סייבר ישראל
מערך הסייבר הלאומי

צמצום סיכוני סייבר במערכות לניהול מבנה (Building Management Systems)

סייבר ישראל
מערך הסייבר הלאומי

צמצום סיכוני סייבר
במערכות בקרת מבנים

ספטמבר 2020

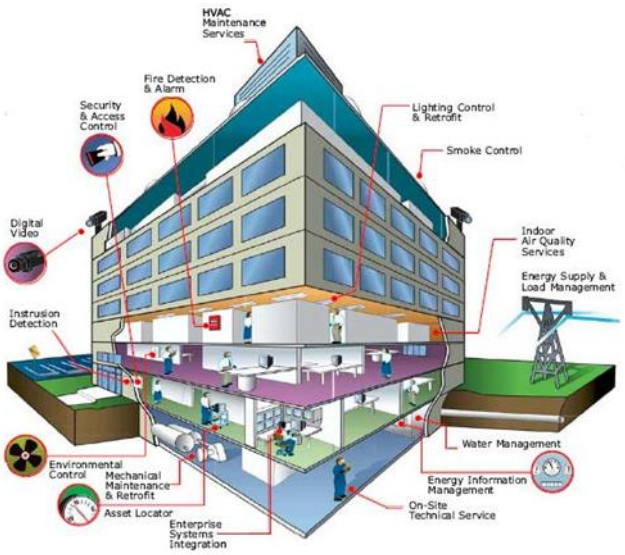
מסמך זה נכתב ע"י מערך הסייבר הלאומי לצורך קידום הגנת הסייבר במשק הישראלי. כל הזכויות שמורות למדינת ישראל - מערך הסייבר הלאומי. המסמך נכתב כשירות לציבור. העתקת המסמך או שילובו במסמכים אחרים כפוף לתנאים הבאים: מתן קרדיט למערך הסייבר הלאומי בפורמט המופיע להלן; שימוש בגרסה העדכנית של המסמך; אי הכנסת שינויים במסמך.
הערות והתייחסויות למסמך ניתן להעביר למייל: Tora@cyber.gov.il.

תוכן עניינים

מבוא 3
מטרת המסמך 5
קהל יעד 5
סקירת רקע של מערכות BMS ומערכות אבטחה 6
דוגמה לסוגי מערכות נפוצות במבנים חכמים 7
ניהול סיכוני סייבר בסביבות BMS 9
המלצות הגנה בהתאם לשלבי מחזור החיים 14
מסמכים ישימים 15

מבוא

בשנים האחרונות, התשתיות המותקנות בבנייני מגורים ומשרדים מנוהלות באמצעות מערכות לניהול מבנה (Building Management Systems). התשתיות האלה כוללות מיזוג-אוויר, אוורור, תאורה, חשמל, מים, ביוב, מעליות, כיבוי אש, חנייה ואבטחה. לאור זאת, נהוג לומר כי בנייני המגורים והמשרדים המודרניים הפכו להיות "חכמים" (Intelligent Buildings). השימוש במערכות שכאלה[1] מאפשר לאנשי התחזוקה לשלוט בתשתיות השונות של הבניין, ובכלל זה, לעקוב אחר היקף המשאבים שהן צורכות (ולקבל החלטות תפעוליות לצורכי אופטימיזציה וחסכון על בסיס זה), כמו-גם לקבל התראות באשר לתקלות או אירועים חריגים המתרחשים בהן. השימוש במערכת לניהול מבנה מאפשר, בין היתר, קישוריות, יעילות וחיסכון.



איור 1: דוגמא למערכות ורכיבי BMS, הכוללים שליטה בתשתיות חשמל, בטיחות, תאורה ועוד

שילוב מערכות אלה בבניין והשימוש בהן טומנים בחובם סיכוני סייבר. הידע, הפוטנציאל והיכולות לנצל חולשות ופרצות אבטחה הם בגדר עובדה קיימת, וכל שנדרש, בעיקרו של דבר, כדי לממשם הוא מוטיבציה של תוקף ורצונו לנצלן

[1] CYBER SECURITY OF INTELLIGENT BUILDINGS: A REVIEW, H.A. Boyes The Institution of Engineering and Technology, Stevenage, UK P-1
https://www.researchgate.net/publication/268191215_Cyber_Security_of_Intelligent_Buildings_A_Review/link/5cc87e9a4585156cd7bd8cc1/download

