מסמך המלצות

צמצום סיכוני סייבר
ממצלמות אבטחה

אפריל 2018

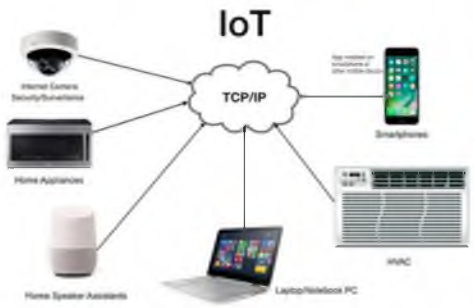
משרד ראש הממשלה
מערך הסייבר הלאומי

תוכן העניינים

תקציר ומטרת המסמך

התלות הגוברת במרחב הסייבר היא תולדה של קידמה טכנולוגית, קישוריות וחיבור גלובלי לרשת. היכולות הטכנולוגיות והאיומים המתפתחים במרחב הסייבר אינם מבדילים בין ארגונים לבין גורמים פרטיים והם מכוונים לאלו וגם לאלו. מסמך ההמלצות נכתב כחלק ממטרה לשפר את החוסן הלאומי, הארגוני אך גם את מרחב הפרטיות והביטחון האישי.

השימוש בסנסורים, מצלמות רשת המכילות יכולת WiFi או מצלמות המכילות רכיבי IoT תפס תאוצה בשנים האחרונות. תקשורת ה- IoT היא תקשורת מתקדמת בין החפצים המאפשרת יכולות איסוף והחלפת מידע. טכנולוגיה זו מאפשרת חיבוריות לאינטרנט, החלפת מידע בין רכיבים וקבלת עדכונים בכל זמן ובכל מקום (Any Time Any Place). למרות היתרונות העצומים בשימוש ברכיבי ה- IoT, קיימים מחקרים רבים שונים המוכחים חולשות אבטחה ברכיבי ה- IoT ותהליכי השתלטות עוינת.[1] טכנולוגיה זו מובילה לאוטומציה ותקשורת בין רכיבים. בכך, נוצרת הזדמנות וסכנה אבטחתית של התוקף להתערב ולבצע מניפולציה על התקשורת בין הרכיבים והמערכת כולה.



דוגמאות למערכות IOT

השימוש בטכנולוגיות מבוססות IOT (ללא הגדרות אבטחה מתאימות), הופך את המצלמות ליעד תקיפה לצורכי גניבת נתונים, שיבוש נתונים, התחזות, חסימה וכד'.[2] שיטות התקיפה מתבססות גם על תהליך של חיפוש מצלמות אבטחה באמצעות שאילתות של שם יצרן המצלמה וסיסמאות ברירת המחדל, וכן התקפות, ניצול מצלמה או כתובת IP והתקפות מכוונות ליצירת עומס ומניעת שירות ושימוש מבצעי במצלמות.

[1] ראו מחקרם של אייל רונן, דוקטורנט במעבדתו של פרופ' שמיר, אחי-אור ויינגרטן, סטודנט לתואר שני במכון ויצמן וקולין או'פלין השתלטות עוינת על רשת IoT של מכון ויצמן - https://eprint.iacr.org/2016/1047.pdf

[2] Security Issues in the Internet of Things (IoT): A Comprehensive Study - (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017 (טבלת שכיחות סיכונים – עמ' 388)

הפריסה הרחבה של המצלמות במרחב הארגוני והפרטי עלולים להגביר את סיכוני האבטחה והחדירה הלא מורשית למערכות האבטחה, לרבות התערבות התוקף בתהליכי עדכוני תוכנה (MITM) וכד'.[3]

מסמך זה, הינו מסמך מותאם למשק והוא כולל בתוכו המלצות שמטרתן לצמצם את סיכוני הסייבר מהמצלמות. **המסמך נכתב בין היתר בהתאמה לאירועי תקיפות סייבר שונים כנגד מצלמות.**

