תשתית אבטחת מידע

גלופת לימוד

גלופה זו מיועדת לסייע בהכנת מסמכי מחזור החיים בפרויקט אבטחת מידע תשתיתי. הגלופה מכילה עץ מערכת מתמחה (ייחודי) אשר בנוי ע״ג עץ המערכת האוניברסלי ומכיל את אותם היבטים ייחודים לפרויקט אבטחת מידע ואת השלכותיהם על מחזור החיים ועל עץ המערכת. הגלופה מדגישה את הנקודות השונות או הנוספות המיוחדות לפרויקט אבטחת מידע ואינה באה במקום מחזור החיים ועץ המערכת האוניברסליים. להבנת הגלופה ושימוש נכון בה, יש לעיין תחילה במדריך הנלווה. ראה גם גלופת עץ מערכת רמה 3 בקיט עץ מערכת אוניברסלי, שבכרך יסודות, שהיא הבסיס לגלופה זו.

לעבודה מעשית, ראה גלופת עבודה נלווה.

תוכן העניינים

תמצית מנהלים

1. יעדים

תמצית יעדי המערכת - היעזר ברכיב 1.0 שבגוף המסמך להלן.

2. יישום

תמצית היישום - היעזר ברכיב 2.0 שבגוף המסמך להלן.

3. טכנולוגיה ותשתית

תמצית הטכנולוגיה והתשתית של המערכת - היעזר ברכיב 3.0 שבגוף המסמך להלן.

4. מימוש

תמצית מימוש המערכת - היעזר ברכיב 4.0 שבגוף המסמך להלן.

5. עלות ומשאבים

תמצית עלויות המערכת, כולל תחזוקה צפויה - היעזר ברכיב 5.0 שבגוף המסמך להלן.

למידע נוסף על אופן כתיבת תמצית מנהלים, ראה קיט תיעוד בכרך נושאים תומכים.

0. מנהלה

פרק זה משמש לניהול ובקרה של השלב הנוכחי בו נמצא הפרויקט:

- גורמים מעורבים,
- תכנית העבודה,
- מעקב ביצוע מול תכנון,
- ניהול תצורה ומעקב שינויים של התיק עצמו,
- אישורים

שים לב להבדל בין פרק זה ובין פרק 4 מימוש להלן. בעוד שפרק זה מיועד לניהול השלב הנוכחי בו נמצא הפרויקט, פרק 4 מתאר את תכנית הפעילויות בכלל הפרויקט (מעבר לשלב הנוכחי) ואת אופן הטמעת אבטחת המידע ושימורה/תחזוקתה. עם סיום השלב הנוכחי, פרק 0 כבר אינו רלוונטי. פרק 4, לעומת זאת, הוא חלק מרכזי של תוצרי המערכת. (בשלב הבא "יתעורר" פרק 0 מחדש לתיאור אותו שלב).

0.0 כללי

תיאור מקוצר של השלב הנוכחי בו נמצא פרויקט אבטחת המידע (ושבמהלכו מופק תיק זה).

0.1 גורמים מעורבים

- גורם מבצע ראשי
- גורמים נלווים: הנהלת הארגון, אנשי IT (תשתיות ויישומים), אחראי אבטחת מידע, יועצים אחרים

0.2 תכנית עבודה

- במקרים מורכבים: תרשים גאנט, CPM/Pert
- ברוב המקרים מספיק: טבלת רשימת פעילויות ראשיות, מועדי סיום, מבצע ראשי וכו'.
- מעקב ביצוע מול תכנון (על התרשים או בתוך הטבלה)

0.3 כלים ונהלי עבודה

כלים ונהלי עבודה של השלב הנוכחי

0.4 ניהול תצורה ומעקב שינויים

להלן טבלת מעקב שינויים (ניהול תצורה) של השלב (התיעוד) הנוכחי:

תאריך	מהדורה / בסיס	מס' רכיב	תיאור השינוי	מאשר

0.5 אישורים

[ניתן להעביר טבלה זו לעמוד השער, בכפוף לנוהלי הארגון]

תאריך	שם	מייצג (מחלקה)	הערות	חתימה

1. יעדים

1.0 כללי - הבהקים

רצוי לכלול בהבהקים הגדרה ראשונית עקרונית של תיחום הפרויקט (סוגי תשתיות) תוך הפניה לרכיב 2.3 (תיחום פנימי). בנוסף, יש לכלול בסעיף זה עקרונות יסוד, תפיסה כללית וכו', נושאים אשר חשוב להדגישם, במבנה של הבהקים (Highlights).

