מכרז מס. 36/25 נספח אבטחת מידע והגנת סייבר

רקע ומטרה

מכרז זה עוסק בפרויקט תשתיתי הכולל הקמה ותפעול של עמדות טעינה מהירות לאוטובוסים, וניהול חניון תחבורה ציבורית. פרויקט זה מערב תשתיות חשמל, מערכות מידע, תקשורת, בקרה וניהול מרחוק – ולכן נדרש להבטיח עמידה קפדנית בדרישות אבטחת מידע והגנת סייבר, בכפוף למדיניות משרד התחבורה, רגולציה ממשלתית, חוק הגנת הפרטיות ותקני סייבר מחייבים.

תחולת הדרישות

הדרישות חלות על כלל הרכיבים הפיזיים והדיגיטליים של המערכת, כולל אך לא מוגבל ל:

- עמדות טעינה מהירה לאוטובוסים
- ארונות חשמל ובקרי טעינה
- מערכת ניהול טעינה (CMS)
- תשתיות רשת ותקשורת
- מערכות ניהול החניון
- תוכנות שליטה ובקרה SCADA (אם קיימת)
- שירותי ענן / ניהול מרחוק
- תחנות קצה, שרתים, מסדי נתונים
- ציודי IT בחדרי שליטה, בקרות או עמדות תפעול

דרישות כלליות

ניהול סיכוני סייבר

- על הזוכה לבצע **סקר סיכוני סייבר** מלא לכלל מערכות המכרז (IT + OT).
- הסקר ייערך לפי מתודות מוכרות (NIST, ISO) וישקף אמצעי טיפול נדרשים.
- מיפוי סיכונים יכלול תקשורת בין רכיבי החניון, בקרי הטעינה והתחבורה הציבורית.

ניהול פרטיות ואחריות רגולטורית

- הגנה על כל מידע אישי או מזהה (כגון מיקום, זהות מפעיל, קוד גישה).
- עמידה בחוק הגנת הפרטיות (כולל תיקון 13), תקנות הגנת הפרטיות, והנחיות הרשות.
- במקרה של שמירת מידע אישי, חובת רישום מאגר מידע.

ממשקי ספקים וקבלני משנה

- כל גורם משנה ייבחן לפי סקר ספקים.
- יחויב בחתימה על הצהרת סודיות (NDA) ועמידה בתנאי אבטחת מידע.
- יבוצע ניהול הרשאות לספקים על בסיס "ידע וצורך".

דרישות טכנולוגיות

אבטחת רשת ותקשורת

- **הפרדה לוגית ופיזית** בין רכיבי OT\IoT (מערכות ניהול חניון, עמדות טעינה) לבין מערכות IT.
- שימוש בפרוטוקולים מוצפנים תקניים לתקשורת בין סביבות ורכיבים.
- יישום **Firewall ייעודי** והתקנת מערכות IDS/IPS למניעת חדירה.

ניהול גישה והרשאות

- מדיניות הרשאות מינימלית (Least Privilege).
- שימוש באימות רב-שלבי (MFA) לכל ממשק ניהול.
- רישום, מעקב ובקרה אחר כל כניסה ושינוי במערכת.

הגנת תחנות קצה

- התקנה ועדכון שוטף של תוכנת EDR בתחנות קצה ושרתים.
- הקשחת מערכות הפעלה (Hardening) וסגירת שירותים מיותרים.
- חסימה של חיבור התקני USB אלא אם הותרו במפורש.

ניטור, רישום והתראה

- חובת התקנת פתרון ניטור לוגים (SIEM) או פתרון חלופי המאושר ע"י החברה.
- שמירת לוגים מאובטחת למשך 6 חודשים לפחות.
- מערכת התרעות פנימית על גישה חשודה, ניסיון חדירה או שינוי הרשאות.

דרישות תשתיתיות ופיזיות

- התקנת אמצעים פיזיים למניעת חבלה / פריצה לעמדות הטעינה.
- נעילה ובקרה של ארונות תקשורת וחשמל.
- מצלמות אבטחה באזורי תפעול רגישים.

