סייבר ישראל
מערך הסייבר הלאומי

המלצות הגנת סייבר

על מערכות כיבוי וגילוי אש

הגנה על מערכות גילוי וכיבוי אש ממוחשבות מבוססי IoT במבנים גבוהים, במבנים רגישים או קריטיים

נובמבר 2020

תוכן עניינים

1. מבוא

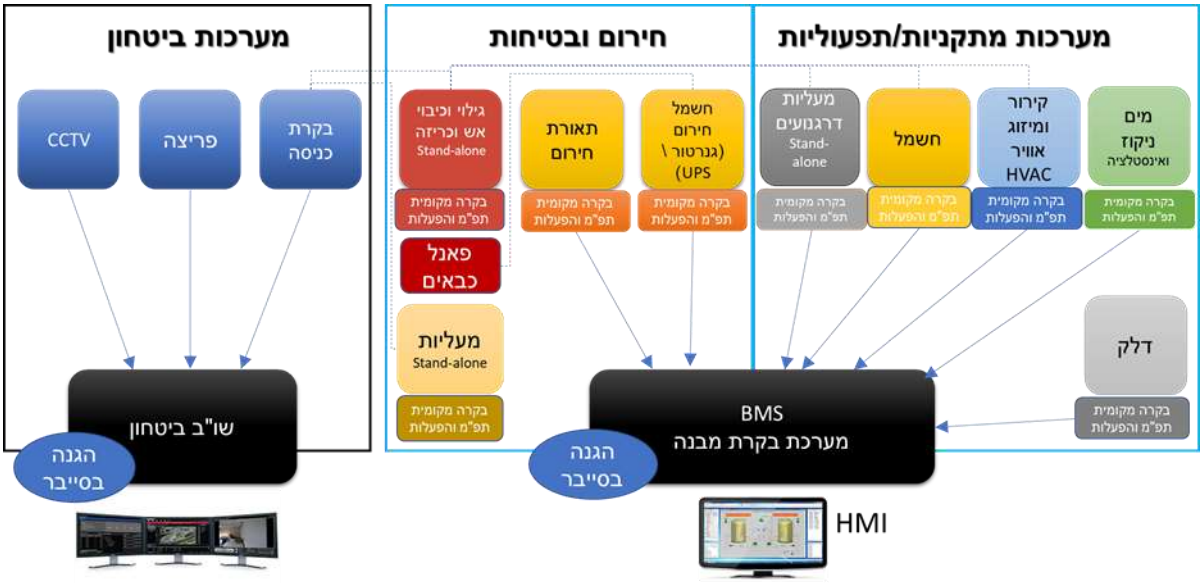
מערכות גילוי וכיבוי אש הינן מערכות ייעודיות, המסייעות לגילוי ונקיטת צעדים למזעור נזקים, בטיחות והבטחת שלום הדיירים (Wellbeing). המערכת מורכבת מגלאיי ניטור, **רכזת** (דיגיטלית הבודקת על בסיס קבוע את תקינות הגלאים) המקבלת את קריאות ה**גלאים** ומתזמנת בהתאם את ההתראה והתגובות למקרי השריפה. סוגי הגלאים הפופולרים הם גלאי עשן, גלאי חום, גלאי להבה וגלאי פחמן דו חמצני. הרכזת היא מוח המערכת והיא מספקת את **התראת** השריפה. מערכות גילוי אש מתקדמות משלבות יכולות של כריזה דיגיטלית והזעקת כוחות הכיבוי. היעילות בשימוש במערכות הגילוי והכיבוי מתבטאת ביתר שאת בקומות גבוהות ואזורים בהם ייתכנו עיכובים או מכשולים לכוחות ההצלה וכן במבנים רגישים. השימוש בטכנולוגיות מבוססות IoT מגבירות את היעילות בהצלת חיים ותקשורת בזמן חירום.[1] פגיעת סייבר יכולה להוביל לפגיעה במערכות חיוניות להצלת חיים, בבטיחות הדיירים והשוהים, בהלה, יצירת כאוס ופגיעה בסדר הציבורי.

לעיתים, מערכות גילוי האש הן חלק ממערכת ניהול מבנים חכמים Building Management System (BMS).[2] מערכות ה- BMS מאפשרות שליטה רחבה על מערכות המבנה לרבות שליטה על המעליות, תאורה, מיזוג, מערכות כיבוי אש, מצלמות אבטחה ועוד. היכולת לשלב מערכות אוטומציה לשליטה ובקרה על מערכות הבניין מאפשרת בין היתר קישוריות, יעילות וחסכון. במקרים אחרים המערכת היא מערכת אוטונומית ללא תלות ברשת הארגונית. שילוב מערכות אלו טומן בחובו גם סיכוני סייבר. הידע, הפוטנציאל והיכולות לנצל חולשות ופרצות אבטחה קיימים והם תלויים בעיקר במוטיבציה של התוקף ורצונו לממש תקיפות אלו לצורך ביצוע מניפולציות או השבתת המערכות ממניעיו השונים. תרחישי תקיפה אלו מכוונים גם לתשתיות קריטיות ומבנים רגישים (כגון שדות תעופה, בתי חולים, משרדים ממשלתיים וכדומה) תוך מטרה לפגוע בתקשורת בין מערכתית, שיבוש נתונים או פגיעה בסדר הציבורי.
העובדה כי מערכת גילוי וכיבוי אש הינה חלק מתוך מערכת ה- BMS מגדילה את מרחב הסיכונים מהרשת למערכות ה- BMS ולחילופין, בהיעדר בידול פיזי או לוגי היא מייצרת דרך פעולה אפשרית (דפ"א) לתקיפת הרשת בהתקפה שתגיע מרכיבי מערכת הגילוי או הרשת הייעודית.

