סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

המלצות ליישום

הגנה על מערכות ERP

ינואר 2019

סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

המלצות ליישום

הגנה על מערכות ERP

ינואר 2019

מסמך זה נכתב ע"י מערך הסייבר הלאומי לטובת הציבור במדינת ישראל, במסגרת מחויבות המערך לשפר את כשירות הארגונים במשק להתגוננות מפני איומי סייבר.
השימוש במסמך זה ע"י המשק הישראלי אינו כרוך בתשלום, כפוף לשמירת הזכויות מדין למדינת ישראל. אין לראות במסמך זה תחליף לייעוץ פרטני אשר מתאים את המלצותיו לארגון מסוים.
המסמך נכתב בלשון זכר מטעמי נוחות בלבד.
התייחסויות לתוכן המסמך ניתן להעביר במייל ל- tora@cyber.gov.il.

כל הזכויות שמורות
למערך הסייבר הלאומי

תוכן עניינים

תקציר המסמך ומטרותיו 7
קהל יעד 9
האיום 10
ארכיטקטורה 11
המלצות הגנה 13
1. ארכיטקטורה רשתית 13
1.1 אבטחה פיזית של שרתי ERP 13
1.2 הפרדה לוגית 13
1.3 הפרדה מהמרשתת (האינטרנט) 14
1.4 גישה מאובטחת 15
1.5 התממשקות למערכות חיצוניות 16
1.6 הקשחת מערכת ההפעלה 16
1.7 התאוששות מאסון 17
2. אפליקציה 17
2.1 הזדהות 17
2.2 סגירת פורטים לא נחוצים 18
2.3 השבתה או מחיקה של משתמשי ברירת מחדל 19
2.4 ניהול ססמאות 19
2.5 הרשאות 20
2.6 תמיכה מרחוק 21
2.7 העלאת קבצים למערכת ERP 22
2.8 גיבוי המידע 22
2.9 הצפנה 24
2.10 אנטי-וירוס 24
2.11 Firewall 25
2.12 מערכות הגנה סטטיות נוספות 26
2.13 עדכוני יצרן ואבטחה 26
2.14 ניהול שינויים 27
2.15 מנגנונים להערכת ההגנה 27
2.16 ניטור ובקרה 27
3. שימוש בשירותי ERP בענן 29
4. הגורם האנושי 30
4.1 כלל המשתמשים 30
4.2 משתמשים פריווילגיים 31
5. פיתוח מאובטח 31
6. מדיניות וציות 32
7. רשימת תיוג 33
נספח: תקיפות מפורסמות 34
ביבליוגרפיה 35

תקציר המסמך ומטרותיו

מערכות ERP - Enterprise Resource Planning הן הפלטפורמה המרכזית לניהול תהליכים עסקיים במרבית הארגונים בעולם. הן מורכבות ומסועפות, ומהוות יסוד מרכזי בתפעול הארגון. מערכות אלה הן הבסיס לפעולות עסקיות, כמו: כספים, ניהול תקציב, ניהול שרשרת האספקה, תכנון משאבים, ניהול ההון האנושי, מכירות ושיווק ועוד. למערכות ERP יש כמה פונקציות עיקריות:

1. כלים לניהול תהליכים פנים-ארגוניים ואינטראקציה מול שרשרת האספקה, דוגמת ניהול כספים, משאבי אנוש (מערכות נוכחות ותיקים אישיים לדוגמה), רכש, מלאי.
2. לאגור את המידע ולבצע בו חיתוכים וניתוחים על מנת לקבל תמונה ברורה על המצב הפיננסי בארגון, ועל מרכיבי התמונה הפיננסית.
3. כלי לשליטה ובקרה של תהליכי ליבה.
4. לאפשר ביצוע אינטגרציה ואוטומציה בעת עבודה עם מערכות משיקות, דוגמת PLM (Product Lifecycle Management).

סוג המידע במערכת, לצד העיבודים הרבים של המידע, כמות התחומים שבהם המערכת נוגעת, ההשלכות הנגזרות על הארגון ברמה הטקטית והאסטרטגית ויכולתו להשיג את יעדיו באמצעותה, הופכים אותה למערכת רגישה ומעניינת מאוד בעבור תוקף.

בשנים האחרונות ניכרת מגמת עלייה בשיעורי הרכישה ו/או המעבר לשירותי ERP בענן, ובמקביל הולך וגובר עניינן של קבוצות פצחנים (האקרים) וארגוני פשיעה בהשגת גישה למערכות אלה כדי להניח את ידם על המידע הרגיש שקיים בהן[1].

חברת Onapsis חקרה ומצאה שיש בנמצא 17 אלף אפליקציות של מערכות ERP המחוברות לאינטרנט, וחלקן לא מעודכנות ולכן פחות מוגנות. ארגונים רבים חוששים מסיבות המוזכרות בהמשך לעשות עדכוני תוכנה ואבטחה. בעקבות זאת פעילות ערה ב-DarkNet לגילוי חולשות במערכות ה-ERP מניבה תוצאות ומובילה למתקפות מוצלחות[2]. היעדר עדכון תוכנה עלול לאפשר לתוקפים לקבל גישה מלאה ואף שליטה על הנתונים ועל התהליכים וכן גישה אפשרית למערכות המתממשקות עם מערכת ה-ERP שנפרצה[3].

לנוכח כל זאת ראינו לנכון להתייחס גם להיבטי האבטחה המורכבים שבשימוש בשירותי ענן.

מערכות ERP סטנדרטיות מורכבות מארבעה חלקים: 1. שרת מאגר הנתונים (DB). 2. שרת האפליקציה. 3. שרת ממשקי תוכנה (Application Programming Interface). 4. תחנות קצה (או כ-Client או דרך משתמש בענן). מערכות מסוג זה כוללות לעיתים מאות פונקציות והטמעתן מתבצעת באופן ייעודי ומותאם לארגון (קסטומיזציה), מה שאומר בהכרח שיישום המערכות שונה בין לקוחות שונים, וכך גם אופן ההגנה. עם זאת עקרונות ההגנה שיוצגו בעמודים הבאים משותפים לרובן.

כמה גורמים מייחדים את מערכות ה-ERP מכל מערכת אחרת בארגון[4]:

1. רגישות וצבר המידע.
2. המורכבות של המערכת ומספר האפליקציות המיושמות בה.
3. מורכבות המערכת עשויה להקשות על יישום אבטחת המידע.
4. התלות הארגונית בזמינות ובאמינות המידע, המערכת והממשקים.

1 ONAPSIS / ERP Applications Under Fire: How cyberattackers target the crown jewels/ July 2018
2 ONAPSIS / ERP Applications Under Fire: How cyberattackers target the crown jewels/ July 2018
3 https://www.us-cert.gov/ncas/alerts/TA16-132A
4 https://downloads.cloudsecurityalliance.org/assets/ /erp-security/ERP_Security_Final_CSA_Feb08-18.pdf

5. זמינות נמוכה של גורמים בעלי מומחיות מוכחת בתכנון ויישום אבטחת המידע וחוסן.
6. קשיים בביצוע עדכוני תוכנה ואבטחה בכלל הרבדים (מערכת הפעלה, בסיסי נתונים ואפליקציה).

מרכיבים אלה עומדים במרכז הדיון הנוגע למורכבות אבטחת המידע במערכת ERP: המידע הנמצא בהן מחייב הגנה משמעותית, אך המורכבות של המערכת והצורך העסקי בממשקים בין אפליקציות השייכות למערכת ובינן למערכות אחרות, מקשה מאוד על יישום הגנה איכותית.

במסמך זה נסקור את החולשות האופייניות במערכות ERP ושל הדרכים והכלים המאפשרים התמודדות עימן. בכל פרק נתייחס לעקרונות המובילים לצורך בהקשחה, ולתהליך שיש לבצע.

נסביר בנפרד את התהליך לביצוע הקשחות במערכות On-premise ובמוצרי ענן ונפנה לפרק הרלוונטי בתורת ההגנה בסייבר או למקור מקצועי אחר.

חשוב לזכור כי יש בשוק טכנולוגיות מסוגים שונים, והן באות עם הנחיות ההקשחה הייחודיות שלהן והפורטים הייחודיים להן. הנחיות ההקשחה של היצרן הן הקו המנחה הבסיסי ביותר ולפיו יש לתחזק את המערכות. ההנחיות הכתובות במסמך זה יכולות לשמש ככלי עזר והרחבה להנחיות היצרן, אך לא להחליף אותן.

נוסף על מסמך זה, חשוב להתעדכן תדיר במוקדי הידע הרלוונטיים: SANS, הרגולטור (אם ישנו) והיצרן וכן להשתמש במסמך "המלצות הגנה לצמצום סיכוני סייבר בתחנות קצה בארגון" של מערך הסייבר[5].

5 https://www.gov.il/he/Departments/policies/endstation

קהל יעד

קהל היעד למסמך זה הוא מנהלי אבטחת מידע, אנשי system ומנהלי IT שבארגונם מערכות ERP והם מעוניינים לוודא שהמערכות מאובטחות דיין לפי רמת הסיכון שהוגדרה לארגון, או להעלות את רמת ההגנה אם אינה מספקת, תוך יצירת שפה בין בעלי העניין בארגון ומול האינטגרטור וספק התוכנה.

האיום

מערכות ERP הן נקודה רגישה ומעניינת בארגון משתי סיבות:

המידע האטרקטיבי - הן מכילות מידע רגיש מאוד: מידע על לקוחות, על עסקאות, על עובדים, על כספים, על אופי העיסוק וכדומה. הן גם מבצעות פעולות המשפיעות על ההיבט העסקי בארגון, מנהלות מלאי, ספרי הנהלת חשבונות, דוחות רווח והפסד ומאזנים המועברים לדיווח בורסאי ועוד. לכן מערכות כאלה מסקרנות מאוד, בעיקר בהיבטים של מודיעין עסקי, שינוי נתונים (שיובילו לאי סדרים בספרים, לפגיעה במוניטין), תקיפת כופרה שתותיר את הארגון ללא יכולת לבצע פעולות עסקיות.

הגישה - מערכות ERP עשויות להיות מותקנות בשרת מקומי (On-premise) או כשירות ענן. יש כמה דרכים להתחבר למערכות הללו:

On-Premise - 1. כ-Client מקומי בעמדת קצה. 2. גישה מעמדת הקצה (קליינט) לפורטל המערכת באמצעות דפדפן.

שירות ענן - 1. בין ענן לענן. 2. באמצעות חיבור לענן.

חלק ניכר מהמשתמשים הם אנשי כספים, ייצור, תפעול ואנשי מכירות. יש עובדים שאינם מודעים לסכנות אבטחת המידע ועלולים לשמש "טרף קל" לתוקף מתוחכם שיצליח להגיע אל אמצעי ההזדהות שלהם, או לשטות כך שיבצעו פעולות באמצעות ההרשאות שלהם, ואלה ישרתו את מטרתו של התוקף. בהתחברות דרך הענן, המחשב עלול להיות חשוף לכל הסיכונים המוכרים שנמצאים ברשת ותלויים באבטחת המידע של ספק הענן, נוסף על אבטחת המידע בארגון.

