נובמבר 2023
עדכון: ינואר 2026

סטנדרטים לאבטחת מידע, הגנת סייבר והמשכיות עסקית באקו-סיסטם של כרטיסי חיוב בישראל

בשנים האחרונות אנו עדים להתפתחויות משמעותיות באקו-סיסטם של פעילות כרטיסי החיוב בישראל. התפתחויות אלו הובילו לעלייה דרמטית במספר הגורמים שלוקחים חלק בשלבים השונים של ביצוע העסקה בכרטיס חיוב.

מפעיל מערכת התשלומים "שירותים בכרטיסי חיוב" (חברת שבא) וכן משתתפי המערכת הינם גופים מפוקחים בעלי סטנדרטים גבוהים בתחומי אבטחת מידע, הגנת סייבר והמשכיות עסקית, אולם ישנם שחקנים רבים באקו-סיסטם ללא פיקוח או מחויבות לעמוד בסטנדרט כלשהו בהיבטים אלו.

פעילותם של שחקנים אלו חושפת את מערכת התשלומים "שירותים בכרטיסי חיוב" לסיכונים שונים בהיבטי אבטחת המידע, הגנת הסייבר והמשכיות עסקית ועלולה לפגוע ברציפות התשלום בכרטיס חיוב.

1. מטרת המסמך

כדי לצמצם את הסיכונים האמורים, עלה צורך בגיבוש סטנדרטים לכל השחקנים באקו סיסטם לרבות שחקנים אשר אינם תחת פיקוח או אסדרה. הסטנדרטים המוצגים במסמך זה גובשו לאחר התייעצות עם השוק וזאת תוך איזון בין הצורך לאפשר את המשך התפתחותו הטכנולוגית של שוק כרטיסי החיוב בישראל לבין הצורך להבטיח את הפעילות התקינה בכרטיסי החיוב בישראל והכל בשים לב לצרכים של השחקנים השונים לאורך שרשרת ביצוע עסקה בכרטיס חיוב. מסמך זה מפרט את ההסכמות הרחבות אליהן הגיעו השחקנים השונים לאורך שרשרת ביצוע עסקה בכרטיס חיוב בתחומי אבטחת מידע, הגנת סייבר והמשכיות עסקית.

2. תחולה

2.1. ההסכמות אליהן הגיע השוק כוללות עמידה בסטנדרטים אחידים על ידי כל הגופים הפועלים באקו-סיסטם של כרטיסי החיוב בישראל שלהלן:

2.1.1. יצרני קופות

2.1.2. יצרני תוכנה

2.1.3. מפיצי תוכנה

2.1.4. משווקי פינפדים

2.1.5. מתפעלי CLP (Closed Loop Payments)

2.1.6. מאגדי סליקה

2.1.7. שרתי תשלומים (Payment Gateways)

2.1.8. חברות ניכיון

2.1.9. חברות התאמה

2.2. מסמך זה יתוקף ויעודכן מעת לעת בהתאם לצורך ולפי דרישות והסכמות השוק.

3. תנאי סף לפעילות באקו-סיסטם בכרטיסי חיוב

3.1. כל גוף שפועל באקו-סיסטם של כרטיסי החיוב בישראל ומפורט בסעיף התחולה (להלן: "**המשתתף**") יידרש להצהיר בפני מפעיל המערכת, על יכולות טכנולוגיות ומשאבים, לרבות המצאת המסמכים הבאים:

3.1.1. הצגת מסמך תקף AOC (Attestation of completion) לאישור עמידה בתקן PCI-DSS[1] אחת לשנה.

3.1.2. עמידה בדרישות אבטחת המידע והגנת הסייבר כמפורט בסעיף 4 למסמך זה.

3.1.3. עמידה בדרישות המשכיות עסקית כפי שמפורט בסעיף 5 למסמך זה.

יובהר שכל הגופים נדרשים לעמוד בדרישות התקן ולהמציא אישור כאמור, למעט גוף שאינו שומר פרטי כרטיסי אשראי כפי שקבוע בתקן עצמו. גוף כזה יצטרך להצהיר או להציג אישור על כך שאינו שומר פרטי כרטיסי אשראי.

4. דרישות בסיסיות לאבטחת מידע והגנת הסייבר

4.1. **שאלון "יובל"** - מילוי הצהרה עצמית של שאלון "יובל", לכל הפחות ברמת סיכון בסיסית 1 (19 בקרות) וברמת הסמכה B, בנושא הגנת הסייבר ואבטחת מידע אחת לשנה, לרבות רישום למערך ספקים בהערכה עצמית באתר האינטרנט של מערך הסייבר הלאומי.[2]

4.2. **ממונה אבטחת מידע** - המשתתף יגדיר ממונה אבטחת מידע מטעמו לעניין אבטחת מידע והגנת הסייבר כולל האחריות ליישום ההנחיות האמורות במסמך זה.