---

[1] חיוני במיוחד בהתחשב בעובדה שצוותי כיבוי רבים, כמו באסונות 11/9 , התלוננו על תקשורת סלולרית שקרסה, מה שהכביד את זמני התיאום והתגובה

[2] https://www.gov.il/he/departments/general/buildingmng



איור 1: ארכיטקטורה אפשרית לבידול פיזי או לוגי במערכת BMS

2. מטרת המסמך

הגנה על מערכות האש בהיבטי יתירות ושרידות בתנאי סביבה וסייבר הינה הכרחית כחלק מתהליך מבטיח למניעת פגיעה פונקציונאלית במערכות מצילות חיים. הגם שההמלצות מתאימות למערכות אלו באשר הן, בין אם מבנים קרקעיים/תת קרקעיים הנחת העבודה היא כי, מערכות אלו **בבניינים גבוהים** כמו גם תשתיות קריטיות ו**מבנים רגישים** הינן חיוניות ובהתאם לכך, תשומות ההגנה מכוונות בעדיפות גבוהה. מטרת המסמך היא לספק קווים מנחים לצמצום משטח התקיפה על מערכות ממוחשבות לגילוי האש ורכיבי הקצה תוך מתן דגשים עיקריים להגנה על הרשת. זאת על ידי ביצוע פעולות ובקרות להקשחת תשתית הרשת ולהגנה על פונקציונליות התפעול של המערכת והרכיבים בכדי לספק את ההגנה המתאימה על הרשת.

3. קהל היעד למסמך

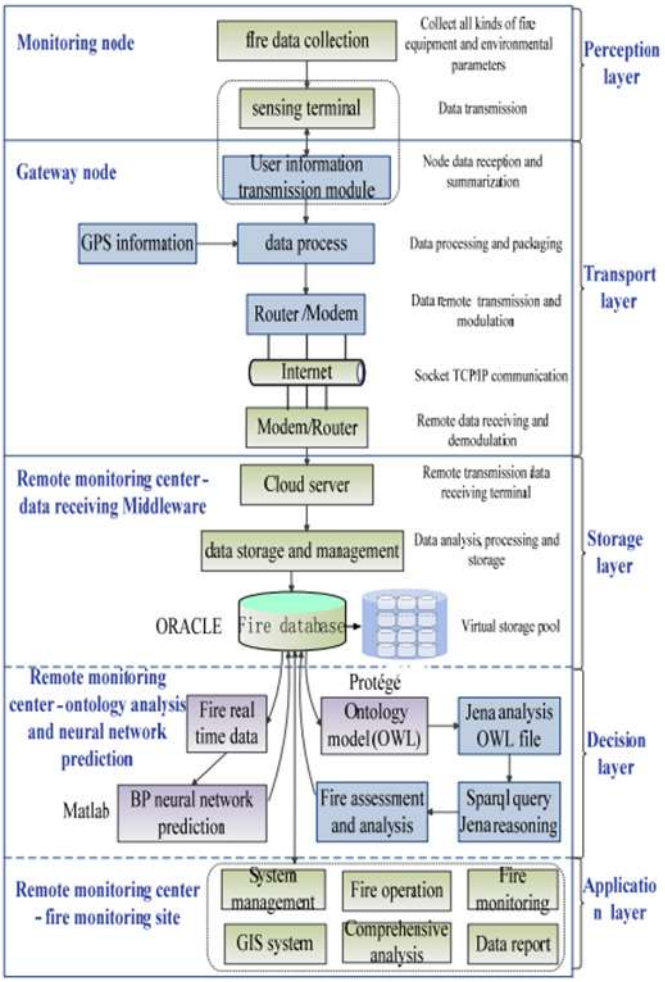
המסמך מיועד לסייע לארגונים ולמשתמשים לצמצם סיכוני סייבר על ידי שילוב הגדרות ובקרות הגנה למערכות הבקרה הרכיבים והמערכות הנלוות לגילוי וכיבוי אש. בתוך כך, מכוון המסמך גם למנהלי הגנת הסייבר (CISO), גורמים ארגוניים האמונים על ארכיטקטורת הגנה בסייבר/טכנולוגי הגנה בסייבר, מיישמי הגנת סייבר (Cyber Security Practitioners) וצוותי ה - SYSTEM, מנהלי ביטחון, מפעילי מערכות בקרת המבנה וגורמים האמונים על הבטיחות והבטחת שלום

הדיירים. המסמך יכול להוות גם כמצע לדרישות אבטחה מיצרנים וספקים לסקטור הכבאות וההצלה בתחום מערכות ובקרים לגילוי אש.

