

## הנדון : המלצות לצמצום סיכוני סייבר ממצלמות אבטחה

ישנם בתי ספר הבוחרים לעשות שימוש במצלמות אבטחה על מנת לשמור על בטחונם ומגנותם של התלמידים והמורים במוסד החינוכי.

חוזר המנכ"ל "מצלמות במוסדות חינוך – הסדרת הכנסתן ואופן התקנתן" מסדיר את הליך ההתקנה והשימוש במצלמות במוסדות חינוך. החוזר מדגיש את החשיבות בשמירה על הזכות לפרטיות ובמניעת פגיעה בצנעת הפרט. סעיף 7 בחוזר המנכ"ל מפרט את ההנחיות לאופן התקנת ותפעול המצלמות בהיבטי אבטחת מידע. לאחרונה פירסם מערך הסייבר מסמך המלצות כללי למשק העוסק בצמצום סכנות סייבר ממצלמות אבטחה. המסמך של מערך הסייבר מיועד לכלל המשק. להלן סיכום ההמלצות והדגשים העיקריים במסמך הרלוונטיים למוסדות חינוך:

### בידוד המצלמה ברשת עצמאית או ברשת מבודלת בהקצאת VLAN ייעודי :

#### **המלצות לרשת מבודדת**

- ככלל יש להעדיף לבודד את המצלמה ומערכות האבטחה לרשת סגורה ומאובטחת לצורך צמצום סיכונים מרשת האינטרנט
- יש לתת מענה מתאים ולצמצם את סיכוני הסייבר הנובעים ממצלמות המבודדות ברשתות סגורות. בתוך כך מניעת גישה, הסתרה, הקשחת תחנות וכד'

#### **המלצות ל VLAN ייעודי**

- במצב בו לא ניתן לבודד את המצלמות ברשת סגורה, יש להגדיר VLAN ייעודי לאחר תכנון ארכיטקטורה מאובטחת, הכוללת גם הגדרות לחומת אש וחוקיות לניטור אירועי אבטחת מידע. בין היתר הגדרת תקשורת לא רצויה עם המצלמות מחוץ לארגון פנימה או מפנים הארגון החוצה.
- מומלץ לבחון הגדרות טכנולוגיות למניעת התקפות DDOS
- מומלץ כי כלל התקשורת מול המצלמות תהיה בטווח מוצפן.
- הרשאות מחשב לצפייה במצלמה מחוץ לארגון מחייבות התייחסות כגון הגדרות אותנטיקציה מתקדמות (לדוגמה אימות דו שלבי והרשאת פניה למחשב לפי כתובת IP מאושרת לפי white list), במטרה למנוע איומי MITM ושימוש לא מורשה.
- המחשבים והרכיבים המורשים לצפיה יוקשחו.

### הגדרות אבטחה בהפעלה ראשונית והגדרות אבטחה כלליות

ספקיות מצלמות אבטחה שונות מאפשרות הגדרות אבטחה כבר בשלב ההתקנה ובתוך כך :

- מנגנון לנעילת מצלמה בסיסמה
- הקצאה וניהול הרשאות צפייה
- הגדרות Firewall מקומיות או חסימת פורטים.
- חסימת תקשורת http
- תשומות למניעת איפוס סיסמה
- שימוש בפרוטוקול 802.1X

### **מניעת גישה פיזית למצלמות**

- יש לנקוט בצעדים למניעת גישה אל מצלמות האבטחה (הגבהה, בידוד וכד')
- צמצום ונטרול של שקעי ה-USB הקיימים במצלמות

### **צמצום סיכוני סייבר בתהליכי תחזוקה, תמיכה וטיפול במצלמות**

- הטיפול במצלמות יבוצע על ידי גורם מורשה
- תהליכי עדכון למצלמות יבוצעו בהתאם להמלצות היצרן
- שינוי והקשחת ססמאות הטכנאי וססמאות ה-Default

לשאלות ובירורים בנושא ניתן לפנות ליחידת אבטחת המידע בבתי ספר:

[school\\_security@education.gov.il](mailto:school_security@education.gov.il)