמי חו"ל.

53. התאגיד הבנקאי יקבע מנגנונים נאותים להגנה על נוכחותו המקוונת (Online Presence) ובפרט, למול הסיכונים הכרוכים בפעילותו ברשתות חברתיות.

54. התאגיד הבנקאי יקבע את הפעולות הנחוצות לוודא, ככל שניתן, שהגורמים הרלבנטיים, לרבות גורמים חיצוניים, נוקטים באמצעים הנדרשים להפחתת חשיפתו לסיכוני סייבר, לרבות ביצוע בדיקות נאותות וניטור באותם גורמים (או גופים) שזוהו כמהותיים לפעילות העסקית התקינה ולאספקת השירותים ברמה הנדרשת.

הגנת סייבר פרואקטיבית

55. התאגיד הבנקאי יבסס מערך דינאמי של הגנת סייבר, בעל יכולות פרואקטיביות, בין היתר, ע"י:

(א) מיפוי והכרת הסביבה – ביצוע מיפוי וניתוח עדכניים של הסביבה התפעולית הפנימית והחיצונית בה הוא פועל, על מנת לזהות גורמים, מערכות ותהליכים קריטיים, לרבות נקודות תורפה, חולשות ו/או תלות הדדית ביניהם;

(ב) חיזוי וחקר איומים – איסוף מידע תוך זיהוי וניתוח שוטפים של שיטות ודרכי תקיפה, כוונות ופעילות של גורמי איום במרחב הסייבר, ושיתוף מידע עם גורמים רלוונטיים אחרים לצורך הפקת מידע אופרטיבי, ניתוח תרחישים ו"חשיבה מחוץ לקופסה", אשר יסייעו לחיזוק מערך הגנת הסייבר והסביבה התפעולית כנגד מתקפות פוטנציאליות;

(ג) תמונת מצב עדכנית (Situational Awareness) – תפיסת מצב הגנת הסייבר של התאגיד, בפרק הזמן הנוכחי, אל מול האיומים, ביצוע ניטור מקיף של הסביבה הפנימית והחיצונית לתאגיד הבנקאי לצורך זיהוי חולשות ו/או איומים ו/או אירועי אבטחה ו/או סממנים לקיומם של אלה, תוך שימוש ביכולות זיהוי שונות - למשל: ניתוח דפוסים, זיהוי אנומאליות, כריית מידע (Big Data Analysis) - ותעדוף של האירועים בהתחשב ברמת הסיכון ופוטנציאל הנזק הגלום בהם, כבסיס לקבלת החלטות אופרטיביות;

(ד) תגובתיות – פיתוח יכולת תגובה מהירה ואפקטיבית לאירוע סייבר וניהולו, על מכלול היבטיו ולאורך כל שלביו, זאת על מנת לצמצם באופן מרבי התרחשות הנזק לתאגיד הבנקאי;

(ה) הטעיה, הסטה ועיכוב – שימוש בטכניקות ובטכנולוגיות ייעודיות (כדוגמת "מלכודות דבש" (Honeypots), הסטת תקשורת וכיו"ב) במטרה להטעות ולעכב את התוקף בדרכו לייעד התקיפה ובכדי לאפשר זיהוי וניתוח של כלים ושיטות (Tactics, Techniques and Procedures) בהן עושה התוקף שימוש;

(ו) עמידות סייבר והתאוששות – יכולת לספוג את השלכותיו של שיבוש תפעולי משמעותי כתוצאה מאירוע סייבר, תוך המשך ניהול תהליכים ושירותים חיוניים, ושיקום הפעולות העסקיות לאחר שחל שיבוש כאמור עד לרמה מספקת לצורך מילוי התחייבויות העסקיות;

(ז) חקירה, תחקיר ומיצוי הדין – יכולת לבצע שימור ראיות וניתוח מעמיק של אירועים לצורך איסוף ראיות, הערכת הנזק שנגרם, זיהוי מקורות וגורמים תוקפים, ביצוע תחקיר, הפקת לקחים ושימור ידע. כל זאת, תוך שימוש במנגנונים חוקיים ושיתוף פעולה עם גורמי אכיפה, במידת הצורך, לצורך מיצוי הדין עם האחראים.