נתייחס לאיום על מערכות ERP על פי משולש ההגנה:

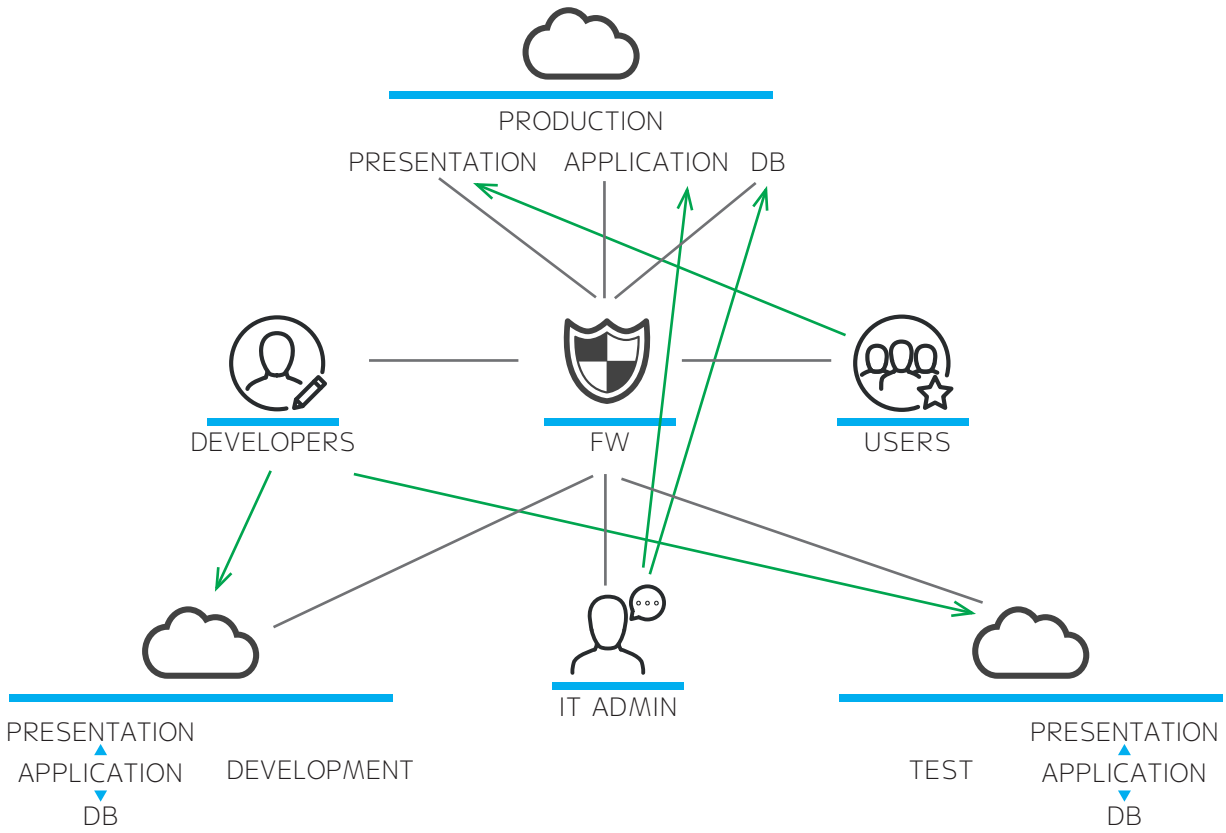
חיסיון (Confidentiality) - גישה למערכות ERP חושפת את התוקף למידע הרגיש ביותר בארגון. הוא יגלה לתוקף פרטים על לקוחות, על ההתנהלות, ועל מעבר הכספים בחברה. כל פרט במערכת עשוי להיות בעל דרגת חיסיון נמוכה כשהוא בפני עצמו, אך כצבר פרטים דרגת חסיון המידע יכולה לעלות.

זמינות (Availability) - אי זמינות של מערכת ERP משבשת באופן חמור את הפעילות השוטפת של החברה. היא יכולה למנוע חיובים או תשלומים, לשבש את ניהול המלאים, לפגוע בעמידה בלוחות זמנים ו/או לפגוע ברמת האיכות של המוצר, אי עמידה במסירת דיווח בורסאי וכן חדירה לפרטיות העובדים ועוד.

מהימנות ושלמות המידע (Integrity) - שיבוש המידע באופן שיגרום לניתוח מידע באופן שגוי, לפגיעה בתקינות תהליך קבלת ההחלטות בארגון, לביצוע לא נכון של תהליכי גבייה וזיכוי וכדומה, עשוי לגרום נזק ניכר ואף בלתי הפיך.

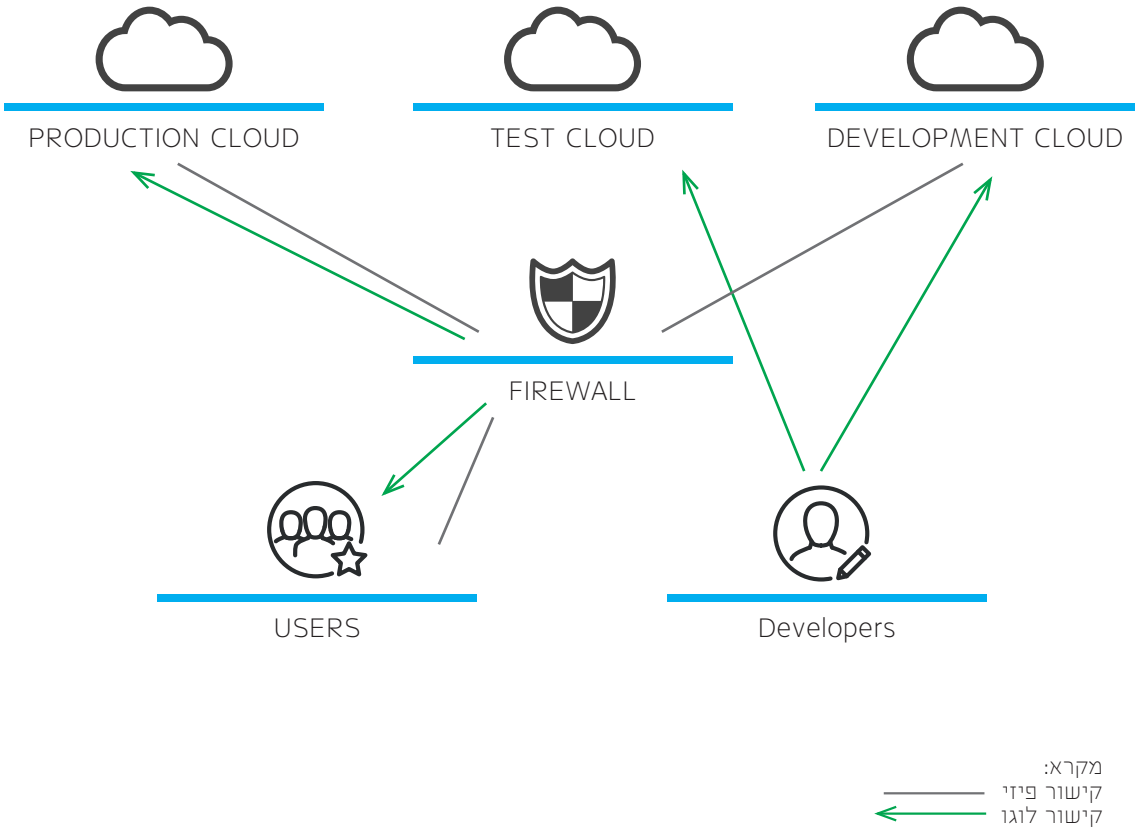
ארכיטקטורה

ארכיטקטורת רשת בהתקנה On-Premise:



מקרא:
קישור פיזי
קישור לוגו

ארכיטקטורה בחיבור לשירותי ענן:



המלצות הגנה

1. ארכיטקטורה רשתית

1.1 אבטחה פיזית של שרתי ERP

עקרון ההגנה

On-premise: מערכות ERP בנויות משני סוגי שרתים (DB, APP) ומעמדות קצה. בשרת ה-DB נמצא מסד הנתונים של הארגון, שרת ה-APP הוא אחד משני הגורמים היחידים המורשים לפנות ל-DB (לצד ה-DBA), ומכאן רגישותו. מסיבות אלה יש לנקוט פעולות שונות על מנת למנוע מגורם זר להגיע לשרתים, לחבר אליהם מדיה נתיקה ולהשתיל נוזקה או לשאוב מידע, או להצליח לפגוע פגיעה פיזית בשרת ולגרום להשבתתו או לאובדן פרטים ממאגר הנתונים.

שירות ענן: לארגון המשתמש בשירותי ERP בענן יש עניין גם ברמת האבטחה הפיזית המיושמת אצל ספק האחסון. יש ארגונים שבהם השרת הוא אותו שרת - בארגונים גדולים מומלץ להפריד בין שרת ה-DB לשרת ה-APP.

תהליך ההקשחה

On-premise:

- יש למקם את שרתי המערכת, בדומה לשאר שרתי החברה, בחדר שרתים שהכניסה אליו היא בהרשאה בלבד (כרטיס/קוד).
- במידת האפשר, את שרתי המערכת יש להפריד באופן פיזי משרתים אחרים בארגון.
- רצוי ליישם נעילה לארונות התקשורת ואמצעים לנעילת השרת עצמו.
- רצוי להציב מצלמת אבטחה שמתעדת את הכניסה לחדר השרתים ולבדוק את הצילומים מדי פעם בפעם, באופן מדגמי.

ארכיטקטורה של רשת: חשוב מאוד לקבל ולייצר בקרה באמצעות כלי הבקרה של SAP (SOLUTION MANEGER). הכוונה היא שבכל מקרה של תחזוקה שדרוג או הוספת שרתים אפשר לתעד את הרשת ואת רכיבי הרשת של SAP הקשורים ולוודא שאין גורם או רכיב חיצוני שמאזין ושהרשת לא מחוברת או חוברה בטעות לרכיב רשת שאינו שייך. כמו כן מערכת הניטור מאפשרת בזמן הרחבה של זיכרון או הרחבה של כל כוח עיבוד לבצע את זה בפרקי זמן מהירים ולפי דרישות העומסים של המערכת.

חשוב לציין שכלי הניטור מאפשרים שליטה על העתקת סביבות וניהול משאבים וירטואליים.

שירות ענן:

- יש לוודא שספק האחסון עומד בדרישות מערך הסייבר בעבור שרשרת האספקה[6] או בתקן ISO 27001, המגדיר בין היתר את הבקרות שיש ליישם כדי לוודא הגנה פיזית על שרתים והתקנים שונים.

תורת הגנה בסייבר לארגון> משפחה: הגנה פיזית וסביבתית> 18.1

1.2 הפרדה לוגית

עקרון ההגנה

ישנם שני היבטים של הפרדה לוגית שיש ליישם בארגון:

1. הפרדה לוגית של שרת בסיס הנתונים משאר הארגון.

On-Premise: שרת ה-DB לא צריך להיות נגיש לכלל התקני החברה, רק לאפליקציות

6 https://www.gov.il/he/Departments/news/querysupply

הרלוונטיות ול-DBA. האפליקציות צריכות לתקשר עם מחשבי העובדים שבהם מותקן Client מקומי.. יש ליצור ארכיטקטורה שתפריד בין הרשת הפנימית לשרת ה-DB ותאפשר גישה לשרתי האפליקציה ול-DBA בלבד.

שירות ענן: נוסף על ההפרדות שהוזכרו, יש לוודא שבאחסון הענן יש הפרדה לוגית בין הלקוחות.

2. הפרדה לוגית בין סביבות העבודה: פיתוח, בדיקות וייצור. על מנת למנוע שיתוק של המערכות בעת שלב הפיתוח, או העברה של קוד פגום לסביבת העבודה, דבר שעלול לגרום נזקים כבדים.

- מערכות ייצור - יש לוודא כי מידע עובר בכיוון אחד בלבד, מהסביבה הגבוהה לסביבה הנמוכה. לטובת כך, יש לוודא כי המידע עובר ערבול לאחר העתקתו לסביבה נמוכה יותר.
- ארגון שנוהג להעתיק את סביבת הייצור לסביבות הפיתוח והבדיקות צריך להקפיד לערבל את המידע אחרי העתקת הסביבה.

תהליך ההקשחה

- אפשר לעשות הפרדה על ידי יצירת תת-רשתות (SUBNET).
- קביעת חוקים המגבילים גישה, חוקי ניתוב ייעודיים ב-Firewall שיגדירו למי תינתן גישה לצפייה בחלקים שונים של המידע, מי יכול לערוך, למחוק או לייצר מידע, הן משתמשים והן מערכות. במערכות SAP, לרוב המימוש יתבצע באמצעות קישור מנגנון ההרשאות המובנה של המערכת לקבוצות במנגנון ההזדהות הארגוני (כגון AD).