1.1. רציונל המסמך לצמצום הסיכונים מבוסס **על** מודל **בסיסי באבטחת המידע** - מודל **ה-** C.I.A:

- **סודיות נתונים** (Confidentiality) - כחלק מ**חשאיות** ו**מניעת חשיפה לא מורשית** של מידע.
- **שלמות הנתונים** (Integrity) - **מניעת שינוי לא רצוי של הנתונים,** זיוף או השחתה והבטחה כי המידע אותנטי ולא עבר שינויים ע"י גורם עוין.
- **זמינות** (Availability) - **ווידוא שניתן לגשת לנתונים בכל זמן.**

1.2 בתכנון מאובטח, שמטרתו לצמצם את סיכוני האבטחה ממצלמות האבטחה יש לשקלל את התרחישים הבאים:

1.2.1 סיכונים הנובעים משימוש ברכיבי IoT.

1.2.2 ניצול תשתיות של מצלמות בתחנות קצה לצורך חדירה למערכות מחשוב ארגוניות - מצלמות ככל רכיב מחשוב אחר המבוסס תוכנה, עשוית לכלול באגים, פערים, דלתות אחוריות ו"הזדמנויות" הניתנות לניצול. איום זה הוא משמעותי שכן הוא מקדם את התוקף ביעדי התקיפה של גניבת מידע עסקי, פגיעה בבסיסי הנתונים, הטמנות של סוסים טרואנים וקודים עוינים לצורכי התקפות המשך וכד'. בהקשר זה קיים גם סיכון של שימוש בתשתית המצלמות והחיישנים לביצוע התקפות של מניעת שירות (DDOS).

1.2.3 התערבות בתווך (MITM) **לצורך צפייה לא מורשית בנתונים** - יכולת התחברות למערכת, השתלטות או האזנה בתווך (MITM) וצפייה בחומרים או בתוצרי הצילום.

1.2.4 התקפות מקוונות לצורך השבתה או מניעת גישה למערכת - השתלטות עוינת ופריצה לצורך השבתת פעילות מצלמות האבטחה. באירועים רבים, ביצע התוקף השתלטות על מצלמות, השבית פעילות ושינה את סיסמאות הגישה אליהן. במקרים אחרים אף בוצעו התקפות כופר על המצלמה[4]. **בהזדמנויות אחרות שיבש התוקף את מצלמות האבטחה במטרה ליצור לעצמו הזדמנות ושעת כושר לפריצה פיזית.**

[3] http://www.newshub.co.nz/home/world/2017/02/hackers-hacked-washington-cameras-before-trump-s-inauguration.html

[4] התקפה בתוכנה זדונית למטרת סחיטת כסף

1.2.5 **מניפולציה על המידע** - מערכת אבטחה שאיננה מאובטחת מאפשרת לתוקף לבצע תהליכי מניפולציה ושינוי מידע בתעבורת הצילום, זאת ללא ידיעת מפעילי המערכת.

1.2.6 **שיבוש או מחיקת הקלטות** -שיבוש או מחיקת הקלטות ע"י גישה בלתי מורשית, ביצוע שינויים בתמונות וכד'.

1.3 המסמך מתרכז במצלמות בתחנות הקצה וכן בתווך התקשורת (בין המצלמות למחשבים וכד') תוך הנחה כי הממשקים הקיימים הם לשרתים ותשתיות ארגוניות שניתנו להן תשומות מתאימות למזעור סיכוני הסייבר (בהתאם לתורת ההגנה בסייבר לארגון).[6] ככזה הוא איננו עוסק בהיבטים פיזיים של אפיון מערך מצלמות, אופן פריסה והתקנת כלל הציוד במערך זה.