צמצום מעטפת התקיפה (Attack Surface)

56. התאגיד הבנקאי יפעל באופן שוטף לצמצום החשיפה לאיומי סייבר. במסגרת זו, ינקוט התאגיד הבנקאי, בין היתר, בפעולות הבאות: הקשחת מערכות ותשתיות; פיתוח מאובטח; צמצום הרשאות של משתמשים על פי העקרונות של "הצורך לדעת" (Need to Know) והרשאות מינימליות (Least Privileged); בקרה וחסימה של התקנים ניידים; סינון סוגי קבצים נכנסים למערכות התאגיד הבנקאי; חסימת מתחמי כתובות ו/או סוגי רשתות המשמשות כמקור להתקפות.

הגנה לעומק (Defense in Depth)

57. הגנה לעומק מאופיינת על ידי שימוש בבקרות שונות בנקודות שונות בתהליך, כך שחולשה בבקרה אחת מפוצה על ידי חוזקה של בקרה אחרת. 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.

58. בפריסת ההגנה לעומק התאגיד הבנקאי יתחשב בניתוח סיכוני הסייבר, מצב הבקרות והחשיפות למול האיומים.

ראיה תהליכית

59. התאגיד הבנקאי ימפה את תהליכי הגנת הסייבר, יקבע מדדי ביצוע ואינדיקטורים, יעריך את רמת בשלות היישום של התהליכים בתאגיד הבנקאי, יזהה את הנקודות הטעונות שיפור, ויישם את השינויים הדרושים בהתאם לתכנית העבודה.

60. תהליכי הגנת סייבר רלבנטיים גם לתהליכים חוצי ארגון, לרבות: ניהול סיכוני סייבר, ניהול מחזור חיים של מערכת, ניהול נכסים, תצורה וטלאים (Asset, Configuration and Patch Management); ניהול זהויות (Identity Management); ניטור ובקרה; שיתוף מידע ודיווח; ניהול אירועים ותגובה; ניהול שרשרת אספקה ותלות בגורמי חוץ (Supply Chain); הדרכה ומודעות; ניהול תכנית הגנת הסייבר.

61. התאגיד הבנקאי יעדכן את הערכת בשלות התהליכים אחת לשנה, לכל הפחות.

הגורם האנושי

62. מתוך הכרה במרכזיותו של הגורם האנושי במערך הגנת הסייבר, התאגיד הבנקאי יגדיר את הבקרות הנחוצות בהיבטי מיון, גיוס וקליטת כח אדם (לרבות עובדים וספקים), ניהול זהויות, מתן הרשאות, הפרדת רשויות, ניוד, מעבר ועזיבה.

63. התאגיד הבנקאי יגדיר ויישם תכנית הדרכה ומודעות מקיפה לנושאי הגנת הסייבר. התכנית תקיף את מכלול קהלי היעד, לרבות עובדים, מנהלים, מפתחים, מנהלי מערכות ותשתיות, גורמי חוץ, ספקים, לקוחות וכיו"ב. התכנית ותכניה יעודכנו מעת לעת בהתאם לתמונת האיומים ולהערכת הסיכון העדכנית.

שיתוף מידע ומודיעין

64. התאגיד הבנקאי יאסוף וינתח מידע רלבנטי, ממקורות פנימיים וחיצוניים, לצורך יצירת תפיסה כוללת ועדכנית של תמונת איום הסייבר והחשיפה של התאגיד הבנקאי למולו, כבסיס לקבלת החלטות מושכלת, תעדוף של דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת.

65. תמונת האיום וחשיפת הסייבר תיגזר, בין היתר, מהמידע הבא: מיפוי גורמי איום רלבנטיים, בחתך מוטיבציה ויכולות; טכניקות, טקטיקות, תרחישים ואמצעי תקיפה; חולשות, הגדרות מערכת, ו/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.

