פרק שביעי

משרדי ממשלה

משרד האוצר

פעולות הביקורת

במשרד האוצר נבדקו היבטים בניהול אבטחת מידע ושרידות של תשתיות אינטרנט ומחשוב עבור משרדי ממשלה, ובכללם: ניהול אבטחת מידע, תכנית שיקום מאסון ותכנית המשכיות עסקית, טיפול באירועי אבטחת מידע, יישום מסקנות של דוחות בדיקה ושל אירועי אבטחת מידע ותהליך קבלת החלטות לחסימת גישה לשירותים הניתנים באתר. בדיקות השלמה נעשו, בין היתר, במשרד החקלאות ופיתוח הכפר, במשרד המשפטים, במשרד התחבורה, התשתיות הלאומיות והזהירות בדרכים ובמשרד להגנת הסביבה.

ניהול אבטחת מידע ושרידות של תשתיות אינטרנט ומחשוב עבור משרדי ממשלה

תקציר

אבטחת מידע מוגדרת בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), כ"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין". בשנת 1997 החל אגף החשב הכללי שבמשרד האוצר בפרויקט להסדרת תשתית האינטרנט למשרדי הממשלה (תהיל"ה)[1], ובשנת 1999 החל בביצוע תת-פרויקטים במסגרת מה שכונה לאחר מכן "פרויקט ממשל זמין"[2]. במאי 2002 החליטה הממשלה[3] 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 - מרכב"ה)[4] ומערכות המידע הממשלתיות לבין הציבור (להלן - ממשל זמין או תהיל"ה).

ממשל זמין סיפק בשנת 2012 לכ-50,000 משתמשים במשרדי הממשלה את השירותים האלה: תשתית למתן שירותי רשת מאובטחים, שירותי גלישה מאובטחת

---

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

2 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.

3 החלטה מס' 1812 מיום 12.5.02.

4 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.

באינטרנט המגובים במוקד תמיכה טכני הפועל 24 שעות שבעה ימים בשבוע, דואר אלקטרוני, שירותי תשתית הכוללים שירות מסרונים, אירוח אתרים ועוד.

בשנת 2011 היה תקציב ממשל זמין כ-116 מיליון ש"ח, והוא אירח כ-300 אתרי אינטרנט ממשלתיים, לרבות אתרים של גופים ביטחוניים (להלן - לקוחות ממשל זמין). באותה שנה נרשמו יותר מ-5.5 מיליון כניסות לאתר האינטרנט של ממשל זמין, ובאמצעות המערכת הממוחשבת שולמו כ-17 מיליארד ש"ח בכ-3.4 מיליון עסקאות. אתר ממשל זמין עומד מדי שנה בשנה בכ-5 מיליון ניסיונות תקיפה, לרבות התקפות על שרתי דואר והתקפות למניעת מתן שירות. פגיעה במערכות הממוחשבות במגזר הציבורי עלולה לגרום לפגיעה בשירותים הניתנים לאזרח ובצנעת הפרט.

פעולות הביקורת

בחודשים מרץ-יולי 2012 בדק משרד מבקר המדינה כמה היבטים של אבטחת מידע ושרידות מערכות בתהיל"ה, ובהם ניהול אבטחת מידע, תכנית שיקום מאסון (DRP)[5] ותכנית המשכיות עסקית (BCP)[6], טיפול באירועי אבטחת מידע, יישום מסקנות של דוחות בדיקה ושל אירועי אבטחת מידע ותהליך קבלת ההחלטות לחסימת גישה לשירותים הניתנים באתר. הביקורת נעשתה במשרדי ממשל זמין שבמשרד האוצר. בדיקות השלמה נעשו, בין היתר, במשרד החקלאות ופיתוח הכפר, במשרד המשפטים, במשרד התחבורה, התשתיות הלאומיות והזהירות בדרכים, במשרד להגנת הסביבה וברשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים.

עיקרי הממצאים

1. הנהלת ממשל זמין לא הגדירה את הסיכונים ואת רמתם לגבי חלק מהפרויקטים ותתי-הפרויקטים בממשל זמין.

2. רק בדצמבר 2010, כחמש שנים לאחר פרסום נוהל "מדיניות אבטחת המידע" של ממשל זמין (להלן - נוהל מדיניות אבטחת מידע), מונתה ועדת היגוי לאבטחת מידע בממשל זמין, והרכבה לא תאם את ההרכב שנקבע בנוהל. נמצא כי ועדת ההיגוי לא התכנסה מאז מינויה בשנת 2010. כמו כן התחלפו חלק מחבריה, ולא מונו תחתיהם חברי ועדה אחרים. מאחר שהוועדה לא התכנסה כלל, היא לא מילאה את תפקידה כנדרש בנוהל, לרבות גיבוש ועדכון המדיניות בתחום אבטחת המידע, התוויית אסטרטגיות פעילות, פיקוח על תכניות העבודה השנתיות, הערכת נזקים שנגרמו מתקלות וגיבוש המלצות לטיפול בהן.

3. מנהל אבטחת מידע בממשל זמין לא מילא חלק מהתפקידים שהוגדרו לו בנוהל מדיניות אבטחת מידע. מדובר, בין היתר, בקביעת רמת האבטחה הנדרשת לכל סיווג;

---

5 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).

6 Business Continuity Plan - תכנית פעולה להפעלת המערכות הקריטיות של הארגון בשעת חירום כדי לוודא המשך פעילות עסקית במהירות וביעילות.

בהגדרת אמצעי טיפול ותהליכי טיפול באבטחת רשומות; בהתוויית רמת האבטחה הלוגית[7] המחייבת בעבור רכיביהן השונים של מערכות המחשוב והתקשורת; בהגדרה ובהענקה של הרשאות גישה למשתמשים על פי נוהל המדיניות; ובקיום ביקורות על הפעילויות הנערכות במידע.

4. מנהל אבטחת מידע בממשל זמין כפוף מהבחינה המקצועית ומהבחינה המינהלית ישירות למנהל ממשל זמין. כפיפות זו עלולה להביא לידי פגיעה באי-תלותו, מפני שמתוקף תפקידו הוא נדרש לבקר חלק מפעילות מערכות המידע של הארגון המצויות בסמכותו ובניהולו של מנהל ממשל זמין.

5. לא הוכנה תכנית להמשכיות עסקית בממשל זמין. רק בנובמבר 2012 מינתה הנהלת ממשל זמין בעל תפקיד האחראי להיערכות להמשכיות עסקית.

6. למרות ההוראות המחייבות שנקבעו בנושא תכנית שיקום מאסון, ואף שכבר משנת 2008 קיימים אתר חלופי ותכנית מפורטת להפעלת מערך השיקום מאסון ונקבעה תדירות התרגול הנדרשת, לא נערכו התרגילים כנדרש.

7. רק במועד סיום הביקורת פורסם ללקוחות ממשל זמין מסמך אמנת שירות, הכולל מענה לתקלות, מענה לפניות שוטפות והתחייבות על רמת זמינות, כפי שדרשה ועדת ההיגוי של ממשל זמין.

8. לממשל זמין אין הסכם עם אף לא אחד מלקוחותיו המגדיר מי הם מורשי הגישה למאגרי המידע של הלקוח כנדרש בחוק הגנת הפרטיות. ממשל זמין גם לא מסר דיווח שנתי לרשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים, כנדרש בחוק הגנת הפרטיות, ובתוקף היותו מחזיק במאגרים של בעלים שונים.

9. חוץ מסיכום ישיבה אחת בנושא סקר הנהלה, שהתקיימה בנובמבר 2010, לא נמצאו מסמכים המעידים על כך שנעשו סקרי הנהלה בשנים 2009-2012. כמו כן לא נמצאו מסמכים המעידים על יישום ההחלטות שהתקבלו בסקר ההנהלה בנובמבר 2010, ושהיו אמורות להתבצע עד סוף 2011.

10. מנור"ה (מערכת ניהול ותיעוד הרכש הממשלתי) הופעלה במרץ 2010, למרות הימצאותן של בעיות במערכת בתחום אבטחת המידע. אישור זמני להפעלת המערכת, שנתן מנהל אבטחת מידע, כשנה וחצי לאחר שהמערכת הופעלה ולאחר שנוהלו בה תשעה מכרזים - ניתן, אף על פי שלא כל הבעיות במערכת טופלו, כפי שעלה בדוח שעשה צוות בדיקה של ממשל זמין.

11. במאי 2012 פרסמה מחלקת אבטחת המידע טיוטת נוהל תפעולי שכותרתו "פעולות לביצוע בעת מתקפת מניעת שירות". התברר שהטיוטה לא אושרה לא על ידי מנהל אבטחת מידע ולא על ידי ועדת ההיגוי של ממשל זמין.

12. מנהל אבטחת מידע בממשל זמין לא גיבש תכנית הדרכה כוללת להגברת מודעות העובדים לכל ההיבטים הנוגעים לאבטחת מידע. הוא אינו מעודכן בנוגע לעובדים חדשים בממשל זמין, וממילא אין הם מקבלים את ההדרכה הנדרשת לפני קבלת הרשאות הגישה.

---

7 הפעלת מנגנוני תכנה ייעודיים, כגון שם משתמש וססמה המוזנים כתנאי להפעלת מחשב.

סיכום והמלצות

אבטחת מידע היא אבן יסוד בפעילותו של ממשל זמין, ומשום כך עליו להעלות את הנושא לראש סדר עדיפויותיו. כספק העיקרי של תשתיות מחשוב ושל שירותי מחשוב למשרדי ממשלה ולגופים ציבוריים, נדרש ממשל זמין לקיים פעילות מלאה ושוטפת בתחום אבטחת המידע במטרה למנוע פגיעה בזמינות המידע הממשלתי לציבור.

ממצאיו של דוח זה מלמדים על כך שממשל זמין לא יישם בהיבטים שונים הוראות ונהלים בתחום אבטחת המידע ובכך גדלה רמת הסיכון לפגיעה בתשתיות המחשוב ובשירותי המחשוב למשרדי ממשלה וגופים ציבוריים.

לנוכח הליקויים שהועלו בדוח, נדרשת הנהלת ממשל זמין לנקוט כמה וכמה פעולות. עליה לקבוע את הסיכונים הנשקפים לכל הפרויקטים בממשל זמין ואת רמת הסיכון הנשקפת מכל אחד מהם; אין להכפיף את מנהל אבטחת מידע בממשל זמין באופן שיפגע בעיקרון אי-התלות שלו; יש ליישם תכניות התאוששות מאסון והמשכיות עסקית בכל הנוגע לתשתית המידע הקריטי שלו, ולבדוק ולתרגל במלואן את ישימותן הן מהבחינה הטכנולוגית והן מהבחינה האנושית. כמו כן, מומלץ שממשל זמין ייקבע קובץ נהלים לגופים הציבוריים המתארחים בו שלפיהם עליהם לפעול. על הנהלת ממשל זמין לבצע את פעולות ההדרכה הדרושות בתחום אבטחת מידע, לרבות הכנת תכנית הדרכה שנתית ומימושה, וכן בקרה על מידת הטמעתן של ההוראות וההנחיות בתחום זה.

♦

מבוא

"מידע" מוגדר בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות): "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו". אבטחת מידע מוגדרת בחוק הגנת הפרטיות, כ"הגנה על שלמות המידע, 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 (תהיל"ה)[8], ובשנת 1999 החל בביצוע תת-פרויקטים במסגרת מה שכונה לאחר מכן "פרויקט ממשל זמין"[9]. במאי 2002 החליטה הממשלה[10] 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

---

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

9 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.

10 החלטה מס' 1812 מיום 12.5.02.

ברשת האינטרנט, המקשר בין "מערכת רוחבית כוללת במשרדי הממשלה" (להלן - מרכב"ה)[11] ומערכות מידע ממשלתיות לבין הציבור (להלן - ממשל זמין או תהיל"ה).

ממשל זמין סיפק בשנת 2012 לכ-50,000 משתמשים במשרדי הממשלה את השירותים האלה: תשתית למתן שירותי רשת מאובטחים, שירותי גלישה מאובטחת באינטרנט, דואר אלקטרוני, אירוח אתרים ועוד. כמן כן, ממשל זמין מנהל את פרויקט כרטיס חכם, 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.

במרץ 2011 החליטה הממשלה[12] על הקמת יחידת מטה ותקשוב ממשלתי במשרד האוצר (להלן - יחידת תקשוב ממשלתי), במטרה לקדם ולייעל את מערך התקשוב הממשלתי ואת שיתוף הפעולה בין המגזר הממשלתי לגופים ציבוריים נוספים בתחומי המחשוב, כדי לשפר את רמת השירות לאזרח. עוד נקבע בהחלטה, כי האחריות על ממשל זמין תועבר למנהל היחידה. עד לאותו מועד היה סגן החשב הכללי שבמשרד האוצר אחראי לממשל זמין.