איור 2: רכזת אחודה - מערכות כיבוי אש

4. ניהול סיכוני סייבר במערכות בקרה לגילוי אש

מערכות ה- **Building Control System** הינן מערכות שליטה ופיקוח מכני וחשמלי של הבניין, הכוללות: אוורור, תאורה, מערכות חשמל, **מערכות כיבוי וגילוי אש** ומערכות אבטחה. מעבר לעובדה כי מערכות אלו מושתתות על בקרים וחיישני שטח, לרוב וכחלק משילוב יכולות מתקדמות, מבוצע גם שימוש ברכיבי IoT פופולריים במערכות מבנה. השימוש ברכיבים אלו, מאפשר חיבור ופנייה לאינטרנט, פונקציונאליות ויכולות חכמות מתקדמות נוספות כדוגמת: דיווח מיקום מדויק בבניין, קצב ההתפשטות, הקפצת כוחות הצלה והמשך שידור נתונים מהזירה, לרבות תרשימים ומיקומים שיאפשרו לצוותים לנתח לפני הגעת הצוותים לזירת האירוע.



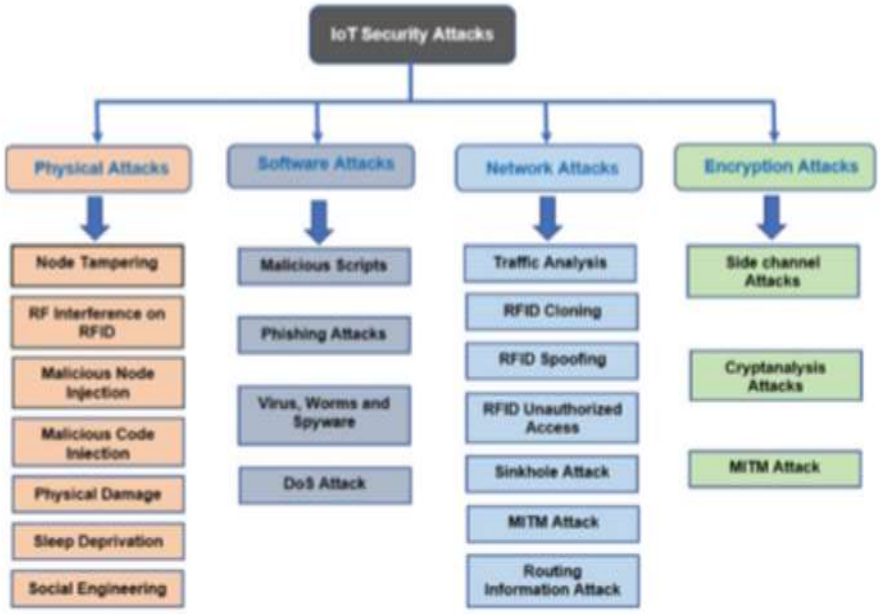
איור 2 -תיאור ארכיטקטורת תהליכים ברכיבי גילוי אש המבוססי IoT[3]

המידע המעובד במערכות זמין וחשוף לסיכוני סייבר. מערכות בניין המבוססות על IoT לרבות מערכות הצלה וכיבוי אש, מחוברות גם לאינטרנט. חיבור זה ברמת הרשת וברמת הרכיבים (כל שכן כשמדובר בשלל רכיבים זעירים משלל יצרניות) לא תמיד מוגן או כולל הגדרות אבטחה. ככזה הוא חשוף ללא מעט סיכוני סייבר ומניפולציה, הוא עלול לסכן ולפגוע באופן הטיפול באירוע כמו גם להסב נזק למערכות המידע, תשתיות המחשוב והרכש. היכולת לתקוף ולבצע מניפולציות על רכיבי IoT ושינוי נתונים ופונקציונליות הוכחו בלא מעט מחקרים ומאמרים. בתוך כך, התקפות , בערוץ סיסמאות DEFAULT המתבססות בין היתר על עיון במפרטי היצרן - הובילו לפריצת לא מעט מכשירים מבוססי IoT.[4] התקפות אפשריות נוספות כנגד הרכיבים הן בציר של התקפות הרכיבים

[3] Developing a Fire Monitoring and Control System Based on IoT - Jianjun Yi

[4] https://www.researchgate.net/publication/341843309_Recurrent_GANs_Password_Cracker_For_IoT_Password_Security_Enhancement

לצורך יצירת עומס ותקיפות DDOS. זאת על ידי חיבוריות רכיבי ה- IoT לתוכנות (Botnets) השולטות ומקשרות בין הרכיבים ליצירת פנייה לשרתי הארגון או מחוצה לו.[5]יכולות תקיפת הסייבר הינן מגוונות כגון: התקפות כופר, השבתה והרס, פגיעה בחשאיות וזמינות הנתונים (בהתאם למודל ה- CIA).



