## נוהל הערכת וניהול סיכונים

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| זכויות יוצרים “התאחדות לכדורגל” ©  מסמך זה והידע הכלול בו הינם הקניין הבלעדי של “התאחדות לכדורגל” ואינם ניתנים לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה במלואם ו/או בחלקם, במישרין, ו/או בעקיפין, ללא הסכמה מראש ובכתב של “התאחדות לכדורגל”.   * מסמך זה מותר לשימוש פנימי בלבד. * כל האמור בנוהל זה בלשון זכר או להיפך נעשה מטעמי נוחות ויש לראותו כאילו נאמר גם בלשון נקבה או להיפך. * בדוק שהנך עושה שימוש בגרסה האחרונה של המסמך! * בכל מקרה בו נדרש לערוך שינויים בנוהל זה, יש לפנות אל אחראי הנהלים ב”התאחדות לכדורגל”   נתונים כללים   |  |  | | --- | --- | | ערך: בוריס קוגן | | | בדק: | | | אישר: | | | סוג המסמך: מדיניות ונהלים | | | תאריך פרסום המסמך: 01.02.2019 | תאריך תיקוף המסמך: | | סטאטוס המסמך: סופי | |   טבלת שינויים   |  |  |  |  |  | | --- | --- | --- | --- | --- | | תאריך שינוי | מהות השינוי | סעיפי השינוי | גרסה | גורם מאשר | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |

1. רקע:
   1. פעילות אבטחת המידע ב”התאחדות לכדורגל” (להלן "המשרד" ו\או "הארגון") נעשית במטרה לוודא שמירה על סודיות המידע, אמינותו וזמינותו, מפני פגיעה במתכוון על-ידי עובדים פנימיים או על-ידי גורמים חיצוניים (כגון יועצים, מבקרים, ספקים ונותני שירותים אחרים, וכו').
   2. הבסיס לפעילות אבטחת המידע הינו תהליך של ניהול סיכונים ברמה כלל ארגונית (כולל התייחסות לטכנולוגיות המידע, אבטחה פיזית וסביבתית, תהליכי עבודה קריטיים בארגון, אנשים, ונכסי מידע).
   3. פעילות זו תתבסס על קריטריונים מתועדים באמצעותם יחולקו הנכסים\מערכות המידע לנכסים\מערכות בשלל רמות סיכון (גבוהה, בינונית ונמוכה).
   4. מסמך זה מתאר את מדיניות הארגון בנושא ניהול והערכת סיכונים בתחום אבטחת המידע.
2. מטרות:
   1. להבטיח מודעות לסיכונים ואיומים אפשריים על הנכסים בארגון ומערכי המחשוב.
   2. להעריך אותם בצורה נאותה ולנהל אותם לאורך זמן.
3. אחראי לביצוע\בקרה הנוהל:
   1. בקרה - מנהל אבטחת מידע והסייבר.
   2. ביצוע – כל הארגון.
4. מסמכים ישימים:
   1. מדיניות אבטחת המידע של הארגון.
   2. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
5. הגדרות ומונחים:
   1. "ניהול סיכונים" – תהליך הזיהוי, הבקרה והמזעור או סילוק של סיכוני אבטחה העלולים להשפיע על נכסים (ראה הגדרה בסעיף 5.3 לנוהל זה) הנעשה בעלות קבילה ומאושרת ע"י הנהלת הארגון. במסגרת ניהול הסיכונים מתבצע סקר סיכונים, שמטרתו לאתר את הסיכונים לארגון ולהעריך את חומרתם, זאת על מנת לאפשר קבלת החלטה מבוססת באיזה סיכונים לטפל, ובאיזה סדר עדיפות, עלות ולוח זמנים.
   2. "*הערכת סיכונים*" – הערכת פגיעותם של הנכסים, הערכת איומים והשפעות עליהם ועל הארגון, תוך התייחסות והערכת הייתכנות התממשותם.
   3. "*נכס (Asset)*" – כל דבר בעל ערך רב לארגון, כגון כח אדם, מידע, ציוד, מתקנים, תוכנה, פעילות שוטפת, הליך עסקי, מוניטין וכו'. ככל שלנכס ערך רב יותר לארגון, כך הנזק יהיה גדול יותר בעת הפגיעה בנכס.
   4. "*פגיעות (Vulnerability)*" – פגיעות היא חולשה בנכסים או באמצעי ההגנה של הארגון \ שהיריב יכול לנצלה על מנת לגרום נזק לארגון ו\או לנכס. אמצעי הגנה מתאימים מפחיתים את הפגיעות.
