אבטחת מערכות מידע

ביקורת מעקב

חטיבת השירות

אגף מערכות מידע ומחשוב

אבטחת מערכות מידע
ביקורת מעקב

1. בשנת 2021 נערכה ביקורת מקיפה בתחום אבטחת המידע אשר תפס תאוצה בשנים האחרונות, לאור הגידול הרב בהיקף השימושים בכלים טכנולוגיים.
2. פעילות עובדי העירייה מחייבת הסתייעות במידע אישי רב על תושבים, בעלי עסקים, ספקים ועוד, ועל כן חלה על העירייה החובה לעמוד בדרישות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו.
3. בנוסף, שימוש בטכנולוגיות אלו חושף את העירייה לסיכונים חדשים אשר על הנהלת העיר לתת את דעתה עליהם.
4. ביקורת המעקב בדקה את אופן תיקון הליקויים ויישום ההמלצות, כפי שפורטו בדוח הביקורת, ובהתייחס לשינויים שחלו בתחום זה.
5. הביקורת התרשמה, כי מאז הביקורת ועד למועד ביקורת המעקב בוצעו פעולות רבות ושינויים רבים על מנת לשפר ולשדרג את תחום אבטחת המידע בעירייה, כולל הגדלת המשאבים הכספיים לעניין זה.
6. מנהל מערכות מידע ומחשוב מציין, כי מלבד תיקון ליקויים כנובע מדו"ח הביקורת, בוצעו פעילויות רבות נוספות בנושא אבטחת המידע, כגון: החלפת/שדרוג Fire Wall, חסימת התחברות מחו"ל, תרגילי דיוג , מערכות אבטחה EDR , NAC – אפיון מחדש, ובחירת מוצר מומלץ/משכ"ל, ייעוץ למימוש העברת מידע לסקר אזרחים ותיקים, טיפול בהודעות SOC בשוטף, הדרכות עובדים ומנהלי מאגרים, ניסיונות התחברות למאגר "אל תתקשר אלי", הסמכות בניהול מאגרי מידע, התייחסות למכרזים וחוזים: שוטף, השלמת רישום מאגרי מידע, ייעוץ למכרז קורקינטים, אפיון וליווי ביצוע סקר סיכונים ובדיקת חוסן, מענה לסוגיות שונות במהלך קורונה (שנת 2022), טיפול בתקלת אבטחה בביי"ס חשמונאים, טיפול בסוגיות שונות בהעברת מידע בין יחידות עירוניות והגדרת הרשאות שימוש במידע, מענה לסוגיות שונות ביישום חוק חופש המידע, ליווי העברות מידע ליועצים במסגרת התחדשות עירונית, אבטחת מידע סביב מערך המצלמות במרחב הציבורי וחיבור גורמי ביטחון שונים, ביצוע תרגיל מתקפת סייבר במסגרת תרגיל מל"ח ביוני 2023, ועוד.
7. כיום, לאחר פרישתה של ממונת אבטחת המידע, תפקידו של הממונה על אבטחת המידע מתבצע על ידי יועץ אבטחת מידע במיקור חוץ ומנהל ממלא מקום. יש לפעול למינויו של ממונה אבטחת מידע כפי שנדרש בתקנות.

8. להלן ממצאי ביקורת המעקב:

	המלצה מדוח הביקורת בשנת 2021	עדכון המצב
1.	לוודא, כי ממונת אבטחת מידע תהיה כפופה למנהל בכיר בעירייה ולא למנמ"ר כפי שקיים היום. יש לוודא, כי יהיו לה הידע המקצועי והנסיון הנדרשים על פי התקנות, ותיאור תפקידים של משרד הפנים. בסיכום הביקורת, הורתה מנכ"לית העירייה להכפיף את ממונת אבטחת המידע ישירות לסמנכ"לית שירות.	**בוצע.** ממונת אבטחת המידע הוכפפה לסמנכ"לית שירות, אולם פרשה מהעירייה. נסיון לגייס עובד חלופי טרם צלח.
2.	לפעול להכשרת ממונת אבטחת המידע של העירייה, על מנת שהיא תרכוש את הידע המקצועי בתחום זה, ותוכל לפעול בהתאם. מנכ"לית העירייה הנחתה לוודא, כי ממונת האבטחה תרכוש ידע מקצועי זה.	**בוצע.** ממונת אבטחת המידע עברה הכשרה מקצועית, אולם כאמור לאחריה פרשה מהעירייה.
3.	להכין תוכנית לשיפור יכולות אבטחת המידע של העירייה, בהתאם לממצאי סקר הסיכונים. לאור העובדה, כי העירייה נמצאת בתוכנית הבראה ומונה לה חשב מלווה, יש לשקול את האפשרויות בהתאם ליכולתה הכלכלית.	**בוצע.** נעשתה פעילות טיוב בכל המישורים האפשריים בסיוע יועץ אבטחת מידע.
4.	לפעול מול החברה המועסקת ע"י העירייה להשלים את הדיווח למשרד הממשלתי הרלוונטי, על מנת לעדכן את ההוצאה בתב"ר מספר 4173, ולקבל את התקציב.	**בוצע, אך טרם הושלם.** נכון למועד הביקורת, התקבלו 129,848 ₪ מתוך 238,848 ₪ (הקמת רשת דיגיטלית).
5.	לערוך תוכנית עבודה שנתית בנושא אבטחת המידע, המפרטת משימות בעלת יעדים מדידים, לוחות זמנים וגורמים אחראים. על תוכנית העבודה להיות מותאמת לתקציב האגף.	**בוצע.** הוכנה ואושרה תכנית עבודה אשר בוצעה או בתהליך ביצוע, ומתקיים מעקב שוטף לביצועה.
6.	לערוך את הוראות העבודה הישנות בנושאי אבטחת המידע, לעדכנן או לבטלן בהתאם לצורך. יש לוודא, כי ינתן ביטוי גם לנושא גיבויים ושחזורים.	**בוצע.** הוכנה מערכת נהלים חדשה ומלאה, הכוללת גם נוהל המתייחס לגיבויים ושיחזורים.

	המלצה מדוח הביקורת בשנת 2021	עדכון המצב
7.	יש לכתוב נוהל בנושא "התאוששות מאסון" – בהקשר למערכות הממוחשבות.	**בתהליך ביצוע.** קיים נוהל המתייחס לאירועי סייבר. בנוסף, נושא קיום המשכיות עסקית מטופל באמצעות מיקור חוץ.
8.	לפעול לאישורם הסופי של הוראות העבודה החדשות על-ידי מנכ"לית העירייה, ולהכלילם בפורטל העירוני, ככל שתוכנם אינו חסוי. במקביל, יש להטמיען בקרב העובדים הרלוונטיים.	**בוצע באופן חלקי.** הוראות העבודה יועברו לאישור המנכ"לית. לדברי מנהל מערכות המידע, אין מנהל לפורטל ואין מחיצה של הוראות עבודה לחטיבת השירות. בוצעה הטמעה חלקית באמצעות הדרכות למנהלי המאגרים ולעובדים.
9.	לעדכן את מסמך הגדרות המאגר בהתאם לזהות המנהלים בפועל.	**טרם בוצע.** יבוצע לאחר השלמת תהליך רישום ועדכון רישום המאגרים הנובעים משינויים פרסונליים בעירייה.
10.	לוודא, כי כלל התוכנות (כולל "ספרת") ינוהלו מול אגף מערכות מידע ומיחשוב.	**בוצע.** ככל הידוע לאגף המחשוב רוב ההתקשרויות מובאות לידיעתם. ככל שיש כאלו שלא, צריך להדק תהליכי אישור על ידי כל המעורבים באישורן.
11.	להמשיך וליישם את המלצות סקר הסיכונים, מוקדם ככל האפשר.	**מתבצע.** באופן שוטף.
12.	לבחון את הצורך בהצפנת תיק האתר, וככל שקיים הצורך, להצפינו.	**לא בוצע.** מדובר בדרישה חריגה. ייבחן בשנית.
13.	לתעד בכתב כניסה ופעילות בחדרי השרתים על-ידי בעלי התפקידים, על מנת לוודא, כי יהיו אלו מורשים בלבד.	**מבוצע.** הכניסה לחדר השרתים מבוקרת.
14.	לוודא העברת דוחות אוטומטיים חודשיים מאגף משאבי אנוש לממונת אבטחת מידע לצורך בחינת עדכון חשבונות המשתמשים במקרים של גיוס עובדים, סיום העסקתם, ושינויי תפקיד.	**מתבצע באופן חלקי.** אין דוחות אוטומטיים, אולם מתקבל מידע שוטף לגבי קליטת עובדים וסיומי עבודה.
15.	לדרוש מהמנהלים לעדכן את אגף מחשוב ומערכות מידע בכל המקרים בהם משתמש שאינו עובד עירייה (כגון: ספקים ונותני	**מתבצע באופן חלקי.** הדבר מעוגן בהנחיות העבודה והתדרוכים, אולם אין ודאות שמיושם.

