תשתיות מידע וטכנולוגיות בע"מ
יועצים לטכנולוגיית המידע ותשתיות הנדסיות
| משרד: 072-250.4385 | פקס: 072-250.7025 | נייד: 052-6704546 |
| ח.פ. 51377466-1 | ת.ד. 53035 ת"א | מיקוד 61530 | ezradyn@iti-il.com | www.iti-il.com |

07/09/2026

לכבוד
איגוד ערים אזור איילון

הנדון: הנחיית ספקים ליישום דרישות תקשורת ואבטחת מידע לטובת
הבטחת רציפות תפקודית של רשתות IOT

שלום רב,

1. מבוא

1.1. איגוד ערים איילון, (להלן המט"ש) נדרש להקים ו/או לשדרג מערכות מתח נמוך מאוד (להלן IOT) הנמצאים בתחום המט"ש. מערכות אלו נועדו לטובת בקרת מבנה (BMS), בקרת מערכות אנרגיה, אבטחה היקפית, ניטור פעילות ו/או לטובת פעילות הקשורה להבטחת תהליכי איסוף ו/או הטיפול בשפכים.

1.2. כחלק מהקמת / שדרוג מערכות אלו – מופעלות רשתות תקשורת ומחשוב המשולבות ברכיבי תקשורת, בקרים מתוכנתים, שרתים, מחשבים, סנסורים והתקני קצה הפועלים בפרוטוקולים Ethernet TCP/IP.

1.3. המט"ש מחויב לשמירה על דרישות אבטחת מידע ורציפות תפקודית שהוגדרו על ידי הנהלת החברה ובכפוף לדרישות הרגולציה – רשות המים ומשרד האנרגיה והנחיות מקצועיות של מטה הסייבר הלאומי.

2. עקרונות נדרשים ליישום

להלן הנחיות נדרשות בתחומי התקשורת, אבטחת המידע והרציפות התפקודית הנדרשים ליישום כחלק מתכנון או הקמה או שדרוג מתקן או מודול / יחידה תפעולית :

2.1. ארכיטקטורה והפרדת רשתות (Network Segmentation)

2.1.1. הפרדה מוחלטת בין IOT ל-IT : חובה לבצע הפרדה פיזית בין רשת המחשוב הארגוני (IT) לבין רשת הייצור / התפעול (IOT) המנהלת את המתקן.

2.1.2. רשת ה IOT תהיה מנוהלת באמצעות חומת אש - Firewall ייעודי לתעשייה

2.1.3. בידוד רשת ה IOT מהאינטרנט : הרשת תפעל במקטע רשת מאובטח ומבודד, ללא גישה ישירה מהאינטרנט.

2.1.4. חסימת פרוטוקולים לא מאובטחים : הגבלת השימוש בפרוטוקולי תקשורת תעשייתיים (כמו Modbus או DNP3) לרשת הפנימית בלבד, והצפנתם במידת האפשר.

2.2. ניהול גישה, הזדהות וגישה מרחוק (Access Control)

2.2.1. ניהול משתמשים מרכזי (Active Directory)

2.2.2. הפרדה מלאה בין משתמשי רשת ה-IOT למשתמשי רשת ה-IT של הארגון (אין Domain Trust בין ה-IT ל-IOT).

2.2.3. אימות רב-גורמי (MFA): חובה ליישם MFA עבור כל גישה מרחוק של עובדים, מנהלי מערכת או קבלני משנה/ספקים למערכות ה-VMS או ה-BMS.

2.2.4. ניהול הרשאות קפדני (RBAC): הגדרת פרופילי משתמשים לפי עיקרון "ההרשאה המינימלית הנדרשת" (Least Privilege). יישום באמצעות Active directory עצמאי ברשת המחשוב.

2.2.5. הקשחת סיסמאות ברירת מחדל: חובה לשנות את כל סיסמאות היצרן של המצלמות, המתגים, בקרי כניסה ובקרי גדר (DDC) ויחידות קצה (RTU) לפני חיבור הציוד לרשת.

2.2.6. מנגנון גישה מרחוק לתחזוקה (Secure Remote Access):

2.2.6.1. איסור מוחלט על גישה ישירה מהאינטרנט או שימוש בתוכנות שליטה מרחוק אזרחיות (TeamViewer, AnyDesk וכו').

2.2.6.2. גישה מרחוק תבוצע אך ורק דרך Secure VPN דרך ה-Industrial DMZ.

2.2.6.3. חובת אימות כפול (MFA - Multi-Factor Authentication) לכל מתחבר מרחוק.

2.2.6.4. הקלטת סשנים (Session Recording) וניטור פעילות קבלנים מרוחקים בזמן אמת.