כדי לבצע מניפולציות בתשתיות המבוקרות או להשביתן. הסיכון הנשקף למערכות אלה גדול, בעיקר לאור העובדה שחלק מהן תוכננו ונבנו לפני שנים רבות - מחד גיסא, ובהתחשב בנזקים הפיסיים שעלולים להיגרם לתשתיות ולבניין עצמו כתוצאה מתקיפות שכאלה - מאידך גיסא. תרחישי תקיפה אלה מכוונים גם כלפי תשתיות קריטיות, מתוך מטרה לפגוע, למשל, בתקשורת בין מערכתית (כדוגמת פגיעה במערכות ליבה בשדות תעופה, בבתי חולים, בבתי מלון, וכד').

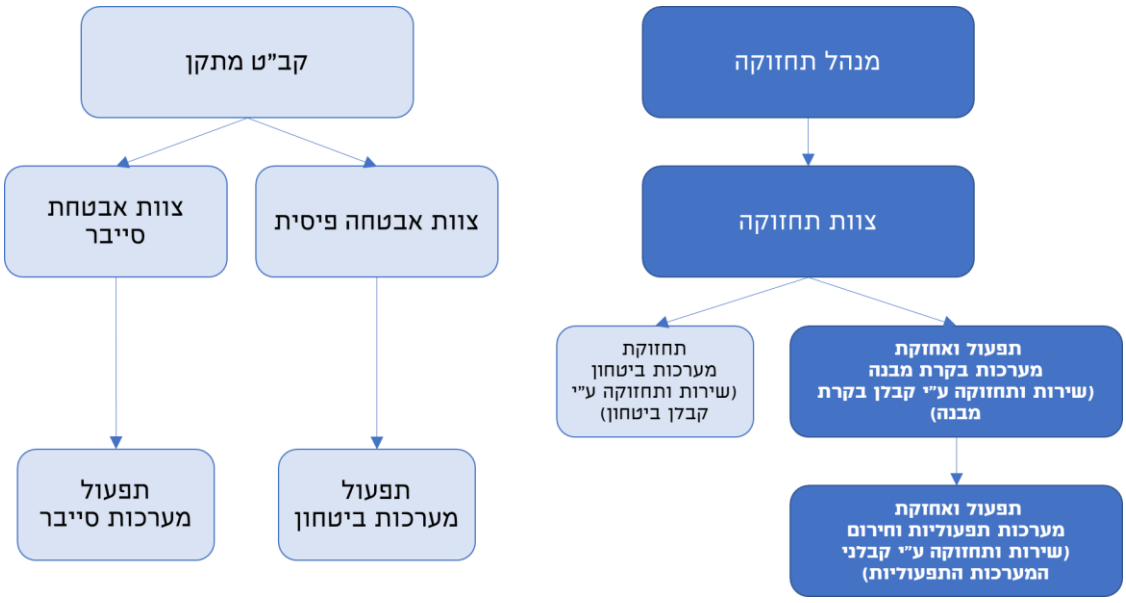
לפיכך, תהליך המעבר למבנים חכמים מחייב את מתכנניו ומיישמיו להבטיח, תוך כדי כך, את ביטחונם ושלומם של דייריהם ואת רציפות התפקוד של התשתיות המנוהלות - בשגרה כבחירום. כנגזר מכך, יש להטמיע בקרות ומעני הגנה הולמים כבר בשלב תכנון המבנה. זאת, תוך שימוש ביכולות זיהוי והכלה של אירועי סייבר פוטנציאליים - ומתן מענה הולם לאלה, אחת שכבר החלו להתחולל בפועל.
מסמך זה מציג את האיומים העיקריים במרחב הסייבר בתחום זה, לצד המלצות לשיטות ופתרונות הגנה אפשריים.

מטרת המסמך

להקנות ידע ויכולת ניהול סיכונים ושילוב בקרות מתאימות בתחום לגורמים המעורבים בהפעלה ותחזוקה של הבניין, לרבות: מנהלים, מפעילים, מהנדסים, אנשי תחזוקה וביטחון ואנשי הגנת סייבר, ובכלל זה, לספק להם את הרקע הכללי לזיהוי האיומים הנשקפים למערכות הניהול של מבנים אלה, את המתודולוגיה הכללית להקטנת החשיפה אליהם, את הידע הבסיסי הנדרש לזיהוי התרחשות של אירועים, ואת הדרכים המומלצות להיערך כראוי לקראתם ולנהל את המענה להם.