בשנת 2011 עמד תקציב ממשל זמין על כ-116 מיליון ש"ח, והוא אירח כ-300 אתרי אינטרנט ממשלתיים (להלן - לקוחות ממשל זמין). באותה שנה נרשמו יותר מ-5.5 מיליון כניסות לאתר האינטרנט של ממשל זמין, ובאמצעות המערכת הממוחשבת שולמו כ-17 מיליארד ש"ח בכ-3.4 מיליון עסקאות. אתר ממשל זמין עומד מדי שנה בשנה בכ-5 מיליון ניסיונות תקיפה, לרבות התקפות על שרתי דואר והתקפות למניעת מתן שירות (בעניין זה ראו להלן).

מחלקת אבטחת המידע בממשל זמין מונה מספר עובדים. המחלקה אחראית לתחומי הקמה, הטמעה ותפעול של מערכות אבטחת המידע, סייבר[13], מתודולוגיה וחסינות מערכות, CERT[14] וניתוח אירועים (להלן - צוות החירום).

בחודשים מרץ-יולי 2012 בדק משרד מבקר המדינה כמה היבטים של אבטחת מידע ושרידות מערכות בתהיל"ה, ובהם ניהול אבטחת מידע, תכנית שיקום מאסון ותכנית המשכיות עסקית, טיפול באירועי אבטחת מידע, יישום מסקנות של דוחות בדיקה ושל אירועי אבטחת מידע ותהליך קבלת החלטות לחסימת גישה לשירותים הניתנים באתר. הביקורת נעשתה במשרדי ממשל זמין שבמשרד האוצר. בדיקות השלמה נעשו, בין היתר, במשרד החקלאות ופיתוח הכפר (להלן - משרד החקלאות), במשרד המשפטים, במשרד התחבורה, התשתיות הלאומיות והזהירות בדרכים (להלן - משרד התחבורה), במשרד להגנת הסביבה וברשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים.

הבסיס הנורמטיבי

1. חוק הגנת הפרטיות ותקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986, קובעים, כי האחריות לאבטחת המידע מוטלת על בעלי מאגר

---

11 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.

12 החלטה מס' 3058 מיום 27.3.11.

13 מרחב מטפורי של מערכות ורשתות מחשב שבהן נאגרים נתונים אלקטרוניים ונעשית תקשורת מקוונת ואינטראקטיבית ללא תלות במיקום הגיאוגרפי של המשתמשים בו.

14 Computer Emergency Response Team - צוות מענה חירום למחשוב.

המידע, על המחזיקים בו ועל מנהליו. הגופים המוזכרים בחוק זה, ובהם משרדי ממשלה, חייבים למנות ממונה על אבטחת מידע שיופקד על אבטחת המידע במאגרים המוחזקים ברשותם.

2. החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), מטיל חובה על גוף ציבורי, המנוי בתוספת לחוק, למנות ממונה ביטחון האחראי במסגרת תפקידו ל"פעולות אבטחה פיזית", לרבות שמירה על רכוש, ול"פעולות לאבטחת מידע" לשמירה על מידע מסווג ולמניעת פגיעה בו. לגופים המנויים בתוספת הרביעית[15] לחוק זה אחריות גם ל"פעולות לאבטחת מערכות ממוחשבות חיוניות", הכוללות את כל הפעולות הנדרשות לשמירה על המערכות הממוחשבות, על המידע שבהן ועל הפעולות למניעת פגיעה בהן.

3. על פי החלטת ממשלה[16] נקבע נוהל מפת"ח (מתודולוגיית פיתוח ותחזוקה) כנוהל מחייב במשרדי הממשלה ובגופים ציבוריים. נוהל מפת"ח מהווה מסגרת לניהול המחשוב בארגון הן במישור הפרויקט והן במישור הארגון כולו, לרבות נושא אבטחת מידע. בנוהל נקבע כי אבטחת מידע כוללת כמה רכיבים: שמירה על חיסיון המידע (Confidentiality), זמינות מערכות המידע (Availability) ושלמות המידע (Integrity). אבטחת מידע באה להגן על ארבע הפעולות הבסיסיות הנעשות בכל מערכת ממוחשבת ובכל בסיס נתונים, ואלה הן: 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 כמו פגיעה בשירותים הניתנים לאזרח ובצנעת הפרט.

4. בפברואר 2007 פרסם מכון התקנים הישראלי את התקן הישראלי 27001 (להלן - תקן 27001) שנועד לשמש מודל להקמה, להפעלה, לניטור, לסקירה, לתחזוקה ולשיפור של מערכת לניהול אבטחת מידע. הטמעת הנוהל בארגון מחייבת קביעת מדיניות, מטרות, תהליכים ונהלים לניהול סיכונים ולשיפור אבטחת המידע. ממשל זמין קיבל כתב הסמכה לתקן זה עד פברואר 2014, והוא עובר מבדקים שנתיים לתיקוף הסמכה זו (בעניין זה ראו להלן).

5. בספטמבר 2005 פרסם האגף הבכיר לביקורת המדינה במשרד ראש הממשלה "נוהל מסגרת לאבטחת מידע" (להלן - נוהל המסגרת). נוהל המסגרת כולל 38 נהלים לאבטחת מידע במשרדי הממשלה, שעניינם קביעת מדיניות ומיפוי מידע, הגורם האנושי ואבטחת המידע, אבטחה לוגית[17], 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 לא נקבע כמחייב במשרדי הממשלה, אך ניתן ללמוד ממנו על התשתית הנדרשת לאבטחת המידע ולשמירה על הפרטיות בגופים ציבוריים.

לדעת משרד מבקר המדינה, מן הראוי שהממונה על התקשוב הממשלתי תבחן לאמץ את נוהל המסגרת כנוהל מחייב לאבטחת מידע במשרדי הממשלה.

6. במאי 2004 קיבלה הממשלה[18] החלטה בנושא ממשל זמין, ובה נקבע, בין השאר, שיש להנחות את משרדי הממשלה לפעול על פי נוהלי העבודה המקובלים ב"פרויקט ממשל זמין", ובהם: 1. אתר שער הממשלה החדש יפורסם בכל אתר מידע ממשלתי. 2. באתר המכרזים המקוונים יתפרסמו כל מכרזי הממשלה. 3. על כל משרד ממשלתי לאפשר תשלום של כל שובר

---

15 תוספת זו כוללת את משרד הפנים ומשרד האוצר וכן תאגידים העוסקים בין היתר בתשתיות.
16 החלטת ממשלה (ועדת השרים לענייני כלכלה) כל/103 מאוקטובר 1991.
17 הפעלת מנגנוני תכנה ייעודיים, כגון שם משתמש וסיסמה המוזנים כתנאי להפעלת מחשב.
18 החלטה מס' 1912 (חכ/83) מיום 20.5.04.

בשירות התשלומים הממשלתי באינטרנט באמצעות כרטיס אשראי או לאפשר תשלום באמצעות בולי הכנסה.

7. במרץ 2011 החליטה הממשלה[19], להפעיל את אתר הממשל הפתוח הישראלי באינטרנט, בכתובת OPEN.GOV.IL, כדי לאפשר שימוש במידע הממשלתי - על ידי הציבור ולטובת הציבור. באתר יוכל אדם, בין השאר, לקבל מידע על מאגרי המידע המפורסמים לטובת הציבור; לשלוח משוב הנוגע לאיכות המידע המופיע באתר; לספק מידע הנוגע לתעדוף של סוגי מידע לפרסום; לקבל מידע על תכניות הממשל הפתוח של ממשלת ישראל.

ניהול אבטחת מידע בממשל זמין

בתקנון כספים ומשק (להלן - תכ"ם) של החשב הכללי במשרד האוצר ובתקנון שירות המדינה (התקשי"ר) נקבע כי נוהל צריך להיות מאושר על ידי סמנכ"ל בכיר ולהיות נדון בוועדה רלוונטית, וכי יש לפרסם את מועד כניסתו לתוקף. כל עדכון בנוהל מחייב שינוי מספר מהדורה.

הביקורת העלתה כי על נוהלי אבטחת המידע, שהוכנו בעקבות הטמעת תקן 27001 בממשל זמין, מופיע שמו של סגן מנהל ממשל זמין כמאשר הנוהל, אך ללא חתימתו. עוד הועלה כי בכל הנהלים שנכתבו לא נרשם מתי ייכנסו לתוקף, ולחלקם אף לא נמצאו מסמכים המעידים על ניהול מהדורות.

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 כמה פעמים עד גרסתו האחרונה מפברואר 2012, נקבע כי פעילותו התקינה של ממשל זמין תלויה בשלמות המידע, סודיותו, אמינותו, עדכניותו, זמינותו ושרידותו. מדיניות זו היא הבסיס הארגוני להחלטות ההנהלה, שלפיו יש לתת מענה ארגוני, אמצעים ומשאבים כלכליים, תוך כדי מיסוד נכון של תהליכי קבלת החלטות הנוגעות לניהול ולבקרה במסגרת אחריות מוגדרת שמטרתה להתוות את מדיניות אבטחת המידע בממשל זמין לצורך צמצום הפגיעה במידע, במאגריו ובמערכותיו. צמצום הפגיעה יביא לידי הקטנת סיכוני הפגיעה בתפעולו של ממשל זמין, וכפועל יוצא מכך, יקטן הסיכון לפגיעה גם במקבלי השירות.

עוד נקבע בנוהל כי אבטחת המידע בממשל זמין כוללת אבטחה פיזית, אבטחת רשומות, אבטחה לוגית, מהימנות עובדים ואבטחת ממשקים עסקיים. היא תיושם בכפוף ובצמידות לחוקים, לתקנות ולהנחיות הנוגעים לתחום אבטחת מידע, לרבות חוק המחשבים, התשנ"ה-1995, וחוק הגנת הפרטיות ותקנותיו, ובהתייחס להחלטות ועדת ההיגוי לאבטחת מידע, שמערך אבטחת המידע צריך לעמוד בדרישות תקן 27001 לצורך שיפור מתמיד שיענה לדרישות מודל PDCA[20] של התקן הישראלי ISO 9001:2008.

---

19 החלטה מס' 2985 (שמצ/4) מיום 14.3.11, בהמשך להחלטת ממשלה מס' 2201 מיום 8.8.10.

20 PDCA (Plan, Do, Check, Act) - סבב פעילויות הכולל ארבע "תחנות" עיקריות: תכנן, עשה, בדוק, פעל. מודל זה מקובל בעיקר בבקרת איכות (איתור תקלות), שם ה"תחנות" הן: תכנן - הגדר מטרות ותהליכים לנוכח ספציפיקציות (דרישות) מוגדרות, עשה - יישם תהליכים אלה, בדוק - מדוד והערך את התוצאות שהושגו מול המטרות והספציפיקציות שהוגדרו, פעל - בצע פעולות לתיקון ולשיפור תהליכים, כולל שיפור מעגל PDCA עצמו. מובן שהמעגל הוא "אינסופי" ומתבצע כל הזמן.

1. קביעת רמות סיכון לפרויקטים בתהיל"ה: בנוהל מדיניות אבטחת מידע נקבע כי הנהלת ממשל זמין מחויבת גם לקבוע את הסיכונים ורמתם בתחום אבטחת מידע.

בנוהל "טבלת סיכונים ונכסים של תתי פרויקטים בממשל זמין" נקבעה טבלת הסיכונים בעבור פרויקטים ותת-פרויקטים בממשל זמין הכוללים, בין היתר, את שירות הכרטיס החכם, את פרויקט כספת ואת שירות הטפסים. נוהל זה, שעודכן לאחרונה בפברואר 2012 לצורך התאמה לתקן 27001 (בעניין זה ראו להלן), נמצא בשלב טיוטה, והוא אינו מקיף את כל הפרויקטים של ממשל זמין.

משרד מבקר המדינה העלה, כי הנהלת ממשל זמין לא הגדירה את הסיכונים ואת רמתם לגבי חלק מהפרויקטים ותתי-הפרויקטים בממשל זמין. מומלץ שהנהלת ממשל זמין תשלים את עדכונו של הנוהל האמור, ותקבע את הסיכונים ואת רמתם לכל אחד מן הפרויקטים ותתי-הפרויקטים בממשל זמין.

