מודלים של ביטחון מידע

עבודת גמר במסגרת קורס מגן סייבר

על- ידי

אמיר ששון

ת.ז : 200913002

אוקטובר 2021

תוכן העניינים:

מבוא

מתקפות סייבר הולכות ונעשות נפוצות מאוד. רק בשנה האחרונה שמענו על מספר מתקפות סייבר שגרמו לנזק רב למספר חברות, לתחנות דלק ואפילו לבית חולים גדול. כיום כל אחד חשוף, שכן כולנו מחוברים לרשת כל הזמן. הגישה לאינטרנט זמינה בלחיצת כפתור, מכל מכשיר, בכל מקום וכל הזמן. לפיכך, ארגונים בכל הגדלים פגיעים לפריצות וחייבים להגן על עצמם ועל המידע שלהם מפני משתמשים זדוניים ולא זדוניים כאחד.

בעבודה זו אציג שני מודלים עיקריים להגנת מידע- NIST CSF ו- Zero Trust. המוד השכיח יותר הוא הNIST CSF, מודל ביטחון מידע שנוצר על-ידי מספר חברות וגוף ממשלתי על מנת ליצור מספר קווים מנחים שיעזרו לארגונים בתעשייה להגן על עצמם ועל המידע הרגיש שלהם. NIST CSF הוא אמנם מודל נפוץ, אבל הוא לא מגן ב-100% על המידע שלנו. כלומר, אם נשתמש רק בקווים מנחים אלו אנחנו עלולים להיפגע.

כתוצאה מכך, נולד מודל ה"Zero Trust" - מודל חדש יחסית, שמסייע לנו לשמור על המידע שלנו. עיקר תפיסת מודל זה הינה "never trust, always verify". מונח זה מתייחס ליכולת הארגונים לא לבטוח באף אחד, ותמיד לוודא שאין פגיעה. לפי תפיסה זו, ברגע שאנחנו נותנים אמון אנו עלולים להיפגע, ולכן אנו חייבים להגן על המידע שלנו בצורה

מטרת העבודה הנוכחית הינה לעמוד על שני מודלים אלו, על שימוש בכל אחד מהם ועל שילוב של שניהם, תוך בניית תוכנית פעולה לאבטחת מידע מיטבית עבור ארגון.

Zero Trust

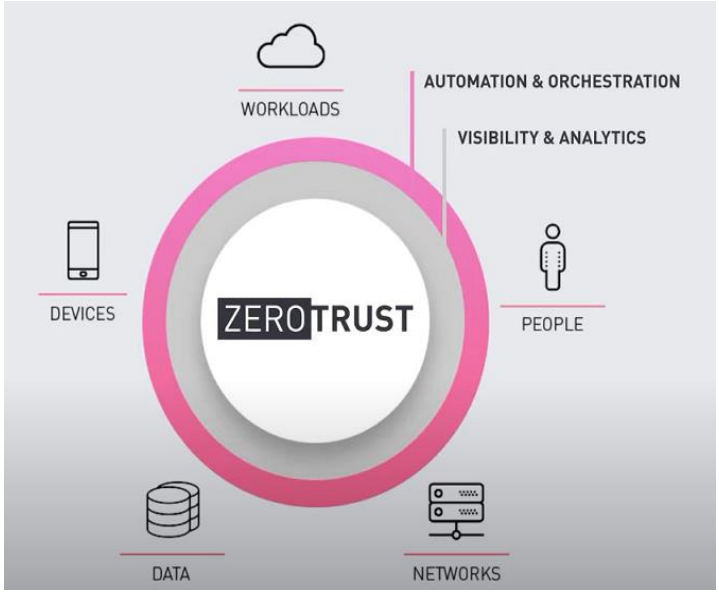
בעבר משתמש היה צריך להגיע בצורה פיזית לארגון שבו הוא עובד על מנת לקבל גישה למערכת ולמידע. כיום כל משתמש כמעט יכול לקבל גישה מרחוק לארגון, לגשת ולהעביר כל מידע שיש לו גישה אליו באמצעות הפלאפון, הענן או על-ידי גישה מרחוק.

