מדינת ישראל
משרד האוצר - אגף שוק ההון, ביטוח וחסכון

כ"ז באב התשע"ו
31 באוגוסט 2016

חוזר גופים מוסדיים 2016-9-14
סיווג: כללי

ניהול סיכוני סייבר בגופים מוסדיים

בתוקף סמכותי לפי סעיפים 2(ב) ו-42 לחוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ"א-1981, סעיף 39(ב)(1) ו-40 לחוק הפיקוח על שירותים פיננסיים (קופות גמל), התשס"ה-2005 ותקנה 8(א)(20) לתקנות הפיקוח על שירותים פיננסיים (דירקטוריון וועדותיו), התשס"ז-2007 ולאחר התייעצות עם הוועדה המייעצת, להלן הוראותיי:

1. כללי

עם ההתפתחות הטכנולוגית ותלותן של פעילויות עסקיות ברשת האינטרנט גדלו היקפם ועוצמתם של איומים קיברנטיים העלולים לשבש את פעילותם התקינה של גופים מוסדיים. על כן, עלה הצורך לעדכן את תפיסת ההגנה של גופים מוסדיים כך שתינתן התייחסות גם לאיומים אלו.

אם בעבר תפיסת ההגנה התייחסה לאבטחת מידע, דהיינו הגנה על המידע בהיבט של סודיות, שלמות וזמינות המידע, הרי שכיום אבטחת מידע הנה רק רובד אחד בתוך תחום ניהול סיכוני הסייבר עליו יש להגן. לצד הגנה על המידע, עולה הצורך להגן גם מפני שיבוש פעילותו התקינה של הרכיב הממוחשב עליו מתבסס הגוף המוסדי.

מטרת חוזר זה הינה לקבוע עקרונות להגנה על נכסי הגוף המוסדי במטרה להבטיח את שמירת זכויות העמיתים והמבוטחים על ידי שמירה על סודיות, שלמות וזמינות נכסי המידע, מערכות המידע, התהליכים העסקיים ופעילותו התקינה של הגוף המוסדי. ניהול סיכוני הסייבר יכלול פעולות של מניעה, נטרול, חקירה והתמודדות עם איומי ואירועי סייבר במטרה לצמצם את השפעתם והנזק הנגרם מהם, בטרם התרחשותם, במהלכם ולאחריהם.

החוזר מגדיר עקרונות לניהול סיכוני סייבר בגוף מוסדי ומחייב לנהל סיכונים אלו. על הגופים המוסדיים לנהל את סיכוני הסייבר באופן אפקטיבי, עדכני ושוטף, ועל בסיס עקרונות ממשל תאגידי נאותים הכוללים התייחסות לשיטות, לתהליכים ולבקרות ובאופן אשר יאפשר להם להתמודד עם איומי סייבר ולנהל אירועי סייבר.

לאור מרכזיות גופים מוסדיים בשוק ההון הישראלי, ולאור הסיכון הגבוה בתחום הגנת הסייבר, מצופה מגוף מוסדי לאמץ סטנדרטים גבוהים בתחום זה.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

תוכן עניינים

1. כללי 1
2. הגדרות 4
3. ממשל תאגידי 6
   א. תפקידים ותחומי אחריות 6
      1) דירקטוריון גוף מוסדי 6
      2) מנכ"ל גוף מוסדי 6
      3) ועדת היגוי לניהול סיכוני סייבר 6
      4) מנהל הגנת סייבר 7
   ב. מסגרת ניהול סיכוני סייבר (Framework) 7
      1) מדיניות 7
      2) נהלים 8
      3) תכנית עבודה 8
4. ניהול הסיכון 8
   א. הערכת סיכונים ועדכניותה 8
   ב. דיווח וניטור סיכונים 9
   ג. יישום בקרות 9
5. הגנת סייבר של גוף מוסדי 9
   א. הגנת סייבר, ניטור ובקרה 9
      1) איסוף מודיעין 9
      2) ניטור ובקרת מערכות מידע 10
      3) מוכנות לאירועים 10
   ב. ביצוע סקרים 11
      1) סקרים ומבחני חדירה 11
      2) טיפול בממצאי סקרים ומבחני חדירה 12
   ג. אבטחת מערכות, תקשורת ותפעול 12
      1) אבטחת רשת וגישה מרחוק 13
      2) קישוריות גוף מוסדי לרשת האינטרנט 13
      3) הוצאת נתונים אל מחוץ לחצרותיו 13
      4) הצפנה 13
      5) אבטחת מערכות ועדכונן 13
      6) אבטחת מערכות קצה 14
      7) מניעת קוד עוין 14
      8) הגנת סייבר בתהליכי רכש ופיתוח 14
      9) הפרדה בין סביבות ואבטחתן 15
   ד. ניהול משתמשים והרשאות 15

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

1) ניהול משתמשים 15
2) סיסמאות ואמצעי הזדהות 15
3) ניהול הרשאות ובקרת גישה 16
ה. מיקור חוץ (Outsourcing) 16
1) דרישות הגנת סייבר בהסכמי מיקור חוץ 16
2) שירות למערכות גוף מוסדי על ידי נותן שירות מיקור חוץ 16
3) שירותי מחשוב ענן 17
ו. אבטחה פיסית וסביבתית 17
1) אזורים מאובטחים 17
2) אבטחת ציוד וניירת 18
ז. הגנת סייבר במשאבי אנוש וגיוס עובדים 18
1) הגנת סייבר בתהליך גיוס עובדים 18
2) אבטחת מידע בעת מעבר תפקיד או סיום העסקת עובדים 18
3) מודעות הגנת סייבר והדרכה 18
6. אבטחת ערוצי קשר עם לקוחות 19
א. אבטחת ערוצי תקשורת מבוססי אינטרנט 19
ב. רישום מבוטחים/עמיתים לפעילות 19
1) וידוא זהות בתהליך הרישום 19
2) הסכמה מפורשת של לקוחות בטרם רישום לפעילות 19
ג. הזדהות לקוחות לערוצי שירות 20
ד. שליחת מידע באמצעים דיגיטליים 20
ה. שיווק מוצרים באמצעים דיגיטליים (ומסחר דיגיטלי) 20
7. אבטחת ערוצי קשר עם גורמים חיצוניים 20
א. אבטחת ערוצי קשר בין גופים מוסדיים לבין בעלי רישיון 20
ב. אבטחת ערוצי קשר בין גופים מוסדיים 21
8. החלת ההוראה 21
א. תחולה 21
ב. תחילה 21
ג. ביטול תקפות 21

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

2 . הגדרות

"**איום – Threat**" – אפשרות פוטנציאלית לפגיעה בסודיות, שלמות, או זמינות המידע.

"**אירוע סייבר**" – כל מקרה של תקיפת מערכות או אמצעי טכנולוגי אחר ששייכים לגוף מוסדי, העלולה לפגוע בסודיות, שלמות או זמינות מערכות או המידע של גוף מוסדי.

"**אמצעי זיהוי**" – אמצעי המאפשר אימות פרטים של אדם או מערכת בעת ניסיון גישה או ביצוע פעולות מטעמם במערכת מידע.

"**בעל רישיון**" – כהגדרתו בחוק הפיקוח על שירותים פיננסיים (ייעוץ, שיווק, ומערכת סליקה פנסיונית), התשס"ה-2005 ולרבות "סוכן ביטוח" או "סוכן" כהגדרתם בחוק הפיקוח על שירותים פיננסיים (ביטוח) תשמ"א-1981

"**גוף מוסדי בעל היקף פעילות נמוך**" – כהגדרתו בשער 1 לחוזר המאוחד - הגדרות.

"**גישה מרחוק – Remote Access**" – התחברות גורם (חיצוני או פנימי) מחוץ לרשת הארגון אל הרשת הפנימית של הארגון.

"**הזדהות חזקה – Strong Authentication**" – מבוססת על שימוש באמצעי זיהוי המתבסס על לפחות שניים מתוך הפריטים הבאים:

א. Something You Are – תכונה פיזיולוגית ייחודית של המשתמש.

ב. Something You Have – פריט הנמצא ברשות המשתמש.

ג. Something You Know – פריט מידע הידוע למשתמש.

"**הערכת סיכונים**" – תהליך של הערכת רמת הסיכון של כלל המידע, מערכות המידע והתהליכים העסקיים והטכנולוגיים בגוף. התהליך ממפה את הסיכונים השונים הנובעים מהפעילות והתהליכים בגוף המוסדי.

"**הצפנה**" – המרת מידע גלוי (Clear Text) למידע מוצפן (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

"**טוקניזציה**" – תהליך המרת נתונים רגישים בערכים חלופיים שאינם רגישים ("טוקנים") אשר אין סכנה בחשיפתם. לרוב, תהליך זה מבוצע על ידי מערכת המחליפה את הערך המקורי בערך חלופי, ומאפשרת את שחזור הערך המקורי בעת הצורך, ובאופן מוגבל.

"**זיהוי חד ערכי**" – ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

"**יעד התאוששות** (RTO - Recovery Time Objective)" – יעד אותו קבע גוף מוסדי להחזרת פעילות עסקית ספציפית ומערכות התומכות בה לרמת שירות מוגדרת בפרק זמן מוגדר;

"**יעד שירות**" – רמת שירות לעמיתים או למבוטחים במצב חירום שעליה החליט דירקטוריון גוף מוסדי;

"**לוג - Log**" – קובץ התיעוד של נתיב בקרה, מכיל פרטים בנוגע לפעולות הממוחשבות המבוצעות בארגון.