2. ועדת היגוי לאבטחת מידע: בנוהל מדיניות אבטחת מידע משנת 2005 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. עוד נקבע בנוהל המבנה של ועדת ההיגוי - צוות של 11 עובדים ממשרד האוצר. בעדכון משנת 2009 נקבע כי בעלי תפקידים בוועדה יהיו מנהל ממשל זמין שישמש יו"ר הוועדה, מנהל אבטחת מידע בממשל זמין (להלן - מנהל אבטחת מידע) שישמש מזכיר הוועדה ומנהלי תתי-פרויקטים רלוונטיים.

עוד נקבע בנוהל כי ועדת ההיגוי נדרשת לגבש קריטריונים להגדרת סיווג רגישות המידע וחיוניותו לפי מידת הנזק שייגרם לממשל זמין, למדינת ישראל או לגורמים אחרים עקב חשיפה, חבלה או שיבוש של מידע - מאגריו או מערכותיו - בין במזיד ובין בשוגג. סיווג המידע יתייחס לכל מצע או מאגר שהמידע קיים בהם. סיווגו של המידע ייקבע על פי רמת הרגישות הגבוהה ביותר הקיימת בקובץ, במאגר או במצע הפיזי שהמידע אגור בהם.

הביקורת העלתה כי רק בדצמבר 2010, כחמש שנים לאחר פרסום נוהל מדיניות אבטחת המידע, מונתה ועדת היגוי לאבטחת מידע בממשל זמין, והרכבה לא תאם את ההרכב שנקבע בנוהל. נמצא כי ועדת ההיגוי לא התכנסה מאז מינויה בשנת 2010. כמו כן חלק מחבריה התחלפו ולא מונו תחתיהם חברי ועדה אחרים. מאחר שהוועדה לא התכנסה כלל, היא ממילא לא מילאה את תפקידה כנדרש בנוהל.

בהתייחסותה למצאי הביקורת מסרה הנהלת ממשל זמין בנובמבר 2012 כי הדרישות לוועדות היגוי לאבטחת מידע מקורן בכמה הנחיות שממשל זמין כפוף להן, לרבות עמידה בדרישות תקן 27001 ובהנחיות הרשות הממלכתית לאבטחת מידע של שירות הביטחון הכללי (להלן - רא"ם). הפעילות על פי הנחיות רא"ם החלה רק בינואר 2011. ועדת היגוי שמונתה על פי הנחיות רא"ם התכנסה פעמיים, בשנת 2011 ובשנת 2012 (בעניין זה ראו להלן). זאת ועוד, ההנחיות של רא"ם מקיפות כיום כ-90% מפעילותו של ממשל זמין והן צפויות להתרחב בעתיד. לכן אין צורך, לדעתה, בוועדות היגוי שונות לאבטחת מידע אלא יש לרכז את כל הנושאים במסגרת אחת.

משרד מבקר המדינה מעיר להנהלת ממשל זמין, כי אם היא סבורה שוועדת ההיגוי שמונתה לפי הנחיות רא"ם מייתרת את הצורך בוועדת ההיגוי שאמורה לקום מכוחו של נוהל מדיניות אבטחת מידע ומקיפה את כלל פעילותה, עליה לפעול לשינוי הנוהל או לביטולו.

3. יישום נוהל מדיניות אבטחת מידע על ידי מנהל אבטחת מידע בממשל זמין: נוהל מדיניות אבטחת מידע מגדיר את תפקידיו של מנהל אבטחת מידע במתן תמיכה שוטפת בתחום אבטחת מידע והטמעה בשטח של סיכומי ישיבות ועדת ההיגוי ושל החלטותיה. הנוהל גם מפרט את הנושאים והתחומים שבאחריותו של מנהל אבטחת מידע.

(א) על מנהל אבטחת מידע לקבוע את רמת האבטחה הנדרשת לכל סיווג מידע. עליו להתייחס לכל מאגר שהמידע קיים בו - קבצים, בסיסי נתונים, מדיה אלקטרונית או אופטית, מסמכים, דוחות ועוד.

נמצא כי נכון למועד סיום הביקורת, ביולי 2012, לא קבע מנהל אבטחת מידע את רמת האבטחה הנדרשת לכל סיווג של מידע המצוי ברשות ממשל זמין.

(ב) רשומות מידע כוללות מידע פיזי כמו מסמכים, תדפיסים, דיסקים, קלטות וסרטים. מנהל אבטחת מידע נדרש להגדיר לפי רגישות המידע את האמצעים והתהליכים לטיפול באבטחת רשומות, תוך כדי התייחסות לשיטות ולכלים של אבטחת מידע והשמדתו על פי סיווג המידע, לאמצעים ולתהליכים של שינוע מידע (פנים-ארגוני וחוץ-ארגוני), לטיפול בחריגים ולאופן ביצוע פיקוח ובקרה.

נמצא כי מנהל אבטחת מידע לא הגדיר את האמצעים ואת התהליכים לטיפול באבטחת רשומות.

(ג) על מנהל אבטחת מידע להתוות את רמת האבטחה הלוגית המחייבת בעבור מערכות המחשוב והתקשורת, לרבות מערכות הפעלה, תכנות, קבצים ובסיסי נתונים.

נמצא כי מנהל אבטחת מידע לא התווה את רמת האבטחה הלוגית לרכיבים השונים של מערכות המחשוב והתקשורת.

(ד) לצורך מניעת ביצוע שינוי לא מבוקר נקבע בנוהל, כי יוגדרו נהלים המתווים את אופן ביצוע השינויים בנתונים, בתכנה ובחמרה של מערכות ממשל זמין. חל איסור על ביצוע שינוי בנתונים שלא במהלך הפעילות הרגילה, אלא אם הדבר נעשה באופן מאובטח ומבוקר ולפי הנחיות מנהל אבטחת מידע, תוך כדי התייעצות עם גורמי ההנהלה הרלוונטיים.

נמצא כי לא נקבעו נהלים המתווים את אופן ביצוע השינויים בנתונים, בתכנה ובחמרה, ולא נקבע מי אחראי לקביעתם.

(ה) על מנהל אבטחת מידע לבצע מידור של המידע ושל המשתמשים בו על פי סביבת עבודתם (פרופילי משתמשים). לכל פרופיל משתמש עליו להגדיר ולהעניק הרשאות גישה רק לפרטי מידע הדרושים למשתמש לביצוע עבודתו בשיתוף עם בעלי המידע. בנוסף לזאת עליו להגדיר את עקרונות המידור בכל תחום פעילות בממשל זמין.

זאת ועוד, נוהל "ניהול ותפעול מערך הרשאות וסיסמאות" (להלן - נוהל ניהול הרשאות) קובע, בין השאר, כי בעבור כל פתיחת הרשאות חדשות לעובד חייב מנהלו לבקש את אישורו בכתב של מנהל אבטחת מידע.

נמצא כי מנהל אבטחת מידע לא הגדיר למשתמשים הרשאות גישה לפרטי מידע הדרושים להם לביצוע עבודתם, וממילא לא שיתף בכך את בעלי המידע. עוד נמצא כי את הרשאות הגישה למשתמשים נותן מנהל המערכת (סיסטם) ולא מנהל אבטחת מידע, וזאת שלא על פי נוהל מדיניות אבטחת מידע.

(ו) על מנהל אבטחת מידע להתוות תהליכים ושיטות טיפול אבטחתי בממשקים עסקיים, כמו תגבור כוח אדם, לרבות קריטריונים להגדרת סיווג הממשק העסקי, דרישות אבטחתיות בכפוף לסיווג הממשק העסקי, שיטות וכלים לאכיפת הדרישות ותהליכים ואמצעים לפיקוח ובקרה ולטיפול בחריגים.

נמצא כי במאי 2005 הוכן נוהל "ממשק עסקי", אך הוא אינו מיושם. לדוגמה, מנהל אבטחת מידע לא התווה את התהליכים ואת שיטות הטיפול בממשקים עסקיים הפועלים בממשל זמין.

(ז) על מנהל אבטחת מידע להגדיר ולהתוות את האמצעים והתהליכים של הבקרה בתחומי אבטחת המידע של ממשל זמין. באחריותו לבקר, באופן שוטף או אקראי, את הפעילויות הנעשות על המידע, כדי לוודא שממשל זמין עומד בדרישות החוקים, התקנות, התקנים והנהלים ופועל על פי סדרי מינהל תקין. כמו כן יינתנו למנהל אבטחת מידע כלים זמינים לבקרת פעילויות אבטחת המידע השוטף בגופים ובאתרי האינטרנט השונים של ממשל זמין.

בשנת 2009 עודכן נוהל "התאמה לקווי מדיניות האבטחה ולתקני אבטחה" בממשל זמין, ונקבע בו כי מנהל אבטחת מידע יכין בתחילת כל שנה תכנית ביקורת שנתית שתתייחס לנושאים המבוקרים, לתדירות הביקורת, לאתרי האינטרנט המיועדים לביקורת, לפורמט התיעוד של הביקורת, לגורמים נוספים האמורים להיות מעורבים ולתפקידם באירוע.

נמצא כי לא נקבעה תכנית ביקורת שנתית כפי שנקבע בנוהל וכי מנהל אבטחת מידע אינו עורך ביקורת על הפעילויות הנערכות במידע.

(ח) במסגרת הטיפול באירועי אבטחת מידע חריגים נקבע בנוהל כי לכל פעילות חריגה בעלת השלכות על אבטחת מידע יוגדר אופן רישומה, הדיווח עליה ואופן התגובה הנדרש. חריגות בתחום אבטחת מידע, המאותרות על ידי גורמי ממשל זמין או אחרים, ידווחו לצוות אבטחת המידע או למנהל הרלוונטי, וכי אירועי אבטחת מידע חריגים ידווחו לוועדת ההיגוי.

נמצא כי בנוהל לא פורט מהם אירועי אבטחת מידע חריגים בעלי השלכות על אבטחת המידע ולא הוגדרו אופן רישומם, הדיווח עליהם ואופן התגובה הנדרש.

4. כפיפותו של מנהל אבטחת מידע: כאמור, החוק להסדרת הביטחון מטיל חובה על גוף ציבורי למנות ממונה ביטחון האחראי במסגרת תפקידו ל"פעולות אבטחה פיזית", לרבות שמירה על רכוש, ול"פעולות לאבטחת מידע" לשמירה על מידע מסווג ולמניעת פגיעה בו. לגופים המנויים בתוספת הרביעית לחוק זה אחריות גם ל"פעולות לאבטחת מערכות ממוחשבות חיוניות" הכוללות את כל הפעולות הנדרשות לשמירה על המערכות הממוחשבות, על המידע שבהן ועל הפעולות למניעת פגיעה בהן. גופים אלה חייבים במינוי אחראי לארגון ולביצוע פעולות לאבטחת מערכות ממוחשבות חיוניות ולפיקוח עליהן. משרד האוצר נמנה עם הגופים שבתוספת

הרביעית לחוק, ועל כן הוא מחויב במינוי אחראי על אבטחת מערכות ממוחשבות חיוניות, אשר מופקד על הטיפול בכלל המערכות הממוחשבות החיוניות של המשרד.

בנוהל המסגרת נקבע, בין השאר, כי לתחום אבטחת מידע בגוף ציבורי אחראי "הממונה על אבטחת מידע", והוא הגורם המוסמך ליישום המדיניות. באחריותו של הממונה לבקר את הפעילויות הממוחשבות הנעשות, כדי לוודא עמידה בדרישות אבטחת המידע הקבועות בחוקים, בתקנות ובנהלים העוסקים בנושא זה. עוד נכתב בנוהל המסגרת, כי המבנה הארגוני ליישום אבטחת מידע יושתת על עיקרון "הפרדת הסמכויות", ואין להכפיף, מהבחינה המינהלית או מכל בחינה אחרת, את הממונה על אבטחת מידע למנהל מערכות המידע "בשל ניגוד עניינים בין שני התפקידים!".

באוקטובר 1998 מונה מנהל אגף בכיר חירום וביטחון של משרד האוצר ל"ממונה על אבטחת המידע במערכות המחשב של משרד האוצר וממשל זמין". באוגוסט 2004 מונה מנהל אגף זה "לאחראי על הגנת מערכות ממוחשבות חיוניות במשרד האוצר וביחידות הסמך".

נמצא כי למרות זאת מנהל אבטחת מידע בממשל זמין כפוף מהבחינה המקצועית ומהבחינה המינהלית ישירות למנהל ממשל זמין. כפיפות זו עלולה לפגום באי-תלותו, מפני שמתוקף תפקידו הוא נדרש לבקר חלק מפעילות מערכות המידע של הארגון המצויות בסמכותו ובניהולו של מנהל ממשל זמין.

לדעת משרד מבקר המדינה, אין להכפיף את מנהל אבטחת מידע בממשל זמין באופן שיפגע בעיקרון אי-התלות שלו.

