Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444

סיכום מפגש שולחן-עגול

ניהול זהויות והרשאות

(IAM/IDM)

מנחה:
סיגל רוסין

לקוחות נכבדים שלום,

תודה על השתתפותכם במפגש שולחן עגול Round Table בנושא ניהול זהויות והרשאות ארגוניות IDM IAM.

מצ"ב סיכום עקרי הדברים שעלו במהלך המפגש. במפגש עלו נושאים מהותיים שתומצתו בסיכום כפי שעלו. אין בסיכום זה המלצה גורפת ללקוחות אלא מתן פרספקטיבה והצגה של ההתלבטויות שעלו במפגש כלומר "מהשטח".

מפגש זה הינו מפגש שלישי ב STKI על תחום ניהול הזהויות וההרשאות. לפי הנראה ניכר כי השוק עבר תהליך מפוכח של הבשלה והתבגרות לקראת פרויקט מסוג זה. המשתתפים במפגש מבינים כי מדובר באחד התחומים המסובכים ביותר להטמעה בעולם אבטחת המידע וגוזרים בעקבות כך את ציפיותיהם. חשוב לציין כי הפרויקט חוצה ארגון ונדרשת תמיכת הנהלה ומודעות ארגונית להתחלת פרויקט בסדר גודל זה.

רוב המשתתפים והמשתתפות במפגש הינם מנהלי אבטחת מידע, תשתיות, מנהלי תחום ניהול הזהויות וממלאי פונקציות נוספות רלוונטיות. המשתתפים מייצגים מספר שלבי התפתחות בכל הקשור לניהול זהויות בארגון ולכן ישנם פערים בין השאלות שהועלו.

ברוב הארגונים מוטמעים פתרונות לניהול זהויות. בכל הארגונים הללו נמשכות ההטמעות גם היום (הרחבה והוספת מערכות\אוכלוסיות לפרויקט\ תחזוקה שוטפת).

במספר ארגונים בודדים התקבלה החלטה להתחיל פרויקט. פתרון מסוים נבחר ובשנה הקרובה הפרויקט צפוי להתחיל. וישנם ארגונים כי אין כיום פרויקטי IDM וניתנים מענים שונים "על פי צורך" לנושא ניהול הזהויות וההרשאות. ארגונים אלה בוחנים מפעם לפעם את התחום ואת הפתרונות המוצעים בשוק.

במספר ארגונים קיימות מערכות או פרויקטים "רדומים" –פרויקטים שהחלו לפני מספר שנים ונעצרו במידה מסוימת בשנים האחרונות מסיבות שונות.

בחלק מהארגונים סביב השולחן התעורר נושא ניהול הזהויות בשנים האחרונות. לא פעם מדובר בארגונים עם סביבות הטרוגנית ומשתמשים רבים עם הרשאות-על. במצב הקיים מנוהל תחום הזהויות על בסיס פתרונות ומנגנונים "מקומיים" שפותחו בארגון.

בברכה,

סיגל רוסין

תוכן עניינים

הקדמה

פרויקטים של ניהול זהויות והרשאות (IDM/IAM) נחשבים לפרויקטים מסובכים לביצוע ויקרים. לא פעם ניתן לשמוע כי פרויקט שהחל בסערה סובל מעיכובים רבים, או אף מבוטל בשל בעיות שונות כמו הגדרה של התפקידים בארגון, בעיות פוליטיות, תיאום ציפיות בין הארגון למבצעי הפרויקט וכן בשל אי הלימה בין מה שהובטח ע"י ספק הפתרון/ אינטגרטור לבין הלקוח הסופי.

יש ארגונים המתחילים מנושא ניהול הגישה של המשתמשים המהווה חלק חשוב מתהליך זה של ציות לרגולציות כגון SOX. מצד שני, אין שום התייחסות באף אחת מהרגולציות ליישום פתרונות לניהול זהויות כתנאי לעמידה ברגולציה אולם פתרונות אלה נותנים מענה לדרישות אחרות כמו ניטור גישה למידע רגיש. כמו כן, טכנולוגיות אלה מאפשרות ביצוע נוח ואוטומטי של בקרות על התנהגות המשתמשים וההרשאות בארגון הנבדק.

מעקב מסודר אחרי פריבילגיות והרשאות משתמשים במערכות הארגון הוא חלק אינטגרלי מתודולוגיות GRC- ניהול סיכונים.

בשולחן עגול נערך דיון פתוח בבירור מצב השוק בנושאים הבאים:

- מה צריך לכלול פרויקט כזה? (SSO, PKI, חיבור למערכות SIEM...)
- מי צריך להוביל את הפרויקט: IT, או"ש, HR, צוות אבטחת מידע, או אולי קצין הביטחון?
- איך מסתדרים עם הבעיות הפוליטיות שמלוות פרויקט כזה (הגדרת תפקידים, מהם התהליכים שמלווים כל עובד)?
- תיאום ציפיות: העובדים רוצים שהמערכת תעבוד מיד עם העלייה לאויר ועבור כל האפליקציות בארגון בעוד שאפיון והטמעה של מערכות אלה יכולים לקחת חודשים רבים ויותר. איך בונים בצורה בריאה את ציפיות הארגון מהפרויקט?
- מאילו אפליקציות/מערכות כדאי להתחיל? מאילו תהליכים ארגוניים?
- איך והאם ניתן להראות לארגון ROI מפרויקט כזה?
- מהם הפתרונות קיימים בשוק, והאינטגרטורים המובילים?
- עד כמה באמת חשובה איכותו של האינטגרטור להצלחת הפרויקט?

סיפורי לקוחות

מצב הארגונים כיום בתהליך ניהול זהויות והרשאות

לקוח אחד מספר כי הם נמצאים בשלבים מתקדמים עם המערכת, תהליך מאד קשה כבר שנה וחצי בתהליך. מגלים כל מיני בעיות שלא חשבו עליהם במיוחד באפליקציות הותיקות ב400as, אפליקציות שנכתבו בשנות ה70-80. כמו כן, אותו לקוח מספר כי כרגע נמצא בשלב של כתיבת RFP של מערכת IDM שהוגדרה ברמה מצומצמת תשתיתית, רק לנושא זה ולא אפליקטיבי. הכוונה היא להביא תועלת תפעולית לארגון- קיצור זמן מרגע כניסת העובד לארגון ועד שעובד. זה נושא כואב לאנשים. כל הנושא של טיוב ופחות טעויות כי היום אנשים עושים זאת. גורם לחוסר איחוד, ביקורות שעוברים. לפני ביקורות עושים המון עבודה ליישר קו. הביקורת הולכת ומכבידה. מאד פוחדים מהעלויות הגבוהות של פרויקט כזה, בהטמעה של מערכת IDM. לכן מפחד לקרוא לזה כך בחברה. אנשי הביזנס והגופים העסקיים פחות מעורבים פה ולקוח אחר מציין כי זה לא תקין. מי שתומך ומלווה זה אנשי מערכות מידע המכירים את כל ההרשאות, זהויות, טבלאות והשילוב בינהם. אנשי הביזנס עושים היום אישור הרשאות במערכות

ויש תהליך נפרד לזה כיום. עדיין אין אוטומציה להרשאות רק בקרת הרשאות. עד אז היו מנהלים באקסלים.

לקוח נוסף מספר כי לאחר הטמעת המערכת של יבם היום מרגע שאדם נקלט לארגון לוקח גג 6 שעות בסניפים בחו"ל להתחלת העבודה עקב הפרשי שעות. הבעיה הארגון היא נושא הקב"ט האחראי לסיווג העובדים והוא שולט בנושא זה, שגורם לפעמים לעיכוב. מבחינת עלויות 50% עובדי HR על המערכת ו50% עובדים חיצוניים לא מוכרים והם גם מחליטים על גיוס העובדים. יש פה בירוקרטיה העלות הכספית של עובד גדולה וזה חלק מהבעיה. הכל תלוי בIT לתת גישה מהירה לעובד להתחלת עבודה אחרת יש בזבוז שעות עבודה.

לקוח אחר מספר כי היום הארגון נמצא בשנה ה-11 לתחזוקת פרויקט ניהול הזהויות עם יבם. תחום ניהול זהויות מורכב 2 פרויקטים : ללקוחות הארגון- צוות ייעודי 5 איש, פנימי- 10 איש המחולקים ל- 3 צוותי עבודה: פיתוח ליצירת ממשקים לחיבור לIDM, תשתיות- תחזוקת המערכת 24/7, מאפיינות אחת ללקוחות המערכת כמו סניפים בחו"ל, בארץ, ספקים, הנהלה ראשית והשנייה בונה את כל מודל ההרשאות הפנימי ודואגת שכל הזמן יהיה סדר. יש בארגון מעל 10000 עובדים ויש גם ספקים ולקוחות יש מעל מיליון . יש ספקים היושבים ב SAP הפנימי אם יש לו כרטיס ואם אין לו כרטיס עובד והוא נותן שירות חיצוני אז יש ממשק למערכת חיצונית לIDM.

לקוח נוסף מספר כי הם התחילו להטמיע נהלים בשנתיים האחרונות בקשר לבניית יוזרים והקצאות זמן להרשאות ואישורים. בעיקר שימוש בסקריפטים ידניים, בעיקר באו להקשיב.