העתקת סביבות: במסגרת תחזוקה שוטפת נדרש לעיתים להעתיק סביבות ייצור. חשוב לציין שתהליך זה מורכב ודורש כמה פעולות של אדמיניסטרטור. חשוב אפוא להצפין ו/או לערבל את המידע שמועתק לסביבות אחרות. כמו כן חשוב מאוד לייצר מצב שרק מידע רלוונטי מועתק. לדוגמה, אין צורך להעתיק את כל המידע מסביבת הייצור, אלא רק מידע שאינו רגיש או מידע שמשמש לצורך תרגול בלבד.

תורת הגנה בסייבר לארגון> משפחה: הפרדת סביבות > 10.7

1.3 הפרדה מהאינטרנט

עקרון ההגנה

On-Premise: שרתי ה-DB וה-APP לא צריכים גישה לאינטרנט, הפניה אל שרת האפליקציה מותרת רק מתוך הרשת הארגונית והפניה לשרת ה-DB מותרת רק למשתמש DBA ולמשתמש אחד מוגדר של האפליקציה מתוך שרת ה-APP.

שירותי ענן: כאשר ה-ERP ניתן כשירות ענן, ה-DB והאפליקציה צריכים להיות מחוברים לאינטרנט כדי להגיע ללקוח.

תהליך ההקשחה

On-Premise: הגדרת חוקים מתאימים ב-Firewall, שיחסמו פנייה לשרתים אלה דרך האינטרנט, או הגדרת כרטיס הרשת לרשת הפנימית בלבד והוספת חוקים רלוונטיים לגישה למשתמשים מסוימים בלבד.

שירותי ענן: הגדרת חיבור מאובטח (TLS ו-MFA) בין המשתמש לאפליקציה שיושבת בענן, שימוש בסיסמה מורכבת ויישום הגנות על תחנת הקצה

(בהמשך המסמך), על מנת שלתוקף שמגיע דרך האינטרנט לא יהיה פשוט לקבל גישה לשירות.

תורת הגנה בסייבר לארגון> משפחה: אבטחת רשת > 9.13

1.4 גישה מאובטחת

עקרון ההגנה

On-Premise: בגישה מרחוק למערכות הארגון טמונה סכנה אינהרנטית. עם זאת יש מצבים שהארגון חייב להשאיר אפשרות של גישה מבחוץ. יש לעשות סקר סיכונים, להעריך את רמת הסיכון ולקבוע אם הצורך העסקי בגישה מרחוק מחייב הכלה של הסיכון.

גישה לשרת DB - בשרת זה מצוי כל המידע הרגיש של הארגון, המחייב גישה מינימלית. גישה זו צריכה להיות מוגדרת ב-Firewall על ידי חוקים מאפשרים וחוקים מונעים. ישנן טכנולוגיות שונות של גישה למידע, ביניהן מאובטחות יותר ומאובטחות פחות. טכנולוגיות גישה לא מאובטחות לניהול או גישה לשרת DB הן פרצת אבטחה קלה לפורץ ולא רק משאירות את המידע ללא הגנה, אלא מייצרות ערוץ גישה פתוח. חשוב להטמיע בארגון כמה טכנולוגיות אבטחה שייתנו פתרונות שונים לבעיות אבטחה שונות.

גישה לשרת האפליקציה - משתמשי המערכת צריכים לפנות לאפליקציה על מנת להזין מידע ולבצע פעולות. האפליקציה הוא זה שיפנה ל-DB וישפיע על הנתונים שבו בהתאם למידע שהזין המשתמש. לכן גם הגישה לאפליקציה חייבת להיות מאובטחת ולהתקיים בהתאם לעקרון "הצורך לדעת" - הגישה תתאפשר רק למי שזקוק לה לצורך עבודתו.

שירותי ענן: כאשר ארגון משתמש ב-ERP בענן, יש צורך בגישה מאובטחת בעת ההתחברות לאתר.

תהליך ההקשחה

On-premise:

- יש לחסום טכנולוגיות גישה לא מאובטחות, כמו Telnet ו-Remote Shell ולהחליפן בגישה מאובטחת.
- יש להטמיע פתרונות הצפנה, הן למידע נייח (At Rest) והן למידע בתעבורה (In Transit).
- יש לבצע ניטור מתמיד על פרוטוקול הגישה שנבחר ולבדוק לוגים כשגרה, באופן מדגמי.
- אצל משתמשים בעלי גישה למידע רגיש, יש להתקין מערכות להקלטת המסך על מנת לבצע תחקור במקרה של חשד לפעילות לא תקינה.

שירותי ענן:

- יש לוודא שספק שירותי הענן מתקשר עם מודל ה-SSO הארגוני כאשר מתחברים לאתר מתוך הרשת הפנימית.
- בהתחברות מחוץ למשרד, יש אפשרות ליישם אחת משתי הגנות: הזדהות ישירה לאתר באמצעות MFA, או התחברות מאובטחת לרשת הפנימית של הארגון ומשם פנייה לאתר.

1.5 התממשקות למערכות חיצוניות

עקרון ההגנה

- מערכות ERP הן, בדרך כלל, מערכות חוצות-ארגון, וככאלה הן מתממשקות עם מערכות אחרות המוטמעות בארגון ומבצעות פעולות שונות מאלה של ה-ERP, כמו DWH, ניהול פרויקטים, ניהול לקוחות (CRM) ועוד ומקבלות מהן או מעבירות אליהן מידע. ההתממשקות הזאת מאפשרת עוד גישה למערכת ומצריכה עוד מנגנוני הגנה. מומלץ לנהל רישום ותיעוד מסודר של כלל הממשקים.
- מומלץ להעדיף עבודה ב-pull על פני push של מידע. יש לשים לב להיבטי הרשאות הגישה לנתונים לאחר הוצאתם מתוך מערכת ה-ERP אל מערכת חיצונית, בפרט במקרה של שימוש בכלי BI משלימים שאינם אינהרנטיים במוצר. במקרה זה מנגנון ההרשאות נסמך על יכולות הכלי שאליו נשאבו הנתונים.
- מומלץ להשתמש ב-WAF להעברה של שדות ספציפיים ומוגדרים במבנה מוגדר ומורשה בלבד.

תהליך ההקשחה

במקרים שחייבים לייצר התממשקות בין המערכות, יש לוודא שמתקיימת הצפנת תקשורת בתווך כדי שלא יהיה אפשר להאזין לנתונים בעת העברתם וכן שהחיבור (API) מאובטח.

התממשקות למערכות אחרות: בכל שלב ביישומי SAP למיניהם יש דרישה או דרישות עסקיות לקבל או להוציא מידע ולשלבו עם מערכות חיצוניות לעיתים גם מחוץ לארגון. במקרה כזה חשוב מאוד לוודא כמה דברים עיקריים: לא מבצעים חיבור כלשהו לשרת בסיס הנתונים. המידע שם אינו תחת מנגנון ההרשאות של SAP, לכן החיבוריות מותרת רק לשכבת האפליקציה (הדבר אף אסור על פי הרישוי המסחרי של היצרן). כמו כן חשוב מאוד ליישם אינטגרציה באמצעות כלי SAP כגון PI/ PO ו/או ע"י כלי אינטגרציה שקיבלו הסמכה של חברת SAP. מומלץ מאוד לבצע ממשקים באמצעות פרוטוקול ODATA שמשמש בסביבות SAP זה כמה שנים.

כדי להימנע מפרצת אבטחה, מומלץ מאוד לבחון שימוש בחבילות אינטגרציה מוכנות שנמצאות ב-SAP וזמינות להורדה באתר. שימוש כזה יכול להבטיח התממשקות למקומות הנכונים במערכת וביצוע הרחבות ושינויים לפי הצורך.

מומלץ לבצע אחת לתקופה סקר אבטחה של הממשקים הקיימים על מנת לוודא שהם פותחו באופן מאובטח.

1.6 הקשחת מערכת ההפעלה

עקרון ההגנה

מערכות ההפעלה משמשות כצינור גישה למידע שנמצא באפליקציה שהן מפעילות. הן מעוצבות באופן שיאפשר עבודה של משתמשים שונים, מבצעות חלוקה של משאבי המערכת וצריכות להגן על המשתמש מפני תקיפות, הן כאלה הנובעות משימוש פסול שלו והן כאלה הנובעות מפעולות של משתמשים אחרים. כיום, כאשר מוצרים רבים ניתנים כשירות ענן, גם מערכת ההפעלה פתוחה לאינטרנט ולכן עלולה להיות חשופה לתקיפות סייבר.

תהליך ההקשחה

- הקשחה של בסיס הנתונים כוללת בין היתר את הצעדים האלה:
- עדכוני תוכנה ואבטחה שוטפים.

- הפעלת אנטי-וירוס על שרת מערכת ההפעלה.
- הפעלת ה-Firewall על שרת מערכת ההפעלה.
- הפעלת IDS (Intrusion Detection System)
- פעולות נוספות להקשחת מערכת ההפעלה:
- הסרת שירותים לא נחוצים.
- סגירת פרוטוקולים שאינם בשימוש.
- יישום מדיניות ההרשאות הארגונית.
- הגדרת תהליכי הזדהות (MFA).

על מנת להקשיח כיאות את בסיס הנתונים של SAP, יש לפעול בהתאם להנחיות שבמסמך ההקשחה ל-SAP: Operating System Security Hardening Guide for SAP HANA[7]

1.7 התאוששות מאסון

עקרון ההגנה

DRP, תוכנית להתאוששות מאסון, היא חלק מתוכנית ההמשכיות העסקית (BCP) שנועדה להגדיר את האמצעים שהארגון מיישם על מנת להמשיך לתפקד כאשר משהו פוגע במערכות (החל בתקלה טכנית, כמו כבל שנקרע, וכלה בתקיפה שהצליחה לחדור למערכות הארגון ולחסום גישה אליהן).

הגיבוי ייבדק בצורה עיתית (שחזור יזום) ואתר הגיבוי ימוקם במרחק פיזי סביר (עשרות קילומטרים מהאתר הראשי).

תהליך ההקשחה

מערכות ERP, בהיותן קריטיות לארגון, חייבות להיות בעלות יכולת התאוששות, גם אם רק לחלקים הקריטיים שבהן.

On-Premise: יש להקים אתר DR (מוטב במיקום גיאוגרפי שונה, שמגדיל את הסיכוי להמשכיות עסקית גם במקרה של אסון טבע, אבל אפשר למקם אותו קרוב, בהפרדת תשתיות), הכולל גיבוי של בסיסי הנתונים, של הרשאות הגישה ושל הגדרות ה-Roles.

שירותי ענן: המעבר לשירותי ענן מקל מאוד על יישום DR, מכיוון שכל המידע נמצא בענן והדרך היחידה שייפגע היא על ידי השחתה שלו, ולכן מאמץ ה-BCP צריך להתמקד בהגנה לוגית על המידע[8].

אף על פי כן יש לשמור עותק של המידע במערכת מקומית, שישמש גיבוי למקרה שהמידע בענן הושחת או הגישה אליו נמנעת. המידע הזה צריך להתעדכן בתדירות שנקבעת במדיניות הארגון.

תורת הגנה בסייבר לארגון> משפחה: המשכיות עסקית <25

2. אפליקציה

2.1 הזדהות

עקרון ההגנה

תהליכי הזדהות לא מתאימים בגישה למערכת עשויים להוות פרצת אבטחה שתאפשר לגורם לא מורשה לגשת למידע השמור במערכות.

תהליך ההקשחה

מערכות ERP יודעות לנהל משתמשים ו- ROLES, וההזדהות בגישה למערכת יכולה להיעשות באמצעות ה-Active Directory של הארגון או ישירות מול המערכת.