בהתייחסותה מנובמבר 2012 מסרה הנהלת ממשל זמין, כי "היישום בפועל של מינוי זה [מינוי מנהל אגף בכיר חירום וביטחון] לא בא לידי ביטוי בממשל זמין בכל הנושאים שהועלו בדו"ח הביקורת ומוגדרים באחריות של הממונה על אבטחת המידע בממשל זמין, למעט בנושא הנחיית רא"ם בהם משמש אגף חירום ובטחון כצינור הנחייה עבור רא"ם (הנחייה עקיפה)". עוד השיבה הנהלת ממשל זמין, כי ימונה ממונה אבטחת מידע (CSO - Chief Security Officer) שתפקידו יכלול הנחיה ובקרה של יחידות התקשוב (ממשל זמין, מרכב"ה, סע"ר); בניית אסדרה וסנכרון מול משרדי הממשלה; סנכרון נושאי אבטחת המידע מול רמו"ט (הרשות למשפט טכנולוגיה ומידע שבמשרד המשפטים) ומטה הסייבר; ועבודה לפי תקנים - נוהל מפת"ח ותקן 27001. הנהלת ממשל זמין הוסיפה כי את אי-התלות ניתן יהיה להשיג על ידי הכפפת התפקיד (ממונה אבטחת מידע) לממונה על התקשוב הממשלתי.

בהתייחס לתגובת הנהלת ממשל זמין מעיר משרד מבקר המדינה, כי מן הראוי שממונה אבטחת מידע לא יוכפף מהבחינה המינהלית, או מכל בחינה אחרת, לממונה על התקשוב הממשלתי, בשל חשש לניגוד עניינים.

תכנית שיקום מאסון ותכנית המשכיות עסקית

1. **הנהלים הנוגעים להמשכיות עסקית ולשיקום מאסון:** בנוהל מדיניות אבטחת מידע נקבע כי תכנית היערכות להמשכיות עסקית (BCP)[21] נועדה לסכל הפרעות בפעילותו השוטפת של ממשל זמין ולהגן על נתונים במערכות המידע שלו מפני הרס, שיבוש ומחיקה הנגרמים ממקרי כשל או ממקרים כמו שריפה, הצפה, אסונות טבע וכדומה. עוד נקבע בנוהל כי הנהלת ממשל זמין אחראית למנות בעל תפקיד האחראי לנושא ההיערכות להמשכיות עסקית. בעל התפקיד, בתיאום עם מנהל אבטחת מידע, יקבע את עקרונות ההיערכות להמשכיות עסקית של מערכות המידע בממשל זמין. עקרונות אלה יובאו לאישור ועדת ההיגוי העליונה טרם עיגונם בנהלים. בעל התפקיד יפעל ליישום עקרונות ההיערכות להמשכיות עסקית, ויהיה אחראי לתחזוקתה ולעדכניותה של התכנית.

בנוהל תכנית היערכות לחירום של ממשל זמין נקבע כי במסגרת תכנית ההתאוששות של ממשל זמין מאסון (להלן - DRP)[22] יינתן מענה להמשכיות התפקוד של אתרי ממשלה קריטיים, כמו אתר משרד החוץ.

עוד נקבע בנוהל כי על מנהל מחלקת מערכות מידע, בשיתוף עם מנהל אבטחת מידע, לנסח ולתכנן תכנית לניהול המשכיות עסקית של ממשל זמין ולהגיש אותה לאישורה של ועדת ההיגוי. הוועדה תאשר את התכנית ותקצה את המשאבים הנדרשים למימושה ולהפעלתה. משתמשי מערכות המחשב יודרכו כיצד ליישם את הנוהל ואת ההנחיות הנלוות אליו. באחריותו של מנהל מערכות מידע, בשיתוף מנהל אבטחת מידע, להדריך את משתמשי הפרויקט כיצד לממש וליישם את התכנית בעת אסון. באחריותו של מנהל אבטחת מידע לבדוק את יישומו של נוהל זה במסגרת מבדק התאמה תקופתי. יש לקיים, לפחות פעם בשנה, תרגיל מימוש לאחד משלבי התכנית, שבעקבותיו יופקו לקחים שיובילו לעדכון התכנית.

בינואר 2012 הגישה חברה א' להנהלת ממשל זמין טיוטת דוח על תקלה במערכות ממשל זמין שקרתה בנובמבר 2011 (להלן - טיוטת דוח התקלה). בטיוטת דוח התקלה נכתב כי בממשל זמין לא קיימת תכנית לניהול המשכיות עסקית. במועד התקלה לא הייתה כל תכנית כתובה שעניינה אופן העלאת גיבויים, וגם לא היו שרתים פיזיים רזרביים באתר המרוחק המיועד להקמת מתקן מחשוב חלופי (להלן - האתר החלופי), למעט כמה שרתים שיועדו לפרויקט אחר ובהם השתמשו. בדוח הומלץ להתחיל בפרויקט של ניהול המשכיות עסקית על פי מתודולוגיה מסודרת ותקנים מקובלים.

הביקורת העלתה כי עד מועד סיום הביקורת לא הוכנה כל תכנית להמשכיות עסקית בממשל זמין. רק בנובמבר 2012 מינתה הנהלת ממשל זמין בעל תפקיד האחראי להיערכות להמשכיות עסקית.

2. **תרגול מעבר לחירום:** באוקטובר 2008 פורסם נוהל "הפעלת מערך ה-DRP של פרויקט ממשל זמין" המגדיר את היערכות תהי"ה לשלב א, של DRP. בנוהל נקבע, בין השאר, כי כל ארבעה עד שישה חודשים יתבצע ניסוי להפעלת מערך DRP - מנהל ממשל זמין יקבע מראש את המועדים, והוא יפעיל את הניסויים. מועדי הניסויים לא יימסרו למתקן שבו נמצא אתר השיקום מאסון, וזאת כדי לבדוק את מוכנות המתקן והעובדים.

---

21 Business Continuity Plan - תכנית פעולה להפעלת המערכות הקריטיות של הארגון בשעת חירום כדי לוודא המשך פעילות עסקית במהירות וביעילות.

22 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).

גם בטיוטת נוהל "היערכות לשעת חירום" של ממשל זמין מיוני 2010 נקבע, בין היתר, כי אחת לשנה ייערך תרגיל מעבר לחירום. התרגיל יכלול את כל הפעולות הדרושות כמפורט בנוהל, לרבות העלאת כוננות, מעבר לאתר חלופי, פעילות בחירום וחזרה לשגרה. בתום התרגיל יבוצע תהליך הפקת לקחים, ובמידת הצורך יעודכנו נהלים והוראות עבודה רלוונטיים. אחת לשישה חודשים ייערך תרגיל מצומצם לבדיקת מוכנות האתר החלופי. בתרגיל תופעל אחת מהמערכות של ממשל זמין מתוך האתר החלופי. מנהל ממשל זמין יקבע מראש את מועדי התרגילים, והם לא יתואמו עם אנשי הקשר באתר החלופי, וזאת כדי לבדוק את מוכנותם.

התברר כי רק ביוני 2010 נערך תרגיל שכלל שינוי כתובת אינטרנט לאחד מאתרי ממשל זמין באופן שהגלישה אליו תתבצע לאתר הגיבוי.

עולה אפוא, כי למרות ההוראות המחייבות שנקבעו בנושא תכנית שיקום מאסון, ואף שכבר משנת 2008 קיים אתר חלופי ותכנית מפורטת להפעלת מערך השיקום מאסון (DRP) ונקבעה תדירות התרגול הנדרשת, לא נערכו התרגילים כנדרש.

3. במרץ 2011 מיפתה רא"ם כמה ממערכות הליבה של ממשל זמין (בעניין זה ראו להלן). בין השאר נכתב בדוח, כי בתהיל"ה לא מצויה תכנית התאוששות מאסון וטרם נערך מיפוי וסיווג נכסים על פי רמת הקריטיות, השרידות והיתירות[23] שלהם. כמו כן הודגש כי לא נערכות בדיקות כמו בקרת שינויים וגרסאות באתר DRP.

הביקורת העלתה, כי הנהלת ממשל זמין לא תיקנה את הליקויים האמורים שהועלו בדוח של רא"ם. משרד מבקר המדינה מעיר להנהלת ממשל זמין, כי יש לתקן את הליקויים ולערוך בקרת שינויים וגרסאות באתר החלופי.

4. **הקמת מערכת DRP**: בפרוטוקול ישיבת ועדת המדע והטכנולוגיה של הכנסת מפברואר 2011, בנושא מוכנות מערכות המידע והמחשוב לשעת חירום במגזר הממשלתי, העסקי והפרטי, אמר חבר הכנסת מאיר שטרית, שמערכות המידע והמחשוב לשעת חירום במגזרים אלה אינן ערוכות לשעת חירום. עוד ציין כי צריך לדאוג שלמערכות הקריטיות במדינת ישראל יהיו DRP, ואולי גם BCP, כך שאם יקרה חלילה אירוע חירום יהיה אפשר להמשיך ולהפעיל את המערכות הקריטיות האלה.

סגן החשב הכללי דאז, מר טל הרמתי, שהיה אחראי באותה עת במשרד האוצר לממשל זמין, ציין בדיון כי היערכות חירום ממשלתית תיעשה בעיקר בהיבטים הארגוניים ולא רק בהיבט הטכנולוגי. הוא הוסיף כי אין אתר DRP ממשלתי אחד לכל הממשלה, וכי בשנת 2011 אמור להתפרסם מכרז לפרויקט DRP ממשלתי.

באפריל 2011 נכתבה בממשל זמין גרסה של מסמך "הקמת תשתיות גיבוי חרום (DR) עבור ממשל זמין". ממסמך זה עולה, כי מתן המשכיות תפקודית מלאה לכלל המערכות שבאחריות ממשל זמין הוא פרויקט בעל מורכבות תפעולית גבוהה, ולכן השירות שיינתן במקרה אסון יתחלק לשלושה שלבים לפי רמת הקריטיות שלהם. המסמך מפרט את הפתרונות הטכנולוגיים הנדרשים ליישום הפרויקט, ונקבע בו גם לוח זמנים - 12 חודשים המסתיימים בניסוי הפעלה באפריל 2012.

---

23 נתונים המופיעים מספר פעמים ומאפשרים המשך מתן שירות גם במקרה של תקלות, ויכולת גיבוי והתאוששות מהירים.

הביקורת העלתה, כי עד מועד סיום הביקורת לא פורסם מכרז מרכזי לפרויקט DRP ממשלתי. כמו כן מכך לא יושם לוח הזמנים שנקבע ליישום תכנית DRP, שעל-פיו היה הפרויקט אמור להיות מושלם עד אפריל 2012, וגם לא נקבע מועד חדש להשלמתו.

בתגובתה מנובמבר 2012 מסרה הנהלת ממשל זמין, כי "המכרז הממשלתי ל-DRP הינו מכרז ל-'שטח רצפה' [שכירת מקום בו יוקם אתר DRP] ולא לפתרון DRP עובד. המכרז המדובר יצא השנה בחודש אוגוסט, עדיין המרחק בין אתר DRP לפתרון DRP זמין ועובד יכול להיות משמעותי ביותר".

משרד מבקר המדינה מעיר לממשל זמין, כי לפי האיומים והתקיפות שחווה ממשל זמין, ולנוכח המסקנות שעלו בדיונים השונים שקוימו בנושא, מן הראוי שיוקם DRP ממשלתי, שייתן מענה אמיתי ומלא בעת חירום.

5. הרקע לתקלה משנת 2011 והליקויים שנחשפו בבדיקתה: מטיוטת דוח התקלה שהגישה חברה א' עולה כי בסוף 2011 התגלתה אי-זמינות של מערך אחסון מסוג מסוים; תקלה זו השביתה אתרים ושירותים הניתנים על ידי ממשל זמין. התקלה התגלתה על ידי עובדי ממשל זמין כבעיה רוחבית של מספר מערכות שאינן מגיבות. כל המערכות חזרו לזמינות מלאה תוך זמן קצר יחסית.

בפרוטוקול ישיבת ועדת המדע והטכנולוגיה של הכנסת מיום 16.11.11, בנושא קריסת אתרי האינטרנט של משרדי הממשלה, ציינה מנהלת ממשל זמין, בין השאר, כי היקף השימוש הגדל מחייב ניהול ותפעול שונים, ואין מדובר בחברת הזנק (סטרט-אפ) קטנה.

