



אוגוסט 2023

דרישות אבטחת מידע מספקי SaaS

רקע:

בנוף הדיגיטלי של היום, תוכנה כשירות (SaaS) חוללה מהפכה באופן שבו עסקים פועלים, ומציעה פתרונות גמישים ותהליכים יעילים. עם זאת, ככל שהאימוץ של SaaS גדל, כך גם החששות לגבי הגנת נתונים, בטיחות ממשקים, פרטיות ועמידה ברגולציה. כדי להבטיח את בטיחות המידע הרגיש ולשמור על אמון המשתמשים, דרושות הנחיות הגנת מידע והתנהלות טכנולוגית מאובטחת לספקי SaaS.

מסמך זה מתאר את דרישות הסייבר הבסיסיות שספקי SaaS צריכים לעמוד בהן. הוא מכסה מגוון תחומים קריטיים, כולל הצפנת נתונים, בקורות גישה, ניהול עדכונים/פגיעויות, תגובה לאירועים ועמידה בתקני התעשייה. על ידי יישום דרישות אלה, ספקי SaaS יכולים ליצור סביבה מאובטחת לנתוני המשתמשים שלהם, להפחית סיכונים ולהפגין את מחויבותם לשמירה על מידע.

בנוסף, מצורף שאלון שנועד להדריך את הן אותנו והן את ספקי ה-SaaS דרך הערכה מקיפה של הגדרות ונוהלי אבטחת המידע שלהם. על ידי התייחסות לשורה של שאלות מפתח, הערכה זו תסייע בזיהוי נקודות תורפה פוטנציאליות, להבליט תחומים לשיפור, ותבסס בסיס איתן לשמירה על הסודיות, המהימנות והזמינות של נתוני לקוחות ונתונים קנייניים כאחד.

יש לשקול את המשמעות של כל שאלה ביחס להקשר הייחודי של הארגון ולפרופיל הסיכון. התשובות ישמשו כמפת דרכים לחיזוק פרוטוקולי אבטחת המידע וחיזוק האסטרטגיה הכוללת לניהול סיכונים. נוף אבטחת סייבר הוא עולם דינמי, עם איומים חדשים שצצים באופן קבוע. הערכה והתאמה מתמשכת הם המפתח להקדמת אתגרים פוטנציאליים ולהבטחת תצורת אבטחה מיטבית.



דרישות

1. היגיינת סייבר

- 1.1. החברה תדווח על אירועי סייבר משמעותיים שפגעו בחברה בשנתיים האחרונות. החברה תעביר לבנק פרטים נדרשים לגבי אירוע הסייבר לפי בקשתו.
- 1.2. במידה והחברה עברה אירוע סייבר בשנה האחרונה, שבמהלכו דלפו נתונים של לקוחות החברה, על החברה להוכיח לבנק שבוצע תהליך הפקת לקחים ושהליקויים טופלו באופן מלא, אחרת הבנק יראה לנכון לפסול את הפתרון.

2. עמידה בתקנים

- 2.1. במסגרת הצעתה תפרט החברה באלו תקנים בינלאומיים בנושא אבטחת מידע היא עומדת, כגון ISO27001 או CSA.
- 2.2. אם החברה תרצה להעסיק קבלני משנה נוספים, היא תידרש למסור לבנק מידע לגבי עמידתם בתקנים בינלאומיים של אבטחת מידע.

3. אבטחת תשתיות

- 3.1. החברה תאחסן את נתוני הבנק בנפרד מחשבונות או לקוחות אחרים: טבלה נפרדת בבסיס הנתונים שלה, או instance נפרד או תצפין נתונים אלה ע"י מפתח ייעודי לנתוני הבנק. חוזק המפתח יהיה AES 256-Bit מינימום.
- 3.2. החברה תתקין עדכוני אבטחה בסיווג יצרן של "קריטי" על מערכות הפעלה, שרתי אפליקציה, שרתי DB עד חודשיים מתאריך פרסומם לכל היותר.
- 3.3. החברה תיישם הזדהות חזקה (2 factor authentication) עבור הדהות מנהלי רשת ומפתחים לערכות הייצור שלה הנוגעות לנתוני בנק ישראל.
- 3.4. החברה תשתמש בפרוטוקול הצפנה בגרסת TLS 1.2 ומעלה כדי להצפין את התקשורת בין שרתי ה DB שלה עד ליישומי הלקוח.
- 3.5. תחנות העבודה והשרתים של סביבת הפיתוח יוקשחו על בסיס תקנים ציבוריים כמו NIST או CIS.