קהל היעד למסמך

מסמך זה מיועד לארגונים פרטיים, ציבוריים, וגופים ממשלתיים אשר בכוונתם להטמיע או לשלב מצלמות באופן מאובטח, תוך מטרה לצמצם את סיכוני הסייבר ממצלמות האבטחה. נושא זה מחייב חשיבה והיערכות מתאימה במטרה להבטיח את ביטחונם ופרטיותם של המשתמשים והאזרחים ומנגד לצמצם את סיכוני הסייבר ככל שניתן. המסמך מספק קווים מנחים ודגשים כבר בשלבי ההצטיידות, ההתקנה והגדרות ו/או צמצום סיכוני הסייבר במצלמות קיימות ופעילות. ככזה, הוא יכול להוות כמסמך המלצות אבטחה המכוון בין היתר לספקיות ציוד מערכות ומצלמות אבטחה, יועצי אבטחה ומתח נמוך ואנשי התשתיות בארגון.

[6] https://www.gov.il/he/Departments/Guides/cyber_security_methodology_for_organizations_test

איומים טכנולוגיים במצלמות - רקע

מצלמות אבטחה חשופות לאיומי סייבר ואירועי אבטחת מידע לרבות דליפת מידע והפרת פרטיות. הטריגר והאטרקטיביות לתקיפה נובעים בין היתר בשל הרצון של התוקף להגיע למידע רגיש ופגיעה בפרטיות (תמונות, סרטים וכד'), או כחלק מניצול מערכות אבטחה בכלל ומצלמות אבטחה בפרט לצורך איסוף מודיעין לפני מבצע (אמל"מ).

ההתפתחות הטכנולוגית מובילה בין היתר לחדשנות ושימוש במצלמות אבטחה בצרכים שונים וכחלק מפלטפורמות מורכבות כדוגמת ערים חכמות המושתתות על מערכות מחשוב וטכנולוגיות מידע ותקשורת מתקדמות. בניהול סיכונים באירוע מסוג זה יכולה להוות המצלמה כתווך וסלילת דרך לתקיפת רשת המחשוב או לחילופין תקיפת המצלמות בדרך הפוכה דרך פלטפורמות ורכיבים אחרים ברשת המושתתות בטכנולוגיית העיר החכמה.

עיקרי ההתקפות נשענות על **תקיפת מנגנוני הסיסמה** (שימוש בסיסמאות Default, סיסמאות טכנאי וניחוש סיסמאות), **וניצול קישוריות** (לרבות נושאי ה- IoT) וערוצים לא מאובטחים ומוצפנים לצורכי התערבות והאזנה בתווך.

המלצות לצמצום סיכוני אבטחה ממצלמות

1. המלצות לפני רכישה:

1.1 רצוי להצטייד במערכות שאינן מבוססות IoT, כאלו שאינן כוללות רכיב תקשורת עצמאי מובנה כמו מודם, משדר אלחוטי וכד'.

1.2 לחילופין, בחינת אפשרות נטרול חומרתי או תוכנתי (רצוי בתיאום ובסיוע היצרן).

1.3 רצוי למנוע התקנת מוצרי תוכנה שאינם מתוצרת יצרן המצלמות. במידה ונדרשת התקנת תוכנה שלא מבית היצרן יש לבצע זאת בתהליך ניהול סיכונים מושכל הכולל גם זיכוי התוכנה מפני פוגעניים (הרצת אנטי וירוס וכד').

1.4 יש לקחת בחשבון כי מצלמות עלולות להוות דלת כניסה של פוגענים לארגון ולהכיל את כל היבטי הסייבר ושיקולי אבטחת המידע הקיימים בארגון בדיוק כדין הכנסת ציוד מחשוב באשר הוא לארגון ובתוך כך, מצמצום סיכונים בשרשרת האספקה.

2. המלצות לפני התקנה ובתהליכי התחזוקה (במידה ולא ניתן להימנע משימוש ברכיבים המכילים WiFi)

2.1 יש לחייב אותנטיקציה חזקה באמצעות שרת RADIUS או LDAP והחלפת סיסמת טכנאי וסיסמאות ה- default לסיסמה מורכבת (סיסמה 8-12 הכוללת אותיות, ספרות ותווים מיוחדים) לצמצום סיכונים של MITM.