4.3. **מדיניות הגנה על המידע ו/או הגנת הסייבר** - באחריות המשתתף לוודא שקיימת בידיו תשתית ארגונית תומכת להכלה והתמודדות נאותה עם אירוע דוגמת השתלטות על חשבון הניהול, התקפת מניעת שירות, השחתה, דלף מידע ואיומים נוספים.

4.4. **מרכז סייבר ורציפות פיננסית** – המשתתף יתחבר לפעילות מרכז סייבר ורציפות פיננסית ויפעל מולו בשיתוף פעולה, לרבות; העמדת איש קשר, שיתוף מידע בנוגע לחשדות ואירועי סייבר, מימוש ויישום כלים ושירותים שיועמדו לרשותו וכן ביצוע פעולות לצמצום השפעתן ומתן היזון חוזר במקרה של קבלת מידע מחשיד ו/או התרעה מהמרכז לסייבר פיננסי.

4.5. **סקר חוסן ובדיקות חדירות** - המשתתף ישלים סקר חוסן ובדיקות חדירות למערכות המידע בחצרותיו אחת לשנה, לרבות שמירת תיעוד והצגתו. אם יעלו בסקר או בבדיקה ממצאים שליליים, על המשתתף לקבוע תכנית הפחתה ולוחות זמנים לטיפול בכל הממצאים.

---

[1] Payment Card Industry Data Security Standard (PCI-DSS)

[2] הסבר על שאלון "יובל" של מערך הסייבר הלאומי וקובץ שאלון ב-Excel:
https://www.gov.il/he/departments/news/querysupply

4.6. **נהלים ותיעוד לוגים (log)** - המשתתף נדרש לבנות מערך נהלים לתיעוד לוגים ומידע שקשורים לפעילות בכרטיסי חיוב, לשמור מידע זה לכל הפחות לתקופה של שנתיים ולהציגו ככל שיידרש.

4.7. **פיתוח מאובטח** - באחריות המשתתף לקיים תהליכי פיתוח המבוססים על נהלי פיתוח מאובטח מקובלים. ככל שהפיתוחים נכתבים ו/או מבוצעים באמצעות גוף צד ג', יש לוודא כי אלה עברו תהליכי סריקה ותקינות הקוד.

4.8. **הגנה על עמדות קצה ושרתים** – על המשתתף להגן באמצעים מקובלים על המחשב שמחובר לאינטרנט ולבצע עדכוני אבטחה שוטפים במערכת ההפעלה. אם נדרשים עדכוני אבטחה ברמת חומרה גבוהה וקריטית יעדכנם באופן מיידי. למען הסר ספק, קופה נחשבת לחומרה רגישה ואינה אמורה להתחבר לאינטרנט, אלא לפי הצרכים העסקיים המינימליים הדרושים לפעילות העסקית השוטפת. אם נדרשת גישה לאינטרנט על המשתתף לוודא שהדבר נעשה באמצעות 'גלישה בטוחה'.

4.9. **בדיקות מהימנות** - באחריות המשתתף לבצע בדיקות מהימנות לכלל העובדים אשר יעבדו ישירות מול המערכת, לרבות תיעוד הבדיקות והצגתן לפי דרישה.

4.10. **מענה למתקפות מניעת שירות- (DDOS)** – אם המשתתף מחצין שירותים עבור נקודות קצה כחלק מפעילות התשלומים עליו לתת התייחסות ורמת הגנה הולמת למתקפות מניעת שירות תשתיתית ואפליקטיבית כחלק מתהליך המשכיות עסקית של מערכת התשלומים.

4.11. **הרשאות** - על המשתתף לוודא כי מתן הרשאות לעובדיו הינו על בסיס הצורך לדעת. בנוסף, על המשתתף לבצע בקרות ותיעוד על תהליכי עזיבה, ניוד, הקמה, גישה מרחוק של עובדיו, לרבות שמירת תיעוד ההרשאות והבקרות והצגתו ככל שיידרש.

4.12. **מודעות עובדים** - המשתתף יבצע הדרכת מודעות לעובדיו בנושאי אבטחת מידע, אחת לשנה לכל הפחות, כולל מעקב נוכחות, ויתעד את ההדרכות ומי המשתתפים בהן.

