

משרד הנגב, הגליל והחוסן הלאומי
המשרד לשיתוף פעולה אזורי
אגף הביטחון, חירום, מידע וסייבר

חלק ב'

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

אוקטובר 2024 / V.2

עמוד מס 2 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

תוכן עניינים

1. מבוא..... 3
2. מטרות המסמך..... 3
3. תחזוקה למערכות קיימות..... 3
4. פירוט מערכות הביטחון..... 5
5. חדר התקשורת..... 14
6. שולחנות המאבטחים ועמדת הקבלה..... 14
7. מוקד הביטחון..... 14
8. קווי VPN..... 15
9. תחום הסייבר-בקרת גישה לוגית..... 15
10. הקשחת מערכת..... 16
11. חשבונות משתמשים ופעילות (SESSION)..... 16
12. הגנה על מידע..... 17
13. תפעול שוטף..... 18

אוקטובר 2024 / V.2	מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה
עמוד מס 3 מתוך 19	

1. מבוא

- 1.1. למשרד הנגב, הגליל והחוסן לאומי והמשרד לשיתוף פעולה אזורי, קיימים מספר אתרים שבהם נדרש להתקין לשדרג ולבצע תחזוקה למערכות ביטחון קיימות.
- 1.2. רשימת האתרים (נכון למועד כתיבת המכרז):
 - 1.2.1. בית שר- נגב גליל וחוסן לאומי (ת"א).
 - 1.2.2. בית שר- שיתוף פעולה אזורי (מעלה אדומים).
 - 1.2.3. רשות החברות הממשלתיות- 2 קומות בגן הטכנולוגי בירושלים.
 - 1.2.4. המשרד לשוויון חברתי יוכל גם להשתמש בשירותים כמפורט בנספח זה בהתאם לנקבע במסמכי המכרז.
- 1.3. חברת טנדו מבצעת את תכנון מערכות הביטחון על גבי תוכניות אדריכליות בהתאם לתפיסת האבטחה של מנהל הביטחון.
במסגרת העבודה, נדרש לספק, להתקין ולהפעיל את כלל המערכות המפורטות במסמך זה.
- 1.4. בהתאם להנחיות הגופים המנחים, לא תאושר התקנה של מערכות מתוצרת סין או רוסיה.

2. מטרות המסמך

- 2.1. הגדרת הדרישות הטכניות, המקצועיות, הפונקציונאליות והפרויקטאליות לטובת אספקה, התקנה, תחזוקה ומימוש המערכות המתוכננות.
- 2.2. הגדרת סל מוצרים מגוון ורחב המכיל את כל סוגי האמצעים הנדרשים למענה המבצעי עבור פרויקט זה.

3. תחזוקה למערכות קיימות

- 3.1. ב-2 האתרים של הבתי השרים נדרש לבצע תחזוקה שידרוג והוספת אמצעים בהתאם להחלטת מנהל הביטחון.
- 3.2. נדרש לבצע שדרוג למערכות הבאות:
 - 3.2.1. בקרת כניסה.
 - 3.2.2. מע' ניהול וידאו.

אוקטובר 2024 / V.2

עמוד מס 4 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

תכולת העבודה המפורטת לאחר החלטה של מנהל אגף הביטחון, חירום, מידע

וסייבר.

- 3.3. באתר רשם החברות הממשלתיות לא קיים תכנון.
- 3.4. לתכולת העבודה המפורטת במסמך זה תצורף תוכנית פריסת אמצעים שעל פיה ימומש פרויקט זה.
- 3.5. ביצוע התקנת האמצעים השונים, לרבות תשתיות תומכות, יבוצע בהתאם לפריסת האמצעים בכל קומה.
- 3.6. המערכות אשר יותקנו יהיו מודולאריות ויאפשרו הגדלה והרחבה ככל שיידרש בכל שלב.
- 3.7. כלל מערכות הביטחון באתר יתממשקו למערכת שו"ב מרכזית (במטה המשרדים בירושלים) אשר תאפשר עבודה מרוכזת במוקד הביטחון ועמדת המאבטח, זאת לצד יכולת הפעלה של כל תת מערכת באופן פרטני ונפרד ממערכת השו"ב.
- 3.8. המערכות אשר יותקנו באתר הלקוח:
 - 3.8.1. טמ"ס (טלויזיה במעגל סגור)
 - 3.8.2. פריצה/מצוקה
 - 3.8.3. בקרת כניסה
 - 3.8.4. וידאופון
 - 3.8.5. מולטימדיה
 - 3.8.6. *WIFI*
 - 3.8.7. *LPR*
 - 3.8.8. קווי *VPN*

