אבטחה פיזית ושרידות של תשתיות אינטרנט ומחשוב עבור משרדי ממשלה

פעולות הביקורת

במערך ממשל זמין, הכפוף למטה התקשוב הממשלתי שבמשרד האוצר, נעשתה ביקורת על כמה היבטים של האבטחה הפיזית של תשתיות אינטרנט ומחשוב עבור משרדי הממשלה ועל שרידותן של התשתיות. נבדקו בעיקר האבטחה הפיזית וההיערכות לסיכונים ביטחוניים, סיכוני אש וסיכוני מים. הבדיקה היא בדיקת השלמה לביקורת שעשה משרד מבקר המדינה בנושא וממצאיה פורסמו בדוח מבקר המדינה 63ב בשנת 2013.

תקציר

אבטחה פיזית הינה "מכלול השיטות, אמצעי הגנה פיזיים ונהלים, שמטרתם למדר את מערכות המידע ולהגן פיזית על אזור מוגדר כדי לאפשר גישה לאזור זה או למנוע אותה, לפי הצורך, וכן להגן על הנכסים הנמצאים בו מפני השמדה, השחתה או גניבה"[1].

בשנת 1997 החל אגף החשב הכללי במשרד האוצר בפרויקט להסדרת תשתית האינטרנט למשרדי הממשלה (להלן - תהיל"ה)[2], ובשנת 1999 החל בביצוע תת-פרויקטים במסגרת מה שכונה לאחר מכן "פרויקט ממשל זמין"[3]. במאי 2002 החליטה הממשלה[4] לבסס את מימוש "פרויקט ממשל זמין" מול הציבור באמצעות פרויקט תהיל"ה, שייעל את זרימת המידע בין הממשלה לציבור ולהיפך, על ידי יצירת מנגנון מאובטח ברשת האינטרנט, המקשר בין "מערכת רוחבית כוללת במשרדי הממשלה" (להלן - פרויקט מרכב"ה)[5] ומערכות מידע ממשלתיות לבין הציבור (להלן - ממשל זמין או תהיל"ה). באוקטובר 2006 אוכלס בניין על ידי ממשל זמין, מקום מושבו עד היום (להלן - האתר הראשי).

---

1 מתוך תקן ישראלי 1495 חלק 5, "אבטחת מערכות מידע ממוחשבות - היערכות למצב אסון".

2 פרויקט שמטרתו חיבור משרדי הממשלה לאינטרנט, ויצירת תשתית מאובטחת לאחסון ולניהול של אתרי אינטרנט ממשלתיים ולמתן שירותים נלווים.

3 לסקירה על פעולות הממשלה בנושא בשנים 1997-2002: ראו **מבקר המדינה, דוח שנתי 53ב** (2003), השימוש בטכנולוגיית התקשוב למתן שירותים ממשלתיים לציבור, עמ' 202-210.

4 החלטה מס' 1812 מיום 12.5.02.

5 פרויקט שיזם אגף החשב הכללי במשרד האוצר בשנת 2000 להקמה ולהטמעה של מערכת מחשוב אחידה במשרדי הממשלה, לניהול המשאבים בתחומים האלה: כספים, כוח אדם, רכש (לוגיסטיקה) ונכסים ולביצוע פעולות נוספות, כגון פניות לקבלת תמיכות ולהקצאתן.

ממשל זמין סיפק בשנת 2012 למשרדי הממשלה ולגופים ציבוריים וכן לכ-50,000 ממשתמשיהם את השירותים האלה: תשתית למתן שירותי רשת מאובטחים, שירותי גלישה מאובטחת באינטרנט, דואר אלקטרוני, אירוח אתרים - תשתית מחשבים (חוות שרתים) לאחסון של דפי אינטרנט ועוד. כמן כן, ממשל זמין מנהל את פרויקט כרטיס חכם[6], את מנור"ה (מערכת ניהול ותיעוד הרכש הממשלתי), את שירות הטפסים הלאומי ועוד. בממשל זמין מועסקים כ-250 עובדים במקומות שונים באמצעות חברות כוח אדם ובתי תכנה.

פעולות הביקורת

בחודשים אפריל ומאי 2013 בדק משרד מבקר המדינה כמה היבטים של אבטחה פיזית ושרידות מערכות של תשתיות אינטרנט ומחשוב בתהי"ה. הבדיקה נערכה כבדיקת השלמה לביקורת שערך משרד מבקר המדינה בנושא ניהול אבטחת מידע ושרידות תשתיות אינטרנט ומחשוב עבור משרדי ממשלה[7]. נבדקו בעיקר האבטחה הפיזית וההיערכות לסיכונים ביטחוניים, סיכוני אש וסיכוני מים. הביקורת נערכה באתר הראשי של ממשל זמין שבמשרד האוצר ובאתר החלופי (DRP)[8] של ממשל זמין בטירת הכרמל.

עיקרי הממצאים

1. קיים עיכוב משמעותי ביישום נוהלי תורה ומתודולוגיה רוחבית (תמ"ר) בממשל זמין; בביקורות שעשתה הרשות הממלכתית לאבטחת מידע של שירות הביטחון הכללי (להלן - רא"ם) בתהי"ה הושגו "ציונים נמוכים מהמצופה".

2. הליקויים שעלו בתרגילים שעשתה רא"ם מצביעים על חולשות ממשיות בתחום האבטחה. חמורה בעיקר העובדה, כי ליקויים משמעותיים שהועלו בתרגיל הראשון שבו ועלו בתרגיל השני, למרות שעל חלקם הוער כבר בעבר בביקורות קודמות שערכה רא"ם בנושא.

3. ממצאי סקר מערכות ותחזוקה לחדר השרתים של ממשל זמין שנערך ביולי 2012 (להלן - סקר המערכות), לא נדונו בוועדת ההיגוי לאבטחת מידע. עד מועד סיום הביקורת, מאי 2013, לא תוקנו הליקויים שהועלו בסקר בנושא מערכות האל-פסק[9].

4. בחדר השרתים (להלן - חדר השרתים או חדר המחשב) של ממשל זמין קיימים פערים מול המלצות התקן הישראלי 1243. בין היתר, קיימים שני פערים יסודיים:

---

6 פרויקט שנועד לספק תשתית לחתימה אלקטרונית ולזיהוי.

7 מבקר המדינה, **דוח שנתי 63ב** (2013), ניהול אבטחת מידע ושרידות תשתיות אינטרנט ומחשוב עבור משרדי ממשלה, עמ' 277.

8 Disaster Recovery Planning - אוסף נהלים והנחיות המגדירים תהליכים חיוניים לארגון, פעולות הנחוצות להמשך מתן שירותים חיוניים, לוחות זמנים, מערך חלופי, הסכמי שירות וניסוי מערך התאוששות (לתרגול ולווידוא מוכנות הארגון למצב אסון).

9 מערכות שנועדו להגן ולגבות מחשבים ושרתים מפני הפרעות בהספקת רשת החשמל, ומקפיצות ותנודות בלתי רצויות במתח החשמל, העלולות לגרום נזק בעת התרחשותן.

האחד, לחדר המחשב של ממשל זמין ארבעה חלונות חיצוניים, והשני, אחד מקירות חדר המחשב עשוי מזכוכית, ואין בו דלת אש כנדרש בתקן.

5. חדר המחשב של ממשל זמין הוקם במבנה שאינו מבנה ייעודי עמיד אש.