4.13. **תרגול -** המשתתף יבצע תרגול תקופתי לעובדים ותרגול תקופתי להנהלת הארגון.

5. דרישות בסיסיות לניהול המשכיות עסקית

5.1. **ממונה המשכיות עסקית** - המשתתף יגדיר ממונה המשכיות עסקית מטעמו לעניין ניהול ההמשכיות העסקית כולל האחריות ליישום ההנחיות האמורות במסמך זה.

5.2. **זיהוי איומים ותהליכים** - המשתתף יזהה איומים בעלי פוטנציאל לחשוף את מערכותיו לסיכונים ושיבושים, וימפה תהליכים קריטיים לפעילות בתחום התשלומים ומשאבים נדרשים (כגון: מערכות נלוות, אמצעים, תשתית וכדומה).

5.3. **תכנית המשכיות עסקית** - המשתתף יגבש תכנית המשכיות עסקית להבטחת הרציפות התפקודית תחת שיבושים, לרבות תהליכי גיבוי והתאוששות למערכות המידע בחצרותיו שקשורות לפעילותו בתחום התשלומים.

5.4. **דיווח אירועים** - במקרה של מצב חירום או אירוע תפעולי חריג (לרבות סייבר), המשתתף ידווח למפעיל המערכת, על פרטי האירוע במצב החירום עד שעתיים מרגע תחילת האירוע. על המשתתף להכין תחקיר אירוע עד שבעה ימי עסקים לאחר תחילת האירוע.

5.5. **ספק תשתית** - המשתתף יבטיח את יכולתו להחליף ספק תשתית אינטרנט תוך פרק זמן קצר במקרה של כשל אצל ספק תשתית האינטרנט שלו. משתתפים שמספקים שירותי תשלום ל"מפעלים למתן שירותים קיומיים", כגון: מפעלי ייצור מזון, תחנות דלק, שדות תעופה, שירותי חירום וכדומה (להלן: "**שירותים קיומיים**") יבטיחו יכולת החלפה אוטומטית בין 2 קווי נל"ן, בנפח 2 MB כל אחד, במקרה של כשל.

5.6. **ספק שירות** - המשתתף יבטיח את יכולתו להחליף ספק שירות אינטרנט תוך פרק זמן קצר במקרה של כשל אצל ספק שירותי האינטרנט שלו. משתתפים שמספקים שירותי תשלום לשירותים קיומיים לאוכלוסייה יבטיחו יכולת החלפה אוטומטית בין ספקי שירות במקרה של כשל.

5.7. **גיבוי תקשורת** - המשתתף יבטיח יכולת גיבוי אינטרנטי או סלולרי למידע ויכולת אחזור מידע חיוני במקרה כשל.

5.8. **רוחב פס** – המשתתף, למעט משווק פינפדים שאינו עוסק בפעילות נוספת כמפורט בסעיף 2.1 לעיל, יגדיר רוחב פס שיתחשב בהיקף התנועות ובשינויי שוק צפויים עבורו ויחזיק רוחב פס שלא יפחת מ-150% מנפח שיא הפעילות שלו.

5.9. **ניטור ובקרה** - על המשתתף, למעט משווק פינפדים שאינו עוסק בפעילות נוספת כמפורט בסעיף 2.1 לעיל, לבצע ניטור שוטף לתקינות קווי התקשורת ורוחב הפס.

5.10. **גיבוי אנרגטי** – משתתף, למעט משווק פינפדים שאינו עוסק בפעילות נוספת כמפורט בסעיף 2.1 לעיל, יערך לגיבוי אנרגטי במקרה של הפסקת חשמל (UPS, גנרציה וכדומה).

5.11. **סקר המשכיות עסקית -** משתתף יבחן אחת לשנה את מידת מוכנותו להתמודדות עם אירועי המשכיות עסקית כמפורט בפרק זה.

5.12. **מודעות עובדים** - המשתתף יבצע הדרכת מודעות לעובדיו בנושאי המשכיות עסקית, אחת לשנה לכל הפחות, כולל מעקב נוכחות, ויתעד את ההדרכות ומי המשתתפים בהן.

5.13. **תרגול -** המשתתף יבצע תרגול תקופתי לעובדים ותרגול תקופתי להנהלת הארגון.

6. הגדרות

- **מפעיל מערכת התשלומים** - הגוף שאחראי לתפעול מערכת התשלומים.