"**מידע רגיש**" – כהגדרתו בחוק הגנת הפרטיות, תשמ"א-1981, וכל מידע אשר סווג על ידי הגוף כרגיש.

"**מיסוך נתונים**" – טכנולוגיה המבצעת הסתרה של נתונים או חלק מהם אשר הוגדרו סודיים, כך שבעת הצגת נתון, הוא מוחלף ברצף תווים אחר. שימוש בטכנולוגית מיסוך מאפשר לעבד נתונים כך שהצפייה בהם תהיה מוגבלת לגורמים מועטים בלבד.

"**מערכות ליבה**" – המערכות שהוגדרו על ידי גוף מוסדי כמערכות מרכזיות של הארגון ואושרו ככאלה על ידי הדירקטוריון, לרבות כל מערכת אשר יש לה השפעה ישירה על זכויות עמיתים ומבוטחים וכל מערכת שהמידע המנוהל בה עשוי להשפיע באופן מהותי על עסקי הגוף המוסדי ויציבותו, בין היתר, לרבות המערכות שלהלן וכל אחת מאלה:

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

א. מערכות ביטוח חיים;

ב. מערכות ביטוח כללי;

ג. מערכות ביטוח בריאות;

ד. מערכות תפעול זכויות עמיתים ומבוטחים;

ה. מערכות ההשקעות והפיננסים;

ו. מערכות מקבילות ו/או מערכות התומכות מהותית בפעילות המערכות המפורטות לעיל כגון: מערכת הכספים, מערכת אקטוארית, מערכת תביעות, מערכת ביטוח משנה וכד'.

"**מערכות מידע**" – כלל המערכות התומכות בפעילות העסקית בגוף מוסדי, לרבות ציוד ממוכן, תשתיות וטכנולוגיות התומכות בתפעולן, בין השאר: שרתים, ציוד תקשורת, ציוד הגנת סייבר.

"**מערכות OT (Operation Technology)**" – מערכות (לרבות תוכנה וחומרה) המיועדות לשליטה ובקרה של מערכות תעשייתיות או אוטומציה (באמצעות בקרה ושליטה ישירה) של התקנים פיזיים.

"**נכסי מידע**" – נכס מידע הוא מאגר נתונים, התקן, או רכיב של סביבה התומך בפעילויות הקשורות במידע (לרבות תשתיות). נכסי מידע כוללים, בדרך כלל, חומרה, תוכנה ומידע.

"**נתיב בקרה**" – תיעוד פעולות המתבצעות במערכות מידע. התיעוד מקשר את הפעולה לנתונים נוספים כגון: שם מבצע הפעולה, המועד, הפעולה עצמה ועוד, לצורך זיהוי האלמנטים שהשתנו.

"**סייבר**", "**המרחב הקיברנטי**" – המתחם הפיזי והלא פיזי שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה ולרבות רובד אנושי (האנשים המשתמשים בכל אלה). הגנת סייבר כוללת בתוכה את כלל היבטי אבטחת המידע.

"**סיכון סייבר**" – סיכון לשימוש לא מורשה בזהות, הפרעה לפעילות על ידי פגיעה בפעילות הרשת או השבתת שירותים, פגיעה במערכות, גניבה של נכסים דיגיטליים, החדרה של קודים או תוכנות זדוניות, חדירה למערכת או חשיפת מידע.

"**סיכון שורשי**" – סיכון מובנה. מאפיין את פעילות הגוף ללא תלות באמצעי הגנת סייבר המיושמים בגוף.

"**סיכון שיורי**" – סיכון שנותר לאחר יישום בקרות ואמצעי הגנת סייבר בגוף.

"**סקר סיכונים**" – תהליך שמטרתו זיהוי האיומים, הערכת הסיכון הנובע מהם (תוך התחשבות בסבירות התממשותם והנזק הפוטנציאלי כתוצאה מכך) וזיהוי הבקרות הנדרשות לצמצום סיכונים אלה.

"**סריקת חשיפות אבטחת מידע – Vulnerability Scan**" – סריקה לאיתור חולשה במערכת העלולה להוביל להתממשות איום.

"**קוד עוין**" – קוד המושתל על ידי משתמש זדוני ועשוי לגרום לביצוע פעולות לא רצויות, פגיעה במערכות הארגון וזליגת מידע רגיש לגורמים לא מורשים.

"**הצפנה מקצה לקצה**" – הצפנת תווך התקשורת או הנתונים מהתחנה או השרת (למשל: תחנת עבודה של משתמש) היוזמת את השירות אל התחנה או השרת (למשל: מערכת מידע) המספקת את השירות.

"**רשת פנימית – Local Area Network (LAN)**" – קבוצת מחשבים המקושרים זה לזה בעזרת ציוד תקשורת ונגישים למשאבים בתוך הארגון. במובן של הוראה זו, רשת פנימית הנה רשת המופרדת מרשתות ציבוריות.

"**תווך תקשורת ציבורי – Public Network**" – תשתיות תקשורת המשרתות או משתפות מספר רב של צרכנים ואינן שייכות לאחד מהם. תשתיות אינטרנט מוגדרות כתווך תקשורת ציבורי.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

"**תעודת הצפנה – SSL Certificate**" – תעודה הניתנת על ידי "רשות אמון" המאשרת את אמינות החיבור ומאמתת את מהימנות מקור החיבור.

"**DNS**" – שרות הממיר כתובות IP לכתובות מילוליות(URL) ובכך מקל את השימוש ברשת האינטרנט.

3 . ממשל תאגידי

א. תפקידים ותחומי אחריות

1) דירקטוריון גוף מוסדי

א) יאשר מדיניות כאמור בסעיף 1.ב.3) בתחום ניהול סיכוני סייבר, לכל הפחות אחת לשנה.

ב) ידון בתכנית מעודכנת לניהול סיכוני סייבר והערכת סיכונים, הכוללת תכנית להפחתת סיכונים ופירוט השינויים במסגרת ניהול תחום סיכוני הסייבר, לכל הפחות אחת לשנה.

ג) יאשר את כתב מינוי ועדת ההיגוי בתחום סיכוני סייבר שבמסגרתו יוגדרו תפקידיה וסמכויותיה של הוועדה כאמור בסעיף 3.א.3) להלן.

2) מנכ"ל גוף מוסדי

א) יבטיח את ניהולו התקין של תחום סיכוני הסייבר בהתאם ליעדים, למדיניות ולצורכי הגוף המוסדי.

ב) יקיים מסגרת נהלים בהתאם לאמור בסעיף 2.ב.3) ויאשר תכנית עבודה שנתית בתחום ניהול סיכוני סייבר בהתאם לאמור בסעיף 3.ב.3).

ג) יעמיד משאבים נאותים ליישום תכנית עבודה לניהול סיכוני סייבר.

ד) יקיים מבנה ארגוני הולם לניהול סיכוני סייבר ויגדיר את אחריות הגורמים העוסקים בתחום ואת הממשקים ביניהם, תוך שמירה על עקרונות של הפרדת תפקידים וסמכויות.

ה) יקיים מנגנוני בקרה ופיקוח נאותים בתחום ניהול סיכוני סייבר.

ו) יקבע הוראות דיווח אליו ולגורמים רלוונטיים אחרים בעת אירועי סייבר.

ז) ידון בהמלצות ועדת ההיגוי בהתאם לאמור בסעיף 3.א.3)ח).

ח) יבחן אימוץ תקן ת"י ISO 27001 של מכון התקנים הישראלי.

3) ועדת היגוי לניהול סיכוני סייבר

א) גוף מוסדי ימנה ועדת היגוי ובראשה יעמוד המנהל הכללי של הגוף המוסדי ובין חבריה יכללו מנהל מערכות המידע, מנהל הסיכונים ומנהל הגנת הסייבר.

ב) יכול שהמנהל הכללי של הגוף המוסדי לא יעמוד בראש ועדת ההיגוי, ובלבד שהתקיים דיון בהנהלת הגוף המוסדי בו הוצגו הנימוקים לבחירתו של חבר הנהלה אחר בעל כישורים מתאימים.

ג) בגוף מוסדי בעל היקף פעילות נמוך יכול שלא תוקם ועדת היגוי לניהול סיכוני סייבר ובלבד שכל תפקידי הוועדה שיפורטו להלן יועברו לאחריות המנכ"ל.

ד) קבוצת חברות שהינן תחת אותו בעל שליטה, יכולה לקיים ועדת היגוי אחת לקבוצת החברות (להלן – ועדת היגוי קבוצתית) ובלבד שהגורמים המוסמכים לכך בכל גוף מוסדי בקבוצה, יאשרו את מינוי ועדת ההיגוי הקבוצתית כוועדת ההיגוי של הגוף המוסדי. בהינתן ומונתה ועדת היגוי קבוצתית, ניתן שיתקיימו דיונים משותפים הרלוונטיים לכל חברות הקבוצה ובלבד שבנוסף, יתקיימו דיונים בנושאים פרטניים הייחודיים לכל חברה בקבוצה, בנושאים שבהם נדרש גוף מוסדי בקבוצה לדון בוועדת ההיגוי, בהתאם להוראות חוזר זה. לדיונים הפרטניים

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

יוזמנו כל הגורמים שהוגדרו בחוזר זה וגורמים שהוסמכו לכך מטעם הגוף המוסדי שבקבוצת החברות.

ה) הוועדה תתכנס לכל הפחות אחת לרבעון ותערוך פרוטוקולים של ישיבותיה.