   5. "*איום (Threat)*" – איום מזוהה עם יריב, שיש לו גם כוונות וגם יכולות לבצע פעולה שתפגע בנכס\בארגון. מלבד הכוונות והיכולות, גם פעילות היריב בעבר נלקחת בחשבון בעת הערכת האיום. מקובל להניח שהאיום מוכתב ע"י היריב, למרות שמידת הנזק האפשרית, הפגיעויות, הנכסים ואמצעי ההגנה שיינקטו, יכולים להשפיע על כוונות היריב לפעול.
   6. "*אמצעי הגנה (Controls/Safeguards)*" – פעולות או אמצעים שמפחיתים את הסיכון על ידי השפעתם על הנכסים (ובכך הנזק האפשרי), הפגיעויות והאיומים.
   7. "*סיכון (Risk)*" – סיכון מאירוע כלשהו מורכב מגודל הנזק שייגרם לארגון בקרות האירוע, ומהסבירות שהאירוע יתרחש. הסבירות מושפעת על ידי רמת האיום ורמת הפגיעות. ישנם מודלים בהם נותנים ערכים מספריים לרמת הנזק, רמת האיום ואמת הפגיעות בכל אירוע אליו מתייחסים. הסיכון מחושב עפ"י
   8. סודיות המידע" (Confidentiality): הבטחת נגישותו של מידע רק לגורמים מורשים.
   9. "שלמות המידע" (Integrity): שמירת הדיוק והשלמות של מידע ושל שיטות עיבוד המידע.
   10. "זמינות המידע" (Availability): הבטחה שמשתמשים מורשים יוכלו לגשת למידע ולמשאבי המחשוב לפי הצורך.
   11. "*סיכון שיורי" ( Residual Risk)*" – מהי רמת הסיכון שנותרה לאחר יישום אמצעי הבקרה.
   12. "רמת סבילות לסיכון" (Acceptable Level of Risk) - מהי רמת הסיכון (הסיכון השיורי) שהנהלת הארגון מקבלת, מאשרת, ומוכנה לחיות איתו מבלי לנקוט באמצעים נוספים למזער או להעביר אותו לצד ג'
6. גוף הנוהל:
   1. כללי
      1. הערכת הסיכונים הינה שלב מקדים והכרחי בעיצוב מדיניות אבטחת המידע בארגון.
      2. תוצאות ההערכה יסייעו לקבוע מהן פעולות הניהול שראוי לנקוט, איך לקבוע קדימויות לניהול סיכוני אבטחת המידע, ואיך ליישם את אמצעי הבקרה שנבחרו, כדי להתגונן מפני הסיכונים.
   2. תפקידים ואחריות
      1. הנהלת הארגון:
         1. מתן אישור וגיבוי (תקציבי, כח-אדם, פוליטי) לטיפול בממצאי הסקר.
         2. קביעה ואישר רמת הסיכון הקבילה בארגון (Acceptable Level).
      2. מנהל אגף מערכות מידע:
         1. עדכון מדיניות ניהול והערכת הסיכונים.
         2. עדכון מתודולוגיה לניהול והערכת הסיכונים.
         3. אחראי על פיקוח ביצוע תהליך סדיר של ניהול סיכונים.
      3. מנהל תחום אבטחת מידע:
         1. אחראי על יישום תהליך של הערכת סיכונים מחזורי בארגון.
         2. אחראי על תוכנית לטיפול בממצאי הסקר ויישומה.
      4. מנהלי המערכת \ בעלי הנכס:
         1. אחראי על קביעת רמת הסיווג של המערכות\נכסים.
         2. אחראי על קביעת רמת הקריטיות של המערכות\נכסים.
         3. אחראי על קביעת רמת האבטחה של המערכות\נכסים (כולל הרשאות).
   3. הגדרת מטרות ויעדים
      1. כללי:
         1. מטרתו של תהליך הערכת הסיכונים הינו לאתר ולהציג את סוגי ורמת הסיכונים שבו מצויים הנכסים הנמצאים בארגון.
         2. אחד מיעדי תהליך הערכת הסיכונים יהיה מיפוי כלל הנכסים בארגון וסיווגם עפ"י רמות הסיכון.
         3. כמו כן, יעד מרכזי נוסף יהיה לעמוד בביצוע הסקרים ומבדקי החוסן (ראה סעיף 6.6 לנוהל זה) בהתאם לרמות הסיכון של המערכות.
      2. יעדים ומדידה:
         1. כל סיכון יימדד בשני פרמטרים:
            1. מידת הנזק: תום מתן ציון בין1 – 5 .