תהליכים נדרשים

תגובה לאירועים

- נוהל תגובה והתמודדות באירוע סייבר, כולל תחקור והפקת של לקחים.
- חובת דיווח מיידי במקרה של תקיפה/חשד לאירוע.
- שיתוף בכל מידע רלוונטי לאירוע במידת הצורך.

ניהול שינויים

- כל שינוי בקונפיגורציה, תוכנה או רכיב חומרה יחייב תיעוד ואישור מוקדם.
- חובה על שמירת גרסאות (version control) ושחזור מהיר במקרה של שיבוש.

התאוששות מאסון וגיבויים

- פתרון DRP מלא למערכת CMS וניהול טעינה.
- ביצוע גיבוי יומי של מידע קריטי.
- אחסון הגיבויים במיקום מאובטח שאינו נגיש למערכת הפעילה (offline\cold storage).

עמידה בתקנים ורגולציות

הספק יידרש להוכיח עמידה בתקן/הנחיות הבאות:

- ISO/IEC 27001 - אבטחת מידע
- ISO 27019 - אבטחת OT עבור מערכות תשתית חשמל
- NIST SP 800-82 - מערכותICS/SCADA
- תקנות הגנת הפרטיות - תיקון 13
- הנחיות משרד התחבורה בנושא תשתיות טעינה לרכבים חשמליים
- מדיניות מערך הסייבר הלאומי בנושא הגנת הסייבר למגזר התחבורה

התחייבויות הספק

- מינוי ממונה אבטחת מידע מטעם הספק.
- העברת תוכנית הגנת סייבר שנתית לאישור החברה.
- ביצוע מבדקי חדירה (Pen Testing) שנתיים במועד שיקבע ע"י נתיבי איילון, על רכיבי מערכת טעינה וניהול חניון (חומרה ותוכנה), ע"י מעבדה אשר אושרה מראש ע"י נתיבי איילון.
- טיפול בממצאי מבדקי החדירה בתוך פרק זמן שיוגדר ע"י נתיבי איילון ולשביעות רצונה.
- התחייבות לעמידה בכללי רגולציה לאומית ועדכון החברה בכל ממצא חריג.

סנקציות

- החברה שומרת לעצמה את הזכות להשעות שירות או לבטל התקשרות מול ספק במקרה של:
  - אי עמידה בדרישות אבטחה
  - הסתרת אירוע סייבר
  - כשל חמור בהגנת נתונים או שירותים

דרישות אבטחת מידע למערכת ניהול הטעינה החשמלית (Charging Management System – CMS)

מערכת ניהול הטעינה (CMS) הינה רכיב קריטי במערך התשתיות, האחראי לניהול, שליטה, תזמון, ניטור וחיוב של פעולות טעינה לאוטובוסים. לאור תפקידה המרכזי והחיבוריות שלה לתשתיות OT ו -IT, נדרשת הגנה ברמה גבוהה על כלל רכיביה.

ניהול גישה ואימות

- המערכת תאפשר ניהול הרשאות מבוסס תפקידים (RBAC).
- כל כניסה תדרוש אימות דו-שלבי (2FA/MFA) למשתמשים בעלי הרשאות ניהול.
- תנוהל ותתועד היסטוריית כניסות מלאה (audit log).
- לאף גורם לא תינתן הרשאת גישה למערכת ללא אישור מפורש, כל אישור יתועד באופן פרטני.

ממשקים ואינטגרציות

- כל ממשק בין מערכת ה-CMS לרכיבי OT, מערכות חיוב, מערכות ניהול חניון או שירותי ענן – יוגן בהצפנה חזקה.
- כל API חיצוני/פנימי יישם מנגנוני אימות rate limiting ו-logging.
- לא יתאפשר ממשק פתוח ללא הרשאה ואימות ברמת יישום (Application-layer authentication).

תיעוד ובקרת פעילות

- המערכת תחזיק מנגנון מובנה לניטור חריגות, התרעות בזמן אמת ודיווחים אוטומטיים.
- שמירת לוגים:
  - הפעלות/כיבויים של מטענים
  - שינויי תצורה
  - פעולות משתמשים בעלי הרשאות גבוהות
  - שגיאות מערכת או כשלי חיבור

מניעת שיבוש והונאה

- יש לוודא כי מערכת ה-CMS כוללת מנגנוני הגנה בפני:
  - מתקפות שליטה מרחוק (remote command injection)
  - מניפולציות על נתוני חיוב או צריכה
  - גישה לא מורשית לעמדות הטעינה דרך המערכת
- כל שינוי בפרופיל טעינה, הגדרה או תמחור – יחייב אישור כפול (dual control).

