יחידת ממשל זמין
gov
רשות התקשוב הממשלתי
משרד ראש הממשלה

לכבוד

עו"ד רעות אופק, 19.2.2019

מחלקת ייעוץ וחקיקה (אזרחי) ט"ו אדר א' תשע"ט

משרד המשפטים

שלום רב,

הנדון: חוות דעת מקצועית בעניין אמינות מערכות הדואר האלקטרוני והמסרונים, לצורך שילוב חזקות מסירה בהסדרים דיגיטליים .

סימוכין: פניותייך בדוא"ל מיום 27.12.18 ו-16.1.19

בהמשך לפניותייך שבסימוכין, לקבלת חוות דעת מקצועית בקשר לשימוש בדואר אלקטרוני ובמסרונים, כאמצעים טכנולוגיים אמינים, השומרים על שלמות המסר ומבטיחים את אי-שיבושו, או אובדנו בתהליך השליחה, להלן התייחסותנו המקצועית:

ככלל, שירות הדואר האלקטרוני (E-Mail) ושירות המסרונים (SMS), הינם שירותים המתבססים על טכנולוגיות ותיקות ואמינות[1]. ארגונים רבים במשק, בכלל, ובממשלה, בפרט, עושים שימוש רב בשירותים אלו כערוצי תקשורת, הן פנים-ארגוניים, והן בינם לבין לקוחותיהם וגורמים חיצוניים נוספים. למותר לציין, כי המגמה העולמית בקשר לשימוש בדיגיטל לצרכים שונים, ולהפצת מסרים, בפרט, מצביעה על כך שהשימוש בדיגיטל רק הולך וגובר, כאשר מנגד המקבילה הפיסית להפצת מסרים, מתמעטת ונעלמת מן העולם.

שירות המסרונים (SMS):

שירות ה-SMS (Short Message Service) פותח בשנת 1992 והושק בארץ בשנת 1998.

השירות נחשב לשירות אמין שבו הודעות מגיעות ליעדן, אלא אם כן הן נשלחו אל: מנוי אשר אינו קיים (מספר אשר אינו קיים ברשת); יעד אשר לא הוגדר לקבלת מסרונים, לרבות, עקב מגבלה טכנולוגית (לדוגמא, טלפון קווי), או עקב בקשת מנוי היעד (לדוגמה, מנוי היעד הינו בעל מספר כשר או שמסיבה אחרת מגביל את עצמו מפני קבלת מסרונים).

במרכזי שירות שליחת הודעות (Short Message Service Center), קיימים מנגנוני "ניסיון חוזר" (Retry), לשליחת המסרונים, במקרה של כישלון בהעברת המסרון, בזמנים בהם המנוי אינו מחובר לרשת, כבוי, או מחוץ לטווח קליטה. כמו כן, קיים חיווי על אי-הגעת מסרון ליעדו. למשל, במערכת הפצת המסרים - notify, שבה נעשה שימוש בממשל זמין עבור משרדי הממשלה, המעוניינים בכך, ישנו חיווי מהרשת הסלולרית על גורלו של כל מסרון שנשלח. כך, שגם במקרה שבו מסיבות שונות, כמפורט לעיל, שליחת ההודעה נכשלה, ניתן לקבל על כך חיווי מהמערכת.

[1] הנתונים במסמך זה מבוססים על נתונים שהתקבלו מספקי הפצת מסרים של רשות התקשוב והן על בסיס נתונים זמינים באינטרנט.

החיווי מתקבל מספק הסלולר של הנמען, כאשר ההנחה המקצועית המקובלת היא, שמסר שהגיע ליעדו, הוא בהכרח כזה שהגיע גם באופן תקין ושלם.

למעלה מן הצורך, יוער כי בסקרים שבוצעו נמצא כי אחוזי קריאת המסרונים הינם גבוהים גם כן, ונעים בין 73% ל- 97% תלוי בזהות השולח[2]. (המקבילה של נתון זה בעולם הדואר הפיסי הוא אחוז האנשים שפותחים את המכתב וקוראים אותו).

שירות הדואר האלקטרוני (E-Mail):

שירות הדואר האלקטרוני ותיק אף יותר משירות המסרונים. השירות פותח בשנת 1971, נכנס לשימוש בישראל בשנת 1980 והוא מבוסס על פרוטוקול SMTP (Simple Mail Transfer Protocol).