Zero Trust (אפס אמון) הינו מודל ביטחון מידע אסטרטגי למניעת דלף, השואף להסיר כל אמון במבנה של ארכיטקטורה של ארגון. מודל זה הפך לשם דבר בכל מה שקשור לביטחון מידע בארגונים. הוא מונע על-ידי עקרון של "אף פעם אל תבטח, תמיד תוודא", והיא עוצבה על מנת להגן על סביבות דיגיטליות באמצעות סידור חלוקת הרשת, מניעת תזוזה ברשת ופישוט חלוקת הגישה על- ידי בקרת גישה.

מודל זה מבוסס על ההבנה שמודלים של ביטחון מידע מסורתיים מונעים ע"י הנחת יסוד מיושנת לפיה אפשר לבטוח בכל כלי תקשורת ברשת או משתמש בתוך רשת של ארגון, לעומת כל מה שנמצא מחוץ לרשת- שבו אסור לבטוח. מודל זה בא לקרוא תיגר על הנחת היסוד השגויה לפיה שכל זהות של משתמש בטוחה, שאפשר לתת אמון במשתמשים שיפעלו באחריות ואפשר לבטוח בהם. מודל זירו טראסט מבוסס על הבנה שדרך נתינת אמון אפשר להיפגע.

במודלים המסורתיים כל משתמש, גם משתמש זדוני, יכול לשוטט ברשת הארגון ולהעביר כל מידע שיש אליו גישה. החידוש במודל זירו טראסט הוא שכל משתמש צריך לקבל גישה מחדש בכל תנועה ברשת. כלומר, הוא תוכנן לא כדי לתת אמון, אלא בשביל למנוע מתן אמון.

המודל מורכב מ7 עקרונות של בטחון מידע.



העיקרון הראשון הוא "**זירו טראסט ברשת**". לפי עיקרון זה, יש לפצל נכון את רשת הארגון ולשלוט על כל חלק בנפרד, בד-בבד זיהוי כל נכס ברשת. עיקרון זה חשוב ביותר, והפיצול בו הכרחי. חשוב ביותר לפצל את הרשת לנכסים שונים ולחסום גישה לכל רשת בנפרד- הרשת הראשית של הארגון,

המידע שנמצא בענן , משתמשים וסניפים נוספים של הארגון. בדרך זו, ניתן ליצור חומות אבטחה לכל נכס בנפרד ובכך למנוע מעבר בין הנכסים, וכך במקרה של פריצה הפריצה מבודדת וקשה יותר להרחיב אותה לשאר נכסי הארגון.

העיקרון השני הוא "**זירו טראסט במשתמשים**"- כיום, ובעיקר בעידן הקורונה, נהוג לעבוד מהבית. כך, לעובדים רבים יש גישה מרחוק למערכות בארגון על-ידי ענן או התחברות מכוונת, גישה למיילים דרך פלאפון או כל מכשיר חכם אחר. הארגונים הפכו לפגיעים ואיך דרך לדעת אם המשתמש הוא באמת מי שהוא, וכך נוצרת חולשה בביטחון המידע בארגון, אם זה במודע ע"י משתמשים זדוניים שרוצים לפגוע ברשת או לא במודע ע"י לחיצה על לינק זדוני. חשוב לנהל את הגישה לרשת בצורה מוקפדת ולהקשיח את ההתחברות לרשת, בצורה כזאת שמשתמש מרוחק צריך לעבור אימות לפני התחברות לרשת ושמשתמש מרוחק יכול לגשת רק לאן שאנחנו רוצים ונותנים לו גישה מבלי לגשת למקומות נוספים ברשת בצורה מרוחקת.

העיקרון השלישי הוא "**זירו טראסט במידע**". כמות המידע שנשלחת ממשתמש למשתמש היא בלתי נדלית. פעמים רבות, מדובר במידע שמגיע מחוץ למערכת שלנו, ונע בין שרתים במערכת, ולכן חשוב מאוד להגן על המידע שלנו ולהגן על הרשת ממידע זדוני. ניתן לעשות זאת על-ידי הגבלת חשיפה לנתונים רגישים ועל-ידי הגנה רב שכבתית על נתונים. בדרך זו, ניתן למנוע דלף מידע, השחתה ואובדן של נתונים ברשת.

