"מערכות אבטחה מהותיות ברשות המכס ובמס הכנסה אינן מתוחזקות. זו רשלנות פושעת"

בכירים ברשות המסים וברשות הסייבר התריעו על הסכנה שבהעתקת כל נתוני המס ממערכת המחשוב המאובטחת של הרשות למערכות המכס, שאבטחתה חלשה. למרות זאת התעקש ראש הרשות, ערן יעקב, להמשיך במהלך. באוגוסט דלף ממערכות המכס קובץ עם נתוני כל 6000 עובדי רשות המסים. רשות המסים: "לדליפה אין קשר למערכות המחשוב שביניהן הוחלט להחליף מידע והניסיון לקשור ביניהן נובע ממניעים זרים ומאבקים פנימיים". אבל לדברי גורמים ברשות המקרה מלמד על הסיכונים בתרחיש שבו מידע פיננסי סודי על אזרחי ישראל ידלוף החוצה

עמיר קורץ 06:4519.11.20 **כלכליסט**

דליפת מידע רגיש ממערכת המחשב של המכס, אשר הוגדרה בדיונים פנימיים בתוך רשות המסים כ"מגה אירוע", עמדה בלב ישיבה דחופה שכונסה ב־17 באוגוסט השנה תחת הכותרת "דלף מידע ברשות". יגאל תזזו, מנהל תחום אבטחת המידע במכס, היה מי שגילה כמה ימים קודם לכן את הדליפה. הוא התקשר אל אבנר שריקר, מנהל חטיבת אבטחת מידע וסייבר בשע"ם (שירות עיבודים ממוכנים), וסיפר לו כי קובץ עם פרטים מלאים של כל 6,000 עובדי רשות המסים נחשף במלואו ודלף החוצה. חלק מעובדי הרשות, הוא סיפר, מקבלים בעקבות זאת הטרדות שונות. בישיבה הדחופה שכונסה בעקבות המקרה סיפר שריקר, על פי פרוטוקול הדיון, כי "תזזו אמר: אני צריך יועצים, יש לי מגה אירוע. קבצים מעודכנים יוצאים החוצה ואני לא יודע איך. רשימת 6,000 עובדים יצאה החוצה."

מנהל רשות המסים וממלא מקום מנכ"ל משרד האוצר ערן יעקב. נטען כלפיו כי החלטתו לאפשר העברת מידע למכס יצרה פרצת אבטחה

האירוע קרה חודש אחד בלבד אחרי שמנהל רשות המסים ערן יעקב הורה להעביר מידע שאגור במחשבי יחידת שע"ם, המספקת שירותי מחשוב לרשות המסים ולגופים נוספים, ומאובזרת ב־7 חגורות הגנה, אל מערכת של המכס שנקראת ג'נרי, שכוללת הגנה נמוכה בהרבה - שכבת הגנה אחת. מדובר במידע פיננסי מקיף ביותר על נישומים פרטיים, חברות וארגונים שהצטבר במשך השנים ברשות המסים. למעשה ,כמעט כל סודות המס של מדינת ישראל.

הסיבה להחלטה היא שינוי ארגוני רחב שיעקב מוביל ברשות, בין השאר ביחידת שע"ם . לטענת ועד העובדים, מטרת המהלך היא להחליש את כוחו, ובנוסף להגביר את זמינות המידע עבור מחלקות נוספות ברשות, בין השאר כדי להקל את הבירוקרטיה הפנים־ ארגונית. זאת, כאשר ברקע ביקורת ציבורית שספגה הרשות על עיכוב בהעברת מענקי הקורונה לבעלי העסקים והעצמאים, כשהשיא היה "נזיפה פומבית" של ראש הממשלה בנימין נתניהו ביעקב בשיחה עם נציגי העצמאים .

דליפת המידע ממערכות המכס אמנם לא היתה של המידע החדש שהועבר לשם, אולם היא חידדה עוד יותר את הסכנות שבהעברת המידע הרגיש מיחידת שע"ם - סכנות שעליהן התריעו גורמים בכירים במערכת, כפי שייחשף כאן דרך התכתבויות דואר אלקטרוני פנימי שהגיעו לידי "כלכליסט."

