

האם אי פעם נצליח להתגבר על סיכוני הפרדת התפקידים (SOD) במערכת ה-SAP?

מאת: אריאל אונגר, מנהל בכיר בפרקטיקת SAP Security & Authorization

לא מעט ארגונים מנהלים את ליבת התהליכים העסקיים של החברה באמצעות מערכת SAP (ECC, S/4 HANA) ודואגים לוודא שאכן הפעילות והמדיניות העסקית של החברה ממומשת בצורה תקינה במערכת. עם זאת, לעיתים מערך ההרשאות נדחק הצידה ואיתו גם הסיכונים העולים מהפרדת התפקידים הקיימים במערכת. מהם המושגים הבסיסיים בנושא, הסיכונים האפשריים, והחשוב מכל - הדרכים לטיפול?

מערכת SAP מאפשרת פלטפורמה גמישה ונוחה לעיצוב, פיתוח ויישום התהליכים העסקיים של הארגון במסגרת מתכללת אחת גדולה בשם ERP. כבודה במקומה מונח, אך המערכת נושאת איתה גם כמה "תופעות לוואי" בתחום עיצוב מערך ההרשאות של המערכת, אשר מחייבות את הארגונים לתת דגש ולפעול בכדי להפחית ככל הניתן את סיכוני הפרדת התפקידים והגישה לפעולות רגישות בקרב משתמשי המערכת.

אזהרת אקסיומה שגויה: בתהליך יישום ותחזוקת מערכת SAP בארגון נטייתו של הארגון המיישם היא לוודא שהמערכת תפעל בצורה תקינה וחלקה. לצורך כך שמים את עיקר הדגש על אופן פיתוח המערכת ברמה הפונקציונאלית, כשהמטרה היא "שהמערכת תעבוד". מה נוטים לפספס? לסיכונים ולקונפליקטים הנוצרים בעולמות הפרדת התפקידים (SOD) בקרב משתמשי המערכת, יחד עם "גרירת" הרשאות אצל המשתמשים לאורך השנים במעבר בין תפקידים שונים, נוצר מצב בעייתי של רמת סיכון גבוה שלרוב קברניטי הארגון אינם מודעים אליו ולחשיבות הטיפול בו. סיכון כזה יכול להיות קשור ליצירת הזמנת רכש והרשאות האישור שלה, עדכון מחירון, עדכון קטלוג, הרשאות לאישור שינויים וכן הלאה.

ריכזנו מספר מושגי ייסוד שכיחים בתחום הפרדת התפקידים שיש לשים אליהם לב:

1. **ROLE** - סל הרשאות המכיל בתוכו אוסף של פעולות עסקיות שונות, כאשר עבור כל פעולה מוגדרות הפעילויות השונות הניתנות לביצוע עבור כל פעולה עסקית, למשל כל הקשור לעולם התוכן של ניהול ספקים – יצירה, עדכון, צפייה וכן הלאה.
2. **משתמש מערכת (User)** - כל משתמש אנושי אשר מבצע כניסה למערכת ע"י הזדהות של שם משתמש וסיסמא ומבצע פעולות במערכת.
3. **סיכון הפרדת תפקידים (Segregation of Duties) - SOD** - מצב בו למשתמש בודד במערכת קיימות הרשאות לביצוע מספר פעולות במערכת המאפשרות לו לסגור מעגל/תהליך עסקי ללא התערבות של גורם (אנושי/אפליקטיבי) נוסף, למשל משתמש שיכול לעדכן פרטי חשבון של ספק ולאשר (לבד) עבורו תשלום.
4. **פעולה רגישה (Sensitive/Critical Action/Access) - S/CA** - פעולות עסקיות/אפליקטיביות שונות המוגדרות ע"י החברה כרגישות/קריטיות ועל כן רק לעובדים מסויימים/מוגדרים צריכה להיות להם גישה במערכת.
5. **חוקת הסיכונים - Rule Set** - מכלול הסיכונים השונים המוגדרים על ידי החברה כסיכונים בעלי פוטנציאל לפגיעה בפעילותה. עבור כל סיכון יוגדרו משתנים כגון: מזהה סיכון, תיאור, רמת חומרה, וההשפעה שלו על החברה במידה והוא מתממש.

היכן אנו פוגשים לרוב את סיכוני הפרדת התפקידים (SOD) והפעולות הרגישות (SA)?

סיכוני ה-SOD נמצאים לרוב בשתי רמות שונות במערכת:

1. ברמת המשתמש (User)- כאשר למשתמש בודד ניתנת הרשאה למספר רולים **שונים**, בכל רול ישנה הרשאה לביצוע מספר פעולות שונות וחיבור/התנגשות של לפחות שתי פעולות מרולים שונים מציפה סיכון מסוים. למשל: ברול מסוים יש למשתמש הרשאה, בין השאר, לביצוע הזנת הפרשי ספירת מלאי ולאותו משתמש יש הרשאה דרך רול אחר לאשר הפרשים של ספירות מלאי.
2. ברמת הרול (Role)- כאשר מראש בנו רול **בודד** במערכת המכיל בתוכו הרשאה לביצוע מספר פעולות אשר לפחות שתיים מתוכן מהוות התנגשות וסיכון מסוג SOD, למשל אם ברול A הגדירו הרשאות **גם** לאישור הזמנות מכירה **וגם** לעדכון מחירון, כך שכל משתמש שיקבל הרשאה לרול הזה, יקבל גם סיכון SOD מובנה.