העיקרון הרביעי הוא "**זירו טראסט בעומסי העבודה**". כיום משתמשים רבים עובדים מרחוק. אותם משתמשים מתחברים בצורה מכוונת לשרתי החברה או לשרתי ענן של החברה ובעקבות כך אנחנו צריכים להגן על אותם מרחבי העבודה בדרך שונה ממה שהיינו רגילים עד היום. כאשר אותם מרחבי עבודה נמצאים בענן או בשרת מרוחק הם הרבה פעמים מטרה קלה למשתמשים זדוניים, בגלל שאפשר להתחבר אליהם מכל מקום. חשוב מאוד להגן על אותם מתחמים ולבצע ניטור מידע וכן להגביל את פעולות המשתמשים. בזירו טראסט ניתן להגיע למצב שבו תהיה אפשרות לבודד מוצר משאר הרשת במקרה של פריצה או דלף מידע.

העיקרון החמישי הוא "**זירו טראסט במוצרים**". כיום, כאשר פריצות רבות הקשורות למוצרים שיש לנו ברשת, כל מוצר מהווה איום על הרשת שלנו. לכן, חשוב מאוד להגן על המוצרים שמחוברים אלינו לרשת בד-בבד הגנה מהמוצרים שמוצעים מחוץ לרשת, כגון, מצלמות רשת, מדפסות, או כל מוצר תקשורת אחר. אותם מוצרים פגיעים ועלולים להוות איום לרשת הארגון, ולכן יש לבודד כל מכשיר.

העקרונות האחרונים הם "**זירו טראסט Analytics & Visibility**". עקרונות אלה גורסים כי לא ניתן להגן על מה שאין אפשרות לראות או להבין. לכן, חשוב מאוד לבצע בקרת גישה ותיעוד של כל פעילות הרשת. מודל זירו טראסט דורש פיקוח, תיעוד וניתוח של תעבורת הרשת, בין אם מדובר בבקרת גישה למשתמשים, זיהוי המשתמש בכל התחברות מחדש, תעבורה של מידע ברשת, שימוש באפליקציות, או גישה למידע ברשת הארגון. בכל מצב, אנו חייבים לבצע מעקב אחרי פעולות אלו ללא הפסקה.

ארכיטקטורת Zero Trust :

ארכיטקטורה כללית של מודל זירו טראסט מבוססת על מצב שבו אנחנו רוצים לזהות את כל הדברים החשובים לנו ברשת- מידע, נתונים, נכסים, אפליקציות ומשאבי רשת חשובים, ובכלל לזהות את "שטח ההגנה" של הארגון. שטח ההגנה ייחודי לכל ארגון ומכיל רק את מה שחשוב לפעילות השוטפת של הארגון. חשוב להיות מודעים לשטח ההגנה של הארגון, על מנת ליצור בקרת גישה ולהבין מי המשתמשים וכיצד הם מתחברים למשאבי הארגון. באופן זה, תיאכף מדיניות שמבטיחה גישה בטוחה על ידי זיהוי כלל המשתמשים.