ו) הוועדה תסייע למנהל הכללי לקבל החלטות ולבצע את תפקידיו בכל הקשור לניהול התקין של תחום ניהול סיכוני סייבר, מתוך ראיה אינטגרטיבית של התחום ברמה כלל ארגונית.

ז) הוועדה תבצע מעקב אחר יישום תכנית העבודה בתחום ניהול סיכוני סייבר.

ח) הוועדה תדון בתוצאות הערכת סיכונים ובתכנית להפחתתם בהתאם לאמור בסעיף 4.ב..

ט) הוועדה תדון בסיכונים אפשריים בהפעלת שימוש במערכות מבוססות ענן בהתאם לאמור בסעיף 5.ה.3)א).

י) הוועדה תתחקר ותפיק לקחים לגבי כל אירוע סייבר משמעותי בהתאם לאמור בסעיף 5.א.2)י).

יא) הוועדה תדווח לדירקטוריון הגוף המוסדי, לכל הפחות אחת לשנה, על פעילותה, מסקנותיה והמלצותיה בנושאים שהוסמכה לעסוק בהם.

יב) ועדת היגוי שבראשה עומד חבר הנהלה אחר מהמנהל הכללי, תדווח למנהל הכללי על סטטוס ביצוע תכנית העבודה אחת לרבעון ותעביר לו את המלצותיה בעניין תוצאות הערכת סיכונים והתכנית להפחתתם בהתאם לאמור בסעיף 4.ב. ולגבי כל אירוע סייבר משמעותי בהתאם לאמור בסעיף 5.א.2)י).

4) מנהל הגנת סייבר

א) גוף מוסדי ימנה מנהל הגנת סייבר בעל מומחיות וניסיון מוכחים בתפקיד ניהולי בתחום הגנת הסייבר.

ב) מנהל הגנת סייבר לא ימלא כל תפקיד שעלול לפגוע ביכולתו לבצע כראוי את תפקידו כמנהל הגנת סייבר או להגבילה, ויהיה כפוף לאחד מחברי ההנהלה החברים בוועדת ההיגוי.

ג) חבר ההנהלה הממונה על מנהל הגנת סייבר יהיה אחראי על הפעילות המתבצעת בתחומי ניהול סיכוני הסייבר וכן על בקרת תכנית העבודה בנושא זה, בהתאם למדיניות ניהול סיכוני הסייבר של הגוף המוסדי.

ד) מנהל הגנת סייבר יפעל ליישום מדיניות בתחום ניהול סיכוני סייבר בגוף המוסדי, ייעץ וינחה את הגוף מוסדי בנושאי הגנת סייבר, יקבע נהלי עבודה, ומסגרת דיווחים ויבצע פיקוח ובקרה בנושאים אלו והכל בהתאם להוראות חוזר זה.

ה) למנהל הגנת סייבר יוקצו המשאבים והמקורות הנאותים לביצוע תפקידו.

ב. מסגרת ניהול סיכוני סייבר (FRAMEWORK)

1) מדיניות

גוף מוסדי יגדיר מדיניות לניהול סיכוני סייבר הקובעת עקרונות מנחים להגנת סייבר ליישום בגוף. עקרונות אלו יתייחסו, בין היתר, ליעדים שהוגדרו, למסגרת ארגונית (תחומי אחריות, קווי דיווח, פיקוח ובקרה), ליישום הגנת סייבר בהיבט של מחשוב ענן (סוגי השירותים והיקפם, אחריות, פיקוח ובקרה), ליישום הגנת סייבר בהיבטי משאבי אנוש (מהימנות עובדים, הדרכה ובקרה), ליישום הגנת סייבר פיסית ולוגית בתהליכים, במערכות ובתשתיות הגוף ולכל הנושאים שיש להם השפעה רוחבית על יחידות גוף מוסדי.

2) נהלים

א) גוף מוסדי יקבע נהלים המגדירים את תהליכי הגנת הסייבר בגוף והמתייחסים לנושאים המפורטים בהוראה זו ויפעל להטמעתם.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) הנהלים ייגזרו ממדיניות ניהול סיכוני סייבר ומהנחיות חיצוניות (כגון אסדרה או מחויבויות חוזיות).

ג) גוף מוסדי יגדיר נוהל לדרישות הגנת סייבר ביחס לסיכוני מיקור חוץ בהתאם לאמור בסעיף 5.ה.1)א).

ד) הנהלים יעברו תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בסביבה הטכנולוגית או שינוי במתאר הסיכונים של הגוף המוסדי, ולכל הפחות אחת ל – 24 חודשים.

3) תכנית עבודה

תכנית העבודה תיגזר ממדיניות ונהלי סיכוני סייבר של גוף מוסדי. התכנית תתייחס לאופי המידע, לתהליכים, לתשתיות ולמערכות הגוף המוסדי ותכלול, לכל הפחות, תכנית לניהול סיכוני סייבר כאמור בסעיף 4, לרבות תכנית להפחתתם, תכנית להעלאת רמת מודעות העובדים בהתאם לאמור בסעיף 3.ז.5), תכנית לביצוע סקרים בהתאם לאמור בסעיף 5.ב.1)ד) ותכנית היערכות וניהול אירועי סייבר בהתאם לאמור בסעיפים 5.א.3)ב) – 5.א.3)ד).

4. ניהול הסיכון

גוף מוסדי יגדיר תכנית לניהול סיכוני סייבר, שתעסוק בסיכונים לתהליכים, למערכות ולמידע ותתבצע בהתאם לסעיפים שלהלן:

א. הערכת סיכונים ועדכניותה

1) גוף מוסדי יעריך את סיכוני הסייבר כדי לספק תמונת מצב עדכנית של מכלול הסיכונים שהוא מתמודד עמם.

2) הערכת הסיכונים תכלול, בין היתר, את השלבים הבאים:

א) זיהוי תהליכים, מערכות ונכסי מידע.

ב) מיפוי סיכונים לתהליכים, מערכות ולנכסי מידע כאמור.

ג) מיפוי סיכונים שורשיים.

ד) מיפוי והערכת הבקרות למזעור סיכונים אלה, לרבות בחינה של מידת השפעת הבקרות עליהם.

ה) הערכת סיכון שיורי (בהתאם להשפעת הבקרות שיושמו).

3) לצורך זיהוי והערכת הסיכונים, גוף מוסדי ישתמש, בין היתר, בממצאי ביקורות וסקרים, איסוף וניתוח אירועי סייבר שהתרחשו בגוף המוסדי בעבר וניתוח תרחישים לזיהוי אירועים פוטנציאליים של התממשות הסיכון.

4) הערכת הסיכונים תתייחס בין היתר למערכות OT ולסביבות פיתוח ובדיקות, העשויות להכיל מידע רגיש או לגלם חשיפות למערכות הגוף המוסדי כולו.

5) הערכת הסיכונים תתייחס למכלול שרשרת האספקה ולסיכונים הנובעים מאופי הפעילות אל מול הגורמים השונים במרחב (מיקור חוץ, נותני שירותים, לקוחות, חו"ל וכו').

6) גוף מוסדי יוכל להסתמך על הערכת סיכונים שביצע ספק מיקור חוץ שהינו גוף מוסדי או תאגיד בנקאי, ובלבד שקיבל את תוצאותיה והניח דעתו בעניין.

7) גוף מוסדי יוכל להסתמך על הערכת סיכונים של ספק מיקור חוץ ובלבד שבוצעה על ידי גורם בלתי תלוי בספק מיקור חוץ וניתנה לגוף המוסדי חוות דעת (לרבות מידע מספק לגבי תהליכי הבקרה ותוצאות הבדיקות שנעשו) כי רמת ההגנה שמיישם ספק מיקור החוץ תואמת את הדרישות מגוף המוסדי.

8) גוף מוסדי ינהל רשימה עדכנית של נכסי המידע ותהליכים הקיימים בו. הרשימה תעודכן לכל הפחות

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

אחת לשנתיים.

9) הערכת הסיכונים תעבור תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בתהליכים עסקיים, בסביבה הטכנולוגית או במתאר הסיכונים, ולכל הפחות אחת ל-36 חודשים.

ב. דיווח וניטור סיכונים

1) הערכת סיכונים תהווה בסיס לתכנית להפחתתם, תשולב בתכנית העבודה ותנחה את הגוף המוסדי בהקצאת משאבים להטמעת אמצעים לניהול סיכוני סייבר.

2) תוצאות הערכת סיכונים ותכנית להפחתתם ידונו בוועדת היגוי יאושרו בה ויוצגו לדירקטוריון. הצגה זו תכלול, לכל הפחות, פירוט סיכונים שיוריים, תכנית הפחתת סיכונים ופירוט הסיכונים המשמעותיים שגוף מוסדי החליט שלא להפחית לרמה מזערית ככל שניתן.

ג. יישום בקרות

בהתאם להערכת הסיכונים וכחלק מהתוכנית להפחתתם יגדיר גוף מוסדי בקרות הגנת סייבר מתאימות ואפקטיביות. על הבקרות להתייחס, למידע, למערכות ולתהליכים בגוף וכן לצדדים שלישיים המספקים שירות לגוף המוסדי.

5 . הגנת סייבר של גוף מוסדי

גוף מוסדי יבצע הערכה שנתית של התאמת אמצעי ההגנה למכלול סיכוני הגנת הסייבר שלו. הערכה זו תתחשב בהתפתחויות מתאר האיומים, באופי ההתקפות הנוכחי ובטכנולוגיות הקיימות במטרה להתמודד עם איומים אלה.