בעקבות השיחה מתזזו, שלח שריקר ב־14 באוגוסט מייל חריף ביותר תחת הכותרת "אזהרה חמורה ביותר לפני פגיעה בביטחון המדינה", לערן יעקב, לאלי גזית ,ראש אגף בכיר במערך הסייבר הלאומי במשרד ראש הממשלה, ולשורה של גורמים בכירים נוספים ברשות המסים. "בימים האחרונים", כתב שריקר, "הגיעה לאוזניי ידיעה על ידי אחד הנציגים שלכם כי ישנו דלף מידע ברמת 'מגה אירוע'... אותו גורם ציין בפניי ששנים רבות מערכות אבטחה מהותיות אינן מתוחזקות ואינן פעילות ברשות מכס ונמ"ה (נציבות מס הכנסה)". הוא הוסיף כי "ימים ארוכים אני פונה לכל הגורמים ברשות המסים ובמערך הסייבר אך ללא מענה הולם. לטעמי זאת רשלנות פושעת הן של מערך הסייבר והן של הנהלת רשות המסים בישראל, כאשר בראשם עומדים שניכם."

הוא דרש במייל לבצע שורה של פעולות מיידיות על מנת למנוע דליפת מידע גולמי מהמערכת ולתאם פגישה דחופה בנושא. במייל הוא מציין עוד: "המידע אשר נצבר בשע"ם הוא חסוי, פרטי ורגיש. פגיעה בזמינות, שלמות או חשיפת המידע מהווה פגיעה בתשתית המדינה הקריטית, בחוק הגנת הפרטיות ובכללים בינלאומיים .חשיפת המידע אשר קיים בקבצים הנדרשים, עלולה להביא לפגיעה בתשתית השלטונית והביטחונית של מדינת ישראל."

במייל נוסף ששלח שריקר לרחלי קופרבאר, אחת היועצות של יעקב, הוא כתב כי "העובדה שכמות רשומות כזאת יוצאת ללא בקרה היא מטרידה". הוא כתב כי תזזו ביקש עזרה ביישום טכנולוגיות מניעת דלף המיושמות בשע"ם. "מיד שאלתי אותו כיצד טכנולוגיה שנרכשה ברשות לא מיושמת. נאמר לי כי לאורך כל השנים לא הגיעו לזה. כמובן באותו רגע השאלה הראשונה שקפצה לי - כיצד אתה ישן בלילה, כאשר אתה יודע שיש מידע רגיש אצלך והוא לא מוגן. משגע אותי שגם מערך הסייבר וגם אנשי האבטחה של הרשות יודעים זאת, אך מסיבות פוליטיות כוחניות לא צועקים זאת בפומבי."

היד שמנענעת את שאלטר המידע

אי אפשר להגיד שדליפת המידע היתה מפתיעה: מתכתובות דוא"ל פנימיות שנשלחו ברשות המסים בחודשים האחרונים, עולה כי היו כמה גורמים שהתריעו על הסכנה בהוצאת מידע ממערכת שע"ם דרך "צינור" להעברת מידע שמכונה "הכספת" והעברתו למערכות פחות מאובטחות - כמו זו של המכס. וכן על השינויים הארגוניים שמבוצעים ביחידה המונה יותר מ־500 עובדים. מדובר במידע רגיש ביותר, הכולל קרוב ל־95% מכלל המידע הפיננסי בישראל על נישומים, ובכלל זה אנשים פרטיים ,עסקים ומוסדות, כולל המסווגים ביותר. לא בכדי הושקעו במהלך השנים יותר מ־100 מיליון שקל בבניית מערכת ההגנה הרב־שכבתית להגן על מערכת המחשוב של שע"ם ומערך ה"כספות". בנוסף, מקפידים שם כי ניתוח המידע הרגיש והסודי יתנהל רק בתוך מערכת מאובטחת שמכונה פרויקט מו"ח (מידע ויישומים חכמים), כדי למנוע זליגת מידע גולמי .