7 https://www.suse.com/media/guide/os_security_hardening_guide_for_sap_hana.pdf
8 https://downloads.cloudsecurityalliance.org/assets/research/erp-security/ERP_Security_Final_CSA_Feb08-18.pdf

בבחירה באחת מדרכי ההזדהות הללו צריך להביא בחשבון את היתרונות והחסרונות של כל אחת מהן:

הזדהות דרך Active Directory - כל תהליך הזדהות דורש סיסמה. כאשר הזדהות יחידה (SSO) מאפשרת גישה הן לרשת הארגונית והן למערכת ה-ERP, והעובד לא צריך לזכור עוד סיסמה, פוחת הסיכוי לבחירה של סיסמה פשוטה מידי וקלה לפריצה, או אפילו סיסמה זהה לסיסמאות אחרות הנמצאות בשימוש העובד בארגון. החיסרון בבחירה בשיטת הזדהות זו נובע ישירות מהיתרונות - מכיוון שאין צורך בסיסמה נוספת ואין מנגנון הגנה מרגע שהמשתמש מחובר למערכת הארגונית, גורם שהצליח להשיג את פרטי ההזדהות למערכת הארגונית מקבל גישה גם למערכת ה-ERP, שבה יש מידע רגיש.

הזדהות מקומית - בדיוק הפוך מהזדהות דרך ה-Active Directory, היתרון של סיסמה המשמשת שכבת הגנה נוספת לפני הגישה למידע, הוא גם חיסרון והסיסמה עלולה להיות פרצת אבטחה בעצמה.

לגבי הזדהות, מערכות SAP מנהלות משתמשים בצורה מרכזית עבור כל יישומי SAP. כדי להקל את תהליך ההזדהות של משתמשי הקצה, נהוג ליישם הזדהות מול שרת ה-AD הארגוני ולהעביר את שם המשתמש למערכות SAP. במקרה כזה מומלץ לוודא שמיישמים מערכת SSO בטוחה.

כן חשוב לשים דגש על שיטת ההצפנה, הגדרות אבטחה של רכיבי הSSO השונים ובכלל על תכנון מאובטח של מנגנון ההזדהות של משתמשי קצה, ממשקים וכו'.

2.2 סגירת פורטים לא נחוצים

עקרון ההגנה

פורטים פתוחים עשויים להוות סיכון. ישנם 65535 פורטים אפשריים שמשמשים שירותים ויישומים שונים כדי לאפשר התקשרות בין שני מחשבים. מקובל לחלק את הפורטים לשלוש משפחות: פורטים ידועים (0 - 1023), פורטים רשומים (1024 - 49151) ופורטים דינמיים/פרטיים (49152 - 65535). הפורטים הידועים הם קריטיים לפעילות מערכת ההפעלה. הפורטים הרשומים הם אלה שניתנים לשימוש על ידי שירות או יישום מסוים. במשך השנים הצליחו תוקפים לנצל פורטים פתוחים ולהשיג גישה למערכת ההפעלה. השרת אינו משתמש בכל הפורטים הללו, ולכן אפשר לנטרל פורטים שאינם נחוצים על ידי חוקי Firewall, וכך לעזור להתקן לאבטח את עצמו מפני תוקפים.

תהליך ההקשחה

לכל מערכת ERP יש פורטים ייעודיים לגישה למידע. יש לוודא בהנחיות היצרן אילו פורטים הכרחיים לפעילות התקנית של שרתי ה-ERP ולחסום גישה דרך כל שאר הפורטים באמצעות Firewall או IPS. יש לוודא שהפורטים שנותרו פתוחים הם פורטים מאובטחים ושהגישה אליהם אפשרית רק מהמשתמשים שאמורים להגיע אליהם לפי הגדרת התפקיד.

תורת הגנה בסייבר לארגון> משפחה: אבטחת רשת > 9.12

2.3 השבתה או מחיקה של משתמשי ברירת מחדל

עקרון ההגנה

במוצרים שיש בהם "משתמשי מערכת" אשר מגיעים עם המוצר כברירת מחדל, משתמשים אלה מהווים חולשה מוכרת לתוקפים, כיוון שהסיסמה בהם נותרה הסיסמה הראשונית ויש להם גישה למידע. אם אי אפשר למחוק את המשתמשים מסיבות תפעוליות, מומלץ לוודא כי יש להם סיסמה קשה לניחוש וכי הם שמורים בכספת (בפרט יש לשים לב ל - SAP* ו- DDIC).

מערכות ERP מטבען מתממשקות עם מערכות אחרות ושואבות מהן מידע. התממשקות זו עלולה גם להוות חולשה אם המערכות האחרות אינן מוגנות דיין, אם לא מבוצעות בהן חלוקת אחריות והרשאות לפי עיקרון "Need to Know" - חשיפת מידע רק לגורם שצריך אותו לעבודתו.

תהליך ההקשחה

- מומלץ להסיר משתמשי ברירת מחדל או לשנות את שמם ואחת לתקופה שנקבעה מראש במדיניות החברה, לוודא שלמערכת יש רק משתמשים פעילים. טרם המחיקה יש לעשות בדיקה בסביבת מעבדה ולוודא שהמחיקה לא פוגמת בפעילות המוצר.
- בעת התקנת המערכת וחיבור לממשקים עם מערכות אחרות, יש לוודא שמתנהלת תקשורת רק עם מערכות רלוונטיות. כמו כן יש לבצע בדיקות אחת לתקופה שנקבעת במדיניות הארגון ולוודא שכל המערכות המתממשקות נותרו רלוונטיות ולמחוק את אלה שהפעילות איתן הופסקה.

2.4 ניהול סיסמאות

עקרון ההגנה

כלל מערכות הארגון אמורות להיות מוגנות על ידי סיסמת כניסה לכל הפחות. אפשר להוסיף MFA להעלאת רמת ההגנה, כמו קוד זמני שנשלח לטלפון הנייד או למייל האישי או טביעת אצבע. סיסמה טובה, שמנוהלת נכון, יכולה לשמש מחסום אמיתי ואיכותי בפני תוקפים. לעומת זאת, סיסמה שנחשפה תאפשר לתוקף לפעול חופשי במערכת (במגבלות ההרשאות שניתנו למשתמש שדרכו הוא נכנס) בלי לגלות זאת, לאורך זמן.

תהליך ההקשחה

- חשוב שמנהל הרשת יגדיר מדיניות סיסמאות במערכות של הארגון בעזרת GPO ויוודא שכל הרשת אכן עומדת במדיניות סיסמאות שהארגון קבע.
- חובה לשנות את הסיסמה הראשונית שמגיעה עם פרטי ההתקשרות למשתמש חדש.
- יש לתעד תהליך של ניהול משתמשים: הקמת משתמשים, ביצוע שינויים במשתמשים ומחיקת משתמש.
- סיסמת הגישה לשרת הנתונים: שינוי תכוף של הסיסמה של שרת זה עלול לגרום לתקלות, להיעדר פעילות בחלקים מהמערכת מכיוון שקשה מאוד, ולעיתים אף לא אפשרי, לעדכן את כל התהליכים האוטומטיים המתקשרים עם השרת בסיסמה החדשה. על כן הסיסמה לבסיס הנתונים צריכה להיות ארוכה מ-**10** תווים, מורכבת מאוד ויש לשנות אותה אחת לשנה בתהליך מסודר ומתועד, כדי להקטין את הסיכוי שתוקף יצליח לפצח אותה.
- את הסיסמאות המאוחסנות יש להצפין.

המונח Brute Force מתייחס לתהליך או לאלגוריתם שפועל באופן של ניסוי וטעייה בעבור כל האפשרויות לפתרון בעיה נתונה עד למציאת הפתרון הנכון. מקרה פרטי של שיטת תקיפה זו הוא התקפת מילון, ועל פי שיטה זו, התוקף יוצר מראש "מילון" של סיסמאות נפוצות או הסבירות ביותר להצליח, ומנסה אותן בזו אחר זו. ככל שהסיסמה ארוכה יותר ומכילה מגוון רחב יותר של תווים, יידרש זמן רב יותר לפצח אותה.

2.5 הרשאות

עקרון ההגנה

הרשאות גישה למידע הן הכרחיות כדי שארגון יתפקד, אך מהוות בעצמן חולשה אינהרנטית. אם משתמשים לא יוגדרו כהלכה, באופן הכולל מגבלות על החשיפה, תוקף שיצליח להשיג פרטי גישה למשתמש בעצם יקבל גישה לכל הידע הארגוני ולעיתים אף יכולות עריכה ומחיקה.

כאשר עוסקים בהרשאות גישה במערכות ERP (Roles), הדבר מורכב יותר מאשר הרשאות גישה בתחומים אחרים: מבנה הרשאות הגישה מסובך, יש לאפשר גישה ממודרת למאגר הנתונים והרשאות גישה לאפליקציה, הרשאות עריכה והרשאות יצירה או מחיקה של מסמך או נתונים. הרשאות לחלקים שונים בתוך המערכת (מודולים), לתיקיות שונות ולחלקים שונים במידע, כך שעובדים שונים יוכלו להיחשף למסמכים שונים, לפי צורכיהם, באותה התיקייה.

בארגונים גדולים, עם צורכי גישה מורכבים וריבוי של אפליקציות במערכת המצריכות Roles רבים, יש נטייה להימנע מהניהול המורכב שהדבר מייצר ולהגדיר מעט Roles עם הרשאות רבות, גם כשאין צורך בכך[9]. שינויים והתאמות (כסומטיזציה) של Roles, ייבדקו לפני כן בסביבה נמוכה יותר.

תהליך ההקשחה

הרשאות גישה לשרת הנתונים:

- ראשית, יש להגדיר מי יכול לפנות ישירות לשרת בסיס הנתונים. ההמלצה היא להקים משתמש חזק, DBA, שיוכל לפנות לבסיס הנתונים כדי לנהל אותו (הרשאות אדמיניסטרטיביות), אבל לא יהיו לו הרשאות גישה של עריכה. אם בארגון יש כמה אנשים שעובדים כ-DBA, יש לתת לכל אחד מהם משתמש Admin עם גישת ניהול של החלק במאגר שהוא מנהל;
- נוסף על כך יש להקים משתמש שמאפשר לאפליקציה לפנות אל בסיס הנתונים ולערוך בהם שינויים. למשתמש של האפליקציה יינתנו הרשאות מלאות לניהול הנתונים (חשיפה מלאה, עריכה, יצירה, מחיקה) ללא הרשאות ניהול השרת, כמובן.
- על מנת למנוע מצב שבו לעובד יש הרשאות עודפות, יש לקבוע נוהל מסודר של הענקת הרשאות בעת קבלה לעבודה או שינוי תפקיד ושל מחיקת הרשאות בעת עזיבה או שינוי תפקיד. הנוהל צריך להיות נגיש לעובדים המנהלים את ההרשאות וצריך להיות מצורף אליו טופס שינוי הרשאות שיתעד את השינוי ויאפשר מעקב.
- הרשאות גישה לשימוש במערכת ה-ERP:[10]
- המערכות מורכבות ממספר רב של תפריטים ופעולות שאפשר לעשות. כדי להגדיר

9 https://chapters.theiia.org/los-angeles/Events/Documents/IIA%20%20Los%20Angeles%20%20SAP%20Security%20Presentation%20.pdf

10 https://www.sapsecuritypages.com/authorization-groups-brgru/

הרשאות גישה ביעילות יש להגדיר Roles שכוללים הרשאות שימוש שונות, ולהם מוגדרים משתמשים שזקוקים להרשאות הללו בעבודתם. יש להגדיר גישה לתפריטים או לחלקים בתפריט וכן אילו פעולות ניתן לעשות בכל חלק של התפריט (קריאה בלבד, צפייה, עריכה/שינוי, יצירה). מקובל לחלק את ההרשאות ל"משפחות": הרשאות גישה כלליות, הרשאות גישה למידע, הרשאות גישה לטרנזקציות, הרשאות סיסטם ו-DBA.