קהל יעד

- **בעלי התפקידים בבניין/בארגון** - בהתאם לתחומי האחריות (ראה איור 2).
- **מהנדס/טכנאי** - אחראי על תכנון, הקמה ותחזוקה של מערכות OT, וניהול הרשת והאפליקציות.
- **מפעיל/איש בקרה** - אחראי על ביצוע עבודות יום יומיות של הפעלה ובקרה של התשתיות.
- **מנהל אבטחת מידע** - אחראי על ביצוע סקר סיכונים, איפיון והגדרה של בקרות נדרשות להגנת מערך ה-OT וניהול סיכונים מתמשך (לרבות ביצוע ביקורות ומעקב תיקון ליקויים, ניהול אירועים, בחינת ממשקים מול SOC, וכו').
- צוותי ה-IT ושאר הגורמים המופקדים על מערכות המחשוב בבניין.
- **מנהל בניין** - אחראי על אישור שינויים, הגדרות רכש וכד'.



איור 2 -בעלי תפקידים ותחומי אחריות

סקירת רקע אודות מערכות ניהול מבנה

בדיוק כמו מערכת SCADA, מערכת ניהול מבנה כוללת, על פי הרוב, את הרכיבים האלה:

- **HMI (Human-Machine Interface) -** ממשק אדם-מכונה, המציג מידע אודות תהליך מסויים למפעיל, וכך מאפשר למי שמנהל ומתפעל אותו לנטרו ולבקרו.
- **MTU (Master Terminal Unit) -** מערכת פיקוח מרכזית שנועדה לנטר, לפקח ולהפעיל רכיבי קצה.
- **DDC\PLC (Direct digital control\Programmable Logic Controllers) ובקרי Embedded PC -** בקרים לוגיים, המתוכנתים לקבל קלט, להפעיל לוגיקה (שנטענת מראש) ועל פיה - להעביר פקודות לרכיבים שונים. לבקרים אלה ניתן לשרשר גם יחידות RIO שונות (Remote I/O).
- **RTU (Remote Terminal Unit) -** יחידת ניטור ממוחשבת המעורבת בתהליך, וככזו, מחוברת לחיישנים הממוקמים באתרים מרוחקים.
- **Historian -** מערכת האוגרת לאורך זמן את נתוני הרכיבים והבקרים מהשטח, ומציגה מגמות בשינוי ערכי הפרמטרים הנמדדים בתהליך. המערכת בדרך כלל משמשת את מהנדסי הבקרה לשיפור ולכוונון של התהליך.
- **Sensor -** חיישן: אמצעי המודד את ערכיו של משתנה פיזי מסויים.
- **Actuator -** פקד: אמצעי המופעל על ידי חיישן ומחולל פעולה נדרשת (כגון פתיחת שסתום).
- **תשתית תקשורת -** מקשרת את מערכת הפיקוח ליחידות הבקרה (תקשורת: קווית, רדיו, סלולר, Wi-Fi, לוויין).
- **IOT (Internet of Things) -** כינוי למאגר של רכיבים פיסיים ייעודיים, הנעזרים בתשתית האינטרנט כדי לאפשר תעבורה של מידע בינם לבין עצמם.

IIOT (Industrial Internet of Things) - רכיבי IOT ייעודיים לתעשיית הייצור.

תשתיות אופייניות במבנים חכמים - חלוקה תפקודית

- תשתיות מתקניות ותפעוליות
- תשתיות בטיחות וחירום
- תשתיות אבטחה

תשתיות אלה נבדלות זו מזו במהות השירות אותו הן מספקות, בצוותים האחראים עליהן, המתפעלים ומתחזקים אותן, באופי הרכיבים הנמצאים בשימוש בהן, ובעיקר - באופי רכיבי הקצה (חיישנים, מצלמות, בקרים וכד')[2].

שונות זו בין התשתיות מחייבת גם שונות בין הגישות להגנת הרכיבים. גישה ,בין היתר, להפרדה בין תשתיות אלה על מנת לספק הגנת סייבר נאותה. לדוגמא מערכת השליטה במערכות המיזוג תהיה מבודלת ממערכות חירום ובטיחות, ממערכות מתקניות ותפעוליות וכן ממערכות האבטחה.