אוקטובר 2024 / V.2

עמוד מס 5 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

4. פירוט מערכות הביטחון

4.1. טמ"ס

4.1.1. מערכת ניהול וידאו תהיה *Over Ip* מסוג *NVR* המבוססת על חומרת

מחשוב ושרתים סטנדרטיים ותומכת *Client - Server*.

4.1.2. יכולת אחסון החומר המוקלט תהיה למשך 30 יום לפחות 24 שעות

ביממה.

4.1.3. המצלמות בכל קומה יחווטו לריכוז קומתי אשר קיים בחדר תקשורת

בכל קומה.

4.1.4. כלל הריכוזים יקשורו לריכוז הקומה הבאה עד לארון תקשורת הראשי

בקומת המרתף.

4.1.5. רצפי הוידאו ינוהלו וישמרו בשרתים ייעודיים בארון.

4.1.6. ניהול כלל המצלמות יהיה מעמדת המוקד ומעמדות המאבטחים תהיה

צפייה במצלמות הרלוונטיות לכל עמדה.

4.1.7. בקומת משרד פיתוח הנגב והגליל יותקנו מצלמות אבטחה מסוג

DOVE (כיפה) ומסוג צינור *Bullet* לכיסוי של האזורים הבאים :

- לובי המעליות
- מעברים ראשיים
- מסדרונות המועצה
- עמדת הבידוק
- חדרי תקשורת
- חדר נשק

4.1.8. רזולוציית המצלמות תהיה לפחות *4mp* בהתאם למפרט הטכני המצורף

למסמך זה.

4.1.9. כלל המצלמות החיצוניות יהיו בעלות מיגון אנטיונדלי, בהתאם

להגדרות המפרט הכללי.

4.1.10. המצלמות יותקנו ע"ג תקרה אקוסטית.

אוקטובר 2024 / V.2

עמוד מס 6 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

4.2. מערכת פריצה

- 4.2.1. במסדרונות המתחם ובחדרים קריטיים יותקנו גלאי פריצה לטובת התראה במקרה של חדירה לא מאושרת למתקן.
- 4.2.2. כלל אמצעי הפריצה יחווטו אל רכזת הרחבה קומתית אשר תקשור אל רכזת הפריצה הראשית בחדר התקשורת אשר נמצא בקומת המרתף.
- 4.2.3. פרט לגלאי נפח תקרתיים המתוכננים בקומה, יחווטו אל הרכזת גם מתגים מגנטיים על הדלתות המבוקרות לטובת התראה במקרה של "דלת מוטרדת".
- 4.2.4. בכל חדר תקשורת קומתי יותקן מתג מגנטי לאינדיקציה על פתיחת הדלת וגלאי נפח תקרתי אשר ינוטרלו וידרכו מלוח מקשים אשר יותקן בתוך החדר.
- 4.2.5. בחדר הנשק יותקנו מתג מגנטי, גלאי נפח תקרתי, גלאי כספת משולב אשר יחוברו לרכזת 1337 עפ"י תקן המשטרה למיגון חדרי נשק.
- 4.2.6. מערכת הפריצה תתממשק עם מערכות נוספות כגון מערכת הטמ"ס ומערכת השו"ב.