6. כל מערכות המחשב הנמצאות בחדר המחשב מקוררות על ידי מערכת קירור מבוססת מים (צ'ילר), הפרושה בצינורות על קירות חדר המחשב, בתוך ארונות השרתים ועל רצפת החדר. רצפת החדר אינה מנוקזת כמומלץ בתקן 1243, זאת למרות כל הסיכונים הקיימים ממים.

7. מערכת מיזוג האוויר באתר הראשי של ממשל זמין אינה מושבתת באופן אוטומטי במקרה של תקלה (כדי שלא תדלל את חומר הכיבוי). כמו כן, ובניגוד להמלצות תקן 1243, באתר החלופי של ממשל זמין נמצאו קרטונים, שידות ושולחנות העשויים מעץ.

8. לא הוכנו כל הנהלים, הנדרשים להבטחת תקינות הפעילות של ממשל זמין, כגון נוהל בנושא "הגנה מפני איומים חיצוניים וסביבתיים", המציע דרכים להגנה פיזית מפני נזקים של שרפה, הפצצה, רעידת אדמה, פיצוצים וסוגים אחרים של אסונות.

9. בכניסה לחדר המחשב לא קיימת רשימת מורשים, וחדר המחשב אינו מסומן כחדר ממודר. כמו כן, אורחים או גורמים זרים, הנדרשים בתוקף תפקידם לשהות בחדר המחשב, אינם מלווים על ידי גורם מורשה. עוד נמצא, כי בדלתות הכניסה למתחם ממשל זמין אין התראת דלת פתוחה.

10. מחלקת מערכות מידע אינה עורכת מעקב אחר ציוד מחשוב הנמצא מחוץ למתחם ממשל זמין לצורך תחזוקה; מצעי מידע[10], שלא ניתן לנתקם מהציוד, מוצאים מהמתחם ללא אישור מנהל אבטחת מידע וללא קביעה של סדרי שמירתם. כמו כן אין מתעדים השמדת מצעי מידע פגומים.

סיכום והמלצות

האבטחה הפיזית של מבנה ממשל זמין ושל מערכות תשתית האינטרנט והמחשוב של ממשל זמין אינה עולה בקנה אחד עם הדרישות, התקנים וההנחיות לפעילות ממשל זמין בכלל ולחדר המחשב בפרט. ליקויים אלו מצביעים על כך שההיערכות למניעת אירוע של אבטחה פיזית חסרה; וכן על סיכון לפגיעה בפעילות השוטפת של ממשל זמין במקרה שתתרחש פגיעה במבנה ממשל זמין או באחת המערכות הקריטיות שבו, וכן לפגיעה בזמינות המידע הממשלתי לציבור ולניתוק משרדי הממשלה מרשת האינטרנט.

נוכח זאת, על הממונה על התקשוב הממשלתי לפעול לכך שממשל זמין, המספק בין השאר את שער היציאה של משרדי הממשלה לרשת האינטרנט, יעמוד, כאתר המחשוב המרכזי של הממשלה, בתקנים הנדרשים ובהנחיות הגופים המנחים אותו.

---

10 רכיב במערכת מחשוב בו מאוחסן מידע דיגיטלי, כגון כונן קשיח.

עד למציאת פתרון העומד בסטנדרדים הנדרשים לאתר ממשל זמין, מן הראוי כי ממשל זמין יתקן את כל הליקויים שהועלו בביקורות שנערכו בנושא האבטחה הפיזית נוכח הסיכונים הגלומים בהם לפעילותו השוטפת.

כמו כן על ממשל זמין ליישם את הוראות הנהלים שהוא עצמו קבע בנושא אבטחה פיזית, ומעל לכל, יש לפעול לאלתר למזעור הסכנות הנשקפות לחיי אדם באתר הראשי, ובראשם עובדי ממשל זמין, כפי שפורטו בדוח.

♦

מבוא

1. אבטחה פיזית של מערכות מידע הינה "מכלול השיטות, אמצעי הגנה פיזיים ונהלים, שמטרתם למדר את מערכות המידע ולהגן פיזית על אזור מוגדר כדי לאפשר גישה לאזור זה או למנוע אותה, לפי הצורך, וכן להגן על הנכסים הנמצאים בו מפני השמדה, השחתה או גניבה"[11]. אבטחת מידע מוגדרת בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), כ"הגנה על שלמות המידע"[12], או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין".

בשנת 1997 החל אגף החשב הכללי במשרד האוצר בפרויקט להסדרת תשתית האינטרנט למשרדי הממשלה (להלן - תהיל"ה)[13], ובשנת 1999 החל בביצוע תת-פרויקטים במסגרת מה שכונה לאחר מכן "פרויקט ממשל זמין"[14]. במאי 2002 החליטה הממשלה[15] לבסס את מימוש "פרויקט ממשל זמין" מול הציבור באמצעות פרויקט תהיל"ה, שייעל את זרימת המידע בין הממשלה לציבור ולהיפך, על ידי יצירת מנגנון מאובטח ברשת האינטרנט, המקשר בין "מערכת רוחבית כוללת במשרדי הממשלה" (להלן - פרויקט מרכב"ה)[16] ומערכות מידע ממשלתיות לבין הציבור (להלן - ממשל זמין או תהיל"ה).

ממשל זמין סיפק בשנת 2012 למשרדי הממשלה ולגופים ציבוריים וכן לכ-50,000 ממשתמשיהם את השירותים האלה: תשתית למתן שירותי רשת מאובטחים, שירותי גלישה מאובטחת באינטרנט, דואר אלקטרוני, אירוח אתרים - תשתית מחשבים (חוות שרתים) לאחסון של דפי אינטרנט ועוד. כמן כן, ממשל זמין מנהל את פרויקט כרטיס חכם[17], את מנור"ה (מערכת ניהול ותיעוד הרכש הממשלתי), את שירות הטפסים הלאומי ועוד. בממשל זמין מועסקים כ-250 עובדים במקומות שונים באמצעות חברות כוח אדם ובתי תכנה.

---

11 מתוך תקן ישראלי 1495 חלק 5, "אבטחת מערכות מידע ממוחשבות - היערכות למצב אסון".

12 "מידע" מוגדר בחוק הגנת הפרטיות כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו".

13 פרויקט שמטרתו חיבור משרדי הממשלה לאינטרנט, ויצירת תשתית מאובטחת לאחסון ולניהול של אתרי אינטרנט ממשלתיים ולמתן שירותים נלווים.

14 לסקירה על פעולות הממשלה בנושא בשנים 1997-2002: ראו מבקר המדינה, **דוח שנתי 53ב** (2003), השימוש בטכנולוגיית התקשוב למתן שירותים ממשלתיים לציבור, עמ' 202-210.

15 החלטה מס' 1812 מיום 12.5.02.

16 פרויקט שיזם אגף החשב הכללי במשרד האוצר בשנת 2000 להקמה ולהטמעה של מערכת מחשוב אחידה במשרדי הממשלה, לניהול המשאבים בתחומים האלה: כספים, כוח אדם, רכש (לוגיסטיקה) ונכסים ולביצוע פעולות נוספות, כגון פניות לקבלת תמיכות ולהקצאתן.

17 פרויקט שנועד לספק תשתית לחתימה אלקטרונית ולזיהוי.

