

תאריך: 20/03/2014

לכבוד חה"כ גדעון סער, שר הפנים
רח' קפלן 2, ירושלים 91950

הנדון: המערך הביומטרי – אי-עמידה בתקני אבטחה

שלום רב,

סעיף 10א(א) לצו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע (תקופת מבחן), התשע"א-2011 (להלן, צו המבחן), קובע כי אין להתחיל את תקופת המבחן בטרם יודאו רשות האוכלוסין וההגירה והרשות לניהול המאגר הביומטרי (להלן, הרשות הביומטרית), כי כלל מערכי הטכנולוגיה, התפעול והמערך הביומטרי, עומדים בתקני האבטחה המחמירים לפי הנחיות הרשות הממלכתית לאבטחת מידע של שירות הביטחון הכללי (להלן, רא"ם):

רשות האוכלוסין [וההגירה] והרשות [לניהול המאגר הביומטרי] יודאו טרם תחילת תקופת המבחן כי כל מערכי הטכנולוגיה, התפעול והמערך הביומטרי למימוש מטרות תקופת המבחן עומדים בתקנים וברמת האבטחה של הרשות הממלכתית לאבטחת מידע במשרד ראש הממשלה ושל נוהלי רשות האוכלוסין והרשות.

ביום 14/07/2013, פנינו אליך ואל שרת המשפטים בשל התעוררות חשש ממשי בדבר עמידת המערך הביומטרי והמערכים הנלווים בתקני אבטחת מידע הנדרשים לפי צו המבחן והנחיות רא"ם. ביום 28/08/2013, קיבלנו מענה חלקי ממר יוגב שמני, מנהל אגף מערכות מידע ברשות האוכלוסין וההגירה, אשר פסק כי טענותינו אינן מבוססות, וכי מקורן, לדבריו, "[ב]חוסר הבנה לגביי יישום חוק הביומטריה (התש"ע 2009)¹ בכלל וחשיבותם של היבטי אבטחת המידע בפרט". (רצ"ב מכתבנו מיום 14/07/2013 ותשובת רשות האוכלוסין וההגירה מיום 28/08/2013).

ביום 04/02/2014, פרסמה הרשות הביומטרית דו"ח תקופתי למחצית השנייה של שנת 2013², ממנו עולה כי חששותינו לא היו מופרכים כלל וכלל, וכי ההנפקה החלה תוך הפרה חמורה של דרישות האבטחה האמורות בצו המבחן.

א. תקני אבטחת מידע – רמת האפיון ורמת הבדיקות

כל תקן אבטחה מודרני³ מכתוב התייחסות בשתי רמות: רמת האפיון, ורמת הבדיקות הנדרשות כדי לוודא עמידה באפיון. ברמה הראשונה, התקן מכתוב אפיון של **תצורת המערכת**, כגון תקן חומרה, אבטחה פיזית, מנגנוני בקרה, הפרדת מערכות וכדומה. ברמה השנייה, התקן מכתוב **בדיקות הכרחיות**, הכוללות בין השאר **ביצוע סקרי סיכונים וביצוע מבדקי חדירות**. בנוסף, כאשר מתגלים ליקויי אבטחה ("פערים"), התקן דורש את תיקונם בלוחות זמנים הנגזרים מחומרתם.

ניתן להקביל את תקן האבטחה לאפיון מערך שמירה בבסיס צבאי. ברמה הראשונה, האפיון מגדיר את התצורה "על הנייר": תקן בנייה של הגדר, טווחי ביטחון, תקני כ"א, סדרי שמירה וכדומה. ברמה השנייה, האפיון דורש בחינה ע"י גורם מקצועי חיצוני (סקר סיכונים), וכן עריכת ביקורות פתע (מבדקי חדירות). בנוסף, האפיון דורש כי אם מתגלה פרצה בגדר, היא תטופל מיידית.

