מדינת ישראל
משרד החינוך
המינהל למדע וטכנולוגיה

בדיקות חוסן אפליקטיבי לספקים באמצעות חוות הדעת

(תאריך עדכון: 20.09.2015 ; גרסה 1.6)

1. במסגרת חוות הדעת ניתן שירות לספקים בתחום החינוך המאפשר ביצוע בדיקת חוסן אפליקטיבית. ניתן לבצע בדיקה מקבילה לפי המפרט המפורט בנספח, ובכפוף להנחיות במסמך זה.
2. עלות השירות היא 320 ₪ לא כולל מע"מ.
3. השירות ניתן לספקים המתארחים בחוות הדעת בלבד.
4. ספקים שאינם מתארחים בחוות הדעת יכולים לבצע בדיקה מקבילה בכפוף לאמור במסמך זה ובנספח "דרישות לבדיקת חוסן בתצורת BlackBox", וזאת לאחר קבלת אישור המשרד.
5. השירות כולל:
   5.1. בדיקה אפליקטיבית של יישום אינטרנטי אחד בלבד.
   5.2. במקרה שלספק קיימים כמה יישומים – יש לבצע בדיקה נפרדת לכל יישום.
   5.3. בסיום הבדיקה יופק דוח ליקויים/אישור לתקינות המוצר מבחינת חוסן אפליקטיבי.
   5.4. פירוט השירות כמפורט במכרז חוות הדעת, עמוד 48, סעיף 2.3.11:

2.3.11 <u>שירותי בדיקות אבטחה ליישומים מתארחים</u>

2.3.11.1 הספק יבצע בדיקות אבטחה בתצורה של BlackBox לכלל היישומים ה-Web-יים המותקנים על גבי השרתים בחווה.

2.3.11.2 עבור יישומי המשרד יינתן שירות זה לפני העברת גרסה של היישום לסביבת הייצור. באחריות המשרד תיקון היישום בהתאם לממצאים ולתיאום מועד התקנת היישום.

2.3.11.3 עבור יישומי הלקוחות הנוספים יינתן שירות זה לפני ההתקנה בסביבת הייצור. הלקוחות הנוספים יהיו אחראים לתיקון היישום בהתאם לממצאים ולתיאום מועד התקנת היישום.

2.3.11.4 פעם בשנה תבוצע בדיקה מקיפה לכלל יישומי ה-Web המותקנים בסביבת הייצור של המשרד ושל הלקוחות הנוספים.

2.3.11.5 הספק יעביר למשרד וללקוחות הנוספים דו"ח המפרט את תוצאות הבדיקה מיד לאחר ביצועה.

2.3.11.6 הספק יתאר את הפתרון המוצע (S)

קישור למכרז: http://retro.edu.gov.il/michrazim/documents/3021.doc

6. יש לבצע בדיקה עם שמות משתמשים וסיסמאות וכניסה המדמה משתמש אמיתי, בכל סוגי התפקידים לרבות תלמיד, מורה ומנהל.
7. על הספק לתקן את הליקויים כמפורט בדוח, ולהגיש את המוצר לבדיקות חוזרות ככל שיידרש עד לקבלת אישור תקין. כל בדיקה חוזרת תחויב בעלות נוספת כמפורט בסעיף 2.

8. דוח הבדיקה המופק בתהליך זה הוא דוח המקובל כבדיקת חוסן במסגרת בדיקת אבטחת מידע של ספקים כמפורט בקישור:

http://sites.education.gov.il/cloud/home/meyda_le_sapakim/Pages/lobi_meyda_les apakim.aspx

למעט למערכות מהסוג הבא שנדרשת להן בדיקה רחבה יותר כמפורט בתקן אבטחת מידע:

8.1. מערכות המתממשקות למערכת מנב"ס/נט.

8.2. מערכות המחזיקות מידע רפואי או מידע רגיש מהסוגים הבאים: תוצאות מבחנים/מבדקים וכדומה בנושאי חינוך מיוחד, קשב, זיכרון ועוד.

9. אנשי קשר: בזק בינלאומי, אלעד הלפרין 050-4014250 EladA@bezeqint.co.il

10. משרד החינוך יעדכן מסמך זה מעת לעת.

מדינת ישראל
משרד החינוך
המינהל למדע וטכנולוגיה

נספח - דרישות לבדיקת חוסן בתצורת BlackBox

1. להלן מפרט לבדיקת חוסן בתצורת BlackBox לביצוע הבדיקה תבצע באמצעות כלי בדיקה אוטומטיים.
2. הבדיקה תכלול בדיקת:

2.1. חוזק מנגנוני ההזדהות אל מול התקפות התחזות, גניבת זהות, גניבת SESSION, ועקיפתם באמצעים שונים כגון: SQL\FILE Injections.

2.2. חוזק מנגנוני המידור וההרשאות אל מול התקפות של גישה בלתי מורשית למידע. (ניהול\הגבלה של משתמשים וסיסמאות)

2.3. בדיקת רמת זליגת מידע מהמערכת באמצעים השונים.

2.4. בדיקות לחשיפה של מידע רגיש פנימי או גישה ישירה לקבצים פנימיים.

2.5. התקפות DOS ברמת השרת\רשת\אפליקציה למניעת שירות ממשתמשי המערכת.

2.6. מניפולציה של בקשות POST\GET.

2.7. בדיקת התמודדות המערכת עם ניסיונות בדיקת מנגנוני ההגנה של המערכת על ממשקי ניהול התכנים וההגדרות.

2.8. בחינת השימוש באמצעים קריפטוגרפים על מנת להגן על נתונים רגישים ובכלל זה על תווך התקשורת- הצפנה וכו'.

2.9. העברת נתונים רגישים בתווך לא מוצפן.

2.10. בדיקת התמודדות המערכת עם תקיפות ידועות כגון: HTTP TUNN, SQL Injections, XML,LDAP,FILE, Session Hijacking, Cookie Poisoning ועוד.

2.11. לאיתור חולשות בעמודי HTML, CGI, ASP, FrontPage Extensions