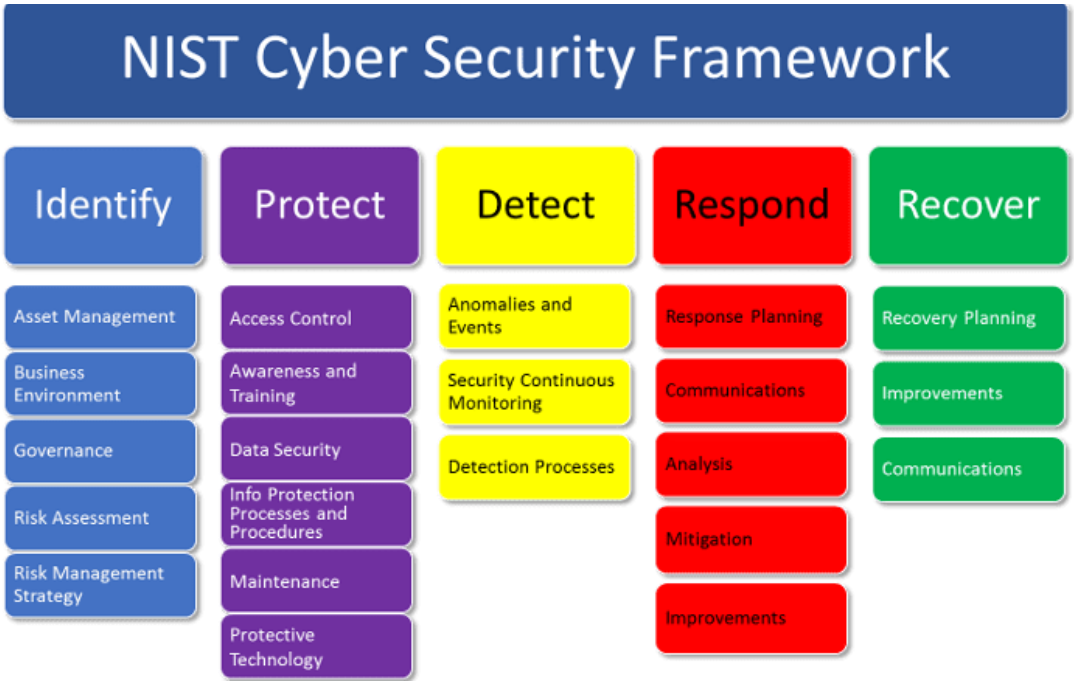
בדרך זו, ניתן להגדיר security control לנכסי הארגון. דרך זו תבטיח צמידות לשטח ההגנה, פעולה שתאפשר לבצע בקרת גישה ותנועה מורשת ולגיטימית ברחבי רשת הארגון- מתן גישה בטוחה, ביצוע מעקב, בקרה ופיקוח על משתמשים בכל רגע נתון.

NIST CSF

כיום, ששכיחות האינטרנט גדולה, עולים גם הסיכונים ברשת, סיכונים שחברות וארגונים מכל הסוגים והגדלים מוכרחים להגן על עצמם מפניהם. לעתים, מתרחש מצב שהארגונים מזהים את התקיפה לאחר מספר חודשים, אם בכלל. בעקבות כך, מכון התקנים האמריקאי (NIST) החליט לבנות תורת הגנה ששמה דגש גם על שלבי ההיערכות וההגנה, בהם שלבי האיתור, ההכלה וההתאוששות במקרה של תקיפה. תחת גישה זאת מתבצעת הגנה על ארגון מפני תקיפה עתידית בד-בבד חיזוק יכולתו של הארגון לגלות תקיפה שהצליחה, להכילה ולהתאושש ממנה במינימום נזק לארגון וחזרה לעבודה מלאה.

מודל אבטחת מידע NIST CSF - National Institute of Standards and Technology Cybersecurity Framework , הוא מודל אבטחת מידע שנוצר בשיתוף פעולה בין חברות בתעשייה לבין הממשלה בעקבות ההבנה שיש ליצור קווים מנחים בסיסיים להגנה על ארגון. מטרת ההתאחדות הינה לעזור לארגונים לייצר לעצם מערך הגנתי שיפחית את התקיפות ברשת. במקרה של תקיפה המודל מאתר אותה ומסייע בתוכנית עבודה להשבת הארגון לפעילות מלאה בצורה המהירה והטובה ביותר. בנוסף לכך, המודל מאפשר להיות מעודכנים בכל חידושי אבטחת המידע לארגון בשוק.

המודל מחולק למספר קווים מנחים שיש לפעול על פיהם על מנת לייצר מערך הגנתי נרחב ככל האפשר וקווים מנחים איך להתכונן לתקיפה רשתית, להתאושש ממנה או למנוע אותה .