להלן יפורטו אמצעי ההגנה שעל גוף מוסדי ליישם:

א. הגנת סייבר, ניטור ובקרה

גוף מוסדי יבסס תמונת מצב עדכנית אודות הגנת הסייבר שלו תוך זיהוי חולשות ואיומים ויפעל לצמצום חשיפות לסיכונים אלו.

1) איסוף מודיעין

א) גוף מוסדי יאסוף וינתח מידע רלוונטי, ממקורות פנימיים וחיצוניים לצורך יצירת תפיסה כוללת ועדכנית של איום הסייבר וחשיפת הגוף המוסדי למול האיום, כבסיס לקבלת החלטות מושכלת, תעדוף של דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת.

ב) גוף מוסדי יבחן עבודה מול המרכז הלאומי להתמודדות עם איומי סייבר (Cert-il) ולשיתוף הדדי של מידע קיברנטי אופרטיבי עמו.

2) ניטור ובקרת מערכות מידע

א) גוף מוסדי יקיים מערך ניטור ובקרה לקבלת דיווחים בזמן אמת ממערכותיו השונות אודות חשש לאירוע סייבר.

ב) גוף מוסדי יישם נתיב בקרה וניטור של פעולות ושאילתות המתבצעות במערכות המנהלות מידע רגיש על לקוחות וכן במערכות שרמת החשיפה שלהן לביצוע פעילות בלתי מורשה הינה גבוהה (בהתאם להערכת הסיכונים של הגוף), במטרה לאפשר התחקות אחר פירוט הרישום לצורך ביקורת, זיהוי של פעילות בלתי מורשה, תחקור לאחר מעשה ומניעת התכחשות.

ג) נתיב הבקרה האמור יתייחס לפעולות ושינויים המבוצעים במערכות וכן לשאילתות וגישה לנתונים ולכל הפחות גישה למידע רגיש. יתועדו גם ניסיונות לביצוע פעולות (לרבות ניסיונות חיבור למערכות, שאילתות ועדכוני נתונים) שלא צלחו.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ד) נתיב בקרה יכלול מידע על מועד ביצוע הפעולה, מקור הפעולה, הגורם שביצע או ניסה לבצעה ועל מי בוצעה הפעולה. במערכות ליבה - לרבות ערך טרום ביצוע הפעולה ולאחריה.

ה) פרק הזמן לשמירת נתיב בקרה יתאים למטרות נתיב הבקרה, ובכל מקרה לא יפחת מ-12 חודשים.

ו) נתיב הבקרה יהיה מוגן מפני מחיקה או שינוי בלתי מורשה.

ז) גוף מוסדי יתבסס על ניתוח מודיעיני בהתאם לאמור בסעיף 5.א.1)א) וישתמש במערכות ותהליכים שיזהו ויתריעו על פעילות המוגדרת אסורה או חשודה. ההתרעות יתוכננו בהתבסס על הגדרת תרחישי איום ובהתאם להערכת הסיכונים.

ח) זיהוי והתרעה בגין אירועים חריגים כאמור בסעיף 5.א.2)ז) יתייחס לפעולות שמקורן מחוץ לגוף או בתוכו, תוך שימת דגש על מערכות תשתית, מערכות אפליקטיביות ומערכות המנוהלות או מאוחסנות מחוץ לגוף.

ט) זיהוי והתרעה של פעולות חריגות שמקורן מחוץ לגוף מוסדי יכול להתבצע על ידי מיקור חוץ בהינתן והוא עומד בדרישות גוף מוסדי לביצוע ניטור ומתריע לגוף מוסדי בעת התגלותם של אירועים חריגים.

י) מנהל הגנת סייבר יתחקר אירועים חריגים. ועדת ההיגוי תדון בממצאי כל אירוע משמעותי, תפיק ממנו לקחים ותעביר המלצותיה למנכ"ל תוך פרק זמן סביר שלא יעלה על שלושה חודשים.

יא) גוף מוסדי יבחן מעת לעת את חוקי הניטור שהוגדרו, תקינותם ואיכות האירועים שמתקבלים, ולכל הפחות אחת לשנה.

3) מוכנות לאירועים

א) גוף מוסדי ימפה את גורמי האיום ויפעל להבטחת יכולת מוכנות, התגוננות ושרידות בפני התקפות.

ב) גוף מוסדי יגדיר תכנית היערכות וניהול אירועי סייבר, בהתאם להערכת סיכונים ולניתוח תרחישי קיצון (כגון: גישה לא מורשית לנכסי הגוף, זליגת מידע, התחזות, נוזקות, הונאה, מניעת שירות וכדומה).

ג) התכנית תכלול את השלבים הבאים:

(1) גילוי - גילוי וזיהוי השלב בו נמצא האירוע תוך פירוט שלבי פעולה (בידוד, חקירה, איסוף ראיות, הסקת מסקנות וכדומה).

(2) הערכת מצב - בירור וניתוח אירוע הסייבר ובחינת דרכי פעולה להתמודדות עם האירוע.

(3) הכלה ובלימה - השגת שליטה על האירוע ועצירת החמרתו.

(4) התאוששות - הכרעת האירוע תוך מזעור הנזק שנגרם.

(5) השבה לשגרה - חזרה לפעילות מלאה של הגוף המוסדי לאחר תיקון כל נזק שנגרם.

ד) בנוסף, התכנית תפרט לכל הפחות, את הבאים:

(1) אופן תגובה ודרכי פעולה של הגוף, בהתייחס לתרחישים שונים, את אופן יישומן ואת הגורמים האחראים על הפעלתן.

(2) התקשרות עם גורמים פנימיים וחיצוניים, ובכללם לקוחות, בהתאם לתרחישים שונים.

(3) מתכונת ותדירות דיווח על אירועים. לרבות, גורם מדווח, נמען הדיווח וזמן התגובה הסביר לדיווח.

ה) התכנית תעודכן על בסיס שנתי, בהתאם להערכת סיכונים מעודכנת, ותכלול התייחסות גם לעובדים חדשים ולמיקור חוץ.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ו) גוף מוסדי יגדיר תכנית התאוששות ויעדי התאוששות מאירוע סייבר עד לתפקוד מלא בעת חזרה לשגרה, תוך התייחסות לאיומי הייחוס, תרחישי הייחוס, יעדי השירות בחירום שקבע לעצמו ויעדי השירות שהוגדרו כאמור בחוזר "ניהול המשכיות עסקית בגופים מוסדיים" 2013-9-11 ובכל חוזר אחר שיבוא במקומו.

ז) גוף מוסדי יקיים, לכל הפחות, אחת לשנה תרגול של כלל המערכים הרלוונטיים במטרה להכין אותו להפעלת התוכניות שהוזכרו לעיל ולשיפורן בהתאם ללקחי תרגולים שבוצעו.

ח) גוף מוסדי יקים צוות תגובה להתמודדות עם אירועי סייבר, שיערוך תרגול אירוע אמת אחת לשנה, תוך שימוש במערכות ותשתיות הגוף המוסדי.

ט) גוף מוסדי יקבע מנגנון דיווח על אירועי סייבר שיהיה נגיש לעובדים.

י) מנהל הגנת סייבר ידווח לוועדת ההיגוי דוח המסכם אודות כלל ניסיונות התקיפה ואירועי סייבר שהתרחשו (לרבות כאלה שלא הובילו לפגיעה חמורה), ההחלטות והפעולות שבוצעו, אחת לרבעון.

יא) גוף מוסדי ידווח בהקדם האפשרי לדירקטוריון הגוף המוסדי ולממונה על שוק ההון, ביטוח וחיסכון על כל אירוע סייבר משמעותי שכתוצאה ממנו, באופן ישיר או עקיף:

(1) נפגעו או הושבתו מערכות ייצור המכילות מידע רגיש למשך של יותר מ-3 שעות.

(2) יש אינדיקציות לכך שמידע רגיש של לקוחות הגוף המוסדי או עובדיו נחשף או דלף.

ב. ביצוע סקרים

1) סקרים ומבחני חדירה

א) גוף מוסדי יישם כחלק מתכנית העבודה הרב-שנתית, סקרים ומבחני חדירה המכסים את המערכות והתהליכים הארגוניים.

ב) הסקרים והמבחנים יבחנו תאימות מערכות ותהליכים למדיניות ולנהלי סיכוני סייבר של הגוף, הן ברמת בדיקת קיום בקרות להגנת סייבר והתאמתן והן ברמת בדיקת אפקטיביות הבקרות.

ג) הסקרים יכללו ממצאים והמלצות.

ד) תכנית העבודה לביצוע הסקרים והמבחנים תיישם את הנושאים הבאים, בהתאם להערכת הסיכונים:

(1) כיסוי של כל רמות האבטחה של התהליכים והמערכות (ניתן גם באופן רוחבי), לרבות: הגנות פיסיות וסביבתיות, הגנות תשתיתיות הכוללות אחסון, מערכות הפעלה, רשתות, בסיסי נתונים, רכיבי Middleware וכדומה, הגנות אפליקטיביות, הגנות ברמת הלוגיקה העסקית המיושמת במערכת וכן התהליכים הסובבים את המערכת כגון ניהול משתמשים והרשאות, תהליכי גיבוי, ניטור וכדומה.

(2) ביצוע מבחני חדירה תקופתיים הכוללים: מבחן המדמה ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים), בדיקות הנדסה חברתית, התחזות ופישינג, לכל הפחות אחת לשנה.