ראש ועד העובדים בשע"ם דורון דודו. "להחליש את הוועד על חשבון פגיעה באבטחת המידע

כך למשל, במיילים ששלח עפר דרורי, מנהל אגף מע"מ בשע"ם, אחרי גילוי הדליפה הוא כתב כי "התרעתי בעבר כמה פעמים. היה סיכום שכל המידע שנמצא בשרתים לא ניתן

להוריד או להעביר מהם קבצים. זה לא בוצע". במייל אחר ציין דרורי: "חייבים למצוא דרך שהמידע השע"מי לא ייצא מגבולות הארגון ולא יזלוג החוצה."

מהתכתבויות דוא"ל פנימי שנשלחו עוד לפני אירוע הדליפה עולה כי אחד המתריעים המרכזיים מהוצאת מידע ממחשבי שע"ם היה יו"ר הוועד של שע"ם דורון דודו. זאת בין השאר כחלק ממלחמתו העיקשת זה זמן רב **נגד השינויים שמובילה ההנהלה בשע"ם**. לתפיסת הוועד, ההנהלה בראשות יעקב מנסה "להפריט ולייעל" את שע"ם, ובגלל שהיחידה יושבת עם היד על "שאלטר המידע", ההנהלה מנסה לגרום לכך שעוד גורמים ברשות יהיו נגישים למידע כדי להחליש את הכוח של הוועד במו"מ, גם אם זה יבוא על חשבון רמת האבטחה של המידע.

דודו, יו"ר הוועד, כמובן, מתנגד לכך .הוא התלונן לא אחת להנהלה הבכירה ברשות על הפרת הסכמים מול הוועד על שימוש במיקור חוץ ועל פגיעה בעובדים והורה בכמה הזדמנויות למנוע הוצאת מידע ממערכות שע"ם. כמה פעמים הוא גם הורה שלא להכניס לשע"ם יועצים חיצוניים והכריז על השבתת מוקד התמיכה. "ועד שע"ם בראשותי לא יאפשר שינוי מבנה ארגוני ולו הקטן ביותר ללא הסכם", הוא כתב באחד המיילים להנהלה וציין כי משבר הקורונה אינו סיבה מספקת לפגיעה בעובדי שע"ם.

באחד המיילים ששלח דודו בסוף חודש יוני לכל עובדי שע"ם הוא כתב: "אנו חוזרים ומדגישים כי חל איסור להוציא מידע גולמי מלא מחוץ לשע"ם ורשת שע"ם .אין לאפשר עבודה ליועצים עם רשת שע"ם בכרטיסים חכמים המונפקים להם... כל האמור נובע מטעמי אבטחת מידע וסיכומים בעבר עם ועד העובדים."

במייל אחר באותם ימים הוא גם ביקש למנוע מתן גישה למידע מהמערכת למנהל תחום הדאטה ברשות המסים ויועצו של יעקב, שמעון (שימי) אברביה. "יש לבטל את ההרשאות לשימי מרשות המסים וחבריו", כתב דודו, "ואם לא ניתן לבטל את ההרשאות לשימי יש להוריד את הכספת. אין אישור להוציא מידע גולמי משע"ם .למיטב הבנתי גם מאבטחת מידע אין אישור להחזיר את הכספת."

"ערן יעקב פסק בניגוד למתריעים"

התנגדות להוצאת מידע מטעמי אבטחה באה לידי ביטוי גם במיילים ברוח דומה ששלח עוד קודם שריקר. זאת בתגובה לבקשה מהמכס לקבל גישה לנתונים רבים במערכות שע"ם ובהם: מרשם האוכלוסין (כולל תיקי ניכויים), רשם החברות ועוסקים מורשים, מאגר הרכב, רשימת תיבות דואר ובעליהן, נסיעות לחו"ל ,חשבוניות בין ישראלים לפלסטינים, תיקי חקר ומידע מודיעיני. באחד המיילים לתזזו מהמכס כתב שריקר כי "אין אישור להוציא את הקבצים כחומר גלם מלא. יש לבצע מחיקה של כל הפרטים המזהים ורק אז לקבל אישור חדש ממני."