שכבת מערכת בקרת מבנה - BMS	מערכת ניהול - HMI ◦◦◦◦ מבנה המציגה את כלל נתוני המערכות - ניטור וניתוח
	רשת תקשורת ומחשוב לבקרת מבנה
	בקרי בקרת מבנה BMS
	סנסורים

שכבת מערכות	מערכת בקרה וסנסורים אינטגרלית - (בקר צ'ילר, בקר גנרטור וכדומה)			
	מיזוג אוויר HVAC	**חשמל**	**מים**	**דלק**
	צ'ילרים	לוחות מתח גבוה	מערכת בורות שאיבה	מיכל סולר
	יחידות אוויר צח	לוחות חשמל מקומיים	מערכת מי צריכה	מיכל יומי
	מפוחים	מערך UPS	ברזים	משאבות
	Crack	גנרטורים	מאגרי מים (צריכה וכיבוי)	ניהול דלק
		תאורה	טיפול במים והכלרה	
		ניהול חשמל חכם		

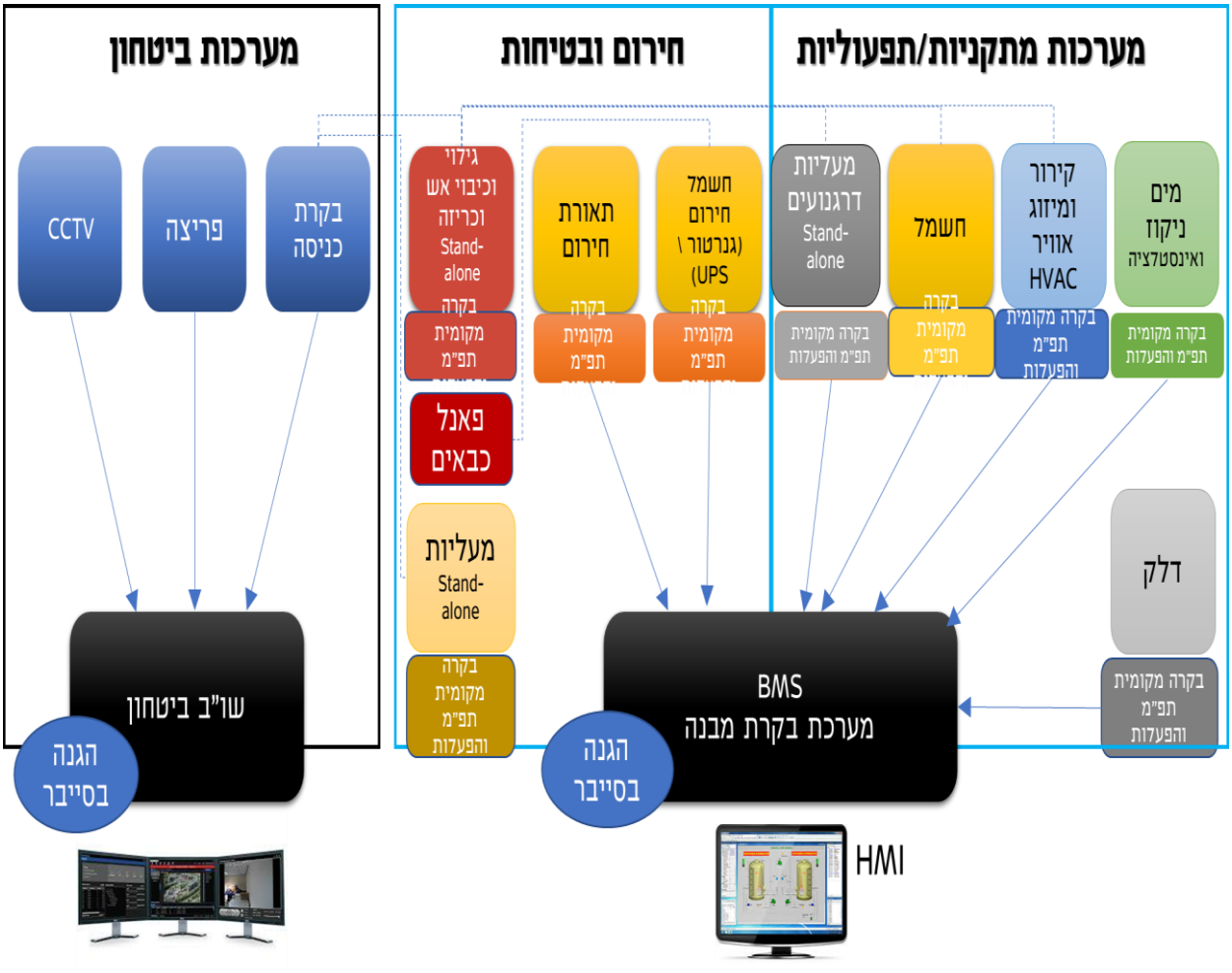
איור 3 - שכבות מערכות המתקניות והאלקטרומכאניות אל מול שכבת המערכת בקרת המבנה