מממצאי טיוטת דוח התקלה עולה, כי התקלה חשפה כשלים בכל הקשור להיערכות הכוללת בממשל זמין בנושא ניהול המשכיות עסקית, שעת חירום וגיבויים. ביולי 2008 נחתם חוזה עם חברת האתר החלופי - אתר גיבוי DRP ליחידות ממשל זמין ופרויקט מרכב"ה - לאירוח ארונות שרתים. במסגרת ההסכם הוצבו ארונות שרתים של ממשל זמין לצורך גיבוי, אך לא נעשה בהם כל שימוש, ולא הייתה כל תקשורת בין הגיבוי לבין המערכת הראשית. ביוני 2011 נחתם הסכם המשך עם חברת האתר החלופי.

עוד נכתב בדוח כי מהניסיונות להפעיל ולסנכרן את אתר הגיבוי וליצור גיבוי לנתונים עם האתר הראשי עלה כי, בגלל בעיות טכניות לא צלח הנושא. תכנית הגיבוי באתר החלופי לא עבדה. בשנת 2011 גובשה תכנית DRP חלופית, אך גם היא לא יושמה בשל בעיות מבעיות שונות שפורטו בהמשך טיוטת דוח התקלה.

עוד צוין בדוח כי במועד התקלה פעל קוד לא מעודכן על המערכת הראשית באתר. התקלה הטכנית בקוד הייתה ידועה לחברה ב' (ספקית ציוד מחשוב של ממשל זמין), שהתריעה עליו בפני ממשל זמין, והיא המליצה על שדרוגו. בסופו של יום לא נעשה השדרוג האמור עקב חילוקי דעות בנושאים טכניים בין החברה לממשל זמין.

בהמלצות טיוטת דוח התקלה נכתב כי יש צורך ליישם את פרויקט DRP בלוחות זמנים מידיים. וכי באתר החלופי לא קיים בפועל גיבוי שניתן להפעילו, אף שקיימת התקשרות חתומה. כמו כן, תכנית DRP החדשה שהכינו אנשי ממשל זמין אינה בת-ביצוע בגלל בעיות טכניות ופערים טכנולוגיים שנוצרו מאז הכנתה של התכנית הישנה. עוד הומלץ, לקבוע ועדת היגוי לפרויקט שתאשרר בהקדם את תכנית DRP החדשה מהבחינה הטכנולוגית. בנוגע להמלצה זו השיבה מנהלת ממשל זמין, כי ההמלצה מקובלת עליה, והוסיפה כי ממשל זמין נערך במסגרת ועדת היגוי פנימית לבניית תכנית

DRP בשני שלבים: שלב א׳ - גיבוי מידי לעשרה אתרי אינטרנט מרכזיים שגיבש שירות הלקוחות, ושלב ב׳ - יציאה למכרז ייעוץ לליווי תכנון, ובהמשך גם להקמת מערך DRP מקיף.

בדצמבר 2011 הוקמה בממשל זמין ועדת היגוי לנושא DRP, והיא התכנסה פעמיים בלבד, בדצמבר 2011 ובינואר 2012, ומאז לא התכנסה עוד. במועד סיום הביקורת פועל בנושא ההיערכות לחירום צוות עבודה המורכב מנציגי יחידות במשרד האוצר במסגרת יחידת התקשוב הממשלתי. כמו כן עד מועד סיום הביקורת לא מונה יועץ לליווי, לתכנון ולהקמת מערך DRP.

בתגובתה מנובמבר 2012 השיבה הנהלת ממשל זמין, כי בימים אלו מתחיל את עבודתו אחראי ל-Data Centers ו-DRP. בד בבד נעזר ממשל זמין החל מיולי 2012 גם בשירותי ייעוץ בתחום היערכות לחירום באמצעות יועץ של אגף חירום וביטחון במשרד האוצר.

לדעת משרד מבקר המדינה, על הנהלת ממשל זמין להכין תכניות התאוששות מאסון והמשכיות עסקית לתשתית המידע הקריטי שלה, לקיים במלואם תרגילים לישימותן, הן מהבחינה הטכנולוגית והן מהבחינה האנושית, לתחקר אותם ולהפיק מהם לקחים. כמו כן, על בעל התפקיד, שמונה לנושא התאוששות מאסון בממשל זמין, להכין מסמך אסטרטגי לנושא, שיתוקף בוועדת ההיגוי ויעוגן כנוהל, כפי שנקבע במסמך מדיניות אבטחת מידע.

ממשל זמין ולקוחותיו

במרץ 1998 החליטה הממשלה[24], שכל אתרי האינטרנט הממשלתיים יופעלו בתהיל״ה או שקישורם לרשת האינטרנט יהיה באמצעותה. עוד נקבע כי המידע שיירשם במאגרים יהיה מוגן במערכת הגנה שתבטיח קיום ביטחון מידע שימנע מגורמים לא מורשים לשבשו.

על סמך החלטת ממשלה[25], מדצמבר 2002, הוקמה ועדת היגוי עליונה להגנה על מערכות ממוחשבות במשרד ראש הממשלה. בינואר 2012 אישרה הוועדה מסמך מדיניות לאומית בנושא חיבור גופים ממשלתיים לאינטרנט (להלן - מדיניות חיבור לאינטרנט). מסמך המדיניות קובע עקרונות חיבור לאינטרנט לכל הגופים הממשלתיים לצורכי גלישה באינטרנט, אירוח אתר אינטרנט, דואר אלקטרוני, העברת קבצים, גישה מרחוק ועוד.

בעקרונות מדיניות חיבור לאינטרנט נקבע כי חיבור קבוע של גופים ממשלתיים לרשת האינטרנט יבוצע באמצעות תשתית ממשל זמין לפי הסטנדרדים שהוא יקבע ויפרסם. ממשל זמין ייתן מענה מיטבי לצרכים התפעוליים של הגופים הממשלתיים בחיבור לאינטרנט, תוך כדי שמירה על רמת שירות גבוהה, על פי אמנת שירות שתיקבע ביניהם. עוד נקבע כי כל גוף ממשלתי המקבל שירותים מממשל זמין יזכה למעטפת שירותי הגנה מתקדמת, שתכלול, בין השאר, יכולת גיבוי באתר אחר וצוות אבטחת מידע מקצועי.

---

24 החלטה מס׳ 3573 (מט/9) של ועדת השרים לענייני מדע וטכנולוגיות מיום 15.3.98, שקיבלה תוקף של החלטת ממשלה ביום 1.4.98.

25 החלטת ממשלה ב/84 מיום 11.12.02.

עוד נקבע במדיניות החיבור לאינטרנט, כי ממשל זמין יפרסם תקנים נדרשים בכל הנוגע לאבטחת המידע הנדרשת בין מערכות המידע של הגופים הממשלתיים לרשת ממשל זמין. מנהל מערכות המידע בגוף הממשלתי ומנהל אבטחת מידע יהיו אחראים לתיאום ולעמידה בתקני אבטחת המידע שיפורסמו. תהליך יישום המדיניות יבוצע לפי הוראת שעה שתופץ מטעם המנמ"ר[26] הממשלתי. הוראת השעה תכלול את התכנית להיערכות ממשל זמין ואת היערכות הגופים הממשלתיים ליישום שיושלם עד סוף 2013.

1. **אמנת שירות (SLA - Service Level Agreemet) ונוהלי עבודה בנושא אבטחת מידע מול הלקוחות:** אמנת שירות מגדירה את רמת השירות שהספק מתחייב לתת ללקוח בגין שירותים (או מוצרים) שהוא מספק. רמת השירות מתמקדת במאפייני שירות כמו זמינות, שעות הפעלה, זמני השבתה, זמני קריאה, תפוקות, זמני תגובה וזמני סבב. למאפיינים אלה מוגדרים מדדים כמותיים, יחידות מדידה, תדירות ותקופות מדידה ואופן דיווח ללקוח, למשל, הזמן המרבי למענה טלפוני במוקד שירות לא יעלה על 30 שניות ב-90% מהמקרים. לעתים תכלול אמנת השירות גם מנגנון של פיצוי מוסכם (קנס) בגין אי-עמידה ברמת השירות או מתן פרס אם נתוני המדידה בפועל טובים מהמדד המוסכם.

מפרוטוקול ישיבת ועדת ההיגוי של ממשל זמין מנובמבר 2009 שבה הוצגה תכנית העבודה לשנים 2009-2011, עולה, כי נדרש להגדיר אמנת שירות למערך ממשל זמין באמצעות הוראות וחקיקה.

נמצא כי רק במועד סיום הביקורת פורסם ללקוחות ממשל זמין מסמך אמנת שירות, הכולל מענה לתקלות, מענה לפניות שוטפות והתחייבות על רמת זמינות, כפי שדרשה ועדת ההיגוי של ממשל זמין.

2. **הפצת דוחות ללקוחות ממשל זמין והטיפול בהם:** בשנת 2009 החל צוות אבטחת המידע של תהיל"ה להפיץ דוחות שבועיים לכל לקוחותיו. דוחות אלה כוללים, בין השאר, את הנתונים האלה: סקירות על כלי אבטחת מידע שונים כמו כלי סריקה אוטומטיים למחשבים; הערות לדוח ובהן מפורטות כתובות מכל מיני מדינות בעולם שניסו לבצע פעולות זדוניות לאתרי לקוחות תהיל"ה, כמו ניסיון להכניס פרמטרים משובשים לאתר משרד ממשלתי וסטטיסטיקות שבועיות המדרגות את הלקוחות לפי כמות ניסיונות הגישה לאתרים החשודים כערוצי שליטה של "סוסים טרויאנים"[27], ואף הצגה גרפית של הפעילות הטרויאנית לפי התפלגות הלקוחות. "סוס טרויאני" יכול להסב נזק לארגון אם יצליח להעביר מידע רגיש או עסקי של הארגון למתחריו, או בארגונים ביטחוניים לאויביו.

משרד מבקר המדינה בדק את אופן הטיפול בממצאים שעלו בדוחות השבועיים המופצים לחלק מלקוחות ממשל זמין. להלן הממצאים:

(א) לגורם ממלכתי המתארח בתהיל"ה זה כ-12 שנים קיימת רשת תקשורת מחשבים. מתחקיר שערכה מחלקת אבטחת המידע של תהיל"ה (להלן - התחקיר) עלה, כי באוקטובר 2009 נשלחו למשרדי הגורם המתארח שני נציגים של תהיל"ה לצורך איתור מחשב המכיל "סוס טרויאני" או וירוס, שאם היה חודר לשרתי ממשל זמין היה מהווה סכנה לכל הגופים המחוברים אליו. הבדיקה העלתה כי לא נשלפו נתונים פיננסיים מהמחשב או מידע רגיש אחר.

---

26 מנהל מערכות מידע ראשי, האחראי בארגון על תכנון ויישום של פתרונות טכנולוגיים שיתמכו בהשגת יעדי הארגון, על הטמעת מערכות המידע שנבחרו בתוך הארגון, ועל התפקוד התקין שלהן.

27 תכנת "ריגול" הנשתלת במחשב כשהיא מצורפת לתכנה אחרת, לרוב ללא ידיעת המשתמש, ועוקבת בחשאי אחר כל פעולות הגלישה שלו.

הווירוס שהתגלה היה אמור לחפש במחשב נתונים פיננסיים כדי להעבירם ליוצר הווירוס ולצרף אותו לרשת של מחשבים נגועים המשמשים את השולט בהם למתקפות רשת מבוזרות ולביצוע עברות מחשב שונות. ממסקנות התחקיר עלה, כי יש לבצע עדכון לתכנות האנטי-וירוס על בסיס יום-יומי, וכי תכנת האנטי-וירוס במחשב הנגוע לא עודכנה למעלה מחצי שנה; לו הייתה מעודכנת היא הייתה מונעת את חדירתו של הווירוס למחשב כבר בהגעתו. בתחקיר צוין כי קיים שימוש בהחסנים ניידים שאינם נבדקים לפני חיבורם למחשב.

במאי 2011 כתב עובד הגורם הממלכתי המתארח בתהיל"ה לצוות בקרה בתהיל"ה כי הוא אינו מצליח להתחבר לאתר אינטרנט מסוים; בכל פעם שהוא מנסה להתחבר לאתר, הוא מקבל הודעה שעליו להתקין תכנה שכבר קיימת במחשבו. הוא הוסיף שעליו לנתק את המחשב שלו מרשת התקשורת של תהיל"ה ולחבר אותו לרשת האינטרנט של אותו גורם (ADSL), כדי להיכנס לאתר הזה. בעקבות התלונה כתבה מנהלת צוות החירום בממשל זמין (להלן - מנהלת צוות החירום) באוגוסט 2011 למנמ"ר אותו גורם, שכנראה יש במערכת המחשוב שלהם "סוס טרויאני" או תכנה זדונית אחרת.