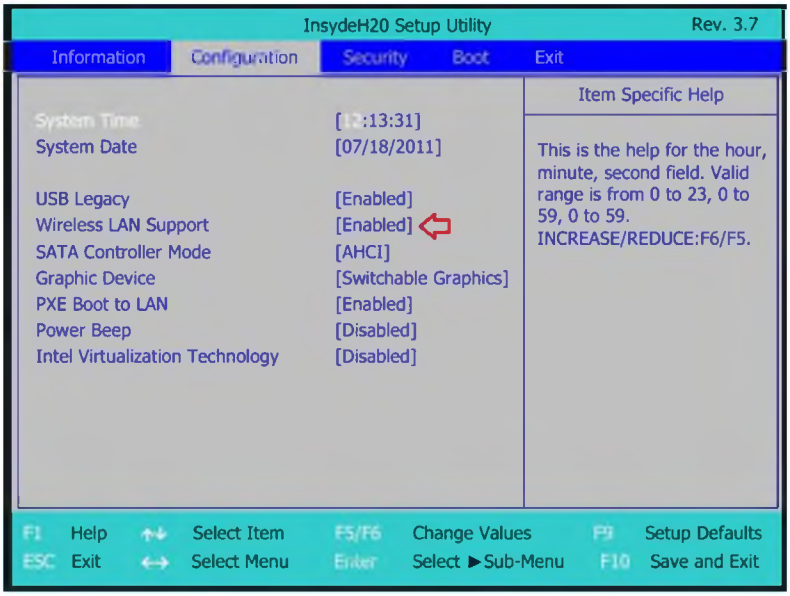
2.2 באם לא ניתן להצטייד במצלמה ללא רכיבי IoT מומלץ לנטרל את הקישוריות לאינטרנט בהגדרות המערכת (לשקול נטרול ה- WiFi בהגדרות מערכת ההפעלה).

2.3 במקרים בהם נדרש חיבור לאינטרנט (לצורך צפייה מרחוק או שיקולים אחרים) יש לוודא בקרה מתאימה ומניעת פנייה ודיווחים אוטומטיים לרשת האינטרנט ולכתובות שאינן לגיטימיות. יש לבחון הצפנת תווך התקשורת בהצפנה חזקה (כדוגמת הצפנות מדף AES-256).

2.4 דאגו לבצע עדכוני תוכנה וקושחה בהתאם להמלצות היצרן בערוצים בטוחים ומאובטחים (TRUSTED) - למניעת מניפולציות ואיומי נוזקה[7].

2.5 לאחר כל עדכון, טיפול או שדרוג וודאו כי הגדרות אלו לא שונו והוחזרו להגדרות ברירת המחדל.

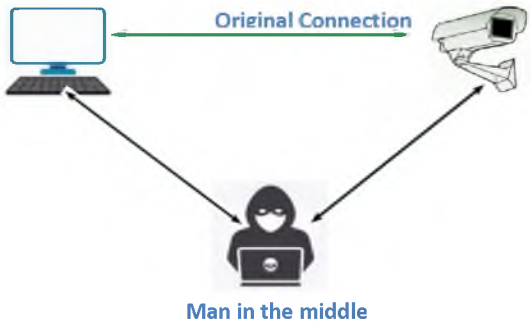
[7] כדוגמת חתימת קובץ העדכונים ע"י היצרן ושליחה בתווך מוצפן



דוגמה לנטרול יכולות wireless במערכת ההפעלה

3. בידוד המצלמה ברשת עצמאית או ברשת מבודדת בהקצאת VLAN ייעודי:

בידוד המצלמה ברשת אוטונומית עצמאית ומאובטחת בהתאם ל- BP תצמצם באופן ניכר את יכולת הגישה ואת הסיכונים הנובעים מהרשת הארגונית עצמה וכן את סיכוני ההתקשרות עם המצלמה ואירועי סייבר אפשריים (התקפת DOS, צפייה לא מורשית, פרטיות ברשת וכד').



