המועצה האזורית תמר
ים המלח

תקנות הגנת הפרטיות, אבטחת מידע ותפעול אתר האינטרנט של המועצה

אפריל 2021

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

מבקר המועצה דוח ביקורת

יום רביעי ט״ז אייר תשפ״א
28 אפריל 2021

לכבוד
מר ניר ונגר
ראש המועצה

נכבדי,

הנדון: **דוח מבקר המועצה בנושא – אבטחת מידע, הגנת הפרטיות ותפעול אתר האינטרנט של המועצה**

הנני מתכבד להגיש לך את דוח הביקורת בנושא ״אבטחת מידע, הגנת הפרטיות ותפעול אתר האינטרנט של המועצה״, בהתאם לסעיף 145)ו(לצו המועצות המקומיות.

להיקף השירותים שהמועצה מעניקה ולאיכותם, יש השפעה על איכות החיים של תושבי המועצה והבאים בשעריה. המועצה מגדילה בעקביות את מרחב פעולותיה בסביבה משתנה וחדשנית, רוויית הזדמנויות וסיכונים. הביקורת סבורה כי לצורך קבלת החלטות מושכלת, נדרשות למועצה מערכות מידע וניהול מתקדמות ובסיסי נתונים תומכי החלטה.

במועצה קיימים מאגרי מידע רבים בתחומים שונים, חלקם כוללים גם מידע רגיש כהגדרתו בחוק הגנת הפרטיות, התשמ״א-1981, שחשיפתם עלולה לפגוע, בין היתר, בפרטיותם של תושבי המועצה ועובדיה, ולכן מוטלת על בעלי המאגרים החובה להגן על המידע.

אבטחת מידע וסיכוני סייבר הם נושאים שבסדר היום העולמי, הארצי והעירוני. בסקרי סיכונים שנערכו בשנים 2020-2021 ע״י ה – ECIIA)הקונפדרציה האירופית למבקרים פנימיים(ב 11 מדינות ברחבי אירופה ובישראל בקרב מבקרים פנימיים ראשיים, עולה כי הסיכון העיקרי של הארגונים, שכ

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

המועצה האזורית תמר
ים המלח

– TOP 5, הוא סיכון הסייבר

ומעלה מהמשיבים סימנו לאורך השנים כחלק מרשימת ה
ואבטחת מידע.

במסגרת הדוח נבדקה נאותות ניהול אבטחת המידע במועצה ואפקטיביות מנגנוני המידע הקיימים להתמודדות עם מתקפות סייבר מתקדמות.

ראוי לציון פעילות הצוות לתיקון ליקויים בראשות מנכ"לית המועצה עוה"ד מורן יצחקי, הדן בדרכים ובמועדים לתיקון הליקויים ובדרכים למניעת הישנותם.

בהתאם לסעיף 145ו)א(עותק של הדוח נמסר לחברי הוועדה לענייני ביקורת.

בכבוד רב,

רן שלום אורפני, רו"ח
מבקר המועצה וממונה על תלונות
ציבור

העתקים: חברי הוועדה לענייני ביקורת

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

המועצה האזורית תמר
ים המלח

תוכן עניינים

1.	**מבוא**	**4**
2.	**מטרת הביקורת**	**6**
3.	**מתודולוגיה**	**7**
4.	**פירוט הממצאים**	**8**
4.1	מדיניות אבטחת מידע ונהלי אבטחת מידע	8
4.2	ממשל תאגידי בהיבטי אבטחת מידע	10
4.3	ועדת היגוי להיבטי אבטחת מידע, תכנית עבודה ופיקוח	12
4.4	סקרי אבטחת מידע ומבדקי חדירה	13
4.5	בחינת מהימנות עובדים ויועצים לפני מתן גישה למאגרים	15
4.6	הדרכות עובדים	16
4.7	בקרת הרשאות גישה	17
4.8	בקרה ותיעוד גישה	18
4.9	קיום הגנה אפקטיבית כנגד מתקפות מתוחכמות	19
4.10	אבטחת טלפונים ניידים וטאבלטים	21
4.11	אבטחת התקנים ניידים	21
4.12	מדיניות בקרת גלישה באינטרנט	22
4.13	הרשאות אדמיניסטרטור	23
4.14	אבטחת גישה מרחוק למשאבי המועצה	24
4.15	סגמנטציה של הרשת הפנימית	25
4.16	מערכת מניעת חיבור התקנים זרים לרשת הפנימית	26
4.17	שימוש במערכות הפעלה לא מעודכנות	27
4.18	ניטור, דיווח ותגובה לאירועי אבטחת מידע	30
4.19	מיקור חוץ	31
4.20	מסמכי הגדרות מאגר ובדיקת מידע רב מן הנדרש	33
4.21	מיפוי מערכות המאגר	34
4.22	מבדקים לבדיקת מודעות עובדים	34
4.23	מבדקים לבדיקת אפקטיביות מערך האבטחה	35
4.24	בדיקת אתרי האינטרנט של המועצה.....	37
5.	**תגובת המועצה**	**40**

נספח א' – פירוט מאגרים המנוהלים במועצה

נספח ב' – סיכום מבדקים טכנולוגיים

נספח ג' – הנחיות מערך הסייבר הלאומי ורשות הגנת הפרטיות בנושאי סיכוני סייבר במשבר קורונה

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

1. מבוא

1.1. במועצה האזורית תמר פועלות מערכות מידע ממוחשבות ומנוהלים מאגרי מידע לצורך אספקת שירותים מגוונים לתושבים, מפעלים ועסקים.)ראה נספח א' – לפירוט מאגרים מנוהלים במועצה(

1.2. הגברת שימוש במערכות מידע והגברת השימוש במאגרי מידע תוך הרחבת אספקת שירותים דיגיטליים לתושבים בשנים אחרונות, מגביר את הסיכון כי מידע אישי ייחשף ברבים בזדון או בתום לב ויפגע בפרטיות התושבים והעובדים של המועצה.

1.3. כמו כן, שימוש זה חושף את המועצה לסיכונים במרחב הסייבר העלולים לפגוע בפעילותה.

1.4. סיכוני סייבר עלולים להתממש כתוצאה מניצול של חולשות במערכות, תהליכים וגורם אנושי עד כדי לשבש את הפעילות השוטפת, למנוע מהמועצה אספקת שירותים לתושבים, לחשוף את המועצה לתביעות משפטיות ועיצומים רגולטוריים וכד'.

1.5. בשנים האחרונות ישנה עלייה משמעותית בהיקף ובעוצמת האיומים בעולם כולו ובישראל בפרט. איומים אלה נובעים מכך שמרחב הסייבר התרחב ממחשב הקלאסי וחושף כל התקן חכם המשתמש ברשת האינטרנט - ובכך מאפשר תקיפה נרחבת, זאת לצד היותו של האינטרנט רשת נטולת גבולות המאפשרת אנונימיות גבוהה לגורמים זדוניים שעברו מפשע פיזי לפשע דיגיטלי, כנ"ל גורמי טרור שבחלק מהמקרים נתמכים על ידי מדינות.

1.6. בשנים האחרונות גדל היקף התקיפות באמצעות תוכנות נוזקות [1])Malware(, תוכנות כופרות [2])Ransomware(שונות ו/או הפרות חוק ו"פשיעת מידע". תוכנות אלה מתפשטות הן דרך רשת אינטרנט בגלישה או דרך דוא"ל והן באמצעות חיבור פיזי של התקני זיכרון שונים למחשבים ברשת הארגון. התקיפות הופכות למתוחכמות יותר ויותר תוך אוטומציה שלהן והפצה המונית ושימוש בטכניקות הנדסה חברתית כדי לפתות משתמשים להפעיל אותן. בשנים אחרונות התרחשו מספר אירועי מתקפות בערים בישראל כמו מועצת חוף אשקלון, עיריית נוף הגליל, עיריית הוד השרון, עיריית הרצליה ועוד.

1.7. לשם שמירה על צנעת הפרט ועל הוראות החוק, יש לנקוט אמצעים לאבטחת המידע ומערכי המידע, ולהגן עליהם מפני פגיעה, חשיפה ושינוי במזיד או בשוגג. זאת, באופן שישמרו הזמינות, השלמות, המהימנות, הסודיות והשרידות של המידע ומערכות המידע.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

[1] תוכנה זדונית המותקנת במחשב ללא ידיעתו של המשתמש ופוגעת בפעולתו התקינה.

[2] תוכנה זדונית המופעלת על מחשב במטרה להצפין את תכולת הדיסק ותוכן המחשב. לאחר מכן מקבל המשתמש דרישה לתשלום כופר על מנת לקבל גישה לקבצים.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

1.8. <u>חוקים, תקנות והנחיות רלוונטיים בהיבטי הגנת הפרטיות ואבטחת מידע</u>

- חוק הגנת הפרטיות, התשמ"א-1981)להלן - חוק(להלן הגדרות לפי סעיף 7 לחוק:

אבטחת מידע - **"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין."**

מאגר מידע - **"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב..."**

- בחודש מאי 2017 פורסמו תקנות הגנת הפרטיות)אבטחת מידע(, תשע"ז-2017)להלן - תקנות(מכוח החוק. התקנות אשר נכנסו לתוקף ב-8.5.18, מגדירות חובות מפורטות לבעל מאגר מידע, ליישום בקרות תהליכיות וטכנולוגיות לצורך אבטחת מאגרי מידע בהם מנוהל מידע אישי.
- תורת הגנת הסייבר של מערך הסייבר הלאומי. כוללת בקרות מומלצות.
- ב-11 במרץ 2020 פרסם מערך הסייבר הלאומי "המלצות הגנה לארגונים ועסקים לעבודה מהבית בעקבות התפשטות הקורונה")להלן - המלצות המערך לעבודה מהבית(. ראה נספח ב.
- 24ב - במרץ פרסמה רשות הגנת הפרטיות: 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. ראה נספח ב.

1.9. <u>המשימות העיקריות בהיבטי הגנת הפרטיות ואבטחת מידע של מועצה כבעלת המאגר</u>

- לקבוע מדיניות ונהלים
- להעריך ולנהל סיכוני סייבר
- להדריך עובדים ולהגביר מודעות שלהם
- להקצות משאבים מתאימים
- לאתר, להגיב ולטפל באירועי אבטחה חריגים
- לפקח ולבקר באמצעות תפקיד של ממונה אבטחת מידע לגבי יישום דרישות תקנות
- להטמיע כלים טכנולוגיים נאותים להגנה על מערכות, תשתיות ומאגרים
- לפקח ולבקר על פעילות מיקור חוץ

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

2. מטרת הביקורת

מטרת הביקורת הינה לבחון את נאותות ניהול היבטי אבטחת מידע במועצה, בהתייחס לדרישות תקנות הגנת הפרטיות, הנחיות רשות הגנת הפרטיות ומערך הסייבר תוך בחינת תהליך יישום תקנות חדשות במועצה ואת אפקטיביות מנגנוני אבטחת מידע הקיימים במועצה להתמודדות עם מתקפות סייבר, תוך זיהוי חולשות אבטחה, פגיעות ופערים. במסגרת הביקורת גם נבחנו היבטי אבטחת מידע בנושא עבודה מהבית במהלך משבר קורונה.
בנוסף נבחנו היבטי ניהול ותפעול של אתר האינטרנט בעירייה בהתייחס להמלצות של דוח מבקר המדינה משנת 2015 " ניהול ותפעול של אתרי אינטרנט בשלטון המקומי".

