

תאריך: 14/07/2013

לכבוד שרת המשפטים, חה"כ ציפי ליבני
רח' צלאח א-דין 29, ירושלים 91010

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

הנדון: תחילת הניסוי הביומטרי על-אף ספק בדבר עמידה בתקני אבטחה

שלום רב,

צו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע (תקופת מבחן), תשע"א-2011 (להלן, צו הניסוי) קובע כי אין להתחיל את תקופת המבחן של המאגר הביומטרי בטרם כל מערכי הטכנולוגיה, התפעול והמערך הביומטרי עומדים בתקני האבטחה המחמירים של הרשות הממלכתית לאבטחת מידע של שירות הביטחון הכללי (להלן, רא"ם):

10א(א). רשות האוכלוסין 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.

סעיף זה מטיל על הרשות לניהול המאגר הביומטרי ועל רשות האוכלוסין וההגירה חובה לוודא את עמידת כלל המערכים בתקנים אלו, טרם מועד תחילת הניסוי. מלשון הצו עולה כי לא שהמערך הביומטרי לבדו יעמוד בתקנים המחמירים, אלא נדרש כי גם מערכי העזר – הטכנולוגי והתפעולי – יעמדו בתקנים המחמירים, שכן כשלי אבטחה במערכי העזר מקרינים על רמת האבטחה של המערך הביומטרי בכללותו.

המערך הביומטרי מקושר לשתי מערכות מחשוב טכנולוגיות (לפחות) – מערכת ממיל"א ומערכת אביב. המערך התפעולי מתבסס על הרשת הפנימית של מנהל האוכלוסין וההגירה. הניסוי הביומטרי החל ביום 08/07/2013, אולם ממסמכים שפורסמו לאחרונה עולה ספק אם כלל המערכים הטכנולוגיים והתפעוליים עומדים בתקני האבטחה הנדרשים.

1. **מערכת ממיל"א מקושרת באופן דו-כיווני רציף למערך ההנפקה, ולפי-כך מהווה מערך טכנולוגי כלשון הצו.** חברת קומסק ערכה מבדקי חדירות עבור מערכת ממיל"א, ובהתאם לדו"ח הבדיקה, התגלו חריגות הדורשות התייחסות נוספת. זאת ועוד, בוצעו מבדקי חדירות חלקיים בלבד, וטרם הושלמו כלל הבדיקות הנדרשות. על-אף המלצות צוות הבדיקה, לא ברור אם בשבוע שבין מועד העברת דו"ח האבטחה החלקי ועד יום תחילת הניסוי, הושלמו הבדיקות הנדרשות ותוקנו כל הליקויים שנמצאו.
2. **מערכת אביב מקושרת אף היא באופן רציף למערך ההנפקה, ולפי-כך מהווה מערך טכנולוגי כלשון הצו.** עקב מספר הלקוחות הרב של מערכת זאת, כל עוד קיים קשר רציף עם מערך ההנפקה, ספק רב אם המערך בכללותו עומד בלשון הצו.
3. **המערך התפעולי מתבסס על הרשת הפנימית של רשות האוכלוסין וההגירה, המתבססת בתורה על תשתית IP/VPN של חברה חיצונית.** בשל המספר הרב של הלקוחות ברשת זאת, כל עוד אין הפרדה לוגית ופיזית בין הרשתות, ספק רב אם המערך התפעולי עומד בלשון הצו.
4. **קיים ספק ממשי אף בדבר עמידת המערך הביומטרי עצמו בלשון הצו.** חברת קומסק ערכה מבדקי חדירות למערך הביומטרי, אך דו"ח הבדיקה המסכם הועבר לרשות לניהול המאגר הביומטרי רק ביום חמישי ה-04/07/2013. הניסוי החל ביום שני ה-08/07/2013. **קשה להאמין כי תוך יום עבודה אחד תוקנו כל הליקויים המצוינים בדו"ח זה.** מכאן עולה חשש ממשי כי המערך הביומטרי אינו עומד בלשון הצו.
5. בהתאם לצו הניסוי, על כלל המערכים לעמוד בתקנים שנקבעו בנהלי האבטחה של הרשות לניהול המאגר הביומטרי. אולם, מכיוון שעדיין לא נבחר לתפקיד יועץ אבטחה שתפקידו לערוך את הנהלים ולוודא את העמידה בהם, ספק אם תנאי זה התקיים.