בחודשים אפריל ומאי 2013 בדק משרד מבקר המדינה כמה היבטים של אבטחה פיזית ושרידות מערכות של תשתיות אינטרנט ומחשוב בתהיל"ה. בדיקה זו נערכה כבדיקת השלמה לביקורת שערך משרד מבקר המדינה בנושא ניהול אבטחת מידע ושרידות תשתיות אינטרנט ומחשוב עבור משרדי ממשלה[18]. נבדקו בעיקר אבטחה פיזית והיערכות לסיכונים ביטחוניים, סיכוני אש וסיכוני מים. הביקורת נערכה במשרדי ממשל זמין שבמשרד האוצר ובאתר החלופי (DRP)[19] של ממשל זמין בטירת הכרמל.

אתר ממשל זמין נמצא בירושלים. הבניין בנוי מאגף אחד הכולל שבעה מפלסים, וצורתו מלבנית: אורכו 60 מטרים, רוחבו 40 מטרים וגובהו 14.5 מטרים. הבניין כולל 2.5 קומות משרדים, 3.5 קומות של חדרים טכניים וקומת חניה בשטח של כ-1,500 מ"ר. הבניין מוקף בחלקו בגדר אבן טבעית בגובה 2.5-2 מטרים ובצדו הצפוני כביש גישה ללא מוצא.

2. על פי החלטת ממשלה נוהל מפת"ח - נוהל מסגרת לניהול המחשוב בארגון הן במישור הפרויקט והן במישור הארגון כולו, הוא נוהל מחייב במשרדי הממשלה[20]. נקבע בו כי אבטחת מידע כוללת כמה רכיבים: שמירה על חיסיון המידע (Confidentiality); זמינות מערכות המידע (Availability); ושלמות המידע (Integrity). אבטחת המידע מטרתה להגן על ארבע הפעולות הבסיסיות הנעשות בכל מערכת ובסיס נתונים: יצירה והוספה של מידע חדש (Create); קריאה ושליפה של מידע (Read); עדכון ושינוי של מידע (Update); ומחיקה וביטול של מידע (Delete). פגיעה במערכות הממוחשבות במגזר הציבורי עלולה לגרום לנזקים כבדים, כמו פגיעה בשירותים הניתנים לאזרח, פגיעה בצנעת הפרט וניתוק משרדי הממשלה מרשת האינטרנט.

האגף הבכיר לביקורת המדינה במשרד ראש הממשלה פרסם בספטמבר 2005 "נוהל מסגרת לאבטחת מידע" (להלן - נוהל המסגרת). נוהל המסגרת כולל 38 נהלים לאבטחת מידע במשרדי הממשלה, לרבות אלה: קביעת מדיניות ומיפוי מידע; הגורם האנושי ואבטחת המידע; אבטחה לוגית; אבטחה פיזית; גיבוי, שחזור והתאוששות; אבטחת תקשורת ושימושי אינטרנט; ואבטחת מידע במחשבים המנותקים מרשתות המשרד. לפי נוהל המסגרת, על תחום אבטחת מידע בגוף ציבורי יהיה מופקד "הממונה על אבטחת מידע", ובאחריותו לבקר את הפעילויות הממוחשבות, כדי לוודא שהמשרד עומד בדרישות אבטחת המידע שמקורן בחוקים, בתקנות ובנהלים. נוהל המסגרת אינו מחייב, ואולם יש בו כדי ללמד על התשתית הדרושה לאבטחת המידע ולשמירה על הפרטיות בגופים ציבוריים.

מכון התקנים הישראלי פרסם כמה תקנים (לא רשמיים) בעניין אבטחת מידע, ובכללם: תקן ישראלי 1243 בנושא בטיחות אש של מחשבים וציוד היקפי; ותקן 27001, שנועד לשמש מודל להקמה, להפעלה, לניטור, לסקירה, לתחזוקה ולשיפור של מערכת לניהול אבטחת מידע. מכלול תקנים אלה משמש נורמה מקיפה לאבטחת מידע בארגונים (להלן - התקנים הישראליים).

בהיעדר חלק מהנהלים לממשל זמין, בחר משרד מבקר המדינה להציג בחלק מפרקי דוח זה את נוהל המסגרת, שנועד להנחות את משרדי הממשלה וגופים ציבוריים, וכן את התקנים הישראליים, כאבן בוחן להערכת נקודות התורפה בממשל זמין.

---

18 מבקר המדינה, **דוח שנתי 63ב**, (2013) ניהול אבטחת מידע ושרידות תשתיות אינטרנט ומחשוב עבור משרדי ממשלה, עמ' 277.

19 Disaster Recovery Planning - אוסף נהלים והנחיות המגדירים תהליכים חיוניים לארגון, פעולות הנחוצות להמשך מתן שירותים חיוניים, לוחות זמנים, מערך חלופי, הסכמי שירות וניסוי מערך התאוששות (לתרגול ולווידוא מוכנות הארגון למצב אסון).

20 החלטת ממשלה (ועדת השרים לענייני כלכלה) כל/103 מאוקטובר 1991.

טיפול ממשל זמין בליקויים שהעלתה הרשות הממלכתית לאבטחת מידע

1. מאז הקמת תהיל"ה בשנת 1997 ועד לשנת 2011 לא הונחה ממשל זמין על ידי אף גורם רגולטורי. על רקע חיוניותה ההולכת וגוברת של תהיל"ה למדינת ישראל, ולנוכח הנזק העלול להיגרם מפגיעה ניכרת בזמינות, באמינות או בסודיות של המידע הממשלתי והשירותים שהיא מספקת, הוכרזה תהיל"ה בשנת 2011 על ידי הרשות הממלכתית לאבטחת מידע של שירות הביטחון הכללי (להלן - רא"ם), כתשתית חיונית המונחית על ידיה.

משרד מבקר המדינה העלה, כי לממשל זמין הוגשו כמה דוחות ביקורת, שנעשו על ידי גורמים שונים, אך לא כל הליקויים שהועלו בהם תוקנו. להלן הפרטים:

במרץ 2011 הגישה רא"ם לממשל זמין דוח "ביקורת למיפוי מערכת ממוחשבת קריטית במשרד האוצר - תהיל"ה" (להלן - דוח רא"ם הראשון). דוח רא"ם הראשון חשף ליקויים בתחום האבטחה הפיזית, ובהם פערים באבטחת המבנה.

ביולי 2012, כשנה וחצי לאחר שהוגש דוח רא"ם הראשון, הגישה רא"ם לממשל זמין דוח ביקורת נוסף - "ביקורת אבטחת מערכת ממוחשבת קריטית במשרד האוצר מערכת תהיל"ה" (להלן - דוח רא"ם השני). מדוח רא"ם השני עולה, כי חלק מהליקויים שהועלו בדוח רא"ם הראשון לא תוקנו, וכי רמת האבטחה של המערכות שהוגדרו כקריטיות נמצאה נמוכה. בתחום האבטחה הפיזית עלו בדוח ליקויים באבטחת מבנה ממשל זמין.

בהתייחסותו לליקויים האמורים השיב ממשל זמין למשרד מבקר המדינה באוגוסט 2013, כי הותקן תא סינון בכניסה לחדר השרתים, והותקנה "דלת מוטרדת" בכניסה לחדר מעדכני האתרים.

כמו כן הועלו בדוח רא"ם השני ליקויים בתחום אמצעי אבטחה היקפיים במתחם ממשל זמין, שעלו כבר בדוח רא"ם הראשון, אך עדיין לא תוקנו.

בהתייחסותו מאוגוסט 2013 מסר ממשל זמין, כי בדוח "סטאטוס טיפול בפערים בעקבות ביקורת תמ"ק [תשתית מידע קריטי]" מיולי 2013 נמצא שנושא הסורגים בחלונות נמצא תקין, וכי כל החלונות הינם ממוגני הדף.

