

דוח מבקר המדינה | סייבר ומערכות מידע | התשפ"ג-2022



הרשות הממשלתית למים וביוב

**היבטים באסדרה
ובפיקוח בנוגע
לספקי המים
המקומיים בתחום
הגנת הסייבר**



היבטים באסדרה ובפיקוח בנוגע לספקי המים המקומיים בתחום הגנת הסייבר

רקע

מרחב הסייבר כולל מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן דיגיטלי, נתוני תעבורה ובקרה. תקיפת סייבר היא רצף הפעולות שמבצע יריב במרחב הסייבר. איומי הסייבר הולכים ומתעצמים עם צמיחתו של מרחב הסייבר, ועלולים להוביל לפגיעה הן בתוך המרחב והן בעולם הפיזי, כגון במתקני התפלה, בספקי מים ובתשתיות. לפי מסמכי רשות המים, בשנים האחרונות חלה החמרה באיומי הסייבר על מערכות המחשוב של משק המים והביוב בישראל. קיימת חשיבות רבה להגנת סייבר עבור כלל הגורמים במשק המים, ובכלל זאת הספקים הרבים.

נתוני מפתח

חלק	חלק	נמצא פער
מתאידי המים שנבדקו בידי רשות המים בשנת 2021 קיבלו ציון נמוך על מוכנותם למתקפות סייבר	מכלל ספקי המים שלדעת רשות המים יש לחברם, חוברו למק"ם משרד האנרגייה עד מאי 2022	בתקן כוח האדם ביחידה המגורית ברשות המים לעומת תקן המשרות על פי טיוטת התקן ליחידת המגורית שגיבש מס"ל

פעולות הביקורת

בחודשים יוני עד דצמבר 2021 בדק משרד מבקר המדינה כמה היבטים באסדרה ופיקוח בנוגע לספקי המים המקומיים בתחום הגנת הסייבר. הבדיקות נעשו ברשות המים ובמערך הסייבר הלאומי (מס"ל). בדיקות השלמה נעשו במשרד האנרגייה ובחברת מקורות.

הדוח שבנדון הומצא לראש הממשלה ביום 31.7.2022 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על



אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא הונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.

תמונת המצב העולה מן הביקורת



הגדרת גופי תשתיות מדינה קריטיות (תמ"ק) במשק המים - חברת מקורות היא גוף התמ"ק היחיד במשק המים, והיא מונחה ישירות על ידי מס"ל. יתר הגופים במשק המים מונחים בהנחיה מגזרית. סוגיית הגדרת גופי תשתית גדולים נוספים במשק המים טרם נבחנה ונידונה בוועדת ההיגוי הייעודית לכך.

אסדרה של כללי ביטחון מים - במועד סיום הביקורת, דצמבר 2021, מועצת רשות המים לא אסדרה בכללים בהתאם לסמכותה על פי סעיף 18א לחוק המים את חובת ספקי המים להפעיל מערך ניטור ובקרה ומערך הגנה מפני אירועי סייבר; את חובותיהם להגיש תוכנית לאבטחת מידע לאישור רשות המים; ואת חובתם לחבר את מערכות המחשב שלהם למרכז הקיברנטי. כמו כן לא אסדרה סמכות מנהל היחידה המגזרית ברשות המים לתת הנחיות לספקי המים, ולא אסדרה סמכותם של הספקים לפעול על פיהן. הצעת אסדרה כאמור נקבעה בטיטת כללי המים (אירוע פגיעה במים), התשפ"ב-2022, אשר נידונה במועצת הרשות בינואר 2022.

היחידה המגזרית ברשות המים - עד מועד סיום הביקורת, דצמבר 2021, מערך הסייבר לא קבע תקן של יחידה מגזרית ברשות המים. נמצא פער בתקן כוח האדם ביחידה המגזרית ברשות המים לעומת תקן המשרות על פי טיטת התקן ליחידת המגזרית שגיבש מס"ל. כמו כן עד מועד סיום הביקורת כל המשרות שאינן מתוקננות ביחידה המגזרית ברשות המים מאוישות על ידי עובדי מיקור חוץ.

בדיקות חדירה - נמצאו פערים בתחום זה.