(3) ביצוע סריקת חשיפות אבטחת מידע (Vulnerability Scan) תקופתית לכל הפחות אחת לרבעון (בגוף מוסדי בעל היקף פעילות נמוך אחת לשנה), לזיהוי חשיפות אבטחת מידע טכנולוגיות במערכות הגוף. הסריקות תתייחסנה לחשיפות הנובעות מחיבור מערכות הגוף לרשתות חיצוניות ("סריקה חיצונית") ולחשיפות הנובעות מניסיונות תקיפה מתוך רשת הגוף ("סריקה פנימית").

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

(4) תדירות ביצוע סקרים תיקבע בהתאם למידת החשיפה של המערכת לאיומים, רגישות המידע המנוהל במערכת ושינויים שבוצעו במערכת או בסביבתה.

(5) תדירות ביצוע סקרים למערכות שיש אליהן גישה מרשת ציבורית לא תפחת מאחת ל-18 חודשים, עבור מערכות שאין אליהן גישה מרשת ציבורית לא תפחת מאחת ל-36 חודשים. ועבור מערכות שאין אליהן גישה מרשת ציבורית ולגביהן נקבע סיכון נמוך בהערכת הסיכונים, לא תפחת מאחת ל-48 חודשים.

(6) על אף האמור לעיל, טרם הטמעת שינוי משמעותי במערכת שהוערכה כבעלת סיכון גבוה, או בסביבתה הטכנולוגית, יבוצע סקר לבחינת תאימותה למדיניות ולנהלי סיכוני סייבר של הגוף המוסדי.

ה) סקרים, מבחני חדירה וסריקת חשיפות אבטחת מידע יבוצעו על ידי גורם מקצועי, עצמאי, חיצוני ובלתי תלוי שאינו מעורב בפיתוח והטמעת מערכות בגוף.

ו) גוף מוסדי יגדיר תכנית לביצוע סקרים אצל ספקי מיקור חוץ המאחסנים או מעבדים נתונים של הגוף המוסדי. רמת הכיסוי של הסקרים תותאם לרגישות המידע ולרמת הסיכון, ותכלול בדיקות שמטרתן לוודא את עמידת הספק בדרישות הגנת סייבר ולזהות חשיפות לסיכונים אלו. סקרים אלו יבוצעו בתדירות המותאמת לרמת הסיכון ולקצב עדכון התהליכים ומערכות הספק, ולכל הפחות אחת ל-36 חודשים. יתאפשר שימוש בסקרים שיזם ספק מיקור החוץ בהינתן והוא עומד בדרישות חוזר זה לביצוע סקרים ובוצע על ידי גורם בלתי תלוי.

2) טיפול בממצאי סקרים ומבחני חדירה

א) גוף מוסדי יגדיר תהליך שוטף לטיפול בחשיפות אבטחת מידע המתגלות במהלך סקרים ומבחנים, וליישום ההמלצות לטיפול בחשיפות אלו.

ב) תמצית ממצאי סקרים ומבחנים תוצג בוועדת ההיגוי.

ג) במקרים בהם חשיפות בסיכון גבוה לא טופלו במהלך שישה חודשים מעת ביצוע הסקר, מנהל הגנת סייבר יציג בוועדת ההיגוי את הסיבות לאי הטיפול בחשיפות אלו, ואת משמעויותיהן להערכת סיכוני סייבר של הגוף.

ג. אבטחת מערכות, תקשורת ותפעול

כדי ליצור שכבות הגנה על מערכות של גוף מוסדי ועל תהליכיו העסקיים, למנוע התממשות סיכונים, לזהות התממשות סיכונים באופן מהיר, לעצור התפשטות התקפות על מערכות גוף מוסדי ולאפשר שחזור מערכות וצמצום הנזק שנגרם כתוצאה מהתממשות סיכונים, גוף מוסדי ישתמש באמצעים להפחתת סיכונים כדלהלן:

1) אבטחת רשת וגישה מרחוק

א) גוף מוסדי ישתמש באמצעי הגנת סייבר המתאימים לסיכוני גישה מרחוק לרשת הגוף, כגון אמצעי סינון תקשורת ותוכן, אמצעי ניטור הגנת סייבר ותהליכי בקרה.

ב) האמצעים יותאמו לסיכונים ייחודיים לשירותי רשת שונים, כגון דואר אלקטרוני, DNS, שירותי העברת קבצים, שירותי Web ועוד.

ג) גוף מוסדי יישם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיסית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרגישות הנתונים המנוהלים במערכות.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ד) גוף מוסדי יגדיר אמצעי אבטחה מיוחדים כגון שימוש בהזדהות חזקה, הצפנה מקצה לקצה וניטור מוגבר בגישה מרחוק לרשת הגוף, על גבי תשתית תקשורת ציבורית או מנקודות קצה שאינן מאובטחות דיין.

ה) גוף מוסדי יישם מנגנונים שינטרו ויצמצמו את הסיכונים הנובעים מחיבור התקן זר או התקן בלתי-מאובטח לרשת הגוף.

2) קישוריות גוף מוסדי לרשת האינטרנט

א) גוף מוסדי יצמצם את רמת הגישה של העובדים לרשת האינטרנט למינימום הנדרש, לצורך הגנה מפני סיכוני סייבר.

ב) קישור מערכות גוף מוסדי לרשת האינטרנט יבוצע תוך יישום אמצעי הפרדה מתאימים, שמטרתם למנוע הפעלה של קוד עוין, הכנסה בלתי מבוקרת של קבצים לרשת גוף מוסדי או יצירה של ערוצים חשאיים אל מחוץ לארגון.

ג) גוף מוסדי יבצע הפרדה מוחלטת של רשתות אלחוטיות מרשת הייצור שלו. לחילופין וככל שלא מדובר ברשת אלחוטית לשירות אורחיו, גוף מוסדי יישם מנגנונים מספקים לאבטחת רשתות אלחוטיות, לרבות הצפנה, הזדהות חזקה, מניעת התקפות על הרשת ומניעה של התחברות גורמים או ציודים בלתי מורשים לרשת האלחוטית.

3) הוצאת נתונים אל מחוץ לחצרותיו

א) גוף מוסדי יקבע את האופן שבו תאושר הוצאת נתונים אל מחוץ לחצרותיו, בהתאם לרמת רגישותם.

ב) גוף מוסדי יגדיר את אופן הגנת הסייבר ההכרחי ליישום בתהליך העברת מידע מחוץ לחצרותיו (כגון: הצפנת נתונים, וידוא הגעת נתונים ליעדם וכדומה) בהתאם לרמת רגישות מידע.

4) הצפנה

א) עבור מידע רגיש, גוף מוסדי יישם הצפנה להגנה על חיסיון בתווך התקשורת מחוץ לחצרותיו, יישם טכניקות הצפנה מוכרות שהוכחו כיעילות ויתקף את האפקטיביות של אלה באופן תקופתי.

ב) גוף מוסדי יגדיר נהלים מתאימים ליצירה, עדכון, חידוש, התקנה וביטול של מפתחות הצפנה ככל שרלוונטי לפעילותו.

5) אבטחת תשתיות ומערכות מידע ועדכונן

א) גוף מוסדי ישמור רשימה עדכנית של תשתיות ומערכות מידע לצורך הגנה מפני סיכוני סייבר, ויגדיר תהליכים לשמירת עדכניות רישום זה.

ב) גוף מוסדי יגדיר תהליכי עדכון מבוקרים למערכות ולתשתיות, תוך התייחסות למקוריות קבצי העדכון, בדיקת עדכונים בטרם יישומם, ושמירה על יציבות מערכות בתהליך העדכון.

ג) גוף מוסדי יתייחס לסיכונים הנובעים מחוסר עדכניות או היעדר תמיכה.

ד) גוף מוסדי יישם עדכוני אבטחת מידע שוטפים למערכות ולתשתיות באופן תקופתי.

ה) גוף מוסדי יעקוב באופן תדיר אחר פרסום עדכוני אבטחת מידע למערכותיו ולתשתיותיו, ויישם עדכונים קריטיים בהקדם האפשרי, בהתייחס לרמת חשיפתם לסיכונים הקשורים לעדכונים אלה.

6) אבטחת מערכות קצה

א) גוף מוסדי יישם אמצעי הגנה על מערכות קצה, תוך התחשבות בסיכוני הפעלת קוד עוין וסיכוני חדירה למערכות, תוך ניצול התקנים המחוברים למערכות קצה.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) גוף מוסדי יישם הצפנת מידע רגיש במערכות קצה ניידות (כגון מידע הנמצא על מחשבים ניידים, טאבלטים, התקני אחסון ניידים וטלפונים ניידים), במטרה למזער את הסיכון לחשיפתם.

ג) גוף מוסדי ישתמש במערכות בקרה, במטרה לצמצם זליגת נתונים רגישים ממערכות קצה או להגביל את היכולת לשמור מידע רגיש על מערכות קצה.

7) מניעת קוד עוין

א) גוף מוסדי יטמיע אמצעי אבטחה, למניעת חדירה והתפשטות קוד עוין במערכותיו, שיכללו מספר שכבות אבטחה כגון: סינון תקשורת וקבצים נכנסים, סריקת מערכות קבצים, הגנה בזמן אמת על שרתים או תחנות קצה, ומערכות ניטור ומניעה ייעודיות.