לקוח נוסף גם בא לשמוע להתעניין במה שקורה. כיום יש מאגר של משתמשים בAD, ששם הכל מסודר כולל חברות בת. נושא ההזדהות יחסית מאורגן, חוץ מיועצים חיצוניים או ספקי צד ג'. כל מי שמשתמש חייב להיות בHR, לא כל האוכלוסיות קיימות שם. מי שלא בHR, זה בAD. כרגע הכל מתבסס על AD, גם SSO, גם 400AS יהיה מאורגן בחודשים הקרובים. הנושא של provisioning הוא הבעיה. כיום הוא ידני ולא מספיק טוב. אין בקרה יזומה בנושא, אך עקב הSOX זה מניע אותם להתחיל פרויקט זה.

לקוח אחר מספר כי כל נושא הביקורת ושיפור השירות מביא אותם לפרויקט כזה, נעזרים ביועץ חיצוני לגבי איך לתקוף את הבעיה ואיזו מערכת. יועצים חיצוניים העובדים מולם מתחברים מרחוק למערכות

ארגוניות, העמדה עצמה עצמאית לאותו יועץ חיצוני. מי שנמצא ברשת הארגונית אין הבדל בין העמדות כל אחד יכול להיכנס מכל עמדה ולקבל את ההרשאות שלו- זה הכוונה בניוד עובדים. העובדים החיצוניים נמצאים בסביבת הDMZ, ועושים לוגין לAD חיצוני. יש להם הזדהות ביומטרית בקטע מסוים אבל לא של העובדים בכניסה למחשב. עשו פיילוט בנושא של הזדהות עובדים בצורה ביומטרית וזה לא צלח עקב תשתית מיקרוסופט מוגבלת, יש להם רק בכרטיס חכם. זה לא מספיק אמין ויש להיעזר ביצרן אחר להזדהות. המוטיבציה הינה שיפור שירות, אוטומציה ויעילות- אך ROI לא רואים פה. קשה להראות צורך עסקי מובהק, תועלת כספית- הפרויקט מאד יקר וROI לא נראה כל כך. אם זו תועלת חיצונית מובהקת יש ROI, וזו בעיה. נושא הרגולציה גם משפיע פה SOX. עדיין מתלבטים איך תוקפים את הבעיה הזו ובעיקר באו לשמוע. כרגע מנסים ליצור חוקה ברורה עבור העובדים ללא שרשורים , התחילו מיפוי חוקה מסודר- בסיס.

לקוח אחר מספר כי לאחר הטמעת מערכת NETIQ-נובל, היום התשתית מבוססת על תפקידים עם מיפוי , ישנם המון טעינה של קבצי אקסל למערכות מסוימות ומנסים לעשות ממשקים בינהם כדי שיהיה אוטומטית. האתגר הוא ספקים בחוץ והם ירצו בעתיד לעשות federation איתם, היום הכל פתוח ויש לשתף עוד גורמים באוכלוסייה לגשת לאתר הארגון. הם עובדים עם גורמים נוספים בנושא ליצירת עץ היררכי מורחב יותר. לוקח זמן עד שה IDM נתפס בארגון וכמות הפניות גדלות בחיבור למערכות, זה כמו "תמנון". 4 שנים מהרגע של הזיהוי במערכת ועד אוטומציה לקח לארגון – יש הרבה עבודת או"ש לפני. לפני היו המון פרויקטים בנפרד לכל מערכת וניהול הרשאות בכל מערכת בנפרד. היום זה לא ככה, הכל מקושר לIDM, מקושר לAD והכל במקום אחד. IDM הוא מנוע שיושב על מאגר הנתונים על DB התפעולי ובודק את השינויים, אם מישהו לא נמצא שם הוא מפיץ בהתאם כולל הרשאות.

לקוח נוסף גם בא לשמוע מה קורה בנושא ניהול זהויות, כולם רואים פה תהליך ארוך ומיגע שרצו להתחיל לפני מספר שנים. הלקוח טוען כי אצלהם הנושא מסובך היות ויש הרבה פוליטיקה ארגונית, וגם כספית. לדעתו יתחילו להיכנס בשלבים קטנים.

לקוח נוסף מספר הם עדיין לא התחילו תהליך ניהול זהויות רק נעזרו כבר שנה ביועץ מSECOZ לבחינה של הצורך והתהליכים. הנושא הגיע כמענה לצרכים עסקיים, שירות טוב יותר וזירוז תהליכים עסקיים. בגיוס עובד לוקח עד שבועיים להקים אותו במערכות, כמה מערכות יש אדמינים שונים בכל מערכת. הנושא נופל במחלקת אבטחת מידע ונמצאים בשלבים של RFP, יש כבר עץ ארגוני שהיועצים הרכיבו.

מיפו את כל התהליכים ונכסי המידע, ממפים נתונים בפלטפורמות מרכזיות בארגון לשם התחלת הפרויקט. היום לכל מערכת יש תהליכים פנימיים ולוקח זמן, מערכות תפעוליות ישנות UNIX. כיום ישנם מנגנוני הרשאות עבור כל מודול וזו בעיה. זה מכביד על הארגון, SSO פותח על ידי הארגון דרך הפורטל הארגוני, וכל המערכות העיקריות פועלות דרכו.

לקוח נוסף מספר כי כיום הצוות שאחראי על המערכת שנבחרה VELO הוא 3 איש ומטפל מעל 1500 עובדים כאשר הפרויקט מנהל באבטחת מידע עם ליווי של מנהל פרויקט. חשוב לציין כי המערכת מטפלת בניהול זהויות של עובדי הארגון ולא כלפי חוץ- לקוחות הארגון.

לקוח נוסף מתחום התשתיות מספר כי הם רכשו את מערכת TIVOLI של יבמ לפי מכרז וביחד עם סקוז עושים את היישום. נמצאים ממש בהתחלה ומנסים להבין איך ניתן להטמיע מערכת כזו בצורה הכי נכונה והגיונית לארגון כאשר הם מסתכלים על היבט השירות – נגישות לעובד חדש למערכות הארגוניות והתחלת עבודה מהירה עם הרשאות מסוימות והיבט נוסף של אבטחת מידע.

הסיבות לכניסה לפרויקט

אחד הלקוחות מספר כי הצורך במערכת כזו הגיעה מהרגולציה –SOX- ניהול תהליכים ארגוניים בצורה מסודרת. זה עוזר מאד לביקורת שבאה לבדוק את התרחשות התהליכים הארגוניים ומתן ההרשאות. כיום, ביקורות שיש לארגון הולכות ומעמיקות בנושא התהליכים הארגוניים וזה הוביל את הארגון לנושא IDM.

לקוח אחר טוען כי IDM זה אסטרטגיה ובהתחלה לפני מספר שנים הפרויקט של ניהול זהויות הגיע מאבטחת מידע והפרויקט נכשל מהסיבה כי אבטחת מידע לא יכול לקחת אחריו ארגון שלם כולל HR, עסקי וזו בעיה. לקח להם 3 שנים לחשוב וקיבלו דוחות מהרגולציה וביקורות. הגיעו לסיטואציה להשתמש במחלקת הביקורת הארגונית לבדוק אם יש בעיה בארגון. א"מ באה לביקורת ואמרה לעשות ביקורת על הרשאות ארגונית. בלי הביקורת הזאת לא הייתה אופציה להגיע להנהלה לפרויקט כזה. ראו דו"ח גרוע של ביקורת ועלה למנכ"ל והרגולציה ראתה זאת, ראו שיש בעיה מההנהלה. יש דיון הנהלה המסביר למנכ"ל מי הבעיה, "נהג האוטובוס" של הפרויקט זה הIT, HR לא יכולים לארגן תהליכים טכנולוגיים ולא המחלקות העסקיות כי תפקידם למכור. מי שלא יכול לארגן תמיכת הנהלה בפרויקט כזה זה לא יצליח. לדעתו אם אין תמיכת הנהלה עדיף ללכת לפתרונות כמו AVEKSA. זהו פרויקט מנכ"ל וחובה מעורבות הנהלה, לא מנהל אגף אלא מנכ"ל. רק שנה וחצי לקח זמן להסביר לארגון למה יש צורך

בפרויקט זה. חובה אסטרטגיה אחרת הכישלון ידוע מראש. לא ניתן לעשות זאת היות וזו לא האג'נדה של הארגון.
לקוח אחר טוען כי אחד הדברים החשובים הינו ברגע שעושים סדר, ניתן לנהל מעקב תקין של ביקורת למשל SOX. בארגון אחר מספרים כי ניתן לעקוב אחר הפעולות וכך לדעת על אותו האדם. לכן, אין מצב שעובד אחר יעבוד עם אותו משתמש שלעובדת בחופשת לידה או בחופשה רציפה . כל המערכות בנויות ככה כי המשימות לא מוצמדות לאדם באופן אישי אלא לאותו תפקיד. למשל, פקיד במחלקה מסוימת כל הפקידים יראו את משימותיו. אם מישהו לא נמצא בארגון, הוא למעשה לא עובד אז אף אחד לא נוגע ביוזר שלו.

לקוח אחר מגיע מאבטחת מידע ומספר כי התחיל את תהליך ניהול הזהויות עקב רגולציה. מבקרי SOX באים למשאבי אנוש ובודקים דרך IDM ורוצים לראות התאמה מלאה בתהליכים. נמצאים כבר בפרויקט 5 שנים ואפשר להכתירו לדעתו כסיפור הצלחה. כלומר, המערכת עובדת והם רק מתחזקים אותה.

אחריות הפרויקט בארגון

אחד הלקוחות מספר כי הנושא מטופל על ידי מחלקת אבטחת מידע וטוען כי זה כאב ראש מאד לאנשי אבטחת מידע ולדעתו לא צריך להיות ככה.

