אלי יצחקוב, סמנכ"ל שרשרת האספקה בקבוצת טבת שירותים לוגיסטיים
אלון משה, מנהל ההנדסה ואבטחת המידע בקבוצת טבת שירותים לוגיסטיים

אלון משה

אבטחת מידע על-פי תקן ISO 27001

אבטחת המידע (אב"מ) על-פי התקן לעיל באה להגן על מידע ארגוני חיוני, והגדרתה כוללת את חיסיון המידע, את שלמותו של המידע ואת זמינותו

בשנים האחרונות, ההכרה בחשיבות אבטחת המידע גוברת מאוד, וארגונים מובילים בארץ ובעולם מאמצים את התקן למערכת ניהול אבטחת מידע - ISO 27001. התקן מגדיר את העקרונות לתכנון מערכת ניהול אבטחת מידע (מנא"מ)*, להקמתה, לניהולה, לתחזוקתה, לבקרתה, ולשיפורה המתמיד. יישום התקן הוא הוכחה, שהארגון נוקט את האמצעים המתאימים לשמור על המידע, לנהלו ביעילות, ולהגן עליו על-פי מודל שיטתי, ועל-פי מפרט מקובל.

אבטחת המידע (אב"מ) על-פי התקן לעיל באה להגן על מידע ארגוני חיוני, והגדרתה כוללת את חיסיון המידע, את שלמותו של המידע ואת זמינותו (Confidentiality, Integrity and Availability) [CIA]. קרי, שמירה על מידע רגיש, כדי שלא ייחשף לגורמים לא מורשים; שמירה על המידע מפני שינוי, או שיבוש; והבטחת האפשרות, שהמידע יעמוד בעת הצורך לרשות המשתמשים המורשים.

נכסי המידע (Information assets) של הארגון הם: בסיסי נתונים (קבצים ומסמכים), מיקום מידע, תוכנה, חומרה, תהליכים, תשתיות, מערכות תמיכה, כוח-אדם, וכו'. התקן מבחין בין בעל המידע (האחראי על נכס המידע, על-פי דין) לבין מחזיק המידע. בעל המידע אחראי להגדרת רמת החיסיון הנדרשת ולוודא, כי ההגנה על המידע תואמת את דרישותיו. לעומתו, מחזיק המידע אחראי לזיהוי הסיכונים באבטחת המידע, לנתחם ולנהלם; לנהל את ההגנה לעיל; ולדווח לבעל המידע על כל אירוע חריג, העלול להזיק למידע.

תקני מנא"מ ותקן ISO 27001

סדרת תקני מנא"מ (ISO 27000) כוללת: תקן ISO 27001, המכיל את הדרישות למנא"מ; תקן ISO 27002, המכיל את קובץ הכללים לניהול אב"מ; תקן ISO 27003, המכיל את ההנחיות ליישום מנא"מ; תקן ISO 27004, המכיל את ההנחיות למדידת ניהול אב"מ; תקן ISO 27005, המכיל את ההנחיות לניהול סיכוני אב"מ; ועוד. נוסף על-כך, הסדרה כוללת מדריכים ייעודיים, כגון: אב"מ ברשומות רפואיות (ISO 27799), בתחום הסייבר (ISO 27032), וכו'.

תקן ISO 27001 הוא תקן תהליכי/מערכתי, המבוסס על מתודולוגיה ניהולית לשיפור מתמיד. המתודולוגיה מבוססת על תהליך מחזורי, הכולל את ארבעת השלבים הבאים: תכנן-בצע-בדוק-שפר (Plan-Do-Check-Act) [PDCA]**. התקן כולל: מבוא, תכולה, אזכורים, מונחים והגדרות (פרקים 0-3), ותהליך להקמת מנא"מ ולשיפורה המתמיד, על-פי המתודולוגיה לעיל (פרקים 4-10).

להלן שלבי התהליך על-פי תקן ISO 27001:

- שלב ה-Plan (פרקים 4-7): ההקשר של הארגון (Context of the organization), מנהיגות (Leadership), תכנון (Planning), ותמיכה (Support).
- שלב ה-Do (פרק 8): תפעול (Operation).
- שלב ה-Check (פרק 9): הערכת ביצועים (Performance evaluation).
- שלב ה-Act (פרק 10): שיפור (Improvement).

נוסף לעיל, התקן כולל נספחים, שהעיקרי בהם (נספח A) כולל את מטרות הבקרה של המנא"מ ואת אמצעי בקרה זאת.