ב) גוף מוסדי יעדכן בתדירות גבוהה את אמצעי האבטחה האמורים לעיל, ויגדיר תהליכים לווידוא אפקטיביות אמצעי האבטחה כאמור (כגון: קבלת התרעות על כשל בעדכון קבצי חתימות).

ג) בעת חיבור אמצעי מדיה למערכות מידע יעשה שימוש במנגנוני הגנה אפקטיביים המונעים חדירת קוד עוין, כגון שימוש במערכות "הלבנת קבצים".

8) הגנת סייבר בתהליכי רכש ופיתוח

א) גוף מוסדי יגדיר דרישות הגנה מפני סיכוני סייבר בכל תהליך רכש או פיתוח של מערכות חדשות, ובעת שדרוג מהותי של מערכות מידע קיימות.

ב) שילוב ניהול סיכוני הסייבר בתהליכי פיתוח ותחזוקה יכלול לכל הפחות, את השלבים הבאים:

(1) ייזום ואפיון מערכת: הערכת סיכוני סייבר רלוונטיים והגדרת דרישות הגנה מתאימות בעת ייזום ותכנון מערכת.

(2) פיתוח מערכת: מימוש דרישות סיכוני סייבר המופיעות באפיון מערכת.

(3) בדיקת מערכת: בדיקות במהלך פיתוח ומבחני חדירה, תוך יישום היבטי סיכוני סייבר ולרבות ביצוע סקר אבטחת מידע.

(4) קליטת מערכת: קבלה והתקנה מאובטחת ומאושרת של המערכת על ידי גורמים מוסמכים לכך, תוך וידוא יישום דרישות הגנת סיכוני סייבר.

(5) שינויים במערכת: מנהל הגנת סייבר יקבל דיווח טרם ביצוע שינוי במערכות המידע, ויקבע את רמת המעורבות הנדרשת בהתאם לאופי השינוי, לרגישות נתונים ולהשפעה אפשרית של השינוי על סיכונים וחשיפות המערכת.

ג) הגנת סייבר תוטמע בכל רכיבי המערכת, לרבות: תשתיות, אפליקציה (ככל שרלוונטי), וברמת הלוגיקה העסקית המיושמת במערכת.

ד) מבחני חדירה יבוצעו בטרם הטמעת מערכות בגוף המוסדי.

ה) מבחני חדירה יכללו, לכל הפחות, את הנדרש בעת ביצוע סקר אבטחת מידע, בהתאם לסעיפים 5.ב.1)ד)(1) ו-5.ב.1)ד)(2).

ו) כחלק מן התקשרות לפיתוח מערכת מידע על ידי גורם חיצוני, גוף מוסדי יבטיח כי קוד המקור עבר בדיקה נגד חשיפות אבטחת מידע ואי קיום קוד זדוני.

9) הפרדה בין סביבות ואבטחתן

א) סביבת יצור תופרד מסביבות אחרות, כגון פיתוח ובדיקות.

ב) רשת המשתמשים תופרד מסביבות אחרות וכל גישה מהסביבה תאושר על ידי מערכת להגנה על מפני התקשרויות בלתי רצויות.

ג) הרשאות משתמשים לסביבות ייצור תוגדרנה בנפרד מההרשאות לסביבות האחרות.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ד) סביבות פיתוח ובדיקות לא יכילו נתונים אמיתיים, אלא אם רמת הגנת הסייבר המיושמת בסביבות אלו הינה בהתאם לרמת ההגנה המיושמת בסביבת הייצור.

ה) העברת נתונים מסביבת ייצור לסביבה אחרת תתבצע בהתאם להנחיות מנהל הגנת סייבר.

ו) העברת מערכות ונתונים מסביבות פיתוח ובדיקות לסביבת ייצור תיערך בצורה מבוקרת, בהתאם לנהלים, כדי למנוע פגיעה בנתונים בסביבת הייצור.

ד. ניהול משתמשים והרשאות

1) ניהול משתמשים

א) גוף מוסדי יגדיר נהלים המתייחסים לתהליכים שונים במחזור חיים של ניהול חשבונות משתמש במערכות מידע של הגוף, החל מיצירת חשבון משתמש ואופן אישורו, ועד לאופן נעילת החשבון בתום העסקה.

ב) תינתן התייחסות מיוחדת ליצירת חשבונות משתמשים עבור ספקים חיצוניים, עובדי מיקור חוץ, ועובדים זמניים, לרבות הגדרת אופן אישור חשבונות אלה, הגבלת השימוש בהם והמעקב אחר ביטולם בתום תקופת העסקה או בתום הפרויקט.

ג) חשבון משתמש ישויך לעובד מסוים, ותוגדר אחריותו של העובד על חשבון זה ועל הפעולות המבוצעות במערכות גוף מוסדי באמצעות חשבון זה.

ד) ככלל, יעשה שימוש בחשבונות משתמש אישיים. עם זאת, במקרים בהם יש צורך בקיום חשבונות שאינם אישיים, כגון כאלה המיועדים לשימוש על ידי תהליך ממוכן, יוגדרו תהליכים מיוחדים לשמירה על סודיות אמצעי ההזדהות של החשבון, להגבלת השימוש בו ככל הניתן ויוגדר גורם האחראי על החשבון. בנוסף, תוגדר מדיניות ניהול סיסמאות סדירה במשתמשים אפליקטיביים.

ה) גוף מוסדי יגדיר תהליכי סקירה תקופתיים ומתועדים שמטרתם לוודא את הצורך בקיום חשבונות המשתמשים. תהליכי הסקירה לכלל החשבונות, יבוצעו לכל הפחות אחת לשנה.

ו) גוף מוסדי יגדיר את אופן נעילת חשבון משתמש במקרה של אי שימוש בחשבון במשך תקופה ממושכת, ואת תהליך אישור שחרור נעילה זו.

2) סיסמאות ואמצעי הזדהות

א) גוף מוסדי יגדיר אופן הזדהות למערכות מידע, באופן המתאים לרמת רגישות המידע המנוהל במערכת ולסיכונים השונים בתהליך ההזדהות.

ב) גוף מוסדי יגדיר נהלים המתייחסים למסירת אמצעי הזדהות, כגון מסירת אמצעי הזדהות באופן מאובטח למשתמש לאחר זיהויו, שמירה על סודיות הסיסמה והחלפת סיסמה ראשונית על ידי המשתמש.

ג) יש לאמת זהות משתמש כאשר נמסרת לעובד סיסמה ראשונית למערכת. המשתמש יחויב לשנותה בהתחברות הראשונה למערכת. תוקף הסיסמה הראשונית ייקבע למינימום אפשרי, בהתאם לאופי השימוש בחשבון ולא יעלה על 14 ימים.

ד) סיסמאות או אמצעי הזדהות אחרים לא יישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.

ה) גוף מוסדי יקבע את חוזק אמצעי ההזדהות, כגון הצורך בסיסמה חד-פעמית או מורכבות הסיסמה בהתאם להערכת הסיכונים. גוף מוסדי יגדיר אמצעי בקרה על מערך ההזדהות, כגון

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

נעילת חשבון משתמש לאחר ניסיונות גישה כושלים או אי שימוש ממושך בחשבון, החלפה תקופתית של סיסמה ובקרה על מורכבותה.

3) ניהול הרשאות ובקרת גישה

א) גוף מוסדי יגדיר תהליכים מתועדים למתן הרשאות גישה למערכות ושירותים, לרבות: אחריות גורמים עסקיים על אישור הרשאות למערכות עסקיות, התאמת הרשאות לצרכי תפקיד, רמת הסיכון מהרשאות, שינוי הרשאות בעת שינוי תפקיד וביטול הרשאות בעת סיום העסקה.

ב) מתן הרשאות גישה יתבצע על בסיס מינימום הרשאות נדרשות בהתאם ל"צורך לדעת ולבצע".

ג) גוף מוסדי יגדיר תהליכי סקירה תקופתיים, שמטרתם לוודא את הצורך בקיום הרשאות משתמשים. תהליכי הסקירה לכלל ההרשאות, יבוצעו לכל הפחות אחת לשנה.

ד) תהליכי סקירה תקופתיים של חשבונות ספקים חיצוניים, עובדי מיקור חוץ ועובדים זמניים יבוצעו בתדירות גבוהה יותר.

ה. מיקור חוץ (OUTSOURCING)

בהמשך לחוזר מיקור חוץ בגופים מוסדיים 2013-9-16 וכל חוזר אחר שיבוא במקומו, גוף מוסדי יישם את ההוראות הבאות הנוגעות להגנת סייבר בעת השימוש במיקור חוץ:

1) דרישות הגנת סייבר בהסכמי מיקור חוץ

א) גוף מוסדי יגדיר נוהל לדרישות הגנת סייבר ביחס לסיכוני מיקור חוץ וביחס לאבטחת שרשרת האספקה. נוהל זה יישום בעת התקשרות עם גורם מיקור חוץ חדש.

ב) במסגרת הסכם התקשרות עם קבלת שירותי מיקור חוץ:

(1) יאסר על נותן השירות להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.

(2) בעת הצורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים לצורך מתן השירות, ולא שכפול כלל בסיס הנתונים.

(3) תיבחן דרישה לעמידה בתקן ת"י ISO 27001 של מכון התקנים הישראלי.

ג) תחולת סעיף זה לגבי הסכמי התקשרות קיימים תהיה במועד חידושם.