בדוח רא"ם השני נכתב גם, כי דרישות האבטחה בהיערכות לחירום אינן עומדות ברמה הנדרשת של רא"ם, ובכללן: נוהל חירום שנכתב עונה חלקית לדרישות רא"ם - הוא אינו מתייחס לפעולה הנדרשת מאיש הצוות האחראי; בוצע תרגיל להעלאת רמת כוננות לרמה 3 בלבד, ללא שילוב כלל המעורבים בחירום; אין תהליך של שימור ידע, תיעוד תהליכים והפקת לקחים אפקטיבית; כמו כן לא נקבע נוהל המגדיר מהם אירועי אבטחה.

עוד ציין ממשל זמין בתגובתו למשרד מבקר המדינה, כי נוהל החירום (פק"מ חירום) אושר במאי 2013 כחלק מהליכי ההסמכה של ממשל זמין. כמו כן החליטה רא"ם לפטור את ממשל זמין מתרגול חירום לשנים 2011 ו-2012 בעקבות שני אירועי אמת שהתרחשו בנובמבר 2011 ובנובמבר 2012.

יוצא אפוא מדוח רא"ם השני, מיולי 2012, כי חלק מהליקויים שהועלו בדוח רא"ם הראשון, ממרץ 2011, בנושא אבטחה פיזית לא תוקנו.

2. בעקבות הנחיית ממשל זמין על ידי רא"ם ולצורך טיפול בבעיות ובהטמעת נוהלי תמ"ר בממשל זמין, הוקמה ועדת היגוי משותפת, ובה נציגים של רא"ם, אגף הביטחון של משרד האוצר ונציגי ממשל זמין (להלן - ועדת ההיגוי). בפברואר 2013 התכנסה ועדת ההיגוי לדון בעניניה השוטפים.

מסיכום ועדת ההיגוי מפברואר 2013 עלה, בין השאר, כי קיים עיכוב משמעותי ביישום נוהלי תמ"ר בממשל זמין; הושגו "ציונים נמוכים מהמצופה" בביקורות שעשתה רא"ם בתהיל"ה; קיימים התעלמות וחוסר הטמעה בקרב העובדים לנהלים, והיעדר נהלים.

משרד מבקר המדינה מעיר, כי מן הראוי, שממשל זמין יטפל בליקויים שעלו בסיכום ועדת ההיגוי, כדי לעמוד ברמת האבטחה הנדרשת מארגון ממשלתי האחראי על תשתית חיונית.

בתשובתו מאוגוסט 2013 מסר ממשל זמין, כי ב-12.5.13, במהלך הביקורת, קיבל הסמכות ראשונות במסגרת תהליך ההסמכה של תמ"ר. עוד ציין ממשל זמין, כי הוא כתב ואישרר את נוהלי תקן 27001 לפי הנחיות רא"ם, וזאת כחלק מתכנית ההסמכה האמורה.

3. ביולי 2011 ערכה רא"ם תרגיל אבטחת מידע בתהיל"ה. "התרגיל הסתיים בכישלון" לממשל זמין, כאשר המתרגל הצליח להגיע עד לחדר השרתים, והטמין בו מדמה של אמצעי לחימה.

בעקבות התרגיל, הוציא באוגוסט 2011 סגן קצין הביטחון (האחראי על המתחם שבו ממוקמים משרדי ממשל זמין) מסמך ולפיו יינקטו הפעולות הבאות לתיקון הליקויים: יבוצע תרגיל ערנות בתיאום עם קב"ט המתקן; כל מבקר או ספק או נותן שירותים יירשם ביומן אירועים; מערך האבטחה יתודרך בנוהלי העבודה ופרטי האירוע יועברו לידיעתם; נקודות תורפה בבניין בתחום אמצעים פיזיים ואלקטרוניים יטופלו; ייעשו פעולות לקידום המודעות וליישום הנחיות בסיסיות וגילוי אחריות בפתיחת דלתות בכניסה למתחם ממשל זמין ובחדרים רגישים השייכים לממשל זמין; כמו כן הומלץ לבחון אפשרות למיגון פיזי ואלקטרוני, כולל צפייה מעמדת בקרה למתחם הראשי ולחדר הרגיש.

רא"ם ערכה תרגיל נוסף כשנה ושלושה חודשים מאוחר יותר, באוקטובר 2012. בסיכום התרגיל נרשם, כי "תוצאת התרגיל הינה - כישלון". ממסקנות התרגיל עולה, כי הכניסות לבניין אינן מפוקחות ומבוקרות ברמה מספקת; מודעות העובדים לגורמים שאינם מוכרים נמוכה.

בעקבות תרגיל רא"ם מאוקטובר 2012, הכין קצין הביטחון באותו החודש תחקיר, ובו נכתב כי "מערך האבטחה הפיזי נכשל כמו כן נכשלו העובדים 'בשטח הפרטי' של משרדי תהילה". בתחקיר עלה גם כי בבניין ממשל זמין מספר נקודות תורפה שלא טופלו בגלל היעדר תקציב. נקודות תורפה אלה אפשרו לכוח המתרגל לבצע את התרגיל בהצלחה; עוד נכתב בתחקיר שישנם פערים בתשומות הפיזיות והאלקטרוניות בבניין הידועים "<u>גם מתרגיל דומה שבוצע לפני כשנה...</u>" (ההדגשה במקור); ושמערכת האבטחה לא פעלה לפי הנהלים. בין ההמלצות שיש לנקוט נוכח הממצאים שהועלו במסמך צוינו: מיגון נקודות תורפה; עדכון נוהלי עבודה; רענון נוהלי עבודה לעובדי מערך האבטחה ולעובדי ממשל זמין; ותדרוך כל מערך האבטחה על התרגיל.

בביקורת לא נמצא כי תועדו הצעדים שנעשו בעקבות הליקויים שהועלו בתרגילים מיולי 2011 ומאוקטובר 2012. במצב זה לא ניתן לדעת אילו צעדים ננקטו לשם תיקון הליקויים, אם בכלל.

בהתייחסותו מאוגוסט 2013 מסר ממשל זמין כי בעקבות הליקויים ננקטו בין השאר הצעדים הבאים: נקבעו הנחיות למבקר במתקן ממשל זמין הכוללות הצהרה על שמירת סודיות; הותקנו

אמצעי אבטחה פיזיים מתקדמים, כגון: דלת מבוקרת בקומה הראשונה, תריס גלילה בכניסה לחניון הרכבים; עמדת השומרים נבנתה מחדש תוך התקנת אמצעי אבטחה מהמתקדמים בשוק; הותקן אמצעי בקרה על דלת הכניסה מגרם המדרגות; התקיימה הדרכה בנושא אבטחת מידע בסוף שנת 2012; והוסף מאבטח נוסף.

משרד מבקר המדינה מעיר, כי הליקויים שעלו בתרגילים מצביעים על חולשות ממשיות בתחום האבטחה. ואולם חמורה בעיקר העובדה, כי ליקויים משמעותיים שהועלו בתרגיל הראשון שבו ועלו בתרגיל השני. יש לתת גם את הדעת לכך, שלגבי חלק מהנושאים שעלו כליקויים בתרגילים הוער כבר בעבר בביקורות שערכה רא"ם בנושא. תגובת ממשל זמין מצביעה אמנם על נקיטת פעולות לתיקון הליקויים, אולם נדרשות פעולות נוספות בעיקר בכל הנוגע להתקנת אזעקה במתחם התקשורת בין אתרים והכנסת מערכת מבקרים ממוכנת. כמו כן, על הנהלת ממשל זמין ועל קב"ט משרד האוצר להדריך ולהטמיע בקרב העובדים נושאים בתחום האבטחה הפיזית ומשמעותה, על מנת לבסס את ההיערכות בתחום זה.