התחומים העיקריים שנבדקו:

- פעילות מחלקת מערכות מידע
- פעילות ממונה אבטחת מידע
- פעילות ומעורבות הנהלת המועצה
- פעילות בהיבטי משאבי אנוש
- אבטחת מידע ניהול ותפעול של אתר האינטרנט.

במסגרת זו נבדקו, בין השאר, הנושאים הבאים:

- הדרכה והגברת מודעות עובדים
- ביצוע סקרי אבטחה ומבדקי חדירה
- פעילות ועדת היגוי בהיבטי אבטחת מידע
- פעילות ממונה 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
- תהליכי ניהול ותפעול של אתר אינטרנט
- אבטחת מידע של אתר אינטרנט

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

המועצה האזורית תמר
ים המלח

3. מתודולוגיה

לצורך הביקורת נערכו הפעולות הבאות:

- פגישות ושיחות עם: מנהל מערכות מידע, נציגי חברת תשתיות חיצונית.
- העברת שאלון ביקורת בנושא תפעול ותחזוקה של אתר האינטרנט.
- עיון בחומרים: נהלים, סקרים, מבדקים, תיעוד לפעילות מחלקת מערכות מידע, הסכמים עם ספקים, ועוד.
- ביצוע בדיקות טכנולוגיות מדגמיות:
  - שילוב של כלי תוכנה לסריקה מקצועית ובדיקות ידניות שונות.
  - מבדקי חדירה דרך האינטרנט בהתאם לכתובות IP חיצוניות שסופקו לביקורת, ומזוהות עם המועצה ואתר המועצה.
  - ביצוע סריקות לאיתור חשיפות אבטחה בשרתים, בסיסי נתונים, ציוד תקשורת ותחנות קצה באמצעות כלי סריקה מקצועי NESSUS.
  - ביצוע סריקות לאיתור חולשות אבטחה באתר האינטרנט.
  - ביצוע בדיקות לנאותות הגדרות אבטחה בתחנת קצה מדגמית.
  - בדיקת מחשב נייד של מבקר הפנימי ממנו מבוצעת גישה מרחוק.
  - בדיקת הגדרות מדגמית במוצרי אבטחה והגדרות גישה מרחוק.
  - בדיקת הרשאות גישה רגישות, הרשאות חיבור מדיה נתיקה וגלישה באינטרנט.
  - סימולציה של ניסיון גישה לישיבת ZOOM של הנהלה לבדיקת ערנות לכניסה לזרים.
  - סימולציה של קמפיין פישינג לתרגול מודעות עובדים.
  - סימולציה של פנייה טלפונית לעובדים במטרה להשיג גישה למחשב וסיסמאות.
  - סימולציה של החדרת נוזקות מדומות דרך דואל ואינטרנט.

הביקורת נערכה בין חודשים מאי עד ספטמבר 2020 .

הביקורת בוצעה בידי יועצים חיצוניים לביקורת, בעלי הסמכות בינלאומיות בתחומי אבטחת מידע וביקורת מערכות מידע)כגון CISSP, CISA, ISO 27001 Lead Auditor(המתמחים בביקורת ויישום רגולציות בתחומי אבטחת מידע והגנת הפרטיות, בניהול סיכוני סייבר ואבטחת מידע ובביצוע מבדקים טכנולוגיים ומבדקי חדירה וסימולציה של תקיפות סייבר.

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

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

4. פירוט הממצאים

4.1. מדיניות אבטחת מידע ונהלי אבטחת מידע

סעיף 3)2(לתקנות קובע כי "הממונה על אבטחה יכין נוהל אבטחת מידע **ויביאו לאישור בעל המאגר;**"

מתוך מדריך ליישום תקנות הגנת הפרטיות של רשות הגנת הפרטיות: "הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו **לאישור ההנהלה הבכירה של הארגון"**

סעיף 4)ג(לתקנות קובע כי "נוהל אבטחת מידע" שייקבע בעל מאגר מידע, יכלול, בין היתר:

)1(הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר...;

)2(הרשאות גישה למאגר המידע ולמערכות המאגר...;

)3(תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך;

)4(הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר;

)5(הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר... אופן קביעת סיכונים אלה, ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר;

)6(אופן התמודדות עם אירועי אבטחת מידע... לפי חומרת האירוע ומידת רגישות המידע;

)7(הוראות לעניין ניהול של התקנים ניידים ושימוש בהם...

סעיף 4)ד(קובע כי במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול "נוהל אבטחת מידע" התייחסות אף לסעיפים הבאים:

האבטחה לפי נוהל האבטחה ולפי תקנות אלה...;

- אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר...;
- אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר...;
- הוראות לעניין עריכת ביקורות תקופתיות לווידוא קיומם ותקינותם של אמצעי

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

המועצה האזורית תמר
ים המלח

)1(הוראות לעניין גיבוי הנתונים... ;
)2(הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר."
)3(

)4(
)5(

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

ממצאים:

לביקורת הוצגו קבצי מסמכים של נהלים הבאים: -

נוהל מדיניות אבטחת מידע – גרסה 1.0 מאוקטובר 2018 והוא כולל התייחסות להיבטי אבטחת מידע שונים וגם נספחים כמו כללי אבטחת מידע לעובדים. **נרשם כי נוהל מאושר על ידי המנכ"ל.**

- נוהל מאגרי מידע – גרסה 1.0 מאוקטובר 2018 והוא כולל התייחסות להיבטי ניהול ואבטחת מאגרי מידע ומידור הרשאות גישה. נרשם כי נוהל מאושר על ידי המנכ"ל.
- נוהל טיפול באירוע אבטחת מידע גרסה 1.0 מאוקטובר 2018.
- נוהל הכלת אירוע אבטחת מידע גרסה 1.0 מאוקטובר 2018.
- נוהל גיבוי ושחזור מגיבוי גרסה 1.0 מאוקטובר 2018.
- נוהל אבטחה פיזית וסביבתית גרסה 1.0 מאוקטובר 2018.
- נוהל אבטחת מידע מול ספקים חיצוניים גרסה 1.0 מאוקטובר 2018.
- נוהל אבטחת מידע לקליטת עובד, שינוי תפקיד לעובד וסיום העסקה גרסה 1.0 מאוקטובר 2018.

הביקורת מצאה כי, חסרה התייחסות כלשהו או התייחסות מפורטת להיבטים הבאים במסמכים:

- נוהל המרכז כלל תפקידיו, אחריותו וכלל פעילות ממונה אבטחת מידע לרבות הכנה, ביצוע ודיווח על תכנית בקרה שוטפת לעמידה בדרישות התקנות להנהלה לרבות ועדת היגוי. יצוין כי, חלק מתפקידיו מפורטים בנוהל מאגרי מידע בהתייחס לניהול הרשאות, אבטחה פיזית ובקרת לוגים.
- נוהל לגבי אופן ביצוע ובקרת פעולות פיתוח, תחזוקה ושינויים במאגרים ותיעודן.
- נוהל הצבה של מצלמות אבטחה, אבטחת מידע של הקלטות ממצלמות אבטחה וניהול הרשאות גישה למערך מצלמות.
- נוהל הקשחה ועדכון מערכות הגנה ואבטחת מידע למעט אנטי וירוס.
- נוהל ביצוע עדכוני אבטחה ושדרוגי גרסאות של ציוד תקשורת, תחנות קצה ושרתים ומערכות המאגרים.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

<u>המלצות הביקורת</u>

1. לעדכן ו/או לאשרר את נהלי אבטחת מידע בתדירות תקופתית ולכל הפחות בתדירות שנתית.
2. להשלים כתיבת נהלים בנושאים שכיום לא נכללים בנהלים הקיימים כפי שמפורט בממצאי הביקורת לעיל .

4.2. ממשל תאגידי בהיבטי אבטחת מידע

סעיף 17ב. לחוק הגנת הפרטיות קובע כי המועצה מחויבת למנות אדם בעל הכשרה מתאימה לתפקיד הממונה על אבטחת מידע.

סעיף 3 לתקנות קובע:

"חלה חובה למנות ממונה על אבטחת מידע, או מונה ממונה על אבטחת מידע במאגר המידע יחולו הוראות אלה:

(1) ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר...

(3) הממונה יכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו;

(4) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה;

(5) הטיל בעל מאגר המידע על ממונה על אבטחה משימות נוספות על החובות המנויות... לשם ביצוע תקנות אלה, יגדירן בצורה ברורה;"

תכנית הבקרה תכלול היבטים רבים לרבות בדיקת סטאטוס עדכוני אבטחה, תקינות מוצרי אבטחה, נאותות הרשאות גישה למאגרים, בקרה על חיבור מדיה נתיקה, הפרדת מאגרים, בקרה על אבטחת גישה פיזית לרבות מורשי גישה, חוזק מנגנונים, בקרה על תקינות לוגים במערכות ועוד.

התייחסות בנוגע לתפקיד של ממונה אבטחת מידע קיימת בשאלות ותשובות שפורסמו באתר רשות הגנת הפרטיות.

https://www.gov.il/he/Departments/Guides/data_security_fqa?chapterIndex=2

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

האם ממונה אבטחת מידע יכול שיהיה כפוף למנמ"ר (מנהל מערכות מידע)?

סעיף 3(4) לתקנות קובע כי הממונה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי התקנות. המטרה של ההוראה היא לשמר את עצמאות שיקול דעתו וחוסר התלות של ממונה האבטחה. עמדת הרשות היא שלא ניתן להשיג מטרה זו אם ממונה האבטחה יכהן בעצמו גם כמנמ"ר של הארגון. חשש לניגוד עניינים קיים גם במקרה בו הממונה יהיה רק כפוף למנמ"ר, אולם ניתן לצמצם את החשש אם חוסר תלותו ועצמאות שיקול דעתו של הממונה תובטח בדרך יעילה אחרת, בשים לב למבנה הארגון ולמאפייניו הספציפיים. לדוגמא, באמצעות אפשרות דיווח ישיר למנכ"ל או לדירקטוריון, ומעורבות שלהם במינוי הממונה ובקביעת תנאי העסקתו.

האם ניתן למנות ממונה אבטחת מידע חיצוני (מיקור חוץ)?

ניתן למנות ממונה אבטחת מידע חיצוני, שאינו עובד הארגון. בעת המינוי יש לוודא כי הממונה מבין כי הינו חב באחריות אישית לאבטחת המידע במאגר כפי שמוגדר בסעיף 17ב(ב) לחוק הגנת הפרטיות.

ממצאים:

לביקורת נמסר כי, מנהל מערכות מידע חיצוני מכהן גם בתפקיד של ממונה אבטחת מידע במועצה אשר אמור לבקר ולפקח על העמידה בדרישות התקנות הגנת הפרטיות. במצב הנוכחי ייתכנו להיווצר ניגודי עניינים בין תפקידו כמנהל מערכות מידע לממונה אבטחת מידע.

בהתאם להבהרת רשות הגנת הפרטיות מצב זה אינו עומד בדרישות תקנות הגנת הפרטיות.

מנהל מערכות מידע אחראי ליישום בפועל של תכנית עבודה שוטפת בהיבטי מערכות מידע ובתפקיד הממונה למעשה מבקר ומפקח על פעולותיו של עצמו ושל עובדים הכפופים לו. יכולים להתרחש מצבים רבים בהם תיווצר התנגשות בין צרכי מערכות מידע וצרכי אבטחת מידע והגנת הפרטיות.

נמסר לביקורת מהממונה כי, הממונה אינו מבצע פעולות ניהול ותחזוקה של מערכות מידע ומערכות אבטחה בפועל, אלא מפקח על ספק חיצוני אחר שאחראי לנושא ולכן ניגודי עניינים שלו פחותים. עדיין המצב הנוכחי עומד בסתירה להנחיה של רשות הגת הפרטיות.