חיבור ספקי המים למרכז הקיברנטי (מק"ם) של משרד האנרגיה - רק חלק מכלל ספקי המים שלדעת רשות המים יש לחברם, חוברו למק"ם משרד האנרגיה עד מאי 2022.



מוכנות להגנת סייבר בקרב תאגידי המים והביוב - בשנים האחרונות ועד מועד סיום הביקורת עשתה רשות המים ביקורות סייבר בחלק מכלל התאגידים. חלק מתאגידי המים שנבדקו בידי רשות המים בשנת 2021, קיבלו ציון נמוך על מוכנותם להגנת סייבר.



הקמת מק"ם - משרד האנרגיה הקים מק"ם המנטר את כלל תשתיות האנרגיה, מתכלל מידע המתקבל מהן ומשקף תמונת מצב בנושא הגנת סייבר על משק האנרגיה.



עיקרי המלצות הביקורת

- מומלץ כי מס"ל יבחן מפעם לפעם את הנתונים העדכניים של הגופים הגדולים והמרכזיים במשק המים והביוב, כדי לקבוע אילו מהם צריכים להידון בוועדת ההיגוי הייעודית לכך. 
- מומלץ שמועצת הרשות ורשות המים יפעלו לקידום של הליכי אסדרת חובת ספקי המים להפעיל מערך ניטור ובקרה ומערך הגנה מאירועי סייבר, להכין תוכניות לאבטחת מידע ולעגן בכללי ביטחון מים את סמכות רשות המים לתת לספקי המים הנחיות בתחום הסייבר. 
- מומלץ שמערך הסייבר ישלים את הליך קביעת תקן כוח אדם הנדרש ביחידה המגזרית לסייבר ברשות המים. 
- מומלץ שרשות המים תפעל לתיקון הפערים בתחום בדיקות החדירה. מומלץ שרשות המים תפעל לחיבורם של כל ספקי המים שנדרש לדעתה לחברם למק"ם. 



סיכום

בשנים האחרונות חלה החמרה באיומי הסייבר על מערכות המחשוב של משק המים והביוב בישראל. מומלץ שמועצת הרשות ורשות המים יפעלו לקידום של הליכי אסדרת חובת ספקי המים להפעיל מערך ניטור ובקרה ומערך הגנה מאירועי סייבר, להכין תוכניות לאבטחת מידע ולעגן בכללי ביטחון מים את סמכות רשות המים לתת לספקי המים הנחיות בתחום הסייבר. כמו כן מומלץ כי הרשות תפעל לחיבורם של כל ספקי המים הנדרשים למק"ם. עוד מומלץ כי רשות המים תשלים את ביקורות הסייבר בתאגידי ובספקי מים אחרים שטרם נבדקו בשנתיים האחרונות, ותפעל להגברת מוכנותם של התאגידיים למתקפות סייבר.



היבטים באסדרה ובפיקוח בנוגע לספקי המים המקומיים בתחום הגנת הסייבר

מבוא

מרחב הסייבר הוא המרחב הפיזי והקיברנטי הכולל מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן דיגיטלי, נתוני תעבורה ובקרה. תקיפת סייבר היא רצף הפעולות (חד-פעמי או מתמשך) שמבצע יריב במרחב הסייבר לתכלית קונקרטית כגון חבלה, איסוף מידע או השפעה תודעתית.

איומי הסייבר הולכים ומתעצמים בשנים האחרונות. איומים אלה עלולים להוביל הן לפגיעה בתוך מרחב הסייבר (במידע או בתפקוד) והן לפגיעה בעולם הפיזי, בין היתר במתקני התפלה, בספקי מים ובתשתיות מים.