במייל אחר לגורמים שונים בשע"ם וברשות המסים כתב שריקר כי הוא מתנגד ל"הכפלת בסיס הנתונים עבור שימי כפי שדרש בשבוע שעבר. דרישתו היתה לקבל את כל נתוני שע"ם על מחשב נייד חיצוני אשר מנותק מהרשת ונמצא תחת חסותו. הבעתי את התנגדותי באופן גורף וזאת מהסיבות הבאות: כל הכפלת מידע חושף את מדינת ישראל לדלף מידע נוסף; על המחשב הנוסף אין בקרות אבטחה כפי שיש על המידע אשר יושב בשע"ם, כלומר

עמידה מלאה ברגולציות שונות. ביצוע כל הבקרות על המחשב הנוסף הן לא ריאליות. לכן אני לא מאשר את הבקשה". אולם הוא כתב כי "המידע הוא באחריות מנהל רשות המסים בישראל ואי לכך כל בקשה שלו בכתב ומאושרת על ידי מערך הסייבר תבוצע. המנדט שלי הוא להגן על המידע, אך יש סמכויות מעליי והם יקבעו בסופו של יום."

בעקבות דין ודברים מתמשך שהיה בין הגורמים השונים בנושא, כונס דיון מיוחד על הסכנות שבהעברת המידע משע"ם, דרך ה"כספת" למערכת ג'נרי של המכס, ב־17 במאי. "מטרת הדיון", נכתב בפרוטוקול הישיבה, "הבנת הסיכון והמשמעויות של המידע שהועבר באמצעות הכספות לרשת ג'נרי – וללמוד כדי להבין פתרונות אפשריים". המשתתפים בישיבה דיברו בה על ההיערכות להעברת עשרות אלפי רשומות הכוללות קבצים של דו"חות תקופתיים לעוסקים הרשומים במע"מ, עסקאות, תשלומים, החזרים, פרטי עוסקים ועוד .

בפרוטוקול הישיבה צוין בפירוש כי לא ניתן לייצא למערכת הג'נרי של המכס את רמת האבטחה הגבוהה הקיימת בשע"ם. לדברי קובי קרודו, מנהל אבטחת מידע ברשות המסים, "מדובר במידע שנמצא ברמת אבטחה 5. מדובר ברמה גבוהה שלא ניתן לייצא לרשת ג'נרי."

על פי הפרוטוקול, מנהלת שע"ם ליאורה בן אפרים התריעה גם היא באותה ישיבה כי "ישנה חשיבות ברמה לאומית למידע כזה. מדובר במידע כלכלי. יש כאן מידע רגיש מאוד... הוצאתו מהווה סיכון. יש מידע שיצא בגודל של עשרות ג'יגות ...יש צורך לבדוק את דלף המידע מרשת ג'נרי – באחריות מערך הסייבר... הפתרון הנכון הוא לא לשנע את המידע אלא לעבוד ברשת של שע"ם. כל תהליך שידרוש שינוע מידע החוצה יגרום לחשיפה רבה". גם נציג רשות הסייבר בדיון, אורי הלפרט ,הסכים: "רמת האבטחה שונה ברשתות ויש צורך להבין זאת... כל שינוע מידע הוא סיכון אבטחתי גדול מאוד המתלווה עם סכנות ממשיות", הוא אמר. בעקבות זאת סיכמו הנוכחים כי יבוצעו פעולות שונות לאבטחת המידע. "יש צורך במציאת פתרון", אמר תזזו מהמכס, "על מנת שיינתן מענה ראוי לעבודה ובכך לא ייגרמו שגיאות אבטחתיות מהמשתמשים."