יצוין כי, כלל תפקידי הממונה, סמכויותיו ואחריותו בתחומי אבטחת מידע והגנת הפרטיות לא מוגדרים בכתב המינוי. לביקורת הוצג כתב מינוי במסמך WORD מתאריך 8 במאי 2018 עם חתימה מצולמת של המנכ"ל המועצה. בכתב מינוי רק בכותרת נרשם כי, מדובר בכתב מינוי ממונה אבטחת מידע ותשתיות חיוניות ובגוף המסמך קיימת התייחסות רק לגבי " בהתאם לכך, מוטלת עליך האחריות למערכות המחשוב החיוניות ולדיווח על כל אירוע אבטחת מידע בהתאם לנהלי הארגון."

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

בנוסף הממונה כיום אינו כפוף לגורם ניהולי בכיר אלא לסגן הגזבר דבר שעלול לפגוע ביכולת שלו להעביר הנחיות מחייבות לכלל הגורמים במועצה. במבנה הארגוני של המועצה שהוצג לביקורת לא נכללת כלל פונקציה של ממונה אבטחת מידע.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

הומצא לביקורת תיעוד לכך שהוכנה תכנית עבודה שוטפת בשנים 2018, 2019 צורך עמידה בתקנות הגנת הפרטיות)שנת 2018 בעקבות סקר סיכונים חיצוני(ופעולות אבטחה בתוכנית עבודה של גזברות לשנת 2019. לגבי שנת 2020 הוצג קובץ תכנית עבודה גזברות 2020 **אך הוא לא כולל התייחסות מפורטת להיבטי אבטחת מידע.**

<u>המלצות הביקורת</u>

1. מומלץ כי ימונה ממונה אבטחת מידע במועצה שאינו מכהן בתפקיד מנהל מערכות מידע, הממונה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגודי עניינים.
2. לחלופין מומלץ כי יוגדרו מנגנוני פיקוח כדי לצמצם סיכונים לניגודי עניינים של הממונה הנוכחי כגון : התכנסות ועדת היגוי תקופתית שתפקח על פעילות הממונה, ביצוע סקר בקרה תקופתי על ידי מומחה חיצוני ועוד. 3.
3. לצורך המינוי יוכן כתב מינוי שיכלול תפקידיו, אחריותו וסמכויותיו של ממונה וכפיפותו לגורם ניהולי בכיר.
4. מומלץ כי הממונה יכין תכנית בקרה שוטפת ומפורטת לעמידה בתקנות הגנת הפרטיות בכל שנה, יגיש לאישור ההנהלה וידווח על ביצועה להנהלה ומנהלי מאגרים.
5. על ממונה אבטחת מידע להעביר דיווח תקופתי בכתב במסגרת ועדת היגוי או ישירות להנהלה בכירה ולמנהלי מאגרים בו יוצגו תוצאות פעולות הבקרה שלו ואיזה פערים עדיין קיימים לעמידה בדרישות התקנות. במסגרת זו על ממונה אבטחת מידע <u>לתעד</u> באופן מפורט כל הפעילות הבקרה המבוצעת על ידו.

4.3. ועדת היגוי להיבטי אבטחת מידע, תכנית עבודה ופיקוח

כיום בארגונים רבים הוקמו ועדות היגוי לנושא אבטחת מידע והגנת הפרטיות לצורך קידום נושאי אבטחת מידע. תפקידי ועדת היגוי מקובלים:

- אישור ועדכון בכל הנוגע למדיניות אבטחת המידע ונהלים ;
- אישור תכנית העבודה בתחום אבטחת מידע, הקצאת תקציבים ומעקב אחר יישום תכנית העבודה בתחום ;
- לקבל דיווח תקופתי על אירועי אבטחת מידע ולדון באירועי אבטחת מידע חריגים ;

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

- להבטיח קיומם של מנגנוני פיקוח ובקרה נאותים על נושאי אבטחת מידע;
- לסייע להנהלת המועצה בקבלת החלטות בכל הקשור לתחום אבטחת המידע מתוך ראיה אינטגרטיבית של התחום במועצה.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

- קבלת דיווחים תקופתיים מממונה אבטחת מידע והנחיית ממונה אבטחת המידע לכל הפחות בתדירות רבעונית.

הוועדה תתכנס בתדירות קבועה ומספקת שתקבע ותדווח לראש המועצה ולמנכ"ל המועצה, אחת לשנה לכל הפחות, על פעילותה ועל מסקנותיה והמלצותיה בנושאים בהם הוסמכה לעסוק ותערוך פרוטוקולים של ישיבותיה. רצוי כי לפחות בדיון השנתי בו תאושר תכנית העבודה ותקציבים בתחומי אבטחת מידע יהיה נוכח מנכ"ל המועצה. כמו כן, חברי הועדה צריכים להיות מתחומים מנהליים ולא רק מערכות מידע לרבות יועץ משפטי, קצין הביטחון, מנהל משאבי אנוש, אחראי על תאגידים עירוניים, מנהלי מאגרים ועוד.

ממצאים:

הביקורת מצאה כי, לא הוגדרה באופן פורמאלי ועדת היגוי לנושאי אבטחת מידע באמצעות כתב מינוי או במסגרת נוהל ארגוני לרבות תפקידיה, סמכויותיה וחבריה. הוצג כי מתקיימות ישיבות עבודה בין סגן הגזבר למנהל מערכות מידע בתדירות לא קבועה ובין היתר עולים היבטי אבטחת מידע שונים אך לא מועלים בישיבות אלה כל הנושאים הנדרשים לפי תקנות הגנת הפרטיות.

<u>המלצות הביקורת</u>

1. להגדיר באופן פורמאלי ועדת היגוי לנושאי אבטחת מידע והגנת הפרטיות לרבות משתתפיה, תפקידיה וסמכויותיה.
2. לכנס ועדת היגוי בתדירות תקופתית כולל ולפחות דיון שנתי ביחד עם מנכ"ל המועצה תוך תיעוד מסודר בפרוטוקולים של נושאים שנדונו, החלטות ומעקב ביצוע.

4.4. סקרי אבטחת מידע ומבדקי חדירה

בסעיף 5 בתקנות הגנת הפרטיות נקבע כדלקמן:

"(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

בעקבותיהן ,ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר ,ככל שהתגלו ;סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות.

(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה ,בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים ,אחת

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

לשמונה עשר חודשים לפחות ;בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שהתגלו ,ככל שהתגלו.״.

מבדיקת הביקורת נמצא כי, סקר סיכונים להערכת סיכוני אבטחת מידע, בוצע בשנת 2018 על ידי חברה חיצונית לשירותי ייעוץ באבטחת מידע. הוכנה תכנית עבודה לטיפול בממצאים והמלצות והוצג סטטוס טיפול לביקורת.

ממצאים:

א. מבדיקה חוזרת שבצעה הביקורת חלק מהמלצות הסקר משנת 2018 טרם בוצעו למשל רכש מערכות אבטחה נוספות כמו SOC ,SIEM ,DLP, תרגול מודעות עובדים באמצעות ״תקיפות דמה״, הקשחת מדיניות סיסמאות גישה, הפרדת רשתות פנימית ועוד .

ב. טרם בוצעו מבדקי חדירה תשתיתיים ואפליקטיביים פנימיים בכל מערכות ותשתיות המאגרים המנוהלים במועצה עצמה. יצוין כי, קיימת חובה לביצוע בנוגע למערכת ברמת אבטחה גבוהה בלבד)מידע על מעל 100,000 בני אדם(אך מומלץ לבצע גם במאגרים אחרים בהתאם להנחיות מערך הסייבר הלאומי. במועד הביקורת לא בוצע תהליך מעמיק לקביעת רמת אבטחה של מאגר. לכן לא ברור אם נדרש או לא מחויב לביצוע.

ג. בנוסף המועצה לא קבלה תוצאות סקרי אבטחה ומבדקי חדירה מצד ספקי מקור חוץ מהותיים שמחזיקים במאגרי מועצה הכוללים מידע אישי רגיש רב כגון חברת מטרופולינט.

<u>המלצות הביקורת</u>

1. לבצע בדיקה מעמיקה לגבי כמות מספרי ת.ז שונים המנוהלים)כולל היסטוריה(במאגרי המועצה ולקבוע לכל מאגר אם מדובר במאגר ברמת אבטחה גבוהה המחויב במבדק חדירה בתקנות.
2. ליזום ביצוע סקרי אבטחת מידע ומבדקי חדירה כנדרש בתקנות והמלצות מערך הסייבר הלאומי במערכות ותשתיות המועצה.
3. לכל הפחות לדרוש לקבל מספקי מיקור חוץ של מערכות המשמשות את המועצה להציג בתדירות שתקבע תוצאות סקרי אבטחה ומבדקי חדירה.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

4 לקיים דיון בוועדת היגוי בתוצאות סקרים ומבדקי חדירה.

5. לקבוע תכנית עבודה, לו"ז ותיעדוף לתיקון הליקויים שמתגלים ולדווח תקופתית לוועדת היגוי.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

6. לקבוע תכנית מפורטת פר מערכת ומאגר לביצוע סקרים ומבדקי חדירה במערכות המאגר כנדרש בתקנות. במסגרת זו יש לקבוע לכל מאגר את רמת האבטחה המתאימה.

4.5. בחינת מהימנות עובדים ויועצים לפני מתן גישה למאגרים

סעיף 7)א(לתקנות קובע:

"לא ייתן בעל מאגר מידע גישה למידע המצוי במאגר ולא ישנה היקף הרשאה שניתנה, אלא אם כן נקט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר;"

ממצאים:

אגף משאבי אנוש אמון על גיוס עובדים למועצה בהתאם לצו המועצות ונוהל גיוס. המועמד נדרש לספק מסמכים שונים לרבות תעודות השכלה ורישיונות, קורות חיים ועוד. בהתאם לסוג תפקיד מבוצעים ראיונות מקצועיים ומשאבי אנוש, ובמכרזים קיימת ועדת בקבלה.

כיום, קיים הליך נפוץ בגופים רבים של ביצוע מבחן ממוחשב שמטרתו לבחון את רמת המהימנות של המועמד לפני מתן גישה למידע רגיש. לביקורת נמסר כי, מבחן מהימנות ממוחשב אינו מתבצע במסגרת הליך המיון במועצה.

<u>המלצות הביקורת</u>

הביקורת סבורה כי כדאי לבחון שילוב מבחן מהימנות ממוחשב היכול להוות כלי מיון נוסף בנוגע לתפקידים בהם נדרשת גישה למידע אישי רגיש. הן בנוגע לעובדים והן בנוגע ליועצים חיצוניים שיכולים להיחשף למידע רגיש של המועצה.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

4.6. הדרכות עובדים

סעיף 7 לתקנות הגנת הפרטיות קובע:

"(ב) בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם, יקיים בעל מאגר מידע הדרכות לבעלי הרשאות בנושא החובות לפי החוק ותקנות אלה, וימסור להם מידע על אודות חובותיהם לפי החוק ונוהל האבטחה.

(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר פעילות הדרכה תקופתית לבעלי הרשאות שלו, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידיהם, ובדבר חובות בעלי ההרשאות לפיהם; הדרכה כאמור **תיערך אחת לשנתיים לפחות**.."