אוקטובר 2024 / V.2

עמוד מס 7 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

4.3. מערכת בקרת כניסה וניהול תנועת אדם

- 4.3.1. ייעוד המערכת הינו חוצץ בין האזורים לטובת מידור המקום.
- 4.3.2. לטובת מידור כל קומה ובקרה על תנועת האנשים הנכנסים\יוצאים מהאתר תוכננו מספר דלתות מבוקרות בכל קומה ומגנומטר בחדר הבידוק שבקומת המרתף.
- 4.3.3. כלל אמצעי הבקרה יחווטו אל בקרי הדלתות בריכוזים קומתיים אשר נמצאים בחדר התקשורת הקומתי.
- 4.3.4. ריכוז מכל קומה יחובר אל הריכוז הראשי אשר נמצא בחדר התקשורת הראשי בקומת המרתף.
- 4.3.5. כיוון הבקרה יהיה לפי מיקום קורא הקרבה בתוכניות.
- 4.3.6. אמצעי בקרת הכניסה לרבות קוראי קרבה, לחצני פתיחה, קופסאות ניפוץ וכיו"ב, יבוצעו בהתאם לפרטי הדלתות השונים כפי שמופיע בתוכנית פריסת האמצעים עבור כל דלת באופן פרטני.
- 4.3.7. במסגרת הפרויקט יותקנו מס' סוגי מנעולים (בהתאם לפרט הדלת):
 - מנעול אלקטרומכאני (נטרק ננעל).
 - מנעול אקטרומגנטי.
 - מנעול חשמלי זוויתן.
- 4.3.8. בין פרטי הדלתות קיימת דלת לא מבוקרת עם מתגים מגנטיים לטובת אינדיקצית פתיחה בלבד.
- 4.3.9. כל דלת תמוגן בהתאם לפרט הפירזול של הדלת (חומר, חד/דו כנפי), יעוד הדלת (אש/מילוט) ותפיסת האבטחה.

אוקטובר 2024 / V.2

עמוד 8 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

4.4 מערכת אינטרקום IP

- 4.4.1 ברחבי האתר יותקנו אמצעי מערכת וידאופון.
- 4.4.2 המערכת תהיה דיגיטלית - Over IP.
- 4.4.3 בהתאם לתוכניות פריסת האמצעים, יותקנו יחידות קצה של וידאופון אשר יקושרו למוקד, עמדת הקבלה ועמדות המאבטחים.
- 4.4.4 כלל יחידות הקצה יאפשרו תקשורת של היחידה לכל עמדה הנדרשת למענה.
- 4.4.5 מיחידת הווידאופון השולחנית תתאפשר פתיחת דלתות מבוקרות.
- 4.4.6 מיקומי האביזרים יהיו בהתאם למצוין בתוכנית וואו בהתאם לפרט הדלת.

4.5 מערכת השו"ב

- 4.5.1 מטרת המערכת היא תפעול, שליטה ובקרה על אלמנטים שונים בפרויקט באמצעות מערכת אחת מרכזית
- 4.5.2 מערכת השו"ב תאפשר שליטה על ציוד הקצה ואת ניהולן של תתי המערכות בסנכרון ואינטגרציה מלאה, להלן המערכות:
 - מערכת הטמ"ס.
 - מערכת אזעקה/ מצוקה.
 - מערכת בקרת הכניסה.
- 4.5.3 מערכת השו"ב תהיה מערכת פתוחה – יכולת התממשקות לציוד חומרה/ תוכנה, אשר ניתן להתממשק אליו בפרוטוקול כלשהו תוך הגדרתו כחלק מרכיבי המידע המנוהלים ע"י המערכת.
- 4.5.4 חשוב לציין כי מערכת השו"ב, למרות תפקידה החשוב, אינה רכיב קריטי במערכת.
- משמעות הדבר היא שיכולות הניהול והבקרה של כל תת מערכת אמורים להישמר למקרה בו יתגלה כשל במערכת השו"ב.
- 4.5.5 עבודה נוחה וידידותית על גבי מפת האתר.
- 4.5.6 המערכת תתמוך בסט כללים ותרשימים עבור התראות והחיוויים המתקבלים.

אוקטובר 2024 / V.2	מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה
עמוד מס 9 מתוך 19	

4.5.7. המערכת תאפשר יכולת גמישה לגידול והתממשקות לציוד חדש.

4.5.8. המערכת תאפשר הפקת דוחות בחתכים שונים לפי הגדרת המשתמש

4.5.9. כלל מערכות המקור כגון מערכות הטמ"ס, הפריצה, בקרת הכניסה

וכיו"ב יתממשקו למערכת השו"ב באמצעות פרוטוקול תקשורת

TCP/IP

4.5.10. המערכת תסופק יחדיו עם ה-*SDK* וה-*API*.