דרישות האבטחה של רא"ם מתחלקות גם הן לרמת האפיון ולרמת הבדיקות. כדי שהמערך הביומטרי יעמוד בדרישות, רא"ם צריכים לספק אישור כפול: ראשית, אישור כי התצורה (המתוכננת) של המערכת מסוגלת לספק את רמת האבטחה הנדרשת. שנית, אישור כי המערך עצמו נבדק ונמצא בטוח – לאחר עריכת סקר סיכונים ולאחר שעמד במבדקי חדירות מקצועיים.

1 כוונתו לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009.
2 בהתאם לסעיף 13 לצו המבחן, תקופת הניסוי החלה ביום 01/01/2013. הרשות הביומטרית לא הייתה מוכנה במועד, ולכן ההנפקה בפועל החלה חצי שנה לאחר מכן. בשל כך, לא פורסם דו"ח תקופתי עבור המחצית הראשונה של 2013. נציין כי תקופת המבחן לא נדחתה, ובהתאם לצו המבחן היא עתידה להסתיים ביום 31/12/2014.

3 לדוגמה, תקן האבטחה הבינלאומי המוביל, ISO/IEC 15408 – Common Criteria for Information Technology Security Evaluation, מתחלק לאפיון מערכות אבטחת מידע (חלק 2) ולבדיקות אבטחת מידע (חלק 3).

ב. זרישות האבטחה חלות על כלל מערכי ההנפקה והתפעול

כמוסבר במכתבנו הראשון, צו המבחן קובע כי על כלל מערכי ההנפקה לעמוד בתקני רא"ם. המאגר הביומטרי הוא אמנם ליבת המערך, אך הצו מתייחס הן למאגר והן למערכות הנלוות. לדברי מר שמני, רא"ם אישרו את תקן האבטחה הפיזי של ליבת המאגר ביומטרי. לא ברור האם ובאיזו מידה רשות האוכלוסין וההגירה ומשרד הפנים קידמו את הליך הבחינה והאישור של המערכים הנלווים.

ג. במועד תחילת ההנפקה⁴, המערך הביומטרי לא עמד בהנחיות רא"ם

אין כל מחלוקת כי במועד תחילת ההנפקה (08/07/2013), הוחל בביצוע סקרי סיכונים ומבדקי חדירות, אך אלו לא הושלמו במועד. עובדה זאת הודגשה במכתב רמו"ט מיום 30/06/2013 (מענה לבקשה לקיום חובת ההיוועצות בהתאם לתקנות מרשם האוכלוסין), בהתייחס למערכת הביומטרית עצמה:

נמסר לנו [...] כי רא"ם יבצעו ביקורת לבחינת תשתיות חומרה, תוכנה ותשתיות תקשורת אשר תחל ב-9/7/2013, וכן יבוצעו תרגיל תקיפה על המערכת;

נמסר לנו [...] כי על תשתיות המערכת המשמשים את הרשות, בוצעו ביקורות של מערך אבטחת המידע של הרשות וכן נערכו בדיקות על ידי רא"ם. כמו כן נמסר כי רא"ם אישרו שהמערכת עומדת ברמת האבטחה הנדרשת לתשתיות מהסוג האמור, אך נאסר על הרשות להעביר לעיונו את ממצאי הבדיקות שנערכו.

ואכן, במכתבו, מבהיר מר שמני כי "תצורת האבטחה הפיזית ואבטחת מערכות המידע, נבדקה ואושרה על ידי הרשות הממלכתית לאבטחת מידע בשב"כ". כלומר, הוא מאשר כי רא"ם אישרו את תצורת המערכת, אך לא מתייחס לסקרי סיכונים ולמבדקי חדירות. הנחנו כי הוא נמנע במכוון להתייחס למבדקי החדירות, שכן באותה העת (חודש לאחר תחילת ההנפקה) הרשות הביומטרית עמלה על תיקון הליקויים.

כמוסבר להלן, נראה כי חטאנו בהערכת-יתר של הרשות הביומטרית.