חמש אבני היסוד של מודל ה -NIST CSF

מודל אבטחת מידע זה מורכב מחמש פעולות בסיסיות שיש לפעול על פיהן :

1. **Identify** - הבנה ומיפוי של האובייקטיבים בעלי ערך בארגון על מנת ליצור רצף עבודה מלא ולהכין אסטרטגיות לניהול סיכונים- מה יכול להיפגע במקרה של תקיפה.
2. **Protect** - לאחר שעשינו מיפוי של כל הנכסים שהם בעלי ערך בארגון אנחנו צריכים להבין איך להגן עליהם. עלינו להיות מעודכנים עם עדכוני האבטחה האחרונים ולשפר את ההגנה שלנו ככל שמתפרסמים ומתעדכנים.
3. **Detect** - ביצוע של מעקב ברשת הארגון ויצירת מערך שמטרתו לאתר תקיפה או ניסיון תקיפה ברשת הארגון.
4. **Respond** – תגובה. פעולה זו עוסקת במה שעושים ביום שאחרי. במידה שגילינו ניסיון או חדירה לארגון, עלינו לפעול מיד לאחר התקיפה כדי למזער נזקים ולעצור אותה.
5. **Recover** - תכנון פעולות שיש לבצע ביום שאחרי התקיפה- איך להחזיר את הארגון לפעילות מלאה כמה שיותר מהר.

- Identify

- מיפוי נכסים (Asset Management)

על מה יש לנו להגן בארגון שהוא בעל ערך לשמירה על רצף עבודה מלא, סוגי ציוד מחשוב, מידע שיש להגן עליו , נכסים בענן ועוד , מיפוי הנכסים יתבצע כך שנדע להגדיר איזה נכס הוא קריטי לעבודה מלאה ואיזה הוא משני ואפשר להסתדר גם אם הוא נפגע או הושבת. יש למפות אילו מכשירי מחשוב פיזיים יש לנו בארגון , באילו תוכנות או אפליקציות או מערכות אנחנו משתמשים, לייצר מפה של של מעבר המידע שיש לנו בארגון , דרך איפה המידע עובר ואיך לשמור עליו, אמצעים שיש לנו בארגון , אם זה מיפוי העובדים לפי חשיבות ועד לציוד המחשוב הקריטי להם להמשך עבודה רציף.

- סביבה עסקית - (Business Environment)

יש למפות מה היא הסביבה העסקית של הארגון, משימות, מטרות , בעלי העניין ופעולות הארגון , המיפוי מתבצע ע״פ תיעדוף מהקריטי ביותר ולמשני, יש להבין את כל אלו על מנת ליצור מערך אחראי של ניהול סיכונים.

- ממשל (Governance)

מדיניות נהלים ודרישות רגולטוריות ומשפטיות של הממשלה להגנה מפני תקיפות סייבר על ארגון, דרישות רגולטוריות ואישורים שהממשלה מציגה כחובה או כהמלצה כהגנה מפני תקיפות סייבר על ארגון.

- הערכת סיכונים (Risk Assessment)

הבנה של הסיכונים המוצבים בפני ארגון בכל מה שקשור לאבטחת מידע ארגונית, מה הסיכונים שיש לקחת מחשבון , אם זה תדמית מוניטין או נכסים ארגוניים שעלולים להיפגע בעקבות תקיפה.

- אסטרטגיית ניהול סיכונים (Risk Management Strategy)

זיהוי הערכה וניהול סיכונים, בניית תהליך לעדכון ובדיקה קבועה של סיכונים שארגון ניצב בפניהם. פעולה זו נעשית על-ידי פיתוחים חדשים ופעולות-מנע המגנות על ארגון מתקיפת סייבר.

- Protect

- בקרת גישה (Access Control) -

ניהול, אימות ובקרת גישה, ניהול הגישה למשתמשים ולמתקני הארגון באמצעות סיווג משתמש. פעולה זו נעשית על מנת לאפשר גישה למשתמשים לאזורים מותרים בלבד, תוך אימות אותו משתמש בזמן ההתחברות.

- מודעות והכשרה (Awareness and Training)

הכשרת אנשי הארגון למודעות אבטחת מידע, הכשרות בנושא אבטחת מידע והדרכות למקרים שיכולים לקרות. בהכשרות אלה מתבצע אימון המשתמשים על-ידי ביצוע תרגולים פנימיים של הארגון. התרגולים ידעו להתמודד עם פגיעה פיזית- בן אדם ששמנסה להיכנס לארגון ללא היתר, וגם עם פגיעה דיגיטלית- לדוגמה, מקרה של שליחת אימיילים של פישינג. במקרה כזה, אנשי הארגון ידעו לבדוק מה אחוז ה"נופלים בפח" בקרב המשתמשים.