אוקטובר 2024 / V.2

עמוד מס 10 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

4.6. תשתיות תקשורת כבילה ותיעול

4.6.1. התקשורת עבור מערכות האבטחה הטכנולוגיות באתר תהיה מערכת

תקשורת ייעודית ונפרדת פיזית עבור מערכות האבטחה בלבד.

4.6.2. טופולוגיית הרשת תהיה בתצורת טבעת ותתבטא בקישור סיב אופטי

מכל ארון תקשורת קומתי ומן הארון בקומה האחרונה לארון הראשי בקומת המרתף.

4.6.3. כלל הכבילה של כל מערכות הביטחון יועברו בתיעול נפרד שיוקצה

לטובת ייעוד זה בלבד.

4.6.4. המרחק המרבי בין אביזר הקצה לארון הציוד לא יעלה על 90 מטרים.

4.6.5. ככלל, כבלי התקשורת של המערכות המנהלתיות יועברו בתוואי נפרד

מזה של מערכות הביטחון, אך אופן העברת הכבילה יהיה זהה:

5.6.5.1. תוואי ראשי

5.6.5.1.1. תעלות רשת לאורך המסדרונות, פירי

התקשורת בין המתחמים המקשרים את

ארונות ריכוז הציוד וחדר התקשורת.

5.6.5.1.2. הכבילה תועבר בחלל התקרה האקוסטית

ובפירי התקשורת בתוך תעלות רשת.

5.6.5.1.3. בשטחים בהם לא קיימת תקרה אקוסטיות

תועבר הכבילה בתעלות פח אשר יותקנו על

גבי הקירות והתקרות.

אוקטובר 2024 / V.2

עמוד מס 11 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

5.6.5.2 תוואי משני

- 5.6.5.2.1 המתייחס לכבילה בין אביזרי הקצה לתוואי הראשי.
- 5.6.5.2.2 בנוסף, עבור האמצעים המותקנים בסמוך לתקרה, על הרצפה ועל הקירות ברחבי האתר.
- 5.6.5.2.3 הכבילה מהתעלות הראשיות (תוואי ראשי) תועבר לאמצעי הקצה במיקום התקנתם הסופי באמצעות

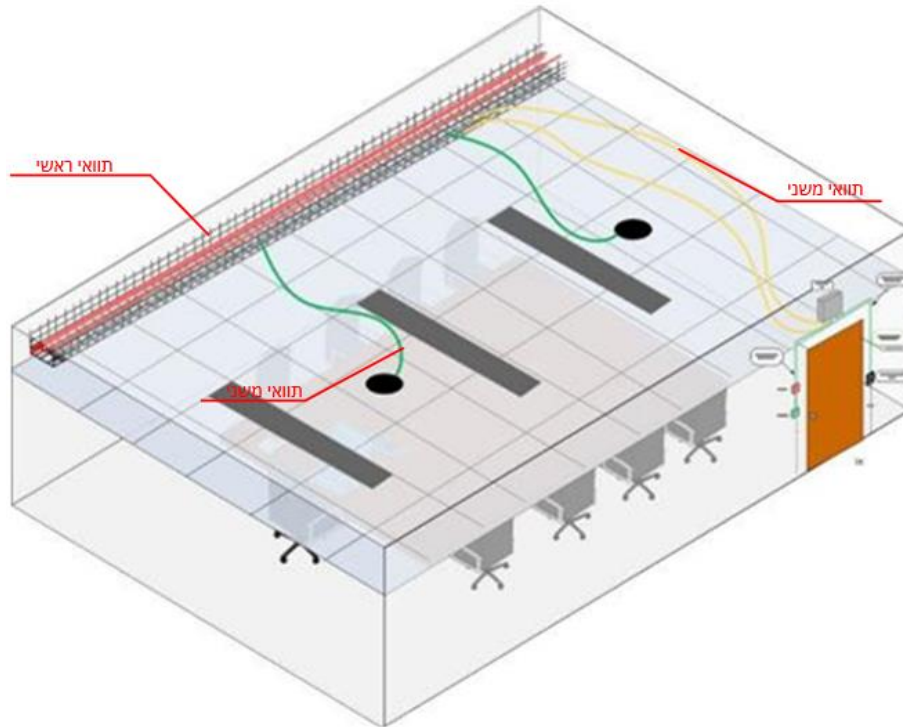
- 4.6.6 במידה ויוחלט על ידי הלקוח כי לא תבוצע תשתית תקשורת פאסיבית נפרדת (אישור בכתב ע"י הלקוח), תשתיות התקשורת (תעלות) יהיו משותפות למערכות נוספות, כלומר: כל הכבלים של כל מערכות האבטחה יועברו בתשתית משותפת לכבלים של מערכות אחרות.
- 4.6.7 במסגרת פרויקט זה, תותקן עבור מערכות הביטחון כבילה ייעודית המופרדת מכל מערכת אחרת.
- 4.6.8 כבלי הנחושת יהיו יעודיים למערכות הביטחון בלבד.
- 4.6.9 כלל הכבלים עבור מערכות הביטחון יהיו בצבע זהה, אשר יהיה שונה מכל כבל אחר של מערכת אחרת לצורך איתורן בנקל.