דוגמא

מטרת הפרויקט לבצע סקר אבטחת מידע לכלל תשתיות הארגון, לכתוב מדיניות ונהלים בהתאם לסיכונים שנמצאו ברמת חומרה גבוהה, להטמיע בקרות ארגוניות וטכניות לסגירת הפערים עד לרמה סבילה, וליצור תהליך המשכי לסקירה תקופתית לצורך מציאת סיכונים חדשים והתאמת מדיניות אבטחת המידע בהתאם.

1.1 לקוח/מומחה יישום

פרויקט אבטחת מידע ברמת התשתית בארגון כולל עיסוק בקביעת מדיניות אבטחת מידע המחייבת אישור ע"י הנהלת הארגון. לכן, חשוב להגדיר בין הלקוחות העיקריים של הפרויקט אישיות בכירה (לרוב מנהל הארגון).

מנהל תחום אבטחת המידע יהיה "מומחה היישום" של הפרויקט.

בסעיף זה (1.1) יש לפרט את אותם משתמשים עיקריים שיכולים לייצג את כלל המשתמשים. בסעיף 2.2 יש לפרט את כל סוגי המשתמשים השונים.

מומחה היישום לפרויקט אמור להתמצא במדיניות ונהלי אבטחת מידע, בתשתיות, כלים ומנגנוני אבטחת המידע.

1.2 יעדים ומטרות

יש להגדיר הן יעדי אבטחת מידע כלליים, כגון העלאת רמת האבטחה בכלל רשתות המחשוב בארגון, והן מטרות מיידיות, כגון מזעור הדבקות שרתי הארגון בוירוסים ותולעי מחשב.

1.3 בעיות

1.3.0 תמצית הבעיות במצב הקיים

בעיות עיקריות הנובעות ממצב אבטחת המידע הקיים, כגון:

- אין רישום ומעקב אחר אירועי אבטחת מידע.
- העדר הפרדת רשתות (סגמנטציה) הופכת את כלל הרשת לפגיעה מאד.
- הרשת פגיעה בפני וירוסים עקב עדכון האנטי וירוס באופן לא סדיר.
- מנגנוני ההרשאות חלשים עקב ריבוי בעלי יכולת להגדיר הרשאות למשתמשים ללא פיקוח.

1.3.1 בעיות שהפרויקט פותר / אמור לפתור

בעיות אופייניות שפרויקט אבטחת מידע תשתיתי פותר:

- קביעת נושאים לטיפול לפי סדר עדיפויות.

- בניה ו/או עדכון מדיניות כבסיס להתנהלות בנושא בארגון.
- אינטגרציה ומקסום התועלת של מנגנוני אבטחת מידע קיימים.
- הבאת הארגון לתאימות להוראות וחוקים מחייבים בנושא אבטחת מידע.
- מזעור הסיכונים הנובעים ממצב אבטחת המידע בארגון לרמה סבילה.

1.3.2 בעיות שהפרויקט יוצר / עלול ליצור

- בעיות טכניות בעת הטמעת פתרונות לאבטחת מידע העלולות לגרום לפגיעה בזמינות או בשלמות מערכות המידע בארגון.
- השקעה כספית גבוהה.
- שינוי בדפוסי התנהגות של העובדים עם קשיי הסתגלות למדיניות החדשה.
- צורך בהשקעת משאבים להדרכות טכניות של פתרונות אבטחת מידע, או לחילופין לקליטת עובדים בעלי מיומנויות חדשות.

1.3.99 בעיות שיידחו

רשימת פערי אבטחת המידע שלא נכללו בתכולת הפרויקט (בעלי עדיפות נמוכה).

1.4 הקשר ארגוני/עסקי

1.4.1 יעדי הארגון, אסטרטגיה

הקשר של הפרויקט לאסטרטגיה הכוללת של הארגון (תכנית אב), לדוגמה: להכשיר את הארגון לאפשרות של התקשרויות עסקיות עם ארגונים ביטחוניים וממשלתיים.

היעזר בערכה תכנון אסטרטגי - תכנית אב למחשוב שבכרך ניהול כולל.

1.4.2 השלכות או"ש

השלכות הפרויקט על תהליכי או"ש ותהליכים עסקיים בארגון, כגון קליטת עובדים חדשים לתפעול מערכות אבטחת המידע החדשות.