תרחיש MITM לתוקף המתערב בתווך (לצורך צפייה לא מורשית והתקפות מתקדמות נוספות)

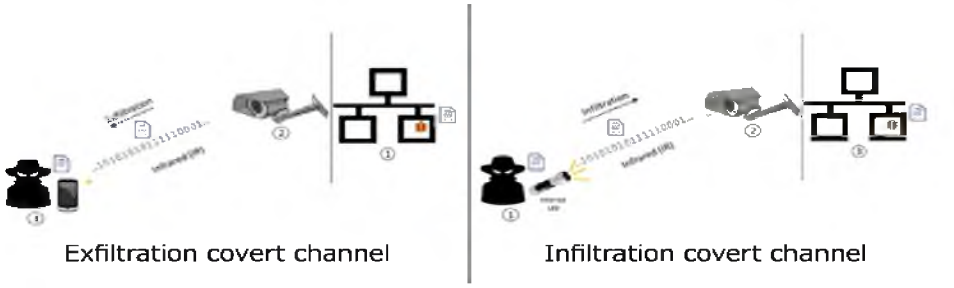
4. <u>המלצות לרשת מבודדת</u>

4.1 ככלל, יש להעדיף לבודד את המצלמה ומערכות האבטחה **לרשת סגורה ומאובטחת בהתאם ל-** BP לצמצום סיכונים מרשת האינטרנט.

4.2 יש לתת מענה מתאים ולצמצם את סיכוני הסייבר הנובעים ממצלמות המבודדות ברשתות סגורות. **בתוך כך, מניעת גישה, הסתרה, הקשחת תחנות וכד'**. פעילויות מחקר

שונות הוכיחו יכולת התקשרות מרחוק ותקיפה של מצלמות אבטחה המחוברות לרשתות סגורות לצורכי ניצול והזלגת מידע או גישור לרשתות מסווגות.[8]

4.3 מומלץ לשקול **הצפנת תוך התקשורת כמעגל אבטחה נוסף** (גם ברשת סגורה).



מתוך מחקר - aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR) - **אוניברסיטת בן גוריון**

5. <u>המלצות ל- VLAN ייעודי (לאחר תהליך ניהול סיכונים)</u>

5.1 במצב בו לא ניתן לבודד ברשת סגורה, יש להגדיר VLAN ייעודי לאחר הגדרות SECURITY VLAN BP וארכיטקטורה מאובטחת, הכוללות גם הגדרות לחומת אש וחוקיות ניטור לאירועי אבטחה מתאימים. בין היתר, הגדרות לניטור תקשורת לא רצויה עם המצלמות מחוץ לארגון פנימה או מפנים הארגון החוצה.

5.2 מומלץ לבחון הגדרות טכנולוגיות למניעת התקפות DOS (למניעת פגיעה ברצף הפעילות) ובתוך כך ליישם בקרות מתאימות באמצעות כלים כגון: הגדרות במערכות חומת אש, הגבלת כמויות נפח תעבורה לכיוון רשת המצלמות וכד'.

5.3 אל מול האיומים ואירועי התקיפה המתועדים מומלץ כי כל התקשורת מול המצלמות תהייה בתוך מוצפן.

5.4 הרשאות מחשב לצפייה במצלמה מחוץ לארגון מחייבות הליך של ניהול סיכונים ומתן התייחסות בהגדרות אותנטיקציה מתקדמות לזיהוי המשתמש וכתובת הרכיב ייעודי (לדוגמה: אימות דו שלבי והרשאת פניית מחשב לפי כתובת IP מאושרת לפי WHITE LIST), במטרה למנוע איומי MITM ושימוש לא מורשה.