אוקטובר 2024 / V.2

עמוד מס 12 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

איור ב' – תיאור ההבדל בין תוואי ראשי לתוואי משני



5.6.5.3. גם עבור האמצעים המותקנים ע"ג הקירות, במקומות בהם

קיים חלל בין קיר הגבס לקיר הבטון, תועבר הכבילה כנ"ל.

5.6.5.4. במקומות בהם לא קיים קיר כפול, תועבר הכבילה בחציבה

ביציקות הבטון של הקירות או באמצעות צנורות/תעלות

PVC שיוצמדו לקירות. הכל ע"פ תכנון מראש וסיכום עם

מנהל הפרויקט בכל מיקום ספציפי.

אוקטובר 2024 / V.2	מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה	
עמוד מס 13 מתוך 19		

4.7. הפרדות חשמל

לפי חוק החשמל והתקנים הרלוונטיים יש להקפיד על הפרדות מתח נמוך מאוד ממתח נמוך.

אוקטובר 2024 / V.2

עמוד מס 14 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

5. חדר התקשורת

- 5.1. ככלל, תשתיות תומכות ותשתיות חשמל עבור עמדות המוקד והמאבטחים יבוצעו ע"י קבלן הבינוי והקבלן הזוכה יידרש להתקנת כבילה ייעודית וחיבור האמצעים.
- 5.2. כלל נקודות התקשורת אשר יותקנו בעמדות אלו יקושרו לארון השרתים המרכזי אשר ימוקם בחדר התקשורת.
- 5.3. בחדר זה יותקן מסד, אשר יכיל את החומרות הנדרשות להפעלת כלל המערכות הנדרשות.
- 5.4. הארון יותקן כך שתתאפשר גישה ל- 2 דפנות לכל הפחות.
- 5.5. הארון יוזן מ 2 מקורות חשמל נפרדים לטובת גיבוי (1P, 16A).
- 5.6. בארון יותקן *UPS* לטובת ייצוב המתח ושמירה על רציפות תפקודית- מבצעית בעת נפילת חשמל / החלפה בין מקורות הזנה בעת תקלה.

6. שולחנות המאבטחים ועמדת הקבלה

- 6.1. האמצעים אשר יותקנו על שולחן המאבטחים :
 - 6.1.1. 3 מסכי עבודה (2 ביטחון + אחד מנהלתי).
 - 6.1.2. יחידת וידאופון שולחנית.
 - 6.1.3. מחשב תחנת עבודה לטובת עמדת הקליינט.
 - 6.1.4. מחשב מנהלתי – באחריות הלקוח.
- 6.2. בשולחן המאבטחים יותקנו אמצעי הקצה למערכות האבטחה לרבות מסכי עבודה. חומרות המחשוב של תחנות העבודה יותקנו בחדר השרתים ויקושרו לאמצעי הקצה באמצעות מרחיקים
- 6.3. בחדר הבידוק יותקן מגנומטר אשר יוזן משקעי 220V.
- 6.4. בכל שולחן המאבטח תהיה קופסת חיבורים הכוללת ריכוז חשמל ותקשורת להעברת התשתיות הנדרשות לקיום מערכת הביטחון הנדרשת לעמדה.
- 6.5. מקבץ החשמל יכיל 4 שקעי חשמל מגובי חשמל על ידי *UPS* ושני שקעי תקשורת.
- 6.6. תעלות התשתית הנ"ל יהיו נפרדות.