עדכונים והקשחה

- המערכת תיתמך בעדכוני אבטחה תקופתיים – אוטומטיים או מנוהלים לפי נוהל קבוע.
- כל התקנה של עדכון תתועד, תיבדק ותאושר ע"י ממונה אבטחת המידע.
- תבוצע הקשחת שרת/תחנה לפי סטנדרטים מקובלים וידועים (CIS Benchmarks, hardening guides).

גיבויים ושחזור

- גיבוי מלא של בסיס הנתונים והקונפיגורציה יבוצע אחת ל-24 שעות.
- הגיבויים יוצפנו וישמרו במיקום נפרד פיזית/לוגית.
- בדיקות שחזור (Restore Test) יבוצעו אחת לרבעון.

זמינות ושרידות

- תכנון תשתיתי לעמידות גבוהה:
  - תשתית HA/Failover למערכת הניהול
  - יכולת עבודה גם בעת ניתוק מהענן (Local fallback mode)

יש לקבוע מדדי RTO\RPO לשחזור המערכת בעת תקלה.

מערכות ניהול חיצוניות- תקשורת:

- גישה למערכות ניהול חיצוניות במרחב הרשתי באמצעות SIM, תתבצע באישור מקדים ועדכון המפעיל לקבלת הנחיות אבטחה משלימות מטעמו לצרכי הפעלה, בקרה ושימוש שוטף.
- במידה ועמדת-טעינה מתקשרת (באופן קבוע ו/או במצבים של פרקי-זמן כלשהם) עם מערכות ניהול בשרתים מרוחקים (מרחב WAN), על היצרן ליידע את המפעיל כבר בשלב של ההצגה הראשונית של נתוני/מאפייני העמדה ובמיוחד טרם התקנה, לקבלת הנחיות משלימות וקביעת ארכיטקטורה מתאימה.

- מבלי לגרוע מהאמור לעיל, במידה ועמדת-טעינה מחוברת למערכת ניהול חיצונית (מרחבי LAN/WAN), נדרשות בדיקות PT שנתיות עפ"י אפיון ודרישות המפעיל, ע"מ לוודא כי מדיניות האבטחה בהיבטי CS מתקיימת כנדרש באופן שוטף וכן תהליך עוקב לתיקון הליקויים.

עדכון גרסאות תוכנה:

- על היצרן ליידע את המפעיל טרם שליחת/ביצוע עדכוני גרסאות בעמדת-טעינה ובכל מקרה ללוות התהליך עם הנחיות רשמיות מטעמו.
- על היצרן לעמוד בדרישות 'אבטחת מידע' שיוגדרו ע"י המפעיל, לכל גרסה שתותקן.
- כל עמדות-הטעינה יעודכנו בגרסת מערכת זהה בכדי לייצר אחידות אבטחתית, תחזוקתית וניהולית.
- עדכוני התוכנה לעמדות-טעינה יהיו חתומים והמערכת תבדוק את חתימתם בעת ביצוע העדכון /
- עדכוני תוכנה לעמדות-הטעינה יבוצעו ע"י היצרן (מפעיל, בהתאם לסיכום ואכוונה מראש) ובכל מקרה, יתועדו ע"י המפעיל.

ממשקי-תקשורת פיזיים:

- על עמדת-טעינה לממש מנגנון בקרת-גישה לממשקי תקשורת פיזיים USB, ETH לחיבור רכיבים המאושרים אבטחתית ע"י המפעיל בלבד.

הזדהות למערכת ניהול הפנימית של עמדת-טעינה:

- נדרש ממשק הזדהות עם טוקן אבטחה ייעודי בעת גישה למערכת עם משתמש בהרשאות גבוהות (Root, Admin).
- יש לוודא קיומו של מנגנון וולידציה כי כל שימוש הינו בהתאם להרשאות לצורך הפעולה הייעודית הנדרשת.
- יש ליישם בקרה מפצה למתקפות Brute force על ממשקי הניהול של המערכת.