בשנים 2019 - 2021 אירעו כמה מתקפות סייבר במתקני מים בארה"ב. לדוגמה, ב-19.3.27 עובד לשעבר של מפעל הטיפול במים בעיר Ellsworth, Kansas, נכנס מרחוק למערכות התפעול הממוחשבות של מפעל הטיפול במים בעיר וסגר את המערכות שתפקידן לחטא את המים המטופלים במפעל קודם לאספקתם לתושבים. במקרה זה לא נגרם כל נזק לצרכני המים. ב-15.1.21 נעשה ניסיון פריצה למערכות התפעול של מפעל לטיפול במי שתייה במפרץ סן פרנסיסקו. במהלך הפריצה נעשה ניסיון לפגוע במי השתייה באמצעות מחיקת תוכנות המשמשות בתהליך הטיפול במים. הפריצה התגלתה ביום המחרת, אך לא נגרם נזק בפועל. ב-5.2.21 נפרצו מערכות התפעול הממוחשבות של מפעל הטיפול במים של העיר Oldsmar, Florida. בפריצה נעשה ניסיון להעלות את ריכוז החומר המוסף למים לשם טיפול בהם (סודיום הידרוקסיד) לרמה של פי 100 מהתקן. שתיית מים עם ריכוז כה גבוה של חומר זה עלולה לגרום נזקים חמורים לשותים אותם. מפעיל המתקן הבחין בניסיון להעלות את ריכוז החומר והצליח למנוע אותו.

תקיפת מערכות מים עלולה להתבצע לצורך גרימת נזק; פגיעה ברציפות התפקודית ובאספקת המים; השבתה או הדלפה של מידע מסווג או פגיעה בתהליכים עסקיים. היריב במקרה זה יכול להגיע ממגוון רב של גורמים - מדינתיים; טרור; גורם מסחרי מתחרה; גורמים פוליטיים ואחרים.

תקיפה כאמור עלולה לגרום, בין השאר, לפגיעה ישירה בתשתיות, לפגיעה במערכות מחשוב, שהן הכרחיות לתפקוד התקין של תשתיות המים והביוב, להרעלת מקורות מים או מאגרי מים ולאיומים נוספים על איכות המים.

מסמכי רשות המים עולה שבשנים האחרונות חלה החמרה באיומי הסייבר על מערכות המחשוב של משק המים והביוב בישראל, וכי בשנים 2020 ו-2021 נרשמו אירועים של תקיפת תשתיות מחשוב.

במרץ 2021 הציגה רשות המים את ממצאי סקירתה בנושא היערכות משק המים בתחומי ביטחון מים חירום וסייבר לפני מועצת המים. מהסקירה שהוצגה עולה בין היתר כי משק המים מבוזר מאוד וכי יש פער באסדרה למגזר הכפרי המתבטא בקושי בהטמעת הנהלים ובעריכת הבקרה במגזר.



פעולות הביקורת

בחודשים יוני עד דצמבר 2021 בדק משרד מבקר המדינה כמה היבטים באסדרה ופיקוח בנוגע לספקי המים המקומיים בתחום הגנת הסייבר. הבדיקות נעשו ברשות המים ובמערך הסייבר הלאומי (להלן - מס"ל). בדיקות השלמה נעשו במשרד האנרגיה ובחברת מקורות.

הדוח שבנדון הומצא לראש הממשלה ביום 31.7.2022 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא הונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.

הקמת יחידה מגזרית במשרד האנרגיה להגנת סייבר

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), מסמך, בין היתר, את מערך הסייבר הלאומי (להלן - מס"ל)¹ להנחות מהבחינה המקצועית גופים ציבוריים מסוימים², המוגדרים כגופי תשתיות מדינה קריטיות (להלן - תמ"ק) בתחום אבטחת מערכות מידע ממוחשבות חיוניות.

מס"ל משמש גוף מטה במשרד ראש הממשלה, ובין היתר ממליץ על מדיניות לאומית ומקדם את יישומה בתחום הסייבר. מס"ל מנהל, מפעיל ומבצע, בהתאם לצורך, את כלל מאמצי ההגנה האופרטיביים במישור הלאומי במרחב הסייבר, ובכלל זה מטפל באיומי סייבר ובאירועי סייבר בזמן אמת, מגבש תמונת מצב שוטפת ומרכז מחקר מודיעין³.

לגבי אותם גופים שאינם מוגדרים כגופי תמ"ק, תפיסת האסדרה בתחום הגנת הסייבר שנקבעה בהחלטת ממשלה מפברואר 2015⁴ הייתה שלא להוסיף למשק עוד רגולטורים, אלא להעצים

1 המס"ל פועל בין היתר גם מתוקף החלטות הממשלה הבאות: החלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי (7.8.11); החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת סייבר" (15.2.15); החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15); החלטת הממשלה 3270, "איחוד יחידות מערך הסייבר הלאומי" 17.2.17.