4. אבטחת אפליקציה

- 4.1. החברה תבצע מבדק חוסן אחת לשנה על כלל מערכות המידע המנהלות את נתוני בנק ישראל: שרתי DB, שרתי אפליקציה וכל מערכות נלוות אחרות. החברה תספק לבנק את שם הספק שאר ביצע את מבדק החוסן, ואת תוצאות מבדק החוסן לפי דרישת הבנק.



4.2. החברה תערוך הדרכות פיתוח מאובטח למפתחים שלה פעם בשנה לפחות. החברה תספק פרטים על מועד והיקף ההדרכה, וגם על המתודולוגיה של ההדרכה (SDLC, OWASP וכד') לבנק לפי דרישה.

4.3. הזדהות הלקוחות לאפליקציה תבצע על בסיס הזדהות חזקה (Multi Factor Authentication). שאיננה מבוססת SMS אלא על בסיס דוא"ל או יישום (אונתנטיקטור).

5. ממשקים אפליקטיביים

5.1. הממשקים בין מערכות החברה למערכות הלקוחות שלה יהיו מבוססי תקנים פתוחים: XML/XSD, Web Service /WSDL

5.2. הגישה לממשקים אלה תהיה אך ורק דרך פרוטוקולים מאובטחים כגון: HTTPS, TLS

6. תהליכי אבטחת מידע

6.1. החברה תציג לבנק את תוכנית המענה שלה לאירועי אבטחת מידע.

6.2. החברה תציג לבנק את אמצעי הבקרה והפיקוח שלה על שימוש בשירותי ענן ציבוריים.

6.3. החברה תציג לבנק את פתרון איסוף וניתוח קבצי הלוג שלה מהמערכות השונות הנוגעות לנתוני בנק ישראל.

6.4. החברה תציג לבנק את פתרון ניהול ההתראות תיאום האירועים (SIEM/SOC) שלה.

6.5. החברה תציג לבנק את הפתרון שלה למניעת דלף מידע.

6.6. החברה תודיע לבנק ישראל על כל גישה של עובדי החברה או ספקי החברה לנתוני הבנק באופן מיידי.

6.6.1. החברה תשמור רישום של כל הגישות של עובדי החברה או ספקי החברה אל נתוני

הבנק למשך שלוש שנים. הרישום יוצג לבנק לפי דרישה ללא דיחוי.

6.6.2. החברה תספק לבנק דוחות לגבי גישות משתמשים לנתוני בנק דרך האפליקציה לפי דרישה.

6.7. החברה תנטר גישה בלתי מורשית למערכות הנתונים המכילות את נתוני בנק ישראל.

6.8. החברה תתקין כל אמצעי הגנה נדרש ברשתות ובמערכות שלה על מנת להגן על נתוני בנק ישראל.

6.9. הבנק שומר לעצמו את הזכות לערוך ביקורת שתבדוק את עמידת קבלני החברה בדרישות אלה לפחות אחת לשנה.

6.10. החברה, או קבלני המשנה, ידווחו לבנק באופן מיידי על כל אירוע אבטחת מידע, או אירוע חריג אחר שהתרחש אצלם. "אירוע חריג" יאופיין מול החברה, או קבלני המשנה, לאחר זכייה במכרז.

6.11. החברה, או קבלני המשנה, יאפשרו לבנק, או לנציגיו, לבצע תחקור במערכות המידע שלהם לאחר אירוע המוגדר בסעיף זה, לפי שיקול דעת הבנק. התחקור יכלול גישה למערכות מידע



של החברה, או קבלני המשנה, ויצירת עותקים של מידע רלוונטי לשימוש הבנק, או נציגיו, לצרכי ניתוח האירוע בלבד.