איור 3- מגוון שיטות תקיפה בפילוח לפי: התקפות פיזיות, תוכנה, רשת ויחידת קצה[6]

השימוש בבקרים והקישוריות לרשת (לרבות רשתות האינטרנט ושימוש בטכנולוגיות IoT) מעלה גם את סיכוני הסייבר (לרבות SCADA) ומניפולציות אפשריות האפשריות.[7] החל מפעילויות של פגיעה בזמינות המערכת (DDOS למשל) עובר בפגיעה ברכזת על ידי הזנת נתונים כוזבים אודות מצב המערכות, הפעלה כוזבת של מערכות ההתראה והחיווי, נטרול המערכת, הקפצת כוחות הצלה לצורך יצירת כאוס, בהלה ובלבול. תהליך זה הינו מורכב, והוא מחייב תהליך ניהול סיכונים המשלב את התהליכים הבאים:

---

[5] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[6] https://www.researchgate.net/publication/332859761_IoT_Security_Privacy_Safety_and_Ethics/download - IoT Security, Privacy, Safety and Ethics -Hany F. Atlam and Gary B. Wills

[7] https://drum.lib.umd.edu/bitstream/handle/1903/16803/Wills_umd_0117N_16267.pdf?sequence=1&isAllowed=y
https://books.google.co.il/books?id=bIqPDQAAQBAJ&pg=PA65&lpg=PA65&dq=FIRE+CONTROL+SYSTEM+CYBER+SCENARIO&source=bl&ots=cP-0Fnoyhr&sig=ACfU3U3iJY_zQE0KOt9LjfV_2-9YCFWkfA&hl=iw&sa=X&ved=2ahUKEwiWwoH2w8nqAhVN3aQKHUCYCbUQ6AEwAXoECAsQAQ#v=onepage&q=FIRE%20CONTROL%20SYSTEM%20CYBER%20SCENARIO&f=false

4.1 **סקירת מערכת כללית** - לרבות ארכיטקטורה, שמות מערכות, מדריכים, ספק, סקירה כללית של כל הקודים, התקנים, שיטות העבודה המומלצות ומדריכי המערכת. אלו יאפשרו לרכז ולהצביע על איומי סייבר, כשלים וחולשות אפשריים לניצול.

4.2 **פגישות עם גורמים תפעוליים, עסקיים וטכנולוגיים לצורך ניתוח תהליכי עבודה, זיהוי ומיפוי סיכונים**

4.3 **הגדרת מערכות או רכיבי גילוי וכיבוי אש החשופים לסיכוני הרשת**

4.4 **תהליכים להפחתת הסיכון -** שיוך בקרות, מבנה מערכת, וארכיטקטורת רשת תומכת

לעיתים קיימת העדפה פונקציונלית תוך פשרה בשימוש במכשירי IoT במערכות תפעוליות. עם זאת ההיתכנות, האטרקטיביות וקלות המימוש שהוכחו בלא מעט דו"חות ומחקרים מעלים את הצורך לשינוי תפיסה אבטחתי גם באופן הרכישה, ההטמעה והמענים האבטחתיים במערכות גילוי אש, פריסתם במבנה וחיבורם לרשת. בין היתר דרישות אל מול היצרנים כבר בשלבי הפיתוח, ההצטיידות ולכול אורך מחזור חיי הרכיב (Product Life Cycle).[8]

[8] http://www.opengroup.org/iot/iotwp/p2.htm

5. המלצות לבקרות לצמצום סיכוני סייבר במערכות גילוי אש

הגנת סייבר על מערכות גילוי אש כוללת בקרות ייעודיות להגנה על מערכות הבקרה, בקרים, תצורת מצב העבודה של חיישנים (NORMALY NORALY CLOSE\OPEN) ושימוש ברכיבי IoT והקישוריות לרשת. הגם שישנן מס' בקרות המתייחסות גם לטופולוגית הרשת, אין מעניינו של מסמך זה לדון על הקשחת תחנות הקצה, השרתים וכדומה. השימוש בבקרים ורכיבי IoT והחיבוריות לרשת חושף את הארגון לסיכוני סייבר ומחייב נקיטת תשומות ובקרות הגנה במטרה למנוע התקפה כנגדם או באמצעותם (לדוגמא אירוע בו משמשים הרכיבים ליצירת פניות ועומס על השרתים או התקפות כופר). באוריינטציה של רשת המשלבת רכיבי IoT ובקרים, כול שכן בקרים מבוססי IoT, יש לזכור כי לא קיימת טכנולוגיה יחידה כלשהי שישימה עבור כול סוגי המערכות ולכן קיימים פערי אבטחה בין המוצרים שיכולים להשליך על רמת האבטחה הכללית. עובדה זו, מקשה על יצירת סטנדרטיזציה וניהול רכיבים אחיד. בהתאם קיים צורך בהגנה ומימוש ברכיבים ובסביבותיהם תוך שילוב בקרות שונות (מדיניות, טכנולוגיות, ארכיטקטורה, פיזיות וכו'). ההגנה היא גם בהגדרות המימוש ברכיב עצמו (ככול שניתן) אך היא נשענת גם על דרישות בהגנת הרשת והקשחת סביבות המחשוב ותחנות הקצה אליהם מחובר הציוד.[9]