להלן פירוט הסעיפים בנספח: (A5): מדיניות אבטחה, (A6): ארגון, (A7): אבטחת משאבי-אנוש, (A8): ניהול נכסים, (A9): בקרת גישה, (A10): הצפנה, (A11): אבטחה פיזית וסביבתית, (A12): בקרות התפעול, (A13): בקרות התקשורת, (A14): רכש מערכות, פיתוחן ותחזוקתן, (A15): יחסי גומלין עם ספקים, (A16): ניהול אירועי אב"מ, (A17): היבטי אב"מ בניהול המשכיות עסקית, (A18): התאמה.

הקמת המנא"מ בארגון

הקמת המנא"מ היא תהליך מובנה, שמטרתו ליצור מערכת אב"מ אפקטיבית להגנה על נכסי המידע, ויעילה

* המונח הלועזי של מערכת ניהול אבטחת מידע (מנא"מ) הוא: Information Security Management System (ISMS).

** המונח מוכר גם כמחזור דמינג (Deming cycle) וכמחזור שיוהרט (Shewhart cycle).

(המשך בעמ' 62)

עוצמת האיגוד היא עוצמת החברים בו

האיגוד הישראלי לניהול שרשרת האספקה ISCMA- הינו האיגוד המקצועי המוביל באיכותו בישראל, פועל זו השנה ה-16, חברים בו מאות (למעלה מ830) מנהלים בכירים ממאות ארגונים מובילים במשק,
ממגוון התעשיות, להשבחה ולקידום תחום "ניהול שרשרת האספקה בישראל" עם דגש על:

- קידום התחום - מקצועית, ארגונית, אישית וציבורית: השבחה מקצועית של העוסקים בתחום, קידום המעמד המקצועי בארגון ובכלל, לובינג -להוות כוח איכות והשפעה בעשייה ציבורית.
- מפגשים לחילופי ידע, למידה מקצועית מניסיונם של ארגונים המובילים במשק, ארגונים ישראליים, ארגונים גלובליים חובקי עולם, למידה ושיתוף אסטרטגית וטכנולוגית.
- גישה לגלובליזציה - מפגש עם שרשרות אספקה גלובליות מורכבות.
- מפגש עם מנהלים בכירים בתחום, מקבלי ההחלטות בניהול שרשרת האספקה מהתעשיות השונות
- ייזום, פיתוח תכניות מקצועיות, פיתוח מיומנויות, ידע וביצוע בהתאם
- שיתוף באתר ידע של האיגוד: www.adar-yoz.net
- ניוזלטר מקצועי: "ניהול שרשרת האספקה Online" המופץ ללמעלה מ13000 קוראים בכל זירת שרשרת האספקה.
- ירחון של האיגוד: "מי ומה בשרשרת האספקה" - הירחון וכתב העת
- השמת כוח אדם מקצועי בכיר ודרג ניהול ביניים בתחומי: ניהול שרשרת האספקה, תפעול, רכש, לוגיסטיקה, תכנון ועוד.
- חברי האיגוד מוכנים להשקיע מזמנם, ניסיונם ויכולתם המקצועית ולהתחייב בכדי לקדם את מטרות האיגוד.

ISCMA
Israeli Supply Chain Management Association

- 12/1/16 - מפגש פורום הפצה עירונית-CityLogistics- בעירית תל אביב
- 29/2/16 - כנס רכש מקצועי ייחודי: "Show me the Money" הרכש כמייצר כסף לארגון
- 8/3/16 - מפגש 2 של פורום אקדמיה- תעשייה במכללת רופין
- 15/3/16 - כנס בנושא: 'חדשנות בלוגיסטיקה וניהול שרשרת האספקה' במרכז הכנסים קריפטון הכפר הירוק
- 3/16 - מפגש וועדות: רכש, לוגיסטיקה, Planning
- 28/3/16 - מפגש פורום בכירים- סמנכ"לי שרשרת אספקה ISCMA בתעשייה האווירית
- 5/4/16 - מפגש פורום- ISPL- הרכש האסטרטגי בטמבור
- 12/4/16 - השתתפות בכנס השנתי של הפקולטה לתעשייה וניהול - מכללת רופין- מושב בניהול והרצאות של חברי האיגוד הישראלי ניהול שרשרת האספקה ISCMA בנושא: "חדשנות ואתגרים בניהול שרשרת האספקה"
- 13/4/16 - כנס מקצועי למנהלים:Balance your supply chain Priorities, במרכז הכנסים קריפטון הכפר הירוק
- 6/6/16 - הפסגה הבינלאומית ה-16 לניהול שרשרת האספקה, מרכז הכנסים Avenue קרית שדה התעופה
- 20/6/16 - מפגש וועדת Planning באסם בהנחיית חיים שפיר- בנושא: "ניהול סיכונים מול ניהול תחזית"
- 7/16 - מפגש וועדות: רכש, לוגיסטיקה, Planning
- 7/7/16 - מפגש מקצועי וסיור במרלו"ג שטראוס החדש בשוהם- באירוח: משה ריעני, סמנכ"ל שרשרת אספקה, שטראוס
- 26/10/16 -סיור מקצועי בקרית ההדרכה- עיר הבהד"ים- צה"ל אט"ל
- 9/16 - מפגש פורום בכירים - סמנכ"לי שרשרת אספקה ISCMA
- 22/11/16 -הכנס השנתי ה-3 ל'לוגיסטיקה חכמה- הלוגיקה מאחורי הלוגיסטיקה