מכלל האמור לעיל, עולה חשש ממשי כי הניסוי הביומטרי החל **טרם התמלאו התנאים האמורים בסעיף 10א(א) לצו הניסוי, וייתכן שאף תוך הפרתו ביוזעין.**

התנועה לזכויות דיגיטליות

^[7] Digital Rights Movement

ראוי לציין כי מסקנה דומה עולה ממכתבה של עו"ד רבקי דב"ש, ראש רמו"ט (בפועל), בו נאמר כי בהתאם לנתונים החלקיים שעמדו בפניה, לא ניתן לקבוע כי כל מערכי הטכנולוגיה, התפעול והמערך הביומטרי עומדים בתקנים האבטחה המחמירים הנדרשים לפרויקט מסוג זה. לכן, היא ממליצה לדחות את תחילת הפרויקט עד לעמידה בתקנים אלו:

אציין כי בשים לב למידע החלקי שנמסר לידנו, לחוות דעתו של יועץ האבטחה של רמו"ט ולמועד בו נמסר לידנו המידע, אין באפשרותי לציין כי לעניין הצורך במבדקי החזירות והצורך בתיקון ליקויים בעקבות תוצאותיהם, הונחה דעתי כי הנתונים שהוצגו בפניי מספקים לעניין עמידות המערכת כנדרש בפרויקט מסוג זה.

כפי שנאמר על ידי לגורמים המקצועיים של הרשות ושל ממשל זמין – בהינתן כי תמונת האבטחה שנפרסה בפנינו ראשונית מחד (ממצאי ביניים) וחלקית מאידך (ללא ממצאי רא"ם וללא הדו"ח המפורט של חברת קומסק) ולאור לוחות הזמנים שנקבעו לפרויקט שאינם מאפשרים לנו להרחיב את המידע המצוי ברשותנו, אין בידנו להשלים את בדיקתנו בעניין זה.

לסיכום אציין כי אני סמוכה ובטוחה כי לאור רגישות הפרויקט, הגורמים המקצועיים המעורבים בו והתחייבותך בפנייתך אליי בדבר החשיבות שאתה נותן לממצאי האבטחה – יישקל מועד תחילת הפרויקט בשים לב לתמונה הכוללת המצויה בפניך (ושלא נפרסה בפני), וכי הבדיקות הנדרשות יושלמו בהקדם. כמו כן, סיכוני אבטחה, ככל שיתגלו, יטופלו במהירות תוך בחינה מחודשת בדבר השלכתם על המשך קידום הפרויקט.

עוד ראוי להעיר, כי בהתאם לסעיף 10ד(ב)(3) לצו הניסוי, ראש רמו"ט היא אחת מחברי הוועדה המפקחת על הניסוי. תמוה הכיצד מידע בדבר תוצאות בדיקות האבטחה מודר מחברי הוועדה המפקחת.

לסיכום – מכל האמור עולה חשש ממשי, כי על-אף החובה החוקית לוודא לפני תחילת הניסוי את עמידת כלל המערכים בתקני האבטחה המחמירים, הניסוי החל בטרם הסתיימו הבדיקות הנדרשות, וממילא הליקויים שהתגלו בבדיקות שנערכו, ככל שנערכו, טרם תוקנו – וזאת בניגוד לנהלים הרלוונטיים.

על-כן, נבקשכם בזאת להורות על השהייה מיידית של המשך הניסוי הביומטרי, וזאת עד שהרשות לניהול המאגר הביומטרי ורשות האוכלוסין יעמדו בחובות המוטלות עליהן בהתאם לסעיף 10א(א) לצו הניסוי, דהיינו כי יתקבל אישור מטעם רא"ם בדבר עמידת כלל המערכים – ובכללם המערכים הטכנולוגיים והתפעוליים הנלווים כאמור לעיל – בתקנים וברמת האבטחה הנדרשת לפי נהליה, וכי כל הליקויים אשר התגלו בבדיקות שנערכו בשבועות האחרונים תוקנו לשביעות רצונה, טרם תחילת הניסוי.

נציין כי אין באמור לעיל כדי להפחית מהתנגדותנו העקרונית להקמת המאגר הביומטרי, שכן לשיטתנו אין כל צורך במאגר זה לשם הנפקת תעודות זהות חכמות, והניסוי הביומטרי אינו בודק את נחיצות המאגר הביומטרי הנלווה.

בכבוד רב,

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

העתקים:

מר גון קמני, ראש הרשות לניהול המאגר הביומטרי, משרד הפנים
מר אמנון בן-עמי, מנכ"ל רשות האוכלוסין וההגירה, משרד הפנים
הממונה על היישומים הביומטריים, משרד ראש הממשלה
חברי ועדת המדע והטכנולוגיה של הכנסת
חברי ועדת הפנים והגנת הסביבה של הכנסת
חברי ועדת החוקה חוק ומשפט של הכנסת
מבקר המדינה