- אבטחת נתונים (Data Security)

כל המידע ונתונים של הארגון מנוהלים בהתאם לאסטרטגיית הסיכון של הארגון כדי להגן על סודיות, שלמות וזמינות המידע ולמנוע דלף מידע בארגון.

- תהליכי ונהלי הגנת מידע (Information Protection Processes and Procedures)

מדיניות אבטחה (המתייחסת למטרה, היקף, תפקידים, אחריות, מחויבות ניהול ותיאום בין גופים ארגוניים), תהליכים ונהלים נשמרים ומשמשים לניהול הגנה על מערכות מידע ונכסים.

- טכנולוגיות הגנה (Protective Technology)

עדכון טכנולוגיות ופתרונות הגנת המידע מנועלים ומעודכנים ע"פ פרסומים אחרונים על מנת להבטיח הגנה וחוסן של מערכות ונכסים בארגון.

- Detect

- אנומליות ואירועים (Anomalies and Events)

זיהוי, חקירה וניתור של פעילות חריגה בארגון והכרת ההשפעה האפשרית של אותם אירועים. פעולה זו מתבצעת באמצעות חקירה לאורך זמן של פעולות הארגון ובפרט פעולות חריגות, וכן זיהוי פעילות חריגה ע"י חוקים, למשל משתמש שטועה בסיסמא שלו מעל 3 פעמים.

- ניטור אבטחה רציף (Security Continuous Monitoring)

מערכות המידע והנכסים מנוטרים תמידית על מנת לזהות אירועי אבטחת מידע ולאמת את יעילות אמצעי ההגנה בארגון- כמות המשתמשים המחוברים לארגון לא חריגה, מספר ניסיונות ההתחברות לא חריג ועוד.

- תהליכי גילוי (Detection Processes)

תהליכי ונהלי הגילוי מעודכנים ונשמרים על-ידי משתמשי הארגון , על מנת לאפשר זיהוי וגילוי של אירועים חריגים בארגון במהירות וביעילות.

- Respond

תכנון תגובה (Response Planning)

תכנון נהלי תגובה למקרים, מה צריך לעשות בכל זיהוי של מקרה מסוים מרגע הזיהוי ועד לסיום האירוע ובכך להבטיח מענה נכון ומהיר לאירועי ביטחון מידע.

- תקשורת (Communications)

תקשורת מלאה ונהלים שבהם כתוב למי צריך לפנות במקרה של תקיפה או זיהוי דלף מידע, כולל תמיכה חיצונית במקרה הצורך פנייה אל גורמי אכיפת החוק.

- ניתוח נתונים (Analysis)

יש לבצע ניתוח נתונים מתמיד בארגון על מנת לזהות פעילות חריגה ולהבטיח מענה הולם ותמיכה בפעילויות התאוששות. פעולה בדרך שכזו תביא לכך שפעילות הארגון תהיה ידועה וצפויה ובכך תאפשר זיהוי של חריגות בארגון.

- הקלה (Mitigation)

ביצוע פעולות על מנת למנוע התרחבות של אירוע, להקל על השפעותיו ולפתור את האירוע במהירות וביעילות.

- שיפורים (Improvements)

שיפור כל התהליכים וההגנות במקרה של אירוע, הבנה מדויקת של ההתרחשות וקבלת כלים לפעולות אופרטיביות שימנעו אירוע דומה בעתיד. כחלק מתהליך השיפורים, מתכוננים גם לדרך תגובה נכונה יותר במקרה שמתרחש אירוע חוזר.

- Recover

- תכנון השחזור (Recovery Planning)

יש לבצע תכנון נהלי שחזור מידע במקרה של אירוע, נהלים אלו חייבים להיות מתוחזקים ומעודכנים על מנת להבטיח שיקום מהיר ככל שניתן של מערכות או נכסים המושפעים מאותו אירוע בטחון מידע.

- שיפור (Improvement)

יש לבצע הסקת מסקנות אחרי אירוע ובכך לשפר את כל תהליכי ההתאוששות, ובכך לאפשר תגובה והתאוששות מהירות יותר במקרה של אירוע דומה בעתיד.