המורכבות והסכנות הרבות ריחפו גם מעל ישיבה רבת־משתתפים שכינס יעקב עצמו ב־5 ביולי בנושא "שימוש בנתונים על ידי המחלקה הכלכלית". בישיבה נידונה העברת המידע ממחשבי שע"ם למערכת ג'נרי של המכס, ובמהלכה הציגה המשנה למנהל הרשות, מירי סביון, את חשיבות המהלך כדי להגביר את הנגישות לנתונים. מנגד, הציגו כמה מאנשי שע"ם את המורכבות והסיכונים במהלך. בן אפרים עמדה בהתנגדותה להוצאת המידע, וזכתה לרוח גבית הן משריקר והן מנתי לרנר, בכיר בשע"ם המנהל את פרויקט מו"ח.

" החבורה הזו התנגדה והסבירה את הסיכון", אומר גורם הבקיא בפרטים, "היו ממש צעקות בישיבה, אבל לבסוף יעקב פסק בניגוד לעמדת המתריעים. הוא אמר קודם תעבירו את המידע ובמקביל נפתח את מערכות ההגנה. לא עזר שניסו להסביר שלקח שמונה שנים ועשרות מיליוני שקלים לפתח אותן."

בסיכום אותה ישיבה נתן יעקב הוראות ברורות: "יש להעביר את הנתונים לרשת ג'נרי על מנת לאפשר יעילות מרבית לעבודת המחלקה הכלכלית ושאר הלקוחות". הוא ציין כי הדבר יבוצע באופן מיידי, ובאחריות בן אפרים. בנוסף, לאור ההערות שניתנו בנושא האבטחה, קבע יעקב, על פי פרוטוקול הישיבה, ש"יש לחזק את רמת האבטחה של רשת ג'נרי". עוד נכתב

בסיכום הישיבה שבמידה שיש אילוץ המצדיק עצירה בהזרמת הנתונים, יש ליידע באופן מיידי אותו ואת המשנה שלו סביון .בנוסף, "לגבש החלטה מה תהיה סביבת העבודה, ולבחון משמעויות מבחינת אבטחת מידע יחד עם יכולת העבודה של המשתמשים. לאחר בדיקת הנושא על כל היבטיו על ידי כל הגורמים המעורבים, יש לקיים ישיבה להצגה לערן, לעדכון ולהכרעה בסוגיות שבמחלוקת ככל שישנן."

כאמור ,חודש וחצי בלבד לאחר אותה החלטה, כונסה ישיבה דחופה ב־17 באוגוסט בעקבות אירוע דליפה ממערכת המכס. על פי פרוטוקול הפגישה, שריקר ציין במהלכה כי "מספר פעמים התריע על הבעיות של דלף מידע, ולכן החליט לזעזע עם מייל קשה כדי לטפל בבעיה". שריקר ציין עוד כי "השקענו כ־100 מיליון שקל באבטחת מידע בשנים האחרונות וכיום הדברים עובדים. ההשקעה הגדולה היתה כדי להגן על המידע ובסיס הנתונים. אם המידע יודלף לא יהיה אמון במערכת הרשות. כשיש מידע רגיש אסור שישב במקומות אחרים, ניתן לבצע עיבודים וגזרות אך אסור להזיזו". הוא גם תקף בחריפות את העובדה שהמידע שעבר למכס לא מאובטח. בפרוטוקול הדיון נכתב: "אבנר אמר ליגאל (תזזו): חמור מאוד, אתם יודעים שהמידע שעובר אליכם אינו מאובטח. שום טכנולוגיה לא עובדת אצלכם ."

גורמים שנחשפו לאירוע הדליפה מהמכס אומרים כי פרטי עובדי הרשות הגיעו לכמה רואי חשבון וגורמים פרטיים, וכי ברשות התקבלו בעקבות זאת מסרים מאנשים מחוץ למערכת, כי פרטי כלל העובדים יופצו באינטרנט, איום שלא מומש.