ממצאים:

מבדיקת הביקורת עלה כי, העובדים בכניסתם לעבודה החל אוקטובר 2018 חותמים על טופס הצהרת סודיות ו- על טופס התחייבות למדיניות אבטחת מידע ומקבלים תדריך ממחלקת מחשוב. יחד עם זאת קיימים עובדים ותיקים שלא הוחתמו בדיעבד על טפסים החדשים.

לביקורת הוצג תיעוד כי, בשנת 2018 ו- 2019 בוצעו הדרכות ריענון לעובדים הקיימים.

בנוסף, כיום לצורך הגברת מודעות וכושר התמודדות של עובדים עם מתקפות סייבר בארגונים רבים נפוץ תהליך של ביצוע סימולציה של קמפיינים של פישינג באמצעות שליחת דוא"ל פישינג לעובדים לצורך תרגול מודעות ובדיקת תגובה שלהם (האם העובד ילחץ על הלינק למשל). קיימת אפשרות לייצר תרגול כזה באופן פנימי או להשתמש בשירות חיצוני.

הביקורת בצעה במסגרת ביקורת סימולציה של קמפיין פישינג בדוא"ל וטלפון ותוצאות המבדק מראים כי, מודעות העובדים למתקפות פישינג במועצה אינה גבוהה בנוסף הביקורת גם בחנה ערנות העובדים לגבי שיחות ועידה באפליקציה ZOOM וגם פה נראה שעובדים לא מודעים לסיכונים בשימוש באפליקציה. לפירוט הבדיקות של מודעות עובדים ראה סעיף 4.22 .

<u>המלצות הביקורת</u>

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

1. להחתים כלל העובדים הקיימים על טפסי הצהרת סודיות והתחייבות למדיניות אבטחת מידע של מועצה.
2. לבצע הדרכה ייעודית למנהלי מאגרים בנוגע לחובותיהם לפי חוק הגנת הפרטיות.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

3. לבצע תרגולי קמפיינים של פישינג להגברת יכולת עובדים להתמודד עם אירועי פישינג אמיתיים ולהעביר הדרכות ממוקדות לעובדים שנכשלו.

4.7. בקרת הרשאות גישה

בסעיף 8 בתקנות ניהול הרשאות גישה נרשם כדקלמן:

"(א) בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

(ב) בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן - רשימת ההרשאות התקפות)."

ממצאים:

לא קיים תהליך ניהול הרשאות מבוקר באופן מלא במועצה הכולל טופס הענקת הרשאות מובנה ומפורט וטופס טיולים בעזיבת העובד.

המועצה טרם בצעה מיפוי מדויק של איזה סוגי הרשאות נדרשות ברמת כל תפקיד כנדרש בתקנות. מתן הרשאות באמצעות העתקת הרשאות מעובד אחר עלול לגרום לכך שעובד חדש עלול לקבל הרשאות עודפות שצבר עובד ותיק שלא בהכרח נחוצות לו למילוי תפקידו.

כמו כן, טרם בוצע תהליך תקופתי של תיקוף הרשאות גישה קיימות לכלל מורשי גישה ולכל המאגרים באמצעות סקירת הרשאות על ידי כל מנהלי המאגרים. במסגרת תהליך תיקוף כזה כל מנהל מאגר נדרש לקבל הרשאות גישה לכל מאגר פר משתמש ולקבוע אם עדיין הרשאה זו נחוצה לכל משתמש או מדובר בהרשאה עודפת.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

<u>המלצות הביקורת</u>

1. לבצע מיפוי מדויק של איזה סוגי הרשאות נדרשות ברמת כל תפקיד למערכות מאגרים.
2. לבצע תיקוף תקופתי של נאותות הרשאות בכל המאגרים תוך מעורבות כל מנהל המאגר בנוגע להרשאות הגישה למאגר עליו הוא אחראי.
3. לייצר טופס קליטת עובד חדש וטופס טיולים שיאפשרו תיעוד מדויק ואישור של סוגי הרשאות שנדרש להגדיר לעובד פר מאגר מידע/מערכת וסוג שירות כמו גישה מרחוק, גלישה באינטרנט, שימוש בדיסק און קי.
4. לבטל פרקטיקה של מתן הרשאות לעובד חדש כמו לעובד קיים על מנת לא לגרום למצבים של עודף הרשאות.

4.8. בקרה ותיעוד גישה

בסעיף 10 בתקנות בנושא בקרה ותיעוד גישה נרשם:

(א) במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (בתקנה זו - מנגנון הבקרה ,) ובכלל זה נתונים אלה :זהות המשתמש ,התאריך והשעה של ניסיון הגישה ,רכיב המערכת שאליו בוצע ניסיון הגישה ,סוג הגישה ,היקפה ,ואם הגישה אושרה או נדחתה.

(ב) מנגנון הבקרה לא יאפשר ,ככל יכולתו ,ביטול או שינוי של הפעלתו ;מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.

(ג) בעל מאגר מידע יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

(ד) נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.

ממצאים:

במהלך הביקורת נמסר על ידי ממונה אבטחת מידע כי, טרם בוצע תהליך מיפוי מקיף ברמת

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

כל מאגר ומערכת מאגר האם אכן מנגנון תיעוד אוטומטי לפעולות משתמשים עומד בדרישות

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

התקנות, לרבות שמירת תיעוד לתקופה של 24 חודש. טרם נקבע נוהל בדיקה שגרתי של נתוני התיעוד כפי שנדרש בתקנות.

<u>המלצות הביקורת</u>

1. להגדיר נוהל בדיקה שגרתי של תקינות נתוני התיעוד בכל המאגרים כולל מערכות מאגרים שמסופקים על ידי ספקי מיקור חוץ ברמת סיכון בינונית וגבוהה ולדווח על תוצאות בדיקה לועדת היגוי.
2. בהתאם לתוצאות הבדיקה לבצע תיקונים נדרשים בכל מנגנון תיעוד על מנת לעמוד בדרישות התקנות.

4.9. קיום הגנה אפקטיבית כנגד מתקפות מתוחכמות

רקע:

סעיף 14)א(לתקנות קובע:

"בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב."

בשנים אחרונות התגברו מתקפות סייבר מתוחכמות המנצלות פרצות ZERO DAY. אלו הן פרצות שמתגלות על ידי גורמים זדוניים ולא מועברים לידיעת יצרנים לצורך ביצוע תיקונים. לפרצות אלה טרם הוגדרו חתימות בתוכנת אנטי וירוס ומוצרי אבטחה נוספים ולכן הן עלולות לא להתגלות ולא להיחסם . כמו כן, גורמים זדוניים כותבים נוזקות ייעודיות חדשות לניצול פרצות חדשות אשר לרוב, מופצות בקמפיינים של דיוג)פישינג(בדואר אלקטרוני או דרך אתרי האינטרנט ואף מופצות ללא ידיעת המשתמש באמצעות התקן נייד.

לצורך התמודדות עם פרצות מתוחכמות אלה פותחו טכנולוגיות שהוכיחו אפקטיביות

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

בשילוב של מספר טכנולוגיות, כגון: SANDBOX (קופסת חול-סביבה וירטואלית בה נבחנת התנהגות קובץ לאיתור פעילות זדונית לפני שחרורו למשתמש), Endpoint Detection and Response EDR, Anomaly detection-Behavioral Analysis, Honey pots, CDR (Content Disarm and Reconstruction – הלבנת קבצים).

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

נמצא כי, במועצה קיים שימוש במערכת חומת אש עם מודולים שונים, מערכת אנטי וירוס בגרסה עדכנית, כולל ניהול התקנים ניידים, מסנני תוכן לדוא"ל וגלישה באינטרנט, עמדות הלבנה למדיה נתיקה.

ממצאים:

הביקורת סבורה כי, לאור התגברות מתקפות סייבר, קיים מקום להוסיף שכבות הגנה נוספות כמפורט להלן:

- נדרש להפעיל בחומת אש הקיימת במועצה מודול SANDBOX לבדיקת קבצים מורדים מאינטרנט.
- נדרש להוסיף מודול SANDBOX במסנן דוא"ל או מודול הלבנה CDR בחומת אש הקיימת לבדיקה מתקדמת של קבצים מצורפים בדוא"ל נכנס.
- במערכת חומת אש במועצה נדרש להפעיל מודול DEEP HTTPS INSPECTION לבחינה מעמיקה של תעבורה מוצפנת לאתרים עם תעודות SSL שכיום מהווים מעל 80 אחוז מתעבורת אינטרנט.
- במערכת חומת אש נדרש להוסיף מודול GEO Protection שמאפשר חסימת גישה למדינות למשל מדינות ערב איתן אין למדינת ישראל יחסים, ומדינות נוספות מסוכנות בהיבטי סייבר לגביהן לא קיים צורך ארגוני לתקשורת מולן.
- נדרש להפעיל בתחנות קצה מערכת EDR לאיתור אנומאליות מעבר לאנטי וירוס הקיים שכיום אפקטיבי רק ב 70-80 אחוז.

יצוין כי, מדובר בטכנולוגיות נפוצות כיום בארגונים בסדר גודל של המועצה ואף בארגונים בעלי פעילות פחותה.

<u>המלצות הביקורת</u>

1. להפעיל מודולים והגדרות נוספות במוצרי אבטחה הקיימים במועצה לשיפור אפקטיביות המוצרים להתמודדות עם מתקפות סייבר.
2. לבחון יישום טכנולוגיות מתקדמות נוספות בהיבטי עלות תועלת על מנת להשיג יכולת נאותה להתמודד עם מתקפות סייבר מתוחכמות.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

4.10. אבטחת טלפונים ניידים וטאבלטים

באמצעות אפליקציות זדוניות שמשתמשים תמימים מורידים למכשירים ניידים שברשותם, ניתן לגנוב מידע רגיש מהטלפון או מהטאבלט, כולל סיסמאות גישה ופרטי דואר אלקטרוני ארגוני שעלולים לכלול נתונים רגישים כולל אישיים.

בארגונים רבים קיים כיום שימוש בטכנולוגיה לניהול ואבטחת התקנים ניידים (MDM) המספקת הגנה מלאה על המידע הנמצא במכשיר, מבלי לפגוע בפרטיות המשתמש.

ממצאים:

נמסר כי, טרם הוטמע במועצה פתרון להגנה על טלפונים ניידים מסוג MDM .

נוסף על כך, לא יושמו הגדרות אבטחה בסיסיות, כגון אכיפת הגדרת קוד גישה למכשיר אשר מבצע סנכרון לדוא"ל ארגוני, וחיבור רק ממכשיר מורשה המזוהה לפי פרמטרים של מכשיר.

<u>המלצות הביקורת</u>

מומלץ לבחון ליישום הפתרון MDM ועד להשלמת יישום להפעיל מנגנוני אבטחה בסיסיים כפי שתוארו לעיל בממצא לצמצום הסיכון.

4.11. אבטחת התקנים ניידים

סעיף 12 לתקנות קובע כי "בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה ; בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד באותו מאגר מידע ; לעניין זה יראו

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד."

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

ממצאים:

1. נמצא כי, מיושמת חסימה למניעת חיבור מדיה נתיקה לתחנות קצה לחלק גדול ממשתמשי קצה. כיום חלק מהמשתמשים מורשים לחבר מדיה נתיקה ספציפית בלבד (לפי מספר סיריאלי) שהולבנה.
2. יחד עם זאת, לא הופעלה טכנולוגיה להצפנת נתונים במדיה נתיקה ובדיסקים קשיחים של המחשבים הניידים.
3. לא נעשה שימוש בטכנולוגיה למניעת זליגת מידע רגיש בזמן העתקת נתונים למדיה נתיקה (מסוג DLP).