[8] Mordechai Guri, Boris Zadov, Yuval Elovici. "**LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED**". Detection of Intrusions and Malware, and Vulnerability Assessment - 14th International Conference, DIMVA 2017: 161-184

תהליך אימות דו שלבי בגישה מרחוק

5.5 המחשבים והרכיבים המורשים לצפייה יוקשחו בהתאם ל- BP לאבטחת תחנת קצה או MDM לרכיבים ניידים המאושרים לצפייה (כול שכן שמדובר ברכיבים מרוחקים ולא בסביבת הארגון).

המלצות נוספות לאבטחת הרשת - ראו תורת ההגנה בסייבר לארגון (בקישור[9]).

בקישוריות לענן יש לוודא בנוסף יישום בקרות הגנה לשירותי ענן (בקישור[10]).

6. הגדרות אבטחה בהפעלה ראשונית והגדרות אבטחה כלליות

ספקיות מצלמות אבטחה מובילות מאפשרות הגדרת אבטחה כבר בשלב ההתקנה ובתוך כך:

6.1 מנגנון לנעילת מצלמה בסיסמה. חלק מהספקיות מאפשרות הגדרות נעילת מצלמה בסיסמה במנגנון המחייב סיסמה חזקה (Strong Password Enforcement)[11].

[9] https://www.gov.il/he/Departments/policies/cyber_security_methodology_for_organizations
[10] https://www.gov.il/BlobFolder/policy/cloud_services/he/Use%20of%20Cloud%20Services.pdf
[11] https://technet.microsoft.com/en-us/library/ff741764.aspx - Best Practice Strong Password Enforcement

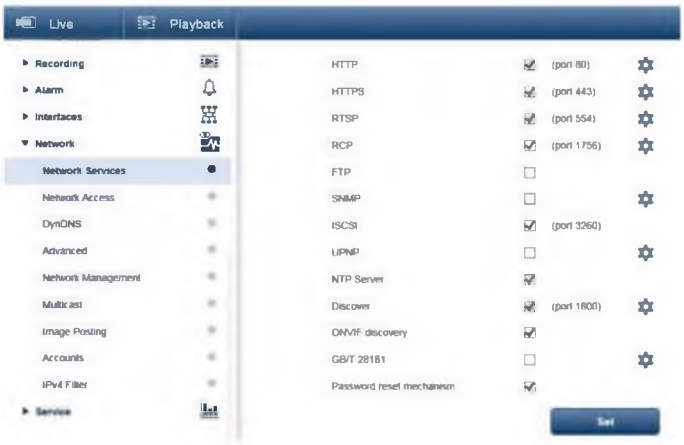
דוגמה למסך של אחת מהיצרניות המחייב סיסמה חזקה בעת התקנה

6.2 הקצאה וניהול הרשאות צפייה (רמה 1 - הרשאת צפייה בווידאו חי, רמה 2- הרשאה צפייה בווידאו חי, הקלטות ויכולת שליטה, רמה 3- הרשאת טכנאי).

6.3 הגדרות FIREWALL מקומיות להגדרה או חסימת פורטים.

6.4 חסימת ב- DEFULT תקשורת http.

6.5 תשומות למניעת איפוס סיסמה.