- במסגרת הרשאות הגישה יוגדרו הפעולות שכל מי שנמצא תחת Role זה יכול לבצע: קריאה בלבד או הרשאות כתיבה ומחיקה (במוצרים שונים יהיו הגדרות פעילות שונות. אלה ההגדרות הנפוצות). כך תהיה לכל משתמש גישה למידע שהוא זקוק לו, ולו בלבד, לפי עיקרון "הצורך לדעת" וללא גישה לתיקיות אחרות, פעולות אחרות או מידע אחר מכל סוג שהוא.
- יש להקפיד שלכל עובד יהיה משתמש משלו ושלא ייווצר מצב שבו שני עובדים משתמשים באותה גישה, מכיוון שאז אי אפשר לזהות מי האדם שביצע פעולה מסוימת באמצעות אותו משתמש.
- בעת הגדרת ה-Roles והפעולות שאפשר לבצע (טרנזקציות) יש לוודא שאין הרשאות סותרות שיובילו להיעדר פיקוח על התהליך שהוגדר (למשל, שלא ייווצר מצב שעובד מסוים הוא גם מבצע התהליך וגם המאשר שלו) - הפרדת תפקידים.
- יש להגדיר הרשאות גישה גם בתוך תיקיות המערכת, על מנת למנוע מגורם שאינו רלוונטי לשנות מידע (כמו איש IT, שתפקידו לנהל את המערכת ולא את המידע שבה).

כדי להשלים את נושא ניהול המשתמשים וההרשאות מומלץ מאוד ליישם 2 מוצרים שאחד מנהל את הגישה של משתמשי הקצה למערכת והשני מנהל ומנטר את התהליכים העסקיים שמשתמשי הקצה מורשים אליהם. ניטור זה חשוב למניעת הונאות ו/או מצב שמישהו מחדיר נתונים בעלי אופי זר למערכת.

בנוסף מומלץ לערוך סקר הרשאות תקופתי לבקרת תהליכים קריטיים בארגון.

תורת הגנה בסייבר לארגון> משפחה: בקרת גישה > 4.1

2.6 תמיכה מרחוק

עקרון ההגנה

תמיכה במערכות ERP נעשית לעיתים קרובות מרחוק על ידי אינטגרטור, באמצעות השתלטות איש צוות התמיכה של האינטגרטור על התחנה הרלוונטית. ברוב המקרים אי אפשר להימנע משימוש בשירותי תמיכה מרחוק ועל כן יש להכיר את הסכנות האינהרנטיות בשירות זה ואת הדרכים להתמודד עמן.

יש ארגונים שיעדיפו להתמודד עם האיום הזה על ידי הקמת צוות תמיכה In-House. כך הארגון מגייס את אנשיו ואחראי למנגנוני ההגנה שהוא מוצא כנכונים ביותר.

תהליך ההקשחה

- בעת החתימה על הסכם ההתקשרות עם ספק ה-ERP, יש להתייחס להליך התמיכה הטכנית ולהגדיר אם הוא חלק מהשירות ובאילו דרכים הוא מיושם.

- יש להחתים את העובדים נותני השירות על הסכם סודיות למקרה שיצטרכו להיחשף למידע עסקי רגיש במסגרת התמיכה שיעניקו.
- יש להגדיר את הממשק שדרכו מתנהלת ההשתלטות מרחוק ולוודא שמערכות ההגנה בארגון לא חוסמות את הגישה בפורטים הרלוונטיים (שמגדירה החברה המספקת את התמיכה מרחוק).
- ניתן להגדיר ב-firewall, אם ישנו, התראה המעדכנת על התחברות דרך הפורטים האמורים. כך אפשר לנטר פעילות התחברות מרחוק ולגלות אם נעשתה התחברות אף שאיש מעובדי הארגון לא ביקש זאת.
- חשוב לוודא שההתחברות מרחוק נעשית באופן מאובטח ומבלי שגורם זר יצליח להאזין לתעבורה.
- יש להגדיר מראש אם התמיכה הטכנית עשויה לכלול שליחת קובץ כלשהו למקבל התמיכה, כמו קוד או דאטה מכל סוג אחר. יש לקבוע הליך בדיקות מסודר וקבוע ולבצע את הצעדים הטכניים ובדיקות האבטחה הנדרשות על מנת לוודא שהקובץ אמין ואינו מכיל קוד זדוני, וכן שלא יוביל לשינוי ביישום שיגרום לפרצת אבטחת מידע.
- יש לבנות טווח מאובטח לחיבור של SAP לצורך תמיכה. יש כמה אפשרויות להקשחת החיבור בהתאם לטופולוגיית הרשת, המוצרים וסוגי המערכות שאליהם צריך להתחבר.

2.7 העלאת קבצים למערכת ERP

עקרון ההגנה

לעיתים קרובות עובדים נדרשים להעלות קבצים שונים לתוך מערכת ה-ERP. הקבצים חיוניים הן לשם תיעוד המידע, שמירה על סדר ומעקב אחרי הפעולות הנעשות בתחום מסוים, והן לשם ביצוע חישובים, פעולות נוספות ואף קובצי קוד ופיתוח.

תהליך ההקשחה

יש לקבוע מנגנון להלבנת קבצים שיסרוק את הקובץ טרם עלייתו למערכת ה-ERP ויוודא שאינו נגוע בקוד שיזהם את המערכת.

2.8 גיבוי המידע

עקרון ההגנה

כל התקני הארגון זקוקים לגיבוי למקרה של נזק, מכוון או לא, ולמניעת אובדן של מידע. מערכות ERP מחייבות גיבוי הן מפאת רגישות המידע שבהן והן לנוכח כמותו הגדולה. יש לגבות את המידע אחת לתקופה שנקבעה מראש. אובדן של מידע במערכת עלול לפגוע פגיעה אנושה בארגון, הן בתפקוד שלו והן במוניטין שלו.

בעת התקשרות בהסכם הכולל גישה למידע, יש לקבוע SLA (Service level Agreement) - פרק הזמן המרבי שבמהלכו הארגון מתחייב לאפשר נגישות למידע אחרי שהיא נמנעה.

יש כמה שיטות גיבוי:
- גיבוי מלא - כל החומר שהוגדר מגובה.
- גיבוי שינויים - רק השינויים מאז הגיבוי המלא האחרון מגובים.
- גיבוי מצטבר - רק השינויים מאז הגיבוי המצטבר האחרון מגובים.

לכל שיטה חסרונות ויתרונות, ועל הארגון לבחור את שיטת הגיבוי בהתאם לקיבולת הנתונים לגיבוי ולתכיפות השינויים.

תהליך ההקשחה[11]

אחד מתפקידיו של ה-DBA הוא להכין תוכנית גיבויים מקיפה, ובה יוגדרו הנושאים האלה:

- מה לגבות - הן מה-ERP והן אפליקציות נוספות, המקושרות ל-ERP (מאגר הנתונים, מערכות הפעלה, אפליקציות שונות, סיסמאות ועוד).
- באיזה סוג גיבוי להשתמש - גיבוי לוגי, גיבוי פיזי אונליין, גיבוי פיזי אוף-ליין.
- קביעת אסטרטגיה לטיפול במאגרי מידע גדולים מאוד (VLDB). שיטות העבודה שונות בין ספקי המערכת השונים.
- קביעת לוח זמנים לגיבויים - באופן שימזער את הפגיעה בתפקוד הארגון. מוטב לעדכן אחת לשבוע, בשעות שלא עובדים (לילות, סופי שבוע) אך יש לוודא לפני כן שהגרסה הנוכחית תומכת בעדכון ברמה שבועית.
- לבחור היכן לאחסן את הגיבוי - גיבוי לדיסק או לקלטת ואחסון באתר DR. ההמלצה היא להעתיק לדיסק, מכיוון שזה יותר מהיר, ומשם להעביר לקלטת ולשלוח ל-DR.
- מדיניות שמירת הגיבוי - צריכה להתבסס על קצב הגיבוי ועל ה-SLA שנקבע בחוזים למיניהם, ולהתחשב בהכרח למחוק מידע כדי לפנות מקום למידע חדש. לבעל המידע צריכה להינתן הזכות לקבוע למשך כמה זמן יישמר המידע, בדרך כלל מדובר בפרקי זמן של חודשים או שנים, כפוף לחוק המקומי.

לאחר הגיבוי יש לתחזק את הקלטות לפי העקרונות האלה:

- גיבוי אוטומטי.
- ניטור ובקרה.
- לוגים וקטלוגים של גיבויים - יש לבצע אחת לתקופה סקירה של הלוגים והתיקיות שבהן הם מאוחסנים ולוודא שכל מה שצריך להישמר נשמר כראוי.
- תחזוקה שוטפת של תיקיות הגיבוי ומחיקה של מידע מיותר.
- על מנת לוודא שהמידע עולה בלי בעיות בעת הצורך, יש לתרגל ולהעלות מידע מהגיבוי:
  - בדיקת העלאת הנתונים מהגיבוי.
  - וידוא גיבויים - לבצע תיקוף של הגיבויים בלי לאחסן מחדש.
  - תרגול בהעלאת גיבויים בתוך סביבת בדיקות שהיא חיקוי של סביבת הייצור.
  - ביקורת שנתית/דו-שנתית, שבה מסבירים את תהליך השימוש בגיבויים, ומציגים את הלוגים ואת צילומי המסך שיציגו את סוג הגיבוי שנבחר.
- כאשר צריך לשחזר מידע מגיבוי, צריך קודם כל לגבות שוב, כדי לוודא שכלום לא יאבד, ואז להחליט האם תהיה העלאה מלאה מהגיבוי או העלאה חלקית. להחלטה זו יש משמעויות הקשורות למשך הזמן שיידרש לשחזר את המידע ולחזור לתפקד והיא צריכה להתקבל תוך התחשבות בצרכים העסקיים.
- אסטרטגיית התאוששות מהשחתת בסיס הנתונים - ה-DBA צריך לבחור אסטרטגיה בהתאם לטכנולוגיה המוטמעת בארגון, וכפוף להנחיות היצרן.

תורת הגנה בסייבר לארגון> משפחה: המשכיות עסקית

11 https://www.isaca.org/Journal/archives/2012/Volume-1/Pages/Database-Backup-and-Recovery-Best-Practices.aspx

2.9 הצפנה[12]

עקרון ההגנה

הצפנה היא כלי להסתרת המידע על ידי קידוד. הכלי הנפוץ למימוש הצפנה היום הוא החלפת מפתחות. כל צד מחזיק במפתח הצפנה ורק כאשר שני הצדדים משתמשים באותו המפתח המידע הופך לנגיש. מטרת ההצפנה היא למנוע יכולת פענוח של המידע במקרה ששאר ההגנות לא היו מספיקות ותוקף הצליח להשיג גישה למערכות הארגון. ההצפנה היא שכבת הגנה נוספת בעת העברת המידע ובאחסונו.

תהליך ההקשחה

On-Premise:

- יש לבחור שיטת הצפנה שתואמת לצורכי הארגון ולוודא שההצפנה פועלת על מידע המועבר (Data in Transit) ועל מידע מאוחסן (Data at Rest).
- יש להצפין את הכונן הקשיח.
- הצפנה טובה תמנע כמעט לחלוטין את היכולת להשתמש במידע, גם אם הגיעו אליו.
- מומלץ מאוד להתייעץ עם מומחה הצפנה ולקבל המלצה לשיטת ההצפנה המתאימה ביותר לצורכי הארגון.

שירותי ענן: יש להפעיל פרוטוקול תקשורת מאובטח לגלישה אל המערכת.