אמנם כ- 0.5% מההודעות נשלחות אל כתובות שגויות[3] אולם בשליחת הודעות דוא"ל מתקבל (אצל השולח) , חיווי משרת הדואר (של ספק הנמען), במקרה של כל כשל בשליחת הודעת דוא"ל. היינו, ככל שאין חיווי על כשל, המשמעות היא שהמסר הגיע לשרת הדואר של ספק הנמען באופן תקין.

חריג לכך, הוא שליחת הודעת דוא"ל המסווגת כ-'דואר זבל' (Spam). סיווג, אשר יביא לכך שרוב הסיכויים, כי נמען ההודעה לא יקרא אותה. במצב זה, שרת הדואר (המקבל) לא ידווח על כשל בהעברת ההודעה, אך בפועל ההודעה לא תועבר לתיבת הדואר הנכנס של הנמען, אלא לתיבת 'דואר זבל' (Spam).

יחד עם זאת, סיווג הודעה כ-'דואר זבל', תלוי בדרגת האמון המוקנית לשרת הדואר השולח, דבר אשר נבנה במשך זמן רב של פעילות ברשת, וככל שמדובר בהודעות דוא"ל לגיטימיות של הממשלה, הסבירות להתעוררות בעיית אמינות מסוג זה היא נמוכה.

בשירות הדואר האלקטרוני קיימות מספר שיטות בהן ניתן לקבל חיווי האם הנמען פתח את הודעת הדואר (בעולם הפיסי ניתן להשוות את זה לפתיחת הדואר הפיסי על ידי המקבל וקריאתו). שיטות אלו, אינן מצויות בתשתית של שירות הדואר האלקטרוני, אלא מדובר ברכיבים/יישומים החיצוניים לתשתית, והשימוש בהם טעון, בין היתר, בחינה משפטית ביחס להיבטים של פגיעה בפרטיות המשתמשים.

סיכוני אבטחת מידע

יצוין כי ערוצי התקשורת מסוג דוא"ל ומסרונים, אינם חפים מסיכוני הגנה בסייבר ואבטחת מידע, כגון יירוט המסרים הנשלחים בערוצים אלו. יחד עם זאת, יובהר כי בהשוואה לסיכוני המידע של הדואר הפיסי, הרי שרמת אבטחת המידע של ערוצים אלו גבוהה עשרות מונים מערוץ הדואר הפיסי, כיוון שיכולת המעקב אחר תהליך שליחת ההודעה ושרשרת אספקת המסר היא נמוכה באופן משמעותי מהערוצים הדיגיטליים, של מסרונים ודוא"ל[4]. בערוצים אלו, בשונה מתהליך הדואר הפיסי, המבוסס על המרכיב האנושי, מדובר בתהליך אוטומטי, המתועד

---

[2] https://www.esendex.co.uk/blog/post/what-is-the-open-rate-for-sms-in-2018/ וכן נתונים מחברת 'inforu'.

[3] נתונים לפי חברת 'inforu'.

[4] בעת התממשות סיכוני אבטחת מידע בשליחת דואר פיסי, ייתכנו מקרים שבהם לנמען תהיה אינדיקציה מסוימת בדבר התממשות הסיכון כגון: נמען שמקבל מעטפה שנראה כי פתחו אותה.

באמצעות קבצי יומן (log), המהווים מידע על אודות פעילות המחשב - המטא-דאטה (המידע על אודות המידע), ומשמשים ראיה לתהליך שליחת המסר מרגע שליחתו, ועד הגעתו למכשיר הקצה של הנמען, במקרה של מסרונים, ולשרת ספק הדוא"ל של הנמען, במקרה של שליחת דוא"ל.

יוער כי גם במקרה שמסר יורט, ברוב המקרים, המסר יגיע לנמען ולתוקף. היינו, שגם במקרה הבלתי סביר שמסר שנשלח במסרון או בדוא"ל ייורט, בהיבט של הגעת המסר ליעד (בשונה מהיבטי סיכוני פרטיות למסר), הדבר לא יעלה ולא יוריד.

בנוסף, רוב ספקי הדוא"ל כדוגמת גוגל (תשתית gmail), מצפינים את תעבורת הדוא"ל שלהם, באופן שמקשה על יירוט המסר ועל פתיחתו.

<u>מערכת הדיוור הממשלתית</u>

בהמשך לאמור לעיל, ראוי לציין, כי רשות התקשוב הממשלתי, מעלה בימים אלו לאוויר את מערכת הדיוור הממשלתי הדיגיטלי, שמטרתה לשמש כחלופה למערך הדיוור הממשלתי הנוכחי, בהתייחס להעברת מידע אישי, המבוסס בין היתר, על משלוח דואר רגיל ודואר רשום[5] באמצעים קונבנציונליים (דואר פיסי).

