

4.ד בדיקה בנושא הרשאות רכש

אבטחה ושמירת מידע מחויבים מכח החוקים :

1. סעיף 7א לחוק יסוד כבוד האדם וחירותי סעיף, התשנ"ב 1992 7א אשר קובע כי "כל אדם זכאי לפרטיות ולצנעת חייו".
2. חוק הגנת הפרטיות תשמ"א-1981 ותקנות (תנאי להחזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים) תשמ"ו – 1986 שהותקנו מכוחו.
3. חוק חופש המידע, תשנ"ח - 1998.
4. חוק המחשבים, התשנ"ה – 1995.

חוקים אלה מגדירים כללים הקובעים את חובות הרשות המקומית כמוסד ציבור בשמירה על מאגרי המידע הנתונים בידיה והאופן בו על הרשות המקומית לפעול על מנת להבטיח את ההגנה על פרטיות המידע מחד ואת זכויות האזרח לחופש המידע מאידך.

בכלל הסיכונים הכרוכים בניהול מערכות מידע ניתן למנות :

1. חשיפה של מידע אישי עליו חלה חובת החיסיון והסודיות.
2. זליגת מידע לגורמים בלתי רלוונטיים ו/או בלתי רצויים מחוץ לרשות המקומית.
3. שיבוש מידע האגור במערכות המידע על ידי הזנת נתונים שגויים למערכת, שינוי נתונים קיימים או מחיקתם
4. פעילות בלתי מורשית של עובדים, העלולה לסייע לגורמי חוץ לפגוע ברשות המקומית.

קיימים שני תקני ISO מרכזיים בתחום אבטחת מידע :

1. ISO – 27001 תקן לניהול אבטחת מידע
התקן לניהול אבטחת מידע מגדיר עקרונות שיטתיים ותכליתיים להקמה, ניהול ותחזוקה של מערכת אבטחת מידע בהתאם לדרישות הארגון. התקן מתייחס למגוון נושאים, בין היתר : זיהוי וניהול הסיכונים למידע, בחירת הבקורות הנחוצות לארגון, הגדרת יעדים לניהול אבטחת מידע, התאמה לדרישות החוק והתקנות הרלוונטיות, תהליכים לשיפור ופיתוח, המשכיות עסקית ומניעת הונאות.
2. ISO – 27032 אבטחת מידע בתחום הסייבר
התקן נועד לסייע לארגונים להתמודד עם תופעת הסייבר וכולל מערך הנחיות והמלצות המסייעים לארגון להתמודד עם איומי סייבר.

מערך הרשאות תקין, המתאים למבנה הארגוני ולנוהלי הארגון, הכרחי ומהווה בסיס לניהול אבטחת מידע תקין.

תכנית הבדיקה

תהליך הרכש/ הן של טובין והן של עבודות ושירותים (להלן "תהליך הרכש"), מתבצע ברשות המקומית באמצעות מערכות הרכש והפיננסים של בתי התוכנה. ניהול תקין של אבטחת המידע ברשות מחייב כי לא תינתן הרשאה לגורם בלתי מורשה, בין מתוך הרשות המקומית ובין מחוצה לה, וכי רמת ההרשאות למורשים תתאים למבנה הארגון ולהגדרות התפקיד של בעלי ההרשאות השונים.

מטרת הבדיקה למפות את ההרשאות הקשורות בתהליך הרכש ולבדוק האם קיימים עובדים או גורמים אחרים שלהם הרשאות למערכות הרכש והפיננסים, על אף שאינם נדרשים לכך מכוח תפקידם ו/או על אף שאינם עובדים ברשות.