טיפול ממשל זמין בממצאי סקר מערכות של חדר השרתים

בנוהל "מדיניות אבטחת המידע" של ממשל זמין (להלן - נוהל מדיניות אבטחת מידע), שהוציא אגף הביטחון של משרד האוצר בדצמבר 2005, ועודכן על ידי ממשל זמין במשך השנים, נקבע כי באחריותה של ועדת ההיגוי לאבטחת מידע בממשל זמין (להלן - ועדת ההיגוי) לטפל במכלול נושאים, ובהם גיבוש ועדכון המדיניות בתחום אבטחת מידע, התוויית אסטרטגיות פעילות, פיקוח על תכניות העבודה השנתיות, קיום הערכת נזקים בעקבות תקלות, וגיבוש המלצות לטיפול בהן.

1. **סיכוני מים**: פעולתם השוטפת של מחשבים פולטת חום. חום זה אם לא יסולק ממערכת המחשוב עלול להביא לעליית טמפרטורת העבודה של המעבד ולקריסתו. לצורך עבודתם התקינה של מחשבים בכלל וחוות שרתים בפרט, נדרשת שמירה על טמפרטורה של עד $25^{o}c$[21]. קיימות מגוון שיטות לקירור חדרי מחשב, חלקן מבוססות מים וחלקן לא, ובהן: מזגני אוויר וצ'ילרים. בחדר השרתים של ממשל זמין מותקנות מערכות קירור מבוססות מים (צ'ילרים) לצורך שמירה על טמפרטורה נאותה.

לבקשת ממשל זמין, ערכה חברה א' ביולי 2012 סקר מערכות ותחזוקה לחדר השרתים של ממשל זמין (להלן - סקר המערכות). ממצאי הסקר בתחום מערכות מיזוג האוויר העלו פערים שיש להם השלכות לעניין חשיפת שרתי ממשל זמין לסיכוני מים. עוד נמצא בסקר, כי ביצוע תחזוקת מערכות המיזוג הינו מינימאלי, ותואם רק חלקית לדרישות יצרני המערכות.

הביקורת העלתה, כי ממצאי סקר המערכות לא נדונו בוועדת ההיגוי לאבטחת מידע, כפי שנדרש בנוהל מדיניות אבטחת מידע.

---

21 לפי ארגון ASHRAE - אגודה אמריקנית למהנדסי חימום, קירור ומיזוג אוויר.

משרד מבקר המדינה ביקש מממשל זמין דיווח על הצעדים שננקטו לתיקון המצב בעקבות סקר המערכות, ובתשובה נענה, כי מאחר שהממצאים מתייחסים למיקום חדר השרתים וקיימת תלות בגורמים חיצוניים, ותיקון הליקויים וחולשות החדר דורשים שינוי תפיסה לגבי תשתיות מן היסוד, ממשל זמין בשיתוף מטה התקשוב הממשלתי[22] החל בבחינת חלופות למיקומו של חדר השרתים ולבניית חדר שרתים חדש.

לדעת משרד מבקר המדינה, על ממשל זמין לפעול בהקדם לטיפול בליקויים שהועלו ככל שניתן בתקופת הביניים עד למציאת פתרון יסודי.

2. **מערכות אל-פסק (UPS)**: נועדו לגיבוי והגנה, בין השאר, על מחשבים ושרתים מפני הפרעות בהספקת רשת החשמל, וקפיצות ותנודות בלתי רצויות במתח החשמל, העלולות לגרום נזק בעת התרחשותן, ואף לגרום להשבתת רכיבים אלקטרוניים, ולאבדן מידע שלא גובה.

בנושא מערכות אל-פסק נמצאו בסקר המערכות כשלים. עוד נמצא בסקר, כי תחזוקת מערכות האל-פסק נעשית על ידי צד שלישי (גורם חיצוני).

משרד מבקר המדינה העלה, כי עד מועד סיום הביקורת, מאי 2013, לא תוקנו כל הליקויים שהועלו בסקר המערכות מיולי 2012 בנושא מערכות האל-פסק.

בהתייחסותו מאוגוסט 2013 מסר ממשל זמין למשרד מבקר המדינה כי טמפרטורת חדר מערכות האל-פסק הותאמה לנדרש; הכניסה לחדר מצברים ולחדר אל-פסק אפשרית רק למורשים; וכי "המערכות [המצברים והאל-פסק] מנוטרות כחלק ממערכת ניטור המבנה".

משרד מבקר המדינה מעיר, כי יש לטפל בליקויים שלא תוקנו לאלתר.

התאמת מבנה ממשל זמין לתקן הישראלי 1243

1. **פתחי חדר המחשב**: בתקן ישראלי 1243 "בטיחות אש של מחשבים וציודם ההיקפי" (לא רשמי, להלן - תקן 1243) נקבע, כי בבניין שנמצא בו חדר המחשב (להלן - חדר השרתים או חדר המחשב) יש להתקין אמצעי הגנה אלה: קירות בנויים בלא פתחים; אלמנטים חוצצים בין חדר המחשב לבין יתר חלקי הבניין בקירות, הרצפה והתקרה יהיו עמידים באש לא פחות משעתיים; עמידות האש של הקירות או המחיצות המקיפים את חדר המחשב או את חדרי ההחסנה, תהיה במלוא גובהם - מהרצפה הקונסטרוקטיבית (רצפה צפה) שמתחתם ועד לתקרה הקונסטרוקטיבית (תקרה מונמכת) שמעליהם; בכניסה לחדר המחשב יותקנו דלתות אש תקניות, שעמידות האש שלהן 30 דקות לפחות.

---

22 מטה התקשוב הממשלתי אחראי על התווית אסטרטגיה ומדיניות טכנולוגיות המידע והשירות של המגזר הממשלתי בשיתוף גופים ציבוריים ובקרתם, ניהול והובלת גוף הביצוע הממשלתי לפרויקטים ומערכים רוחביים, ולייעץ לממשלה בנושאים הקשורים לטכנולוגיות המידע.

משרד מבקר המדינה העלה, כי בחדר השרתים של ממשל זמין קיימים פערים מול המלצות התקן הישראלי, בהם שני פערים יסודיים.

יצוין כי לפערים אלו ניתנה התייחסות בסקר המערכות.

משרד מבקר המדינה מעיר, כי על ממשל זמין לטפל בפערים אלה כך שיפחיתו את הסיכונים הנגזרים מהם בהיבטי מערכת הכיבוי האש והביטחוני.

2. **מיקום המתקן:** בתקן 1243 נקבע בין השאר כי מומלץ לשכן את השרתים ואת ציודם ההיקפי במבנה ייעודי עמיד אש[23], וכשאין אפשרות כזו, הומלץ לשכן אותם במבנה נפרד, באגף נפרד או בחדר נפרד, שהותאמו לייעוד זה. עוד נקבע בתקן, כי כיוון שמחשבים וציודם ההיקפי הפכו לאחרונה יעד למעשי חבלה והצתה, יתוכנן חדר השרתים וימוקם באופן שתצומצם האפשרות לחדור לתוכו עם חומרי חבלה או עם כלי הצתה. כמו כן נקבע, כי חדר השרתים לא יימצא מעל אזורי פעילות שמבצעים בהם תהליכים מסוכנים, לא מתחתם ולא בסמוך להם, אלא אם הותקנו שם אמצעי הגנה נאותים.