הביקורת העלתה, כי לאחר ביצוע התחקיר, באוקטובר 2009, המשיך הגורם הממלכתי להופיע בדוחות השבועיים של תהיל"ה, ובכמה מהם אף במקום הראשון, בכל הנוגע לכמות הניסיונות של תכנות זדוניות להתקשר עם יוצרן. עוד הועלה כי עד מועד סיום הביקורת עדיין לא הותקנו במערכת המחשוב של אותו גורם מערכות "הלבנה"[28] להתקני אחסון ניידים, אף שכבר הומלץ בתחקיר להגביל את השימוש בהתקני אחסון ניידים רק לאחר הלבנתם.

בהתייחסותה מנובמבר 2012 לממצאי הביקורת מסר הגורם, כי "החל מחודש אוגוסט 2012 הותקנה מערכת חדשה... לראיה אודות איכות המערכות שהותקנו, דוחות אבטחת המידע שמנפיקה תהיל"ה מציגים ירידה דרמטית בכמות התוכנות הזדוניות".

לדעת משרד מבקר המדינה, יש לנקוט פעולות זהירות ולהימנע מחיבור המחשב פעם לרשת האינטרנט ופעם לרשת תהיל"ה כדי להפחית סיכונים להחדרת וירוסים. יתרה מזאת, האירוע האמור מדגיש את החשיבות בקיומו של קובץ נהלים וסטנדרדים שעל הלקוחות למלא בעת שהם מתארחים בתהיל"ה, ומעלה את הצורך בהדרכתם של כל הנוגעים בדבר בעניין הנהלים וסטנדרדים אלה.

(ב) מבדיקה שנעשתה במאי 2012 במשרד החקלאות, בהשתתפותם של מנמ"ר המשרד, של מנהל אבטחת מידע ושל מנהל תפעול - שירות למערכות מידע, המשמש גם איש הקשר של משרד החקלאות עם תהיל"ה, עולה כי איש מן מהנוכחים לא הכיר את הדוח השבועי שתהיל"ה מפיצה.

בהתייחסותו מאוקטובר 2012 לממצאי הביקורת מסר משרד החקלאות: "עד לאותה ישיבה [מאי 2012] עם נציגי משרד מבקר המדינה, איש מבין שלושת בעלי התפקידים במשרד החקלאות לא הכיר את הדוח השבועי של תהיל"ה. עם גילוי הכשל, פנה המשרד מידית לתהיל"ה בבקשה לפעול לאלתר לתיקונו, התיקון תוקן באופן חלקי. הדוחות המלאים נשלחים למנהל השל"מ (השירות למערכות מידע) באורח שוטף וקבוע, אולם שני גורמי המקצוע האחרים (ממונה אבטחת מידע, ומנהל התפעול), מקבלים מתהיל"ה רק את הדוח הראשון [הדוח השבועי]. אנו פועלים יחד עם תהיל"ה להשלמת הטיפול בתקלה. בשלב זה המסמכים החסרים מופצים על ידי מנהל היחידה,

---

28 מערכת מחשוב הבודקת שמדיה נתיקה אינה מכילה וירוסים או תכנות זדוניות אחרות.

לממונה האבטחה, ולמנהל התפעול, ומתבצע מעקב שוטף על הנתונים, ועל האירועים הנוגעים למשרד החקלאות".

גם משרד החקלאות מופיע בדוחות השבועיים של תהיל"ה כמי שיש במערכת המחשוב שלו וירוסים.

(ג) מבדיקה שנעשתה במשרד התחבורה במאי 2012, בהשתתפותו של איש הקשר לתהיל"ה האחראי למערכות ההפעלה במשרד, עולה כי הטיפול בדוחות תהיל"ה כולל איתור התחנה החשודה, פירמוטה[29] או ניתוקה מרשת האינטרנט. משרד התחבורה אינו מדווח בכתב לתהיל"ה על אופן הטיפול בווירוס, והוא מטפל באירועים באופן מקוון. עוד עולה כי אף על פי שהותקנה מערכת בקרה על התקני אחסון נתיקים, ואף מצוין שאסור להכניס למערכת המחשוב התקני אחסון נתיקים לא מוצפנים או לא מאושרים על ידי המשרד, עדיין מוכנסים התקנים כאלה שלעתים נגועים בווירוסים.

גם משרד התחבורה מופיע בדוחות השבועיים של תהיל"ה כמי שיש במערכת המחשוב שלו וירוסים.

(ד) מבדיקה שנעשתה במשרד המשפטים במאי 2012, בהשתתפותם של מנמ"ר המשרד, של יועץ אבטחת מידע חיצוני ושל נציג אבטחת המידע ומנהל הטכנולוגיות במשרד, עולה כי הטיפול בדוחות תהיל"ה נעשה על פי האירועים. לדוגמה, לפני כשנה וחצי נמצא "סוס טרויאני" בשני מחשבים ניידים, והם פורמטו. לאירוע הזה לא כתבה מחלקת מערכות מידע דוח טיפול.

גם משרד המשפטים מופיע בדוחות השבועיים של תהיל"ה כמי שיש במערכת המחשוב שלו וירוסים.

(ה) מבדיקה שנעשתה במשרד להגנת הסביבה ביוני 2012, בהשתתפותו של איש הקשר לתהיל"ה, עולה כי הוא מקבל פעם בחודש דוח ובו חשד לווירוסים. איש הקשר ציין כי אין נוהל מסודר בעבודה מול ממשל זמין בנושא זה.

גם המשרד להגנת הסביבה מופיע בדוחות השבועיים של תהיל"ה כמי שיש במערכת המחשוב שלו וירוסים.

בהתייחסותה מנובמבר 2012 לממצאי הביקורת מסרה הנהלת ממשל זמין, כי "יש לציין כי האחריות על ניהול המערכות ואבטחת המידע בכל משרד ומשרד הינה על מנמ"ר המשרד ולממשל זמין אין כל סמכות להתערב בנעשה בתוך הרשת המשרדית".

לדעת משרד מבקר המדינה, מן הראוי שהנהלת ממשל זמין תקבע מתכונת דיווח לגופים המתארחים בתהיל"ה על ניסיונות חדירה לאתריהם. עוד מוצע כי בנוהל שייקבע יפורטו, בין היתר, הפעולות שעל המשרד המתארח בתהיל"ה לבצע בעקבות קבלת הדיווח, וכן הגורמים שהוא נדרש לדווח להם על הפעולות שעשה ועל תוצאותיהן.

3. ניהול מאגרי מידע של גופים ציבוריים המתארחים בממשל זמין

בחוק הגנת הפרטיות נקבע כי המחזיק במאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשה במפורש לעשות זאת בהסכם בכתב בינו לבין בעליו של אותו מאגר. עוד נקבע כי מחזיק שברשותו לפחות חמישה מאגרי מידע החייבים ברישום, ימסור לרשם מדי שנה בשנה רשימה של מאגרים אלה בצירוף שמות בעליהם, תצהיר על כך שנקבעו בעלי

---

29 התקנה מחדש של קובצי מערכת ההפעלה על ידי מחיקת כל הכונן או חלק ממנו (מחיצה).

זכות הגישה לכל אחד מהמאגרים בהסכם שנקבע בינו לבין בעליו, וכן שמו של הממונה על האבטחה.

בחוק הגנת הפרטיות מוגדר מאגר מידע כ"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב"[30]. "מידע רגיש" מוגדר כ"נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו" וכל מידע ששר המשפטים קבע בצו, באישורה של ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש.

בממשל זמין קיימים מאגרי מידע של הלקוחות השונים הכוללים מידע רגיש. לדוגמה, בשירות הטפסים הממשלתי נאגרים מאות טפסים שונים של משרדים, המכילים מידע על אזרחים. למשל, טופס בקשה להקלה ולתיאום בחישוב ניכויי מס מכיל מידע רגיש על אזרחים ומצבם הכלכלי; טופס בקשה לתעודת עיוור או לקוי ראייה מכיל פרטים אישיים ומידע על מצבו הבריאותי של האזרח; טופס פנייה למפקח על הביטוח שבמשרד האוצר מכיל נתונים אישיים של הפונה ויכול להכיל נתונים על מצבו הכלכלי.

בנוהל מדיניות אבטחת המידע של ממשל זמין נקבע בעניין התאמה לדרישות שעל פי דין כי כל הדרישות הרלוונטיות על פי חוק, יוגדרו במפורש, יתועדו וייושמו בעבור כל המערכות והיישומים של ממשל זמין. הגנה על הנתונים ושמירה על הפרטיות יובטחו כנדרש מתוקף הוראת חוק הגנת הפרטיות. בקרות הצפנה ייושמו לפי כל ההסכמים, החוקים והתקנות הרלוונטיים.

הביקורת העלתה כי לממשל זמין אין הסכם עם אף לא אחד מלקוחותיו, שלהם מאגר מידע כהגדרתו בחוק הגנת הפרטיות, המגדיר מי הם מורשי הגישה למאגרי המידע שלהם כנדרש בחוק הגנת הפרטיות. ממשל זמין גם לא מסר דיווח שנתי לרשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים כנדרש בחוק זה, בתוקף היותו מחזיק במאגרים של בעלים שונים.

משרד מבקר המדינה מעיר להנהלת ממשל זמין, כי עליה לקיים את הוראות חוק הגנת הפרטיות ותקנותיו בכל מאגרי המידע שממשל זמין מחזיק בהם; למשל, שרת הטפסים שבו מאגרי מידע של משרדי הממשלה השונים, המכילים מידע רגיש על אזרחים.

יישום מסקנות של דוחות בדיקה ושל אירועי אבטחת מידע

1. **דוח הרשות הממלכתית לאבטחת מידע**: 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 כתשתית חיונית המונחית על ידי רא"ם. במסגרת הפעילות המשותפת של מערך ממשל זמין, משרד האוצר ורא"ם הקימו ועדת היגוי לעניין תחומי אחריותה של רא"ם בתהיל"ה (להלן - ועדת היגוי משותפת). במרץ 2011 ערכה רא"ם, אשר החלה לפעול כרגולטור מול תהיל"ה, ביקורת מיפוי בתהיל"ה, וסיכמה את ממצאיה בדוח (להלן - דוח רא"ם). הביקורת של רא"ם התמקדה במיפוי ובבחינה של נכסי המידע, והתהליכים בתהיל"ה.

---

30 "למעט - (1) אוסף לשימוש אישי שאינו למטרת עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף".

ממצאי דוח רא"ם עולה כי מדיניות האבטחה ותפישת האבטחה בתהיל"ה נותנות מענה טוב לאיומים הקיימים. עם זאת נמצאו בתהיל"ה כמה היבטים המצריכים בחינה: היבטי האבטחה הלוגית, האבטחה הפיזית, ההתאמה הביטחונית, כללים ותהליכים; וכן ההיערכות לחירום.

הדוח העלה, בין היתר, כי אין תכנית הדרכה ותהליך מוסדר ומחזורי להגברת מודעות העובדים לנושא אבטחת המידע. בעקבות ממצאי הדוח הוציאה רא"ם ביולי 2011 הנחיות מפורטות לטיפול בליקויים שהועלו בדוח. ההנחיות נחלקו להנחיות לביצוע מידי (עד סוף שנת 2011) ולהנחיות לביצוע לפי תכנית ההטמעה הרב-שנתית (להלן - תכנית ההטמעה) של תשתית מידע קריטי בתהיל"ה.

מסיכום דיון של ועדת ההיגוי המשותפת מפברואר 2012, שעסק בפעילויות שנעשו בעקבות דוח רא"ם בשנת 2011 ובפערים שנותרו ביישום אבני דרך של תכנית ההטמעה, עולה גם שבאותה עת עדיין לא הועברו כל טופסי הסיווג החתומים על ידי העובדים בתהיל"ה, וכן נדרש להשלים את כתיבת המסמכים המתעדים את המערכות הקריטיות, שאמורים היו להיות כתובים עד סוף שנת 2011. עוד עולה ממצגת שהוצגה בדיון, כי יש חריגות בביצוע משימות במסגרת ההנחיה של רא"ם.

משרד מבקר המדינה בדק את תיקון הליקויים שהועלו בדוח רא"ם. הביקורת העלתה כי כמה מהליקויים, שהיה צריך לתקנם עד סוף שנת 2011, טופלו חלקית בלבד או לא טופלו כלל. לדוגמה, בדיקות להתאמה ולסיווג של העובדים טרם הושלמו; מסמך מדיניות אבטחת המידע טרם עודכן באופן שיכלול את כל המערכות והרשתות בתהיל"ה; והגדרת הגבלת גישה בערכות שליטה ובקרה נעשתה באופן חלקי בלבד.