<u>המלצות הביקורת:</u>

1. ליישם שימוש במנגנונים לצמצום הסיכון כתוצאה מחיבור כגון: טכנולוגיה להצפנת נתונים, יישום מודול DLP ועוד.
2. יש לבצע הצפנת דיסקים קשיחים בכל מחשבים ניידים המונפקים על ידי המועצה.

4.12. מדיניות בקרת גלישה באינטרנט

סעיף 14)א(לתקנות קובע:

"בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב."

כיום הגלישה באינטרנט מבוצעת דרך חומת אש ומופעל מודול סינון אתרים וקבצים. המודול אמור לחסום גישה לקטגוריות של אתרים שמוגדרים כחסומים לגלישה כמו אתרים עם תוכן לא הולם וגם לחסום הורדה של קבצים בפורמטים לא מורשים.

ממצאים:

נמצא כי, מדיניות הגלישה במועצה הינה מתירנית כאשר לא מיושמת חסימה של חלק

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

מקטגוריות מסוכנות כמו אתרי שיתופי ואחסון קבצים, שירותי VPN, אתרי משחקים, אתרי סטרימינג. בנוסף לא קיימת חסימה להורדה של קבצי הרצה וסקריפטים. לפירוט ממצאים ראה נספח א'.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

<u>המלצות הביקורת</u>

1. יש לבדוק מחדש את מדיניות הגלישה הקיימת כיום במועצה ולהטמיע מדיניות גלישה מחמירה יותר לכל קבוצות העובדים בהתאם לעקרון של אפשרות גלישה לצורכי עבודה בלבד תוך צמצום סיכונים לזליגת מידע רגיש תוך חסימת קטגוריות נוספות.
2. יש לבדוק את הגדרות סינון הקבצים הקיימת כיום במטרה למנוע הורדת קבצי הרצה וסקריפטים.

4.13. הרשאות אדמיניסטרטור

מרבית הנוזקות כיום מנצלות הרשאות של משתמשי קצה על מנת לבצע פעולות זדוניות במערכות מחשב. לאור זאת הבקרה המומלצת כיום הינה כי, למשתמשי קצה יוקצו הרשאות נמוכות ביותר ברמת מערכת ההפעלה.

ממצאים:

נמצא כי, בתחנות קצה קיימת עדיין הרשאה של לוקל אדמין למשתמש קצה המאפשרת לו לבצע התקנה של תוכנות וביצוע שינויים בהגדרות מחשב. בנוסף ממשק POWERSHELL שהינו כלי ניהול סיסטם פתוח למשתמש קצה ומאפשר להריץ פקודות מערכת הפעלה רגישות.

קיים כלי אפקטיבי וחינמי מבית מיקרוסופט לניהול הרשאות לוקל אדמין בתחנות קצה בשם LAPS.

<u>המלצות הביקורת</u>

1. לבצע הסרה של הרשאות לוקל אדמין מכל המשתמשים הרגילים בתחנות קצה.
2. לחסום למשתמשים הרגילים יכולת הפעלת ממשק PowerShell.
3. לקדם בהקדם שימוש במוצר LAPS לניהול משתמש לוקל אדמין המשמש את טכנאים בתחנה.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

4.14. אבטחת גישה מרחוק למשאבי המועצה

בסעיף 14(ג) בתקנות נרשם "במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, ייעשה שימוש נוסף על אמצעי אבטחה כאמור בתקנות משנה (א) ו(ב), באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של בעל הרשאה למאגר מידע ברמת האבטחה הבינונית והגבוהה ייעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה."

מערך הסייבר ורשות הגנת הפרטיות פרסמו הנחיות לגבי אמצעי אבטחה נאותים בגישה מרחוק מהבית לרשת אירגונית לפירוט ראה נספח ב.

כיום אמצעי אבטחה מקובל בגישה מרחוק הינו מנגנון הזדהות חזקה הכולל שני שלבים בהזדהות לפחות. סיסמה קבועה כבר אינה מהווה בקרה חזקה כאשר קיימים דרכים רבות להשגת הסיסמא על ידי גורמים זדוניים. ההזדהות החזקה הנפוצה הינה קיום מנגנון לחילול סיסמה חד פעמית באמצעות התקן הנתון לשליטה בלעדית של המשתמש קצה.

ממצאים:

1. הביקורת מצאה כי, מיושמת הזדהות חזקה בגישה מרחוק למערכות המועצה בממשק VPN בחומת אש על ידי עובדים וספקים. מוגדר זמן ניתוק במקרה של חוסר פעילות.
2. נמצא כי, לא מבוצעת חסימה להעתקת קבצים בין תחנת קצה המרוחקת לרשת אירגונית. במצב זה ניתן להעתיק קבצים ממחשב הקצה לרשת האירגונית ובאופן זה ניתן להעביר נוזקות לרשת אירגונית או להעביר קבצים רגישים מחוץ לרשת אירגונית למחשב מרוחק.
3. ממשק ה -VPN אינו מוגן ב GEO PROTECTION ומתאפשרת גישה מכל העולם. בפועל כל הגישה מרחוק על ידי עובדים מבוצעת מישראל בלבד.
4. לא מבוצעת בדיקה של מחשב קצה לפני חיבורו לרשת האירגונית אם קיימים בו אמצעי אבטחה נאותים. כיום מאפשרים חיבור כל מחשב כולל מחשבים בבתי העובדים ללא

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

אנטי וירוס.

5. נמצא כי, לא מיושמת הקשחה נאותה של מחשבים ניידים ארגוניים מהם מבוצעת גישה מרחוק)נבדק מחשב נייד של מבקר המועצה(. קיימות הרשאות מנהל מקומי להתקנת תוכנות ואפשרות להריץ פקודות POWERSHELL. גרסת אנטי וירוס במחשב הנייד

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

שנבדק הייתה 7.0 וקיימת גרסה 7.3 מתקדמת יותר. נמצא כי לא הותקנו חלק מעדכוני אבטחה. לא מיושמת הצפנת דיסק קשיח במחשב הנייד.

6. בנוסף קיים שירות OWA לגישה מרחוק לדוא"ל ארגוני אשר מאפשר גישה לתיבת דוא"ל מכל מקום בעולם)לא מיושם GEO PROTECTION(דרך דפדפן עם סיסמת גישה של המשתמש לרשת הפנימית בלבד ולא מיושם מנגנון סיסמה חד פעמית של צורת הזדהות חזקה. במצב זה גורמים זדוניים עלולים לנחש את הסיסמא או לגנוב אותה בתרגילי פישינג וחדירה למחשב הקצה ממנו מבוצעת גישה מרחוק. **הביקורת בצעה מבדק כזה והשיגה גישה לתיבות דוא"ל ארגוני כמפורט בנספח ב'.**

<u>המלצות הביקורת</u>

1. ליישם צורת הזדהות חזקה בגישה לדוא"ל ארגוני בשירות OWA או לבטל שימוש בשירות זה.
2. לחסום אפשרות להעתקת קבצים בין מחשב מרוחק לבין הרשת הפנימית של המועצה לכלל הניגשים מרחוק.
3. לבצע הקשחה נאותה במחשבים ניידים ארגוניים מהם מבוצעת גישה מרחוק.
4. להגדיר בדיקה של נאותות אמצעי אבטחה במחשב קצה ממנו מבוצעת גישה מרחוק ולא לאפשר חיבור מחשבים לא מוגנים באנטי וירוס מעודכן, מערכת הפעלה עדכנית ועדכוני אבטחה מותקנים. 5.
   לצמצם אפשרות גישה מכל העולם לממשק ה- VPN ו- OWA ככל שניתן באמצעות GEO PROTECTION.

4.15. סגמנטציה של הרשת הפנימית

בתקנות הגנת הפרטיות בסעיף 13 ב) נרשם: "בעל מאגר מידע יפריד, בהיקף ובמידה הסבירים האפשריים , בין מערכות המאגר אשר ניתן לגשת מהן למידע ,לבין מערכות מחשוב אחרות המשמשות את בעל המאגר."

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

ממצאים:

נמצא כי, בנוגע למערכות המסופקות על ידי ספקי מיקור חוץ מתקיימת הפרדה פיזית כאשר מערכות נמצאות ברשתות של הספקים. בנוסף קיימת סגמנטציה חלקית של חלק ממחלקות הפועלות מבניינים מרוחקים לבניין הראשי של המועצה.

יחד עם זאת נמצא כי, בבניין הראשי של המועצה כיום הרשת הפנימית של המועצה שטוחה וניתן להגיע ברמת תקשורת מכל רכיב לכל רכיב בתוך הרשת הפנימית כולל גישה תקשורתית למאגרי נתונים רגישים.

סגמנטציה מיטבית מושגת באמצעות חומת אש רשתית הממוקמת בתוך הרשת ומחלקת את הרשת באמצעות הפרדה פיזית ולוגית ולכל הפחות הפרדה בין סגמנט של תחנות קצה ושרתים וגם סגמנטציה פנימית לפי מחלקות .

<u>המלצת הביקורת:</u>

יש ליישם סגמנטציה ברשת הפנימית בדגש על מידור של שרתים ובסיסי נתונים של מאגרי מידע רגישים בהם מנוהל מידע אישי.

4.16. מערכת מניעת חיבור התקנים זרים לרשת הפנימית

בהינתן גישה פיזית של גורם זדוני למשרדי הארגון, הגורם יכול לבצע ניסיון חדירה באמצעות חיבור מחשב או התקן זר לרשת הפנימית תוך קבלת כתובת IP תקינה ברשת. באופן זה למעשה הגורם הזדוני עוקף מנגנוני אבטחה היקפיים המיושמים ברשת לרבות חומת אש. על מנת לספק מענה לחשיפה זו פותחה טכנולוגיה בשם NETWORK ACCESS CONTROL-NAC- בקרת גישה לרשת. הטכנולוגיה באמצעות מנגנונים שונים מסוגלת לזהות התקן לא מורשה המנסה להתחבר לרשת הפנימית בארגון ולנתק אותו מהרשת)על ידי ניתוק של ניקודת רשת חמה במתג(ובאופן זה למנוע חדירה לרשת הפנימית.

ממצאים:

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

נמצא כי, לא מיושמת טכנולוגית NAC ברשת הפנימית של המועצה.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

<u>המלצות הביקורת</u>

לבחון הטמעה של טכנולוגית NAC בכל הרשת הפנימית.

4.17. שימוש במערכות הפעלה לא מעודכנות

רקע:

סעיף 13)ג(לתקנות קובע כי "בעל מאגר מידע ידאג לכך שייערכו עדכונים שוטפים של מערכות המאגר, לרבות חומר המחשב הנדרש לפעולתן ; לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים".

ממצאים:

הביקורת מצאה כי, מיושמת מדיניות אחידה לביצוע עדכוני אבטחה ברמת מערכות הפעלה WINDOWS ו- OFFICE בשרתים ותחנות קצה באמצעות כלי לעדכון וניטור מרכזי WSUS.