[2] צמצום סיכוני סייבר ממצלמות אבטחה - https://www.gov.il/BlobFolder/policy/iotcamers/he/Security%20Cameras_575480_Sharon2_Web%20digital%20final%20להפצה%20גרסה.pdf

חלוקה פיזית אופיינית

השכבות הפיזיות של במבנה החכם מכילות את רכיבי הקצה שמבצעים את הפעולות המכניות של המערכת ואת רכיבי הקצה החשים (חיישנים) המדווחים על מצב המערכת בכל רגע נתון. כמו כן, ניתן לשייך לשכבה זו גם את הבקרים המתוכנתים, הממירים את אותות החיישנים למידע דיגיטלי ומעבירים את הפקודות לרכיבי הקצה. בקרים אלו מבצעים את האוטומציה (הפיזית) על פי לוגיקה מוגדרת מראש.

כדוגמא, ניתן לקחת את מערכת המיזוג, המורכבת מרכיבי קצה "חשים" (כגון רכיבים המכילים חיישני טמפ' למי הקירור ולטמפ' החדר) ורכיבי קצה שמבצעים אוטומציה פיזית (כגון: מנועי משאבות המים הקרים הווסתים והשסתומים וכן ומנועי הצ'ילרים (מכונות הקירור) המקבלים פקודות באמצעות בקר הצ'ילר).



איור 4 - חלוקה לפי קטגוריות מבנה (קיימת הפרדה בין תשתיות חירום ובטיחות ומעליות מתשתיות מנוהלות אחרות)

ניתוח סיכוני הסייבר הנשקפים למערכות ניהול מבנה

מטרת תהליך ניתוח הסיכונים היא למפות ולדרג את סיכוני הסייבר במערכות ה- BMS ולהגדיר את המענה לפערי ההגנה. במקרה של פרויקט חדש אשר נמצא בשלב התכנון, מומלץ לבצע סקר סיכונים ייעודי למתקן כבר בשלב הזה, וזאת, על מנת לקבוע את הבקרות המותאמות הנדרשות.

התהליך כולל את ניסוח תרחישי הסיכון העשויים לפגוע בארגון, הערכת פוטנציאל הנזק בעת התממשותם, הערכת הסבירות להתממשותם, שקלול שני פרמטרים אלה, ותעדוף בקרות להפחתת הסיכונים על סמך זאת.

להלן רשימה של סיכונים לדוגמה:

1. הגדלת משטח תקיפה בעקבות שימוש בקישוריות לא מאובטחת (ערוצי השתלטות, תמיכה ולצורך הורדת עדכונים).
2. שימוש בממשקים אלחוטיים (לרבות רכיבי IoT).
3. מצוקת כוח אדם של מומחי סייבר (שלב התכנון, התמיכה, ניהול סיכונים וכד').
4. פערי בידול והפרדה בין מערכות וסביבות ניהול.
5. שימוש במערכות העומדות לפני סיום מחזור-החיים שלהן (End of life/Support).
6. שגיאות אדם (מפעיל), העלולות ליצור פערי אבטחה והזדמנויות אטרקטיביות לתוקף.
7. העדר הגנה נאותה על תהליכי התמיכה הטכניים.
8. נגישות פיזית לגורמים לא מורשים למערכות הניהול.
9. שימוש ברכיבים שקיימת לגביהם אינדיקציה מודיעינית/טכנולוגית (לרבות בפרסומים גלויים) שהותקנו בהם "דלתות אחוריות".
10. מדיניות לא סדורה של עדכון רכיבי חומרה ותוכנה.