1 = לא מהותית

2 = נמוכה

3 = בינונית

4 = גבוהה

5 = קריטית

* + - * 1. הסתברות ההתרחשות. תוך מתן ציון בין 1-5.

1 = נדיר

2 = לא סביר

3 = אפשרי

4 = צפוי

5 = בוודאות גבוהה

* + - 1. מכפלת שני הפרמטרים תגדיר את מידת הסיכון (בין 1-25)
         1. סיכון לא מהותי: בין 1-3
         2. סיכון נמוך: 3
         3. סיכון בינוני: בין 4-8
         4. סיכון גבוה: בין 9-16
         5. קריטי: בין 25 - 20
      2. כיעד, הארגון יטפל בסיכון ברמת סיכון גבוהה בתוך חודש מיום איתור הסיכון. היעד הכמותי הינו:
         1. טיפול ב-100% מהסיכונים ברמת סיכון קריטית בתוך שבועיים מיום איתורם.
         2. טיפול ב-80% מהסיכונים ברמת סיכון גבוהה בתוך חודש מיום איתורם.
         3. טיפול ב-20% מהסיכונים הנותרים ברמת סיכון גבוהה בתוך חודשיים מיום איתורם.
         4. טיפול ב-80% מהסיכונים ברמת סיכון בינונית תוך שלושה חודשים מיום איתורם.
         5. טיפול ב-20% מהסיכונים הנותרים ברמת סיכון בינונית בתוך שישה חודשים מיום איתורם.
         6. טיפול ב-80% מהסיכונים ברמת סיכון נמוכה תוך 12 חודשים מיום איתורם.
         7. טיפול ב-20% מהסיכונים הנותרים תוך 18 חודשים מיום איתורם.
      3. יעד זה יימדד וייבחן בכל ישיבת וועדת היגוי לאבטחת מידע.
  1. תהליך ניהול סיכונים
     1. כללי
        1. ניהול סיכונים בארגון הוא תהליך רציף, ואינו מיועד להציג את הסיכונים לארגון רק בנקודת זמן אחת.
        2. על הארגון לבחון בכל עת את השינויים בנכסים, באיומים ובפגיעויות על אותם נכסים, וכן בסביבה בה מתקיים הארגון. כשמזהים שינויים, יש להעריך מחדש את הסיכונים ולבחון את התאמת אמצעי הבקרה.
        3. במידת הצורך, יש להמליץ על יישום אמצעי בקרה חדשים ועל ביטול או שינוי אמצעי הבקרה הישנים.
     2. תהליך ניהול הסיכונים
        1. מנהל תחום אבטחת המידע בארגון ינהל ויתחזק את טבלת ניהול הסיכונים. בטבלה יתועדו הסיכונים העקרוניים בתחום אבטחת המידע, הנובעים מכלל התהליכים בארגון, מכלל מערכות המידע בארגון ומכלל המחלקות בארגון.
        2. מנהלי יחידות הסמך יבצעו תהליך של הערכת סיכונים בסיסית בנוגע לנכסים (מערכות, מידע, ותהליכים) שבאחריותם. תהליך זה יוגדר במסגרת וועדת ההיגוי לאבטחת מידע.
        3. מנהל תחום אבטחת המידע בארגון יוודא כי בכל יחידות הסמך מנוהלות טבלאות סיכונים עדכניות, וכי לכל הסיכונים אופיין פתרון אשר אושר ע"י הנהלת הארגון.
        4. לכל סיכון יוגדרו הפרמטרים הבאים:
           1. המשאבים הנחוצים לטיפול בסיכון (מערכות, כח אדם, וכו')
           2. מי האחראי לטיפול בסיכון.
           3. מהו לוח הזמנים לטיפול בסיכון.
           4. מהות התקציב הנחוץ.
           5. מהו הסיכון השיורי.
           6. מה חומרת הסיכון השיורי.
           7. שמו של מאשר הסיכון (נציגת הנהלת הארגון)
     3. מתודולוגיה
        1. תהליך ניהול והערכת הסיכונים בארגון יתבצע בהתאם למתודולוגיה של NIST SP800-30 כפי שמפורט בנספח א' לנוהל זה.
        2. יש להנחות את הגורמים החיצוניים אשר מבצעים סקרי סיכונים עבור הארגון לעבוד עפ"י מתודולוגיה זו (לפחות מבחינת הצגת הממצאים - ראה סעיף 6.3.6 בנוהל זה).
     4. הגישה להערכת סיכונים
        1. יש לזהות את הסיכונים באופן שוטף באמצעות התהליכים והאירועים המתוארים בסעיף מספר 6.4.4.3 לנוהל זה.
        2. כל הסיכונים יתועדו בטבלת ניהול סיכונים אשר תתוחזק ע"י מנהל תחום אבטחת המידע

בארגון.

* + - 1. שיטת הערכת הסיכונים בארגון מתבצעת באופן שוטף ע"י יישום נוהל זה, ובאמצעות:
         1. ביצוע סקרי סיכונים ומבדקי חוסן על המערכות בהתאם לטבלת מיפוי המערכות אשר מנוהלת ע"י מנהל תחום אבטחת המידע בארגון.
         2. ביקורות המנא"מ השוטפות בארגון.
         3. ניתוח אירועי אבטחת המידע שקרו בארגון.
         4. בדיקה שוטפת של הלוגים של המערכות וניתוחם (מגמות תקיפה).
         5. מבדקים פנימיים.
         6. סקרי תהליכים.
         7. דיווחים של עובדים על אירועים ו\או פגיעויות.
         8. אירועים הקורים בעולם ומתפרסמים בתקשורת.
         9. אירועי סייבר והתרעות על איומים שמתקבלים משירותי מודיעין סייבר
         10. תלונות של גורמי חוץ (כגון אזרחים, לקוחות, שותפים עסקיים)
      2. ההנהלה רואה בשיטת הערכת הסיכונים ותיקון הליקויים הנובעים מהסקרים והביקורות חלק בלתי נפרד מתהליך השיפור המתמיד על מערכת ניהול אבטחת המידע (מנא"מ) של הארגון.
      3. הערכת הסיכונים תתבצע ע"י גוף בלתי תלוי (חברת צד ג') אשר אין לה ניגוד אינטרסים עם הארגון.
    1. שיטות לביצוע הערכת סיכונים
       1. כללי
          1. מנהל תחום אבטחת המידע יקבע תוכנית שנתית לביצוע הסקרים, בהתחשב ברמות הסיכון של הנכסים הקיימים בארגון.
          2. תוכנית ביצוע הסקרים תתבסס גם על ממצאי סקרים קודמים ותוכנית הטיפול בליקויים.
          3. תוכנית ביצוע הסקרים תתחשב גם במערכות חדשות שאמורות להיות מותקנות בארגון.
          4. סקרי הסיכונים ייעשו ע"י גורם חיצוני, מנוסה ובלתי תלוי בארגון.
          5. הטיפול בממצאי סקר הסיכונים יבוצע במסגרת תוכנית העבודה השנתית באמצעות הפניית משאבים נאותים להטמעת אמצעי אבטחת מידע כנדרש.
          6. במידה ויימצאו ממצאים חמורים שהינם בעלי השלכה עסקית\תפעולית משמעותית עבור הארגון, יובאו הממצאים לידיעת חברי וועדת ההיגוי לאבטחת מידע עוד לפני שגובשה תוכנית העבודה בנושא, במטרה לקבל החלטות בנושא.
       2. ביצוע סקרי סיכונים
          1. סקר סיכונים הינו תהליך של סקירת המערכות, בעלי התפקידים, התהליכים והמתקנים הפיזיים הקיימים בארגון, על מנת לאשר את הסיכונים הקיימים בהם.
          2. מטרת סקר הסיכונים היא לקבל תמונה ברורה של רמת הסיכון הקשורה לכל אחד ואחד מנכסי המידע, התהליכים והמחלקות, ולקבוע את הפתרון הנדרש על מנת למזער את הסיכון ולהביאו לרמה המקובלת על ההנהלה (רמת סבילות הסיכון).
          3. סקרי תהליכים יבוצעו באופן שוטף ע"י מנהל תחום אבטחת המידע בארגון או מי מטעמו, בהתאם לתוכנית העבודה השנתית בתחום אבטחת המידע.
          4. מתודולוגיית לביצוע סקרי סיכונים מכילה מספר מרכיבים עיקריים:

סקר סיכונים כלל ארגוני (כולל אבטחה פיזית, ובקרות ניהוליות).

סקר מערכת.

סקר תהליכים.

מבדקי חוסן (Penetration Testing).

* + - * 1. לאחר ביצוע שינויים מהותיים במערכות המידע, יבוצע מבדק קבלה בהיבטי אבטחת מידע לפי העלאת המערכת המשודרגת לאוויר. המבדק יתבצע בשיטה של מבדק חוסן ויינתן דגש על המודול בו בוצע השינוי (מערכת הפעלה, תקשורת, אפליקציה, מודול הזדהות, וכו').
        2. לפני העלאת מערכת חדשה לאוויר, יבצע הארגון מבדק קבלה בהיבטי אבטחת מידע. המבדק יתבצע בשיטה של הערכת סיכונים ויכיל תשאול אודות מבנה המערכת, צורך ההטמעה בארגון, צורת מתן וניהול הרשאות הגישה וכו'.
        3. לגוף המבקר יוגדר מועד קבוע לביצוע סקר חוזר לבדיקת יישום תיקון הליקויים.
        4. על הגוף המבוקר להעביר תכנית לתיקון הליקויים לצורך אישור.
        5. חריגה מהגדרות המסגרת המופיעות בנוהל זה מחייבות אישור וועדת ההיגוי לאבטחת מידע.
      1. שיטות לביצוע הערכת סיכונים
         1. סקר סיכונים כלל ארגוני

בסקר זה ייבדקו כל הנכסים בארגון בהיבטים של איומים ופגיעויות ברמת אבטחה פיזית וסביבתית, ברמה הטכנולוגית וברמה הניהולית.

במסגרת סקר סיכונים כלל ארגוני, ייבדקו כלל הנכסים בארגון, כולל תהליכי עסקיים ו\או תהליכים תפעוליים קריטיים.

כמו כן, יילקחו בחשבון דרישות חוק, רגולציה ותקנות רלוונטיות.

* + - * 1. סקר מערכת

בסקר זה תיבדק רמת אבטחת המידע במערכת מידע ספציפית, מבחינת היבטי תשתיות, אפליקציה, אבטחה פיסית, סביבת המערכת והעמידה בדרישות חוקים ותקנות רלוונטיים.

* + - * 1. סקר תהליכי

במסגרת ביצוע סקר תהליכים, ימופו כל התהליכים בארגון. מתוכם, יסווגו כל התהליכים אשר קריטיים (הן מבחינת רגישות המידע והן מבחינת המזינות) ועליהם יבוצע תהליך של הערכת סיכונים.

* + - * 1. מבדק חוסן

מבדקי חוסן ידמו ניסיונות פריצה למערכות הארגון (מבחוץ ומתוך הרשת) בהתאם להמלצותיו של מנהל תחום אבטחת המידע בארגון ובהתאם לתוצאות סקר הערכת הסיכונים.

מבדקי החוסן יתבצעו ע"י גורם חיצוני, מנוסה ובלתי תלוי בארגון.

הטיפול בממצאי מבדקי החוסן יטופלו במסגרת תוכנית העבודה השנתית באמצעות הפניית משאבים נאותים להטמעת אמצעי אבטחת מידע כנדרש.

במידה ויימצאו ממצאים חמורים שהינם בעלי השלכה עסקית\תפעולית משמעותית עבור הארגון, יובאו הממצאים לידיעת חברי וועדת ההיגוי לאבטח מידע עוד לפני שגובשה תוכנית העבודה בנושא במטרה לקבל החלטות בנושא.

