ניהול שרשרת האספקה

"השרשרת חזקה כחוזק החוליה החלשה שלה"

רקע

סיכון עיקרי

סיכון הסייבר הפך לאחד משלושת הסיכונים העיקריים שאיתם מתמודדת הנהלת הארגון

חשיבות הסיכון

ניהול סיכון הסייבר והשקעת משאבים בהפחתתו הפך להכרחי בכל ארגון מבלי קשר לגודלו ולפעילותו העסקית

התוקף הפוטנציאלי

כיום הגנת הסייבר היא רחבה הרבה יותר ותלויה בכל אחד שיכולה להיות לו גישה לארגון ובעצם יכול להוות דלת כניסה לתוקפים

יעדי התוקף

תקיפות סייבר הפכו לפופולריות בכל סוגי הקשת של ארגונים לדוגמה בנקים, רשתות קמעונאות, מוסדות רפואיים, חברות תעופה, חברות תעשייה וכמובן תשתיות קריטיות של מדיניות

רקע

תקיפות

במהלך השנתיים האחרונות אנו עדים לעלייה במספר התקיפות שבוצעו דרך ניצול שרשרת האספקה בארגונים שונים

סטטיסטיקה

על פי נתוני חברת סימנטק, בשנת 2017 אחוז התקיפות משרשרת האספקה עלו כב- 200% (10 תקיפות גדולות שבוצעו דרך שרשרת האספקה לעומת 4 תקיפות בלבד שבוצעו בשנים 2015-2016)

כפי שאומר הפתגם - השרשרת חזקה כחוזק החוליה החלשה שלה.

ככל שהשרשרת ארוכה ומבוזרת יותר, כך היא פגיעה יותר. הארגונים פגיעים כמו הספק הקטן ביותר והפגיע ביותר שלהם.

האיומים הנובעים מתוך שרשרת האספקה

- התלות בגורמי חוץ יוצרת מגוון רחב של איומים העלולים לפגוע בארגונים
- תקן ISO27036 מספק הנחיות ומסגרת בקרות נדרשות על מנת לסייע לארגונים לאבטח את המידע ומערכות המידע שלהם בהתקשרות מול ספקים
- להלן דוגמאות לאיומי אבטחת המידע וסייבר המתוארים בתקן בקשר בין לקוח וספק חיצוני:
  - ✓ תקיפת מערכות הארגון דרך הספק;
  - ✓ גישה למידע או למערכות מידע של הארגון על ידי עובדי הספק;
  - ✓ גישה פיזית של עובדי הספק לאתרי הארגון;

האיומים הנובעים מתוך שרשרת האספקה

- ✓ הפעלת יישומים של הארגון על תשתיות הספק;
- ✓ אירוח (Hosting) של ציוד הארגון באתרי הספק;
- ✓ אחסון נתוני הארגון (לרבות גיבוי) אצל הספק;
- ✓ עיבוד מידע של הארגון על ידי הספק מחוץ לאתרי הארגון.

שורש הבעיה בניהול אבטחת שרשרת האספקה

- קיים קושי לנהל את אבטחת שרשרת האספקה באופן אפקטיבי ואקטיבי
- לחלק גדול מהארגונים יש מאות ואלפי ספקים
- קושי בביצוע סקרים לספקים – היקף, איכות ותכולה
- ניהול/טיפול/תיעדוף ממצאי סקרים
- חוסר בתכניות שיפור ומיטיגציה לספקים ותחזוקה שוטפת של הספקים

סוגי התוקפים

- ארגוני פשיעה
- מתחרים
- מדינות
- צבאות/ארגוני טרור
- האקטיביסטים
- האקר בודד ומיומן
- גורם פנימי (ספק, קבלן, עובד)

כיצד עלינו לנהל את שרשרת האספקה הארגונית

שלב 1: מיפוי הספקים

ראשית, נדרש למפות את כלל הספקים בארגון

נדרש להבין מיהם הספקים ? איזה שירותים הם מספקים

לארגון ? מיהם אנשי הקשר אצל הספק? האם הספק חתום

על הסכם סודיות והנחיות אבטחת מידע?

כיצד עלינו לנהל את שרשרת האספקה הארגונית

שלב 1: מיפוי הספקים

בשלב הבא יש למפות את רשימת הספקים לפי דרגות חשיבות

נדרש לבחון מיהם הספקים המהותיים לארגון ומי לא.

ניתן לדרג את רשימת הספקים לפי רמת חשיבות גבוהה, בינונית, נמוכה,

ואפשר להסתפק בפרמטרים של ספק מהותי ולא מהותי.