בינואר 2006 כתבה חברה ב', העוסקת בין השאר בחומרים מסוכנים, את המסמך "פעולות מטה חרום וצוותי חרום בעת אירוע חומרים מסוכנים" עבור המתחם שבו שוכן ממשל זמין.

משרד מבקר המדינה העלה, כי חדר המחשב של ממשל זמין הוקם במבנה שאינו מבנה ייעודי עמיד אש.

עוד העלה משרד מבקר המדינה, כי לא נמצא שנערכו דיונים כלשהם על הסיכונים הגלומים באכלוס ממשל זמין ומערכותיו בבניין האנרגיה הממשלתי.

בהתייחסותו מאוגוסט 2013 מסר ממשל זמין, כי "אין ספק כי נתונים אלה בעייתיים מאוד באשר למיקומה של החווה הממשלתית, ויחד עם זאת מטרידים ביותר לאור העובדה שבבניין עובדים 250 עובדי ממשל זמין, הנמצאים בסכנה יומיומית עקב ממצאים אלו".

לדעת משרד מבקר המדינה, מן הראוי שייעשה מאמץ מערכתי לנקוט בצעדים הנדרשים, כדי להקטין את הסיכונים לחיי אדם ולחוות השרתים מהסכנות האורבות להם במיקומם הנוכחי ובתנאים הקיימים בו כיום.

3. **הגנות מפני סיכוני מים:** בתקן 1243 נקבע, כי במבנה שאינו עמיד אש ימוקם חדר המחשב באופן שייחשף חשיפה מזערית לאש ולמים, לאדים ולחום, לעשן ולזיהום. עוד נקבע בתקן 1243, כי רצפת חדר המחשב תנוקז גם כשהציוד מוצב במישרין על הרצפה, וגם כשהוא מוצב

23 מבנה שעמידות האש של רכיביו נבדקת לפי התקן הישראלי ת"י 931, לרבות קירות ומחיצות, עמודים ורצפות, קורות, תקרות וגגות, אינה פחותה מהנדרש בתקן זה.

על רצפה צפה[24]. הניקוז ימעיט ככל האפשר את הנזק העלול להיגרם למחשב ולציוד ההיקפי מדליפות מים ונוזלי קירור מהצנרת, ומפעילות כיבוי אש.

כאמור, כל מערכות המחשב הנמצאות בחדר המחשב מקוררות על ידי מערכת קירור מבוססת מים (צ'ילר) הפרושה בצינורות על קירות חדר המחשב, בתוך ארונות השרתים ועל רצפת החדר. עוד נמצא, כי רצפת החדר אינה מנוקזת כמומלץ בתקן, זאת למרות כל הסיכונים הקיימים ממים.

משרד מבקר המדינה מעיר כי, על ממשל זמין לצמצם את הסיכונים ממים וכך שבמקרה של תקלה במערכות המים לא ייגרם נזק לשרתי ממשל זמין.

4. הגנות מפני סיכוני אש: בתקן 1243 נקבע, כי להגנת חדר המחשב וציודו ההיקפי מומלץ להשתמש בין השאר באמצעים אלה: גלאי אש ועשן או גלאים אחרים באגף המחשב, בחדר המחשב, ומעל לתקרה דקורטיבית, בהתאם לתקן הישראלי 1220 (בנושא מערכות גילוי אש) על חלקיו. כמו כן נקבע כי יש להתקין מערכת כיבוי אש בהצפה בגז כשיש צורך חיוני להגן על נתונים בשלבי עיבודם, להקטין את הנזק ככל האפשר ולאפשר חזרה מהירה למצב של פעילות תקינה. מערכת ההצפה בגז תופעל אוטומטית על ידי מערכת גלאים עם אפשרות השהיה והפעלה ידנית. בעת הפעלת מערכת כיבוי אש בהצפה בגז, יש להשבית את מערכת מיזוג האוויר, כדי שזו לא תדלל את חומר הכיבוי במקום הדלקה. כשמופעלת מערכת כיבוי האש בהצפה, תופעל בו-זמנית גם התרעה קולית למצויים ביחידת המחשב. התקן אוסר על אחסנתם של הבאים בחדר מחשב: כל פריט שאינו קשור ישירות למערכת המחשב; חומרים דליקים, כגון נייר ומוצריו, תיבות קרטון, כרטיסים ודיו בכמות גדולה מהנדרש לתפעול יומי; מכשירים או ציוד מקולקלים; וחומרים או ציוד דליקים, שאפשר להוציאם מהחדר.

מסקר המערכות עולה, כי קיימות מספר נקודות כשל בנושא מערכות גילוי וכיבוי אש באתר ממשל זמין.

בדיקה שערך משרד מבקר המדינה באתר הראשי של ממשל זמין בירושלים העלתה, כי מערכת מיזוג האוויר אינה מושבתת באופן אוטומטי במקרה של תקלה (כדי שלא תדלל את חומר הכיבוי). בנוסף לכך ובניגוד להמלצות תקן 1243, באתר החלופי של ממשל זמין (בעניין זה ראו להלן) נמצאים קרטונים, שידות ושולחנות העשויים מעץ (ראו תמונה).

משרד מבקר המדינה מעיר, כי על ממשל זמין לפנות לאלתר את גורמי הסיכון לאש הקיימים באתר החלופי, ולהחליפם בציוד מתאים אחר.

באוגוסט 2013 התייחס ממשל זמין לעניין זה ומסר, כי הקרטונים באתר החלופי פונו.

---

24 רצפה מוגבהת המורכבת מחלקים פריקים, שמותקנים עליה הציוד ואבזריו, ושבינה לבין הרצפה הקונסטרוקטיבית של הבניין יש חלל, המשמש למעבר כבלים ולעתים משמש גם כתא-אוויר להספקת אוויר ממוזג למחשב, לציודו ההיקפי ולמבנה שהם משוכנים בו.

עמידת ממשל זמין בנוהלי תקן ישראלי 27001

1. נספח א׳ של תקן 27001 (להלן - נספח א׳) שממשל זמין הוסמך לפיו, מפרט את מטרות הבקרה ואמצעי הבקרה, שעל הארגון לכתוב נהלים עבורם. פירוט זה אינו ממצה, וארגון יכול להחליט שיש צורך במטרות או באמצעי בקרה נוספים. פרק 9 לנספח א׳ עוסק ב״אבטחה פיזית וסביבתית״, ומציע 13 אמצעי בקרה (להלן - פרק א-9). ממשל זמין הכין נהלים בשישה מבין 13 הנושאים המפורטים בפרק א-9.

משרד מבקר המדינה העלה, כי למרות הצורך בהכנת נהלים נוספים הנדרשים להבטחת תקינות הפעילות של ממשל זמין, כגון נוהל בנושא ״הגנה מפני איומים חיצוניים וסביבתיים״, המציע דרכים להגנה פיזית מפני נזקים של שרפה, הפצצה, רעידת אדמה, פיצוצים וסוגים אחרים של אסונות, נהלים אלה לא הוכנו.