לקוח אחר מספר כי בארגונים גדולים לדעתו האו"ש צריך להתעסק בזה, כמו שנאמר מקודם טכנולוגיה זה לא הנושא אלא הניהול תהליכים משהו שבא לשנות ארגון ואיך כל אחד עובד היון- מכניס את כולם לסדר ומשקל. תהליכי provisioning, מתייחס ושינוי עבודת HR. והערנות של אבטחת מידע- הבלאגן בניהול זהויות. הם ערים לבלאגן המתרחש בארגון. לקוח אחר רואה עצמו כלקוח של פרויקט זה ולא מוביל פרויקט. יש למצוא את הגוף הבעל עניין יותר גדול בפרויקט זה.
השאלה מהי המטרה בפרויקט כזה? אבטחה למשתמש או תהליכים. לדעתו אמור להגיע מהאבטחה, כי אף אחד לא מתעניין באבטחה חוץ מגוף א"מ. אם אבטחה לא יקבע שאדם שנוצר בHR מקבל הרשאות ופרופיל מסוים לפי מערכות מסוימות הכל תלוי באבטחת מידע.

לקוח אחד מספר כי הצליח לעניין את ראש האגף- מנהל התפעול בנושא פרויקט IDM. אח"כ סמנכ"ל אגף משאבי אנוש, התחילו לשכנע למעלה אנשים כדי להרים פרויקט זה. היה ברור להם שאם לא יבוא מלמעלה זה ייכשל ואין טעם להתחיל בפרויקט זה.

לקוח נוסף מספר כי זה פרויקט ברמת הארגון מי שיוביל את זה אבטחת מידע וIT, כי אף אחד לא ייקח אחריות אבל לפחות המנמ"ר בארגון גדול צריך להיות מודע לזה. בשנת 2002 עשו RFP עם יבמ. המתחרים בתחום נשארו אותם מתחרים. עשו POC ל AD לראות איך עובד, בהתחלה לא האמינו בפרויקט זה וקיבלו תקציב קטן. בתקציב זה לקחו בהתחלה 4 מנהלי סניפים ומנהלת מחלקה שמתאמת בין הנהלה ראשית לסניפים ו2 אנשי א"מ. התחילו לשכנע את הגורם העסקי שלפחות לא יפריע בהמשך. כך זה התחיל כי הם לא רוצים שיפריעו להם בתהליך עבודה יומי שלהם, כי מנהל הסניף היה בהתחלה מנהל אותם הרשאות וזה היה נשאר רק אצלו ואף אחד לא מפריע לו. כאשר עשו סדר איתם גייסו את מחלקת הביטחון היות ובארגון גדול ומבוזר מישהו צריך להוציא כרטיסים ושהעובד בסניף לא יחכה. הייתה דרישה עסקית והפרויקט רץ בתוך א"מ והארגון מבין זאת לבד. א"מ דוחפת את הפרויקט מול הארגון והיום נלחמים לא להכניס מערכות לתוך הIDM, היות וזה כבר מפלצת ויש לפתח את תהליך ולחבר עוד מערכת, בקרות, תהליכי אונליין , ניטורים. היום זו תשתית לכל הארגון אוטומטית. הלקוח מציין כי שהתחיל את התהליך הבין אחרי חצי שנה שמשאבי אנוש לא יודע אילו עובדים יש לו בארגון ולמי הוא משלם משכורת, אין להם מושג לגבי היררכיה תפקידית בארגון. בהתחלת הפרויקט א"מ טייבו את הנתונים עם משאבי אנוש וא"מ קבעו את ההירכיה והתפקידים בארגון. למעשה א"מ עשו למשאבי אנוש סדר בכמות העובדים בארגון גדול. משאבי אנוש לא יכולים לשנות כלום הכל תלוי בא"מ. מי אחראי לתכולת התפקידים- תכולה עסקית היות ויש ממשק בין ההנהלה לסניפים, בין הIT לצד העסקי יש דו שיח שמקיימים. אם רוצים להוסיף תכולה/הרשאה לתפקיד יש תהליך מסודר. לפני יציאה לפרויקט יש לבדוק בסניפים וגורמים עסקיים בדיוק להגדרת הפרופיל. הצד העסקי מתאר את הפונקציונליות העסקיות והאבטחה מתרגמים זאת למערכות והרשאות. מחליטים ביחד איזה הרשאות יש לתת לאותו עובד. יש עובדת המאפיינת בתוך הפרויקט את התפקידים, יושבת עם כל הגורמים וכותבת את דרישותיהם לגבי אותו תפקיד. היא למעשה מעין מתווכת.

לקוח אחר מספר על התהליך אצלו בארגון הייתה מערכת ניהול זהויות לא access management, לא הרשאות גישה, אלא ניהול זהויות כבר 20 שנה שהייתה בMF. המערכת נתנה הרשאות בחלקן אוטומטיות וחלקן ידניות לכל העובדים בארגון ואנשי ההנהלה. למעשה העובדת שניהלה את המערכת פרשה לפנסיה והארגון נתקל בבעיה, זה מה שדחף את הארגון לפעול בנושא ולהחליף מערכת לניהול זהויות.

לקוח אחד מספר כי זו בעיה בתור אנשי אבטחת מידע- תשתיות , קשה להכריח את משאבי אנוש לעשות את הקשר הזה. במידה והייתה הנהלה חזקה המצב היה שונה ואולי הקשר בין האבטחה למשאבי אנוש היה אחרת. לקוח אחר טוען כי זה לא נכון, בכל ארגון המטרה להגדיר מישהו מנהל מחלקה למרות שהוא קשור לתפקיד אחר או מנהל סניף וקשה להשפיע על זה כי הכל זה מההנהלה. זה החלטות מלמעלה וקשה להגיע לשם. צריך להשתדל להסתדר ויש להחליט איך עובדים בצורה הכי טובה. הרבה ארגונים חיים עם המציאות הזו אבל יש יותר סדר בהרשאות בצורה אוטומטית כולל אימייל. בהנהלה זה המקום היחיד בו ההתערבות ידנית. בסופו של דבר, צריך להגיע לאוטומציה פה.

לקוח נוסף מתלבט בשאלה מי עושה זאת? תשתיות? כרגע זה נופל בIT, מי יכול להוביל פרויקט כזה? משאבי אנוש לא מעניין אותם ולא מכירים ולא ניתן לסמוך עליהם. אולי למעלה מנכ"ל, כי יש הרבה גורמים עסקיים אבל איך משכנעים ניהול זהויות? הכל פה זה אסטרטגיה, יש מנכ"ל קשוב למנהל אבטחת מידע, או רק להשתיק אותו. אם אבטחת המידע בארגון חזקה יש יכולת להקים פרויקט כזה, להפך הסיכוי אפסי. חשוב להשתמש בגורמי הבקרה והרגולציה וזה יעלה למעלה בצורה קלה יותר. הטיפ הוא שניתן לעשות זאת, מסובך אך אפשרי. יש לרתום את הארגון יחד, לא רק משאבי אנוש, הרגולציה פה קובעת ויש ועדת היגוי בנושא. חשוב להיעזר בביקורת וניהול הסיכונים. חשוב להיעזר במישהו להמשך הדרך.

לקוח אחר מספר כי אצלהם יש מחלקת ניהול זהויות תחת אגף תשתיות הכוללת 10 איש. הארגון מחולק לשני ארגונים כך שאחד עובד עם SAP, והשני עם מוצר אחר- פיתוח שלהם. אילו 2 מקורות מידע לIDM, משם הנתונים זורמים לIDM ולמערכות הקצה.

לקוח נוסף מספר כי מי שאחראי על פרויקט זה מחלקת הפיתוח יחד עם התשתיות כדי לנסות להבין איך משלבים את התהליך עם מערכות שנמצאות בפיתוח או יפותחו בהמשך, איך יכניסו את הROLL כבר לשלב האפיון ופיתוח ההרשאות של משתמשי המערכת החדשה בפיתוח. יש לציין כי בארגון רוב המערכות מפותחות פנימית ולכן החיבור למחלקת הפיתוח חשוב מאד.

סוגיות טכנולוגיות בהטמעה

אחד הלקוחות מספר כי הטמיע מערכת בשם Aveksa שמטרתה לתמוך בכל נושא אישרור ההרשאות ולפתור בעיה זמנית אך היא יכולה להפוך בהמשך להיות מערכת provisioning. הלקוח טוען כי יש לה

מודול כזה ואין לדעת מה יהיה אולי יספיק או לא לארגון. לקוח אחר אומר שזה לא מספיק טוב אך עדיין לא התקבלה החלטה ארגונית. לדעתו פרויקט כזה צריך להוביל PMO כי זה חוצה ארגון, הכי הרבה עבודה זה מול אנשי מערכות המידע בהקמה. יכול להיות כי שזה הHR, אך אין להם ידע טכני והם לא מכירים את התהליכים הארגוניים ואין להם עיניין בכלל בנושא זה.

