## נוהל פיתוח מאובטח

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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: 01.25.2019 | תאריך תיקוף המסמך: | | סטאטוס המסמך: סופי | |   טבלת שינויים   |  |  |  |  |  | | --- | --- | --- | --- | --- | | תאריך שינוי | מהות השינוי | סעיפי השינוי | גרסה | גורם מאשר | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |

1. רקע:
   1. “התאחדות לכדורגל” (להלן "הארגון") מפעיל מספר מערכות מידע, אשר מכילות בין היתר מידע רגיש.
   2. תקשורת לא מאובטחת או מאושרת עלולות לגרום לנזקים חמורים לארגון, כגון: חשיפת מידע רגיש, העברת מידע לגורמים לא מורשים, שינוי לא מורשה של מידע, האטה של הפעילות ברשת ו\או של המחשב הנגוע, מחיקת מידע לא מורשית והשבתה מוחלטת של מערכות המחשוב ב”התאחדות לכדורגל” (להלן "הארגון").
   3. קיימת חשיבות ראשונה במעלה למנוע פגיעה במערך המחשוב בכלל וע"י מערוכת ההגנה בפרט.
   4. לצורך עבודה שוטפת, יש צורך בהגדרת עקרונות מנחים לניהול ועדכון מערכות פיירוול ומערכות תקשורת
2. מטרה:
   1. בארגון עובדים על הכנת הארגון לעמידה בהגנת הפרטיות . מסמך המגדיר מה הם הדרישות שאותם מפתחי האפליקציה חייבים למלא ע"מ לעמוד בתקנות
   2. הגדרת דרישות האבטחה עבור כל פיתוח של תוכנת או אפליקציות מבוססות WEB אשק משדרות, מעבדות או מאחסנות נתונים רגישים
3. אחראי לביצוע\בקרה הנוהל:
   1. בקרה - מנהל אבטחת מידע והסייבר.
   2. ביצוע - נחל על כלל העובדים, הקבלני משנה, היועצים והעובדים החיצוניים אשר עובדים בארגון. נוהל זה חל על כל הרשתות והמידע בהן נשמרים או מעובדים נתוני רגישים בארגון.
4. מסמכים ישימים:
   1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
5. גוף הנוהל:
   1. כל פיתוח תוכנה חייב להיעשות בסביבת פיתוח נפרדת מסביבת הייצור. אין לפתח או לשנות תוכנה בסביבת הייצור ללא תהליך מוסדר המוגדר בנוהל ''בקרת שינויים".
   2. חל איסור על שימוש בנתוני סביבת הייצור ללא ביצוע סניטציה וזיהוי ומחיקה של מידע רגיש.
   3. לפני ביצוע העברת מערכת לסביבת הייצור יש לוודא כי כל נתוני הבדיקה (הכוללים: ת.ז , מספרי כרטיסי אשראי, נתונים רגישים וכו') ימחקו טרם הפעלת המערכת. יש לדאוג שבמערכת אין משתמשים מקומיים וסיסמאות מקומיות שמורות.
   4. יש לוודא כי קיימת הפרדת תפקידים בין צוותי הפיתוח לבין צוותי הייצור.
   5. יש לוודא כי התבצע סקר קוד על ידי גורם בלתי תלוי לאפליקציות או פיתוחים לפני העברתם לסביבת היצור.
   6. ניהול תהליכים של גילוי וסגירת פרצות, הגדרת רמת סיכון לכל פרצה, ופיתוח והתקנה של Patch לכל פרצה שמתגלה.
   7. התחברות וניהול של האפליקציה חייבים להיות מאובטחים, בהתאם לדרישות הבאות:
      1. מנגנון של שמירת Logging על פעולות המערכת.
      2. גישה אפליקטיבית למערכת חייבת להיות מוצפנת.
      3. גישה מופרדת לניהול המערכת, מוצפנת ועם הזדהות.
      4. פיתוח ע"פ Software Development Lifecycle.