7. מוקד הביטחון

- 7.1. במוקד הביטחון יותקנו 2 עמדות עבודה.
- 7.2. בנוסף לעמדות העבודה יותקנו 4 מסכי קיר לטובת שיקוף מסך עמדת העבודה.

אוקטובר 2024 / V.2	מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה	
עמוד מס 15 מתוך 19		

7.3. כלל אמצעי הוידאו יקושרו למחשב שמותקן בארון שרתים בעזרת מרחיקים.

8. קווי VPN

8.1. באחריות קבלן הביצוע להוסיף קווי *VPV* בהתאם לצורך התעבורה, שליטה, תפעול ופיקוח מהמוקד המרכזי שבמטה במשרדים על שאר האתרים.

9. תחום הסייבר- בקרת גישה לוגית

- 9.1. נדרש כי מערך המצלמות (*NVR, DVR* וכדומה) אינו חשוף
- 9.2. לאינטרנט. בהינתן כי נדרשת גישה מרחוק מומלץ לנקוט בצעדים הבאים:
 - 9.2.1. מתן גישה בהתאם ל-*Allowlist* פרטני של כתובות מורשות.
 - 9.2.2. מתן גישה באמצעות שימוש ב-*VPN* או *SDP*.
- 9.3. אירוח דף המצלמה כ-*Iframe*, וחשיפתו כדף אתר אינטרנט המוגן באמצעות *WAF* ו-*IPS*.
- 9.4. נדרש כי הגישה למערך המצלמות מוקנית בהתאם לעקרון מתן רמת גישה נמוכה (*Least Privielge Access*), וזאת החלת בקרת גישה הן ברמת ה-*FW*. ארגוני, והן ברמת ההתקן עצמו (מצלמה, *DVR* וכדומה).
- 9.5. נדרש כי מערך המצלמות מוטמע בסגמנט או *VLAN* ייעודי שאינו מקושר לנכסי הסייבר האחרים של הארגון. בארגון בעל רמת סיכון בינונית ומעלה מומלץ לכל הפחות לממש *Microsegmentation*.
- 9.6. נדרש באופן רציף כי לא ניתן לחבר לרשת המצלמות נכסי סייבר לא מורשים, וזאת על-ידי שימוש באלמנט זיהוי חד-ערכי של נכס הסייבר, אשר לא ניתן
- 9.8. בקלות לזייפו או לשכפלו.
- 9.9. דוגמא ליישום: מימוש פרוטוקול *x802*. במערך תקשורת הנתונים תוך שימוש במערכת *NAC*, ותהליך אימות מבוסס פרוטוקול *TLS-EAP*.
- 9.10. נדרש כי גישה לממשק הניהול תתבצע מתוך הארגון וזאת באמצעות רשת *OOB*.
- 9.11. נדרש תעבורת מצלמות האבטחה הזוכה לתעדוף, כך שבמקרה של אירוע סייבר או עומס חריג, ניתן יהיה לגשת לממשק הניהול. דוגמא ליישום: שימוש במנגנון *QoS*.

אוקטובר 2024 / V.2

עמוד מס 16 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

9.12. נדרש כי נקודות רשת שאינן פעילות יוגדרו במתג התקשורת ב"מצב קר" (*Shutdown*).

10. הקשחת מערכת

10.1. נדרש כי במסגרת פיתוח מערך המצלמות היצרן מימש עקרונות מקובלים לעיצוב מאובטח, ולעיצוב לפרטיות, וכי מנגנוני האבטחה למימוש עקרונות אלו מופעלים כברירת מחדל.

10.2. נדרש יחסים אפשרות לעבודה עם פרוטוקולים פגיעים. להלן דוגמא לפרוטוקולים פגיעים:

10.2.1 *Telnet HTTP*

10.2.2 *SSL FTP TFTP*

10.2.3 *TLS v1.0*

10.2.4 *TLS v1.1*

10.3 *UpnP SNMP v2*

10.4. נדרש יחליף את התעודה הדיגיטלית שמגיעה באופן מובנה (ברירת מחדל) בתעודה ייעודית למטרה זו.