2 "גוף ציבורי" הוגדר בחוק להסדרת הביטחון כלהלן: "כל גוף המנוי בתוספות, ולגבי משרד ממשלתי המנוי בתוספות - לרבות יחידות הסמך שלו".

3 סעיף 18(א) לחוק הסדרת הביטחון.

4 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15) (להלן - החלטת הממשלה מפברואר 2015).



את הרגולטורים הקיימים באמצעות מגוון הכלים העומדים לרשותם וחיזוק כלים אלה ככל הנדרש לתחום הסייבר, על מנת להעלות את רמת החוסן של המגזר האזרחי לאיומי סייבר.

לפיכך, בהתאם להחלטת הממשלה מפברואר 2015 המנכ"לים של משרדי הממשלה שבמסגרתם מופעלות סמכויות רגולציה כלפי גופים או פעילויות החשופים לאיומי סייבר יידרשו להקים יחידה להכוונה מקצועית בתחום הגנת הסייבר "בהתאם לסמכויות הרגולציה המופעלות על ידי המשרד הממשלתי או במסגרתו" (להלן - יחידה מגזרית); היחידה המגזרית תפעל בכפיפות למשרד הממשלתי שאליו היא שייכת ובהנחיה מקצועית של הרשות הלאומית להגנת הסייבר⁵.

בין תפקידי היחידה המגזרית, בהתאם להחלטת הממשלה מפברואר 2015: הכוונה והנחיה בהיבטי הגנת הסייבר, לרבות הגדרת המדיניות ודרישות האסדרה בתחום הסייבר; ליווי מקצועי שוטף ומענה על פניות מקצועיות, בהתאם למאפיינים של הגופים אשר ביחס אליהם מתבצעת הפעילות (להלן - המגזר); בקרת ביצוע הדרישות המקצועיות בהתאם לאסדרה וברמה המקצועית הנדרשת; פיתוח והפעלה של תהליכי שיתוף מידע פנימיים וחינוכיים בתוך המגזר, לרבות דיווח על אירועים, איומים, חולשות, פוגענים ונזקות למרכז לסיוע בהתמודדות עם איומי סייבר, וכן הגדרת נוהלי הדיווח ושיטות הדיווח בין הגופים במגזר; יזום ומימוש של פעילות חובתית, לרבות הקמת תשתיות והפעלת מנגנונים שתכליתם שיפור הגנת הסייבר במגזר.

כמו כן, בהחלטת הממשלה נקבע כי המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך יידרשו לפעול להעלאת רמת הגנת הסייבר ולשם כך - למנות ממונה על הגנת הסייבר, להקים ועדת היגוי משרדית, להסדיר את אנשי המקצוע בתחום הגנת הסייבר המועסקים במשרד, להקצות תקציב ייעודי להגנת הסייבר במסגרת התקציב הקיים של המשרד ולקדם עמידה של המשרד בתקני אבטחת מידע.

משרד האנרגייה הקים אגף חירום, ביטחון מידע וסייבר אשר, בין היתר, אחראי להיערכות המשרד לאיומי סייבר ואבטחת מידע מסווג. נוסף על כך הוקם במשרד האנרגייה מרכז קיברנטי מגזרי (להלן - מק"ם) לניטור של מתקני תשתית המק"ם פועל מספטמבר 2016, ובמועד סיום הביקורת היו מחוברים אליו מתקנים ממגזרי תשתיות האנרגייה.

משרד מבקר המדינה רואה בחיוב את העובדה כי משרד האנרגייה הקים את המק"ם, המנטר את תשתיות האנרגייה, מתכלל מידע המתקבל מהן ומשקף תמונת מצב בנושא הגנת הסייבר של משק האנרגייה.

היחידה המגזרית ברשות המים פועלת באגף ביטחון מים, חירום, מידע וסייבר ברשות המים, והיא נושאת באחריות להכוונה ולבקרה בעניין תחום האבטחה והביטחון של כל ספקי המים אשר בתחום האחריות הרגולטיבית של רשות המים, ובכלל זה בעניין אבטחת מידע ותשתיות ממוחשבות החיוניות לרציפות התפקודית של המשק⁶.