שים לב: כאן מדובר בהשלכות כלליות \ ארגוניות \ עסקיות. בסעיף 4.7 להלן מדובר בשינויים מעשיים של נהלי עבודה והוראות הארגון.

1.5 תוכנית עבודה שנתית

בפרויקטים גדולים, יש להקפיד על תקצוב רב שנתי, בנוסף לחלק המתוקצב בשנה הנוכחית. יש לתאם תוכן סעיף זה עם סעיף 1.7 להלן.

1.5.1 תלות במערכות אחרות

מערכות אחרות (מידע ותשתית) שמופיעות בתוכנית העבודה השנתית או כבר בפיתוח שפרויקט אבטחת המידע תלוי בהן או משפיע עליהן. כאן הכוונה ל"תלות תקציבית", תלות הנובעת מתכנית הפיתוח הכוללת (תכנית העבודה) של הארגון.

1.6 ישימות ועלות/תועלת

לבדוק היטב בעיות היתכנות וישימות, ע"מ להימנע מדרישות אבטחה שפוגעות במטרות ובתפקוד הארגון, ובסופו של דבר לא תיושם מסיבה זאת.

לגבי התועלות ועלות/תועלת, הדרך המומלצת היא לנסות להעריך את הנזקים האפשריים לארגון מפריצות ואיומים, והסבירות שהם יקרו לעומת ההשקעה הנדרשת. אמנם יש ארגונים המחויבים לאבטחת מידע מכוח החוק או מתכתיב אחר, אך גם בארגונים אלה אין אבטחת מידע "בכל מחיר".

1.7 אופק הזמן

פרויקט מסוג זה יכול להמשך 2-3 שנים, אך הוא חייב לתת תוצאות ראשונות בפרק זמן של שנה לכל היותר.

2. יישום – מהות המערכת

2.0 תפיסה כללית – הבהקים

בסעיף זה מומלץ לתאר את מודל אבטחת המידע המוצע להשתמש בו.

2.1 מאפיינים כלליים של פרויקט אבטחת המידע

תיאור תמציתי של מצב אבטחת המידע הקיים, ללא חזרה על הבעיות (סעיף 1.3) והמטרות (סעיף 1.2), וציון המאפיינים של הפרויקט, כגון: פרויקט חדש, רה-ארגון התשתיות, פרויקט המשך וכד'.

2.1.1 אילוצים

יש להתמקד באילוצי חוק והנחיות ממלכתיות, כגון חוק שמירת הפרטיות תשמ"א, הנחיות משהב"ט עבור גופים מונחים, הוראה 357 לניהול טכנולוגיות המידע עבור גופים פיננסיים.

2.1.2 מילון מונחים

אזכור מספר מונחים עיקריים בנושא אבטחת מידע.

2.2 תיחום חיצוני

2.2.0 תיחום כללי

סעיף זה חשוב כדי להגדיר את גבולות הגזרה של הפרויקט מול עולם סבוך של תשתיות המחשוב בארגון. יותר מהגדרת התיחום של הפרויקט, כאן מגדירים את הנושאים הלא כלולים בפרויקט.

נדרש תיאור הגבולות של מכלול התשתיות הכלולים בפרויקט, מול שאר התשתיות הן בארגון והן מחוץ לארגון.

לדוגמה, עבור פרויקט אבטחת מידע שכולל את כל תשתיות ה-Unix ובמערכות הרצות מעל ל-Unix, הגבולות יבהירו מה לא כלול בפרויקט – תשתיות מיקרוסופט, רכיבי תקשורת מסוימים, תשתית הקישור לאינטרנט וכד'.

2.2.1 משתמשים

הגדרת המשתמשים של תשתיות הפרויקט, הן בתוך הארגון והן מחוצה לו.

2.2.2 תשתיות ומערכות משיקות

הגדרת תשתיות ומערכות משיקות אשר מחוץ לתיחום הפרויקט, אך המושפעות מהפרויקט.

2.3 תיחום פנימי

פירוט התשתיות והמערכות הכלולות בפרויקט זה. התיאור יכלול:

- רשימת התשתיות והמערכות
- חלוקה לתתי פרויקטים אפשריים
- עדיפות לטיפול עבור תתי הפרויקטים

2.4 ממשק משתמש

סעיף זה רלוונטי באם במסגרת הפרויקט נבנית מערכת לניהול מרכזי של אבטחת המידע בסביבה המטופלת ע״י הפרויקט. במקרה זה, מומלץ לפרט את המודולים או רכיבים אשר יכללו במערכת.