דוגמה למסך ה- Network Service **של אחת מהיצרניות**

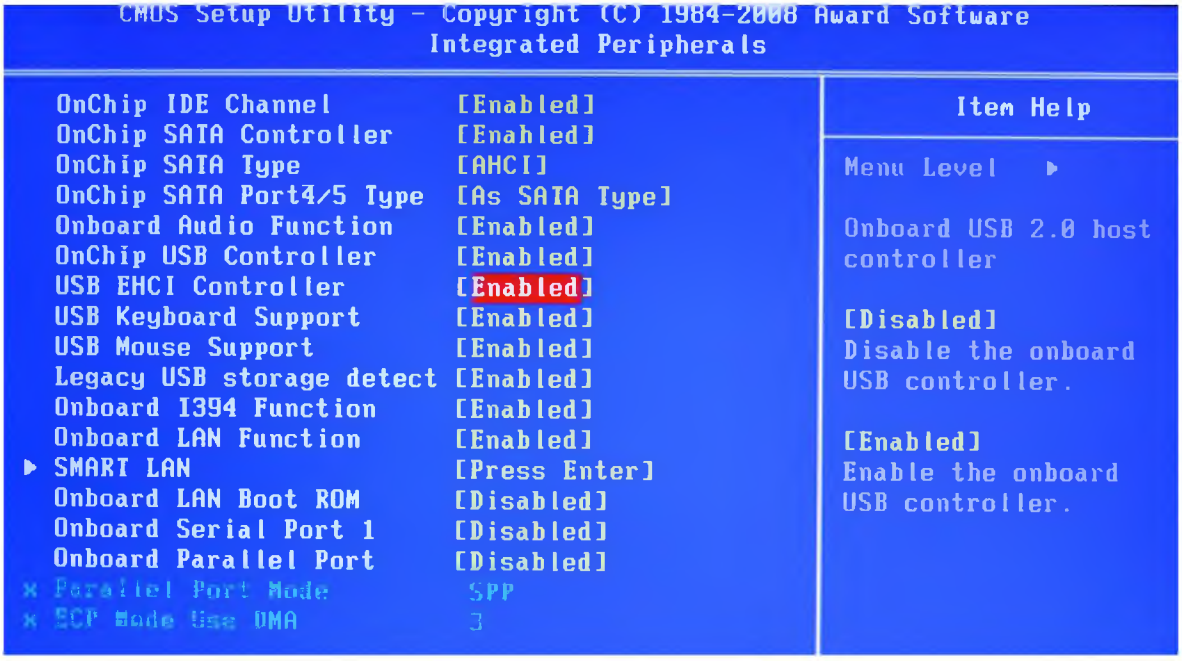
6.6 שימוש בפרוטוקול 802.1X - פרוטוקול מגדיר בקרה על הגישה בין לקוח לשרת, המאפשר מניעת גישה של לקוחות לא מורשים להתחבר אל רשת LAN דרך PORTS זמינים (ומצמצם את איומי MITM וצפייה לא מורשית במצלמות).

6.7 ניהול הרשאות צפייה (לפי 3 רמות).[12]

7. <u>תשומות אבטחה פיזית ומניעת גישה למצלמות ורכיבי הקצה</u>

7.1 כחלק מתהליך צמצום סיכוני הסייבר וטיפול בתחנות הקצה (לצורך גניבה, החדרת קוד עוין וכד') יש **לנקוט בתשומות מניעת גישה אל מצלמות האבטחה** (הגבהת מצלמה, בידוד, וכד').

7.2 שימוש במדיה נתיקה (התקני USB למיניהם) הינו אחד מווקטורי התקיפה הנפוצים. על כן, יש לנקוט בתהליך צמצום ונטרול מבוקר של שקעי USB הקיימים במצלמות.



תצלום מסך - דוגמה לנטרול USB במערכת ההפעלה

7.3 הגדרות אנליטיקה ל- TAMPER DETECTION , לזיהוי הסטה של המצלמה, התזה של נוזל, טשטוש עדשות, שינוי פוקוס, שוטטות בסביבת המצלמה, התארגנות בקרבת מקום וכד'.

[12] רמות הרשאת צפייה - רמת הרשאה 1 - צפייה בוידיאו חי בלבד, רמת הרשאה 2 – צפייה בוידאו חי, הקלטות ויכולת שליטה, רמת הרשאה 3 – הרשאת טכנאי

8. צמצום סיכוני סייבר בתהליכי תחזוקה, תמיכה וטיפול במצלמות

8.1 הטיפול במצלמות יתבצע בתהליכים מבוקרים ע"י גורם מורשה (מהימן).