את מבדקי החוסן ניתן לבצע בשלוש שיטות עיקריות: בשיטת קופסא שחורה (Black Box), בשיטה של קופסא לבנה (White Box) ובשיטה משולבת (Gray Box).

מבדק Black Box: מטרת המבדק בשיטה זו היא לדמות את הסביבה הטבעית של התוקף (ההאקר). הספק המבצע את הבדיקה, אינו יודע רב אודות הארגון, מלבד מה שניתן למצוא באינטרנט. המטרה היא לבחון היטב את מוכנות הארגון (כולל בחינת הבקרות הקיימות וגם את רמת התגובה של צוות אבטחת המידע הקיים בארגון).

מבדק White Box: מטרת מבדק זה היא לדמות סביבה שבה לתוקף יש מידע פנימי (כגון במקרה של עובד פנימי או יועץ הנותן שירותים לארגון, ומכיר את המערכות). בדיקה זו יכולה לחסוך זמן מבחינת ממצאי הבדיקה ולהעלות מהר יותר על ממצאי אבטחה חמורים, מה שיכול להקטין את תקופת תיקון הליקויים.

מבדק Gray Box: מבדק זה משלב בין שתי השיטות הקודמות במטרה לייעל את תהליך המבדק מבחינת זמן ומשאבים נדרשים.

* + 1. זיהוי והערכה של חלופות לטיפול בסיכונים
       1. כללי:
          1. הערכת הסיכונים הינה שלב מקדים והכרחי בעיצוב מדיניות אבטחת המידע בארגון.
          2. תוצאות ההערכה יסייעו לקבוע מהן פעולות הניהול שראוי לנקוט, איך לקבוע קדימויות לניהול סיכוני אבטחת המידע, ואיך ליישם את אמצעי הבקרה שנבחרו, כדי להתגונן מפני הסיכונים.
          3. ייתכן שאת תהליך ההערכה ובחירת אמצעי הבקרה צריך יהיה לבצע כמה פעמים, כדי לטפל בחלקים שונים של הארגון או במערכות מידע שונות.
          4. חשוב לסקור את סיכוני האבטחה באופן סדיר וליישם אמצעי בקרה, כדי להבטיח:

שהובאו בחשבון שינויים בדרישות העסקיות\תפעוליות של הארגון ובקדימויות שלו.

שהובאו בחשבון איומים חדשים ופגיעויות חדשות.

שהובטח שאמצעי הבקרה לא יאבדו את האפקטיביות ואת הנאותות שלהם.

* + - 1. הטיפול בסיכונים:
         1. בהתאם לממצאי סקר הסיכונים יוסקו מסקנות והגורמים המקצועיים הרלוונטיים יפעלו לשיפורים נדרשים.
         2. יש להביא לאישור ממונה אבטחת המידע בארגון ובפני וועדת ההיגוי לאבטחת מידע כל סיכון שלא טופל בזמן הנקוב לעיל או סיכון שיוחלט לקבל ולא לטפל בו במודע ובאופן אובייקטיבי.
         3. הטיפול בסיכון יהיה על ידי צוות מקצועי של הארגון. לחלופין ניתן להעביר את האחריות לטיפולה של חברה חיצונית כגון לחברת ביטוח וספקי נותני שירות.
         4. אחת לשנה תוצג במסגרת סקר הנהלה טבלת ניהול הסיכונים להנהלת הארגון לצורך אישור הסיכונים והסיכונים השיוריים.
    1. הצגת הממצאים
       1. הצגת ממצאי הסקר ו\או מבדקי החוסן תתבצע בהתאם למפורט בנספח ב' לנוהל זה.
       2. יש לוודא מול הספקים המבצעים את הבדיקות (סקר סיכונים ו\או מבקי חוסן) סנכרון והתאמה אל מול מבנה הדו"ח.
    2. דיווח להנהלה
       1. מנהל תחום אבטחת המידע יציג בפני וועדת ההיגוי לאבטחת מידע את הממצאים העיקריים של סקרי הסיכונים ומבדקי החוסן וההמלצות כפי שגובשו ושולבו בתוכנית טיפול בסיכונים (Risk Treatment Plan).
       2. תיעוד הסקר יכלול את שמות הנכסים\מערכות, את רמות הסיכון של כל נכס\מערכת, את הגורמים להימצאותם של הנכסים\מערכות ברמת סיכון זו ואת ההמלצות לשיפור אמצעי ההגנה להורדת רמת הסיכון לרמה נמוכה יותר (סיכון שיורי), שאותה הנהלת הארגון מוכנה לקבל (רמת סבילות הסיכון).
       3. הטיפול בממצאי סקרי הסיכונים ומבדקי החוסן יבוצע במסגרת תוכנית העבודה השנתית באמצעות הפניית משאבים נאותים להטמעת אמצעי אבטחת מידע כנדרש.
       4. הנהלת הארגון תקיים דיון בנושא ממצאי הסקר (אפשרי במסגרת וועדת ההיגוי לאבטחת מידע ו\או מחשוב), ותחליט לגבי יישום ההמלצות המופיעות בו בהתאם לתיעדוף ורמת החומרה של הסיכונים.
       5. מנהל תחום אבטחת המידע יגדיר תוכנית עבודה שנתית בתחום אבטחת המידע, בהתאם להערכת הסיכונים וכנדרש במדיניות האבטחה של הארגון, בה יצוינו תחומי הפעילות הנדרשים (קבועים ומזדמנים) ולצידם המשאבים הנדרשים.
       6. מנהל תחום אבטחת המידע יביא כל שנה את תוכנית העבודה לאישור וועדת ההיגוי לאבטחת מידע (כולל התייחסות לסטאטוס פרויקטים, עדכונים בתוכנית, בדרישות וכו').
  1. סיווג מערכות לצורך הערכת סיכונים
     1. כללי:
        1. מנהל תחום אבטחת המידע יבצע תהליך של הערכת סיכונים, בתדירות שתקבע הנהלת הארגון, כפי שנדרש בסעיף 6.7 לנוהל זה.
        2. תוצאות הסקר יכללו הצגה של כלל הנכסים הקריטיים בארגון עפ"י רמות הסיכון הפוטנציאלי.
     2. סיווג רמת הסיכון של הנכסים\מערכות בארגון:
        1. כלל הנכסים\מערכות בארגון יסווגו לרמות סיכון כפועל יוצא מסיווג המערכות לפי המידע האגור בהן, ורמת הקריטיות של אותן מערכות (עפ"י ייעודן וחשיבותן התפעולית בארגון).
        2. רמת הסיווג של המערכת תיקבע עפ"י:
           1. רמת רגישות\סודיות המידע הקיים במערכת.