2.5 תהליכים

תאור של התהליכים המטופלים במסגרת הפרויקט.

לדוגמה:

- הזדהות ואימות הזהות ברמת הרשת.
- בקרת גישה ומתן הרשאות לתשתיות וליישומים.
- תהליכי בקרה ופיקוח (Audit)
- יצירת התראות על אירועים חריגים.
- Secure Single Sign On (SSSO)

2.6 טרנזקציות

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.7 מודולים ותוצרים (של אבטחת מידע)

רשימה של התוצרים בפרויקט, החל ממסמך סקר סיכונים, מסמך מדיניות אבטחת מידע, תכנית עבודה שנתית, תתי מודולים של אבטחה המיועדים למימוש, וכד׳.

2.8 מהלכים (פרוצדורות בקרה)

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.9 שגרות (אובייקטים משותפים)

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.10 טבלאות קודים

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.11 קבצים לוגיים

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.12 קבצים פיסיים – Data Base

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.13 מילון פריטי-מידע (שדות)

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.15 דו"חות (ושאילתות)

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.16 קלטים (טפסים)

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.19 אבטחת מידע

רכיב זה מוקדש להגדרת תהליכי ומנגנוני אבטחת מידע הנדרשת בעת ביצוע הפרויקט. לצורך העניין, הטפול צריך להיות כמו בפיתוח מערכת חדשה (ראה סעיף 2.19 בעץ המערכת האוניברסאלי).

להלן מספר דוגמאות לאבטחה הנדרשת במסגרת פרויקט אבטחת מידע תשתיתית.

- באם במסגרת הפרויקט יש צורך בהחלפת מנגנון ההצפנה של תעבורת הרשת, יש צורך לנקוט במנגנוני אבטחה כדי למנוע העברת מידע לא מוצפן בפרק הזמן שבין הסרת ההצפנה ה"ישנה" לבין הטמעת ההצפנה החדשה.
- כל המסמכים שנכתבים אודות הפרויקט הם רגישים ויש צורך לשמור על סודיותם ועל מידור אנשים בארגון שלא שותפים לפרויקט.

2.20 הצלבות וחיתוכים

לא רלוונטי לפרויקט אבטחת מידע תשתיתי.

2.21 נפחים עומסים וביצועים

כאן יתוארו מנגנוני ותהליכי אבטחת מידע המיועדים למימוש, ואשר עלולים להשפיע לרעה על עומסים וביצועים ברשת הנדונה בפרויקט. מנגנונים היוצרים עומסים משמעותיים עלולים להוות סיכון ממשי לפרויקט, ולכן חשוב לזהות סיכונים אלה בשלב המוקדם האפשרי במהלך הפרויקט.

2.22 ממשקים וקישורים

- תאור של תשתיות וממשקים למערכות שיהיו מושפעים מהשינויים הנובעים מהפרויקט.

2.23 דרישות מיוחדות

לדוגמה:

- תמיכה בעברית ואנגלית במוצר אבטחה.
- גמישות: עמידות בהכנסת שינויים והרחבות.
- יבילות (Portability): יכולת העברת נתונים וקוד על פני פלטפורמות שונות.

3. טכנולוגיה ותשתית

כל הפרק של טכנולוגיה ותשתית הינו רלוונטי לשלב במחזור החיים בו אופיין כבר פתרון טכני לשיפור אבטחת המידע של התשתיות נשוא הפרויקט.

3.0 ארכיטקטורה כללית - הבהקים

הצג תרשים ארכיטקטורה ורכיבי הטכנולוגיה המרכזיים הכלולים בפרויקט לאבטחת מידע.

3.1 חומרה מרכזית

תאר בפרוט את רכיבי החומרה הנדרשים להוספה במסגרת הפרויקט.

3.2 אחסנת נתונים מרכזית

תאר את אמצעי אחסנת הנתונים הנובעים מהפרויקט.

3.3 ציוד קצה

תאר את ציוד הקצה עבור החומרה המרכזית הנובע מהארכיטקטורה המאובטחת.

3.4 ציוד מיוחד

לדוגמה, מערכות אבטחה ייעודיים הנובעים מהארכיטקטורה המאובטחת, כגון מצלמה ליצירת כרטיס חכם, נעילות פיסיות וכד'.