66. התאגיד הבנקאי ישתף מידע שעשוי לסייע לתאגידים בנקאיים אחרים בהתמודדות מול איומי סייבר.

67. איסוף ושיתוף המידע יתבצע בהתאם להנחיות המפקח ובכפוף לדין.

ניטור, בקרה וזיהוי אירוע סייבר

68. התאגיד הבנקאי 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 סייבר, וייזום פעילויות דיווח ותגובה במידת הצורך.

69. על אף האמור בסעיף 68 לעיל, המפקח על הבנקים רשאי להתיר, במקרים חריגים, איוש שאינו רציף כאמור, ובלבד שמערך הניטור והבקרה יעבוד בתצורת עבודה המספקת רציפות תפקודית.

70. לצורך זיהוי אירועי סייבר יעשה התאגיד הבנקאי שימוש גם באמצעים לזיהוי חריגות (אנומאליות) ברמה הטכנולוגית (פעילות המערכות) וברמת הפעילות העסקית.

71. התאגיד הבנקאי יקבע את פרק הזמן הנחוץ לשמירת המידע הדרוש לצורך זיהוי אירועים, לרבות אירועים בחתימה נמוכה, כדי לאפשר ביצוע תחקירי אירוע.

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

73. התאגיד הבנקאי יבחן מעת לעת תרחישי אירוע סייבר לצורך הערכת יכולתו לזהותם, ויעדכן בהתאם את מערך הניטור והזיהוי.

תגובה וניהול אירוע סייבר

74. בניהול אירוע סייבר יזהה התאגיד הבנקאי את השלב בו נמצא האירוע (ראה סעיף 13 לעיל) וינהלו בהתאם למאפייניו. סיום אירוע סייבר יתקיים רק לאחר סיום הטיפול בכל שלביו.

75. התאגיד הבנקאי יקבע נוהלי דיווח, ניהול, תגובה וסיום של אירוע סייבר ושל התרעה על אירוע סייבר, בהתאם לחומרתו ובהתאם לשלבי הטיפול באירוע.

76. לצורך ניהול אירוע סייבר 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.

77. התאגיד יבצע רישום ומעקב מסודר של אירועים שטופלו והפעולות שננקטו בידי הגורמים הרלבנטיים. בפרט, התאגיד ינהל "יומן אירועים" בו יתועדו, בסמוך ככל הניתן למועד ההתרחשות, מכלול הידיעות, ההחלטות והפעולות שבוצעו בקשר לאירוע סייבר.

78. התאגיד הבנקאי יגדיר מאגר של פעילויות תגובה (כדוגמת שינויי קונפיגורציה, הגבלה ו/או הסטה של תקשורת, פריסה של תוכנות וכיו"ב) בהתאם לתרחישים השונים, ויגדיר את 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 המסוים שבמסגרתו הופעלה.

79. התאגיד הבנקאי 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.

תרגולים

80. התאגיד הבנקאי יגדיר תכנית לביצוע תרגולים של מערכי התגובה השונים בתאגיד, תוך התחשבות בסוגי תרגול שונים (דימוי התקפות, "משחקי מלחמה", תרגילים "מועמדים" וכיו"ב) ובהתייחס לגורמים המעורבים (למשל: גורמים טכניים, צוותי ניהול משבר, דרגי מקבלי החלטות, דוברות וכיו"ב).

דיווח על אירוע סייבר

81. התאגיד הבנקאי יקיים מערך דיווח פנימי נאות כחלק מניהול סיכונים ואירועי סייבר. במסגרת זו תוגדר מדיניות דיווח מפורטת, שתקבע בין היתר את הגורמים הפנימיים והחיצוניים אליהם יתבצעו הדיווחים, את מתכונתם ואת תדירותם.

82. התאגיד הבנקאי ידווח לפיקוח על הבנקים על אירוע סייבר או התרעה על אירוע סייבר, בהתאם להוראת הדיווח לפיקוח על הבנקים.

עדכונים

חוזר 06 מס'	גרסה	פרטים	תאריך
2457	1	הוראה מקורית	16/3/15