סיכוני גישה לפעולות רגישות לרוב נמצא ברמת המשתמש (User), כאשר הפעולות הרגישות יכולות להיות פעולות של יצירה/עדכון וגם צפייה בנתונים רגישים. הפעולות הרגישות יכולות להיות גם בעולמות התוכן העסקיים אך גם בעולמות ה-IT הקשורים לניהול השוטף של המערכת, לדוגמה:

תחום	יצירה/עדכון	צפייה
פעילות עסקית	פרטי ספק, פרטי חשבון בנק הבית של החברה, עדכון נתוני שכר עובדים, פתיחת תקופה פיננסית.	נתוני שכר העובדים, דוח רווח והפסד, עמלות/הטבות לעובדים/סוכנים
IT/Admin	פתיחת מערכת לשינויים בסביבת הייצור, עדכון ישירות בטבלאות, שינוי מדיניות סיסמאות כניסה, עדכון הגדרות מערכת, ריצת תכניות ישירות בסביבת הייצור	סיסמאות/נתוני כניסה של משתמשי מערכת, גישה ללוח הבקרה והניטור של המערכת

איך ניתן לזהות את הסיכונים האפשריים?

ישנם מספר דרכים בהם ניתן להשתמש בכדי לגלות ולהציף את סיכוני ה-SOD וה-SA שיש לנו במערכת:

1. נהלי עבודה- הגדרת נהלי עבודה עבור הגורמים הרלוונטים בכל הנוגע לתהליך יצירה/עדכון של רולים במערכת ו/או עדכון הרשאות למשתמש וזאת בכדי לוודא כבר בשלב המוקדם של בניית הרול או מתן הרשאה לעובד שלא קיים סיכון SOD מובנה ברול ו/או שעצם מתן ההרשאה לעובד לא יציף עבורו סיכון SOD.
2. הגדרת רשימת פעולות רגישות בחברה- הכנת רשימה של פעולות רגישות אשר יש צורך לבצע עליהם ניטור ובקרה. רשימה זו מכילה את פעולות רגישות הרלוונטיות כמעט לכלל הארגונים ובנוסף פעולות רגישות בהתאם לפעילות העסקית של הארגון.
3. סקירה תקופתית של הרשאות- אחת לתקופה לבצע סקירה של כלל הרשאות המשתמשים במערכת ולאשר אותם מחדש ע"י הגורמים הרלוונטיים, בכדי לוודא תקינות והיקף ההרשאות בקרב המשתמשים.
4. שימוש בכלי/מערכות (GRC (Governance, Risk and Compliance)- שונים- הטמעה/שימוש בכלי GRC אוטומטי לצורך ניטור ובקרה און-ליין ו/או תקופתי של מצב ההרשאות והסיכונים בקרב משתמשי המערכת.

אילו פעולות ניתן לבצע על מנת להפחית את הסיכונים?

1. הסרת הרשאות עודפות/לא נצרכות הקיימות אצל משתמשי המערכת.
2. הגדרת בקורות מונעות/מפצות עבור הסיכונים השונים.
3. במידת הצורך, פיצול/שינוי תכולת הרולים בכדי להסיר סיכונים מובנים.
4. ביצוע פיתוחים/התאמה במערכת בכדי לאפשר בקורות אפליקטיביות שונות מובנות בתהליך העסקי.

אז מה למדנו? מערכת ה-SAP בארגון מאפשרת לנו פלטפורמה גמישה ונוחה למימוש התהליכים העסקיים של החברה במערכת, אך היא מביאה איתה גם סיכון רב בכל הנוגע להפרדת התפקידים בקרב משתמשי המערכת וגישה לפעולות רגישות. אם נכיר בעובדה זו ונדע לנטר את הסיכונים ולהגדיר עבורם מערך של בקורות מפצות נוכל להמשיך ולהשתמש במערכת תוך הפחתת הסיכון ככל הניתן.

אם אתם שוקלים לעבור למערכת SAP, או שעבר הרבה זמן מאז שעדכנתם את חוקת הסיכונים של החברה ואתם מעוניינים לוודא שאין למשתמשי המערכת שלכם אפשרות לסגור מעגל עסקי לבד, וברצונכם להפחית את החשיפה ורמת הסיכון של החברה? המומחים שלנו זמינים עבורכם.



אמירן ספיר

יועץ בכיר, מיישם
הרשאות SAP ו-GRC



אריאל אונגר

מנהל בכיר, מנהל פרויקט
ומיישם הרשאות SAP



עקיבא ארליך

שותף, מוביל פרקטיקת
הרשאות SAP