10.5. נדרש עיקור או חסימה של ממשקים פיזיים שאינם נדרשים לעבודה

10.6. שוטפת דוגמת ממשק *USB*, ממשק *RS-232* וממשק *RS-458*.

10.7. דוגמא ליישום:

10.7.1. שימוש בחסם פיזי למניעת חיבור לא מורשה לממשק *USB*.

10.8. נדרש כי פעולות קריפטוגרפיות מתבצעות ברמת מעבד (*Chip*) ההתקן, ולא ברמת מערכת ההפעלה/האפליקציה. דוגמא ליישום: שימוש ב-*TPM*.

10.9. נדרש יבצע בדיקה עיתית רציפה לאיתור חריגות בהגדרות תצורה וקבצים. דוגמא ליישום: מימוש *FIM*.

10.10. נדרש סנכרון של שעון רכיבי מערך המצלמות מול שעון זמן מהימן פנים ארגוני.

10.11. נדרש כי המשתמש אינו יכול לשמור את פרטי ההזדהות בצד-לקוח (דוגמת שם משתמש וסיסמה בדפדפן), וזאת במטרה למנוע אפשרות לביצוע *Login* אוטומטי.

11. חשבונות משתמשים ופעילות (*Session*)

11.1. נדרש כי לא נעשה שימוש בסיסמאות ברירת מחדל (*Default Password*),

סיסמאות זהות באתרים/שירותים שונים או סיסמאות קלות לניחוש. כבקה

אוקטובר 2024 / V.2

עמוד מס 17 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

מונעת מוצע לרכוש מצלמות שכוללות מנגנון מובנה של שינוי סיסמת ברירת מחדל.

- 11.2. נדרש כי הסיסמאות אינן מאוחסנות באופן גלוי (*Cleartext*) בהתקן. דוגמא ליישום: וידוא כי היצרן מימש מנגנון לאחסון סיסמאות הכולל מימוש *Hash + Dynamic Salt*.
- 11.3. נדרש יעשה שימוש ב-*MFA*, בהינתן כי הדבר ישים.
- 11.4. נדרש החלת נעילת חשבון משתמש (*Account Lockout*) לאחר 5 ניסיונות הזדהות לא מוצלחים, וזאת למשך 60 דקות לפחות.
- 11.5. נדרש ניתוק מצד שרת של חשבון משתמש שאינו פעיל מעל 5 דקות.
- 11.6. נדרש הגבלה של מספר הפעילויות אשר חשבון משתמש מסוגל לעשות בהן שימוש בזמן נתון (*Session Throttling*).
- 11.7. מומלץ לוודא החלת עקרון מתן הרשאות נמוכות (*Least Privilege*) ומתן גישה בהתאם לעקרון הצורך לדעת (*Know to Need*). בכלל זה התייחסות להרשאת צפייה בזמן אמת (*Live*), עיון בהקלטה, שידור חוזר (*Playback*), הוצאת סרטון, ארכיון, שימוש ביכולות המצלמה, וכדומה. בכלל זה מומלץ לבצע הפרדה בין בעלי תפקיד שונים על-ידי שימוש ב-*RBAC* או מודל אחר.
12. **הגנה על מידע**
 - 12.1. נדרש הצפנה של מידע רגיש/חסוי במנוחה (*At Rest*). ראוי לציין כי חלק מיצרני הפתרונות מממשים דרישה זאת כחלק מתהליך הקידוד (*Encoding*) של ההקלטה.
 - 12.2. נדרש כי הגישה לממשקי הניהול ושינוע המידע בתווך (*In Transit*) מתאפשרים בכפוף להחלת הצפנה עדכנית וסטנדרטית. דוגמא ליישום: שימוש בפרוטוקול *TLS1.3* ואלגוריתם *Bit 256 AES* לטובת הצפנה סימטרית.
 - 12.3. נדרש כי סיסמת המשתמש אינה נשלחת *As is* על התווך. דוגמא ליישום: שימוש ב-*Digest Authentication*.
 - 12.4. נדרש כי בזמן אמת ההקלטה נחתמת דיגיטלית ו/או מתווסף לה חתימת מים (*Watermark*) ייעודי לכל לִּפְסֵי לִּפְסֵי (*Frame*), וזאת במטרה לוודא וידוא מקוריות, מהימנות ושלמות של ההקלטות.
 - 12.5. נדרש כי שמירת המידע שנקלט במצלמה ועיבודו עומד בהוראות החוק הרלוונטיות, ובכלל זה חוק הגנת הפרטיות והתקנות מכוחו.