1. **עמותת הפרוטוקול** - העמותה לניהול פרוטוקול מסופי אי.אם.וי בישראל.
2. **מערכת שירותים בכרטיסי חיוב -** המופעלת על ידי חברת שירותי בנק אוטומטיים בע"מ

- **הפרוטוקול** - מפרט טכנולוגי של מבנה מסר אחיד ומאובטח שפותח בהתאם לצרכים והמבנה הייחודיים של השוק הישראלי על בסיס הפרוטוקול של הסכמות הבינלאומיות ומשמש להעברת אישורים, עסקאות ומידע בין גורמים בשרשרת ביצוע עסקה בכרטיסי חיוב בישראל בקטע שבין המסוף למערכת התשלומים בכרטיסי חיוב.

- **יצרני קופות** (Cash register Manufacturers) - גוף שמפתח או מתאים תוכנה של שירותי קופה לבתי עסק הכוללת את ניהול החיובים והזיכויים לפי אמצעי תשלום שונים וכן ניהול מלאי, מבצעים, חיבור למערכות ERP ועוד. תוכנת הקופה מקושרת בפרוטוקול תקשורת למסוף בית העסק ומקבלת ממנו את נתוני פעילות האשראי היומית.

- **יצרני תוכנה** (POS Terminal Software Manufacturers) - גוף המפתח תוכנה לסליקת עסקאות בכרטיסי חיוב על בסיס פרוטוקול.

- **מפיצי תוכנה** (POS Terminal Technology Providers) - גוף המשווק לבתי עסק תוכנה של יצרן תוכנה לסליקת עסקאות בכרטיסי חיוב.

- **משווקי פינפדים** (Pin Pad Distributor) - גוף המספק רכיבי חומרה שמאפשר הקלדה ואימות של הקוד הסודי מול כרטיס החיוב בעת ביצוע עסקת EMV.

- **מתפעלי CLP** (Closed Loop Payments Processor) - חברת תוכנה המספקת שירותי תשלומים למנפיקי מותגים פרטיים, כגון מועדוני צרכנות, אשר מאפשרים ביצוע תשלום ומימוש ההטבות ב"מעגל סגור".

- **מאגד סליקה** (Payment Aggregator) - תאגיד שמרכז חיובים וזיכויים של בתי עסק המבוצעים באמצעות כרטיסי חיוב תחת הסכם סליקה מול סולק.

- **שרת תשלומים** (Payment Gateway) - גוף שמספק תשתית טכנולוגית לבית עסק לצורך ניתוב ועיבוד עסקאות במסחר מקוון ואינו מעורב בטיפול בסליקת הכספים.

- **חברת ניכיון** (Factoring Company) - גוף שמספק לבתי עסק שירותים להקדמת תשלומי האשראי (ניכיון) לפני מועד קבלת התשלום הצפוי מהסולק.

- **חברת התאמה** (Reconciliation Company) - גוף שמספק לבתי עסק שירותי התאמה ובקרה בין החיובים והזיכויים שנרשמו בבית העסק לבין התמורה שהתקבלה בגינם בפועל מהסולק.

- **ספק תשתית אינטרנט** – גוף שמספק את התשתית הפיזית (סיבים, שרתים וכו') שמאפשרת חיבור לאינטרנט.

- **ספק שירות אינטרנט** (ISP) – גוף שמספק ללקוח את הזמינות ואת רוחב פס החיבוריות לאינטרנט.

- **תכנית המשכיות עסקית** (BCP) - תכנית פעולה מקיפה בכתב שקובעת מה הם הנהלים והמערכות הדרושים כדי לשמר את הרציפות העסקית או לשקם את הפעילות במקרה של חירום, שיבושים או כשלים.

- **מפעלים למתן שירותים קיומיים -** כהגדרתם בחוק שירות עבודה בשעת-חירום, תשכ"ז-1967.
- **מרכז סייבר פיננסי (CERT פיננסי) -** מרכז אופרטיבי, בניהול והובלת משרד האוצר, לתמיכה בהגנת הסייבר של המערכת הפיננסית. המרכז הינו גוף מתאם מרכזי בין ארגונים ומשתתפים פיננסיים בישראל לבין גופי המעטפת הלאומית והבינלאומית. המרכז אחראי לתאם את הפעילות לחיזוק חוסן המערכת הפיננסית בישראל, ולספק שירות וטכנולוגיות לשיתוף מידע הגנתי לארגונים פיננסיים ולרגולטורים. המרכז ממוקם ב-CERT הלאומי ופועל בתיאום עם מערך הסייבר הלאומי.

7. מעקב גרסאות

מסמך זה יעודכן מעת לעת בהתאם לשינויים ולהתפתחויות בתחום.

תאריך הפרסום	מהות העדכון
14.11.23	פרסום לראשונה