להלן דוגמאות מייצגות לניצול הסיכונים המנויים לעיל בהקשר של תשתיות ספציפיות:

התשתית	השפעה אפשרית ותרחישי סיכון
תאורה	פגיעה ושיבוש תאורה לצורך האפלה, גרימת כאוס ובלבול ופגיעה בבטיחות[3] תוך ניצול ממשק גישה מרחוק לא מאובטח

[3] http://www.wisdom.weizmann.ac.il/~eyalro/EyalShamirLed.pdf ,
https://www.youtube.com/watch?v=Ed1OjAuRARU ,

התשתית	השפעה אפשרית ותרחישי סיכון
דלתות כניסה ויציאה	- השתלטות לצורך פגיעה בדלתות לצורך פתיחה או סגירה (לצורכי כופר/ השבתה) - פגיעה בסדרי האבטחה ואפשור כניסה לא מורשית לארגון (כדוגמת הוספת משתמשים לא מורשים למערכת) - מחיקת נתונים ולוגים מפלילים במערכת
מצלמות במעגל סגור	- פגיעה במערכות האבטחה ועיוורון מצלמות ומערכת - יכולות כיבוי מצלמות לצרכים קרימינליים (כחלק מפגיעה ביכולת תיעוד) - מחיקה או עריכת קטעים לצורך שיבוש ראיות - איסוף ולכידת תמונות, לצורך פגיעה בפרטיות, יצירת מבוכה וכדי
מיזוג אוויר	- השבתת מערכות המיזוג, העלאה או הורדת טמפרטורות ליצירת תנאי עבודה לא נוחים ואי נוחות לדיירים או פגיעה במערכות המחשוב במטרה לגבות כופר מהארגון
מעליות	- תקיפת מניעת שירות (DOS) - ביטול הרשאות גישה לקומות
ניהול דיירים	- פגיעה במערכות הסליקה ושיבוש הוראות תשלום והעברת כספים
מערכות גילוי וכיבוי אש	- יצירת כאוס פאניקה ובלבול

בסוף תהליך ניתוח הסיכונים, תהיה בידי הארגון רשימה של סיכונים מדורגים בהתאם לעוצמת הנזק ולמידת הסבירות להתממשותם. להלן דוגמה לרשימה אופיינית שכזו:

תרחיש לדוגמה	סבירות (4-1)	עוצמת הנזק (4-1)	רמת סיכון משוקללת
השתלטות על מערכת בקרת כניסה לבית מלון	4	3	**12**

השתלטות על מערכת בקרת כניסה -לבניין משרדים)	2	2	**4**
השתלטות על מערכות כיבוי אש	2	3	**6**
ביצוע מניפולציה על מערכות השליטה בתאורה	3	1	**3**

<u>הסבר לתהליך החישוב של הנתונים המופיעים בטבלה לעיל:</u>

השתלטות על מערכת נעילת דלתות - בבית מלון:

בפרמטר **<u>סבירות</u>** נקבע הציון **4** - לאור שקלול היסטוריית אירועים (כגון מתקפת הכופר שבוצעה על מלון בחו"ל שגרמה לפגיעה בתהליך העסקי המרכזי של המלון), מוטיבציית היריב לממש תרחיש זה (לדוגמא מתחרים באזור שמעוניינים לפגוע בשם בית המלון).[4] וכן היכולת לנצל חולשות והזדמנויות של חוסר בקרה וניהול של טכנאים ונותני שירות, לאור העובדה שהמערכת עצמה מחוברת לאינטרנט (ללא בקרות הזדהות) וכן העובדה שאין נהלים ברורים לשירות ותחזוקה של מערכת בקרת הדלתות. ההסתברות הינה גבוהה באופן יחסי.

בפרמטר **<u>עוצמת הנזק</u>** נקבע הציון **3** - האירוע לא יוביל לנזק בחיי אדם וכן ישנה אפשרות להשבתת נעילת הדלתות הדיגיטאלית וחלופה ומעבר למנגנון מכאני. אך מכיוון שמדובר (בדוגמא זו) בבית מלון, ומרכיב בקרת הדלתות <u>הינו מרכיב מרכזי וקריטי בפעילות העסקית של עסק מסוג זה</u> - עוצמת הפגיעה הינה גבוהה ביותר (זאת לעומת בניין משרדים בו שוכנים משרדים בהם הפעילות העסקית איננה מבוססת על בקרת דלת הכניסה למשרד אותה ניתן תמיד לעקוף באמצעות מפתח).

רמת הסיכון המשוקללת הינה 12 מתוך 16 - רצוי מאוד להציג להנהלה בקרות מפצות שיצמצמו את הסיכון.