אוקטובר 2024 / V.2

עמוד מס 18 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

- 12.6. נדרש את מיקום ואופן אחסון המידע שנקלט במצלמה ומעובד על ידה.
- 12.7. נדרש עם הספק/יצרן אם יש לו נגישות למידע שמוקלט ומעובד על ידי המצלמה. אם כן, ואם אין ברירה להשתמש במצלמה כאמור, מוצע לוודא מה השימושים שהוא יכול לבצע במידע ומי יכול לבצע את השימוש.
- 12.8. נדרש יבצע באופן עתי בדיקה לאיתור ניסיונות להדלפת מידע רגיש/חסוי באמצעות הסנסורים הקיימים במצלמה.

13. תפעול שוטף

- 13.1. נדרש מחיקה עתית של מידע שאינו נדרש לעבודה שוטפת (*Data Minimization*) או העברה של המידע למערך אחסון בעל רמת אבטחה גבוהה יותר.
- 13.2. נדרש כי לא ניתן למחוק או לשנות הקלטות ומידע רלוונטי במשך תקופה מוגדרת (*Data Retention*). במקרה של העדר תמיכה מובנית על-ידי מערך המצלמות ניתן לממש המלצה זאת על-ידי יכולות אבטחה הקיימות במערכי אחסון מקובלים.
- 13.3. נדרש יטמיע עדכוני אבטחה (פאצ'ים) בהתאם לתדירות המומלצת על-ידי היצרן. בכלל זה, מומלץ לוודא כי מנגנון התקנת עדכוני האבטחה מבצע בדיקה של מקוריות (*Authentic*) ומהימנות רכיב התוכנה לפני ההטמעה בפועל. בכלל זה, מומלץ לקבל פרטי קשר של נציג הספק/היצרן של המצלמה לבירורים ועדכוני אבטחה.
- 13.4. מומלץ לוודא כי היצרן מספק עדכוני אבטחה, ומומלץ לוודא את מועד הפסקת עדכוני אבטחה מטעם היצרן (*EOL*). אם היצרן לא מספק עדכוני אבטחה אז מומלץ להימנע מרכישת המוצר.
- 13.5. נדרש יעביר את הלוגים למערך המצלמות למערכת ה-*SIEM* הארגונית, תוך הגדרת התראות רלוונטיות. דוגמאות ליישום:
- 13.5.1. שימוש בפרוטוקול *Syslog*.
- 13.5.2. שליחת התראה במקרה של חיבור התקן לא מורשה לרשת מערך המצלמות.
- 13.5.3. שליחת התראה בגין אירוע סייבר רלוונטי.
- 13.6. נדרש יגדיר באמצעות חוקי האנליטיקה התרעה על הסטת מצלמה, הסרת מצלמה, הפסקת פעולה של מצלמה, פגיעה באיכות הצילום ואירועים חריגים רלוונטיים.

אוקטובר 2024 / V.2

עמוד מס 19 מתוך 19

מסמך תכולת עבודה להתקנת אמצעי ביטחון ואבטחה

13.8. נדרש גריטה של מצעי אחסון מידע, דוגמת דיסק קשיח, בהתאם לדרישות תקן

4. רמה *IEC/ISO 21964*,

13.9. נדרש כי מצעי אחסון מידע, דוגמת דיסק קשיח, לא יוחזרו לספק/ליצרן.

13.10. נדרש יגדיר בנוהל עבודה תהליך סדור ומידי של החלפת סיסמאות בתום פעילות

גורם חיצוני. דוגמא ליישום: בסיום טיפול בתקלה יתבצע הליך מידי להחלפת כל

הסיסמאות של כלל החשבונות אשר גורם התמיכה החיצוני נחשף אליהן.