קבצי מידע

על המבקר לקבל קובץ של בעלי הרשאות עדכון במערכת הרכש והפיננסים לביצוע הפעולות הבאות (*):

נושא	אוטמציה	מטרו	EPR
			בסרגל הכלים
פתיחת ספק	2101	מסך 1020 ובתוכו 1039	רכש - טבלת ספקים/טבלאות - טבלת כרטיסים
שינוי פרטי חשבון	2101	מסך 1020 ובתוכו 1039	רכש - טבלת ספקים - לשונית תנאי תשלום/טבלאות - טבלת כרטיסים - לשונית נתוני תשלום
אישור הזמנה לתשלום	304/333	מסך 2116 העברה לסטטוס 7	רכש - טיפול בהזמנות
אישור פקודת תשלום	3202/3211	מסך 2308 ובתוכו כפתור אישור או קיבוע	תשלומים - ביצוע תשלומים
התאמת בנק	3304	מסך 2603	הנח"ש - כרטיסים חיצוניים - התאמת כרטיס חיצוני

(*) בכוונת בתי התוכנה להפיק קובץ ייעודי לצורך הבדיקה – עדכון יועבר על ידי האגף לביקורת.

מיפוי הרשאות

על סמך קבצי המידע הנ"ל, על הרשות המקומית לציין מי מבין בעלי ההרשאות אינו עובד הרשות המקומית ו/או אינו זקוק להרשאה מתוקף תפקידו.

בקובץ האקסל הייעודי לריכוז ממצאי הביקורת, יש לציין לגבי כל פעולה נבדקת האם קיימים בעלי הרשאות בלתי מורשים ומה מספרם. בטור "מספר שאינם מורשים" יש להזין את מספר בעלי ההרשאות הבלתי מורשים (מספר אנשים ולא כמות הרשאות). לפיכך, סך בעלי ההרשאות "שאינם מורשים" לא יהיה בהכרח סיכום מתמטי של מספר ה"לא מורשים" בכל מסך, שכן יתכן כי קיים גורם חיצוני/עובד בלתי מורשה בעל מספר הרשאות. בקובץ האקסל יש לציין את סך בעלי ההרשאות "שאינם מורשים" ואת סך כמות ההרשאות לגורמים אלה.

הרשות רשאית לתקן את ההרשאות במהלך הביקורת, והמבקר יעדכן את הממצאים בהתאם. בכל מקרה, יציין המבקר בגיליון האקסל את מספר בעלי ההרשאות הבלתי מורשים שאותו בתחילת הביקורת.

דוגמה :

בתחילת הביקורת אותרו 20 עובדים בעלי הרשאות שלא לצורך תפקידם. לאחר שהרשות תיקנה חלק מההגדרות במערכת נותרו הרשאות לא תקינות אלה :

עובד 1 עם הרשאות לפתיחת ספק, פקודת תשלום והתאמת בנק שלא לצורך תפקידו.

עובדים נוספים עם הרשאה לביצוע התאמת בנק שלא לצורך תפקידם.

סך בעלי ההרשאות "שאינם מורשים" הוא 8 עובדים

סך כמות ההרשאות לגורמים בלתי מורשים הוא 11

טבלת מיפוי ההרשאות תציג את המידע הבא :

הרשאות עידכון רכש ופיננסים לנושאים נבחרים לשאינם מורשים			
סך הרשאות	מס אינם מורשים	כן/לא	הרשאות רכש ופיננסים
			נמצאו בעלי הרשאות בנושאים הבאים במערכת הרכש והפיננסים, לשאינם מורשים
	1	כן	פתיחת ספק
	1	כן	שינוי פרטי חשבון בנק לספק
		לא	אישור הזמנה לביצוע
	1	כן	אישור פקודת תשלום
	8	כן	התאמת בנק
11	8	כן	סה"כ בעלי הרשאות לנושאים נבחרים ברכש ופיננסים לשאינם מורשים
	20	כן	יש לציין את המצב שהיה בתחילת הבדיקה לפני התיקונים שביצעה הרשות בעקבות הבדיקה- לגבי בעלי הרשאות עידכון רכש ופיננסים לנושאים הנבחרים לאלו שאינם מורשים