דוגמה 2 - השתלטות על מערכות בקרת כניסה - בבניין משרדים:

בפרמטר **<u>סבירות</u>** נקבע הציון **2** - לאור שקלול היסטוריית אירועים, מוטיבציית היריב לממש תרחיש זה. מצד שני, ישנן בקרות מפצות כגון - המערכת אינה מחוברת לאינטרנט, מודעות צוות האחזקה גבוהה, ישנם נהלים ברורים לעבודת טכנאים כולל עבודה עם מחשבי טכנאי יעודיים וכן נהלים ברורים בתחזוקת מערכות האבטחה\הבקרה. על כן ההסתברות נמוכה יחסית.

[4] https://edition.cnn.com/2017/01/30/europe/hackers-lock-out-hotel-guests-trnd/index.htm

בפרמטר **<u>עוצמת הנזק</u>** נקבע הציון **2** - האירוע לא יוביל לנזק בחיי אדם וכן אין השפעה ישירה על התהליכים העסקיים ו\או על תפקוד המשרדים כאשר ניתן תמיד לעבור לשימוש במפתחות באופן זמני. כמו כן חדרי התקשורת המסווגים (אם ישנם) הינם בעלי מנגנון מנעול קומבינציה עליו לא ניתן להשתלט ומהווה בקרה מפצה נוספת על חדרי שרתים ותקשורת בבניין המשרדים. על כן עוצמת הפגיעה היא נמוכה.

רמת הסיכון המשוקללת הינה 4 מתוך 16

דוגמה 3 - השתלטות על מערכות כיבוי אש:

בפרמטר **<u>סבירות</u>** נקבע הציון **2** - לאור שקלול היסטוריית אירועים, מוטיבציית היריב וכן הקושי ביכולת לנצל חולשות והזדמנויות של מידור המערכת ותשומות למניעת גישה, וכן לאור העובדה כי קיים בידול ממערכות התפעול והמערכת עצמה אינה מחוברת לאינטרנט.

בפרמטר **<u>עוצמת הנזק</u>** נקבע הציון 3 - האירוע לא יוביל לנזק בחיי אדם. על אף שישנה אפשרות לפגיעה במערכת החירום ישנם תהליכים מפצים נוספים לאירוע בטיחות וחירום.

רמת הסיכון המשוקללת הינה 6 מתוך 16.

דוגמה 4 - ביצוע מניפולציה על מערכות השליטה בתאורה:

בפרמטר **<u>סבירות</u>** נקבע הציון **6** - לאור שקלול יכולות השתלטות על מערכות השליטה ורכיבי ה-IoT והקישוריות לאינטרנט.

בפרמטר **<u>עוצמת הנזק</u>** נקבע הציון 1 - האירוע לא יוביל לנזק בחיי אדם. קיימות מערכות גיבוי לתאורת חירום.

רמת הסיכון המשוקללת הינה 3 מתוך 16 - רמת ההגנה מקובלת על הארגון.

מכאן, שבתוכנית העבודה עבור הדוגמא לבניין A (דוגמא של בית מלון) יתבצע תיעדוף להקשחת מערכת בקרת הדלתות בבניין (על בסיס תהליך ניהול הסיכונים).

לטובת הפחתת הסיכונים, יבחן הארגון את הבקרות אותן הוא יכול לממש בהתאם למגבלות הקיימות. להלן דוגמה לרשימת בקרות שכזו:

#	בקרה מפצה	צמצום הסיכון ורמת ההשפעה	עלויות הקמה ותחזוקה	רמת כח האדם הנדרש ליישום	המלצות
1	מדיניות ונהלים - כתיבת מדיניות ונהלים ברורים לניהול ותחזוקת מערכות ה OT- בקרת מבנה והביטחון - שלב בסיסי	צמצום סיכונים רוחבי **משמעותי**	**עלויות נמוכות**	**ידע בסיסי**	מומלץ בכל מתקן
2	מערכות סגורות - ללא חיבור לרשת האינטרנט או כל רשת אחרת.	צמצום סיכונים רוחבי **משמעותי**	**עלויות נמוכות**	**ידע בסיסי**	מומלץ בכל מתקן
3	מחשבי טכנאי ייעודיים ומוקשחים (איסור שימוש במחשבי טכנאי של החברה המתחזקת)	צמצום סיכונים רוחבי **משמעותי**	**עלויות נמוכות**	**ידע בסיסי**	מומלץ בכל מתקן
4	יישום בקרת גישה, ניהול משתמשים, ניהול סיסמאות לכל רכיבי ומשתמשי המערכת	צמצום סיכונים רוחבי **משמעותי**	**עלויות נמוכות**	**ידע בסיסי**	מומלץ בכל מתקן
5	ביצוע הקשחות וסגמנטציה ברמת הרשת הרכיבים והאפליקציה	צמצום סיכונים רוחבי **משמעותי**	**עלויות נמוכות**	**ידע בסיסי**	מומלץ בכל מתקן
6	הגנה פיזית על כל ארונות התקשורת והבקרים של מערכות ניהול המבנה והביטחון - וחיבורן למוקד האבטחה של המתקן	צמצום סיכונים רוחבי **בינוני**	**עלויות נמוכות**	**ידע בסיסי**	מומלץ בכל מתקן
7	בקרות מפצות מורכבות כגון IDS\IPS, NAC, NGFW, AV וכדומה	**צמצום סיכונים ממוקד**	עלויות גבוהות	**ידע ניכר בתחום הסייבר הדורש כח אדם ייעודי להקמה ותחזוקה**	**גיבוש מענים בהתאם לניהול הסיכונים למתקן** כח האדם והתקציב

