10/02/2021

מסמך אבטחת מידע - TRIBU

V1.2

מטרה	**2**
כללי	**2**
מאגר מידע	**2**
פיתוח קוד מאובטח	**3**
טיפול במידע רגיש	**4**
הזדהות וסיסמאות	**5**
Session Management	**6**
שרתים ותקשורת	**7**
תיעוד logging ואזהרות	**8**
טיפול באירועי סייבר	**8**
תקנים	**9**
אירועי סייבר קודמים	**10**

מטרה

מטרת המסמך לאגד את כל נושאי אבטחת המידע של חברת Tribu ומוצריה בהתאם לביקורות ובדיקות חיצוניות שנעשו במהלך שנה קלנדרית נוכחית.

כללי

חברת Tribu מחוייבת על שמירת הפרטיות של לקוחותיה בהתאם לתקנות הגנת הפרטיות של משרד המשפטים הישראלי - תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
(https://www.nevo.co.il/law_html/law01/501_600.htm)
בהתאם לכך החברה עוברת מדי שנה ביקורת אבטחת מידע ובדיקת חדירות למערכת על מנת לוודא עמידה בתקנות.
טריביו עובדת עם משרד החינוך ומוכרת כספק רשמי של המשרד, מה שמחייב אותנו לעמוד במגבלות אבטחת מידע ושמירת פרטיות ברמה הגבוהה ביותר.

מאגר מידע

חברת Tribu מחזיקה מאגר מידע הרשום כחוק במשרד המשפטים.
המאגר מסווג ברמת אבטחה גבוהה.
כתב מינוי מאגר מידע

פיתוח קוד מאובטח

נושא	הסבר	תאימות	הערות
נוהל פיתוח מאובטח	על הארגון להדריך את המפתחים בתהליכי פיתוח מאובטח הרלוונטים לטכנולוגיות בהם נעשה שימוש. יש לתעד הנחיות אלו במסמך	✔	נוהל פיתוח מאובטח
בדיקות קלט (input validation): יש לוודא שהתוכנה בודקת כל נתון המגיע מהמשתמש, בטפסים, cookies, query strings, HTTP headers	כל משתנה המכיל מידע המגיע מהמשתמש חייב להיבדק כדי לוודא שאינו מכיל קוד זדוני, שיכול לגרום לנזק למידע במערכת או למחשב אשר מריץ את התוכנה או גולש לאתר. פונקציות הבדיקה צריכות להתייחס לבדיקות כגון סוג הקלט, encoding, סימנים מיוחדים ומילות מפתח	✔	
בדיקות קלט (input validation): יש לתעד ולהזהיר במקרה של קלט לא חוקי	כאשר המערכת מזהה קלט כלא חוקי- יש להזהיר את המשתמש ובמקביל לרשום את הנתונים בקובץ לוג ו/או טבלה שתאפשר לבצע תיחקור של המשתמש. יש לבצע את הבדיקה בכל הדפים	✔	מעקב על קלט לא חוקי מתבצע רק על login ונשמר בלוג כל הפעולות במערכת מוגנות במערכת הרשאות
קיים מידור הרשאות גישה לטבלאות בבסיס הנתונים לפי סוגי המשתמשים במערכת	משתמש אפליקטיבי צריך לקבל גישה לאובייקטים (טבלאות, פונקציות וכו') הנחוצים בלבד ולא לכלל האובייקטים בבסיס הנתונים. אין להשתמש בהרשאות משתמש admin/root/sa לאפליקציה	✔	מטריצת הרשאות ארגונים אינם נחשפים למידע מארגונים אחרים, כל ארגון הוא סביבה נפרדת.
הצפנה	שימוש במנגנוני הצפנה מוכרים ולא כאלה שנכתבו עצמאית	✔	מצ"ב
שימוש ב-TLS 1.1/1.2 בלבד	יש למנוע שימוש במקודדים פרט ל- TLS 1.3/1.2. יש לבצע בדיקות בסביבת TEST לפני העברה לייצור.	✔	

