דוח ביקורת בנושא:

סייבר, אבטחת מידע והגנת הפרטיות

מבוא

עיריית כפר סבא, כמו כל ארגון גדול, מתנהלת בעזרת מערכות ממוחשבות ומאגרי מידע לצורך אספקת שירותים דיגיטליים לתושבים והתייעלות תהליכי ביצוע העבודה. שימוש במערכות ממוחשבות ומאגרי מידע מגבירים את סיכוני חשיפת המידע הרגיש (בזדון או בתום לב) שעלולים להוביל לפגיעה בפרטיות של התושבים ועובדי הרשות.

סיכון נוסף הינו אבטחת מידע והגנת הסייבר, אשר נובע מחולשות הרשת וגורם אנושי, ובכך, הפעילות השוטפת של העירייה עלולה להשתבש. הדבר עלול להוביל למניעת אספקת השירותים לתושבים ולחשוף את הרשות לתביעות משפטיות ועיצומים רגולטוריים.

יצוין כי, ישנה עלייה משמעותית בהיקף ובעוצמת האיומים בשנים האחרונות (בעולם כולו ובישראל בפרט). איומים אלה נובעים מכך שמרחב הסייבר התרחב כתוצאה מהתקדמות בהיבט הטכנולוגי וחשיפת המחשבים מפני האינטרנט - רשת נטולת גבולות, המאפשרת אנונימיות גבוהה לגורמים זדוניים שעברו מפשע פיזי לפשע דיגיטלי, כנ"ל גורמי טרור שבחלק מהמקרים נתמכים על ידי מדינות.

בשנים האחרונות גדל היקף התקיפות באמצעות תוכנות נוזקות (Malware), תוכנות כופרות (Ransomware) ו/או הפרות חוק ו"פשיעת מידע". תוכנות נוזקות וכופרה מתפשטות הן דרך רשת האינטרנט בעת גלישה באתרים או דואר אלקטרוני, והן באמצעות חיבור פיזי של התקני זיכרון שונים למחשבים ברשת הארגון. התקיפות הופכות למתוחכמות יותר ויותר תוך אוטומציה שלהן, הפצה המונית ושימוש בטכניקות הנדסה חברתית כדי לפתות משתמשים להפעיל אותן.

הזכות לפרטיות וחובת השמירה על צנעת הפרט עוגנו בחקיקה - הזכות לפרטיות היא זכות חוקתית מוגנת על פי סעיף 7 לחוק-יסוד: כבוד האדם וחירותו, הקובע כי "כל אדם זכאי לפרטיות ולצנעת חייו"; חוק הגנת הפרטיות, התשמ"א-1981, קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". החוק מגדיר, בין היתר, "מידע" כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו", ו"מאגר מידע" כ"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב". עוד קובע החוק כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

כמו כן, בחודש מאי 2017 פורסמו תקנות הגנת הפרטיות ואבטחת מידע, תשע"ז-2017 (להלן - "התקנות"). התקנות, אשר נכנסו לתוקף ב-08.05.18, מגדירות את החובות המפורטות לבעל מאגר מידע, ליישום בקרות תהליכיות וטכנולוגיות לצורך אבטחת מאגרי מידע.

ראוי לציין כי לנוכח משבר הקורונה, נדרשנו גם להתבודד ולעבוד מרחוק. עלה הצורך בהגברת אבטחת מאגרי מידע. בהתאם לכך, שני גורמים מקצועיים בתחום פרסמו הנחיות בנושא אבטחת מידע והגנת הפרטיות, כדלקמן:

1. בתאריך 11.03.2020 מערך הסייבר הלאומי פרסם את "המלצות הגנה לארגונים ועסקים לעבודה מהבית בעקבות התפשטות הקורונה" (להלן – "המלצת המערך לעבודה מהבית").

   ראו נספח א'.

2. בתאריך 24.03.2020 רשות הגנת הפרטיות פרסמה מסמך בנושא "הגנת הפרטיות בעקבות התפשטות נגיף הקורונה: שאלות ותשובות להתנהלות הציבור, גופים ציבוריים והשוק הפרטי". המסמך כולל התייחסות גם לנקיטת אמצעי אבטחה סבירים לעבודה מרחוקת של עובדים.

   ראו נספח ב'.

במסגרת דוח ביקורת אבטחת מידע והגנת הפרטיות בוצעה בחינת החוסן הטכנולוגי של מערכות התשתית והמחשוב של הרשת הפנימית של הארגון ושל אתר העירייה.

בחינת חוסן אפליקטיבי באתר השיווקי וחוסן תשתיתי בכתובות חיצוניות

תרחישי הבדיקה שבוצעו כללו סריקה באמצעות כלים אוטומטיים ובדיקות ידניות לאיתור חולשות בכתובות החיצוניות ואתר האינטרנט השיווקי של הארגון.

בחינת חוסן תשתיתי פנימית

- בדיקות שבוצעו במסגרת הביקורת כללו סריקה אוטומטית (באמצעות כלי ייעודי - NESSUS) של תחנות ושרתים ברשת הפנימית של העירייה, תוך איתור חולשות מובנות בארכיטקטורת הרשת, סוג האפליקציות/ מערכות ההפעלה והרכיבים עליהם הינה מושתתת.
- בהתאם לכך, בוצע תרחיש שמדמה ניסיונות תקיפה של גורם בעל גישה פיזית לרשת הארגון, אך ללא חשבון בדומיין (שם מתחם ייחודי המזהה אתר אינטרנט או כתובות דוא"ל ספציפיים).
- כמו כן, בוצע תרחיש בחינת הקשחות והגדרות אבטחה בתחנת עבודה לדוגמה.