על פי חוק להסדרת הביטחון הגדרת גוף תשתית כגוף תמ"ק מתבצעת מטעמים של ביטחון המדינה, שלום הציבור וביטחון, וכרוכה באישור השר לביטחון הפנים, בהתייעצות עם השר

5 בתקופת הביקורת - המס"ל.

6 רשות המים, נוהל אבטחת מחשב בספקי מים (2016).



הממונה על הגוף הציבורי (או עם שר הממונה על ביצוע חוק המסדיר את פעולותיו של גוף ציבורי, לפי העניין); באישור ועדת ביטחון הפנים של הכנסת; ובאישור ראש הממשלה.⁷

חברת מקורות היא גוף התמ"ק היחיד במשק המים המונחה ישירות על ידי מס"ל מכוח החוק להסדרת הביטחון.

יוצא מכך כי חברת מקורות היא הגוף היחיד במשק המים המוגדר כגוף תמ"ק, אשר מס"ל מנחה אותו ומפקח עליו ישירות. יתר הגופים במשק המים מונחים בהנחיה מגזרית. נמצא כי סוגיית הגדרת גופי תשתית נוספים במשק המים, כגופי תמ"ק, טרם נבחנה ונידונה בוועדת ההיגוי הייעודית לכך (להלן - הוועדה).

מס"ל מסר למשרד מבקר המדינה בדצמבר 2021 כי יש תבחינים (קריטריונים) שלפיהם נבחנת מידת התאמתם של גופים להיכלל בהגדרת גופי תמ"ק, וכי תבחינים אלו נידונים בוועדה. עוד מסר מס"ל כי טרם נבחן הצורך לקבוע מתקנים נוספים במשק המים והביוב כגופי תמ"ק.

משרד מבקר המדינה ממליץ למס"ל לבחון מפעם לפעם את הנתונים העדכניים של הגופים הגדולים והמרכזיים במשק המים והביוב, כדי לקבוע אילו מהם יובאו על ידו לדין בוועדת ההיגוי הייעודית לכך.

אסדרה של כללי ביטחון המים

במועד סיום הביקורת, דצמבר 2021, מועצת רשות המים לא אסדרה בכללים בהתאם לסמכותה על פי סעיף 18א לחוק המים את חובת ספקי המים להפעיל מערך ניטור ובקרה ומערך הגנה מפני אירועי סייבר, את חובותיהם להגיש תוכנית לאבטחת מידע לאישור רשות המים, ואת חובתם לחבר את מערכות המחשב שלהם למק"ם. כמו כן לא אסדרה סמכות מנהל היחידה המגזרית ברשות המים לתת הנחיות לספקי המים, ולא אסדרה סמכותם של הספקים לפעול על פיהן.

נמצא כי הצעת אסדרה כאמור נקבעה בטיטת כללי המים (אירוע פגיעה במים), התשפ"ב-2022, אשר נידונה במועצת הרשות בינואר 2022 (להלן - כללי ביטחון מים).

מומלץ שמועצת הרשות ורשות המים יפעלו לקידום של הליכי אסדרת חובת ספקי המים להפעיל מערך ניטור ובקרה ומערך הגנה מאירועי סייבר, להכין תוכניות לאבטחת מידע ולעגן בכללי ביטחון מים את סמכות רשות המים לתת לספקי המים הנחיות בתחום הסייבר.

7 סעיף 18(א) לחוק הסדרת הביטחון.



רשות המים השיבה למשרד מבקר המדינה במאי 2022 כי הליך השימוע של כללי ביטחון מים שפורסמו בינואר 2022 הסתיים במרץ 2022, וכי לאחר השלמת השיח עם הגורמים הרלוונטיים בנוגע לסוגיות שעלו, יובאו הכללים לאישור מועצת הרשות.