בנק הבקרות המובא בטבלה הינו ייעודי ומתאים לסביבות ומערכות גילוי אש. הבקרות מכוונות לרכיבים, לסביבות הממוחשבות למערכות המתממשקות ולטכנולוגיות. ישנן בקרות שחלות על היצרן, הספק או האינטגרטור ועל הארגון לוודא קיומם של דרישות אלו בתהליכי האפיון ודרישות ההצטיידות ולהבטיח כי אלו מיושמות בתהליך ההתקנה וההטמעה (בין אם מדובר במערכת אוטונומית ובין אם מתממשקת לרשת הארגון). הצלחת היישום וההטמעה של בקרות האבטחה לצמצום הסיכונים תלויה בארגון. בחירת הבקרות חייבת להתבצע בסינרגיה מלאה אל מול דרישות **ופונקציונאליות הרשת והרכיבים, תוך הימנעות מפגיעה בזמינות אמינות, שלימות הנתונים ובטיחות.**

---

9 https://www.gov.il/BlobFolder/policy/endstation/heי%20סיכוני%20לצמצום%20הגנה%20המלצות/בר-הנגשה%20סופי.pdf

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.1	**מדיניות הגנה על מערכות בקרת גילוי האש**	יש לכתוב, לנהל ולבקר מדיניות ארגונית להגנה על המערכות (הרשת, הבקרים והגלאים)	יש להתייחס גם לתהליכי רישום מסודר, להיבטים רגולטוריים, הסדרת גורמי אחריות, חלוקת אחריות וכדומה יש לתקף מדיניות זאת אחת לשנתיים
5.2	**מדיניות הגנה למערכות בקרת גילוי אש**	יש להגדיר כללי שימוש נאות בציוד ולהשתמש במדבקות ייעודיות על הרכיבים וכן שילוט מתאים בסביבות הרכיבים הכוללים הסברים אלו	המדבקה (מתאימה לתנאי הסביבה) תכלול את מדיניות השימוש ברכיבים אלו (כדוגמת איסור שימוש חיבור מדיה נתיקה)
5.3	**תהליך הקשחת הבקרים**	יש להטמיע תהליך מובנה להקשחת הבקרים בהתאם להמלצות היצרן ותקינות בינלאומיות עם קבלה והטמעת השימוש	- **התאמה לדרישות UL2900** - יש להבטיח עדכון רכיבים בגרסאות - הקשחת מערכות ע"פ סטנדרט היצרן

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.4	**תיכנון וארכיטקטורה - הגנה על הרשת**	יש לנקוט תשומות לתכנון מאובטח של רשת המערכת תוך תשומות מתאימות למניעת פגיעה וצמצום משטח התקיפה ברשת על ידי ניצול חולשות הבקרים לצורך תקיפת הרשת וכנגדם	בחינת אפשרות לבידוד רשת מערכת לגילוי אש ב- VLAN ייעודי **מנוהל** לצמצום ניצול מרחב תקיפה מבוסס וכן אפשרות ויכולת ניטור לסביבה זו. לחילופין, בידוד אזורים במקרים של התקפות סייבר (כופר וכדומה) **סביבה זו תאפשר גם יכולות ניהול וניטור באמצעות מערכת SIEM לאירועים ולוגים שיועברו מהרכזת (יישום כלים כגון IPS,IDS)** אפשרות נוספת היא שימוש במערכות אוטנומיות שאינן נשענות על הרשת הארגונית (תוך מימוש בקרות המתאימות)

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.5	**השבתת יציאות וחיבורי רשת**	יש לבחון וליישם השבתת יציאות ו / או חיבורי רשת ספציפיים מרכיבי ה- IoT (לרבות רכיבים אוטונומיים) לקישוריות סלקטיבית ברשת הארגונית ורשת האינטרנט	וידוא כי הספק מספק הנחיות למניעת תקשורת זו + וידוא תשומות מתאימות בזמן ההתקנה
5.6	**תיכנון וארכיטקטורה - הגנה בתקשורת אמינה ומאובטחת ברשת ובין הרכיבים**	יש להשתמש בתקשורת אמינה ומאובטחת בין רכיבי ה- IoT, לרשת הארגונית וביניהם , שימוש בחיישני מערכת אנלגיים בתצורת מגע יבש - IO אנלוגי או דיגיטלי	גרסאות מאובטחות עדכניות בפרוטוקולים מאובטחים (HTTPS, , LwM2M SNMPv3 , MQTTוכו') - יש לעקוב אחר גרסאות חדשות בהתאם להתפתחות הטכנולוגיה יש לוודא כי אין פגיעה פונקציונאלית (לרבות האטת זרימת נתונים) בזמינות הנתונים, שלמות הנתונים אמינות ובטיחות