- תקשורת (Communication)

פנייה במידת הצורך לארגונים חיצוניים על מנת להיעזר בשירותים והמידע שלהם על מנת לבצע תכנון וביצוע יסודי של שחזור המידע שנפגע.

ארכיטקטורת NIST CSF

ארכיטקטורת NIST CSF באה לתת שפה משותפת והבנה איך ליצור מערך הגנה פנימי בד בבד מערך חיצוני. מודל זה משמש כעזר לזיהוי ולתעדוף פעולות מסוימות על מנת להפחית כמה שיותר פגיעה בביטחון מידע ודלף מידע של ארגון. המטרה העיקרית היא לאפשר לארגונים הגנה מפני תקיפות סייבר ע"י קווים מנחים. ארגון יכול להשתמש במודל לזיהוי הערכה וניהול של סיכוני אבטחת מידע .

השלב הראשון בארכיטקטורה זו הוא תעדוף והיקף. על הארגון לזהות מה הם נכסי הארגון לפי חשיבות, ולהעריך את רמת החשיבות של כל נכס, ואת רמת הפגיעות שלו. מה הם שרתי המידע, שרתי DB , איפה מאחסנים את כל המידע על הלקוחות, עובדים או כל מידע שאפשר לנצל לרעה ויכול לפגוע בכך בארגון- איזה ציוד מחשוב עלול להיפגע ולפגוע ברצף העבודה של הארגון. הזיהוי מתבצע לפי חשיבות הנכס וכמה הוא יכול לסבול מפגיעה. לאחר מכן ננסה להעריך אילו סיכונים ניצבים מולנו ואיזה נכס יותר או פחות חשוף אליהם , ואז נתכנן אסטרטגיית פעולה למקרה שבו הרשת שלנו נפגעת.

בנוסף, עלינו לתעדף גם את המשתמשים שלנו. בתוך כך, נייצר מערך של בקרת גישה שיגביל את כניסת המשתמשים וימנע מהם להיכנס לאזורים אסורים. נבצע השתלמויות ובדיקות למשתמשים שלנו בנושא ביטחון מידע, נלמד אותם איך להגן על המידע ולא להיות חשופים לסכנות. בד-בבד נבנה מערך הגנתי שמטרתו היא להגן גם במידה שמשתמש ביצע בטעות או בזדון פעילות שיכולה לגרום לדלף מידע.

לאחר מכן נרצה להבין איך אנחנו יכולים לזהות פעילות זדונית או לא מכוונת. פעולה זו נעשית באמצעות ביצוע ניטור וסריקה ברשת אחר מקרים או אירועים חריגים שלא אמורים לקרות ברשת שלנו. בשלב הבא ובשלב הראשון הצעד הבא שלנו הוא לראות שהמערך האסטרטגי שלנו מוכן לכל תרחיש- למי מדווחים, איזה רשת מנתקים ומה סדר הפעולות. כמובן שלאחר כל אירוע נתחקר ונציע שיפורים על מנת לנסות למנוע אירוע נוסף בעתיד.

לסיכום, ניתן לומר שכל ארגון פגיע לתקיפות מסוגים שונים כל הזמן, ואף אחד לא חסין. אם כן, מטרת הארגון צריכה להיות בראש ובראשונה לשמור על יציבות ביטחונית שתביא לצמצום התקיפות. לצד זאת, גם במקרה של פגיעה, השאיפה המתמדת צריכה להיות לחזור לפעילות מלאה תוך צמצום הפגיעות ומיגורן. שימוש בשני המודלים שהצגתי יכול לסייע בכך.

ביבליוגרפיה

"What is a Zero Trust Architecture?". In:

https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

5 Key Changes Made to the NIST Cybersecurity Framework V1.1. In:

https://www.givainc.com/blog/index.cfm/2019/7/24/5-key-changes-made-to-the-nist-cybersecurity-framework-v11

מתוך האתר הממשלתי ל- Nist CSF. נדלה בתאריך 15.10.2021. זמין בקישור:
https://www.nist.gov/cyberframework

מתוך האתר הממשלתי ל- zero Trust. נדלה בתאריך 15.10.2021. זמין בקישור

https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_418_A4.pdf