בלמ"ס.

חסוי.

חסוי ביותר.

* + - 1. רמת הקריטיות של המערכת תיקבע עפ"י:
         1. רמת הזמינות שנדרש מהמערכת

גבוהה.

בינונית.

נמוכה.

* + - * 1. רמת השלמות\אמינות שנדרשת מהמערכת.

גבוהה.

בינונית.

נמוכה.

* + 1. שיטות לסיווג רמת הסיכון של הנכסים\מערכות בארגון:
       1. רמות הסיכון יהיו כדלהלן:
          1. סיכון גבוה - יסווגו המערכות שכוללות מידע רגיש, ורמת הקריטיות שלהן גבוהה
          2. סיכון בינוני - יסווגו המערכות שכוללות מידע בלמ"ס, אך רמת הקריטיות שלהן היא בינונית.
          3. סיכון נמוך - יסווגו המערכות שכוללות מידע בלמ"ס, ורמת הקריטיות שלהן היא נמוכה.
       2. המערכות הבאות יסווגו ברמת סיכון גבוהה ללא קשר לתוצאות סקר הערכת הסיכונים:
          1. מערכות המכילות מידע רגיש (חסוי או חסוי ביותר)
          2. מערכות האינטרנט המשמשות את לקוחות הארגון.
          3. מערכות הפתוחות בתקשורת ציבורית.
          4. מערכות אשר מאפשרות אליהן גישה מרחוק.
  1. ניטור וסקירה
     1. אחריות פיקוח:
        1. הנהלת הארגון אחראית על אישור רמות הסיכון, כולל רמת הסבילות של הסיכון (להלן הסיכון השיורי). תהליך אישור זה יתבצע במסגרת סקר הנהלה שיתקיים לפחות אחת לשנה.
     2. אחריות ביצוע:
        1. מנהל תחום אבטחת המידע ו\או מנהל אבטחת המידע (תשתיות) ינהל תיעוד מסודר של קטגוריות ורמות הסיכון בהן נמצאות המערכות בארגון.
        2. כמו כן, מנהל תחום אבטחת המידע יקיים ויתחזק מערך של תיעוד ממצאי סקרי הסיכונים ומבדקי החוסן לצרכי מעקב.
        3. מנהל תחום אבטחת המידע יבקר אחת לשנה את תוכנית העבודה אל מול ממצאי הסקרים האחרונים שבוצעו, לצורך התאמה ואי-חריגות. כל חריגה תדווח להנהלת הארגון.
  2. תדירות לביצוע סקרי סיכונים
     1. התדירות לביצוע סקרי סיכונים תיקבע עפ"י רמת הסיכון של המערכות.
        1. עבור מערכות בסיכון גבוה - אחת לשנה.
        2. עבור מערכות בסיכון בינוני - אחת ל-18 חודש.
        3. עבור מערכות בסיכון נמוך - אחת ל-3 שנים.

הערות: כל מערכת אשר מותקנת בתהיל"ה מחויבת לעבור מבדק חוסן לפני אישור העלייה לאוויר.

1. אכיפה

6.1 כל עובד שימצא כי הפר את מדיניות זו עשוי להיענש על ידי הגורם הרלוונטי ב”התאחדות לכדורגל”, המחלקה או “התאחדות לכדורגל” עצמו.

1. תחולה
   1. המדיניות חלה על כלל עובדי “התאחדות לכדורגל” (ספקים, עובדי קבלן, יועצים, זמניים) ועובדים אחרים המחזיקים או מתחזקים מידע כלשהו של “התאחדות לכדורגל”.
   2. נוהל זה נכנס לתוקפו מיום פרסומו.
   3. מכניסתו לתוקף, נוהל זה מחליף כל נוהל קודם בעניין.