יחד עם זאת עדיין נמצאו עדכוני אבטחה חסרים ברמת מערכות הפעלה ואפליקציות צד ג' שונות במסגרת בדיקות שבוצעו על ידי הביקורת שכללו סריקה עם כלי ייעודי לאיתור חולשות אבטחה באופן אוטומטי . לפירוט ראה נספח א'.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

Vulnerabilities by Plugin

- 135187 (3) - Dell iDRAC Buffer Overflow Vulnerability (CVE-2020-5344)
- 55933 (1) - Juniper Junos Unsupported Version Detection
- 96316 (1) - Juniper Junos Multiple OpenSSL Vulnerabilities (JSA10759) (SWEET32)
- 41028 (20) - SNMP Agent Default Community Name (public)
- 20007 (5) - SSL Version 2 and 3 Protocol Detection
- 109208 (3) - Dell iDRAC Products Multiple Vulnerabilities (Mar 2018)
- 111604 (3) - Dell iDRAC Products Multiple Vulnerabilities (June 2018)
- 128148 (3) - Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities
- 99130 (2) - ESXi 6.0 U1 < Build 5251621 / 6.0 U2 < Build 5251623 / 6.0 U3 < Build 5224934 Multiple Vulnerabilities (VMSA-2017-0006) (remote check)
- 118466 (2) - ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)
- 118885 (2) - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)
- 123518 (2) - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)
- 97833 (1) - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
- 100464 (1) - Microsoft Windows SMBv1 Multiple Vulnerabilities
- 100995 (1) - Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
- 123642 (1) - Apache 2.4.x < 2.4.39 Multiple Vulnerabilities

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

Vulnerabilities by Plugin

- 10297 (2) - Web Server Directory Traversal Arbitrary File Access
- 84729 (2) - Microsoft Windows Server 2003 Unsupported Installation Detection
- 92606 (1) - Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU)
- 97994 (1) - Microsoft IIS 6.0 Unsupported Version Detection
- 99523 (1) - Microsoft Windows Server 2003 IIS 6.0 WebDAV PROPFIND Request Handling RCE (EXPLODINGCAN)
- 20007 (1) - SSL Version 2 and 3 Protocol Detection
- 87011 (1) - Oracle WebLogic Java Object Deserialization RCE
- 90709 (1) - Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU)
- 94511 (1) - Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU)
- 96803 (1) - Oracle WebLogic Java Object RMI Connect-Back Deserialization RCE (January 2017 CPU)
- 97833 (1) - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
- 100464 (1) - Microsoft Windows SMBv1 Multiple Vulnerabilities
- 109429 (1) - Oracle WebLogic Server Deserialization RCE (CVE-2018-2628)
- 111665 (1) - Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

בנוסף, במבדק נמצאו עדיין מספר שרתים עם מערכת הפעלה WIN 2003 מדובר במערכת הפעלה שהיצרן אינו תומך כבר בהיבטי אבטחה שלה כבר מספר שנים ולכן חשופה לפרצות אבטחה רבות.

כמו כן, קיימות עדיין תחנות קצה בהן מותקן WIN 7, ושרתי WIN 2008 כידוע לפי פרסומי יצרן נגמרה התמיכה במערכת הפעלה זו בינואר 2020.

<u>המלצות הביקורת:</u>

1. להשלים החלפת כל השרתים עם מערכת הפעלה WIN 2003 בהקדם.
2. להשלים בהקדם שדרוג של תחנות מסוג WIN 7 .
3. להשלים בהקדם שדרוג של שרתי WIN 2008.
4. להפעיל באופן תקופתי כלי סריקה ייעודי ומקצועי באמצעותו ניתן לבצע סטאטוס עדכניות מערכות הפעלה ותוכנות המותקנות במחשבים ושרתים ברשת ולבצע עדכוני אבטחה לרבות בתוכנות צד' ג.
5. להשלים ביצוע עדכוני אבטחה ושדרוגי גרסאות בהתאם לממצאים שעלו בביקורת.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

המועצה האזורית תמר
ים המלח

4.18. ניטור, דיווח ותגובה לאירועי אבטחת מידע

סעיף 11 לתקנות קובע:

בשלמות "(א) בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (להלן - אירועי אבטחה); ככל האפשר יבוסס התיעוד האמור על רישום אוטומטי.

(ב) בנוהל האבטחה יקבע בעל מאגר מידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מידיים אחרים הנדרשים וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות."

מצב נוכחי:

- חלק מהתרעות אבטחה מתקבלות בדוא"ל ממוצרי אבטחת מידע מסוימים לממונה אבטחת מידע וצוות תשתיות. מבוצעת בדיקה מדגמית של לוגים בחומת אש ואנטי וירוס אך לא באופן קבוע.
- מתקבלות התרעות בדוא"ל לממונה אבטחת מידע על מתקפות סייבר המתפרסמות בעולם ועל פרצות אבטחה שמתגלות במוצרי תוכנה וחומרה מ – CERT
- קיימים נהלים בנושא הכלה ותגובה לאירועי סייבר.

יחד עם זאת הביקורת מצאה כי,

- נמצא כי, לא מנוהל מאגר ידני או אוטומטי לתיעוד כלל אירועי אבטחת מידע, לרבות אירועים פוטנציאליים.
- לא מיושמת מערכת SIEM ושירות מוקד SOC אנושי לניטור ותגובה רציפה לאירועי סייבר.
- לא מתקיימים דיונים באירועי האבטחה בפורום מנכ"ל/ועדת היגוי כנדרש בתקנות.
- לא הוקם צוות תגובה מקצועי אשר ייתן מענה מהיר ואפקטיבי במקרה של התרעה על אירוע סייבר.
- לא מתקיימים תרגולים תקופתיים לתרגול תגובה לאירועי סייבר.
- לא מתבצע שימוש שוטף בשירות מודיעין סייבר חיצוני וספציפי לארגון אשר יספק התראות

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

על איומים הרלוונטיים לארגון, על חשש לזליגת מידע רגיש שמוצג ברשת הציבורית או רשת האפלה, תוקפים ו/או מטרות פוטנציאליות תוך הספקת הנחיות לאופן התמודדות.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

<u>המלצות הביקורת:</u>

1. מומלץ לבחון רכישה של טכנולוגיה SIEM ושירות SOC חיצוניים.
2. מומלץ לבחון שימוש בשירות מודיעין סייבר מקצועי ייעודי למועצה.
3. מומלץ להקים צוות ייעודי לתגובה לאירועי סייבר ולבצע תרגולים תקופתיים של הצוות.
4. מומלץ לנהל מאגר ידני או אוטומטי לתיעוד כלל אירועי אבטחת מידע, לרבות אירועים פוטנציאליים.
5. מומלץ לדווח על אירועי אבטחת מידע לועדת היגוי בהתאם לנדרש בתקנות.

4.19. מיקור חוץ

<u>במסגרת תקנות הגנת הפרטיות בסעיף 15 נקבע כי:</u>

גורם המחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע;

(ו) חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה (ה);

(ז) התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

)2(ם החיצוני לכלול בהסכם עם הגורם הנוסף
את כל הנושאים המפורטים בתקנה זו;

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

(ח) חובתו של הגורם החיצוני לדווח ,אחת לשנה לפחות ,לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה;

4) ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה ,בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה)1(."

ממצאים:

הביקורת מצאה כי, המועצה התקשרה עם מספר ספקי מיקור חוץ, המהותית ביותר הינה חברת מטרופולינט המספקת מערכות ליבה מרכזיות. קיים מיפוי ספקים אלה והם רשומים כמחזיקי מידע. קיים גם נוהל עבודה בנושא ספקים וספקים חתומים על הסכמים.

המועצה מבצעת פנייה תקופתית לספקיה על מנת לדרוש לקבל מהם סטאטוס עמידה בדרישות תקנות הגנת הפרטיות כנדרש בתקנות.

מבדיקת הביקורת עלה כי, החברה מטרטפולינט וחברת טויסטק שמספקת שירותי תשתיות מחזיקות בתעודת הסכמה לתקן אבטחת מידע מקובל ISO 27001.

יחד עם זאת המועצה לא פנתה לקבל תוצאות מבדקי חדירה וסקרי אבטחה תקופתיים מספקי מיקור חוץ.

<u>המלצת הביקורת:</u>

לדרוש לקבל מספקי מיקור חוץ סיכומי דוחות מבדקי חדירה וסקרי אבטחה תקופתיים ולוודא שאין ממצאים קריטיים ומהותיים שלא מטופלים בזמן סביר

וקיימת תכנית עבודה לטיפול כלל הממצאים.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

המועצה האזורית תמר
ים המלח

4.20. מסמכי הגדרות מאגר ובדיקת מידע רב מן הנדרש

בתקנות הגנת הפרטיות סעיף 2 :

(א) בעל מאגר מידע יגדיר במסמך הגדרות מאגר(להלן - מסמך הגדרות המאגר ,)את כל העניינים האלה לפחות:

)1(תיאור כללי של פעולות האיסוף והשימוש במידע;

)2(תיאור מטרות השימוש במידע;

)3(סוגי המידע השונים הכלולים במאגר המידע ,בשים לב לרשימת סוגי המידע שבפרט בתוספת הראשונה;

)4(פרטים על העברת מאגר המידע ,או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה ,מטרת ההעברה ,ארץ היעד, אופן ההעברה וזהות הנעבר;

)5(פעולות עיבוד מידע באמצעות מחזיק;

)6(הסיכונים העיקריים של פגיעה באבטחת המידע ,ואופן ההתמודדות עמם;

)7(שמו של מנהל מאגר המידע ,של מחזיק המאגר ושל הממונה על אבטחת מידע בו ,אם מונה כזה.

) ג(בעל מאגר מידע יבחן ,אחת לשנה ,אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר.

ממצאים:

1. לא נכתבו מסמכי הגדרות מאגר למאגרים השונים כנדרש בתקנות.
2. במהלך עבודת הביקורת, הוחל ברישום מאגרים נוספים מאגר כוח אדם , מאגר מצלמות אבטחה ומאגר פניות תושבים מוקד 106.
3. מבירור שקיימה הביקורת עלה כי, לא בוצע תהליך בחינה כלשהו אם לא נשמר מידע רב מן הנדרש במאגרים. הביקורת סבורה כי, במידה והיה מתקיים תהליך בחינה כזה, סביר להניח היה מתגלה כי, במאגרים השונים מנוהל מידע ישן על תושבים לשעבר, עובדים לשעבר וכדומה.

<u>המלצות הביקורת:</u>

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

1. מומלץ לבצע בחינה של קיום מידע עודף במאגרים בהקדם האפשרי.
2. נדרש לכתוב מסמכי הגדרות מאגר לכל המאגרים הקיימים במועצה, ולעדכן אותם אחת לשנה .

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

4.21. מיפוי מערכות המאגר

<u>בהתאם לנרשם בסעיף 5 בתקנות:</u>

א(בעל מאגר מידע יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, ובכלל זה:

1(תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע;

2(מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;

3(תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן;

4(תרשים הרשת שפועל בה המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה;

5(תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

ממצאים:

נמצא כי, בניגוד לדרישות התקנות לא מנוהל במועצה תיק אתר ותרשים רשת עדכניים, ארכיטקטורה, מיפוי מצאי לרבות לגבי מערכות במיקור חוץ.

<u>המלצות הביקורת:</u>

להכין תיק אתר ומיפוי מערכות כנדרש בתקנות הגנת הפרטיות.

4.22. מבדקים לבדיקת מודעות עובדים

כיום מתקפות פישינג)דיוג(מהוות מרבית המתקפות המבוצעות דרך אינטרנט. מטרת המתקפות לעקוף מנגנוני אבטחה הנמצאים בכניסה לרשת תוך מיקוד במשתמש הקצה. קיים שימוש בטכניקות הנדסה חברתית תוך ביצוע מניפולציות פסיכולוגיות על משתמש קצה. הדבר כולל התחזות לגורם סמכותי, זיוף אתרי אינטרנט, פרטים, ניסיון קבלת פרטי הזדהות של משתמש קצה, ניסיון להחדיר קובץ שנראה תמים הכולל נוזקה שמאפשרת להשתלט על מחשב המשתמש קצה או להדליף מידע רגיש.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

החוליה החלשה באבטחת מידע הינה הגורם האנושי שנתון למניפולציות מטבעו לתת אמון. לכן נושא חשוב באבטחת מידע זה הדרכות והגברת מודעות.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

צוות הביקורת הכין תשתית ובצע קמפיין פישינג באמצעות שליחת דוא"ל מתחזה. שלבי הבדיקה היו כדלקמן:

א. הקמת אתר עם לוגו של עירייה לרישום להדרכת אבטחת מידע ב ZOOM. העובדים נדרשו להזין שם משתמש וסיסמא ברשת לצורך הרישום להדרכה תוך בחירת מועד מתאים להם.