לקוח נוסף מספר כי התחילו ב2007-2008 לדבר על מערכת IDM. אחרי הרכישה של המוצר שנה וחצי אחרי הפרויקט כולל ROLLS 5000 לכל סביבה, כולל MF. החלטה אסטרטגית ארגונית כל מערכת חדשה שקמה עוברת דרכו והוא מנהל אותה. הפרויקט כולל עץ אירגוני מסודר והירכי ממשאבי אנוש. יש סביבת טסטים, AD מסודר. חייב להיות פלטים מכל מקום. עובדים עם יבמ TIVOLI. מה ROLL נגזרות ההרשאות למערכות. יש לאגוד אותם לתפקידים ובעזרת ה SAP הכל היה. מבנה ארגוני ומבנה ארגוני ב SAP לא אותו הדבר. התפקידים בנויים בארגון אך במערכות פתוחות שמנהלים הרשאות באופן פרטני זה יותר קשה. אם אין סדר במערכות הללו, בניית תפקיד בסיסי אם לא קיים חבל על הכסף והזמן. חובה לבנות קודם תהליכים בארגון. אם יש כבר בנוי זה חיסכון של 2-3 שנים ויש גוף מסודר שאחראי על הרשאות. אם מתחילים לבנות עכשיו את ההרשאות עם משאבי אנוש זה לפחות לוקח שנתיים תלוי בגודל הארגון ואין טעם לרוץ לבחור מוצר. הפרויקט התחיל עם 2-3 עובדים והיום כבר 8 עובדים בנושא זה באופן מלא. בארגון הקב"ט אחראי לנהל ולחלק את הסיסמאות וכרטיסי העובד. כמובן שעם כוח גדול באה אחריות גדולה- טעות קטנה בכח אדם עובדים יכולים בטעות לא להיות קיימים. כאן צריכים להיות מאד זהירים גם מבחינת שירות הארגון והפסדים ארגוניים. חשוב שלא יהיו אשליות שאם לוקחים מוצר מדף יש גם המון סקריפטים ג/אווה ותהליכי עבודה מורכבים זה לא פשוט, זה מחייב דיווח על כל דבר. הם לקחו את כל בסיס הנתונים והעבירו לBO, לדיווח אמיתי. אין דוחות אמיתיים דרך מוצר IDM וזה חסרון. תמיד לוקחים מוצר אחר לנושא הדוחות וחתכים מורכבים יותר. האינטגרטור פה הוא יבמ והפרויקט מוגדר בארגון כמוצלח.

לקוח אחד מספר על תהליך בארגון של קבלת עובד בארגון. חשוב להתחיל פה- משאבי אנוש מכניסים אותו למאגר לא חשוב באיזה מקום בארגון הוא בסוף יתקבל למרות שיש המון סניפים פזורים בארץ. למחרת מתחיל לעבוד, מגיע בבקר והולך לעמדת הנפקה לכרטיס עובד. מגיע לעמדה שלו ויש לו סט הרשאות הבסיסי בהנהלה ראשית והעסקי בסניף. פקיד בסניף מקבל אוטומטית את סט הרשאות שלו כי זה קל מבחינת ROLLS. ככה מתחיל היום בארגון לעומת בעבר שעובד שהגיע היה צריך לחכות 3 שבועות עד לתחילת עבודה. 11 שנים לפני התחילו וזה הפרויקט המודרני הראשון של הארגון של ניהול

זהויות בארץ והצליח יפה. כיום לאחר 30 שניות וחצי עובד מתחיל לעבוד עם סט הרשאות בסיסי בהתאם לסניף. עובד בסניף מקבל מה שצריך ונקבע לפי הפרופיל בסניף ועובד עם זה לעד. זה לא משתנה ואף אחד לא נודע בזה. ב SAP מזרימים אוטומטי את ההרשאות ויש לו את כל המערכות שצריך בהתאם לפרופיל שנקבע. הדרישה העסקית הייתה לקחת עובדים ולהפעיל אותם עם הרשאות כמה שיותר מהר כי כאן זה השירות ללקוח. כאן נולדה הדרישה וכך העסק התחיל לרוץ מול הסניפים עצמם. היום הארגון נמצא בשנה ה11 עם פרויקט IDM. הפרויקט התחיל עם עובד אחד של הארגון אינטגרטור חיצוני לתשתיות securenet, ייעוץ של אירית פוטר IPSEC לייעוץ טכנולוגי , אופיר זילביגר- SECOZ ייעוץ עסקי.

בMF הסוכן לממשק ה IDM לא דורש יוזר מיוחד, אך יש מערכות וממשקים שדרוש יוזר מיוחד ADMIN לחיבור לIDM. אותו סוכן מותקן על הMF, עושה provisioning לכל הפוליסי בIDM לתוך MF. הפקידה במשאבי אנוש מעדכנת אותו סוכן אם יש הרשאה מסוימת בMF.

לקוח אחר מספר כי הוא בא מעולם הMF, וחשוב לציין כי בעולם הזה הכל מאורגן יש תפקידים ויש הרשאות. אך יש המון תזוזה של עובדים – עובד בסניף אחד ולמחרת בסניף אחר, או שעבר תפקיד. אם מוציאים את מתן ההרשאות מחוץ לMF, למעשה נותן למישהו אחר להגדיר את זה ושיתבצע בצורה אוטומטית בMF. לקוח אחר עונה בתגובה ומדבר על מודול הרשאות קיים היום ומשייכים משתמש לקבוצה, לקבוצה נותנים את כל ההרשאות על אותו משאב. למעשה זה מנוהל אצלהם רק חסר הרכיב שמקשר בין ה IDM לקבוצת המשתמש- זה מה שעושה הסוכן קישור לROLL. זה המיפוי של הagent ואז קיבלנו תהליך מלא. האם כל הפונקציונליות שיש כיום במחשב המרכזי עוברת למערכת קצה? הלקוח מספר כי אצלהם מי שעובר מחלקה הוא נמחק בניהול זהויות וה"שרביט" הוא אצל מנהל המחלקה העסקי או אצל משאבי אנוש. אם מנהל מחלקה מוותר על עובד, הוא מודיע למשאבי אנוש כי הוא עזב את מחלקתו, נמחק ישירות מהIDM, כדי להקימו מחדש מנהל מחלקה עסקי לוקח אחריות עליו ודורש להקים את אותו עובד במחלקה לה הוא עבר- זה עובד טוב היום.

משאבי אנוש מגדירים אותו במחלקה אחרת ומערכת הIDM אוטומטית מקימה יוזר במחלקה אחרת, העובד לא ממשיך עם אותו היוזר למחלקה שונה. חשוב לתמוך בתהליכים הללו היות והעובדים זזים ממחלקות שונות ותפקידים שונים- זה כל הפן העסקי בתהליך IDM. במקרה מיוחד יש לתת הרשאות ידניות אם צריך למערכות ספציפיות- זה החלק המסובך. רוב הארגונים אין להם כל כך הרבה מערכות.

לקוח נוסף מספר כי הם בחרו בנובל NETIQ שחברת פרולינק יישמה להם בצורה טובה. הארגון נעזר בעופר גיגי לנושא, היות והיה להם קשר כבר לפני לארגון היה סדר זמנים מאד צפוף היות ואותו עובדת פרשה, למעשה כל חלק של הקמת הזהויות שרובן ניתן באופן אוטומטי עשו בתוך שנה. כיום נותנים באופן אוטומטי את כל הרשאות העובדים עפ"י התפקיד, מחלקה, וכמובן המערכת קשורה לכח אדם HR, ומערכת ניהול הרשאות כאשר דרכם ניתנות ההרשאות. לא ביקשו את שיתוף הפעולה מHR, כי זה קשה אלא לקחו את התפקידים הקיימים כבר לפני. להנהלה זו בעיה לתת הרשאות היות ומשאבי אנוש לא מעדכנים בצורה מסודרת את העץ ההיררכי הארגוני ולכן כל מה שקשור בעובדים מנהלים יש ממשק עם הIDM דרך מערכת HR. אך לגבי סוג העובד וההרשאות זה במקרה ההנהלה ידני. בעתיד אולי יגיעו למצב בו הכל יהיה אוטומטי. היום הארגון רוצה להיכנס לנושא SSO, למרות שארגונים התחילו מזה. כנראה ימשיכו את SSO עם NETIQ אותו מוצר. השאלה היא איך הכניסה למערכות? האם נדרש פורטל ארגוני?

לקוח אחר מספר כי סיים פרויקט SSO לפני שנתיים ולדעתו הוא נפרד לחלוטין מכל נושא ניהול זהויות. SSO מאפשר לאותו עובד להיכנס אוטומטית למערכת אם כבר נמצא בדומיין, למעשה הוא מזהה את חלון ההזדהות ומקליד במקום העובד. יש להפריד בין ההרשאות לבין נושא ההזדהות אליהם. בארגון יש פורטל ארגוני ונותנים אייקונים לפי הרשאות העובד, sandbox לכל סניף, כל עובד מקבל את אותם אייקונים למערכות בהם יש לו הרשאות. אם העובד נכנס פעם ראשונה למערכת , SSO לומד זאת ומכניס אוטומטית את העובד. זהו agent שמותקן על התחנה. ברגע שאדם עשה לוגין לרשת, כל מערכת שקשורה לAD אותו עובד מזדהה אוטומטית. הבעיה היא לא במערכות שנשענות על AD, אלא במערכות אחרות שלא קשורות כלל לAD. יש לתת התממשקות לשרתים לאותו AD.