2.3. ניטור, בקרה ודיווח אירועים

2.3.1. איסוף לוגים (Logging): הגדרת רישום פעולות מלא (Audit Logs) מכל רכיבי הקצה, השרתים, מערכות התפעול ומערכות הניהול באמצעות שרת איסוף לוגים מרכזי (syslog server).

2.3.2. חיבור ל-SOC / SIEM: שרת איסוף הלוגים נדרש להעביר את נתוני הניטור למרכז בקרה ואבטחה (SOC) לצורך זיהוי אנומליות בזמן אמת.

2.3.3. חובת דיווח: חובה לדווח באופן **מיידי** למנהל אבטחת מידע של איגודן על כל אירוע סייבר או חשד לשיבוש במערכות התפעוליות.

2.4. הגנת שרשרת האספקה וספקים חיצוניים (Supply Chain)

| משרד: 072-250.4385 | פקס: 072-250.7025 | נייד: 052-6704546 |
| ח.פ. 51377466-1 | ת.ד. 53035 ת"א | מיקוד 61530 | ezradyn@iti-il.com | www.iti-il.com |

2.4.1. גישה מאובטחת של נציג היצרן (Vendor Access): יצרני רכיבי מחשוב ו/או רכיבי בקרה תעשייתית המבצעים עדכוני תוכנה או ניטור מרחוק, מחויבים לעשות זאת דרך ערוצי VPN מוצפנים, מבוקרים ומוגבלים בזמן.

2.4.2. קבצי העדכון ייבדקו ברמת תקינות קובץ (File Integrity Check) יעברו הלבנה בעמדת הלבנה ככל שניתן יהיה להלבינם.

2.4.3. חתימה דיגיטלית לעדכוני קושחה (Firmware): מניעת התקנת עדכוני תוכנה שלא נחתמו רשמית על ידי היצרן ואומתו, כדי למנוע השתלת נוזקות (Malware) ברמת הרכיב.

2.5. הגנה פיזית על רכיבי המחשוב והתקשורת

2.5.1. נעילת ארונות תקשורת וחשמל: ארונות / מסדים בהם מותקנים רכיבי התקשורת, הבקרים, השרתים וכו', חייבים להיות נעולים פיזית בתוך מבנים או ארונות מוגנים, המנוטרים באמצעות מצלמות אבטחה וחיישני פתיחה (טמפר).

2.5.2. חסימת פורטים פיזיים: השבתת פורטים פנויים (כמו שקעי USB או פתחי רשת RJ45) על גבי הבקרים בשטח, כדי למנוע התחברות פיזית של גורם עוין.

2.5.3. חיישנים, רכיבי I/O מרוחקים (RIO) ומשדרי שדה בחצר (למשל על בריכות, משאבות או בורות חלוקה) יוגנו בתוך קופסאות זיווד מוקשחות (IP66 ומעלה) ומנעולים, למניעת חיבור פיזי ישיר לציוד השדה.

2.6. חוסן תפעולי והמשכיות עסקית (BCP/DR)

2.6.1. גיבויים מנותקים (Offline Backups): ביצוע גיבויים תקופתיים לקובצי הגדרה (Configurations) של מערכות הבקרה, קבצי קונפיגורציה של הבקרים, המתגים וציוד רשת, ותוכנות הניהול, ושמירתם באתר מנותק פיזית מהרשת.

2.6.2. מבדקי חדירות (Penetration Testing): ביצוע מבדקי חדירות תקופתיים (לפחות פעם בשנה או לאחר שינוי משמעותי במערכת) על ידי חברת אבטחה מוסמכת לבחינת עמידות הרשת.

2.7. ניהול עדכוני תוכנה ואבטחה (Patch Management במרחב IOT)

עדכון בתצורת Offline Patching Procedure:

2.7.1. הגדרת מנגנון לעדכון חתימות אנטי-וירוס, עדכוני מערכת הפעלה (Windows Updates) ועדכוני קושחה (Firmware) לציוד הרשת והבקרים ללא חיבור ישיר לאינטרנט.

2.7.2. תחנת הלבנה (Kiosk/Data Diode): דרישה לעמדת בדיקה והלבנה קיימת או ניידת (התקן USB מבוקר) עבור קובצי עדכון, קבצי קושחה וקונפיגורציות של הבקרים וקובצי תכנון המוכנסים למתקן.

2.7.3. בדיקות תאימות (Staging): חובה על הקבלן לבדוק עדכוני קושחה / תוכנה בסביבת בדיקה (Lab) לפני יישום ברשת הייצור במתקן.