המלצות הגנה בהתאם לשלבי מחזור החיים

שלב	תכנון נדרש
מפרטים ותכנון	זמינות ופונקציונאליות קריטיות נדרשות
	איחוד תשתיות IT ותפעול על פי הנדרש
	שינויי תצורה ברכיבי תקשורת על פי הנדרש, לרבות שילוב של רשתות אלחוטיות
	תהליכי שינוי נדרשים (הרחבות, איחודים וכו')
	חיבוריות נדרשת בין רכיבי ה- OT
	תכנון אבטחת מערכות ורשת נדרשים, כולל היבטי מידע ופרטיות אשר נשענים על **הפונקציונליות הנדרשת** לטובת תפעול
	תכנון אבטחה פיזית היקפית ופנימית
	תכנון תשתיות תקשורת
	תכנון ובחירת המערכות לניהול המבנה (בהקשר של HAVC, גילוי אש, וכו')
	תכנון ניטור פונקציונאלי ואבטחתי כנדרש
שלב הבניה	ניהול שרשרת האספקה
	פיקוח על יישום מלא של מפרטי האפיון
	הפעלת אבטחה פיזית
	יישום הטמעת מערכות הגנת סייבר
שלב ההתקנה והתפעול	החלת הגדרות אבטחה מלאות ומותאמות בכל רכיב מותקן
	איתור חולשות (Vulnerability & Pen testing), והחלת הקשחות נדרשות
	הגדרת משתמשים והרשאות פרטניות
	התקנת מערכות מיגון רשתיות (Firewall, IPS, etc)
	מניעת גישה שאינה מורשית וביצוע פעולות ניטור והתמודדות עם גורמי האיום הפנימיים ובשרשרת האספקה
	ניהול השינויים הכוללים גם את גורמי הסייבר הנדרשים לכל שינוי
	ניטור פונקציונאלי ואבטחתי לכל רכיב, ולכלל המכלול גם יחד (ביצוע קורלציות)
	ניהול משתמשים, עדכוני אבטחת מידע ומערכות אבטחת מידע
פירוק/ גריטה	יש לוודא שלא נשארים פרטי מידע אישי (פרטיות)
	הסרת רכיבי OT, מערכות אבטחה ושאר הציוד בצורה מאובטחת

מסמכים ישימים

- ✓ הרחבה מקצועית בנושא "הגנה בסייבר על סביבות ICS"
- ✓ מסמך "ניהול סיכוני סייבר בסביבות OT - מדריך לדירקטוריון"

אודות אופן כתיבת המסמך

מסמך זה הוכן ע"י מערך הסייבר הלאומי - המסמך נכתב תוך הליך של שיתוף הציבור, וקיבל משוב מקבוצת עבודה שהוקמה לטובת הכנת המסמך. בכתיבת מסמך זה לקחו חלק פעיל:

חברת EMG - אלי וליאור פלץ

חברת סקאדה סודו - יגאל גויטע

כמו כן ברצוננו להודות לגורמים רבים נוספים שהשתתפו בשלב המשוב אודות טיוטת המסמך, והם :

PWC גלעד זינגר, אבישי רוטשטיין, חברת אבן דנן - עידו רוזנר, קבוצת מיקוד - בנושא ICS בה לקחו חלק עשרות רבות של גורמים מתחום תוכן זה.