לקוח אחר מספר כי אצלהם יש תמיכה- מפעילים ששם גם הכל מאורגן ובימי שישי במידה ויש הרשאה חריגה מחוץ לשעות העבודה- לא נותנים יום שישי. זה היה קשה לשכנע את הארגון אבל הצליח. הרשאה חריגה יש לבקש מראש, לאשר מראש ואז אחרי workflow מסוים העובד יקבל אותה.
ישנם מערכות בהם אין agent מרכזי והם לא יודעות לדבר עם מאגר מרכזי כמו AD או LDAP, אין ברירות: לייצר תהליכי BATCH ידניים שטוען אל המערכת- מבחינה טכנולוגית אין ברירה או שרואים עד כמה המערכת חשובה, סוגי פרופילים וכמה ערך יש פה- אם היכולת לתת ערך קטנה ביחס להשקעה לא נכנסים לאותה המערכת. זו השקעה רבה לפתח ממשק ל IDM עבור כל מערכת שיש מאות מערכות ארגוניות. לארגון יש המון מערכות כל פלח יש קשת של המון סוגי מערכות, למשל בMF ישנם עשרות

אפליקציות שונות שיש לממשק ל IDM וזו הבעיה. אף ארגון לא מנהל את כל המערכות שלו לגמרי. באותו ארגון רק לפלטפורמות המרכזיות יש סוכנים.
בתוך הארגון יש גם ניהול של SSO (single sign on). יש אפליקציות ויש מערכות צד ג' שהארגון רוכש והם לא עובדות מול מאגר מרכזי ואין להם סוכן- אלא מאגר לוקאלי. אם חשוב לנהל אותם יש למצוא דרך , כמו שפיכת קבצים BATCH. דברים שפחות נעימים לארגון, אין אוטומציה אמיתית פה. השאלה כמה משקיעים באותה מערכת , עד כמה היא חשובה לארגון מבחינה עסקית ואוטומטית?
לגבי SSO, זה פרויקט שעשה המון סדר בארגון לפי טענת הלקוח. הם מימשו אותו בתצורה ביומטרית לגבי תשתיות הארגון, כרטיס חכם וביומטרית (אצבע)- לא ניתן להזדהות אחרת. מי שמסרב למסור תביעת אצבע לא יכול לעבוד בארגון. עדיף להתחיל מSSO, כי זה נותן הרבה יותר סדר בארגון.: מיפוי המשתמשים, הגדרת תהליכים, טכנולוגיות ואז מערכת ה IDM תשתלב בצורה קלה יותר בארגון.
מניסיון הארגון הכרטיס החכם נתן "שקט" – התשתית יקרה אך אין הסתבכות עם סיסמאות בארגון, זה חשוב ומוריד נטל מהאבטחה והתמיכה. לא ניתן לבוא לתחנה ולהזדהות כמישהו אחר. אך מעבר בין עמדה כולל הכרטיס והאצבע כן ניתן, כאשר מזדהים מרחוק (מחוץ לארגון) יש קורא ביומטרי.
איך מתמודדים עם מצב של עובדת בחופשת לידה ומישהו צריך לגשת למשימה בתור המשימות שלה? הארגון טוען כי אין התמודדות פה, היות וכל אדם הוא בעל הרשאות שלו בלבד. יש לעשות סדר בארגון בו יש מאדר קבצים משותף לאותה מחלקה וכל המחלקה יכולה לגשת לשם. כל המחלקה עובדת על אותו עולם תוכן, זה הגדרה בפוליסי – אותו מקום ברשת לכל המחלקה. יכול להיות גם שאותו מנהל מערכת יוכל להעביר את אותה המשימה למנהל המחלקה.
יש סיטואציה בעייתית בין הגדרת התפקיד בHR לעומת התפקיד האמיתי- מה התפקיד האמיתי? לכן חייבים למפות את הארגון ואת העץ ההיררכי. כך קל לעשות מיפוי תפקידים, בהנהלה ראשית השוני בין מתכנת שהופך לבודק הוא בעייתי יותר היות והוא צריך מערכות שונות. יש סט הגדרות תפקיד בHR, וסט הגדרות תפקיד בIDM, יש ליצור ROLLS הגורם העסקי מגדיר לאותו אדם בטרמינולוגיה שלו ואנחנו מפרשים זאת למערכת הIDM.

לקוח אחר מספר על פרויקט ההטמעה שלו עם מערכת נובל NETIQ. השלב הראשון הינו מיפוי העובדים בתוך הארגון לתפקידים, ספקים חיצוניים שיש לנהל אותם כי נכנסים למערכות הארגוניות. המוטיבציה לפרויקט הינה רגולציה , והכל התנהל באבטחת מידע. ישנם עשרות אלפי עובדים ומיליוני לקוחות, חשוב נושא השירות ללקוחות. הארגון חשף שירות חיצוני מערכת WEB, לפי ת.ז וכך הוחלט להגדיל את הפרויקט. רצו לתת שירותי הזדהות כלליים לכלל האוכלוסיות בצורה נוחה יותר. ישנם המון

מערכות בכל סניף, לא נעזרו בפרויקט חיצוני אלא רק מטעם הספק. האתגרים שלהם: העובדים מנוהלים במערכות המשרד, לפי תפקידים – זה היה יותר פשוט. הדבר נהיה מסובך אם צריך לתת לעובדים חיצוניים שהארגון לא מכיר גישה למערכות, למשל תקציבים. יש לתת לפקיד כלשהו שלא מכירים שירותי תמיכה והזדהות, איך יגיע למערכות הארגוניות, איך קולטים אותו, מי אמר שהוא זה הוא. לכן פיתחו חוקה ומי אוסף את הפרטים הללו, איך מגיע לIT. פילחו את האוכלוסיות, הנושא לא טכנולוגי ולא קשור למוצר. השאלה איך גורמים לפרויקט להמשיך? מצד אחד אבטחה לא מאמינה כי אותו אדם זה אותו אדם, כל מיני מנהלות בנושא: להסיר אדם וכדומה. לאט לאט מתמודדים עם נושא זה. פתרו את בעיית ההזדהות למערכות ארגוניות, וגם ספקים חיצוניים בדומיין אחר. עשו SSO בין האתרים וניתן לראות את הפורטל שצריך עם אותה סיסמא. היה להם פרויקט משותף עם מיקרוסופט לתקשורת בין מערכות חיצוניות, עם הזדהות דרך IDM. אחרי שלב ההזדהות, עברו לספק תשתית לשאר האפליקציות. עד היום ברוב המערכות מספיק היה שהעובד מזדהה לאפליקציה ולא היה ברור מה מותר לו או אסור לו בתוך האפליקציה. כל מערכת ניהל הרשאות בפני עצמה ורצו להיכנס גם לעולם זה. כאן נדרש לבדוק תפקידים בתוך הארגון ספציפית לאותם מערכות. ישנם המון מערכות וכל אחד טוען הרשאות אחרות: HR מגדירים מנהל מחלקה בצורה אחרת מאשר באמת נדרש בגישה למערכות. יש לעשות סדר וכאן הנושא אוטומציה. ברגע שעובד נקלט למשרד הוא ניגש ישירות למערכת שזקוק באותו היום ולא רק אחרי כמה ימים, מקבל אימייל. אך כדי להגיע למצב כזה היו צריכים לשבת עם משאבי אנוש ולהגדיר באופן מסודר מי המנהל באותו סניף, תקופות ביניים- הכל יש להסביר כדי שהכל יעבוד. בעיה נוספת יש תפקידים נוספים נישתיים בארגון שלא מנוהלים בHR, שזקוקים להרשאות בימים מסוימים. לכן היו צריכים לדבר עם משאבי אנוש בנושא כדי לא להמשיך ידנית. בנוסף, פיתחו המון ממשקים לIDM, כדי לעבוד בצורה אוטומטית מול כל הסניפים למשל מערכת תמיכה בסיסמאות, ניהול הרשאות- יש מישהו מוגדר בכל סניף במקום לפנות ישירות לIT. יש בעיות עקב כמויות ענקיות של משתמשים, היום מחולל ההרשאות שלהם נותן דברים ספציפיים לאותו עובד, אך אם לאותו עובד יש X תפקידים? מה עושים? זה אתגר בנושא מתן ההרשאות ויכול להיות בעתיד שיפתחו עוד בנושא. השלב הבא הוא גם אוכלוסיות בתוך הארגון ברמה יותר מעמיקה. אם עובד עובר מסניף לסניף- הIT רואים הכל במאגר כי הם מחוברים ישירות לשם ובהתאם ההרשאות ימחקו. יש מערכת מרכזית כ"א ששם הם בודקים את השתנה משהו מבחינת מעבר. כל היום יושבים על המאגר של משאבי אנוש כדי לראות אם משהו השתנה ואז אותו עובד מקבל אוטומטי, הרשאות יורדות ומקבל הרשאות חדשות. יש המון חריגים- עובד עם כמה תפקידים וזו שוב בעיה, בינתיים זה ידני אבל ישתנה בעתיד. העולם מתפתח ויש דרישות חדשות כמו מובייל וצריך להתקדם.