נספח א': - מתודולוגיה לניהול סיכונים עפ"י NIST SP800-30

* 1. כללי
     1. הערכת הסיכונים של הנכסים הינה שלב מקדים מתהליך ממשל אבטחת המידע בארגון, הכולל בין היתר עיצוב מדיניות אבטחת המידע ושיפור רמת האבטחה בארגון.
     2. דרישות האבטחה מזוהות באמצעות הערכה מתודולוגית של סיכוני אבטחה. ההוצאות הכספיות על אמצעי האבטחה צריכות להיקבע עפ"י מידת הנזק העלולה להיגרם לארגון (ו\או לפעילותיו השונות) ממקרי כשל אבטחה.
     3. אפשר ליישם טכניקות של הערכת סיכונים לכל הארגון, או רק לחלקים ממנו, ואפילו למערכות מידע מסוימות בלבד, לרכיבים ספציפיים במערכת או לשירותים או תהליכי עבודה ספציפיים, לפי מידת התועלת ולפי הצורך.
     4. הערכת הסיכונים היא שקלול שיטתי של:
        1. הנזק העלול להיגרם לארגון כתוצאה מכשל אבטחה, בהתחשב בהוצאות אפשריות של אובדן חיסיון, שלמות או זמינות של המידע ושל נכסים קריטיים אחרים.
        2. ההיתכנות הממשית של התרחשות כשל זה, לאור האיומים והפגיעויות הקיימים בארגון (או על הנכסים), ועל סמך אמצעי הבקרה המיושמים באופן שוטף.
  2. שלב 1: מיפוי וסיווג נכסים בארגון (System Characterization)
     1. מיפוי נכסים: בשלב זה על הארגון למפות את כלל הנכסים בארגון (כול נכסים מוחשיים כגון שרת, מחשבים אישיים, מחשבים ניידים, טלפונים חכמים, אל-פסק וכו' וגם נכסים שאינם מוחשיים כגון תהליכי עבודה, מידע, פטנטים, מוניטין וכו').
        1. על הארגון לנהל מצאי (מתוחזק ומעודכן) על כל הנכסים בארגון.
        2. לכל נכס, חייב להיות מוגדר בעל הנכס (אחראי על הנכס).
     2. סיווג הנכסים: לאחר שזוהו כל הנכסים בארגון, יש צורך לסווג את הנכסים עפ"י רמת הרגישות של הנכס (עפ"י רגישות המידע הנמצא בו), וכמו כן גם רמת הקריטיות של הנכס מבחינת זמינות, עבור הארגון.
        1. סיווג המידע יתבצע בהתאם לרמות הסיווג המודרגות בארגון.
        2. רמת הקריטיות של הנכס תוגדר עפ"י סולם של 1-3 כדלהלן:
           1. 1 = רמת קריטיות גבוהה
           2. 2 = רמת קריטיות בינונית
           3. 3 = רמת קריטיות נמוכה
  3. שלב 2: זיהוי האיומים (Threat Identification)
     1. בהתאם לסוגי הנכסים, יוגדרו סוגי האיומים הקיימים והידועים.
     2. ניתן להיעזר במקורות חיצוניים כגון חברות ייעוץ, חברות מחקר, חברות המספקות שירותי מודיעין סייבר, וכו'.
  4. שלב 3: זיהוי הפגיעויות (Vulnerability Identification)
     1. עבור כל נכס, יוגדרו מהן הפגיעויות שקיימות על אותו נכס.
     2. ניתן למזער בממצאים של סקרי סיכונים קודמים, של מבדקים פנימיים וביקורות אבטחה קודמות (פנימיות ו\או חיצוניות).
  5. שלב 4: ניתוח בקרות קיימות (Control Analysis)
     1. בשלב זה ינותחו הבקרות הקיימות מבחינת רמת ההגנה שהן מספקות על הנכסים, לאור הפגיעויות והאיומים שאותרו.
     2. כמו כן, ינותחו הבקרות שמתוכננות להירכש בעתיד כדי לבחון את היכולת שלהם לספק מענה הולם לפגיעויות והאיומים שאותרו.
     3. רמת נאותות הבקרות הקיימות והמתוכננות יוגדרו בין 1-3:
        1. 1 = רמה טובה
        2. 2 = רמה בינונית
        3. 3 = רמה נמוכה
  6. שלב 5: הגדרת רמת סבירות להתרחשות האיום (Likelihood Determination)
     1. אחד הפרמטרים החשובים בחישוב רמת הסיכון, הינה הסבירות למימוש האיום.
     2. הפרמטרים שצריכים לקחת אותם בחשבון הינם:
        1. כמות וסוג האיומים שקיימים על הנכס
        2. המוטיבציה של התוקף (מניעים)
        3. היכולות המקצועיות של התקוף (כולל אמצעים טכנולוגיים)
        4. כמות וסוגי האיומים הקיימים על הנכס
        5. כמות הפגיעויות הקיימות על הנכס
        6. הבקרות הקיימות ורמת חוזקן
     3. רמת הסבירות תוגדר בין 1-5 כדלהלן:
        1. 1 = נדיר
        2. 2 = לא סביר
        3. 3 = אפשרי
        4. 4 = צפוי
        5. 5 = בוודאות גבוהה
  7. שלב 6: ניתוח השלכות (Impact Analysis)
     1. בעת ניתוח מידת ההשפעה של מימוש האיום על הנכס, יש להתייחס לפרמטרים הבאים:
        1. רמת הקריטיות של הנכס
        2. רמת הרגישות של המידע
        3. רמת הקריטיות של המידע
        4. דרישות או מגבלות רגולציה, חוק, חוזיות
     2. התוצר של שלב זה, הינו הגדרת מידת ההשפעה של מימוש האיום על הנכס.
     3. פרמטר זה יוגדר בסולם בין 1-5 כדלהלן:
        1. 1 = לא מהותית
        2. 2 = נמוכה
        3. 3 = בינונית
        4. 4 = גבוהה
        5. 5 = קריטית
  8. שלב 7: קביעת רמת הסיכון (Risk Determination)
     1. רמת הסיכון תיקבע עפ"י מכפלת חומרת מידת ההשפעה של מימוש האיום על הנכס (תוצר של שלב 6) ורמת הסבירות של מימוש האיום (תוצר שלב 5) אל מול רמת האבטחה של הבקרות הקיימות (תוצר שלב 4).
  9. שלב 8: המלצת בקרות (Control Recommendations)
     1. בהמשך לביצוע הערכת הסיכונים, נדרשת המלצה באשר לאמצעי ההגנה שיפחיתו את רמות הסיכון, למינימום האפשרי (סיכון שיורי). בבחינת מידת היעילות של אמצעי הגנה שונים אל מול מיתר האיומים והפגיעויות השונות והיריבים השונים, ובחישוב הסיכון השיורי, ניתן לבדוק מהי הדרך היעילה להפחתת הסיכון, והאם הסיכון השיורי הוא כזה שהנהלת הארגון מקבלת (רמת סבילות הסיכון).
     2. התוצר בשלב הזה הינו המלצה של יישום אמצעי בקרה חדשים.
     3. הבקרות יכולות להיות:
        1. בקרות אדמיניסטרטיביות כגון: נהלים, הנחיות, פעילות להגברת המודעות
        2. בקרות לוגיות (טכנולוגיות) כגון: IPS, DLP, NAC, פירוול, אנטי-וירוס
        3. בקרות פיזיות כגון: מנעולים, כספות, תגי זיהוי, ביומטרי, חיישני תנועה.
  10. שלב 9: תיעוד ודיווח (Results Documentation)
      1. לאחר ביצוע תהליך של הערכה וניהול סיכונים, התוצר הסופי יהיה דו"ח סופי מתומצת עבור הנהלת הארגון, ודו"ח מפורט יותר עבור צוות אבטחת המידע שאמור לטפל בממצאים.
      2. יוצג בפני הנהלת הארגון (ו\או וועדת ההיגוי לאבטחת מידע) עיקרי הדו"ח (ממצאי הסקר), הכוללים תוכנית לטיפול בממצאים (במטרה להוריד את רמות הסיכון לרמת סבילות) הכוללת מספר חלופות.
      3. בכל חלופה תוצג העלות (מחיר המשאבים הנחוצים ליישומה, ומידת פגיעתה בתפקוד הארגון) והסיכון השיורי הנובע מיישומה.