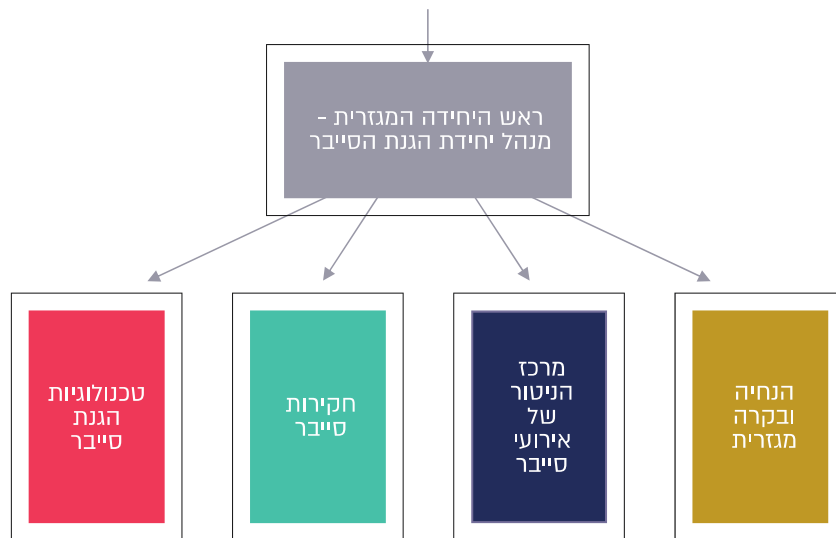
היחידה המגזרית ברשות המים

בהתאם להחלטת הממשלה מפברואר 2015, מס"ל יסווג את היקף הפעילות הנדרשת של היחידה המגזרית בתחום הגנת הסייבר, זאת בהתאם לנזק הפוטנציאלי מפגיעה במערכות הממוחשבות של הגופים במגזר, ובהתאם להיקף הפעילות של היחידה המגזרית.

עוד צוין בהחלטת הממשלה מפברואר 2015 כי המשרדים יאיישו את התפקידים ביחידה המגזרית בהתאם למפתחות המפורטים להלן: גוף בעל היקף פעילות גדול יאייש את תפקידיהם של מנהל וארבעה אנשי צוות; גוף בעל היקף פעילות בינוני יאייש את תפקידיהם של מנהל ושני אנשי צוות; וגוף בעל היקף פעילות קטן יאייש את תפקידו של מנהל בלבד. התפקידים יאוישו באמצעות תקני כוח אדם ועובדים ממוקד חוץ למשרדי הממשלה.

נמצא כי בדצמבר 2021 מס"ל טרם קבע את היקף היחידה המגזרית ברשות המים, אך הוא גיבש טיוטה בנושא.

תרשים 1: מבנה מומלץ על ידי מס"ל ביחידה המגזרית ברשות המים



במועד סיום הביקורת, דצמבר 2021, מערך הסייבר לא קבע תקן של יחידה מגזרית ברשות המים, ובפועל היחידה המגזרית פועלת בעיקר באמצעות מיקור חוץ. מומלץ שמערך הסייבר ישלים את הליך קביעת תקן כוח אדם הנדרש ביחידת המגזרית לסייבר ברשות המים.



עוד מומלץ שרשות המים תפעל לתקנון כוח האדם הנדרש ביחידה המגזרית, בהתאם להנחיית המס"ל, וכן תפעל לאיושו.

בדיקות חדירה

בדיקת חדירה (Penetration test, מכונה בקיצור גם Pentest) היא מתקפה מתוכננת ומבוקרת על מערכת ממוחשבת. את הבדיקה מבצע בודק ("האקר", pen-tester) כדי לאתר חולשות אבטחה, את פוטנציאל הגישה לחולשות אלו, השימושיות שניתן להפיק מהגישה אליהן ואל המידע שהן מאחסנות. בדיקת חדירה מאפשרת בדיקת היתכנות של מתקפות סייבר על התאגיד, זיהוי חולשות והערכת היקף הנזק העסקי והתפעולי שעלול להיגרם על ידי מתקפות סייבר ובדיקה של יכולות מערך ההגנה של המערכת המיועדת לתקיפה מבחינת זיהוי מתקפות ואופן הטיפול בהן.

לביצוע בדיקות חדירה יש חשיבות רבה⁸ בנוגע לבחינה של מימוש הבקורות בפועל ושל אפקטיביות ההגנה.

בביקורת נמצאו פערים בתחום זה.