2) שירות למערכות גוף מוסדי על ידי נותן שירות מיקור חוץ

אספקה של שירותי תחזוקה מרחוק (מידע, תוכנה או ציוד תקשורת) על ידי גורמי מיקור חוץ, תתבצע בתנאים הבאים:

א) נותן שירות מיקור חוץ יקבל אישור פוזיטיבי להתחברות, לפני תחילת עבודתו. מנהל הגנת סייבר יקבע מי בעל הסמכות לאשר התחברות מסוג זה.

ב) גישה מרחוק תתאפשר באמצעות משתמש ייעודי לכל נותן שירות מיקור חוץ ובתיאום מראש עם הגוף המוסדי לאופן ההתקשרות ותדירותה.

ג) גישה מרחוק תתאפשר לזמן מוגבל על פי סוג הפעילות אותה יבצע נותן שירות מיקור החוץ.

ד) גוף מוסדי יישם הזדהות חזקה בכל גישה מרחוק של נותן שירות מיקור חוץ.

ה) גוף מוסדי יישם הצפנה מקצה לקצה לכל אורך נתיב ההתקשרות מרחוק.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ו) גוף מוסדי ינטר כל פעילות מהותית שבוצעה בגישה מרחוק.

ז) חשיפת נותן שירות מיקור חוץ למידע אודות לקוחות תצומצם עד למינימום הכרחי, ובמידת האפשר תחסם במלואה.

3) שירותי מחשוב ענן

שימוש בשירותי מחשוב ענן כפוף להנחיות לעניין מיקור חוץ, ולרבות:

א) בטרם הפעלת שימוש במערכות מבוססות ענן, על גוף מוסדי לבצע הערכת סיכונים ייעודית ולדון בנושא סיכונים אפשריים בוועדת ההיגוי.

ב) גוף מוסדי לא יאחסן מידע רגיש או נתוני לקוחות בענן מחוץ לגבולות מדינת ישראל, אלא אם בדק ווידא שספק הענן מקיים את רמת ההגנה בהתאם לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001 ולדירקטיבה על הגנת המידע במדינות האיחוד האירופי.

ג) בשירותי מחשוב ענן מחוץ לגבולות מדינת ישראל, מידע רגיש יוצפן, גם אם התשתית הינה ייעודית.

ד) גישה לנתונים בענן תבוצע דרך כתובות מורשות בלבד.

ה) במקרים בהם נתוני גוף מוסדי מאוחסנים במערכת שאינה לשימושו הבלעדי של גוף מוסדי (Multi-tenant), יעשה שימוש בטכנולוגיות כגון הצפנה, מיסוך נתונים או טוקניזציה, במטרה למנוע חשיפה של מידע רגיש או נתוני לקוחות לגורמים שאינם מורשים.

ו) גוף מוסדי יכלול בהסכם ההתקשרות עם ספק מחשוב הענן, יכולת שליטה ובקרה שלו על הספק וכן אפשרות חד צדדית להפסקת השימוש בשירותי ספק מחשוב הענן תוך מחיקת המידע ממערכותיו והתחייבותו שלא ניתן לאחזר מידע זה במערכותיו.

ו. אבטחה פיסית וסביבתית

1) אזורים מאובטחים

א) בקרות אבטחה פיסיות יתייחסו למכלול הסיכונים הפיסיים והסביבתיים.

ב) גוף מוסדי יחלק את סביבת העבודה לאזורים מאובטחים לפי רמת רגישות המידע אליו ניתן לגשת מאזורים אלו.

ג) גוף מוסדי יישם מעגלים של בקרות גישה פיסית. מעגלים אלו יכללו בקרות מונעות, כגון דלתות נעולות ושערים אלקטרוניים ובקרות מגלות, כגון מצלמות ומערכות אזעקה. רמת הבקרה הנדרשת תותאם לרמת רגישות המידע אליו ניתן לגשת מאזורים אלה.

ד) גוף מוסדי יאפשר גישה לאזורי העבודה בהתאם לצורך, וימנע בהקדם האפשרי את הגישה לאזורים אלה כאשר אין עוד צורך בגישה זו, לרבות בעת שינוי תפקיד או סיום ההעסקה.

ה) על בקרת הגישה באזורים המוגדרים ברגישות גבוהה לכלול לפחות שער כניסה אחד הנפתח על ידי אמצעי זיהוי חזק, כגון אמצעי ביומטרי או כרטיס חכם.

ו) גופים מוסדיים, המעניקים שירותי קבלת קהל במשרדיהם, יפרידו בין האזור בו ניתנים שירותים אלו, לבין אזורי העבודה השוטפים בגוף. לא יתאפשר לגורם, שאינו מורשה, להסתובב במשרדי גוף מוסדי ללא פיקוח.

ז) אזורים ציבוריים המכילים מידע רגיש ימודרו בפני גישה של אנשים שאינם בעלי הרשאה למידע.

2) אבטחת ציוד וניירת

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

א) הוצאת ציוד המכיל מידע רגיש מאחד ממעגלי האזורים המאובטחים תיעשה בהתאם להערכת סיכונים.

ב) ציוד המיועד להשמדה או תחזוקה או הנמסר אל גורם מחוץ לגוף לא יכיל מידע רגיש הניתן לשחזור שאינו מוצפן. בטרם הוצאה של מערכות מחשב מחוץ לגוף לצורך תחזוקה, תבוצע מחיקת נתונים באופן המונע אפשרות שחזור מידע.

ג) גוף מוסדי יבצע השמדה של ציוד רגיש (פיסי או דיגיטלי) שאין בו שימוש ויגדיר את אופן הטיפול והשמירה עד להשמדתם.

ז. הגנת סייבר במשאבי אנוש וגיוס עובדים

1) הגנת סייבר בתהליך גיוס עובדים

א) עבור משרות שיוגדרו כרגישות על ידי מנהל הגנת סייבר (כגון כאלה המאפשרות גישה למידע רגיש או שיש להן הרשאות העלולות לסכן את הגוף המוסדי), יבוצעו בדיקות לבחינת אמינות המועמדים.

ב) חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי סיכוני סייבר, וילווה בהצהרת סודיות.

ג) חוזה של גוף מוסדי עם חברות כוח אדם/השמה או עם חברות המספקות שירותי מיקור חוץ, יכלול התייחסות לסעיפים לעיל.

2) הגנת סייבר בעת מעבר תפקיד או סיום העסקת עובדים

א) לעובדים (לרבות עובדים במיקור חוץ ועובדי קבלן) העוברים תפקיד או מסיימים את העסקתם ייחסמו הרשאות הגישה למידע שאינם צריכים עוד לביצוע תפקידם ובסיום העסקה לא יישארו נכסי מידע של גוף מוסדי בידי העובד.

ב) גוף מוסדי יגדיר בקרות הגנת סייבר נוספות המתייחסות לתקופת הזמן שבין החלטה על מעבר תפקיד או סיום העסקה של עובד ובין ביטול הרשאות הגישה שלו, כגון מעקב מוגבר של מנהל הגנת סייבר אחר בקשות של העובד להרשאות או פעולות חריגות שמבוצעות על ידו.

3) מודעות והדרכה

א) גוף מוסדי יגדיר תכנית להעלאת רמת מודעות של עובדים לסיכוני סייבר (בסעיף זה: "**התכנית**").

ב) התכנית תשולב במערך הדרכה של גוף מוסדי ותכלול התייחסות לאוכלוסיות העובדים השונות, לרבות מיקור חוץ.

ג) התכנית תגדיר הדרכות תקופתיות לעובדים לפי סוג התפקיד ובמהלך התפקיד ותתייחס להדרכה הנדרשת בעת קבלת עובדים או בעת מעבר לתפקיד חדש.

ד) התכנית תפעל להשגת המטרות הבאות:

(1) העלאת רמת הידע לגבי סיכוני סייבר שגוף מוסדי חשוף אליהם והנגזרות מאופי התפקיד.

(2) העלאת המודעות הארגונית נדרשת כדי לזהות ולהגיב לסיכונים הנובעים מאופי תפקיד העובדים, כגון סיכוני "הנדסה חברתית".

(3) הטמעת נהלי הגנת סייבר של גוף מוסדי תוך הדרכת עובדים באשר לנהלים הרלוונטיים להגנת סייבר במסגרת תפקידם.

6 . אבטחת ערוצי קשר עם לקוחות

א. אבטחת ערוצי תקשורת מבוססי אינטרנט

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

1) גוף מוסדי ימפה את ערוצי התקשורת שלו עם לקוחותיו (בסעיף זה לרבות צדדים שלישיים) ויישם מערך בקרות כנגד סיכוני סייבר.
2) מערך הבקרות בערוצי התקשורת מבוססי אינטרנט, יכלול:
א) הצפנת ערוצי התקשורת למניעת האזנה או התערבות.
ב) אמצעי הגנה למזעור סיכונים הנובעים מרמת אבטחה לקויה של ציוד הקצה של לקוחות.
ג) ניטור ייעודי לזיהוי התקפות על ערוצי תקשורת עם לקוחות, כגון: ניסיונות התחזות, התקפות שונות על מנגנוני אימות זהות לקוח (אותנטיקציה), התקפות "הנדסה חברתית", התקפות על מנגנוני שחזור סיסמה וכדומה.
ד) אמצעים מקובלים למניעת התקפות על ערוצים אלה כגון ניחוש שמות משתמשים (user harvesting), ניחוש סיסמאות (Brute force), מניעת שירות באמצעות נעילת חשבונות וכדומה.
3) גוף מוסדי יוודא כי סיכונים שעלולים להיווצר בעת שינויים במערכות מקוונות או בתהליכי הזדהות של לקוחות לשירותים מקוונים, יטופלו באופן מספק, טרם ביצוע השינוי.