טיפול במידע רגיש

נושא	הסבר	תאימות	הערות
זיהוי וטיפול בנתונים רגישים: סיסמאות, פרטי התחברות לשרת ולבסיס נתונים, נתוני משתמשים אישיים, גישה למשאבים מחוץ למערכת	פרטי התחברות לשרת ולבסיס הנתונים חייבים להיות מוצפנים ע"י מנגנון יעודי או כחלק ממערכת ההפעלה. מידע אישי ורגיש, חייב להיות מוצפן בבסיס הנתונים	✔	מצ"ב
אין לאגור נתונים סודיים לא חיוניים לתפקוד המערכת (כמו כרטיסי אשראי, מידע רפואי)	אין לשמור במערכת מידע עודף, כלומר מידע אשר אינו חיוני לשירותים שהמערכת מספקת.	✔	
במידה ונעשה שימוש באמצעות המערכת לגבייה או סליקת תשלומים, יש לעשות זאת באמצעות שירות העומד בתקן PCI ובהתאם לדרישות הרשות להגנת הפרטיות	יש להשתמש במערכת סליקה חיצונית העומדת בתקן PCI ובדרישות הרשות להגנת הפרטיות. אין לשמור את פרטי הגבייה באתר.	✔	לא רלוונטי

הזדהות וסיסמאות

נושא	הסבר	תאימות	הערות
הזנת שם משתמש וסיסמה אישית	המערכת לא חושפת סיסמאות במסך	✔	
הזנת שם משתמש וסיסמה אישית	לא מתבצעת השלמה אוטומטית של פרטי ההזדהות	✔	
אורך סיסמה	אורך מינימלי של סיסמא - 7 תווים	✔	8 תווים
מורכבות סיסמא	סיסמא תורכב מאותיות וספרות	✔	contain 8-15 characters including uppercase and lowercase letters, a number and a special character. Special characters: @!%$&#
מנגנון "שכחתי סיסמא"	קישור לאיפוס סיסמה ישלח לדוא"ל/טלפון הנתון לשליטתו הבלעדית של המשתמש	✔	
הזנת סיסמא שגוייה פעמיים	שימוש בקאפצ'ה	X	אין תמיכה בקאפצ'ה
הזנת סיסמא שגוייה 5 פעמים	חסימת משתמש וניתוק מהמערכת	✔	
החלפת סיסמאות אחת ל-180 יום	הגדרה ויישום אכיפת החלפת סיסמאות אחת ל-180 יום	✔	
מדיניות שימוש בסיסמאות ישנות	על המערכת לחסום שימוש בסיסמאות קודמות. שמירת היסטוריית סיסמאות, עד 5 סיסמאות אחורה	✔	
2 factor authentication	שימוש באמצעי זיהוי נוסף על סיסמא	X	

Session Management

נושא	הסבר	תאימות	הערות
מנגנון Idle Timeout	יש לקיים מנגנון Idle Timeout אשר יסיים את ה-Session של המשתמש לאחר 60 דקות של חוסר פעילות במערכת	✔	
חיבור מחדש לאחר נפילת מערכת	כאשר ישנה נפילת מערכת או הפעלה מחדש של שרת האינטרנט, יש צורך בהזדהות מחדש בעת חיבור למערכת	✔	
ניתוק ה-Session	ניתוק ה-Session יבוצע על ידי סיום תוקף ה-Session בצד השרת, ולא על ידי העברת הלקוח לדף הכניסה בלבד	✔	