המקרה אמנם הוגדר כ"מגה אירוע" אך היה נקודתי יחסית. עם זאת, לדברי הגורמים הוא מעיד על הסיכונים שעלולים לקרות במקרה שהמידע הפיננסי הסודי ביותר על כל אזרחי ישראל והחברות הפועלות בארץ, ידלוף החוצה. "רק נסה לתאר תקלה של דליפת מידע אודות ההכנסות והשכר של אזרחי ישראל, או כל המידע העסקי והפיננסי של חברה מסחרית", אומר אחד הגורמים. "כל המידע הרי הועבר למערכת המכס שהיא הרבה פחות מוגנת ואם הוא ידלוף החוצה יהיה פה כאוס מוחלט. זו סכנה גדולה."

" רצו שליטה, דליפה פחות הפריעה להם "

יו"ר ועד שע"ם דורון דודו אומר ל"כלכליסט" בהקשר זה כי "אין כל היגיון לעשות מערכת כפולה. יש פה מערכת קיימת שעובדת ומניבה. למה צריך לשכפל אותה ?זה יוצר גם עוד עלויות וגם כשל אבטחתי מיותר. בעיני זו טעות חמורה .להערכתי מדובר במגמה לעקוף את שע"ם ואת אבטחת המידע שלה כדי לא להיות תלויים בצעדים של הוועד, למרות שאנו נוהגים בשיא האחריות. במקום לחפש הרפתקאות רק כדי להכשיל את ועד העובדים ולקחת לו את הכוח, צריך לדאוג להגן על המידע הזה."

דודו אומר כי לא הקשיבו להתרעות שלו משום שלטענתו, "דליפת מידע פחות הפריעה להם, ויותר חשוב היה להם להשיג שליטה, כלומר להוציא את המידע משע"ם כדי שלא נהיה בלעדיים עליו. זו הדרך של ערן יעקב להחליש את ועד העובדים ולקבוע עובדות בשטח, ועוד שלב בדרך לפרק את שע"ם. אני כיו"ר ועד מוכן לשינוי המבני למרות שהוא בעל השלכות על הארגון ומאמין **שצריך להתקדם עם הטכנולוגיה, אך זה צריך להיעשות בהסכמה**

ולא כשינוי מבני זוחל חד־צדדי .הנהלת הרשות בחרה מנהלת רצינית לשע"ם, שמתריעה על הכשל האבטחתי, וכאשר ממנים אנשי מקצוע צריך להקשיב למה שהם אומרים ."

פניות ישירות אל יגאל תזזו, אבנר שריקר וליאורה בן אפרים נענו ב"אין תגובה, תפנה לדוברות רשות המסים."

" כלכליסט" העביר פנייה מפורטת לרשות המסים, לגבי העברת המידע משע"ם למכס, הדליפה שהתגלתה והפעולות שנעשו בעקבותיה. מרשות המסים נמסר: "רשות המסים אינה נוהגת להתייחס לתוכנם של דיונים פנימיים, קל וחומר כאשר מדובר בסוגיות הנוגעות באבטחת מידע. הגוף המנחה את רשות המסים בסוגיות אלה הוא רשות הסייבר במשרד ראש הממשלה וכל פעולה רלבנטית של הרשות מתבצעת בתיאום מלא מולה. לפרסום הפרטים של עובדי הרשות אין קשר למערכות המחשב שביניהן הוחלט להעביר מידע ונסיון השווא לקשור ביניהן נובע ממניעים זרים וממאבקים פנימיים. **רשות המסים פועלת כל העת לשיפור השירות לציבור והפחתת הבירוקרטיה תוך שמירה קפדנית על ביטחון המידע ופרטיות הציבור."**

ממערך הסייבר הלאומי במשרד ראש הממשלה נמסר בתגובה: "מערך הסייבר הלאומי מנחה את רשות המסים בעבודה מאובטחת כנגד תקיפות סייבר. האירוע המתואר בכתבה אינו תוצר של תקיפת סייבר והוא טופל על ידי רשות המסים."