3.5 ציוד מתכלה

תאר את הציוד המתכלה הנובע מהפרויקט.

3.9 תשתית סביבתית

ראה פירוט בעץ המערכת האוניברסאלית.

3.10 מערכת הפעלה

פירוט של מערכות ההפעלה במחשבים ובשרתים המרכזיים המתווספים עקב הפרויקט.

3.11 בסיס נתונים - DBMS

פירוט בסיסי נתונים המתווספים עקב הפרויקט.

3.13 כלים פיתוח ותחזוקה

לא רלוונטי.

3.15 כלי תפעול ויצור

- כלים ליצירת אמצעים להזדהות חזקה (כרטיס מגנטי, כרטיס חכם...).
- כלים לניטור האבטחה ברשת.
- כלים לקבלת התראות אבטחתיות, כגון Beeper.

3.20 חומרה מחשב לקוח

לא רלוונטי.

3.30 תקשורת פרטית מקומית

3.31 תקשורת פרטית רחבה

3.32 רשתות ציבורית

באם מתוכנן חיבור התשתיות נשוא הפרויקט לרשתות ציבוריות, יפורטו בסעיף זה אמצעי האבטחה המתוכננים למימוש במסגרת הפרויקט.

3.33 טכנולוגיות משיקות

4. מימוש

4.0 כללי - הבהקים

4.1 גורמים מעורבים

4.1.1 צוות ניהולי

תפקיד	שם	טלפון	מיקום	אחריות	הערות

4.1.2 צוותים מקצועיים – צוותי הפיתוח

4.1.3 סיוע טכני

4.1.4 ספקים וגורמי חוץ

4.2 תכנית עבודה

4.3 השלב הבא / המיידי

4.4 תפעול שוטף

בפרויקט אבטחת מידע תשתיתי לארגון, בו חלק מהתוצרים הם מסמכים (מדיניות, נהלים) וחלק הם תוצרים טכניים, המושג "תפעול שוטף" מקבל משמעויות שונות.

לגבי מדיניות ונהלים, התפעול השוטף בא לידי ביטוי בהטמעת אותם מדיניות ונהלים בארגון.

לגבי מערכת ניטור אבטחה, לעומת זאת, התפעול השוטף כולל מעבר על לוגים והתראה לממונים במקרה של אירוע חריג. במקרה של Firewall מדובר הן בתחזוקת החוקים והן במעבר על לוגים.

יש צורך להגדיר את הפעילות המתאימה לכל הרכיבים הרלוונטיים.

4.5 אינדקס התיעוד

הפניה לנספחים רלוונטיים, כגון למסמך מתודולוגיה לביצוע סקר סיכונים, או לכתיבת מדיניות אבטחת מידע.

4.6 שירות ותחזוקה

רשימת רכיבי אבטחת מידע קריטיים והגדרת השירות והתחזוקה הנדרשים עבורם להבטחת זמינות המערכות. מומלץ לכלול גורם אחראי, זמני תגובה לטיפול בתקלות, תחזוקה מונעת, הדרכות נדרשות וכד'.

4.7 השתלבות בארגון של השינויים בתשתית הארגון

יש לתכנן היטב את ההטמעה לפי סוגי המערכות והמשתמשים השונים. מומלץ להכין תוכניות הדרכה שונות עבור רכיבי אבטחת המידע השונים.

4.8 חוסן ואמינות

נושא חוסן ואמינות חשובים ביותר עבור מערכות אבטחת מידע, שכן כשלון של רכיב אבטחה עלול לגרום לנזקים גדולים בארגון. נדרשת תוכנית מקפת של בדיקות אבטחת התשתיות עם סיום הפרויקט ולפני הכנסתו לייצור.

4.9 תצורות

5. עלות - משאבים

5.0 תמצית העלויות - הבהקים

5.1 עלות הקמה (פיתוח והתקנה)

שם הנושא	עלות כ"א	עלות משאבים	אחר
סה"כ			

5.2 עלות שוטפת

בחישוב עלות שוטפת (על פני 5 שנים) של תשתיות אבטחת מידע, יש לקחת בחשבון את הגורמים הבאים:

עדכון ושדרוג מערכות אבטחת מידע.

עלות המשאבים הדרושים לתפעול השוטף של מערכות אבטחת המידע.

5.3 עלות לפי תצורות

5.4 מחירון

5.5 עלות כוללת ופריסה

נספחים

נספח א': סקר סיכונים

נספח ב': מדיניות אבטחת מידע