עוד עלה כי יש חריגות מלוחות הזמנים שנקבעו בתכנית ההטמעה. למשל, במועד סיום הביקורת, ביולי 2012, עדיין לא קיים ממשל זמין את הפעילויות הנכללות בתכנית ההטמעה שנקבעו לביצוע עד סוף ינואר 2012, ובכלל זה: לא נערך תרגיל חירום, וממילא לא הופקו ממנו לקחים, ולא נערך במלואו מיפוי המערכות הקריטיות. כמו כן נמצא, כי כמה מהפעילויות נעשו באופן חלקי בלבד: כתיבתו והפצתו של מסמך מדיניות אבטחת תשתית מידע קריטי נמצא בשלב טיוטה לאחר הערות.

בהתייחסותה מנובמבר 2012 מסרה הנהלת ממשל זמין, כי "החלק האחרון בסקר הערכת הסיכונים הסתיים בחודש אוגוסט 2012... כמו כן סיווג המשרות הושלם אך ... [חלק מסוגיות הביטחון] ... עדיין בטיפול באמצעות אגף חירום ובטחון".

2. **מבדקים לתקן ישראלי 27001**: בהצהרת מדיניות אבטחת מידע מאוגוסט 2007 הצהירה הנהלת ממשל זמין על הקמת מערכת ניהול אבטחת איכות ומידע שתעמוד בדרישות תקן 27001. בשנת 2008 אישר מכון התקנים הישראלי את ממשל זמין כמי שעומד בדרישות תקן זה, והוא עובר מבדקי מעקב שנתיים, על ידי חברה פרטית, כדי לבדוק את עמידתו בהוראות התקן. במבדק שנערך באפריל 2009 נקבע, כי המבדק הבא יהיה במרץ 2010. בפברואר 2011 קיבל ממשל זמין לראשונה תעודת הסמכה לתקן למשך שלוש שנים.

בנוהל "סקר הנהלה" של ממשל זמין נקבע כי סקרי הנהלה ייערכו פעמיים בשנה או בעת שחלים שינויים ניכרים. סקר הנהלה הוגדר בנוהל כדיון תקופתי שמטרתו סקירת מערך אבטחת המידע בממשל זמין והתאמתו לתקן 27001, לנהלים ולחוקים. עוד נקבע בנוהל כי באחריות ועדת ההיגוי לאבטחת מידע להתוות את עקרונות האבטחה של ממשל זמין ולסקור ולבקר את פעולותיו של ממשל זמין בתחום ניהול אבטחת מידע. בנוסף לזאת נקבע, כי ועדת ההיגוי תתכנס לפחות פעמיים בשנה. על מנהל אבטחת מידע לבקר ולאכוף יישום הנחיות נוהל זה.

הביקורת העלתה כי למעט סיכום ישיבה אחת בנושא סקר הנהלה, שהתקיימה בנובמבר 2010, לא נמצאו מסמכים המעידים על קיום סקרי הנהלה בשנים 2009-2012. כמו כן לא נמצאו מסמכים המעידים על כך שההחלטות שהתקבלו בסקר ההנהלה מנובמבר 2010 והיו אמורות להתבצע עד סוף 2011, אכן יושמו. עוד הועלה, כי לא נערך מבדק בשנת 2010 לשנת 2009.

3. **דוחות חדירה למערכת ניהול ותיעוד הרכש הממשלתי (להלן - מנור"ה)**: פרויקט מנור"ה החל בשנת 2008 במטרה ליצור מערכת תשתית טכנולוגית לניהול מקוון של מכרזים ממשלתיים. מערכת זו נועדה לאפשר למשרדי הממשלה לנהל באופן מקוון את השלבים הפנים-ממשלתיים של המכרז, משלב הייזום ועד שלב ההתקשרות עם הספק. באמצעות מנור"ה יכולים קניינים במשרדים הממשלתיים לפרסם מכרזים ישירות למציעים הממשלתיים, ובעצם, לבטל את הצורך בהגעה פיזית לכל אחד משלבי המכרז ולחסוך בעלויות ובשעות עבודה. פיתוח הפרויקט החל באפריל 2009, ונכון למועד סיום הביקורת כמאה מכרזים פעילים במערכת מנור"ה.

ביולי 2011 נכנסה לתוקף הוראת תכ"ם[31] בדבר ניהול הליכים במערכת מנור"ה, ופריסתה החלה בכל משרדי הממשלה וביחידות הסמך. בהוראה נכתב כי המערכת נוקטת, באורח סדיר, אמצעי הגנה סבירים מפני חדירה ומפני שיבוש בעבודתה העלולים לפגום במהימנות המידע שבה. מטרת ההוראה היא "להנחות בעלי תפקידים במשרדי ממשלה בניהול מכרזים ממוכנים במערכת מנור"ה".

למערכת מנור"ה נערכו מבדקי חדירה על ידי גורם ממלכתי (להלן - דוח חדירות). מטרת הבדיקה הייתה להעריך את רמת החסינות של מנור"ה ביחס לאיומי לוחמת מידע ולזהות כשלי אבטחה. מדוח החדירות עולה כי התגלו בעיות המוגדרות כסיכון לתהליכים המבצעיים העיקריים ברשת.

גם צוות אבטחת המידע של ממשל זמין ערך בדיקה לפרויקט מנור"ה. מדוח הצוות עלה, כי לא כל הבעיות שדורגו בעדיפות גבוהה תוקנו בהצלחה, ויש לערוך בדיקות חוזרות כדי לוודא פתרון לכלל הבעיות שהתגלו בה. עוד עלה בדוח כי לא כל החשיפות לסיכונים תוקנו במערכת מנור"ה.

בהמשך נתן מנהל אבטחת מידע בממשל זמין אישור זמני להפעלת מערכת מנור"ה. באישור נכתב כי כל הליקויים שאנשי המערכת התחייבו לתקן בדוח צוות הבדיקה של ממשל זמין תוקנו לפי הדרישה. שאר הליקויים שנמצאו בבדיקה יתוקנו על פי תכנית העבודה. בגמר התיקונים שוב תיבדק המערכת כדי לתת אישור אבטחה על כלל המערכת.

חצי שנה לאחר מכן ערך צוות הבדיקה של ממשל זמין בדיקה נוספת. בבדיקה עלה, כי לא כל הבעיות שדורגו בעדיפות גבוהה תוקנו בהצלחה. כמו כן נמצאו חשיפות חדשות שלא עלו בדוח הקודם.

משרד מבקר המדינה העלה, כי מנור"ה הופעלה במרץ 2010 למרות הימצאותן של בעיות במערכת בתחום אבטחת המידע. אישור זמני להפעלת המערכת, שנתן מנהל אבטחת מידע כשנה וחצי לאחר שהמערכת הופעלה ולאחר שנוהלו בה תשעה מכרזים - ניתן אף על פי שלא כל הבעיות במערכת טופלו.

משרד מבקר המדינה מעיר להנהלת ממשל זמין, כי עליה להקפיד על ביצוע בדיקות מעשיות של תיקון הליקויים. כמו כן על מנהל אבטחת מידע להעניק את אישור אבטחת המידע להכנסת כל פרויקט בממשל זמין לשלב הייצור, רק לאחר בדיקה שכל סיכוני אבטחת המידע הוסרו.

---

31 הוראה 7.22.1.

4. **שליפת עותקי טופס ממשלתי**: בספטמבר 2011 ראתה מנהלת צוות החירום בממשל זמין ניסיונות להוריד עותק של טופס ממשלתי ללא תשלום. הממונה על אבטחת מידע במשרד המשפטים, שעודכן בפרטי המקרה ממנהלת צוות החירום, הגיש תלונה במשטרה בעניין זה.

באפריל 2012 כתב הממונה על אבטחת מידע במשרד המשפטים למנהלת האגף הרלוונטי כי החשוד הציג בחקירתו אישורי תשלום לכל עותקי הטופס לצפייה שהיו במחשבו בתקופת התלונה. כמו כן נבדקה התכנה שבנה החשוד לשליפת הטופס באופן אוטומטי. מהבדיקה עולה כי לצורך שליפת מידע יש להזין, בנוסף להזנת פרטים מסוימים, גם מספר אסמכתה לתשלום. לנוכח הממצאים החליטה משטרת ישראל לסגור את התיק. לשאלת הממונה על אבטחת מידע במשרד המשפטים בנוגע למסמכים היסטוריים שלאו דווקא הוצאו בתקופת החקירה ונמצאו במחשב, השיבה המשטרה כי הם לא חקרו את הנושא כיוון שאין הם יכולים לסנכרן את המידע מול תהיל"ה, מפני שבתכנה שבנה החשוד נדרש להכניס מספר אסמכתה לאישור תשלום.

מנהלת האגף מסרה לצוות הביקורת, כי לפי דרישת משרד המשפטים קיימת אפשרות לאחזר עותק הטופס ואישור תשלום עד 48 שעות לאחר הרכישה המקוונת. אולם היא לא מצאה מסמכים המעידים על דרישה זו.

משרד מבקר המדינה מעיר להנהלת ממשל זמין על כך, שבמשך כמעט שנה לא נפגשו נציגיה עם נציגי משרד המשפטים כדי למצוא פתרון לבעיה זו, וזאת לנוכח החשד לחדירה המאפשרת לשלוף העתקי טפסים ללא תשלום ולנוכח הניסיונות להתקשר עם מזמיני הטופס המקוריים, כפי שבוצעו בספטמבר 2011. כמו כן, מן הראוי שיהיו בידי ממשל זמין כל המסמכים הנוגעים לכל דרישות לקוחותיו משירות הפקת האישורים. לדעת משרד מבקר המדינה, יש מקום כי אירוע זה יידון בוועדת ההיגוי לאבטחת מידע ויופקו הלקחים המקצועיים מהמקרה.

5. **אבטחת מידע במערכת ממוחשבת**: אחד מתת-הפרויקטים הכלולים בממשל זמין הוא מערכת ממוחשבת המאפשרת לאזרחים לבצע תשלומים ולקנות מוצרים באמצעות האינטרנט. תת-פרויקט זה עלה לאוויר בנובמבר 2001. לפי אתר השירותים והמידע הממשלתי, נכון ליוני 2011, ניתן היה לשלם באמצעותו 186 סוגי תשלומים ל-39 גופים ומשרדים ממשלתיים - אפשרות לתשלום בשוברי תשלום, אפשרות לתשלום אגרות, כמו רישיון רכב או רישיון נהיגה, ואפשרות לרכישת מוצרים. כאמור, בשנת 2011 שולמו באמצעותו כ-17 מיליארד ש"ח בכ-3.4 מיליון עסקאות.

במהלך דצמבר 2011 נערך סקר על ידי חברה חיצונית על המערכת, שכלל מבדק חדירה[32]. מהסקר עלה, כי במערכת קיימים סיכונים מהותיים העלולים לגרום נזק ללקוחות הארגון ולתדמיתו.

התברר כי סקר זה על ממצאיו לא נדון בוועדת ההיגוי של ממשל זמין, ולא נעשתה כל בדיקה חוזרת לתיקון הליקויים.

בהתייחסותה מנובמבר 2012 לממצאי הביקורת מסרה הנהלת ממשל זמין, כי הממצאים שהועלו תוקנו, אך לא נערכה בדיקה חוזרת מפאת חוסר משאבים.

---

32 מבחנים שמטרתם לבדוק את חוסן אבטחת המידע של מערכת מחשוב או של כלל הארגון.

נוהלי החלטה וטיפול בהעברות מידע חריגות במערכת

בנוהל מדיניות אבטחת המידע בממשל זמין נקבע כי פעילותו התקינה של ממשל זמין מושפעת ותלויה, בין השאר, בזמינות המידע ובשרידותו, ויש להתוות ולייעד מדיניות זו לצמצום הפגיעה במידע, במאגריו ובמערכותיו, ומתוך כך לצמצם את סיכוני הפגיעה בתפעולו הסדיר של ממשל זמין, וכפועל יוצא גם במקבלי השירות.

אשר לטיפול באירועי אבטחת מידע חריגים נקבע במסמך המדיניות כי לכל פעילות חריגה בעלת השלכות על אבטחת המידע יוגדר אופן רישומה, הדיווח עליה ואופן התגובה הנדרש. חריגות בתחום אבטחת המידע, שמאתרים גורמי ממשל זמין או אחרים, ידווחו לצוות אבטחת מידע או למנהל הרלוונטי. הנהלת ממשל זמין תגיב על אירועי אבטחת מידע חריגים. אירועי אבטחת מידע חריגים, ידווחו לוועדת היגוי לאבטחת המידע.