	המלצה מדוח הביקורת בשנת 2021	עדכון המצב
	שירות) אשר סיימו עבודתם בעירייה, על מנת שיוסרו חשבונות המשתמשים.	המידע מגיע מגורמים שונים בעירייה או בדרך מקרה.
16.	לעדכן בהתאם להוראת מנכ"לית העירייה את הנוהל העוסק בגיוס עובדים וסיום העסקתם, כך שחשבונותיהם יסגרו והמידע המקצועי והרלוונטי ישאר לשימושם של בעלי התפקידים הרלוונטיים.	**בוצע.** בהתאם להנחיית המנכ"לית.
17.	לשלוח הודעות בנושא אבטחת מידע למשתמשים מתיבת דואר ייעודית ("סייבר"). המלצה זו יושמה בעת תהליך הביקורת.	**בוצע.**
18.	לוודא ככל האפשר באמצעות המנהלים, כי העובדים נחשפו לתכנים אלו, וזאת על-מנת להעלות את מודעות העובדים לנושא.	**מתבצע.** באופן שוטף.
19.	לנהל באמצעות המנהלים, רשימת הרשאות תקפות בכל המערכות הממוחשבות בעירייה על-מנת לעמוד בדרישות התקנות. בנוסף, לדרוש באמצעות ממונת אבטחת מידע אחת לשנה ממנהלי המאגרים רשימת הרשאות תקפות, ולבחון אותה אל מול רשימת המורשים במערכות הממוחשבות השונות.	**בוצע באופן חלקי**. קיים קושי טכני בביצוע בשל אופן תיעוד פעילות המשתמשים ביישומים השונים. נעשה נסיון לממש את הדרישה באמצעות רשימת משתמשים ממערכת ניהול המשתמשים של מערכות מידע ומיחשוב.
20.	לערוך בקרה אחת לתקופה, אחר הגישה למאגרי המידע על מנת לוודא, כי כל מי שנכנס הוא מורשה. יש לתעד בקרה.	**מתבצע.** באופן שוטף.
21.	לעדכן בהוראת העבודה את ההנחייה, כי ככל שמתקיים "אירוע אבטחה חמור", יש לדווח לרשם, לציין את מועד הדיווח ומי אחראי לדווח.	**בוצע.** ההנחייה מעוגנת בנוהל. נפתחה ספרייה ייעודית לתיעוד האירועים.
22.	לערוך בקרה שנתית אחר מדיניות ה-FW, על-מנת לוודא גישה לרשת העירייה על-ידי מורשים בלבד.	**מתבצע.**
23.	להשתמש באימות דו-שלבי בהתחברות מרחוק למערכות העירייה. שיטת זיהוי זו משתמשת באמצעים הנמצאים בידי העובד (כגון הודעת SMS עם סיסמה) לטלפון הנייד של העובד לצורך אימות רצונו להתחבר	**בוצע.**

המלצה מדוח הביקורת בשנת 2021		עדכון המצב
	למערכת מרחוק. המלצה זו יושמה כבר בתהליך הביקורת. עם זאת, יש לציין כי עדיין חסרים פרטים של טלפונים סלולריים פרטיים של בעלי תפקידים אשר יש להשלימם.	
.24	לבצע תרגיל שחזור יזום.	**בוצע.** בוצע תרגיל ברבעון הראשון של שנת 2023, ומתוכנן תרגיל רחב יותר ברבעון האחרון של שנת 2023.