   8. לאחר סיום הפיתוח והעברה לייצור, כל יכולות הטסט וה-Debug אמורות להיות מבוטלות. יש לדאוג שבמערכת אין משתמשים מקומיים וסיסמאות מקומיות שמורות.
   9. ביצוע של תהליך מעבר על הקוד לפני הבנייה הסופית בצורה אוטומטית או ידנית בכדי לזהות פרצות אבטחה או סיכונים. הבדיקה חייבת להיות מבוצעת ע"י מישהו שלא פיתח את אותו הקטע קוד. הקוד חייב להיות מתוקן ומאושר ע"י מנהל לפני העברה לייצור.
   10. חייב להיות מבוצע תהליך מאורגן של ניהול שינויים, כל שינוי שצריך להיות מבוצע צריך לעמוד בדרישות הבאות (לאחר העברה לייצור):
       1. צריכה להיות הפרדת תפקידים בין אלה המפתחים ואלה שמפעילים את סביבת הייצור.
       2. אין להשתמש במידע אמת בסביבת הפיתוח/בדיקות, למשל מספרי אשראי אמתיים.
       3. כל המידע האפליקטיבי מסביבת הפיתוח חייב להימחק לפני העברה לייצור.
       4. יש לתעד כל תהליך של Patch שנובע מתיקונים לליקויים אבטחתיים. תיעוד זה חייב להכיל את המידע הבא:
       5. רמת ההשפעה של הסיכון שהתגלה.
       6. אישור ניהולי לביצוע השינוי.
       7. בדיקות לאחר ביצוע השינוי לווידוא שלא נוצרות בעיות חדשות.
       8. תכנית של חזרה לאחור.
   11. סביבת הפיתוח והבדיקות חייבת להיות מופרדת לחלוטין מסביבת הייצור. אין לפתח על סביבת הייצור, בנוסף יש לוודא שאין אפשרות לגשת למידע בסביבת הייצור מסביבת הפיתוח.
   12. יש לוודא כי הפיתוח יעמוד בהתאם לדרישות המקובלות בתעשייה, אשר כוללות את ההנחיות כפי שמופיעות באתרים הבאים : <http://owasp.org> , <http://csrc.nist.gov/> . הכוללות מניעה משימוש בקוד אשר מאפשר :
       1. הזרקות חיצוניות של קוד (למשל SQL Injection).
       2. Buffer Overflows, יש לוודא שיש בקוד תהליך שבודק גבולות של ה-Buffer.
       3. שמירה לא מאובטחת של מפתחות קריפטוגרפים, או שימוש באלגוריתמים לא מאובטחים, או גודל מפתח קטן.
       4. מעבר של מידע לא מוצפן ברשת.
       5. ניהול שגוי של שגיאות, אסור ששגיאות יחשפו שום מידע פנימי.
       6. Cross Site Scripting (XSS).
       7. גישה למקומות רגישים ללא בדיקות זהות או מיקום (למשל גישה לממשק ניהול מהאינטרנט).
       8. חשיפה של מידע פנימי ע"י אפשור של Directory Traversal.
       9. Cross-site request forgery (CSRF).
       10. ניהול מאובטח של Session.
           1. הגדרה של Cookies כ-secure.
           2. אין לחשוף מידע כמו Session-ID ב-URL.
           3. הגדרה של Time-out ושינוי ה-Session-ID לאחר זיהוי מחדש.
   13. יש לתעד את התהליך של לימוד המפתחים על פיתוח מאובטח, צריכה להיות רשומה לכל מפתח מתי הוא למד על כך.
   14. יש לדאוג שכל מפתח יכיר את ההנחיות המפורטות להלן ויבין את חשיבותן.
6. אכיפה
   1. כל עובד שימצא כי הפר את מדיניות זו עשוי להיענש על ידי הגורם הרלוונטי ב”התאחדות לכדורגל”, המחלקה או “התאחדות לכדורגל” עצמו.
7. 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.