לקוח נוסף מספר כי המוצרים המרכזיים איתם המחלקה מתעסקת הינם IDM, access manger ו-AVEKSA. ל-IDM יש להם את נובל NETIQ. כיום קורה בארגון מעבר ל-AD, כדי לאפשר SSO מלא לאפליקציות שעובדות קליינט, ההצפנה דרך קרברוס. האפלקיציות WEB שעובדות SSO לוקח את התעודות מהדומיין הישן ויש קשר ל-IDM. כל מערכת בארגון עוברת דרך IDM. העבודה מול משאבי אנוש, כיום אחד הפרויקטים הגדולים במחלקה הינו מבחינת ה-AVEKSA, כל תהליך מתן ההרשאות. מתן ההרשאות נעשה ידני- יש 2 אנשים במחלקה המקבלים קריאות והם נותנים את ההרשאות. מה שקורה היום הינו באמצעות ה-AVEKSA בונים טופס למתן הרשאות בו המנהל או העובד יבקש הרשאות והוא ירוץ ב-ROLL למתן האישורים ובאופן אוטומטי יפעיל את ה-IDM להוספה או הורדה של הרשאות. IDM מבחינתם לא קשור ל-workflow, אך הארגון לא עושה בו שימוש. הם העדיפו להמשיך עם AVEKSA. הם מנהלים את המבנה הארגוני מה-HR (2 מערכות), מנהלים 2 מבנים ארגוניים. פרויקט שאמור להיות שנה הבאה הוא איחוד בין שני הארגונים שמרכיבים את אותו ארגון- כך למעשה תהיה מערכת אחת ל-HR. כי היום צורות העבודה מחולקות שונה בין 2 הארגונים, למעשה היום הכל אוטומטי חוץ מנושא מתן ובקשת ההרשאה לאותו עובד והאישרור. כל מערכת חדשה בתוך הארגון עוברת דרך IDM, בונים לה יישום לתוך מערכת HR באמצעותו נותנים את ההרשאות למערכת קצה. הבקשה נוסעת מה IDM ואז ל-HR. השלב הבא זה דרך AVEKSA למקם את זה דרך טופס בו העובד יגיש לקבלת הרשאות ולא ידני. הייתה מערכת סקירת הרשאות לפני בארגון, בארגון הייתה התלבטות לגבי בחירת מערכת להרשאות או להשתמש בנובל או באבקסה. נבחר לבסוף אבקסה היות ופרולינק ייעצו להם בנושא. כל עובד מזדהה בפורטל בו יש לו את כל הגישה למערכות המורשות לו, לגבי קליינטים עושים שימוש בקרברוס. יש להתקין אותו בתחנה, הכל תלוי במורכבות הארגון. חשוב לסנכרן בארגון בינוני- גדול מצד השרתים ולעשות יותר מאובטח ונכון, פחות תלוי בפורטל.

מדיניות של החלפת סיסמאות- יש מדיניות במקומות שניתן לאכוף אותה. ברור שיש מדיניות של החלפת סיסמה בתקופה. במערכות שמנהלות רשם משתמשים פנימי בעדיפות ראשונה מנסים להשעין אותם על AD. במערכת ישנות זו בעיה וכאן ניתן להכניס על בסיס קריטיות עסקית. הארגון משתמש גם בניהול סיסמאות של סייבראק. אפשר לפתח מוצר שיממשק מערכות ל-AD, מבחינת SSO.
צריך למצוא את אורך הסיסמא האופטימלי גם מבחינת מערכות MF ומערכות ווינדוס.

לקוח נוסף מספר כי בתחילת התהליך חשבו על איזה מערכות מתאימות וכל המתחרים הגדולים נפלו בבחירה שלהם. הם החליטו ללכת עם מערכת open source שנקנתה ע"י REDHAT חברת COVERTIX. המוצר נקרא VELO. המתחרים הגדולים נפלו עקב צרכים ארגוניים ייחודיים שהוגדרו על מנת לתת גמישות מרובה היות והארגון מאד דינמי. הארגון הלך לראות את המוצר פועל בארגון אחר והבינו שיש לו פוטנציאל מאד גדול. למעשה הארגון פעל בשיתוף משאבי אנוש והנהגה של הסמנכ"ל- אי אפשר בלעדי ההנהלה. משאבי אנוש יישרו קו עם IT, אבטחת מידע למד על מערכת HR והמבנה שלו זהו שיקוף של העץ הארגוני. כלומר, כל שינוי בעץ הארגוני אמור להשפיע ישירות על מערכת הIDM- אין פער בין מערכת ניהול הזהויות לבין העץ. העץ היה כבר מסודר, הם הבינו את המבנה שלו ולפי זה בנו את הROLLS. המערכת הראשונה שחיברו הייתה הAD. כאשר על מנת לעשות roll mining נעזרו בחברת ייעוץ חיצונית שנקראת THIS. הם שפכו את כל המידע של הAD לתוך אקסלים, החברה החיצונית ריכזו את הROLLS של נציגי השירות ואילו הרשאות אמורים לקבל בסוף. הם ערכו מעין ועדת היגוי עם מנהלי החברה על מנת להתאים את ההרשאות לכל תפקיד וכל ניתן להתאים למערכת ROLLS רלוונטיים. עד היום יש אחת לחודש ועדת היגוי עם הגורמים הרלוונטיים לפרויקט. מאז המערכת מאד התפתחה, ורוב המערכות הארגוניות מחוברות כאשר הארגון וכל המערכות מבוססות AD למעט MF שגם שם יש חיבור לIDM. הרבה פיתוחים פנימיים גם בנושא SSO. כיום הגיעו למצב שרוב המערכות מחוברות, כמובן שיש מערכות קטנות יותר שהם פחות בעלות חשיבות ומיעוט משתמשים שאין טעם לחבר אותם. פה הם נקטו בנושא של שיקוף הרשאות במערכות הללו. הארגון הבין כי תמיד מה שקורה בשטח "ינצח" למרות שיש ROLLS מסודרים. למשל, מתוך 10 נציגים יהיו 1 או 2 שיש להם הרשאות אקסטרה – בכירי שירות. גם את זה החליטו לנהל בIDM, יש להם ROLL לפי שם האדם, או ROLL לכל מערכת בין אם המשתמש זקוק לנגישות למערכת נוספת.

כיום נמצאים בתהליך של תיקוף הרשאות עם אותו ספק COVERTIX שמספק להם מערכת ייחודית שנשענת על הIDM. יש להם 2 אינטגרטורים שיושבים כבר 5 שנים בחברה ונותנים מענה לכל בקשות בנושא IDM: חיבור למערכת חדשה, טיפול בתקלות, דרישות תחזוקה ועוד. היום שעובד נקלט לארגון מהרגע שמשאבי אנוש סיימו להזין את פרטיו, לוחצים על אישור ויש לו יוזר מלא כולל על ההרשאות שצריך. אין צורך להשלים שום דבר למעט מערכות קטנות שלא מחוברות לIDM. בנוסף, כל תהליך זה לא היה אפשרי בלי החלטה גורפת של אבטחת מידע בה אין מצב שנכנס עובד בלי ידיעתם- הם בודקים את HR ויש להם הרבה טעויות. בארגון אבטחת מידע אחראי על כל הרשאות העובדים בארגון בכל המערכות. אותו ארגון מציין כי אין כל כך ROI כי במקום לעבוד ידנית אותם 3 עובדים מתחזקים את המערכת. כל הרשאה שניתנת היום היא אך ורק דרך IDM, לא נוגעים כלל במערכת הקצה. במידה

ותהיה תקלה או הארגון יחליט להחליף ספק עדיין תהיה האופציה לגעת במערכת קצה. לקוח נוסף שואל היות והמערכת קוד פתוח- כמה יכולות הארגון היה צריך לפתח בעצמו וכמה היה כבר בנוי במערכת? זה תלוי ארגון, אצלהם הארגון מבוסס AD, ובמערכת IDM יש API מובנה. יש דברים שהארגון היה צריך לחשוף API או התערבות של ספק חיצוני אם המערכת מדף. יש הרבה דברים שמומחי המערכת פיתחו לארגון מבוססי IDM. ההסתמכות בתפקידים היא על HR, אם המבנה הארגוני משתנה או נוסף תפקיד הIDM מודיע שאינו מכיר את התפקיד ואז אבטחת מידע מתחילים לתחקר את הצד העסקי, HR, מה בדיוק התפקיד ולשם מה קיים. כאן ההסתמכות הינה על גורם חיצוני וזה שיקול ארגוני וכלכלי של הארגון. לקוח אחר מאמין כי המערכת נמצאת בתוך הארגון והארגון צריך לדעת לתפעל אותה ולא להסתמך על מישהו חיצוני.

הפצת סיסמאות- הIDM עושה provisioning גם לסיסמאות, יש תהליך בIDM המוציא לעובד חדש סיסמא ומפיץ אותה לסמס או למייל של המנהל. בHR יש את כל פרטי העובד ולכן יש אפשרות לבחור איך להפיץ לו את הסיסמא. אחד הלקוחות מספר כי אצלהם שעובד מגיע ביומו הראשון הוא מקבל כרטיס עובד וחותם על ניירת, משאבי אנוש יכולים לחולל לו דרך המערכת סיסמא חד פעמית ונותנים לו אותה. אצל משאבי אנוש יש מחשב נוסף בו העובד החדש יכול להיכנס עם הסיסמא החד פעמית ולשנות אותה בהתאם למדיניות. לקוח נוסף מספר כי במהלך השנה האחרונה עובדים חיצוניים- מכירות פועלים בנוהל הזדהות חזקה ע"י טוקן חד פעמי נוסף ליוזר ולסיסמא. הטוקן נשלח לנייד וכך למעשה המובייל הופך להיות כלי זיהוי נוסף למשתמש. בהקמה של עובד חדש הIT שולח מייל מוצפן וטוקן לטלפון שבעזרתו ניתן לפתוח את המייל ולראות את הסיסמא הראשונית. כאן יש בעיה כי המובייל הופך להיות קריטי ואם המכשיר נגנב או אבד?