לדעת משרד מבקר המדינה, על ממשל זמין לבדוק את אמצעי הבקרה המוצעים בנספח א׳, ולהשלים את כתיבת הנהלים לגבי כל הבקרות הנחוצות לפעילותו.

2. חדרי השרתים בממשל זמין מכילים את מערכות התקשוב התפעוליות החיוניות לפעילותו התקינה של ממשל זמין. בשל רגישותם, ישנה חשיבות גבוהה בהחלת נוהלי אבטחת מידע ובשמירה על תנאי מידור מרביים באתרים אלו. נוהל ממשל זמין בנושא ״בדיקת חדר מחשב״ קובע, בין השאר, כי בקר חדר המחשב יסייר בו אחת לשעה, על מנת לוודא כי אין חשש להתרחשות אירוע חריג בחדר, ויבצע ויוודא את הפעולות הבאות: אין סימן לעשן או כל סימן המעיד על חריגה מהשגרה הנהוגה; הדלת החיצונית בחדר המחשב נעולה; דלת החדר המאובטח (Ecom) נעולה; ארבעת המזגנים המרכזיים פועלים במצב של שעון שבת; הטמפרטורה בחדרי המחשב, כולל חדר פרויקט מרכבה נעה בין 21-24 מעלות, ובחדר המאובטח (Ecom) עד 30 מעלות בלילה; בתקרת חדר בקרים אין סימני קפיאה בשני המזגנים; כי אין נזילה ממשאבות המזגנים.

ברצפת חדר המחשב ממוקמים גלאי איתור הצפות. בעת אירוע חריג על הבקר לערוך סיור בחדר המחשב, אחת לשעה, תוך כדי הרמה אקראית של אריחי רצפה, על מנת לנסות ולאתר הצפות. במקרה שאותרה הצפה, יש לשאוב את המים מהמקום על ידי שואב האבק הממוקם על פי הנוהל בכניסה לחדר המחשב. בסיום אירוע חריג, על הבקר לדווח על האירוע לקבוצת אנשים במסרון. על הבקר לעדכן את המשמרת הבאה אודות התרחשות האירוע, וכן לתעדו בדוח המשמרת או בדף חפיפה.

משרד מבקר המדינה העלה, כי אין מתעדים את הסיורים שעורכים הבקרים בחדר המחשב ואת תדירותם. עוד העלה משרד מבקר המדינה, כי על רצפת חדר השרתים מודבק שטיח פי.וי.סי ולא אריחי רצפה שניתן להרימם כנדרש בנוהל. כמו כן, לא נמצא שואב אבק בכניסה לחדר המחשב, שאמור לתת מענה לניקוז מים בחדר המחשב. עולה אפוא, כי המצב הקיים בשטח אינו תואם למצב המתחייב על פיו.

3. נוהל ״אבטחת חדר מחשב״ קובע, כי רשימת מורשי הכניסה תוצב בכניסה לחדר המחשב. חדרי המחשב בממשל זמין יסומנו בשילוט ובאופן ברור כממודרים וכרגישים. כל אורח או גורם זר הנדרש בתוקף תפקידו לשהייה בחדר מחשב או בחדר שרתים, ילווה על ידי גורם מורשה במשך כל שהייתו בשטח חדר המחשב.

עוד נקבע בנוהל, כי באזורים שמורים תותקן ותופעל מערכת גילוי והתראה מרכזית. חדרי השרתים ימוגנו בפני הצפות, על ידי תעלות ניקוז ורצפה צפה. השרתים בחדרי המחשב בממשל זמין יפוקחו על ידי גששי בקרת טמפרטורה.

משרד מבקר המדינה העלה, כי בכניסה לחדר המחשב לא קיימת רשימת מורשים, וחדר המחשב בממשל זמין אינו מסומן כחדר ממודר. כמו כן, אורחים או גורמים זרים, הנדרשים בתוקף תפקידם לשהות בחדר מחשב, אינם מלווים על ידי גורם מורשה, כעולה מדוח רא"ם השני. עוד נמצא, כי אין תעלות ניקוז ורצפה צפה למיגון בפני הצפות, אין גששי בקרת טמפרטורה.

משרד מבקר המדינה מעיר להנהלת ממשל זמין, כי עליה לתקן את הליקויים שהועלו, ולהבטיח קיום הוראות הנוהל, על מנת למנוע מצב שבו ייגרם נזק לתשתית המידע הקריטית, ולעדכן את הנוהל במידת הצורך.

בהתייחסותו מאוגוסט 2013 מסר ממשל זמין למשרד מבקר המדינה, כי הנהלים עודכנו במאי 2013, במהלך הביקורת, ובכללם: הותקן תא סינון בכניסה לחדר המחשב ובו בקרת כניסה באמצעות כרטיס חכם והתראת דלת מוטרדת, כך שהדרישה כי תוצב רשימת מורשי כניסה לחדר המחשב התייתרה, ולכן בוטל הסעיף בנוהל; חדר המחשב סומן כאזור ממודר; בוטל הסעיף למיגון חדר מחשב מפני הצפות על ידי תעלות ניקוז ורצפה צפה. מדוח סטאטוס טיפול בפערים מיולי 2013 שערכה רא"ם עולה, כי כל מבקר נדרש לליווי בכל זמן שהותו במתקן. כמו כן לא נדרשת אזעקה בקומת ממשל זמין, היות שהיא מאויישת 24 שעות ביממה.

לדעת משרד מבקר המדינה, בהתאם לתקן 1243 ובשל החשש מסיכוני המים בחדר המחשב, על רצפת החדר להיות מנוקזת.

4. נוהל "תחזוקת ציוד" קובע, כי גישה לא מורשית לציוד של ממשל זמין עלולה לגרום לדליפת מידע מסווג ונזק לתפעולו השוטף של ממשל זמין. במטרה לצמצם סיכון זה נקבע בנוהל בין השאר, כי בנושא מתן שירותי תחזוקה תהיה בידי מנהל מחלקת מערכות מידע רשימת ספקי שירות מוכרים ומאושרים על ידי ממשל זמין. ספקי השירות יחתמו על נספח א' לנוהל הנוגע לאבטחת מידע וחיסיון המותאם לרמת רגישות וסיווג המידע אשר ייחשף בפניהם. אין להתחיל בהעסקת ספק שירות כלשהו בלי שחתם על המסמכים הנדרשים ואושר על ידי מנהל אבטחת מידע. מחלקת מערכות מידע תערוך מעקב אחר ציוד מחשוב הנמצא מחוץ למתחם ממשל זמין לצורך תחזוקה; ציוד מחשב ותקשורת המתוחזק ומטופל מחוץ למתחם ממשל זמין, ייצא ממתחם ממשל זמין ללא כל מצע מידע[25]; אם אין אפשרות לנתק את מצע המידע מהציוד, יש לקבל אישור מראש ובכתב של מנהל אבטחת מידע, אשר יקבע את סדרי השמירה על הציוד מחוץ למתחם ממשל זמין. אין להחזיר לספקי חומרה כל מצע מידע אשר אגור בו מידע, גם אם מצע המידע נמצא בתקופת אחריות היצרן. באחריות מנהל אבטחת מידע להשמיד לפחות אחת לשנה מצעי מידע פגומים. באחריות מנהל המחלקה המעסיקה את גורם החוץ לוודא את חתימתו על נספח אבטחת מידע. באחריות מנהל המחלקה לוודא כי גורם החוץ המועסק על ידיו אושר מראש על ידי מנהל אבטחת המידע. מנהל אבטחת מידע יהיה אחראי לביצוע הנחיות הנוהל בכל הנוגע לאישורו של גורם החוץ, כמפורט בנוהל.