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.7	**תשומות הגנה פיזית ומניעת חבלה ברכיבים**	יש לוודא תשומות מתאימות למניעת חבלה ומניפולציה (כדוגמת השבתה ושינויים) לרבות התמודדות עם האיום הפנימי.[10] זאת, בדגש על הפיזור הגיאוגרפי של הרכיבים בסביבות פריסת המערכת	ניתן לשקול חוקיות לפיה כאשר מתבצע ניתוק מהרשת הארגונית או מהתווך הרצוי, יש לחולל התרעה (בשל שיקולי בטיחות יש להימנע מבידוד הרכיב מהרשת)
5.8	**בידוד קודים ונתונים חסויים**	רצוי, להעדיף רכיבי IoT אשר מבודדים קודים, תהליכים ונתונים חסויים, שמקורם בתהליכים בחלקים של הקושחה ואשר צורך בגישה אליהם מחייב תהליך הזדהות	כולל נקיטת תשומות למניעת יכולת לגישה לא מורשית לביצוע שינויים, כיבוי או מניעת פעילות תפעולית רצויה.
5.9	**בדיקת פונקציונאליות**	הטמעת מערכת רישום הרושמת אירועים ומצליבה בין הפונקציונאליות והנתונים הקיימים והמופקים	לדוגמה: התרעה בעת החלפת רשת, שינוי נתונים וכדומה. יש לשמור את היומנים גם באחסון עמיד ויכולת שיחזור (למניעת מניפולציה ושינויים יזומים)

[10] https://www.gov.il/BlobFolder/generalpage/coping_thret/he/Organizational_coping.pdf

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.10	**צמצום משטח תקיפה בסיסמאות**	יש לוודא החלפת סיסמאות לרכזות והמערכות הנלוות יש לוודא תשומות מתאימות למניעת אירועי בטיחות בשל בקרה זו.	- החלפת סיסמת טכנאי. לשם מתן אפשרות לגישה בחירום במקרה של אובדן סיסמה, **יש להציע מנגנון איפוס על בסיס נגישות פיזית מקומית** - לחילופין ניתן להציע מנגנון זכוכית ששבירתו תאפשר גישה מהירה מחד ואינדיקציה מאידך - במידה ולא ניתן להתפשר על החלפת סיסמת יצרן במערכות מצילות חיים יש לוודא ולהבטיח מניעת קישוריות רציפה לאינטרנט במטרה למנוע יכולות תקיפה מזירת האינטרנט (כדוגמת מנועי Shodan) - דיווח (הימנעות מנעילה והשבתה) על ניסיונות/ניחוש סיסמה כושלים

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.11	**מניעת גישה לא מורשית**	לצד התשומות הלוגיות יש לנקוט גם תשומות פיזיות למניעת גישה לא מורשית או ביצוע מניפולציות, בסביבות הרכיבים לרבות שיבושים טכנולוגים באמצעות התקפות SIDE CHANNAL ATTACK[11]	- התאמת מענה ההגנה הפיזית ובקרות מפצות לסביבת המערכת ורכיבי המערכת בפריסה בשטח העבודה
5.12	**מניעת יכולת הזרקת קבצים**	מניעת יכולת הזרקת קבצי XSS, CSRF, SQL	כחלק ממניעת שאילתות לשליפת נתונים
5.13	**עדכוני תוכנה**	הארגון ישלוט בתהליך עדכוני התוכנה בפרקי זמן סבירים שיוגדרו במדיניות הארגון או ע"פ התכיפות. במטרה לצמצם סיכונים הנובעים הנובעים בתוך לרבות MITM ותהליכי מניפולציה על המידע	יש לתאם הליך העברת עדכונים באופן מאובטח לארגון או לרכיב ה- IoT ישירות (זאת לאחר השוואת חתימות הקבצים - ראה פירוט בקרה לתהליך OTA). ככול שניתן: רצוי לבצע את הפצת העדכונים באמצעות שרת ייעודי בארגון. זאת, לאחר תהליך קבלת קבצי העדכונים ובדיקת חתימות מול הספק/יצרן

information.bris.ac.uk/files/210500367/Final_Copy_2019_03_19_Yan_Y_PhD.pdf

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.14	**עדכוני תוכנה**	תהליך מאובטח לעדכון תוכנה **Over-The-Air (OTA)**	-וידוא קבלת הקובץ ממקור מהימן ומשרת מאובטח -העברת קובץ העדכון בתהליך מאובטח ומוצפן -בדיקת אותנטיות בחתימת קבצים (אימות אישור קובץ חתימה) יש לדרוש מהספק עדכוני אבטחה לליקויים חמורים שמתפרסמים
5.15	**עדכוני תוכנה**	שמירת גרסת קושחה אחרונה והגדרות תצורה כחלק מתהליך של שיחזור גרסאות יצרן (משבר/אירוע סייבר והתאוששות מתקלה או אסון)	יש לבצע ביקורות תקופתיות להצלבה בין הגרסאות שקיימות והרפרנס האחרון

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.16	**סביבת תמיכה וטסטים**	יש להקצות סביבה ייעודית (מחשב יעודי , רשת מבודלת מהרשת הארגונית, או גישה מסגמנט ניהול יעודי) לצורך תהליך תמיכה, טיפול בתקלות ותמיכה בתקלות ברכיבים	- תהליך התמיכה יתבצע באופן מבוקר ומנוהל על ידי הצוות המקומי - יוקצה סשן זמני לתהליך התמיכה מרחוק - החיבור לסביבת התמיכה יהיה יזום (על ידי הלקוח/הארגון) ויחייב אוטנתקציה מבוססת 2FA/MFA - לפני החזרת הרכיב או השינוי לרשת יש לוודא עמידה במדיניות ובבקרות
5.17	**רידוד מידע**	שימוש ברכיבים בעלי יכולת פונקציונלית למחיקת מידע ונתונים גולמיים (כהגדרת - DEFULT) לאחר שימוש ותהליך העיבוד או בעת החלפת רכיב	