ב. רישום מבוטחים/עמיתים לפעילות

1) וידוא זהות בתהליך הרישום

א) גוף מוסדי יוודא זהות לקוח בטרם השלמת רישום לשירותים מקוונים.
ב) וידוא זהות לקוח יעשה באמצעות שימוש בערוץ תקשורת המבוסס על מידע מוקדם שיש לגוף על הלקוח (כגון: משלוח מכתב לכתובת הלקוח שנמסרה לגוף מבעוד מועד, משלוח הודעת SMS למספר טלפון שהלקוח מסר לגוף מבעוד מועד וכדומה).
ג) במקרים בהם לא קיים ערוץ תקשורת המבוסס על מידע מוקדם, ניתן לוודא זהות לקוח באמצעות אוסף פרטי מידע שיש לגוף על הלקוח, ושאינם ידועים לגורם אחר מלבד הלקוח ובלבד שייבחנו סיכונים רלוונטיים (כגון: התחזות) ויישמו מנגנוני אבטחה לצמצומם (כגון: ניטור שמטרתו לזהות ניסיונות התחזות). דוגמאות לפרטי מידע מסוג זה, יכולים להיות: תאריך הנפקת תעודת זהות, פרטים שהלקוח מילא בעבר בשאלון של הגוף המוסדי, פרטים מתוך אמצעי התשלום של הלקוח וכדומה.

2) הסכמה מפורשת של לקוחות בטרם רישום לפעילות

א) רישום לקוח לפעילות בערוצים מקוונים, יחייב קבלת הסכמה מתועדת של הלקוח באמצעות טופס ידני או טופס מקוון או הקלטה או באמצעות חשבונו המקוון של העמית באתר האינטרנט של החברה.
ב) לעמית תינתן הזכות לחזור בו מהסכמתו כאמור.

ג. הזדהות לקוחות לערוצי שירות

1) גוף מוסדי יגדיר את אופן הזדהות הלקוחות לערוצי שירות שונים. אופן ההזדהות יתאים לאופי ערוץ השירות, לרמת הרגישות של המידע, לסוג הפעולות המבוצעות באמצעות הערוץ, ולסיכונים השונים לתהליך ההזדהות, כגון התחזות, הכחשה, האזנה לתווך התקשורת וכדומה. בערוצים מבוססי אינטרנט יעשה שימוש באמצעי הזדהות חזקים או אמצעי הזדהות שאינם קבועים, כגון סיסמאות חד פעמיות הנשלחות בהודעת SMS.
2) גוף מוסדי יגדיר נהלים המתייחסים למסירת אמצעי הזדהות, כגון משלוח סיסמה ראשונית באמצעות דואר לכתובת לקוח, מסרון לנייד הלקוח או באמצעות ערוץ אחר המאפשר מסירת אמצעי ההזדהות ללקוח, וצמצום הסיכון לגניבת או העתקת אמצעי זה בדרך אל הלקוח.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

3) גוף מוסדי יוודא כי לעובדיו אין גישה לאמצעי הזדהות של לקוחות, העלולה לאפשר ניצול לרעה של חשבון לקוח, למעט עובדים מורשים.
4) גוף מוסדי יגדיר נהלים לווידוא חוזק סיסמה, שמירה על סודיותה, החלפת סיסמה ראשונית על ידי המשתמש ותוקף הסיסמה הראשונית.
5) בעת שימוש באמצעי זיהוי קבועים גוף מוסדי יגדיר נהלים המאפשרים ללקוח איפוס סיסמה באמצעים האמורים בסעיף 6.ג.2).

ד. שליחת מידע באמצעים דיגיטליים

1) גוף מוסדי ישלח מידע רגיש ללקוחות באמצעים דיגיטליים, בכפוף לתנאים הבאים:
א) גוף מוסדי יצפין את המידע, כך שיימנע חשיפתו לגורם זר או לשיבושו.
ב) גוף מוסדי יוודא כי ההודעה שנשלחה תקינה ולא התקבל סימן שלא הגיעה ליעדה.
ג) גוף מוסדי ישמור כל מידע תפעולי הנחוץ לצורך בקרה, ניהול ומעקב אחר קיום תנאי שליחת מידע באמצעים אלקטרוניים.
2) גוף מוסדי יספק ללקוחותיו מידע והנחיות שיסייעו להם לנקוט באמצעי זהירות נדרשים לשמירה על פרטיות מידע, וינחה אותם כיצד לנהוג במקרה של חשד לאירוע סייבר.

ה. שיווק מוצרים באמצעים דיגיטליים (ומסחר דיגיטלי)

שיווק מוצרים באמצעים דיגיטליים יתבצע בכפוף לתנאים הבאים:
1) ערוץ תקשורת המשמש את תהליך הרכישה יוצפן באמצעות הצפנה חזקה בהתאם לתקנים המקובלים בשוק, שתבטיח את שלמות המידע וסודיותו, תוך שימוש בתעודת הצפנה (Certificate) חתומה על ידי גוף מוכר ואמין.
2) פרטי אמצעי התשלום של המבוטחים הנשמרים בשרתי החברה, ישמרו בהתאם לתקנים המקובלים בשוק.
3) גוף מוסדי יישם אמצעים למניעת הכחשה, כגון תיעוד בלתי ניתן לעדכון של פרטי ההסכם עם הלקוח, וכן יבקר וינטר את אמצעי המסחר הדיגיטלי במטרה למנוע התחזות ללקוח, הונאה או ניצול לרעה של תהליכי המכירה.

7. אבטחת ערוצי קשר עם גורמים חיצוניים

א. אבטחת ערוצי קשר בין גופים מוסדיים לבין בעלי רישיון

1) לבעלי רישיון שאינם עובדי גוף מוסדי לא תותר גישה ישירה אל מערכות המידע ברשת הפנימית (קישור ישיר ל LAN) של גוף מוסדי, אלא דרך מערכת שער מאובטחת (Secure Gateway), הממוקמת באזור מפורז מחוץ לרשת הפנימית שתיזום את ההתקשרות לרשת הפנימית בשם בעל הרישיון. במקרים בהם בעלי רישיון משתמשים באותה רשת של גוף מוסדי והתקשורת ביניהם אינה עוברת על גבי תווך ציבורי, תותר גישה ישירה אל מערכות המידע ברשת הפנימית.
2) בכל חיבור של בעלי רישיון למערכות תפעוליות של גוף מוסדי, על הגוף להבטיח בקרת גישה מאובטחת. בקרת הגישה תכלול הזדהות חזקה, הצפנת תווך התקשורת מקצה לקצה, חלוקת הרשאות על בסיס "הצורך לדעת ולבצע" ויישום בקרות למניעה ואיתור של אירועים חריגים.
3) לכל עובד במשרדי בעלי הרישיון יהיה זיהוי חד ערכי מול מערכות המידע של הגוף המוסדי.
4) גוף המוסדי יגדיר לכל עובד במשרדי בעלי הרישיון הרשאות גישה למערכות השונות על פי צורך בלבד. הרשאות אלו יותאמו לסוג ולתוקף ההתקשרות עמו.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

5) גוף מוסדי יבחן את הרשאות הגישה הניתנות לכל בעל רישיון מעת לעת, ולכל הפחות אחת לשנה.
6) כל גישה של בעלי רישיון למערכות גוף מוסדי תבוצע על תווך תקשורת מוצפן מקצה לקצה.
7) לא יותר שימוש בתוכנות השתלטות על מחשבי בעלי רישיון באופן העלול לגרום לחשיפת מידע רגיש בין גוף מוסדי למשנהו.
8) גוף מוסדי יגדיר כללים מתועדים בתחום ניהול סיכוני הסייבר אותם יישמו בעלי רישיון. שיתוף פעולה בין גוף מוסדי לבין בעל רישיון יותנה בעמידה בכללים שהוגדרו.
9) תיבחן דרישה מבעלי רישיון לעמוד בתקן ת"י ISO 27001 של מכון התקנים הישראלי.

ב. אבטחת ערוצי קשר בין גופים מוסדיים

בעת יצירת ערוצי העברת מידע בין גופים מוסדיים תיושמנה בקרות הגנת סייבר הכוללות הצפנת תווך התקשורת והנתונים מקצה לקצה, אפשרות מעקב אחר הגעת הנתונים ליעדם והגבלת הגישה לנתונים על בסיס "הצורך לדעת", למעט במקרים בהם גופים מוסדיים משתמשים באותה רשת והתקשורת ביניהם אינה עוברת על גבי תווך ציבורי.

8 . החלת ההוראה

א. תחולה

הוראות חוזר זה יחולו על כל הגופים המוסדיים.

ב. תחילה

1) מועד תחילתו של חוזר זה ב- 2 באפריל 2017.
2) על אף האמור בסעיף קטן 1), מועד תחילתם של סעיפים 5.א.2), 6, ו- 7.א. (ניטור ובקרת מערכות מידע, אבטחת ערוצי קשר עם לקוחות ואבטחת ערוצי קשר בין גופים מוסדיים לבין בעלי רישיון) יהיה ב-1 באוקטובר 2017.

ג. ביטול תקפות

חוזר גופים מוסדיים 2006-9-6, "הוראה לניהול סיכוני אבטחת מידע של הגופים המוסדיים" - בטל.

דורית סלינגר
הממונה על שוק ההון ביטוח וחסכון

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il