ישנן כל מיני דרכים לתקוף את אתר ממשל זמין, ובהן מניעת שירות (Denial Of Service - הפסקה פתאומית של שרתי האתר עקב עומס פניות (להלן - מניעת שירות), והשחתת עמוד האינטרנט של הארגון (Defacing) באופן שוטף. לפי הסיכונים הנובעים מהתקפות אלה נדרשים לעתים אנשי ממשל זמין להחליט על חסימת הגישה לכתובות אינטרנט שמהן מגיעות התקפות אלה לאתר של ממשל זמין.

צוות החירום בממשל זמין עוסק במתן מענה מידי לאירועי אבטחת מידע בארגונים ממשלתיים. צוות זה מורכב מעובדים, ומשמש מוקד מענה זמין לכל תופעה של תקיפות ברשת שהם אמונים עליה ולכל הקשור לניהול סיכונים, ליצירת נוהלי אבטחת מידע, לבקרת תעבורה, להתפרצויות וירוסים, למניעת דואר זבל, לפיראטיות ברשת, לזיוף זהויות, לשמירה על פרטיות המידע, להגברת המודעות האבטחתית ולשיתוף ועדכון של ספקי אינטרנט, של גופים צבאיים, של גופים משטרתיים, של השירות החשאי ושל מקביליהם בעולם בתופעות חדשות בתחומים אלה.

1. **עתירת חברה ג׳**: בנובמבר 2011 הגישה חברה ג׳ עתירה לבג״ץ נגד שר המשפטים בגין שיבוש גישה לאתרי האינטרנט של משרד המשפטים וחסימתה. בכתב התגובה מינואר 2012 שהגישו נציגי הממשלה צוין, בין השאר, כי באוקטובר 2011 תועדו בממשל זמין יותר מ-80,000 שאילתות לאתר המשרדי של מחלקת סימני מסחר ברשות הפטנטים. השאילתות בוצעו באופן עקבי ורציף על ידי רובוט[33] של חברה ג׳ והיו בעלות קווי מתאר של תקיפה מקוונת מסוג מניעת שירות. למניעת מצב זה הותקנה במערכות ההגנה של ממשל זמין מערכת ניטור תוכן שחסמה לסירוגין את הרובוט. בדצמבר 2011 הותקן מנגנון אתגר-מענה שמטרתו להבטיח כי התשובה המוזנת אינה מופקת על ידי מחשב (CAPCHA), וחסימת הרובוט הוסרה. בעקבות השינויים ביקשה העותרת ארכה כדי לבחון את האמצעים החדשים שהמשיבים מפעילים. בנסיבות האמורות הוחלט למחוק את העתירה.

הביקורת העלתה, כי במועד חסימת גישת כתובת האינטרנט של חברה ג׳ לשרתי ממשל זמין לא היה נוהל לטיפול במתקפות מן הסוג של מניעת שירות. במאי 2012 פרסמה מחלקת אבטחת מידע טיוטת נוהל תפעולי שכותרתו ״פעולות לביצוע בעת מתקפת מניעת שירות״. התברר שעד למועד סיום הביקורת לא אישרו לא מנהל אבטחת מידע ולא ועדת ההיגוי לאבטחת מידע את טיוטת הנוהל.

---

33 תכנת מחשב המותקנת בשרתיה של העותרת ומתחברת באמצעות האינטרנט אל אתרי משרד המשפטים, מגישה להם שאילתות של מספרי חברה וסימני מסחר, מקבלת תוצאות ומשלבת אותן יחד באתרים של העותרת, בצירוף מידע ממקורות נוספים.

2. **חסימת דואר אלקטרוני:** באוגוסט 2011 חסם ממשל זמין את הגישה מכתובות אתר אינטרנט של ארגון עולמי העוסק בפרסום מקוון, עקב חשד למתקפה מסוג SMTP[34] על שרתי הדואר האלקטרוני שלו. מתכתובות בדואר אלקטרוני מאוגוסט 2011 בין מנהלת צוות החירום לנציגי הארגון עולה כי מכתובות האינטרנט של הארגון התבצעו יותר מ-250,000 חיבורים בשעה לשרת הדואר של ממשל זמין, והן נחסמו.

נציגת הארגון כתבה למנהלת צוות החירום כי הארגון הופתע לגלות ששליחת הודעות דואר אלקטרוני לחברי הכנסת נחסמה ומוגדרת כמתקפת "דואר זבל" (SPAM)[35]. מנהלת צוות החירום השיבה כי ממשל זמין ישמח להסיר את החסימה לשרתי הארגון אם הוא יתחייב שהמתקפה לא תחזור על עצמה. באותו החודש העבירה מנהלת צוות חירום את כל התכתובות שלה עם נציגת הארגון לאחת מהיועצות המשפטיות של משרד האוצר.

בינואר 2012 פנתה נציגה אחרת של הארגון לממשל זמין וטענה כי כתובותיהם נחסמו לחלוטין, והם אינם יכולים לשלוח הודעות לתיבות הדואר האלקטרוני של אנשי ממשל בישראל ואף לממשל זמין עצמו. מנהלת צוות החירום ענתה לה, כי כתובת הארגון אינה חסומה לשליחת דואר אלקטרוני והמערכת לסינון דואר עוצרת אוטומטית כמויות חריגות של דואר כדי למנוע עומס יתר על המערכת. עוד כתבה המנהלת כי לדעתה שליחת 50,000 הודעות בשעה אינה לגיטימית, והארגון מתבקש לבצע את הקמפיינים שלהם בתבונה ובהתחשבות ביכולות הניהול והעיבוד של שרתי הדואר.

הביקורת העלתה, כי אין בממשל זמין נוהל לטיפול בהתקפות מסוג זה, ואף לא מוגדרת מהי הכמות הסבירה למשלוח דואר אלקטרוני מכתובת אינטרנט בפרק זמן נתון. עוד עלה, כי בשני המקרים שנחסמו כתובות אינטרנט לא ניתן ייעוץ משפטי לפני ביצוע החסימה, ולא התקבלה כל התייחסות בכתב מהייעוץ המשפטי לפנייתה של מנהלת צוות החירום. כמו כן, אירועים אלה לא הובאו אל שולחנה של ועדת ההיגוי, ולא נכתב עליהם דוח מסכם כנדרש בנוהל מדיניות אבטחת מידע.

לדעת משרד מבקר המדינה, על מנהל אבטחת מידע ועל ועדת ההיגוי לכתוב ולתקף נוהלי אבטחת מידע תפעוליים לטיפול במצבי חירום היכולים להתרחש בממשל זמין, וכפי שכבר החלו לעשות. בנהלים יש להגדיר, בין השאר, את הסיכונים מהתקפות שונות ואת דרכי ההתמודדות עמם, ולקבוע הוראות ביצוע לצוותים המטפלים. כמו כן יש לבחון את ההחלטות לחסום כתובת דואר אלקטרוני גם מההיבט המשפטי לפני ביצוען ולא בדיעבד.

היבטים נוספים של פעולות אבטחת מידע בממשל זמין

הדרכות והכשרות של עובדים בתחום אבטחת מידע: הדרכת עובדים, ובייחוד עובדים חדשים, בנושאי אבטחת מידע נדרשת, כדי להבטיח מודעותם של עובדי הארגון לקיומם של גורמי סיכון בשימוש במערכות המידע ולחשיבות הפעולות לאבטחת המידע בארגון.

---

34 Simple Mail Transfer Protocol - בהתקפה מסוג זה נשלחות הרבה מאוד פניות לשרת הדואר כדי להאט את שירותיו או להפסיקם.

35 דואר אלקטרוני הנשלח בכמויות היכולות להגיע למיליונים, ללא כל אישור או בקשה של הנמענים.

בנוהל "מודעות לנושאי אבטחת איכות ומידע" של ממשל זמין נקבע, בין השאר, כי מנהל אבטחת המידע ישא באחריות לבקרת ביצוע הנחיות הנוהל ולעדכונו. כמו כן עליו להגיש בתחילת כל שנה תכנית הדרכה כוללת להגברת מודעות העובדים בכל ההיבטים הנוגעים לאבטחת איכות ומידע. עוד נקבע בנוהל כי כל עובד ממשל זמין ישתתף בהדרכה בתחום אבטחת איכות מידע, לפחות אחת לשנתיים, לרבות רענון הנהלים הרלוונטיים בתחום זה. המדריך יתעד את העברת ההדרכה בטופס מעקב הדרכות המצורף לנוהל. תכנית העבודה השנתית להגברת המודעות וטופס המעקב יתויקו בתיק ייעודי ויישמרו במשרד מנהל אבטחת מידע למשך שלוש שנים לפחות. עוד נקבע כי מנהל אבטחת מידע אחראי להדרכתו של כל עובד חדש בנושאי אבטחת מידע ולתדרוכו של כל עובד שעוזב את הארגון בכל הקשור להתחייבותו לשמירת חיסיון המידע שנחשף בפניו.

בנוגע להדרכה ולהטמעה של אבטחת מידע נקבע בנוהל מדיניות אבטחת מידע כי מנהל אבטחת מידע יפעל להטמעת הנושא בכל מערכי המחשוב בסביבות העבודה בכלל ובמערכי התקשוב ובאמצעי העבודה הקשורים לאבטחה פיזית ולאבטחת רשומות בפרט. מנהל אבטחת מידע יפעל להגברת המודעות לנושא בקרב עובדי ממשל זמין, ממשקיו וגורמים אחרים בעלי נגישות למידע.

הביקורת העלתה כי מנהל אבטחת מידע בממשל זמין אינו מקיים את כל הוראות הנוהל. לדוגמה, הוא לא גיבש תכנית הדרכה כוללת להגברת מודעות העובדים בכל ההיבטים הנוגעים לאבטחת מידע; לא נמצא תיק ייעודי ובו מתויקים תכנית העבודה השנתית להגברת המודעות וטופס המעקב; נושא נוהלי אבטחת מידע אינו מופיע במצגות של הדרכות העובדים; ומנהל אבטחת מידע אינו מעודכן בנוגע לעובדים חדשים בממשל זמין, וממילא אין הם מקבלים את ההדרכה הנדרשת לפני קבלת הרשאות גישה.

לדעת משרד מבקר המדינה, מן הראוי שהנהלת ממשל זמין תיישם את פעולות ההדרכה בתחום אבטחת המידע לפי הקבוע בנוהל מודעות לנושאי אבטחת איכות ומידע, לרבות גיבוש תכנית הדרכה שנתית. כמו כן, על מנהל אבטחת מידע להקפיד ולנהל באופן קבוע את רישום ההדרכות כנדרש בנוהל, וזאת לצורך ניהול מערך ההדרכה ומעקב אחריו.

סיכום

אבטחת מידע היא אבן יסוד בפעילותו של ממשל זמין, ומשום כך עליו להעלות את הנושא לראש סדר עדיפויותיו. כספק העיקרי של תשתיות מחשוב ושל שירותי מחשוב למשרדי ממשלה ולגופים ציבוריים, נדרש ממשל זמין לקיים פעילות מלאה ושוטפת בתחום אבטחת המידע במטרה למנוע פגיעה בזמינות המידע הממשלתי לציבור.

ממצאיו של דוח זה מלמדים על כך שממשל זמין לא יישם בהיבטים שונים הוראות ונהלים בתחום אבטחת המידע ובכך גדלה רמת הסיכון לפגיעה בתשתיות המחשוב ובשירותי המחשוב למשרדי ממשלה וגופים ציבוריים.

לנוכח הליקויים שהועלו בדוח נדרשת הנהלת ממשל זמין לנקוט כמה וכמה פעולות. עליה לקבוע את הסיכונים הנשקפים לכל הפרויקטים בממשל זמין ואת רמת הסיכון הנשקפת מכל אחד מהם; אין להכפיף את מנהל אבטחת מידע בממשל זמין באופן שיפגע בעיקרון אי-התלות שלו; יש ליישם תכניות התאוששות מאסון והמשכיות עסקית בכל הנוגע לתשתית המידע הקריטי שלו, ולבדוק ולתרגל במלואן את ישימותן הן מהבחינה הטכנולוגית והן מהבחינה האנושית. כמו כן, מומלץ שממשל זמין ייקבע קובץ נהלים לגופים הציבוריים המתארחים בו שלפיהם עליהם לפעול. על הנהלת *ממשל זמין* לבצע את פעולות ההדרכה הדרושות בתחום אבטחת מידע, לרבות הכנת תכנית הדרכה שנתית ומימושה, וכן בקרה על מידת הטמעתן של ההוראות וההנחיות בתחום זה.