2.8. שרידות חשמל, סביבה ואקלים (Power Resilience & Environmental)

2.8.1. מערכות הזנה ויתירות חשמלית (Dual Power / UPS):

2.8.1.1. דרישה לספקי כוח כפולים (Redundant Power Supplies) בכל ציוד המחשוב והתקשורת (שרתים, מתגים, חומות אש).

2.8.1.2. חיבור כל ארון תקשורת ובקרה למערכת אל-פסק (UPS) מנוהלת, המספקת גיבוי ל-30 דקות לפחות, כולל שליחת התרעת SNMP במקרה של מעבר לסוללה או כשל במערכת החשמל.

2.8.2. מיזוג והקשחה סביבתית:

2.8.2.1. מתגי תקשורת ובקרים בדרגה תעשייתית (Industrial Grade) העמידים בטווח טמפרטורות רחב ($-40°C$ עד $+75°C$) ועמידות בפני לחות וגזים קורוזיטיביים (כדוגמת H_2S במתקני ביוב).

2.9. בטיחות פונקציונלית והפרדה בין בקרה לבטיחות (Safety Domain Separation)

הפרדת מנגנוני בטיחות (Safety PLC / ESD):

2.9.1. במידה וקיימות במתקן מערכות חירום ובטיחות (Safety Systems), הקבלן יבטיח הפרדה מוחלטת בין בקר הבטיחות (Safety PLC) לבקרי מבנה ובקרות כניסה (DDC).

2.9.2. חסימת אפשרות לשינוי פרמטרי בטיחות דרך רשת התקשורת הרגילה או שרתי הניהול של המערכת.

3. הנחיות יישומיות

3.1. ניהול רכיבים (Asset Inventory):

3.1.1. הקבלן מחויב לספק קובץ ניהול תצורות מלא (Asset Register) הכולל: דגם, המספר הסידורי, גרסת Firmware, כתובת MAC, כתובת IP ומיקום פיזי עבור כל רכיב מחשוב/תקשורת/בקרה במתקן.

3.2. מקוריות הציוד ותמיכה (Supply Chain Security):

3.2.1. התחייבות הקבלן לרכישת ציוד מורשה בלבד דרך יבואנים רשמיים, כולל אחריות ותמיכה של היצרן (Vendor Support) למשך 3-5 שנים לפחות.

3.3. הקשחת ציוד מחשוב כדוגמת שרתי הקלטות (VMS), שרתי שו"ב ומתגי תקשורת מנוהלים

3.3.1. חסימה מוחלטת של שירותים ופרוטוקולים שאינם בשימוש (למשל: FTP, Web Server מובנה, Telnet, SNMP v1/v2).

3.3.2. שינוי מובנה של סיסמאות ברירת מחדל (Default Credentials) לסיסמאות מורכבות.

3.3.3. נטרול פורטים פיזיים לא בשימוש בבקר ובכרטיסי התקשורת.

3.4. הגנת גישה לקוד ולשינויים:

3.4.1. הגדרת הרשאות גישה (Read/Write) מוגנות סיסמה לרמת הפרויקט ברמת מערכת ההפעלה (Logic/Program Lock).

3.5. מחשבי מפעילים ותחנות עבודה (Windows PCs):

3.5.1. **הגנת עמדת קצה (EDR/EMS):** התקנת סוכן FortiClient EMS מנוהל מרכזית, כולל מנועי Antivirus, IPS, ובוחן תקינות (Compliance).

3.5.2. חסימת התקנים ניידים (Device Control): חסימה הרמטית של חיבור התקני אחסון USB חיצוניים (כוננים ניידים/דיסק און קי).

3.5.3. הקשחת מערכת הפעלה (OS Hardening): ביטול שירותים מיותרים, ביטול פרוטוקולים ישנים (NetBIOS, SMBv1), והסרת הרשאות Local Admin למפעילים.

3.5.4. GPO (Group Policy Objects): אכיפת מדיניות סיסמאות מורכבות, נעילת מסך אוטומטית (כעבור 5 דקות של חוסר פעילות), וביטול Autorun.

3.6. טופולוגית רשת, שרידות וסגמנטציה (Network Architecture)

3.6.1. טופולוגית רשת שרידה (Redundancy):

3.6.1.1. הקמת טבעת אופטית/אתרנט פיזית בתקן תעשייתי (כדוגמת ERPS / IEC 62443-4-2 / MRP) בזמן התאוששות של פחות מ-20ms במקרה של ניתוק סיב.

3.6.1.2. כבילה כפולה (Path Diversity) במסלולים פיזיים נפרדים בין ארונות תקשורת למניעת קיטוע בודד (Single Point of Failure).