שאלון סיווג מידע שירות SaaS וניהול משתמשים

מטרת מענה על השאלון הוא יצירת תובנות שיסייעו לבנק ישראל להשיג הבנה רחבה יותר של תהליכי שירות ה-SaaS של החברה הנבחנת הקשורים לסיווג מידע וניהול משתמשים.

שם החברה :

תאריך (נא לציין):

משיב על השאלון (שם מלא):

אנא ספק תשובות מפורטות לשאלות הבאות כדי לעזור לנו להבין את התהליך הפורמלי של שירות ה-SaaS של החברה לסיווג מידע וניהול משתמשים.

יש לענות על שלושת הסעיפים בהרחבה (1. סיווג מידע שירותי SaaS, 2. ניהול משתמשים, 3. סיכום \ מסקנות).

סעיף 1: סיווג מידע שירות SaaS

1.1 איזה סוג של מידע/נתונים מועלים בדרך כלל לשירות ה-SaaS של החברה ?

1.2 כיצד אתה מחלק או מסווג כרגע את המידע/הנתונים שהועלו בתוך שירות ה-SaaS של החברה?

[] לפי רגישות (סודי, פנימי, ציבורי).



[] לפי סוג נתונים (למשל, מסמכים, תמונות, סרטונים).

[] אחר (נא לציין):

1.3 אילו קריטריונים או גורמים אתה לוקח בחשבון בעת קביעת סיווג המידע/נתונים שהועלו ?

[] רגישות הנתונים.

[] דרישות משפטיות או רגולטוריות.

[] השפעה עסקית.

[] אחר (נא לציין):

1.4 תאר את התהליך שאתה עוקב אחריו כדי לסווג מידע/נתונים שמועלים לשירות ה-SaaS של החברה :

1.5 האם יש תהליך אישור רשמי להקצאת רמות סיווג למידע/נתונים שהועלו ?

[] כן.

[] לא.

[] אם כן, תאר את תהליך האישור:



סעיף 2: ניהול משתמשים

2.1 מהם תפקידי המשתמש השונים שנקבעו בשירות ה-SaaS של החברה ?

.Administrator []

.User []

.Viewer []

[] אחר (נא לציין):

2.2 כיצד משתמשים חדשים מוכנסים לשירות ה-SaaS של החברה ?

.Administrators Assign Roles []

.Users Select Roles During Onboarding []

.Combination of Both []

[] אחר (נא לציין):

2.3 האם יש תהליך שבו משתמשים יכולים לבקש גישה למערך נתונים ספציפיים או מידע בשירות SaaS ?

[] כן.

[] לא.

[] אם כן, אנא תאר את תהליך בקשת הגישה.

2.4 הסבר כיצד גישת משתמשים מנוהלת ומפוקחת בתוך שירות ה-SaaS של החברה :



2.5 כאשר משתמש אינו זקוק יותר לגישה או עוזב את הארגון, מהו התהליך להסרת הגישה שלו ?

.Administrators Revoke Access []

.Automated Process []

.Combination of Both []

[] אחר (נא לציין):

2.6 האם אתה עורך סקירות תקופתיות של זכויות גישה למשתמשים כדי לוודא שהן מיושרות עם התפקידים והאחריות שלהם ?

[] כן.

[] לא.

[] אם כן, אנא תאר את התדירות של ביקורות אלה:

סעיף 3: סיכום \ מסקנות

3.1 לסיכום, מהם היתרונות העיקריים של התהליך הרשמי של שירות ה-SaaS של החברה לסיווג מידע וניהול משתמשים ?

3.2 האם מתוכננים שיפורים או שינויים קרובים לתהליך סיווג המידע וניהול המשתמשים ?

3.3 האם יש מידע נוסף שתרצה לשתף בנוגע לגישה של שירות ה-SaaS של החברה לסיווג נתונים וניהול משתמשים ?