להקמת סביבת בדיקות להיבטי סייבר נודעת חשיבות רבה, בין היתר כדי לאפשר בחינה מוגנת של תוכנות חדשות, עידכוני אבטחה וגרסאות תוכנה לתוכנות קיימות קודם העלאתן ל"סביבת הייצור".

מוצע כי רשות המים תבחן העלאת עדכוני תוכנה ועדכוני אבטחה הרלוונטיים לכלל תאגידי המים והביוב, לסביבה שונה מ"סביבת הייצור וההפעלה", אם על ידי שימוש בשרת צדדי ואם על ידי הקמת סביבת בדיקות מלאה.

מומלץ כי מס"ל ינחה את רשות המים בעניין הכנת תוכנית עבודה רב-שנתית לביצוע בדיקות חדירה, וכי הוא יפקח על התקדמות יישומה.

רשות המים השיבה כי היא תבחן, בשיתוף עם מערך הסייבר, אפשרויות פעולה נוספות לשם בדיקת מערכות המופעלות במתקני מים וביוב.

מרכז קיברנטי מגזרי במשרד האנרגיה

מתקני ספקי המים שתגדיר רשות המים מיועדים להתחבר למק"ם משרד האנרגיה, שמנטר אותם. נמצא כי רק חלק מכלל ספקי המים שלדעת רשות המים יש לחברם, חוברו למק"ם משרד האנרגיה עד מאי 2022.

8 מערך הסייבר הלאומי "תורת ההגנה בסייבר לארגון" אפריל 2018.



רשות המים השיבה למשרד מבקר המדינה כי נכון למאי 2022 חוברו כמה ספקים למק"ם, וכמה ספקים נוספים "נמצאים בתהליך טיוב לקראת חיבורם למק"ם".

מומלץ שרשות המים תפעל לחיבור כל ספקי המים שלדעתה נדרש לחברם.

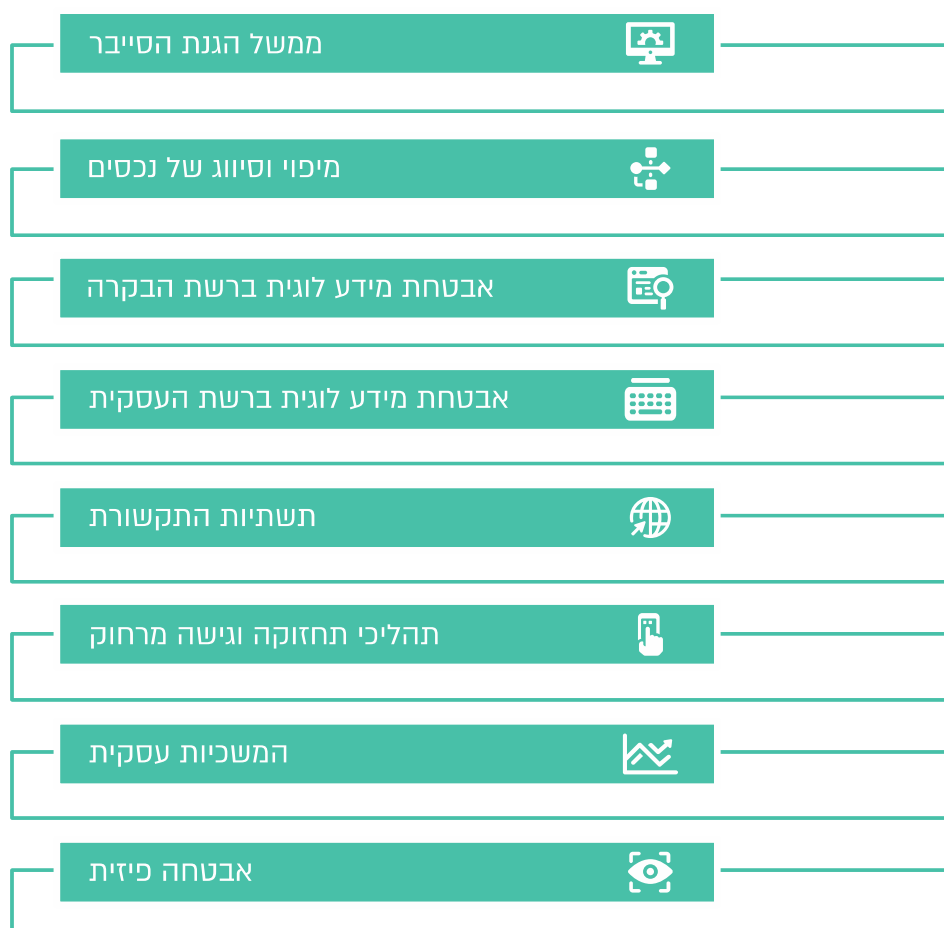
ביקורות מוכנות למתקפות סייבר בתאגידי המים