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.18	**רידוד מידע לשאילתות וזיהוי הרכיבים ברשת**	בחינת מיידעים מזהים היוצאים לרחבי האינטרנט ובחינת חלופות לשינוי לצורך הקטנת וצמצום מרחבי התקיפה	לדוגמא להקשות איסוף מודיעין ויצירת קושי לחיפוש במנועי אינטרנט לפי שם יצרן, שם רכיב (שינוי שם רכיב) ,סיסמאות ברירת מחדל וכדומה[12]
5.19	**פנייה לרשת**	השבתת יכולות פנייה לקישורים סלקטיביים	למניעת שינויים פונקציונאליים, לרבות מידע על מבנה ומיקומים
5.20	**תשומות למניעת סיכוני סייבר מרכיבים אוגרי מידע**	יש לנקוט בבקרות מתאימות לצמצום סיכוני סייבר בתהליכי התחברות לא מורשים לשקעי ה- USB במערכת ולרכיבי IoT	ניתן ליישם חסימה לוגית או פיזית על הרכיב. למניעת אפשרות של החדרת קוד עוין ומניפולציה על הרכיב והמידע
5.21	**הקצאת תשומות סריקה מפני פוגענים (בחיבור רכיבים לרשת הארגונית)**	יש לוודא תהליכי סריקה בציוד הייעודי. וכן, תהליכי תחזוקה של עדכוני טלאי אבטחה יעודיים ושל מערכות הגנה נלוות כגון אנטי-וירוס	מומלץ להשתמש ולהתקין ולעדכן גרסאות מערכת אחרונות ובנוסף את מערכת אנטי וירוס בהתאם להוראות היצרן (למניעת פגיעה בביצועים או בפונקציונליות המערכת)

[12] https://www.comparitech.com/blog/vpn-privacy/emove-deviceshodan/

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.22	**צמצום סיכוני פגיעה בתהליכי עבודה**	וידוא תהליכי עבודה ויישום הגדרות המבטיחות מניעת פגיעה בתהליכי עבודה קריטיים ברשת, תהליך תפעול, ישויות, בטיחות, אמינות או פרודוקטיביות של הארגון	כדוגמת יישום הגדרות מתאימות ברכיב וברשת המבטיחות כי לא יתבצעו מניפולציות על הרכיב לצורכי העמסת מידע ומניעת שירות (ראו גם בקרה להתמודדות עם התקפת DDOS)
5.23	**תשומות לצמצום סיכונים ברכיבי IoT**	יישום מנגנוני אבטחה לרשתות האלחוטיות בהתקנה ב- VLAN ייעודי ונפרד משאר המערכות וכן כיול עוצמת השידור של האות האלחוטי באופן שהאותות לא יקלטו ברדיוס רחב מחוץ למבנה/קומה	יש ליישם מנגנוני אימות והזדהות רכיבים ומכשירים ברשת ולהגביל את השירות לגורמים המורשים בלבד. אחת לתקופה תתבצע החלפת סיסמאות כחלק מתהליך ריענון משתמשים מורשים
5.24	**התמודדות עם התקפת DDOS**	וידוא/הטמעת תשתית עמידה כנגד מתקפות DDOS העלולות להשפיע על הרכיב ו/או באמצעותו על הרשת	הגדרות בידול המערכת על ידי שימוש ברכיבי FW ומימוש חוקות מתאימות

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.25	**הצפנה**	שימוש ברכיבים המשלבים יכולת קריפטוגרפיה במטרה להגן על סודיות ומהימנות המידע ופגיעה בשלמות המידע גם בתהליך המעבר (Transit) וגם בתהליכי המנוחה (Rest)	יש לבחור באלגוריתמי הצפנה סטנדרטיים (כדוגמת AES-128/256) ומפתחות הצפנה חזקים. זאת, תוך וידוא הימנעות מפגיעה בביצועים ובטיחות יש לבצע החלפת מפתחות באופן עיתי
5.26	**אימות קלט ופלט נתונים**	יש לבצע תהליך אימות בכול מודול וזאת בהתאם לרשימה לבנה (white list)	
5.27	**הגנה על מידע ארגוני**	גישה למידע ארגוני (לרבות בסביבות ענן) יחייב שימוש במנגנוני הזדהות ואותנטיקציה חזקה בהתאם להגדרת איום היחוס על המערכת	שימוש במנגנון 2FA/MFA