כיצד עלינו לנהל את שרשרת האספקה הארגונית

שלב 1: מיפוי הספקים - שאלות רלוונטיות

- הפרמטרים לחלוקת ספקים מהותיים ולא מהותיים משתנה בין ארגון לארגון.

להלן כמה נקודות חשובות שעל פיהן ניתן להעריך את רמת המהותית של הספק לארגון:

האם הספק מחזיק במידע רגיש של הארגון ?	האם לספק גישה מרחוק לרשת הארגון ?
האם הספק חשוף למידע רגיש של הארגון ?	האם הספק נוטל חלק מהותי בשירות קריטי של הארגון ?

כיצד עלינו לנהל את שרשרת האספקה הארגונית

שלב 2: הערכת סיכונים

לאחר שלב המיפוי נדרש להבין מהם סיכוני הסייבר אליהם חשוף הארגון

יש לבחון נושאים כגון: בקרת גישה, אבטחה פיזית, הגנה על עמדות קצה ושרתים, רכיבי אבטחת מידע, תחזוקת והקשחות שרתים ומערכות, גישה מרחוק, ניהול וטיפול באירועי אבטחת מידע, גיבויים וכו'.

כיצד עלינו לנהל את שרשרת האספקה הארגונית

שלב 2: הערכת סיכונים

יש לבחון את רמת ההגנה של אותם ספקים

בשלב הראשון יש לבחון את הספקים שהוגדרו מהותיים, לאחר מכן, ניתן להשלים את התהליך לכל שאר הספקים.

ניהול סיכוני הסייבר של שרשרת האספקה

סקרי סיכונים ושאלונים

סקרי סיכונים ושאלונים הם מרכיב מהותי בשלב הערכת הסיכונים, בשלב זה על הארגון לבצע סקר אצל הספק ולבחון את הנושאים לדוגמה שצוינו בשלב מיפוי הספקים

סריקות חיצוניות

ביצוע סריקות חיצוניות למשטח התקיפה של הספק בארגון ולבחון לאילו חולשות הספק חשוף

סקר בחצרות ספק

ביצוע סקרים לספקים אשר קיבלו את הציונים הנמוכים ביותר בשאלון/ או לחילופין בעלי רמת הסיכון הגבוהה ביותר לבנק

ניהול סיכוני הסייבר של שרשרת האספקה

מטרת הסקר היא להעלות מעל לפני השטח את הממצאים השונים ולהציע דרכים ובקרות להפחתתם. הספק מקבל את הממצאים שעלו מתוך הסקר ומתחייב לתקנם תוך פרק זמן מסוים.

ממצאים

הפקת תכנית עבודה המכילה את הסיכונים, הממצאים וההמלצות הנדרשות הינה מרכיב חיוני בתהליך ניהול הסיכונים. חשוב לעקוב אחר יישום ההמלצות ולוודא כי הספק אכן ביצע את מה שמוטל עליו מתוך תכנית העבודה.

הפקת תוכנית עבודה ויישומה

נושאים לבדיקה בביצוע ביקורות על שרשרת האספקה

1

תהליך מיפוי הספקים

האם כל הספקים הפעילים בארגון מופו וקוטלגו לפי רמת חשיבות?

2

תהליך הערכת סיכונים

האם בוצע סקר סיכוני סייבר לספק? האם הארגון מבין את החשיפות של הספק ואת השפעתן הפוטנציאלית על הארגון.

נושאים לבדיקה בביצוע ביקורות על שרשרת האספקה

3

תהליך ניהול הסקרים

האם הארגון מנהל את הסקרים **בכלי מרכזי אחד** המאפשר קבלת תמונה של מגוון הסיכונים עליו הוא חשוף מתוך שרשרת האספקה? ניהול ידני באקסלים פחות יעיל ככל שלארגון מספר רב של ספקים.

4

תהליך ניהול הממצאים

האם קיים **מקום מרכזי לניהול** כלל הממצאים שעלו מתוך הסקרים? האם מתקיים מעקב שוטף אחר תיקון הממצאים?

נושאים לבדיקה בביצוע ביקורות על שרשרת האספקה

5

יעילות ביצוע הסקרים

לעיתים מתבצעים סקרים שאינם מספיקים על מנת להבין את הסיכונים המהותיים של הספק. יש לבצע שאלונים מותאמים למספר סוגים שונים של ספקים ולוודא כי תהליך הסקר הינו מקצועי ומעמיק בהתאם לרמת הרגישות של הספק.