3.6.2. סגמנטציה לפי מודל Purdue Zones and Conduits :

3.6.2.1. רמה 0/1 : Process/Control Zone - רשת ייעודית למצלמות, בקרי כניסה, בקרי BMS מבוססי רכיבי I/O).

3.6.2.2. רמה 2 : Control Zone - רשת נפרדת למחשבי מפעיל.

3.6.2.3. רמה 3 : Site Management - שרתי ניהול מקומיים (AD, VMS, Syslog, Storage).

3.6.2.4. DMZ תעשייתי (Industrial DMZ) : שכבת חיץ המפרידה לחלוטין בין רשת ה-IOT לרשת ה-IT המופרדת על ידי רכיב חד כיווני (דיודה).

3.6.3. אמצעי הפרדה לוגיים ופיזיים :

3.6.3.1. חלוקה ל-VLANs נפרדים לכל שכבה (IOT Control, VMS, Building Management).

3.6.3.2. מעבר בין VLANs יתבצע אך ורק דרך חומת אש תעשייתית מרכזית (Industrial Firewall).

3.6.4. אמצעי הגנה על רשת התקשורת (Network Security)

3.6.4.1. אבטחת פורטים וגישה פיזית (Port Security) :

3.6.4.2. הגדרת Port Security במתגים (חסימת פורט בעת חיבור כתובת MAC לא מוכרת).

3.6.4.3. נעילת פורטים פיזיים שאינם בשימוש ברמת התוכנה (Admin Down) ונעילתם פיזית בארונות.

3.6.5. חומת אש תעשייתית (NGFW / Industrial Firewall) :

3.6.5.1. הפעלת מנוע DPI (Deep Packet Inspection) המזהה פרוטוקולי בקרה תעשייתיים (Modbus TCP, IEC 60870-5-104, S7, ADS).

3.6.5.2. אכיפת מדיניות Default Deny (כל מה שלא הוגדר במפורש כספציפי ומורשה – נחסם).

3.6.6. סנכרון זמן ואירועים :

3.6.6.1. הקמת שרת זמן מרכזי (NTP) ברשת ה-IOT לצורך סנכרון שעונים של מתגים, בקרים, חומות אש ושרתים.

3.6.6.2. העברת לוגים בזמן אמת (Syslog/SIEM) מכל הרכיבים לשרת ניהול אירועים.

4. מנגנון גיבוי אוטומטי (Automated Backup):

4.1.1. גיבוי תוכנות ושינויים: מערכת גיבוי תקופתית אוטומטית לקבצי הקונפיגורציה וסקריפטים של המערכת.

4.1.2. גיבוי שרתים ותחנות: גיבוי יומי מלא (Image-based Backup) של כל ה-VMs, שרת ה-AD, שרת ניהול בקרות כניסה, ניהול גדר אינדוקטיבית וכו'.

5. אחסון גיבויים והתאוששות לאחר כשל במערכת IOT

5.1. שמירת עותק גיבוי אחד לפחות באופן מבודד פיזית ובלתי ניתן לשינוי (Immutable / Air-Gapped Backup), המוגן מפני מתקפות כופרה (Ransomware).

5.2. נוהל התאוששות מכשל במערכת: הקבלן מחויב לספק קובצי Image מוכנים לפריסה מהירה (Bare-Metal Restore) ודף הנחיות התאוששות המאפשר שחזור מלא של המערכת לאחר כשל.

6. תהליכי מסירה ותוצרים נדרשים מהקבלן

6.1. מסמכי אדריכלות רשת (HLD / LLD): שרטוט טופולוגיה מלא כולל IP Schema, סגמנטציה VLANs, ומטריצת פורטים/פרוטוקולים בחומת האש.

6.2. מסמך אישור ביצוע הקשחה: אישור חתום על ביצוע הקשחה לכל תחנות העבודה, השרתים, וציוד ה IOT (מצלמות, בקרות כניסה, BMS וכו').

6.3. תוכנית בדיקות קבלה (ATP): ביצוע בדיקות קבלה מקיפות בשטח, כולל תרחישי כשל (כגון ניתוק סיב, ניתוק ספק כוח, נפילת שרת, וניסיון חיבור התקן בלתי מורשה).

6.4. תיק גיבויים ראשוני: מסירת מדיה פיזית (כונן מוצפן) הכוללת את כל האימג'ים וקונפיגורציות של ציוד הרשת והבקרים במצב Clean & Working.

6.5. תיק אתר As-Made: מסירת תיק מתקן מלא הכולל מדריכי טיפול בתקלות והתאוששות מאסון ברורים בשפה העברית.

בברכה,

עזרא דיין – יועץ
תשתיות מידע וטכנולוגיות בע"מ