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.28	**הגנה על מידע המסופק לצד ג**	אפשור והגדרת ניהול ושליטה על העברת מידע ממערכות ה- IoT לצד ג'	יש לבחון את משמעויות המידע וערוץ העברת המידע שעובר לצד ג גם בהיבטי אבטחה וגם ובהיבטי ארכיטקטורת מערכת, תרשים מבנה וכו'.
5.29	**הגנה על מידע - פרטיות ומניעת חשיפת מידע**	יש לוודא ולהבטיח תשומות מתאימות למניעת מידע אינפורמטיבי בעת הצגת מידע בהודעת שגיאה	מניעת מידעי מערכת אודות מזהי השגיאה, כתובות, גרסת שרת האינטרנט ומידע הקשור למבנה או לארגון
5.30	**הגנה על מידע וגיבוי ברשומות**	יש לוודא כי המידע המופק בתהליכי עיבוד המידע נשמר ומגובה גם כפלט Hardcopy למניעת אובדן מידע הקשור לבטיחות מבנה (לצורכי תחקור, בטיחות והפקת לקחים)	

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.31	**תיעוד וניטור**	יש לקבוע וליישם תהליכי ניטור על רכיבים ואירועים קריטיים אותם המערכת תתעד (Events log)	הגדרה, איסוף לוגים ואנומליות מכל אלמנט, ביצוע קורלציות והפקת התראות לשינויי הגדרות, קונפיגורציה וכו'. תהליך עיון בהתרעות הינו מרכיב חשוב בהגנה, איתור הפרות אבטחה, ניסיונות תקיפה ויכולות התאוששות. בהתאם, יש לערוך ביקורת תקופתית וסקירות של בקרות אבטחה כדי להבטיח תהליך יעיל.
5.32	**שרידות ויכולת התאוששות**	שימוש בטכנולוגיות ורכיבים המכילים יכולות ומנגנונים מכאניים מובנים לאבחון עצמי ותיקון להתאוששות מתקלה או כשל	

זיהוי בקרה	רשימת תיוג לבקרות/דרישות	הסבר משלים (ישים גם כדרישות לפיתוח)	פירוט יישומי בקרות ודוגמאות
5.33	**תיקוף פונקציונאליות**	תהליך סדור (כחלק מבקרה) לבדיקות פונקציונאליות של המערכת ורכיביה במטרה לאתר אירועים חריגים (דיווח לא מדויק/כוזב, אי תאימות במדדים וכדומה)	ניתן לבצע זאת על ידי השוואה אל מול רכיב או מערכת בעלת אותה פונקציונאליות אך יש לוודא כי לא קיימת תלות בין הרכיבים
5.34	**ביצוע בדיקות חוסן**	ביצוע בדיקות חוסן תקופתיות	מטרת הבדיקה לוודא את חוסנה של הרשת והרכיבים. הבדיקה תתמקד בסיכוני סייבר במניפולציה על הרשת ופגיעה בפונקציונאליות הרכיבים, יכולת תקיפה מהרשת לרכיבים ומהרכיבים לרשת.

6. ביבליוגרפיה ומסמכי קריאה והעשרה נוספים

תורת ההגנה בסייבר לארגון גרסה 1.0, אפריל 2018

- ✓ https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_418_A4.pdf

המלצות הגנה לצמצום סיכוני סייבר בתחנות קצה בארגון

- ✓ https://www.gov.il/BlobFolder/policy/endstation/he/המלצות%20הגנה%20לצמצום%20סיכוני%20סייבר-הנגשה%20סופי.pdf

התמודדות ארגונית במרחב הסייבר עם האיום הפנימי

- ✓ https://www.gov.il/BlobFolder/generalpage/coping_thret/he/Organizational_coping.pdf

צמצום סיכוני סייבר במערכות בקרת מבנה

- ✓ https://www.gov.il/he/departments/general/buildingmng

Anatomy of Threats to The Internet of Things

- ✓ https://www.researchgate.net/publication/328043031_Anatomy_of_Threats_to_The_Internet_of_Things

Baseline Security Recommendations for IoT, ENISA, November 2017

- ✓ https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

DEVELOPMENT OF A CYBER PHYSICAL SYSTEM FOR FIRE SAFETY - André Marshall, Associate Professor, Department of Fire Protection Engineering - University of Maryland

- ✓ https://drum.lib.umd.edu/bitstream/handle/1903/16803/Wills_umd_0117N_16267.pdf?sequence=1

IoT Security Architecture and Policy for the Home a Hub Based Approach, Release 1
November 2018

- ✓ https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf

IoTSF IoT Security Compliance Framework, Release 2, December 2018

- ✓ https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf

IoT Security Guidelines Overview Document, Version 2.0, GSMA, October, 2017

- ✓ https://www.gsma.com/iot/wp-content/uploads/2019/01/CLP.11-v2.0.pdf

NIST Releases Draft NIST Internal Report (NISTIR) 8222, Internet of Things (IoT) Trust Concerns, NIST, September, 2018

- ✓ https://www.nist.gov/news-events/news/2018/09/nist-releases-draft-nist-internal-report-nistir-8222-internet-things-iot

NIST Releases Special Publication 500-325, Fog Computing Conceptual Mode, March, 2018

- ✓ https://www.nist.gov/news-events/news/2018/03/nist-releases-special-publication-500-325-fog-computing-conceptual-model

Side Channel Attacks on IoT Applications - Yan, Yan, University of Bristol

- ✓ https://research-information.bris.ac.uk/files/210500367/Final_Copy_2019_03_19_Yan_Y_PhD.pdf