שרתים ותקשורת

נושא	הסבר	תאימות	הערות
עדכון מערכת ההפעלה ו- database, בשרתים	יש לבצע עדכון של מערכת ההפעלה ורכיבים בתוכנה לגירסה העדכנית ביותר. יש לציין את פרק הזמן בו יבוצע עדכון. מומלץ לבצע עדכון כל חודש	✔	
שימוש בגרסאות אחרונות של שפת הפיתוח כולל מוצרים צד ג וקוד פתוח	יש להשתמש בגרסה המכילה את עדכוני אבטחת מידע העדכנים ביותר של הגרסה העיקרית (magor release) עליה המערכת מפותחת כולל מוצרים כגון wordpress moodle וכו'	✔	
פורטים פתוחים	יש לבדוק אילו פורטים פתוחים. יש לודא שאין פורטים פתוחים ללא צורך	✔	מצ"ב
יישום WAF על שרתי WEB	לצורך הגנה על אתר האינטרנט, יש להוסיף שכבת הגנה של Web Application Firewall אשר תאפשר הגנה על האתר (בנוסף ל-FireWall). שכבה זו מנטרת וחוסמת התקפות ברמה האפליקטיבית ומונעת ניצול לרעה של פרוטוקול HTTP/S	✔	אנחנו משתמשים בשרות של Incapsula
יש להתקין AV על כל שרתי Windows יש להתקין AV על שרתי Linux אשר מבצעים אליהם העלאה של קבצים ע"י המשתמשים יש לוודא שה AV מתעדכן בחתימות באופן שוטף		✔	
האם קיים מערך חומת אש ורכיבי IPS למניעת התקפות על היישום?		✔	Incapsula, AWS
תצורת השרתים תכלול מערך זמינות על מנת להבטיח גישה רציפה ליישום	הסבר על הפתרון הקיים	✔	AWS auto scaling
מיקום שרתים			AWS Frankfurt

תיעוד logging ואזהרות

נושא	הסבר	תאימות	הערות
הפעלה של תיעוד מלא ואזהרות מערכת על פעולות לא מורשות	יש לבצע תיעוד של לוגים אפליקטיביים, של השרתים (כגון IIS,Appache) ושל מערכות אבטחת המידע כגון WAF, IPS, FW, אנטי וירוס	✔	
תיעוד פעולות בלוג עם פרטי משתמש	יש לתעד פעולות במערכת בצמוד למבצע הפעולה	✔	
יש לשמור לוגים לתקופה של 24 חודשים		✔	

טיפול באירועי סייבר

נושא	הסבר	תאימות	הערות
האם קיים בעל בחברה מנהל אבטחת מידע במשרה מלאה		X	
האם קיים נוהל טיפול בארועי סייבר		✔	מצ"ב
האם נוהל טיפול בארועי סייבר נבחן לפחות פעם בשנה?		✔	
האם קיים נוהל אבטחת מידע בחברה		✔	מצ"ב
תוך כמה זמן מהתגלות אירוע סייבר אתם מתחייבים להודיע ללקוח?		✔	עד 8 שעות

תקנים

מערכת טריביו הותאמה לתקנות הגנת הפרטיות של מדינת ישראל.
המערכת מותקנת על שרתים של אמזון בפרנקפורט ולפיכך עומדת בכל תקני אבטחת השרתים עצמם.
אמזון עומדת בתקנים הבאים:
ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015
הרשימה המלאה והאזורים הנתמכים -
https://aws.amazon.com/compliance/iso-certified

תקן GDPR - למרות שבאופן רשמי אין לנו תו תקן GDPR המערכת תואמת להגדרות המהותיות שבתקן.
אנחנו לא מעבירים מידע של משתמשים לאף גורם צד שלישי, אין לנו פרסומות, אנחנו מאפשרים למשתמשים למחוק את החשבון שלהם ללא יכולת שחזור באמצעות פניה למחלקת התמיכה, אנחנו לא נוקטים בפעולות שיווק שאינן קשורות ישירות לפעילות טריביו.

אירועי סייבר קודמים

טריביו חוותה אירוע סייבר בינואר 2020.
באירוע התגלתה חולשת אבטחה אשר איפשרה גישה לדוחות שעות של תלמידים לזמן מוגבל גם למשתמשים לא מורשים.
האירוע טופל במיידית וגם הוטמע פיתרון קבע תוך זמן קצר.
עיקר הבעיה הייתה בפעולה א-סינכרונית של ייצוא דוחות:

1. יצירת דוח במערכת
2. לחיצה על כפתור ייצוא - ייצור הדוח בצד השרת ברקע.
3. כאשר הדוח מוכן - שליחת נוטיפיקציה למשתמש עם לינק לדוח.

הלינק לדוח היה פעיל 24 דעות ולא בוצע עליו אימות משתמש.
התיקון היה מעבר לפעולה סינכרונית, כך שדוחות לא נשמרים בכלל בשרת אלא נשלחים כ תשובה לפעולת הייצוא.
מצורף תחקיר האירוע.