דרישות אבטחת מידע

מערכת OTP

גרסה 2.7

מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
1.0	28.4.2015	אלעד פז	גרסא ראשונה
2.0	11.5.2017	יוגב מזרחי	עדכון ותיקוף מסמך
2.1	16.5.2017	אודי ברוך	עדכון סעיף 2.2.3 והסרת סעיף 2.5.6
2.2	10.5.2018	אופיר יהב	תיקוף המסמך. עדכון שמות מאשרי המסמך.
2.3	5.5.2019	אופיר יהב	תיקוף המסמך.
2.4	30.4.2020	אופיר יהב	תיקוף המסמך. עדכון שמות מאשרי המסמך.
2.5	10.11.2021	אופיר יהב	תיקוף המסמך. עדכון שמות מאשרי המסמך. עדכון הלוגו עם המעבר למשרד הדיגיטל הלאומי.
2.6	7.11.2021	אופיר יהב	תיקוף המסמך. עדכון הלוגו עם הקמת מערך הדיגיטל הלאומי.
2.7	7.11.2022	אופיר יהב	תיקוף ועדכון המסמך. עדכון הלוגו לאחר השינוי הארגוני.

נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	ראש תחום מתודולוגיות הגנה בסייבר	אופיר יהב	7.11.2022	(חתימה)
נבדקה ע"י	ראש תחום אבטחת אפליקציות	אברהם ברדה	7.11.2022	(חתימה)
אושרה ע"י	מנהל מערך ההגנה בסייבר	חגי פרלמוטר	7.11.2022	(חתימה)

תוכן עניינים

1. כללי.....4
2. דרישות אבט"מ למערכת OTP 5
2.1 משתמשים 5
2.2 סיסמאות 6
2.3 תהליך זיהוי.....6
2.4 לוגים.....6
2.5 ריבוי בקשות.....6
2.6 כללי 7
2.7 חריגות 7

1. כללי

- אתרים/שירותים המעוניינים לספק מידע אישי/מותאם למשתמש נדרשים ליישם תהליך הזדהות למשתמשים. אחת הדרכים לזיהוי משתמש היא באמצעות סיסמא חד-פעמית התקפה לזמן מוגבל אותה מקליד המשתמש בעת הגישה לאתר בנוסף לשם משתמש ו/או שדה זיהוי אחר.את הסיסמא מקבל המשתמש באמצעות דואר אלקטרוני, SMS, IVR, Token Generator – הסיסמא תתקבל בממשק/נתיב שונה מהנתיב בו ניגש המשתמש לאתר/שירות.
- הטמעת מנגנון של סיסמא חד-פעמית דורש יישום של התהליכים הבאים:
  1. תהליכי ניהול מאגר משתמשים (רישום, מחיקה, עדכון)
  2. תהליך ניהול סיסמא חד-פעמית (יצירה, שמירה עד מועד פקיעת תוקף, זיהוי-Authentication).
  3. תהליך רישום מפורט (לוגים).
- תהליכי ניהול המשתמשים וניהול הסיסמאות הינם תהליכים נפרדים.
- **חשוב לציין כי שימוש ב- OTP הינו תהליך מיישם הזדהות חזקה כתוספת להזדהות ולא כתחליף (2 factor authentication)**
- מסמך זה מיועד עבור עובדי מערך הדיגיטל הלאומי ולקוחותיו והוא יעודכן על ידי ראש תחום מתודולוגיות הגנה בסייבר במערך הדיגיטל הלאומי.

2. דרישות אבט"מ למערכת OTP

2.1 משתמשים

2.1.1. שם המשתמש יהיה ייחודי בכל המערכת לכל אורך חיי המערכת (גם לגבי חשבונות שנמחקו).

2.1.2. יש להימנע משימוש במספרי תעודת זהות/דרכון.