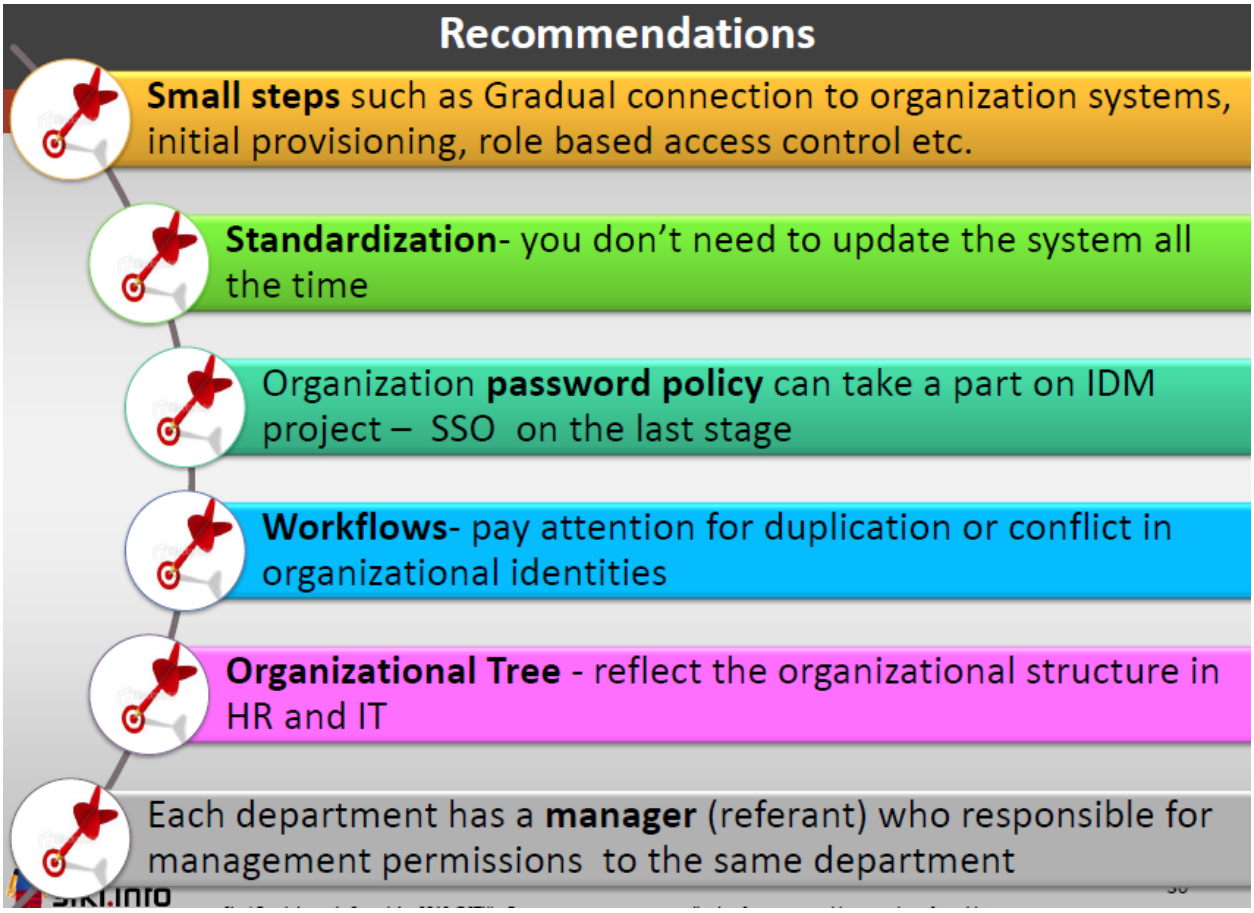
לקוח נוסף מתלבט בשאלה : הארגון פרוס על כמה סניפים עם מערכות שונות- איך יוצרים מצב ללא שיכפול נתונים והרשאות לסביבות טסט? לקוחות אחרים טוענים כי המצב לא הגיוני ולא ניתן להמשיך ככה. אין צורך לשכפל את האפליקציות עצמם אם הן נשענות על AD, מספיק שיש חיבור לAD והמשתמש מוקם כהלכה שם כדי לקבל את כל ההרשאות המתאימות שלו. היעדים שהוגדרו בפרויקט נבחרו 7 מערכות קריטיות לארגון ואותם יטמיעו בשלב הראשון במערכת הIDM, תוך כדי יסדרו את כל ההרשאות ב AD כולל הרשאות ספציפיות לעובדים מסוימים. בהתחלה יתחילו לחבר מערכת או שתיים ויראו איך זה עובד בשטח, ילמדו את התהליך וימשיכו הלאה.

לקוח נוסף מספר כי הם בחרו את יבמ והתהליך בחירת המוצר נתון רק בידי המתחרים הגדולים, מהר מאד מבינים כי כל המתחרים מספקים פחות או יותר את הצרכים. אף מערכת לא תיתן 100% כי יש מערכות ותיקות שפותחו לפני עשרות שנים והתמיכה בהם שונה. הבעיה היא בכלל לא בטכנולוגיה אלא בארגון עצמו, השיתוף פעולה ההנהלה הבכירה. בחירת המוצר גם תלויה בWOEKFLOW הארגוני, נהלי הארגון, לא לחינם אילו פרויקטים ארוכי טווח. המערכות די דומות ואחד הלקוחות טוען כי חשוב פה האפיון , במידה והוא לא מדויק אין לצאת למכרז ולבחור מערכת שלא מספקת את צרכי הארגון. חשובה המוכנות הארגון ליציאה לפרויקט כזה, לקוח אחר ציין כי הם בחנו מה קורה בעולם ובארגונים דומים להם אך הכישלון הראשון היה עקב מוכנות ארגונית לפרויקט סדר גודל כזה. לקוח אחר מצדד וטוען כי שבחר את המוצר של NETIQ לאחר שנתיים נראה כי עיקר העבודה לא במוצר אלא היכרות עם המערכות סביב, השיתוף עם HR. גם בחירת האינטגרטור המוביל בפרויקט זה חשובה תוך היכרותו עם פרויקטים נוספים ומערכת ספציפית שנבחרה.

לקוח נוסף מספר כי להם יש מערכת של SUN שכבר לא נתמכת עוד והיו צריכים לעבור למוצר של אורקל. התהליך החל לפני 4 שנים. כתוצאה מכך, נבחן הנושא מחדש מול יבמ והם בחרו ביבמ בסוף. הרכש היה מעורב מאד ושני המוצרים ענו לדרישות הלקוח. אין הבדל גדול, המחיר קבע בסוף. האינטגרטור גם לקח פה חלק, החלוקה הייתה בין ביצוע לרישיונות. לקחו זאת בחשבון. נראה כי יבמ מאד חזקים בארץ לעומת אורקל. זה לא המצב בחו"ל. בארה"ב התגובות מאד חיוביות למוצר של אורקל. אבל בארץ שמעו כי היישום לא טוב והמיישמים לא מספיק בעלי ניסיון. הלקוח מספר כי הוא במחלקת האינטגרציה והמוצרים מאד דומים גם בנושא WORKFLOW. האינטגרטור שנבחר הוא יבמ. הIDM נופל בתחום האינטגרציה עכשיו עקב פרויקט שדרוג שהיה צריך להיות מSUN ליבמ. בארגון יש אדם אחד האחראי למערכת IDM ועובד יומיים בשבוע והוא מנהל הכל. רוב האפליקציות משתלבות בIDM, מדובר על עשרות מערכות. מוזר לאותו לקוח כי יש צוות בעל מספר עובדים לפרויקט. נראה כי השדרוג הוא כמו פרויקט חדש, אך הלקוח טוען כי זה לא כך היות ותהליכי העבודה כבר קיימים. החלק הכי קשה עבר, עכשיו זה שינויים טכנולוגיים. היישום הוא טכנולוגי ולא משנים עבודה לHR, לHD או לאבטחה. הארגון הלך לניהול זהויות היות ויש לו אלפי עובדים מפוזרים בעולם, כל משרד יש לוקליזציה שלו והכל בא מאבטחת מידע- ניהול נכון. לקוח אחר מציין כי חשוב היה להם לראות ניסיון מעמיק של המיישם במוצר ובארגונים דומים- זה מאד קריטי ויבמ הוכיחו זאת במשך השנים. חשוב מאד כי למיישם יהיה ניסיון במערכת אותה מיישם, ויש אינטגטורים פחות מנוסים בנושא. זה לא פשוט כי יש להכיר את

המערכת והמגבלות שלו- לא כל דבר אפשרי וכמובן הידע הארגוני משמעותי פה כי האינטגרטור לא מכיר את הארגון ולא בא מתוכו.

המלצות STKI



נספח מיוחד התייחסות ספקים ויצרנים לנאמר במפגש

התייחסות חברת F5

איש קשר: רוני פוגל, R.Fogel@F5.com 0546714070

חברת F5 מספקת ללקוחותיה פתרון תשתית עבור זיהוי משתמשים ו-Single Sign On, הפתרון מושתת על פלטפורמת BIG-IP המספקת גם פתרונות Load Balancing, Application Security, Acceleration, וזאת מעל תשתית Reverse Proxy חכמה.

פתרון ה-Access Policy Manager מאפשר לארגון לחשוף בפני המשתמשים דרך הזדהות אחודה, הנקבעת ע"פ דרישות אבטחת המידע, ולפי סוג המשתמש, סוג הרכיב (מחשב, מחשב נייד, טלפון או טאבלט), את המשאבים בצורה מאובטחת ומואצת בין אם בתוך רשת הארגון, או ממקורות חיצונים, אינטרט או רשתות WAN.