הצפנה: במסגרת בסיס הנתונים SAP HANA אפשר להריץ הצפנה במסגרת שירות בבסיס הנתונים שנקרא: SAP HANA Data Privacy. נושא זה חשוב מאוד מפני שהמידע בבסיס הנתונים אינו מוצפן באופן טבעי ויש צורך לבצע זאת באופן ייזום. בנושא ההצפנה חשוב מאוד לייצר מצב שממשקים שעוברים למערכות אחרות גם הם מוצפנים. מומלץ להימנע מהורדת מידע לקובץ שיושב בשרת שיתופי. במקרה זה המידע הרגיש יהיה זמין לכל בעל גישה לשרת הקבצים. כמו כן חשוב מאוד להקפיד על הצפנה של מידע שעובר למערכות שמקימים לצורך לימודים והכשרות - מידע זה יכול להיות מוצפן ועדיין לשרת את מטרות המערכת ללימוד.

תורת הגנה בסייבר לארגון> משפחה: הגנה על המידע > 5.1

2.10 אנטי-וירוס

עקרון ההגנה

תוכנת האנטי-וירוס היא תוכנה שנועדה לאתר וירוסים ולהגן על המחשב מפני פעילותם. במצב אופטימלי תצליח התוכנה לאתר ניסיון הדבקה של ההתקן על ידי תוכנה זדונית טרם התקנתה. במקרה אחר, כשההתקן כבר מודבק בווירוס, תנסה התוכנה לזהות את הווירוס בזמן פעולתו או לזהות את הימצאו על ההתקן על ידי דפוס התנהגות מסוים וחתימות שונות. על כן חשוב מאוד להשתמש בתוכנת אנטי-וירוס בקביעות ולשמור אותה מעודכנת.

תהליך ההקשחה[13]

אופי הפעולה של תוכנות האנטי-וירוס עלול לגרום לאובדן מידע בשרתי נתונים: אנטי-וירוסים פאסיביים עלולים להוביל לניתוקם מהרשת, זיהוי שגוי של קובץ נתונים כווירוס שיוביל למחיקתו. אנטי-וירוסים אקטיביים עלולים לנעול קובץ קריטי בעת סריקתו. זה יכול

---

12 https://it.toolbox.com/blogs/erpdesk/best-practices-in-erp-security-052714
13 https://erpblog.iqms.com/how-to-safely-run-anti-virus-software-on-your-erp-server/

להביא לידי השחתת מידע, אובדן מידע ופגיעה בסנכרון. קשה עד בלתי אפשרי להתאושש מתוצאות שכאלה.

כדי להימנע מזה יש להטמיע את המערכת בהתאם למבנה של מאגר הנתונים הפרטיקולרי: אילו מהקבצים פעילים והיכן הם ממוקמים, ולהגדיר בעזרת היצרן החרגות מומלצות.

תורת הגנה בסייבר לארגון> משפחה: מניעת קוד זדוני 7.3<

Firewall 2.11

עקרון ההגנה

רגישות המידע בשרת ה-DB מחייב הגנה ממוקדת כמה שיותר, כדי שלא תפגע בפעילות השוטפת של הארגון. Firewall משמש כמערכת לניטור וחסימת ניסיונות גישה של גורמים זדוניים לתוך השרתים באמצעות תעבורת אינטרנט או אינטרה-נט על ידי קביעת חוקי גישה ומניעת גישה. הוא מאפשר לבנות סגמנטציה בארגון, לקבוע אילו התקנים שייכים לכל סגמנט ולאילו סגמנטים אחרים אפשר לפנות ובכך למדר את הגישה לשרתים ולאפשרה אך ורק לגורמים מורשים.

אם ההחלטה הארגונית היא לחבר את ההתקן ל-Firewall, חשוב מאוד להשאיר אותו מתפקד כל הזמן, מכיוון שהוא משמש לרוב נדבך חשוב במערך אבטחת רשתות מחשבים בשילוב מוצרי אבטחה נוספים.

תהליך ההקשחה

- יש להגדיר מראש סגמנטציה וחוקי Allow ו-Deny, כאשר הגישה לשרת ה-DB מותרת רק לשני משתמשים, מסגמנטים שנקבעו מראש (שרת האפליקציה ומשתמש DBA), והגישה לשרת האפליקציה מותרת רק למשתמשים רשומים (סגמנט users, למשל) דרך פורטים מאובטחים (443 או פורטים ייעודיים אחרים).
- במידת האפשר מוטב להתקין firewall לפני ה-Database, שישמש נדבך הגנה נוסף, קרוב ככל האפשר לנכס המידע, וכך גם אם יבוצע שינוי כלשהו ב-firewall הארגוני, נכס המידע לא יהיה נתון בסכנה.
- חשוב מאוד להטמיע את עדכוני היצרן ב-Firewall. מוטב שלא להטמיע את העדכונים מיד עם צאתם ולתת להם זמן להתייצב, אך לא לחכות זמן רב מדי מכיוון שהעדכונים מכילים תיקוני תוכנה וחסימה של פרצות שהתגלו. התמהמהות בקבלת העדכון חושפת את המערכת לווירוסים שמהם כבר אפשר להימנע.
- יש בשוק מוצרים המדגישים חולשות וסכנות שרלוונטיות במיוחד למערכות ERP. הם מתמקדים באיתור המידע ושולחים עדכונים לספק ה-Firewall, שמעדכן את הלקוחות שלו[14].

תורת הגנה בסייבר לארגון> משפחה: הגנת תחנות עבודה ושרתים 6.1<

14 https://erpscan.com/press-center/press-release/erpscan-partners-check-point-protect-enterprises-cyberattacks-erp-/systems

2.12 מערכות הגנה סטטיות נוספות

עקרון ההגנה

Firewall אומנם מהווה הגנה טובה, אך לא בלעדית. ה-Firewall מטפל בממשקים החיצוניים לארגון ומונע כניסה לפי חוקים מוגדרים. על מנת להגן גם מגורמים שכן הצליחו לחדור אותו, או מפני פעילות זדונית המתרחשת בתוך הארגון, יש צורך בהגנה "המתבוננת פנימה".

תהליך ההקשחה

הטמעה של פתרונות הגנה סטטיים כמו:

IDS - Intrusion Detection System כלי לזיהוי ודיווח על פעולות זדוניות המתבצעות במערכת או על הפרה של מדיניות הארגון (כפי שהוגדרה בכלי).

IPS - Intrusion Prevention System כלי משלים ל-IDS, בעל יכולות בלימה וחסימה של מתקפות.

2.13 עדכוני יצרן ואבטחה[15]

עקרון ההגנה:

On-Premise: בכל מערכת, ובכלל זה במערכות ERP, מתגלים לעיתים כשלים, המתבטאים ביכולת לנצל את המערכת על מנת להשיג ו/או לשבש מידע. מרבית יצרני המערכות מספקים עדכוני אבטחה למוצרים שהם משווקים, וזאת על מנת לסייע ללקוחותיהם לשמור על המערכות מוגנות.

קושי בביצוע עדכוני תוכנה ואבטחה:

- העדכון פותח בפני הספק גישה למערכות הלקוח ולמידע הרגיש שבהן. הוא יכול לשמש כלי לגורם שלישי להשיג גישה למערכות הלקוח בלי שהספק יהיה מודע לכך.
- מורכבות המערכת מחייבת היערכות מקדימה לקליטת עדכוני תוכנה ואבטחה.
- ארגונים רבים חוששים מעדכון התוכנה יותר מהאיום שמפניו הוא מגן ונמנעים מלעדכן.
- קשה מאוד לבחון את תגובת המערכות והאפליקציות לעדכון מבלי לפגוע בפעילות העסקית של הארגון.
- מכיוון שאין שתי מערכות ERP זהות, קשה ללמוד מארגונים אחרים ולייישם, גם בהיבטי הגנה. כדאי ורצוי ללמוד מניסיונם של ארגונים שונים, אבל היישום צריך להיות זהיר וכפוף לצרכים הארגוניים.
- בארגונים גדולים, שיפור אבטחת המידע עלול לחייב שינויים בקוד.
- מתקפות הזרקת קוד (Code Injection) מתאפשרות כאשר גרסת ה-Web Framework לא מעודכנת, ולכן יש להקפיד לעדכן גם אותה.
- נושא אבטחת המידע אינו זוכה להתייחסות בהסכם מול ספק השירותים ו/או היצרן.

שירותי ענן: על ספק שירותי הענן מוטלת האחריות לעדכן את המערכת. יש לפעול לעדכון בהתאם לצורכי הארגון ולהקפיד שלא לגרום להפסקת השירות, להשחתת המידע או לאי-זמינות של המערכת במהלך העדכון או בעקבותיו. על הלקוח מוטלת האחריות לוודא שספק שירותי הענן מבצע את העדכונים כפי שהוא מחויב. במקרה שהלקוח משתמש ב-IaaS, האחריות לעדכון מוטלת עליו.

תהליך ההקשחה

בעיות אבטחת מידע או פרצות שאותרו במערכת ההפעלה יכולות להיות מנוצלות על ידי האקרים או תוכנות זדוניות. על כן עדכונים שוטפים

15 https://www.panaya.com/blog/erp-security/

ממזערים את האפשרות שתוקף ינצל חולשות אלו:

יש לקבל מהיצרן עדכון תוכנה בצורה מאובטחת ומאומתת.

יש לבדוק את העדכון במערכות ההלבנה.

יש להתקין את העדכון בסביבת test ולוודא שהעדכון אינו פוגע בתפקוד מערכת ה-ERP.

SAP NOTES - יש לשים לב לפעולות הידניות שחובה לבצע אחרי שהמערכת עודכנה, כדי להתאים את העדכון לצורכי הארגון.

תורת הגנה בסייבר לארגון> משפחה: הגנת תחנות עבודה ושרתים <6.1

2.14 ניהול שינויים

עקרון ההגנה

מערכות המתופעלות בתדירות יום-יומית עוברות שינויים בתכיפות גבוהה, החל בהוספת משתמש ושינוי הרשאות וכלה בהוספה או בהורדה של שירותים. היעדר ניהול ותיעוד השינויים ימנע מהארגון להבחין בתהליך שמבוצע על ידי גורם לא מורשה.

תהליך ההקשחה

יש להשתמש בכלי לניהול שינויים שנמצא במערכת ה-ERP. אם אין כלי מובנה כזה, יש לרכוש כלי חיצוני ולהטמיע אותו.

2.15 מנגנונים להערכת ההגנה

עקרון ההגנה

On-premise: בחלק ממערכות ה-ERP יש כלים אינהרנטיים שיודעים להעריך את רמת ההגנה למשתמש (דוגמת Early Watch Alert של חברת SAP). הכלי יודע להציג היכן יש פערים בין רמת האבטחה הרצויה לנוכחית והיכן יש אנומליות.

תהליך ההקשחה

מחלקת אבטחת המידע צריכה לבחון בקביעות במדיניות אבטחת המידע הארגונית את דוחות המערכת ולעקוב אחר שינויים בנתונים.

2.16 ניטור ובקרה

עקרון ההגנה

On-Premise: מערכות ניטור ובקרה אוספות ומתעדות כל פעולה שנעשית בהתקן המנוטר (שרת או תחנת קצה), את התעבורה הנכנסת והיוצאת ופעולות ותעבורה שנכשלו או נחסמו. אם מתקינים את המערכות נכון, הן מתריעות על אירועים שהוגדרו להן כחריגים. ניטור ובקרה חשובים, הן בשרת ה-DB, כדי להיות במעקב מתמיד אחר שינוי הנתונים בו, והן בשרת האפליקציה, כדי לקבל אינדיקציה כאשר גורם לא מורשה מנסה לפנות אליה. ניטור של עמדות הקצה יאפשר זיהוי של התנהגות חריגה על התחנה עוד לפני ניסיון הפניה לשרת האפליקציה.

שירותי ענן: יש לנטר גם בשימוש בשירותי ענן, מכיוון שלגורמי צד שלישי יש גישה חופשית וחוקית למערכות הלקוח. יש לאסוף לוגים ולחפש התנהגות אנומלית או ניסיונות חדירה ושיבוש נתונים.