רשות המים עושה מפעם לפעם ביקורת סייבר בתאגידיים. נמצא כי בשנים האחרונות בוצעו ביקורות סייבר בחלק מכלל התאגידיים.

הביקורות בחודשים נובמבר 2020 - דצמבר 2021 נעשו באמצעות יועץ חיצוני לרשות המים, וכללו, בין היתר, מתן ציון למידת הציות של תאגיד המים לנוהל רשות המים בנושא עקרונות האבטחה וההגנה על מערכות מחשוב עבור ספקי מים. פירוט הממצאים שהועלו הועברו למס"ל ולרשות המים.



תרשים 3: הנושאים שנבחנו במסגרת בדיקת הציות של תאגידי המים לנוהל רשות המים בנושא אבטחה והגנה על מערכות מחשוב



על פי נתוני רשות המים, בעיבוד משרד מבקר המדינה

משרד מבקר המדינה רואה בחיוב את פעולות רשות המים בשנת 2021 בנושא הבקרה על מוכנות תאגידי המים בתחום הסייבר. עם זאת, עלה כי חלק מתאגידי המים שנבדקו בידי רשות המים בשנת 2021, קיבלו ציון נמוך על מוכנותם למתקפות סייבר. נוכח החשיבות של תגובה מהירה באירועי סייבר, מומלץ כי רשות המים תשלים את ביקורות הסייבר בתאגידיים ובספקי מים אחרים שטרם נבדקו בשנתיים האחרונות, וזאת כדי להביא לשיפור מוכנות ספקי המים למתקפות סייבר.



כמו כן, מומלץ שרשות המים תפעל להגברת המוכנות למתקפות סייבר וכי היא תתמקד בתאגידים שקיבלו ציונים נמוכים. על רשות המים לשים דגש על התאגידים שקיבלו ציונים נמוכים לצורך קיום הדרישות למוכנות להתקפות סייבר כנדרש, וכדי למנוע נזקים אפשריים לתושבים שאותם הם משרתים.



סיכום

בשנים האחרונות חלה החמרה באיומי הסייבר על מערכות המחשוב של משק המים והביוב בישראל. קיימת חשיבות רבה להגנת סייבר עבור כלל הגורמים במשק המים, ובכלל זאת הספקים הרבים.

מומלץ שמועצת הרשות ורשות המים יפעלו לקידום מהיר של הליכי אסדרת חובת ספקי המים להפעיל מערך ניטור ובקרה ומערך הגנה מאירועי סייבר, להכין תוכניות לאבטחת מידע ולעגן בכללי ביטחון מים את סמכות רשות המים לתת לספקי המים הנחיות בתחום הסייבר. כמו כן מומלץ שהרשות תפעל לחיבורם של כל ספקי המים הנדרשים למק"ם.

עוד מומלץ כי רשות המים תשלים את ביקורות הסייבר בתאגידי המים והביוב ובספקי מים אחרים שטרם נבדקו בשנים האחרונות, תפעל להגברת מוכנותם של תאגידי המים והביוב למתקפות סייבר ותתמקד בתאגידי המים והביוב שקיבלו ציונים נמוכים בביקורת שלה.

כמו כן, מומלץ שרשות המים תפעל לתיקון הפערים בתחום בדיקות החדירה.

מומלץ שמש"ל יבחן מפעם לפעם את הנתונים העדכניים של הגופים הגדולים והמרכזיים במשק המים והביוב, כדי לקבוע אילו מהם צריכים להידון בהליכים להגדרה כגופי תמ"ק, ובהתאם, יפעל לקידום הליכים אלה.