ל-Access Policy Manager יכולת להתממשק למערכות Directory קיימות (Active Directory, eDirectory, LDAP, RADIUS, HTTP Auth, Oracle Access Manager) ולזהות את המשתמשים בצורה חזקה, בשילוב One-Time Password המופק מתוך הפתרון, או מול אמצעי זיהוי אחרי, לרבות כרטיסים חכמים.

ה APM מאשפר לארגונים מעבר חלק לתשתית Federation דרך תמיכה בפרוטוקול SAML 2.0, ומאפשר חיבור מאובטח למערכות ענן (Salesforce, Office365, Google Apps) בצורה אחידה וזהה לכלל האפליקציות הארגוניות, לפתרון Single Sign-on.

בין היתר ניתן אף לייחצן דרך APM אפליקציות Citrix, RDP של מיקרוסופט, והוא גם משמש כ- PCoIP Proxy למערכות VMware VDI.

לסיכום, פתרון BIG-IP Access Policy Manager הוא פתרון הניתן להפעלה על כל אחת מהפלטפורמות של חברת F5, פיזיות או וירטואליות, ומספק זיהוי חזק ואחיד, Single Sign-on לכלל האפליקציות הארגוניות, לרבות אפליקציות בענן, ומאפשר גישה מאובטחת מרחוק לאפליקציות הארגוניות.

התייחסות חברת NessPro

איש קשר: ג'קי עבאדי – מנהלת פעילות NetIQ בארץ - jackie.abadi@ness.com
נועם שטרמן – מנהל טכנולוגי לפתרונות NetIQ - noam.shterman@ness.com

NessPRO משמשת כנציג המקומי של NetIQ על פתרונותיו בתחום Identity & Access Governance.

הפתרון לניהול זהויות של NetIQ (לשעבר Novell) – NetIQ IDM4 – זכה בפרס אמון הקוראים של המגזין היוקרתי SC, כפתרון ניהול הזהויות הטוב ביותר http://www.scmagazine.com/2014-sc-awards-us-winners/article/334892/. הפתרון מוטמע בהצלחה אצל עשרות לקוחות בארץ.

לפתרון ניהול הזהויות של NetIQ , קיימת הטכנולוגיה להתחבר לרוב המוחלט של האפליקציות והתשתיות הארגוניות לצורך ניהול זהויות, הקצאת הרשאות (Provisioning) וסנכרון סיסמאות ע"פ מתודולוגיה עסקית (Password Policy) בצורה חזקה מהירה ויעילה במיוחד תוך כדי תיעוד מלא של התהליכים השונים בבסיס נתונים קל, נוח ומרכזי.
מרגע שנקלט העובד - ומרגע שעבר אישור ע"י אבטחת מידע, באם נדרש כזה (בתהליך Workflow של המערכת - דבר שמוקפץ רגע בודד לאחר הזנתו ב– HR), העובד יכול להתחיל לעבוד לאחר מספר שניות ועד מספר דקות בודדות עם סט הרשאות מלא לכל צורך תפקידו (ע"י Role תפקידו או ע"י Template, תלוי בהטמעה ובאפיון הספציפי).

פרקי הזמן הארוכים שהיו וקיימים גם היום לפעמים, כמעט ונעלמו עם ההתקדמות והשיפור הטכנולוגי המשמעותי במוצר ניהול הזהויות של NetIQ וכבר כמעט שאינם תלויים בטכנולוגיה.

אז במה בכל זאת תלויים סיכויי ההצלחה של פרויקטי IDM אם לא בטכנולוגיה? הבעיה המרכזית כיום היא המוכנות הארגונית הן מצד מחלקת HR שמגדירה תפקידים והן מצד התשתיות ומחלקת ה IT שמנהלים לעיתים הרשאות במערכות עתיקות יומין שבחלקן עברו כבר את תוקף תמיכת היצרן (EOL). בתכנון וניתוח אסטרטגי מעמיק לגבי סוגיות אלו ואחרות - כאשר הארגון יודע בוודאות מה הוא צריך בצורה ממוקדת ומדויקת ויתרה מזאת - יודע מה הוא יידרש לספק עבור הפרויקט (הן מצד ה HR והן מצד התשתיות) - היישום יכול להיות מהיר יעיל ופשוט.

לקוחות הציפו כמה סוגיות בשולחן העגול:

ROI - ארגונים מחליטים להיכנס לפרויקט IDM מתוך כוונה להשיג שתי מטרות עיקריות:

- ✓ יכולת Provisioning יעילה, מהירה ומתועדת, שהנגזרת מכך היא למעשה צמצום זמני המתנה משבועות עד לכמה שעות (ומטה) – זאת אופטימיזצית ROI מדהימה, הלכה למעשה.
- ✓ נמשלות (Governance) של ניהול הזהויות באופן מרכזי ומבוקר לצורכי תאימות רגולטורית ללקוחת המחויבים לכך.

Provisioning למערכות המנוהלות דרך IDM אמור להיות אוטומטי.

פרויקטים מנוהלים בשלבים ולכן מע' שטרם הוטמעו בפרויקט IDM תנוהלנה ידנית. ככל שינוהלו יותר מערכות דרך IDM, ה ROI ישתפר וכן השקיפות ונראות נושא ההרשאות והזהויות בארגון.
מיכון ומרכוז זה מורידים שעות עבודה וסיכונים ממספר גדול של מערכות ובעלי תפקיד שונים ולא רק של המתפעלים עצמם.

NetIQ IDM הכולל מתודולוגיות יישום והטמעה מוכחות, מאפשר ביצועי ROI אופטימליים.

– SSO

מציאת פתרון SSO (Single Sign On) ארגוני (Enterprise SSO) הינו פרויקט נפרד לחלוטין מפרויקט פתרון IDM ואין לטעות בכך.

במוצר ניהול הזהויות של NetIQ קיימת יכולת איטגרציה לביצוע SSO אפליקטיבי אל מול אפליקציית המערכת – אך אין לטעות, נדרש מוצר ייחודי ונפרד לצורך ביצוע פרויקט SSO ארגוני.
ל NetIQ קיימים שני מוצרים אינטגרטיבים כאלה:

- ✓ Access Manager - עליו ניתן לקבל מידע ב: https://www.netiq.com/products/access-manager/.
- ✓ CloudAccess – עליו ניתן לקבל מידע ב: https://www.netiq.com/products/cloudaccess/.

אכיפת מדיניות החברה –

בתהליכים עסקיים כגון יציאת עובד לחופשה (מסוגים שונים), ניודים פנימיים וחוץ ארגוניים, קליטת ועזיבת עובד, מערכת ניהול הזהויות מבית NetIQ, מוכיחה בשטח אצל עשרות הלקוחות, הלכה למעשה, שליטה ואכיפה מלאה של כל מדיניות עסקית שהלקוח דורש.

בנוסף, לצורך מיפוי מצב קיים והגדרת מדיניות כוללת ברמה העסקית, NetIQ מציעה את הפתרון המוביל Access Governance Suite – עליו ניתן לקבל מידע ב:
https://www.netiq.com/products/access-governance-suite/

התייחסות חברת מתודה

איש קשר: ליאת שמח, מנהל שיווק ומכירות, טל": 0732-263310 או 03-6133336 שלוחה 310

סיכום שולחן עגול בנושא IDM הציף את הדילמות שעומדות בפני כל ארגון שמחליט להתחיל פרויקט מסוג זה. אכן מדובר בפרויקט מורכב עם רמת אינטגרציה ותיאום גבוהים, הן טכנולוגית (בין מערכת IDM ל- AD

ולמערכות שאינן סטנדרטיות) והן מבחינת תהליכי עבודה ואתחול המערכת עם משאבי אנוש, אבטחת מידע ויחידות עסקיות. מתודה ממליצה על 10 השלבים הבאים לביצוע מוצלח של הפרויקט –

1. הגדר את יעדי הפרויקט – ניהול הרשאות מרכזי? ייעול תהליכים ארגוניים? שיפור רמת אבטחת מידע?
2. חשיבות הגורם האנושי - 80% מהצלחת הפרויקט מושפעים משיקולים ארגוניים. רק 20% מושפעים מטכנולוגיה. תמיכת הנהלה הכרחית!
3. הגדר את גבולות הפרויקט – אילו מערכות נכללות בתכולת הפרויקט ולא פחות חשוב מה לא נכלל?
4. מפה תהליכים עסקיים וטכנולוגיים.
5. Data Cleaning–משתמשים והרשאות לא פעילים, משתמשים ללא הרשאות, הרשאות ללא משתמשים.
6. Role Mining - שאיפה להגיע למספר פרופילים מצומצם, כדי להשיג ניהול יעיל ופשוט של הרשאות.
7. נתח תהליכים נדרשים – מי מאשר? מה? מתי? למה? מי מבצע? בד"כ זו תורה שבעל פה בארגון.
8. הגדר ארכיטקטורה נדרשת (להלן ארכיטקטורה בסיסית):

9. בחר ספק / טכנולוגיה
10. התחל בפרויקט

נשמח לשתף אתכם ב- Best Practices שהצטברו במתודה בניהול מקצה לקצה של פרויקטי IDM, משלב ניתוח צרכים, דרך סיוע במיפוי וטיוב נתונים, ניהול מכרז מסודר לבחירת ספק מתאים, ולבסוף ליווי הפרויקט בתהליך המימוש וסיוע בהטמעה.

Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444