8.2 תהליכי עדכונים למצלמות יתבצעו בהתאם להמלצות היצרן ובתהליכי מאובטחים ומהימנים (למניעת הונאות, התערבות בתווך ואיומי MITM).

8.3 שינוי והקשחת סיסמאות הטכנאי וסיסמאות ה- Default לסיסמאות מורכבת לצורך מניעת גישת לא מורשים וכן התקפות המבוססות על אינדקס סיסמאות Default והתקפותGUESSING PASSWORD.

8.4 כחלק ממדיניות סיסמאות, יש להימנע מהעברת הסיסמה לגורמים אחרים. החלפת סיסמאות אחת לחצי שנה (או בהתאם למדיניות הארגון) ובכול תהליך של תחלופה\ עזיבת עובד בעל גישה והרשאה

8.5 יש לוודא כי הגדרות המצלמה מאפשרת טעינה של גרסת קושחה רק בקובץ חתום על ידי היצרן

8.6 במטרה לצמצם סיכוני באגים וקודים עוינים יש לוודא כי לא ניתן להתקין על המצלמה מוצרי תוכנה מצד ג' או תוכנת OPEN SOURCE שאינם מאושרים. מקטעי קוד המקור ישולבו לאחר תהליך CODE REVIEW של קוד המקור או המקטע המשולב ע"י גורמים ותהליכים מהימנים) לדוגמה, השוואה בין קבצי HASA חתומים ע"י היצרן בשלב התקנת התוכנה.

ביבליוגרפיה

- תורת ההגנה בסייבר לארגון, משרד ראש הממשלה - מערך הסייבר הלאומי, גרסה 1.0

- B. Krebs, "Hacked Cameras, DVRs Powered Todays Massive Internet Outage, " October 2016.
- Mordechai Guri, Boris Zadov, Yuval Elovici. "LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED".
- Mordechai Guri, Dima Bykhovsky, Yuval ElovicialR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security
  Cameras & Infrared (IR)"
- Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. "xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs"
- IoT Goes Nuclear: Creating a ZigBee Chain Reaction Eyal Ronen(B) , Colin O' Flynny, Adi Shamir and Achi-Or Weingarten Weizmann Institute of Science, Rehovot, Israel
- Best Practice Strong Password Enforcement - https://technet.microsoft.com/en-us/library/ff741764.aspx

נספחים

נספח א' - תשומות נדרשות ומענים להפחתת סיכונים (במעגלי אבטחה שונים)

	הפחת סיכון שימוש וצפייה לא מורשית	צמצום סיכוני IoT	הפחתת סיכון לצורך שיבוש תעבורה או מחיקת הקלטות	הפחתת סיכוני DDOS להשבתה או מניעת שירות	חדירה דרך רשת המצלמות למערכות הארגוניות
אותנטיקציה	V	V	V		
הקצאת רשת מבודדת (תלוי צרכים, ארגון ומדיניות)	V		V	V	V
הקצאת VLAN ייעודי	V		V		
הגדרות אבטחה IoT	V	V	V	V	
תשומות ביטחון לתמיכה ותחזוקה	V	V	V		V
תשומות למידור המצלמות ומניעת גישה	V		V		V

נספח ב' - טבלת דוגמה למאפייני השוואת דרישות בין יצרנים לפני רכישה

דרישה הכרחית	יצרן א'	יצרן ב'	יצרן ג'	יצרן ד'	יצרן ה'	יצרן ו'
3 רמות אבטחה	√	√	√	√	√	√
סיסמה חזקה	√	√	×	×	×	√
FIRMWARE signed Vendor	×	×	×	×	√*	√
Not allow 3rd party software	×	×	×	×	באופן חלקי ×	√
SSL	√	√	√	√	√	√
חסימת גישה	√	√	√	√	√	באופן חלקי ×
תקני הצפנה	√	×	×	×	√	√