ד. חצי שנה לאחר תחילת ההנפקה, המערך הביומטרי עדיין לא עומד בהנחיות רא"ם

ביום 04/02/2014, פרסמה הרשות הביומטרית דו"ח תקופתי למחצית השנייה של שנת 2013. לחרדתנו הרבה, הדו"ח מעיד על כשלי אבטחה בסיסיים ביותר ומדאיגים ביותר – הרבה מעבר לחששות המפורטים במכתבנו הראשון. כאמור, הנחנו כי נערכו סקרי סיכונים ומבדקי חדירות מבעוד מועד, אך הרשות הביומטרית כשלה בתיקון הליקויים עד למועד תחילת ההנפקה. אולם, מסעיף 4.12 של הדו"ח התקופתי עולה כי עד-כה, המערך הביומטרי לא עמד בהצלחה בסקרי סיכונים ובמבדקי חדירות:

4.12. סקרי סיכונים ומבדקי חדירות

בהתאם ללשון הצו עומדת רשות האוכלוסין בהנחיות הרשות הממלכתית לאבטחת מידע, התקבלו מלוא האישורים להתחיל בתקופת המבחן והניסוי מבוצע על פי הנהלים הקיימים. כמו כן, בהתאם ללשון הצו והפרוטוקול, בימים אלו נשלמות ההכנות ברשות האוכלוסין לביצוע סקר סיכונים ומבדקי חדירה בלתי תלויים.

לא מובן כיצד האמור בחלקה הראשון של הפסקה מתיישב עם חלקה השני. רא"ם דורשים ביצוע סקר סיכונים ומבדקי חדירות כתנאי למתן אישור כי המערך נבחן ונמצא עומד ברמת האבטחה הנדרשת. לא די בהשלמת ההכנות לביצוע סקר סיכונים ומבדקי חדירות, אלא נדרש ביצועם בפועל, ותיקון ליקויי האבטחה המתגלים.

נמסר כי רא"ם אישרו את תצורת המערכת (עמידה בתקן הפיזי), וכי נערכו סקרי סיכונים ומבדקי חדירות החל מיולי 2013. ייתכן כי רא"ם נתנו אישור עקרוני לתחילת ההנפקה, בכפוף להשלמת סקרי סיכונים ומבדקי חדירות. ייתכן כי המערך הביומטרי נכשל במבדקים אלו, ועתה הרשות הביומטרית עמלה על תיקון הליקויים. אם כך, רק לאחר סיום תיקון כשלי האבטחה הידועים, "יושלמו ההכנות" לביצוע סקרי סיכונים ומבדקי חדירות חוזרים. ורק לאחר שהבדיקות החוזרות יושלמו בהצלחה, יעמוד המערך הביומטרי בהוראות צו המבחן.

4 נזכר כי צו המבחן דורש כי המערכים יעמדו בתקני האבטחה הנדרשים "טרם תחילת תקופת המבחן", דהיינו ביום 01/01/2013, לא טרם תחילת ההנפקה בפועל, ביום 08/07/2013.

התנועה לזכויות דיגיטליות

Digital Rights Movement

ליקויים אלו נותנים יתר-תוקף להנחיית השב"כ, המוסד וארגוני ביטחון נוספים לעובדיהם, שלא להצטרף לניסוי הביומטרי⁵, ומסבירים מדוע לאחר פרסום הדו"ח התקופתי, קיומה של הנחייה זו הותר לפרסום. העובדה כי הרשות הביומטרית מתנהלת מזה זמן-מה ללא מנהל אבטחת מידע, מעלה סימני שאלה נוספים, ומקשה על הרשות הביומטרית לעמוד בדרישות האבטחה ובהנחיות רא"ם.

ה. סיכום

חצי שנה אחרי תחילת ההנפקה, ברור כי הרשות הביומטרית הפרה את חובתה החוקית לוודא לפני תחילת תקופת המבחן ולפני תחילת ההנפקה, את עמידת כלל המערכים בתקני האבטחה המחמירים. אך גרוע מכך שבעתיים – חצי שנה לאחר תחילת ההנפקה, המערך הביומטרי טרם עמד בהצלחה בסקרי הסיכונים ובמבדקי החדירות. אין המדובר "רק" על אי-עמידה בלוחות זמנים, אלא על סכנה ביטחונית מתמשכת.