בקרה פנימית

יש לבדוק האם קיימת בקרה פנימית מובנית במערכת היוצרת הפרדת תפקידים נאותה בארגון. לצורך בדיקה זו ייבדקו ארבעה מצבים :

1. האם קיימים בעלי הרשאות גורפות לביצוע כל ארבע הפעולות : פתיחת ספק ו/או שינוי פרטי חשבון בנק, אישור הזמנה לביצוע, פקודת תשלום והתאמת בנק? קיומן של ארבע הרשאות אלו לגורם אחד מהווה ליקוי בבקרה הפנימית. בגיליון האקסל יש לציין את מספר העובדים בעלי ארבע ההרשאות.
2. האם קיימים בעלי הרשאות לביצוע שתי הפעולות : פתיחת ספק ו/או שינוי פרטי חשבון בנק ופקודת תשלום? קיומן של שתי הרשאות אלה אצל גורם אחד מהווה ליקוי בבקרה הפנימית. בסעיף זה אין לכלול שוב בעלי הרשאות שנכללו כבר בסעיף 1.

בכל אחד מהמצבים 1 ו 2 גם אם קיימות הרשאות גורפות, אולם קיימת בקרה מובנית אחרת באופן שביצוע הפעולות דורש אישור של גורם נוסף במערכת, יש לרשום זאת, והמצא לא יהווה ליקוי בפרק עיקרי הממצאים.

דוגמה :

עובד אחד רשאי לשנות פרטי חשבון בנק וגם להפיק פקודות תשלום, אולם בעת שינוי פרטי חשבון בנק נשלחת הודעה אוטומטית לגזבר על ביצוע השינוי ועל הגזבר לאשר זאת במערכת – במקרה זה לא יירשם ליקוי בפרק עיקרי הממצאים.

ריכוז ממצאים

את ממצאי הביקורת יש לרכז בקובץ האקסל הייעודי. תדפיס הטבלאות והממצאים יוצג בדוח המפורט.

דוח ביקורת מפורט

		בקרה טכנית ל-הרשאות	
		ביקורת לקובץ	
הרשאות עידכון רכש ופיננסים לנושאים נבחרים לשאינם מורשים			
סה"כ הרשאות לשאינם מורשים	מס אינם מורשים	כן/לא	הרשאות רכש ופיננסים
			נמצאו בעלי הרשאות בנושאים הבאים במערכת הרכש והפיננסים, לשאינם מורשים
			פתיחת ספק
			שינוי פרטי חשבון בנק לספק
			אישור הזמנה לביצוע
			אישור פקודת תשלום
			התאמת בנק
0			סה"כ בעלי הרשאות לנושאים נבחרים ברכש ופיננסים לשאינם מורשים יש לציין את המצב שהיה בתחילת הבדיקה לפני התיקונים שביצעה הרשות בעקבות הבדיקה- לגבי בעלי הרשאות עידכון רכש ופיננסים לנושאים הנבחרים לאלו שאינם מורשים
בדיקה א:			
			האם נמצאו עובדים להם ניתנו כל 4 ההרשאות המפורטות להלן:
			פתיחת ו-או שינוי פרטי חשבון בנק לספק, אישור הזמנה לביצוע, פקודת תשלום והתאמת בנק
			האם קיימת בקרה מובנת אחרת הדורשת אישור של גורם נוסף במערכת?
			מספר עובדים להם ניתנו 4 ההרשאות?
בדיקה ב:			
			האם נמצאו עובדים שאינם נכללים בבדיקה א להם ניתנו 2 ההרשאות המפורטות להלן:
			פתיחת ו-או שינוי פרטי חשבון בנק לספק ופקודת תשלום
			האם קיימת בקרה מובנת אחרת הדורשת אישור של גורם נוסף במערכת?
			מספר עובדים להם ניתנו 2 ההרשאות?