בנושא ניטור ובקרה מומלץ מאוד ליישם רכיב תוכנה שנקרא Landscape Transformation Management - רכיב המאפשר כמה יכולות ניטור מובנות כולל הורדה והוספה של שרתי אפליקציה לפרקי זמן קצרים. הרכיב מנהל גם את בקרת התצורה במהירות ובקלות.

תהליך ההקשחה

כללי - יש להטמיע מערכת שתתריע על אירועים שהארגון מגדיר חריגים. את המערכת מגדירים לפי צורכי הארגון והיא תשלח התרעות רק בהתאם למה שהוגדר לה אירוע אבטחתי.

- הגנה על SysLog - סטנדרט לטיפול בהודעות לוג: כל פעולה שמתבצעת במערכת ה-ERP, ובכלל זה באפליקציות הקשורות אליה, נשמרת כ"לוג". איסוף לוגים הוא הכרחי בשביל לעקוב אחר הזמינות של המערכת ושל המידע והשימושים שעושים בו. בלוגים עצמם נאסף מידע רגיש ויש לוודא שהוא מאוחסן באופן מאובטח. הדרך הטובה ביותר לשמור על הלוגים היא להעביר אותם לאחסון offline אחת לתקופה שנקבעה מראש ולהגן שם על המידע באמצעים המוצגים במסמך התקני האחסון.

- על הארגון לאבטח את הרשומות כך שלא יהיה אפשר לערוך אותן לאחר קליטתן ולוודא שמוקצה להן שטח אחסון שיתאים לצרכיו ולא יחייב אותו למחוק מידע לעיתים תכופות מדי.

- בארגונים שהוטמע בהם מנגנון של גישה מרחוק, יש לבצע ניטור מוגבר של הגישה.

- יש לנטר גם את סביבת הטסט והפיתוח.
  - התראות הקשורות לניהול: Disk Error, Disk Space, Memory Read/Write Error, Session Timeout, Buffer Overload, CPU Error. התראות מה-DB: Record Not Found, DB Error, DB Read/Write Error.
  - התראות הקשורות לתקיפה: הודעות Failed Login, ניסיונות פנייה ב-Telnet או Remote Shell, כתובות IP חיצוניות שמנסות לפנות לרכיבים ברשת שלא מתקשרים החוצה, כתובות המשתייכות ל-Black List.

- יש לנטר גם שינויים המתבצעים במערכת הניטור:
  - שינוי ומחיקה של לוגים.
  - שינויים בהגדרות הניטור.
  - ניטור משתמשי SYSTEM ומשתמשי ברירת מחדל במערכת.

- יש לבצע הגבלות במערכת הניטור, כך שצוות ה-System לא יוכל למחוק לוגים או לערוך אותם, או לבצע פעולות שיובילו לביטול יכולות הגנה פעילות.

<u>On-Premise:</u> בחלק ממוצרי ה-ERP יש פונקציה לניטור חלקים מבסיס הנתונים ולא בהכרח את כולו. כך אפשר למקד את הניטור לחלקים רגישים ולהימנע מ"הצפה" של לוגים שמקשה להבין את התמונה.

ניטור של קוד:

חשוב מאוד שיהיה מצב של ניטור קוד במערכת. קוד משתנה ומתווסף לעיתים קרובות בסביבת הפיתוח ומשונע לסביבת הבדיקות וסביבת הייצור. בעבור אפליקציות SAP מדובר בעיקר על קוד ABAP, וחשוב מאוד לשמור על מצב שבו הקוד מנוטר ואינו חשוף למקרה שמישהו בתהליך כתיבה או שינוי של קוד מכניס קוד עוין, ובכלל זה הזרקה של משפטי SQL. לשם כך שכבת האפליקציה חייבת להיות מנוטרת. כאן מדובר למעשה ביכולת של SAP לספק ADD IN לשכבת האפליקציה NETWAEVER, שלמעשה

מנטרת שינויים בקוד ABAP בזמן אמת. הפתרון נקרא:

SAP NetWeaver Application Server, add-on for code vulnerability analysis הרכיב הזה מנטר בזמן אמת אובייקטים עסקיים ויישויות עסקיות במערכת ואפילו יכול לנטר כמה אובייקטים עסקיים בתהליך העבודה כשמדובר בפיתוח של צוות עבודה.

תורת הגנה בסייבר לארגון> משפחה: תיעוד וניטור

3. שימוש בשירותי ERP בענן[16]

עקרון ההגנה

ישנם כמה ספקי מערכות ERP שנותנים את שירותיהם בענן. בחירה מושכלת של ספק שירותי ענן, שתכלול את כלל היבטי הצרכים הארגוניים, לצד דרישות אבטחת המידע, תגדיל את הסיכוי לעבודה בלי הפרעות עם הפחתת סכנות.

לגבי יציאה לענן, אנו רואים יותר ויותר שימוש ביכולות ענן כפלטפורמה להרחבות יישומי SAP קיימים בארגון כך שנוצר מצב של עבודה בתצורה משולבת (Hybrid mode). חשוב מאוד אפוא לאבטח את העבודה בשני העולמות, בעיקר בנושא האינטגרציה מסביבת הענן ל-ON PREM. חשוב לציין שחברת SAP מספקת אמצעי הגנה ואבטחה באמצעות רכיב שנקרא: Cloud Connector. רכיב זה מגיע עם כל חשבון ענן של SAP ומציע אבטחה ברמה הגבוהה ביותר בארגון ובהתאם לדרישות מערכות ה-ON PREM של SAP.

תהליך ההקשחה

- בעת בחירת ספק שירותי הענן, יש לוודא שהוא עומד בתנאי אבטחת המידע המוכרים (כגון דרישות המערך להגנה על ספקים, SOC2, ISO 27001 וכו').
- יש לוודא שההתחברות לספק מאובטחת (MFA, SSO).
- שימוש ב-CASB (כלי לניטור הפעילות באפליקציה על ידי המשתמש ואכיפת מדיניות אבטחת המידע. הכלי יודע לשלוח התרעות לאדמיניסטרטור על פעילות חשודה), על מנת ליישם את מדיניות אבטחת המידע של הארגון גם על גבי הענן, כולל הרשאות גישה, Token, הצפנה ועוד.
- עקרונות כלליים ליישום CASB להגנה על מידע בענן[17]:
  - שילוב CASB ב-gateway של הרשת המקומית. כך יתקבלו התראות על גישה לשירותים שאינם מאושרים על ידי מדיניות אבטחת המידע וכן אספקת מידע לגבי משמות שימוש באפליקציות שונות.
  - שילוב CASB במערכות DLP ויישום מדיניות של מניעת דלף מידע כפי שמיושמת בשאר חלקי הארגון. כך ה-CASB וה-DLP שולטים על כל המידע שבענן, אבל הוא מנוהל דרך ה-DLP הכללי של הארגון, במקום לנהל שני מנגנוני DLP שונים.
  - שילוב CASB בתהליך זיהוי המשתמש. כך כניסה יחידה למערכת (SSO) ושימוש

16 https://downloads.cloudsecurityalliance.org/assets/research/erp-security/ERP_Security_Final_CSA_Feb08-18.pdf
17 https://downloads.cloudsecurityalliance.org/assets/research/erp-security/ERP_Security_Final_CSA_Feb08-18.pdf

במנגנון MFA מאפשרים שימוש בכלל האפליקציות. יישום נכון של האינטגרציה, שתמשיך את התקשורת בין כלי ה-CASB לכלי ה-MFA גם לאחר שהסשן נפתח, תאפשר ל-CASB למנוע פעילות עוינת בענן בלי לפגוע בפעילות החוקית על ידי דרישת הזדהות נוספת במהלך הפעילות בענן.

- אינטגרציה המשלבת פתרון CASB עם מנגנון הצפנה, DLP ותהליך זיהוי המשתמש. כך המידע בטוח גם כשהוא נשלח לגורם אחר, מחוץ לארגון. ההצפנה ודרישת ההזדהות מלוות את הקובץ גם כשהוא יוצא מהארגון ובכל מקום שבו ינסו לפתוח אותו. שילוב זה מאפשר לבטל את הגישה לקובץ בכל שלב.
- שילוב CASB עם APT. כך חשבונות הענן יהיו מוגנים מפני תקיפות מתקדמות בדומה להגנה שבתוך הארגון. הוספה של פתרון Sandbox לענן תגביר את רמת ההגנה ותגן גם מפני איומים שחודרים לארגון דרך הורדה של מסמכים, הורדת אפליקציות חדשות לענן, סנכרון משתמשים ושיתוף מסמכים.
- ארגון שעושה שימוש במערכת SIEM יכול לבצע אינטגרציה עם ה-CASB וכך לנטר אירועי אבטחת מידע ולטפל בהם גם בענן.
- על ארגון הבוחר להשתמש במערכת ERP בענן מוטלים תחומי האחריות האלה:
- וידוא של יישום תיקוני ההגנה המיושמים על ידי הספק.
- קונפיגורציה והקשחה של המערכות.
- הזדהות חזקה.
- הגדרת הרשאות גישה ו-Roles.
- ביצוע אינטגרציה בין מערכות הארגון השונות לאפליקציות ה-ERP.
- ניטור ובקרה.
- כאשר השימוש בענן הוא בתצורתPaaS או SaaS, יש לוודא שיש פיתוח מאובטח (SDLC) במערכת ובתוספות שלה ולהביא בחשבון אלמנטים נוספים של הגנה: Threat Monitoring, PT, תרגול להגברת מודעות, עדכוני הגנה ועוד.
- אל שירותי IaaS נתייחס כאל On-Premise מכיוון שכלל האחריות עובדת מהספק אל הלקוח.
- גיבוי הנ"ל במטריצה RACI[18].

תורת הגנה בסייבר לארגון> משפחה: מחשוב ענן ציבורי <11

4. הגורם האנושי

4.1 כלל המשתמשים

עקרון ההגנה

הגורם האנושי הוא "עקב אכילס" בכל ארגון. עובדים עלולים לעשות טעויות אנוש תמימות, שיובילו לדלף מידע, לאובדנו או להשחתתו ולגרום נזק ממשי לארגון.

עובדים גם עלולים לבצע פעולה בזדון, שקשה עד בלתי אפשרי למנוע באמצעות רוב מנגנוני ההגנה, מכיוון שלעובד יש ההרשאות המתאימות והוא מנצל אותן לבצע פעולה שתזיק לארגון.

חברת Onapsis מצאה שברשת האינטרנט יש מאות תיקיות של מערכות ERP שהגישה

18 ראה לדוגמה https://www.isaca.org/chapters3/Atlanta/Events/Documents/2017-04-CloudSharedResponsibility.pdf

אליהן חופשית, וכן שיש פורומים שבהם עובדים משתפים את פרטי ההזדהות שלהם למערכת[19].

תהליך ההקשחה

- הדרכות וימי עיון בנושא אבטחת המידע.
- חלוקת נהלים.
- תרגילי מודעות לעובדים.
- מנגנוני DLP.
- שימוש בשירותי מודיעין סייבר כדי לאתר מידע עסקי שדלף.
- בנוגע לפעולות הנעשות בזדון, עקרון ה-Segregation of Duties יכול למזער את הנזק: בתהליכים מורכבים בעלי חשיבות עסקית גבוהה, יש לערב יותר מגורם אחד. אם פעולה של עובד אחד מחייבת חתימה של עובד אחר, הסיכוי לנזק קטן משמעותית.

תורת הגנה בסייבר לארגון> משפחה: משאבי אנוש >19

4.2 משתמשים פריווילגיים

עקרון ההגנה

משתמשים בעלי הרשאות חזקות, כגון אדמיניסטרטורים, עובדי מחלקת מחשוב וכדומה, משמשים יעד אטרקטיבי במיוחד להשגת פרטי גישה. משתמש חזק יכול לבצע הרבה מאוד, אם לא את כל הפעולות האפשריות במערכת. הגנה מיוחדת על משתמשים מסוג זה היא קריטית בתהליך הקשחת המערכות.