2.1.3. יתבצע תהליך רישום מקדים (ידני \ אוטומטי) שבו המשתמש יזין פרטים של נתיב קבלת סיסמא חד-פעמית (מספר טלפון נייד, כתובת דואר אלקטרוני וכו'). יתבצע אימות ראשוני של המידע שהוזן באמצעות שליחת הודעת אימות בנתיב שהוזן (הודעת דואר, מסרון וכו'). רק מידע שעבר אימות ישמר כחלק מחשבון המשתמש.

2.1.4. תוקף פרטי הזיהוי של משתמש יהיה 6 חודשים מתאריך שימוש אחרון בנתיב שליחת הסיסמא. לאחר תקופה זו יש לבצע אימות מחדש של נתיב השליחה כפי שפורט לעיל.

2.1.5. תינתן אפשרות למחיקת\שינוי משתמש על ידי בעלי החשבון. התהליך דורש אימות באמצעות אחד מנתיבי השליחה המשויכים לחשבון.

2.1.6. תהליך ה- OTP לא יאפשר למבקש הגישה להזין את נתיב קבלת הסיסמה (כלומר הסיסמה תשלח על סמך הפרטים השמורים במערכת) ניתן להחליף שדה זה אחת ל-X זמן שייקבע בהתאם לרגישות המערכת.

2.2 סיסמאות

2.2.1. אורך הסיסמא יהיה לפחות 8 תווים.

2.2.2. הסיסמא תורכב מאותיות באנגלית ומספרים. לא נדרש יישום Upper/Lower Case על האותיות.

2.2.3. תוקף הסיסמא המקסימלי יהיה זמן סביר אשר ייקבע מראש ולא יעלה על 24 שעות. לאחר מכן על המשתמש לבקש סיסמא חדשה.

2.2.4. סיסמאות שהונפקו ישמרו בזיכרון השרת בלבד עד למועד פקיעת תוקפן או כניסה מוצלחת של המשתמש.

2.2.5. יש ליישם מנגנון יצירת סיסמאות המבוסס על מנוע TRNG (True Random Number Generator).

2.2.6. על הפתרון לעמוד במדיניות סיסמאות של מערך הדיגיטל הלאומי.

2.3 תהליך זיהוי

2.3.1. בקשת משתמש לסיסמא תעבור בתווך מוצפן (SSL).

2.3.2. תשובה לבקשת הסיסמא תשלח באמצעות אחד הנתיבים שהוזנו על ידי המשתמש בעת רישום לשירות.

2.4 לוגים

2.4.1. כלל הפעולות במערכת ירשמו בלוגים מפורטים (הן ניסיונות תקינים והן כושלים).

2.4.2. הלוגים לא יכילו נתונים אישיים למעט שם משתמש.

2.5 ריבוי בקשות

2.5.1. על הפתרון ליישם מנגנון למניעת ריבוי בקשות אשר יאושר על ידי מערך הגנה בסייבר של מערך הדיגיטל הלאומי.

2.5.2. מנגנון ריבוי הבקשות יטפל הן בשלב הקלדת הסיסמה והן בשלב שליחת המסר (SMS, דוא"ל וכו').

2.6 כללי

2.6.1. הפתרון יוכפף להנחיות רמו"ט בנושא מאגרי מידע.

2.6.2. הפתרון יאושר מול מערך הגנה בסייבר של מערך הדיגיטל הלאומי

2.6.3. על הפתרון לעמוד במדיניות ונהלי אבטחת מידע במערך הדיגיטל הלאומי.

2.6.4. על הפתרון לעבור מבדק חדירות וסקר קוד.

2.7 חריגות

2.7.1. היות ומסמך דרישות זה הינו כללי, ייתכנו מערכות שעל בסיס רגישות המידע בהן ו\או עקב אילוצים עסקיים, חלק מהסעיפים לא מתאימים. כל חריגה תוגש למערך הגנה בסייבר במערך הדיגיטל הלאומי לבחינה