יצוין כי, הביקורת נערכה בין חודשים ינואר - מאי 2020 ומורכבת משני חלקים:

1. חלק ראשון – דוח ביקורת;
2. חלק שני – מבדק טכנולוגי.

ביקורת התבססה על בדיקות מדגמיות ואין הכרח שתחשוף כל ליקוי אם קיים.

מטרת הביקורת ומתודולוגיה

מטרת הביקורת היא לבחון את נאותות התנהלות העירייה היבטי אבטחת מידע, בהתייחס לדרישות תקנות הגנת הפרטיות, הנחיות רשות הגנת הפרטיות ומערך הסייבר ואת אפקטיביות מנגנוני האבטחה להתמודדות עם מתקפות סייבר, תוך זיהוי חולשות, פגיעות ופערים. כמו כן, נבחן נושא עבודה מהבית בעת שגרת קורונה.

מטרת הביקורת לבדוק את הנושאים, כלהלן:

1. הערכת הסיכונים הפוטנציאליים, חשיפת כשלים וליקויים באופן יישום מערך האבטחה, חשיפת ליקויים באופן היישום של אמצעי טכנולוגיה ותהליכים תפעוליים שחושפים את מערכות המידע לפגיעה או לזליגת מידע.
2. קבלת תמונת מצב עדכנית ואמיתית, המשקפת את נושא אבטחת המידע בארגון באופן שיאפשר לו לבצע הפעילויות הבאות:

- לזהות כשלים עבור נושאים, כגון: מדיניות, ארגון, ניהול, תפעול וטכנולוגיה במערך המחשוב;
- לבצע הערכת הסיכונים ולהגדיר את רמת חומרתם;
- ליישם המלצות לשיפור המצב הקיים;
- לבצע הערכת הדרישות ליישום ההמלצות.

3. מתן פתרונות לצמצום או ביטול האפשרות למימוש החשיפה לפגיעה במערך הטכנולוגי.

במסגרת הביקורת גובשה מתודולוגיה, כדלקמן:

- נערכו פגישות עם מנהל אגף מחשוב ומערכות מידע, ממונה אבטחת מידע ומנהלת אגף משאבי אנוש.
- הביקורת עינה בחומרים רלוונטיים, כגון: נהלים, סקרים, מבדקים, תיעוד לפעילות מחלקת מערכות מידע, הסכמים עם ספקים, ועוד.
- בוצע סקר אבטחה (תוך לימוד מערך המחשוב הקיים ואופן תפעולו) שהתבסס על תשאול ובדיקת גורמים ותהליכים תפעוליים הרלוונטיים לביקורת. כמו כן, נבדקו רכיבים ואמצעים טכנולוגיים הקשורים למערכות המידע של הארגון.

- לצורך בחינת איכות יישום הפרמטרים ואמצעי האבטחה הלוגית של הרכיבים הטכנולוגיים, בוצעו בדיקות חוסן המדמות פורץ פוטנציאלי למערכות המידע של הרשות.
- בוצעו בדיקות טכנולוגיות מדגמיות, כגון:

  - שילוב של כלי תוכנה לסריקה מקצועית ובדיקות ידניות שונות;
  - מבדקי חדירה דרך האינטרנט בהתאם לכתובות IP חיצוניות שסופקו לביקורת, ומזוהות עם העירייה ואתר העירוני;
  - ביצוע סריקות לאיתור חשיפות אבטחה בשרתים, בסיסי נתונים, ציוד תקשורת ותחנות קצה באמצעות כלי סריקה מקצועי - NESSUS;
  - ביצוע בדיקות לנאותות הגדרות אבטחה בתחנת קצה מדגמית;
  - בדיקת מחשב נייד (של מבקר העיריה) ממנו מבוצעת גישה מרחוק;
  - בדיקת הגדרות מדגמית במוצרי אבטחה והגדרות גישה מרחוק;
  - בדיקת הרשאות גישה רגישות, הרשאות חיבור מדיה נתיקה וגלישה באינטרנט;
  - ניסיון גישה לישיבת ZOOM של הנהלה לבדיקת ערנות לכניסה לזרים.

במסגרת הביקורת נבדקו ,בין השאר, הנושאים הבאים:

- פעילות מחלקת מערכות מידע ואחריותו של ממונה אבטחת מידע;
- פעילות ומעורבות הנהלת העירייה ואגף משאבי אנוש והדרכה;
- הדרכה והגברת מודעות עובדים;
- ביצוע סקרי אבטחה ומבדקי חדירה;
- פעילות ועדת היגוי בהיבטי אבטחת מידע;
- גיבוש וביצוע תכנית עבודה בהיבטי אבטחת מידע;
- קיום תקציבים נאותים;
- מדיניות ונהלים בהיבטי הגנת הפרטיות ואבטחת מידע;
- קיום אמצעי אבטחה טכנולוגיים נאותים בפרט בנושא אבטחת גישה מרחוק;
- פיקוח ובקרה על ספקי מיקור חוץ.

להלן פירוט הקריטריונים על פיהם נבחן מערך המתודולוגי של הביקורת:

עיקרי ממצאים

דוח ביקורת זה מכיל מידע רגיש, לכן אינו מפורסם באופן מלא באתר.

ניתן לקבל הסבר טלפוני נגיש לגבי הדוח במספר הטלפון 09-7649121 – לשכת מבקר העירייה.