לגבי ניטור משתמשים, מומלץ מאוד ליישם רכיב תוכנה שמאפשר ניטור וחריגות בקרב משתמשי קצה ומנהלי מערכת. רכיב זה נקרא: SAP Enterprise Threat Detection

והוא מגיע כחלק מחבילת הפתרונות של SAP GRC. הרכיב מנטר את הלוגים של המערכת גם כשמדובר בכמה אפליקציות מבוזרות של SAP ומאפשר ניטור מרכזי למשימה זו.

תהליך ההקשחה

ישנם כלים מסוגים שונים להגנה על משתמשים חזקים:

- טכנולוגיות שונות שמגנות על מספר מצומצם ומוגדר של משתמשים. הן יודעות לנהל ולנטר את פעילות המשתמשים ולדווח על פעילות חריגה בזמן אמת.
- יישום MFA ככלי הזדהות חזק יותר, המקטין את הסיכוי לפריצה למשתמש.

5. פיתוח מאובטח

עקרון ההגנה

מערכות ERP מורכבות ממודולים של הספק ולעיתים גם מאפליקציות של ספקי שירות אחרים המפתחים מוצרים שונים על גבי תשתית ה-ERP בהתאם לדרישות הלקוח, על מנת לשפר את ביצועי העובדים או להוסיף תהליכים מסוימים. את הפיתוח יעשה לרוב הצוות של הלקוח או צוות של ספק האפליקציה המתווספת ל-ERP.

תהליך ההקשחה

הוספת אפליקציות על גבי מערכת ERP עלולה לחשוף מידע רב ורגיש בפני הספק הבונה את האפליקציה, או ליצור כתוצר לוואי פרצת אבטחה שתוביל לפגיעה במידע. על כן יש

19 ONAPSIS / ERP Applications Under Fire: How cyberattackers target the crown jewels/ July 2018

לוודא שהליך הגדרת האפליקציה והכתיבה שלה כוללים היבטים של עקרונות הפיתוח המאובטח.

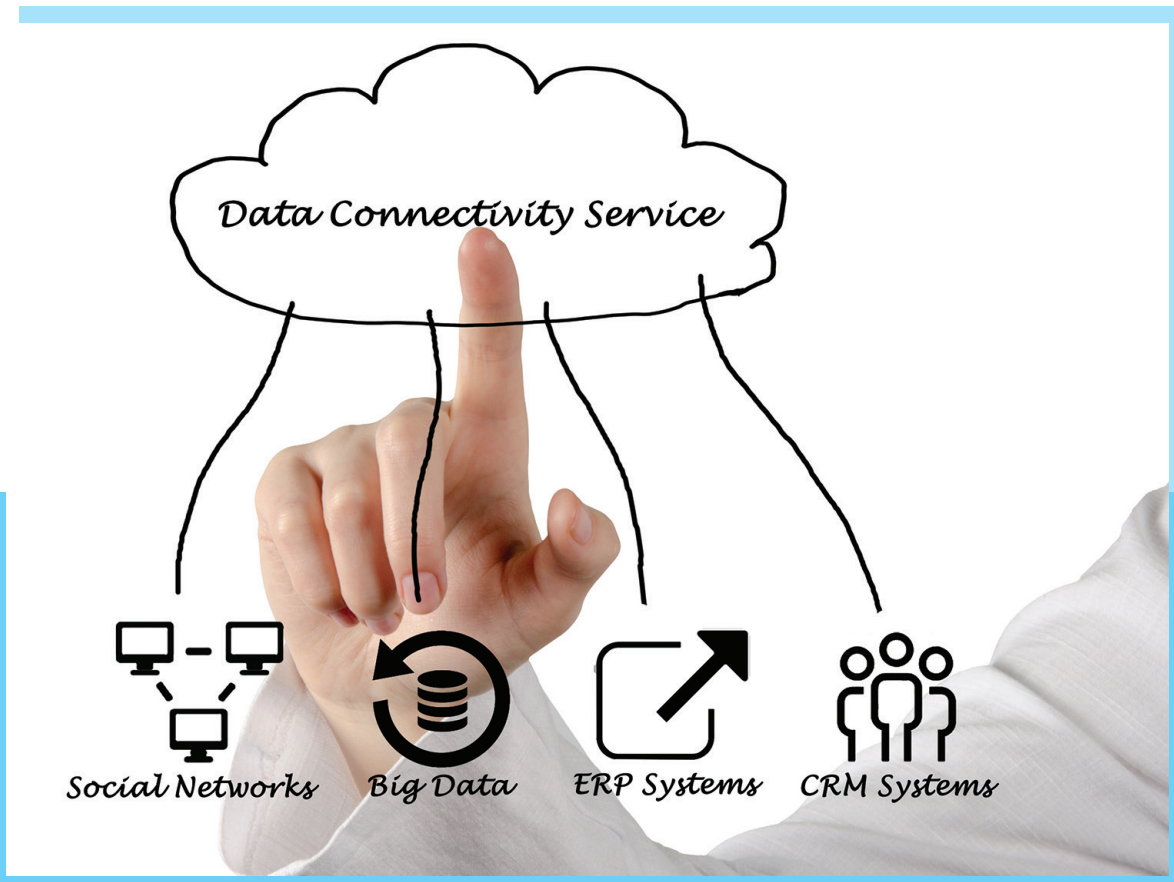
עקרונות מרכזיים לפיתוח מאובטח שיש ליישם במידה שרלוונטי לארגון:

- עבודה בסביבת טסט טרם ההעברה לייצור.
- ההעברה לייצור חייבת להיעשות גם היא באופן מאובטח.
- בדיקת קוד ידנית, סטטית ודינאמית.
- Penetration Test ידני וממוכן.

תורת הגנה בסייבר לארגון> משפחה: אבטחה ברשת ופיתוח > 17.6

6. מדיניות וציות

מערכות SAP כוללות רכיבים האוכפים מדיניות, שמטרתם להבטיח שהמערכת, ואגב כך הארגון שהיא מוטמעת בו, יעמדו בנהלים שקבע הארגון וברגולציות, בתקנים ובהסכמים שהוא מחויב אליהם, כמו: GRC Process Control, GRC Enterprise Threat Detection, GRC Access Control ועוד.



7. רשימת תיוג

נושא	בוצע	חלקי	לא בוצע
אבטחה פיזית של שרתי ERP	☐	☐	☐
הפרדה לוגית	☐	☐	☐
הפרדה מהאינטרנט	☐	☐	☐
גישה מאובטחת	☐	☐	☐
סגירת פורטים לא נחוצים	☐	☐	☐
התממשקות למערכות חיצוניות	☐	☐	☐
הקשחת מערכת ההפעלה	☐	☐	☐
התאוששות מאסון	☐	☐	☐
הזדהות	☐	☐	☐
סגירת פורטים לא נחוצים	☐	☐	☐
השבתה או מחיקה של משתמשי ברירת מחדל	☐	☐	☐
ניהול סיסמאות	☐	☐	☐
הרשאות	☐	☐	☐
תמיכה מרחוק	☐	☐	☐
העלאת קבצים למערכות ERP	☐	☐	☐
ניטור והצפנה של קוד ושינויים בקוד	☐	☐	☐
גיבוי המידע	☐	☐	☐
הצפנה	☐	☐	☐
אנטי-וירוס	☐	☐	☐
Firewall	☐	☐	☐
מערכות הגנה סטטיות נוספות	☐	☐	☐
עדכוני יצרן ואבטחה	☐	☐	☐
ניהול שינויים	☐	☐	☐
מנגנונים להערכת ההגנה	☐	☐	☐
ניטור ובקרה	☐	☐	☐
שימוש בשירותי ERP בענן	☐	☐	☐
כלל המשתמשים	☐	☐	☐
משתמשים פריווילגיים	☐	☐	☐
פיתוח מאובטח	☐	☐	☐
מדיניות וציות	☐	☐	☐

נספח: תקיפות מפורסמות

להלן שתי דוגמאות לתקיפות סייבר שהתאפשרו בעקבות פרצת אבטחה במערכות ERP:

- בשנת 2014 התגלה כי תוקפים סינים הצליחו לנצל חולשת Zero-Day במערכת ה-SAP של שירותי המידע של ארה"ב (United States Information Service), ספק המידע המרכזי של בדיקות רקע לסוכנויות הביון האמריקניות ולארגונים ממשלתיים אחרים. בעזרת החולשה הם הצליחו להשיג גישה למערכת המנוהלת על ידי צד שלישי, ומשם נסללה הדרך לשאר מערכות הארגון[20]. בתקיפה זו נגנב מידע אישי על 27 אלף עובדי הארגון[21].
- Dridex הוא סוס טרויאני אשר מוכוון לפגוע במערכות בנקאיות וב-2017 תוכנת מחדש כדי לפגוע במשתמשי SAP. הוא הופץ באמצעות רשת BotNet דרך קובצי word נגועים, נשתל במחשב הקורבן וחיכה להזנת פרטי גישה במערכות SAP[22]. הפוגען היה ממוקד מאוד והופעל רק בתחנות שבהן למשתמש יש הרשאות גישה גבוהות. לא נמצאו פרטים על היקף הנזק שגרם, אך הוא מהווה 11% מכלל המתקפות הפיננסיות הידועות בעולם[23].

20 https://www.infosecurity-magazine.com/news/report-chinese-breach-of-usis/
21 https://www.forbes.com/sites/forbestechcouncil/2017/07/07/erp-security-deserves-our-attention-now-more-than-ever/#7d948649a010
22 https://www.zdnet.com/article/erp-security-warning-as-hackers-step-up-attacks-on-systems/
23 http://www.eweek.com/security/dridex-banking-trojan-evolves-to-silently-bypass-application-control

ביבליוגרפיה

תורת ההגנה בסייבר לארגון - https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_ pdf.A4_418_organizations/he/Cyber1.0

https://www.sans.org/webcasts/security-geeks-guide-sap-

Security Principles in ERP Systems / jmeds.eu

https://archive.sap.com/kmuuid31/2d3e9ef0-c01-0010-01b8-8fbf154c0aca/SAP20%Hardening20%and20%Patch20%Management20%Guide.pdf

https://erpblog.iqms.com/how-to-safely-run-anti-virus-software-on-your-erp-server/

https://er.educause.edu/articles/11/2007/a-security-checklist-for-erp-implementations

https://www.panaya.com/blog/modern-alm/erp-security/

https://www.zdnet.com/article/dridex-banking-trojan-compromises-ftp-sites-in-new-campaign/

https://downloads.cloudsecurityalliance.org/assets/research/erp-security/ERP_Security_Final_CSA_Feb18-08.pdf

ONAPSIS / ERP Applications Under Fire: How cyberattackers target the crown jewels/ July 2018

https://it.toolbox.com/blogs/erpdesk/best-practices-in-erp-security052714-

https://erpscan.com/press-center/press-release/erpscan-partners-check-point-protect-enterprises-cyberattacks-erp-systems/

https://www.isaca.org/Journal/archives/2012/Volume1-/Pages/Database-Backup-and-Recovery-Best-Practices.aspx

https://csrc.nist.gov/projects/role-based-access-control

https://www.us-cert.gov/ncas/alerts/TA132-16A

https://www.infosecurity-magazine.com/news/report-chinese-breach-of-usis https://www.zdnet.com/article/erp-security-warning-as-hackers-step-up-attacks-on-systems

https://www.forbes.com/sites/forbestechcouncil/07/07/2017/erp-security-deserves-our-attention-now-more-than-ever/7#d948649a010

http://www.eweek.com/security/dridex-banking-trojan-evolves-to-silently-bypass-application-control

https://www.gov.il/he/Departments/policies/endstation

deployment-20-key-integrations-successful-casb-5/https://www.symantec.com/blogs/product-insights

119
tora@cyber.gov.il
www.cyber.gov.il

חפשו אותנו