ב. יצירת תיבת דוא"ל המתחזה לדוא"ל של מחלקת מחשוב.

ג. יצירת הודעת פישינג שאמורה לפתות עובדים ללחוץ על לינק.

ד. ביצוע שליחה ותיעוד פעולות עובדים שלחצו על לינק וחלקם גם הזינו סיסמאות.

הופצו מיילים ל-133 תיבות דוא"ל בהתאם לרשימה שהועברה ממנהל מערכות מידע. סך הכול 28 עובדים לחצו על הלינק בדוא"ל מתחזה ו- 15 עובדים גם הזינו סיסמאות גישה.

הדבר מעיד על רמת מודעות לא גבוהה לסיכוני פישינג.

בנוסף צוות הביקורת בצע פניה טלפונית למספר עובדים בעלי מחשבים ניידים והציג עצמו כנציג חברת מחשוב שעובדת עם מנהל מערכות מידע)הבדיקה בוצעה בתיאום עם מנהל מערכות מידע ואישורו(אחד העובדים שיתף פעולה באופן מלא ואפשר חיבור למחשב נייד ומסר סיסמאות.

לגבי אפליקציית ZOOM הצוות הדגים גישה לישיבת הנהלה שהתקיימה ללא צורך בסיסמא לגישה לחדר וללא שמישהו בקש להזדהות)הצוות לא הפעיל מצלמה(.

לתיאור והמחשת התרגילים ראה פירוט בנספח ב'.

<u>המלצות הביקורת:</u>

1. לפעול להרחבת הדרכות ותרגולים לצורך הגברת מודעות עובדים בפרט בנושא פישינג בערוצי הטלפון ודוא"ל.
2. לחדד הנחיות לגבי אופן שימוש מאובטח באפליקציות שיחות ועידה.

4.23. מבדקים לבדיקת אפקטיביות מערך האבטחה

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

צוות הביקורת ערך מבדקים שונים במטרה לבחון את יעילות מערך האבטחה של המועצה ולזהות חולשות, במידה שקיימות, תוך ביצוע סריקות ובדיקות של הגדרות. הבדיקות בוצעו מרשת האינטרנט ומתוך הרשת הפנימית.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

עיקרי הממצאים:

- מוגדרת מדיניות סיסמאות חלשה בגישה לרשת ארגונית)מותר אפילו 4 תווים(. הביקורת נצלה מדיניות חלשה בצירוף עם קיום ממשק OWA פתוח, והדגימה חדירה מרחוק לתיבות דוא"ל ארגוני ובתיבת מחלקת שיווק נמצאו גם סיסמאות גישה גלויות במסמך לחשבונות ברשתות חברתיות של המועצה.
- נמצאו ממשקי ניהול רגישים חשופים באינטרנט למתקפות סייבר מכלל העולם.
- קיים שימוש במערכות הפעלה מיושנות, לא נתמכות ולא מועדכנות בתחנות קצה ושרתים והדבר חושף את המועצה לחדירה מצד גורמים זדוניים ונוזקות.
- נמצא חוסר בעדכוני אבטחה קריטיים בתחנות קצה ושרתים החושף את הארגון לחדירה מצד גורמים זדוניים ונוזקות.
- נמצאו ממשקי ניהול ברשת הפנימית החשופים לגישה מכל מקום ברשת והדבר מגביר חשיפה לפרצות אבטחה.
- נמצא שימוש בפרוטוקולים לא מאובטחים ברשת הפנימית.
- קיים שימוש בשירותים ואפליקציות בגרסאות מיושנות ולא מאובטחות והדבר מגביר חשיפה לחדירה מצד גורמים זדוניים ונוזקות.
- לא מיושמות חסימות לגלישה מתחנות קצה לאתרים בקטגוריות מסוכנות וחסימה להורדת קבצים מסוכנים מאינטרנט לתחנות קצה, והדבר מגביר חשיפה לזליגת מידע רגיש או חדירת נוזקות לרשת.
- לא מיושם מגנון סינון לתעבורת אינטרנט מוצפנת DEEP HTTPS INSPECTION בחומת אש ולמעשה חומת האש "עיוורת" לחלק גדול מתעבורת גלישה באינטרנט ב HTTPS ולא יכולה למנוע חדירה של נוזקות לתחנות קצה.
- נמצאו פרצות אבטחה באתר אינטרנט של המועצה, לרבות נמצאו ממשקי ניהול רגישים פתוחים לכל העולם והדבר מגביר חשיפה לחדירה לאתר. בנוסף האתר אינו מוגן במערכת חומת אש מקצועית WAF למניעת מתקפות מתקדמות.
- הביקורת העבירה פורמטים שונים של קבצים לבדיקת אפקטיביות סינון בדואל ונמצאו פורמטים שלא נחסמים ומהווים סיכון אבטחה לארגון.

<u>לפירוט הבדיקות , ממצאים והמלצות ראה נספח ב'- סיכום מבדקים טכנולוגיים.</u>

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

4.24. בדיקת אתרי האינטרנט של המועצה

במסגרת המבדק הועבר שאלון ביקורת לגורמים רלוונטיים וגם בוצעה בחינה ויזואלית של האתר. בנוסף במסגרת סעיף 4.23 בוצעו מבדקי אבטחת מידע על האתר.

האתר המרכזי פותח ומתוחזק על ידי ספק חיצוני בהתאם לתנאי המכרז. קיימת עובדת ייעודית במועצה שאחראית לניהול ובקרת תוכן האתר.

<u>ממצאים:</u>

1. נמצא כי, האתר תומך בנגישות באופן נאות.
2. בבדיקה מדגמית, נמצא כי, כל הפרסומים מועלים עם תאריך עדכון.
3. בבדיקה מדגמית לא נמצאו פרסומים מהותיים שחסרים.
4. קיים אתר נפרד לועדה המקומית לתכנון ובנייה.
5. האתר מתוחזק על ידי ספק מוביל בישראל בתחום זה ובהתאם להסכם ותנאי המכרז.
6. יחד עם זאת, נמצא כי, האתר אינו מוגן במערכת חומת אש אפליקטיבית WAF למניעת מתקפות מתוחכמות ומתקפות מניעת שירות DDOS למניעת שירות ולא מבוצעת מניעת גישה ממדינות מסוכנות כמו מדינות אויב באמצעות מנגנון GEO PROTECTION.
7. נמצאו ממשקי ניהול שונים של האתר החשופים לכלל רשת האינטרנט כמפורט בסעיף 4.23.
8. בסריקה אוטומטית על האתר התגלו חולשות אבטחה שונות כמפורט בסעיף 4.23.
9. הפורטל הארגוני אינו כולל תעודת SSL לגישה מאובטחת לפורטל לעובדים.
   http://portal.ma-tamar.org.il/login/
10. נמצא כי, בטופס פניה למוקד 106 באתר ניתן לעלות קבצים שאינם בפורמט תמונה. במצב זה קיים סיכון שגורמים זדוניים יעלו נוזקות לפריצה לאתר או כמתקפת פישינג כנגד עובדי המוקד.
11. לא קיים נוהל ייעודי לאבטחת מידע והגנת הפרטיות של אתרי האינטרנט במועצה.
12. לא בוצע מבדק חדירה או/ו סקר אבטחת מידע לגבי אתרי האינטרנט של המועצה.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

13. נמצא כי, לא מפורסמת מדיניות הפרטיות באתר האינטרנט של המועצה. האתר מאפשר רישום, יצירת קשר, פניות ציבור, וקבלת דיווח. כמו כן, אין סרגל המודיע בדבר שימוש ב"עוגיות" ומעקב אחרי גולשים.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

14. נמצא כי, תקנון האתר מאוד דליל ביחס למקובל לרבות התייחסות להיבטים משפטיים כגון סתירה בין פרסומי האתר לחוקים ותקנות, אבטחת מידע באתר, אזהרת גולשים לגבי סיכוני גלישה באתר, היבטי דיוור ישיר ועוד.

15. נמצא כי, מאגר הנרשמים ופניות ציבור ופניות מוקד 106 באתר האינטרנט כיום, לא רשום במשרד המשפטים כולל לצורך דיוור ישיר. https://www.ma-tamar.org.il/register/

https://www.ma-tamar.org.il/190/

https://www.ma-tamar.org.il/%D7%A4%D7%A0%D7%99%D7%94-%D7%9C%D7%9E%D7%95%D7%A7%D7%93/

https://www.ma-tamar.org.il/newsletter/

16. נמצא כי, האתר כולל תרגום מאוד חלקי באנגלית ולא כולל שפות אחרות ערבית, רוסית, אמהרית. הנושא צוין כליקוי בדוח מבקר המדינה לאור אי הנגשת האתר לשפות אחרות נפוצות.

17. נמצא כי, אתר התיירות הנוסף שהינו באנגלית אינו כולל מסמך Privacy Policy ו-POLICY COOKIE. כמו כן, לא מיושם COOKIE BANNER באתר אשר מודיע לגולשים על שימוש בעוגיות ומעקב אחר גלישה שלהם. לאור זאת, המועצה חשופה לקנסות על פי חוק הגנת הפרטיות באיחוד אירופאי GDPR המחייב כלל הגופים בעולם שפונים ומציעים מידע ושירותים לתושבי איחוד אירופאי ומנהלים מידע אישי שלהם. הגולשים מחו"ל ובפרט מאיחוד אירופאי יכולים ליצור קשר תוך מסירת פרטיהם האישיים ואף להירשם עם פרטים אישיים לקבלת NEWSLETTER.

https://deadsealand.org.il/contact-us/

https://deadsealand.org.il/newsletter/

<u>המלצות הביקורת:</u>

1. להגדיר נוהל אבטחת מידע והגנת הפרטיות לאתרי האינטרנט של המועצה.
2. להטמיע מנגנוני אבטחת מידע מתקדמים כגון WAF באתרי האינטרנט של המועצה.
3. לקבל ייעוץ משפטי לגבי היבטי הגנת הפרטיות לרבות צורך ברישום מאגר, מדיניות הגנת הפרטיות ושימוש בעוגיות באתרי האינטרנט של המועצה ולבצע שינויים בהתאם

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

הן באתרים בעברית והן באתר באנגלית.

4. לעבות את תקנון האתר בהיבטים נוספים כפי שהוזכר בממצאים לעיל.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

5. לבצע בחינה של חולשות אבטחה שנמצאו במהלך הביקורת באתר האינטרנט הראשי של המועצה ולבצע תיקונים מתאימים.
6. לבצע מבדק חדירה וסקר אבטחה תקופתי על כלל אתרי האינטרנט של המועצה.
7. לבחון אם אין צורך בהנגשת האתרים בעברית לאוכלוסיות דוברות שפות נפוצות אחרות.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

5. תגובת המועצה

המועצה האזורית תמר
ים המלח

כ"ד אדר תשפ"א
08 מרץ 2021

לכבוד
מר רן אורפני, רו"ח
מבקר המועצה
מועצה אזורית תמר

שלום רב,

הנדון: **התייחסות לממצאי ביקורת אבטחת מידע - פברואר 2021**

קיבלנו את דוח ביקורת הגנת הפרטיות ואבטחת המידע שנערכה על ידך באמצעות חב' אינטגריטי.