המערכת מבוססת על ערוצי תקשורת דיגיטליים ישירים, מהימנים ומאובטחים, בין התושבים לבין הממשלה, שיאפשרו העברת הודעות, מסמכים ומסרים לתושב, באופן יעיל ובטוח, ותוך הגנה על פרטיות התושבים.

לשם כך, מערכת הדיוור, משלבת בין מספר מערכות טכנולוגיות קיימות, ובהן:

1. מערכת ההזדהות הממשלתית, שבאמצעותה ניתן להירשם מרחוק, למערכת הדיוור, באופן המבטיח את מהימנות המען הדיגיטלי (דוא"ל ומספר טלפון נייד), ככזה השייך לנמען מסויים.
2. מערכת האזור האישי, שהכניסה אליה טעונה הזדהות, ובה ניתן יהיה למצוא את כלל הדיוור הממשלתי הכולל מידע אישי. מערכת זו עוצבה תוך שימת דגש על היבטי אבטחת מידע והגנת הסייבר, במטרה לשפר ולהתגבר על סיכוני אבטחת המידע הקיימים בעת שליחת דוא"ל או מסרון. בכך, מובטחת גם פרטיות המשתמש, וניתנת אפשרות למשלוח של מידע פרטי ורגיש עד רב"א 3[6]. במערכת זו קיים חיווי בעת כניסת משתמש למערכת, דבר המהווה אינדיקציה למועד שבו משתמש/ נמען קיבל את ההודעה, והיה יכול לעיין בה.
3. מערכת הפצת המסרים- מענ"ה, מאפשרת משלוח הודעות או התראות בדבר דואר הממתין באיזור האישי, למען הדיגיטלי שנמסר על ידי התושב. ההחלטה בדבר שליחת הודעות/התראות למען הדיגיטלי, תיעשה בהתאם לרגישות המידע הנשלח. תעבורת הדוא"ל שנשלחת באמצעות המערכת מוצפנת באופן שמקטין את סיכוני אבטחת המידע ומקשה על יירוט המסר ופיענוחו על ידי תוקף[7].

---

[5] בשלב ראשון המערכת לא תחליף דואר רשום, ככל ששליחתו קבועה בחקיקה.

[6] יצוין כי ככל שיהיה צורך בכך, קיימת היתכנות טכנולוגית שבאיזור האישי יהיה מידע ברב"א 4 בכפוף להזדהות ברמה זו. כבר היום מערכת ההזדהות מאפשרת הזדהות ברב"א 4.

[7] יוער כי הדוא"ל היוצא מהמערכת מועבר תמיד באופן מוצפן, אלא שבמקרה שהשרתים של ספק דוא"ל הנמען, אינם תומכים בפרוטוקול ההצפנה (הפרוטוקול שבשימוש יחידת ממשל זמין הוא מסוג TLS1.2 ונחשב לאחד הפרוטוקולים המתקדמים בתחום ההצפנה), אזי יועבר המסר ללא הצפנה (clear text). עם זאת, למיטב ידיעתנו, רוב ספקי הדוא"ל תומכים בהצפנה או מקדמים נושא זה.

לאור האמור, מובהר כי שליחת דיוור ממשלתי באמצעות מערכת הדיוור, היא אמינה יותר, בהיבטי אבטחת מידע, מהשימוש בערוצי התקשורת שפורטו לעיל.

סיכום

לאור כל האמור לעיל, עמדתנו המקצועית היא כי שירותי המסרונים והדואר האלקטרוני הינם אמצעים אמינים להעברת מסרים, אשר בוודאות גבוהה יגיעו לידי הנמענים. בנוסף, מערכת הדיוור הממשלתי, המבוססת גם על שירותים אלו, נותנת מענה כולל לנושא הדיוור, המביאה בחשבון את מהימנות המען הדיגיטלי ומעניקה שכבת הגנה נוספת ביחס לאבטחת המידע הנשלח באמצעותה, כמפורט לעיל.

בברכה,

יאיר פראנק

ראש רשות התקשוב הממשלתי

משרד ראש הממשלה

העתק :

מר יוגב שמני, מנהל יחידת ממשל זמין, רשות התקשוב הממשלתי
עו"ד יערה בן שחר תיק, ס. בכירה ליועצת המשפטית, רשות התקשוב הממשלתי, משרד רה"מ