לא ברור כיצד הרשות הביומטרית טיפלה בליקויים שהתגלו, וכמה חודשים היה המאגר הביומטרי חدير לארגונים זרים. למעשה, לא ברור האם נכון להיום, המערך הביומטרי מאובטח כנדרש. העובדה כי חלפה למעלה מחצי שנה וטרם נערכו מבדקי חדירות חוזרים, רומזת כי המדובר בכשלים מהותיים ביותר – כשלים שעצם קיומם הוסתר מהציבור ומידת חומרתם הוסתרה מהגורמים המפקחים⁶.

כל עוד לא הסתיימו מבדקי החדירות בהצלחה, לא ניתן לומר כי נתוניהם של האזרחים שהתנדבו לניסוי הביומטרי שמורים כיאות. לכן, המשך הניסוי הביומטרי במתכונתו הנוכחית, מהווה סכנה ביטחונית ופגיעה בפרטיות המתנדבים. אנו תוהים כיצד הגורמים המפקחים התיירו את המשך הניסוי, מבלי שהמערך הביומטרי יעמוד בתקני האבטחה הנדרשים – תוך הפקרת ביטחונם של אזרחי ישראל.

לפי-כך, נבקשך להורות לרשות הביומטרית למסור לאלתר לוועדה המפקחת מכוח סעיף 10ד לצו המבחן דו"ח מלא על תוצאות סקרי הסיכונים ומבדקי החדירות שנערכו לפני כחצי שנה ומאז, בו יפורטו כל הליקויים שהתגלו, לוחות זמנים מחייבים לתיקונם, וכן אמות-מידה ברורות להשיג את הניסוי הביומטרי בשל רמת אבטחה לא מספקת. נבקש כי סיכום דו"ח זה יוגש לעיון הוועדה המשותפת לוועדת החוקה חוק ומשפט, לוועדת הפנים והגנת הסביבה ולוועדת המדע והטכנולוגיה.

בכבוד רב,

צבי דביר, דורון אופק
התנועה לזכויות דיגיטליות (ע"ר)
ת"ד 7237, חיפה 31071

העתקים:

חברי ועדת השרים ליישומים ביומטריים
חברי הוועדה המשותפת לוועדת החוקה חוק ומשפט, לוועדת הפנים והגנת הסביבה ולוועדת המדע והטכנולוגיה
מר רם ולצר, הממונה על היישומים הביומטריים במשרד ראש הממשלה
פרופ' דני פפרמן, הסטטיסטיקאי הממשלתי הראשי
עו"ד אלון בכר, ראש הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים
מר איתן בן-דוד, ראש המטה ללוחמה בטרור במשרד ראש הממשלה
ד"ר זאב ז'בוטינסקי, נציג ציבור בוועדה המפקחת
מר גון קמני, ראש הרשות לניהול המאגר הביומטרי
מר אמנון בן-עמי, מנכ"ל רשות האוכלוסין וההגירה
הרשות הממלכתית לאבטחת מידע של שירות הביטחון הכללי
המועצה הציבורית להגנת הפרטיות במשרד המשפטים
מבקר המדינה

5 ראו: אילן ליאור, השב"כ והמוסד אוסרים על עובדיהם להצטרף לניסוי המאגר הביומטרי, הארץ 02/03/14; דרור גלברמן, המודיעין הישראלי אוסר על אנשיו למסור טביעות אצבע לפיילוט המאגר הביומטרי, מאקו 02/03/14.
(קישורים מקוצרים: <http://bit.ly/1pQ01DB> ו-<http://bit.ly/1dStEvC>).

6 רמו"ט דווחה, בהקשר למערך הביומטרי, כי הרשות הביומטרית סרבה להעביר לעיונה את ממצאי סקר הסיכונים ומבדקי החדירות, למרות שראש רמו"ט חבר בוועדה המפקחת מכוח סעיף 10ד לצו המבחן, ועל-אף סמכויות הפיקוח המוקנות לו.