נספח ב': - מבנה ופורמט הצגת ממצאי סקרי סיכונים ומבדקי חוסן

תוצר הסקר יהיה מסמך אשר יכיל את הרכיבים הבאים:

* תמצית מנהלים – התמצית תכלול הסבר על תהליך הסקר וכן את עיקרי הממצאים וההמלצות (עם דירוג רמת החומרה עפ"י רמות הסיכון).
* פירוט הרכיבים\נכסים\מערכות שנבדקו במהלך הסקר\מבדק חוסן
* פירוט מתודולוגית הבדיקה
* תיאור מפורט של הממצאים בפורמט טבלאי. התיאור יכיל את המידע הבא עבור על אחת מהחשיפות שנמצאו:
* תיאור כללי של החשיפה
* תיאור מפורט של החשיפה
* ניתוח חומרת החשיפה בהיבט הנזק שעלול להיגרם ורמת ההסתברות למימושו
* המלצות ראשוניות ליישום
* מידע נוסף הקשור לחשיפה (באם רלוונטי)
* הממצאים ידורגו באחת משלושת רמות החומרה הבאות:
* גבוהה – רמת החשיפה מהווה סיכון לנכסים\לארגון בהיבט של פגיעה בשלמות, סודיות או זמינות המידע. משמעות ממצא זה כי יש לנקוט צעדים בעדיפות גבוהה לתיקון הממצא.
* בינונית – רמת החשיפה מהווה סיכון לנכסים\לארגון בהיבט של פגיעה בסודיות, בשלמות או בזמינות המידע. עם זאת קיימים פרמטרים המצמצמים את החשיפה לאיום כגון הסתברות נמוכה למימושו או רמת פגיעה נמוכה בעת התממשות האיום. בכל מקרה יש לנקוט צעדים לתיקון הממצא.
* נמוכה – אין סכנה מידית וממשית לנכסים\לארגון מחשיפות אלו. על מנת לממש חדירה לארגון או לגרום נזק לנכסים יש להשקיע משאבים גדולים מאוד, וההסתברות לכך נמוכה, כנ"ל רמת הפגיעה. יש לשקול טיפול אבטחתי בטווח הארוך בחשיפות אלו וכמו כן להיות מודעים אליהן במידה ומתבצעים שינויים במערכות שנבדקו.