---

25 רכיב במערכת מחשוב בו מאוחסן מידע דיגיטלי, כגון כונן קשיח.

משרד מבקר המדינה העלה, כי הנוהל הקיים אינו כולל נספח אבטחת מידע וחיסיון, וכי אין בידי מנהל מערכות מידע רשימה של ספקי שירות מאושרים.

משרד מבקר המדינה מעיר, כי היעדר הנספח אינו תקין. עוד נמצא שבפועל מאפשרים לספקים לתת שירות לממשל זמין בלי שחתמו על המסמכים הנדרשים ובלי שאושרו על ידי מנהל אבטחת מידע.

עוד העלתה הביקורת, כי מחלקת מערכות מידע אינה עורכת מעקב אחר ציוד מחשוב הנמצא מחוץ למתחם ממשל זמין לצורך תחזוקה; אין אישורים ממנהל אבטחת מידע על הוצאת מצעי מידע שלא ניתן לנתקם מהציוד, וסדרי שמירתם. כמו כן לא נמצאו סימוכין להשמדת מצעי מידע פגומים על ידי מנהל אבטחת מידע.

5. נוהל "סיכוני אש, חשמל ומים בחדר המחשב", שפורסם בתוך "נוהל מסגרת לאבטחת מידע", שהוציא כאמור האגף הבכיר לביקורת המדינה במשרד ראש הממשלה בספטמבר 2005, קובע, בין השאר, כללים בדבר תדירות ביצוע בדיקות תקינות המחשבים ותדרוך העובדים למקרים של שרפה. בתקן 1243 נקבע כי עובדי חדר המחשב יכירו היטב את מערכות גילוי האש, ולפחות פעם בחצי שנה יעברו אימון לגבי תגובה במקרה של אירוע אש ושימוש בכל ציוד הכיבוי הנמצא במקום.

מסקר המערכות עולה, כי אין בממשל זמין מערך הדרכה וחניכה של העובדים המנהלים את האתר, וכי אין ספר נהלים ועקרונות המגדיר את תחזוקת האתר. כמו כן אין ניהול תקלות סדור, כולל מעקב ממוחשב בזמן אמת, אשר נשמר וניתן להפיק באמצעותו לקחים.

משרד מבקר המדינה העלה, כי לא נמצא כי עובדי חדר המחשב עברו הדרכה ותרגול בנושא אש.

התאמת אתר ממשל זמין לדרישות מכרז לשירותי אתר חלופי

באוקטובר 2007 פרסם אגף החשב הכללי שבמשרד האוצר מכרז[26] "להקמה, תחזוקה ותפעול אתר גיבוי לממשל זמין ופרויקט מרכב"ה DRP". בחוברת המכרז נדרשו המציעים לפרט את התקנים הבין-לאומיים והישראלים שבהם הם עומדים, ולהציג על כך תעודות תקפות. תקנים אלה כללו בין השאר את התקנים הבאים: ISO9001 ותת-תקניו; תקן ישראלי 17799 ותת-תקניו; וכן תקני בטיחות. עוד נדרשו המציעים לציין בפירוט את עמידות האתר המוצע מבחינת מבנה ותשתיות בנושאים הבאים: מבנה, חשמל, קירור, תשתית תקשורת, תקשורת טלפונית, אבטחה פיזית ואלקטרונית גילוי וכיבוי אש, ולצרף אישורים ובהם: אישור קונסטרוקטור לגבי רמת עמידות המבנה ומערכות תשתית ברעידות אדמה; אישור יועץ מומחה לרמת עמידות האתר והחדרים המיועדים כנגד איומי מלחמה, לתקן פיקוד העורף, ואיומי התקפה אטומית; אישור יועץ מומחה לגבי רמת עמידות האתר והחדרים המיועדים כנגד איומי פגיעה ישירה של רקטות מאיומי מלחמה וטרור; אישור לעמידות האתר לאטימות כנגד נשק אטומי, ביולוגי וכימי (אב"ך), בהתאם לדרישות פיקוד העורף למקלטים וממ"דים.

---

26 מכרז 216-2007.

יוצא אפוא, כי המכרז הציב דרישות מחמירות בתחום האבטחה הפיזית. ביולי 2008 נחתם חוזה עם חברת האתר החלופי - אתר גיבוי (DRP) ליחידות ממשל זמין ופרויקט מרכב"ה בטירת הכרמל - לאירוח ארונות שרתים.

משרד מבקר המדינה מעיר, כי האתר הראשי של ממשל זמין אינו עומד בחלק מהדרישות המרכזיות שנקבעו במכרז להקמת האתר החלופי.

בהתייחסותו מאוגוסט 2013 מסר ממשל זמין, כי "איננו רואים את הקשר בין התקנים של האתר החלופי והדרישה שיעמוד באירועי קיצון וחירום לבין האתר בירושלים... אין הדבר הגיוני להוציא משאבים ותקציבים בהיקפים גדולים כדי ששני האתרים יעמדו באותם תקנים...". עוד ציין ממשל זמין, כי חוות השרתים של ממשל זמין הועתקה מבניין משרד האוצר בשנת 2006 לבניין שלא תוכנן במקור לארח חוות שרתים.

לדעת משרד מבקר המדינה, על הממונה על התקשוב הממשלתי במשרד האוצר לבחון את הפערים בתחום התשתית האבטחתית בין המצב הקיים באתר ממשל זמין לבין הדרישות שנקבעו לגבי האתר החלופי, ולקבל החלטות אשר לפעולות המתחייבות מהפערים שנמצאו. בחינה זו צריכה להיעשות תוך שימת לב גם לבעיות נוספות שהועלו בדוח זה.

סיכום

האבטחה הפיזית של מבנה ממשל זמין ושל מערכות תשתית האינטרנט והמחשוב של ממשל זמין אינה עולה בקנה אחד עם הדרישות, התקנים וההנחיות לפעילות ממשל זמין בכלל ולחדר המחשב בפרט. ליקויים אלו מצביעים על כך שההיערכות למניעת אירוע של אבטחה פיזית חסרה; וכן על סיכון לפגיעה בפעילות השוטפת של ממשל זמין במקרה שתתרחש פגיעה במבנה ממשל זמין או באחת המערכות הקריטיות שבו, וכן לפגיעה בזמינות המידע הממשלתי לציבור ולניתוק משרדי הממשלה מרשת האינטרנט.

נוכח זאת, על הממונה על התקשוב הממשלתי לפעול לכך שממשל זמין, המספק בין השאר את שער היציאה של משרדי הממשלה לרשת האינטרנט, יעמוד, כאתר המחשוב המרכזי של הממשלה, בתקנים הנדרשים ובהנחיות הגופים המנחים אותו.

עד למציאת פתרון העומד בסטנדרדים הנדרשים לאתר ממשל זמין, מן הראוי כי ממשל זמין יתקן את כל הליקויים שהועלו בביקורות שנערכו בנושא האבטחה הפיזית נוכח הסיכונים הגלומים בהם לפעילותו השוטפת.

כמו כן על ממשל זמין ליישם את הוראות הנהלים שהוא עצמו קבע בנושא אבטחה פיזית, ומעל לכל, יש לפעול לאלתר למזעור הסכנות הנשקפות לחיי אדם באתר הראשי, ובראשם עובדי ממשל זמין, כפי שפורטו בדוח.