המועצה משקיעה משאבים רבים בכדי ליישם את דרישות אבטחת מידע על פי הנחיות רשות הסייבר, אגף הסייבר במשרד הפנים וכחלק מלימוד ותחקירי תקיפות שבוצעו כנגד גופים דומים בישראל.

מנמ"ר המועצה מיישם ומתקן את הליקויים המפורטים בדוח, שעיקרם הינו:

א. מידור (סגמנטציה) של רשתות התקשורת והמחשוב השונות
ב. הפעלת מערכת Network Access Control (NAC).
ג. הפעלת מערכת EDR לניטור יחידות קצה
ד. שדרוג מערכי אבטחת מידע על פי ההמלצות בדוח

אנו מקבלים את ממצאי הדוח ופועלים לתיקון הליקויים שנתגלו.

דוח מפורט יועבר עם יישום ותיקון כלל הליקויים.

בברכה,

עידן שילמן
גזבר

עזרא דיין – יועץ
תשתיות מידע וטכנולוגיות בע"מ

נווה זוהר, ד.נ. ים המלח מיקוד 8691000 | טל: 08-6688888 פקס: 08-6584150

ארץ ים המלח
DEAD SEA LAND

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

נספח א' – פירוט מאגרים המנוהלים במועצה:

- מאגר שירות לקוחות
- מאגר מצלמות
- מאגר פניות תושבים מוקד 106
- מאגר כוח אדם
- מאגר שירותים חברתיים רווחה

בגוף ציבורי בהתאם לדרישות התקנות רמת אבטחה של המאגר היה לכל הפחות ברמת אבטחה בינונית

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

המועצה האזורית תמר
ים המלח

נספח ב'- סיכום מבדקים טכנולוגיים

הסיכום כולל המלצות טכניות ודוחות סריקה גולמיים, אשר הועברו בנפרד לתגובת המבוקרים, מפאת רגישות המידע.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

נספח ג' - הנחיות מערך הסייבר הלאומי ורשות הגנת הפרטיות בנושאי סיכוני סייבר במשבר קורונה

https://www.gov.il/BlobFolder/news/telecommuting/he/%D7%94%D7%9E%D7%9C%D7%A6%D7%95%D7%AA%20%D7%9C%D7%99%D7%99%D7%A9%D7%95%D7%9D%20%D7%92%D7%99%D7%A9%D7%AA%20%D7%9E%D7%A9%D7%AA%D7%9E%D7%A9%D7%99%D7%9D%20%D7%9C%D7%A1%D7%91%D7%99%D7%91%D7%94%20%D7%94%D7%90%D7%A8%D7%92%D7%95%D7%A0%D7%99%D7%AA%20VPN.pdf

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

7. המלצות ליישום בעת תכנון תשתית VPN ארגונית

פרק זה בא לסייע לארגון בגיבוש תכנון מיטבי של תשתית ה-VPN הארגונית.

א. מיפוי משתמשים וצרכים

מומלץ למפות את המשתמשים אשר נדרשים להתחבר לסביבה הארגונית ע"י שימוש ברשת וירטואלית פרטית (VPN). **נספח א'** מכיל טבלת עזר בנושא.

ב. הערכת סיכונים (Risk Assessment)

מומלץ כי הארגון יבצע הערכת סיכונים וזאת לשם איתור פערי אבטחה המחייבים מתן מענה. בכלל זה מומלץ כי הערכת הסיכונים תכלול התייחסות לנושאים הבאים:

1. איתור ומיפוי תרחישי תקיפה רלוונטיים;
2. איתור ומיפוי פערים קיימים (Gap Analysis);
3. איתור ומיפוי דרישות חקיקה ורגולציה רלוונטיות;
4. איתור ומיפוי דרישות חוזיות ועסקיות;
5. איתור ומיפוי נכסי הסייבר אשר גישה אליהם מחוץ לסביבה ארגונית עשויה ליצור סיכון לא סביר;
6. איתור ומיפוי פעולות אשר מחייבות נוכחות מקומית של משתמשים (לדוגמה: ביצוע שינויים בהגדרות תצורה של מערך הגנת המידע וסייבר מהווה פעולה רגישה, אשר יתכן כי בהתאם למדיניות הארגונית לא ניתן לבצע מרחוק);
7. המלצה על בקרות הגנה ליישום;
8. הגדרת מסגרת תקציב מומלצת.

ראוי לציין כי את ממצאי הערכת הסיכונים על הנהלת הארגון לאשר בכתב.

ג. אימות משתמשים

מומלץ לוודא כי כברירת מחדל תשתית ה-VPN תחייב השלמה מוצלחת של אימות המבוסס על MFA (Multi-Factor Authentication), וזאת לפני מתן גישה של המשתמש לסביבה הארגונית. דוגמה ליישום: סיסמה אישית בת 14 תווים לפחות + סיסמת OTP בת שישה תווים.

יש לוודא את קיומה של החלפת סיסמאות עתית, הן בתשתית ה-VPN, והן בתשתית הפנים הארגונית.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

סייבר ישראל
מערך הסייבר הלאומי

מכלול עמידות

בלמ"ס

8. נספחים (APPENDIXES)

פרק זה מכיל את רשימת הנספחים הנלווים למסמך זה.

נספח א' – טבלת מיפוי משתמשים וצרכים

נספח זה מהווה עזר למיפוי משתמשים וצרכים.

מס'	שם פרטי + שם משפחה	תפקיד	ימים שעות פעילות מותרים	האם מותר/אסור למשתמש להתחבר מכתובת IP שאינה של ISP ישראלי	נכס הסייבר ממנו (מקור) המשתמש יתחבר לסביבה הארגונית	נכס הסייבר אליו (יעד) המשתמש יתחבר בסביבה הארגונית	פרוטוקולים ושירותים מותרים
.1	ישראל ישראלי	מנהל מכירות	א-ה, 08:00 עד 20:00	הגישה מותרת מכתובות IP של ISP's ישראלים בלבד	לפטופ משרדי	שרת דוא"ל	SMTP – TCP Port 25 POP3 – TCP Port 110
.2							
.3							
.4							
.5							

טבלה 2: עזר למיפוי משתמשים וצרכים

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

ה. היגיינה טכנולוגית של נכס הסייבר (Technology Hygiene)[3]

היגיינה טכנולוגית של נכס הסייבר (Technology Hygiene) מהווה שם מאגד לסט בדיקות אבטחה אשר מטרתן להגביר את ודאות הארגון כי ניתן לתת אמון ביעד ההגנה (Trustworthy).

להלן מספר דוגמאות לבדיקות מקובלות אשר ניתן להחילן במסגרת בדיקת רמת ההיגיינה הטכנולוגית של נכס הסייבר:

1. גרסת מערכת ההפעלה הינה עדכנית;
2. גרסת ה-VPN Client הינה עדכנית;
3. עדכוני האבטחה (פאצ'ים) האחרונים הותקנו בהצלחה;
4. אמצעי האבטחה, דוגמת תוכנת אנטי-וירוס, פועלים ועדכניים;
5. גרסת רכיבי התוכנה עדכנית, דוגמת דפדפן (Browser);
6. רשימת רכיבי התוכנה הינה בהתאם למדיניות הארגון (Application Whitelist);
7. וידוא כי כל תעבורת נכס הסייבר (Non-Split-Tunnel) עוברת דרך בקרת גישה מנוהלת (VPN);
8. האנטי-וירוס עושה שימוש בחתימות מזהים עדכניות ל-24 שעות האחרונות;
9. סריקת אנטי-וירוס בוצעה ב-24 שעות האחרונות, ולא דווח על קיומה של נוזקה (Malware);
10. העדר ממצאים/אינדיקטורים (Indicators) המעידים על תוספות לא מורשות בדפדפן;
11. מניעת גישה מכתובת IP בעלת רמת אמון נמוכה (Trust Level). דוגמה לכתובות IP בעלות רמת אמון נמוכה: כתובת IP אשר משויכת לתשתית גישה אנונימית (דוגמת Tor), כתובת IP אשר מודיעין איומים בסייבר גילה וזיהה שמתבצעים דרכה פעולות זדוניות (דוגמת שליחת Spam).

---

[3] חלק מהיצרנים משתמשים במונח חלופי – "בדיקת ציות" (Security Compliance)

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

פרסום רשות הגנת הפרטיות

https://www.gov.il/he/departments/publications/reports/corona_work

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.

24 מרץ, 2020

כ"ח אדר, תש"פ

<u>דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית</u>

מנהלים ועובדים יקרים,

אלו ימים מורכבים אשר עוברים על כולנו. הניסיון לבלום את התפשטות נגיף הקורונה, משפיע באופן משמעותי על ההתנהלות המקצועית ועל וחיי היומיום של כולנו.

ארגונים רבים במשק נקטו בצעדים מהירים וחריגים בכדי לבודד מחד את העובדים ומאידך לאפשר רציפות תפקודית, ופעלו במהירות על מנת לאפשר לעובדיהם עבודה מרוחקת לרבות ממחשבים ביתיים. במידה ופעולות אלו נעשו ללא ביצוע הערכת סיכונים מסודרת, יש בכך כדי להגדיל את הסיכוי להתרחשותו של אירוע אבטחת מידע.

על כן ולצד הצורך החיוני בהמשכיות הרצף התפקודי, יש להקפיד ולוודא כי גם במצבי קיצון ובמציאות דינמית ניתנת תשומת הלב הנדרשת לנושא ההגנה על פרטיות המידע ואבטחת המידע בעת טיפול במידע אישי של עובדים או של נושאי מידע בהם ארגונים אלה מטפלים במסגרת העבודה היומיומית.

ברצוננו להביא בפניכם- מנהלים ועובדים- מידע נוסף ולתת דגשים חשובים בהתנהלות הטכנולוגית של ארגונים ובהתנהלותו של כל אחד ואחת מכם מחוץ לכותלי הארגון.

<u>סט הנחיות למעסיק בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית</u>

המציאות החדשה אליה נקלע המשק הישראלי בדומה לעולם כולו, הכתיבה כי ארגונים רבים שינו את אופן התנהלותם ואפשרו עבודה מרחוק במכשירים זרים למערכת הארגונית, דבר שאפשר להם את המשך הרציפות התפקודית, חיסכון במשאבים ונגישות של העובדים, לעיתים במחיר של הגדלת הסיכונים לארגון ואתגר משמעותי להנהלתו.

במסגרת הסכנות הרבות שאתגר זה מציב בפני הארגון, נכללים לדוגמה- **גניבה או אבדן** של מחשב או מכשיר נייד המכיל חומר רגיש ואפשרות גישה לרשת הארגונית באמצעות אמצעי זיהוי הנשמרים עליו; **חוסר יכולת אכיפה של מדיניות אבטחה ארגונית**; גישה מרחוק דרך **מכשיר לא מאובטח** המהווה נקודת תורפה אבטחתית חמורה; **ניהול עובד שיצא לחל"ת, שחלה או שעזב** ושמכשירו האישי נשאר בידיו ובו מידע ארגוני רגיש ואפשרות גישה למשאבי הארגון ולמערכותיו;

מסמך זה מכיל ממצאי ביקורת האסורים בפרסום מכוח חוק. המפרסם תוכן מסמך זה, כולו או מקצתו, עובר עבירה שדינה – מאסר שנה.