6

ביקורת מעמיקה

לאחר בדיקת הנושאים שצוינו לעיל ניתן לבצע ביקורת מעמיקה יותר אשר תבחן את רמת ההגנה של הארגון מפני תקיפות דרך שרשרת האספקה.

ביקורות מעמיקות על שרשרת האספקה

- ביצוע סימולציה תקיפה תהווה ביקורת מעמיקה ומקיפה יותר על מערך ההגנה הארגוני מפני תקיפות דרך שרשרת האספקה
- ביצוע תרגיל מקיף מסוג Red Team בוחן את שכבות ההגנה השונות, כך שתמונת הביקורת שתוצג לארגון תהיה יעילה יותר ובעצם תראה הלכה למעשה האם ניתן לתקוף את הארגון

דוגמאות לתקיפות סייבר שהחלו בשרשרת האספקה

- ב-9 בפברואר חל אירוע הפתיחה של אולימפיאדת החורף בדרום קוריאה. במהלך האירוע חלו סידרת תקיפות סייבר אשר גרמו לשיבושים במערך הממוחשב של האולימפיאדה, השביתו והשפיעו מערכות שונות (חלקן לא פורסמו), כגון רשתות ה-WiFi של האצטדיון ועמדות השידור. בנוסף על כך, רגע לפני טקס הפתיחה, האתר הרשמי נפל עד למחרת בבוקר, ובכך מנע ממבקרים רבים לקבל מידע ואף להדפיס כרטיסים. **האירוע משמעותי התרחש באמצעות פריצה לחברת Atos ספקית ה-IT הראשית של האולימפיאדה.**

דוגמאות לתקיפות סייבר שהחלו בשרשרת האספקה

- בתחילת חודש יוני תקפה הקבוצה האיראנית MuddyWater את החברה הסעודית Mobily.ws המספקת שירותי SMS לעסקים. הקבוצה, אשר מתמחה בהנדסה חברתית ומשתמשת ביכולת זו ככלי עיקרי להפצת הנוזקה הייחודית לה POWERSTATS פרצה לכתובת הדוא"ל של אחד מעובדי אוניברסיטת Saud King ושלחה אימייל המכיל צרופה זדונית אל החברה הסעודית.

דוגמאות לתקיפות סייבר שהחלו בשרשרת האספקה

- במסגרת ShadowHammer **הותקפה תוכנת ASUS Live Update Utility כנקודת המוצא להתקפה.**
- כלי זה שמותקן מראש ברוב מחשבי ה- ASUS החדשים, משמש לצורך ביצוע עדכונים אוטומטיים של BIOS, UEFI דרייברים ואפליקציות.
- באמצעות תעודות דיגיטליות גנובות, ששימשו את ASUS כדי לבצע חתימה לקוד, שהיא מפיצה, התוקפים הצליחו לחבל בגרסאות ישנות יותר של תוכנת ASUS, כשהם מצליחים להזריק אליהן את הקוד הזדוני שלהם. הגרסאות הפגומות של הכלי נחתמו עם תעודות לגיטימיות, **ונשמרו והופצו בשרתי העדכון הרשמיים של ASUS**, דבר שהפך אותן לבלתי נראות עבור רוב פתרונות ההגנה.
- למעשה, באמצעות פעולה זו כל משתמש בתוכנת העדכון הנגועה עלול להפוך לקורבן. אך הגורם, שמאחורי ShadowHammer התמקד בהשגת גישה למאות בודדות של משתמשים, לגביהם היה לו מידע מוקדם.

סיכום

- עולם הסייבר מאד דינמי ומשתנה יותר ויותר ככל שאנו מרבים להשתמש בטכנולוגיות שונות וחדשניות
- מערך ההגנה הארגוני שלנו אינו מסתיים רק בפרימטר (היקף) הארגוני וכולל גורמים נוספים שמהווים דלת לתוך הארגון
- תקיפות דרך שרשרת האספקה הפכה ליעד מרכזי של תוקפים כדי לקבל גישה לתוך הארגון בדרך קלה יחסית מאשר לפרוץ מערכי הגנה בשלים ומתקדמים

סיכום

- הסיכונים הנובעים מתוך שרשרת האספקה עלולים להוביל לנזק פוטנציאלי משמעותי עבור הארגון ולעיתים אף לאיים על המשך קיומו
- תהליך ניהול שרשרת האספקה הארגונית הינו תהליך חשוב ומהותי על מנת לבחון את סיכוני הסייבר אליהם עלול הארגון להיות חשוף

תודה!