לפרטים, להצטרפות, לכל בקשה ושאלה אנו לרשותכם-
האיגוד הישראלי לניהול שרשרת האספקה ISCMA
navit@adar-yoz.net / 03-9702990

ISCMA
Israeli Supply Chain Management Association

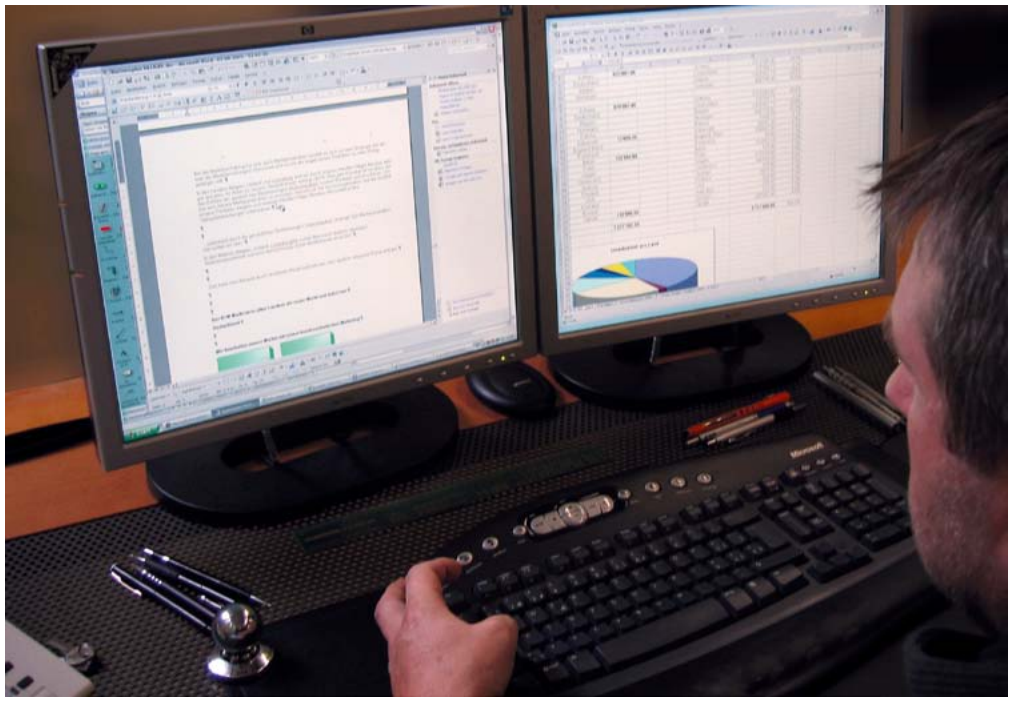
(המשך מעמ' 60)

במבחן של עלות-תועלת.

להלן שלבי התהליך של הקמת המנא"מ:

1. **ניהול תמיכת ההנהלה (Get Management Support):** קיום פגישת הנהלה, כדי לקבל החלטה רשמית על הקמת המנא"מ, להשיג את אחריות ההנהלה ואת מעורבותה בתהליך; בחירת ועדת היגוי; הגדרת מטרות אב"מ, עקרונות, משימות עיקריות ואופק זמן; קביעת בעלי תפקיד במנא"מ, קביעת אחריותם וסמכותם; וכו'.
2. **הגדרת תכולת המנא"מ (Define ISMS scope):** הגדרת ההקשר של הארגון, הגדרתם של הצרכים ושל דרישות בעלי העניין (רגולטורים, בעלי מניות, הנהלה, שותפים עסקיים, לקוחות, וכו'), הגדרת תחום המנא"מ, וכו'.
3. **מיפוי נכסי המידע של הארגון (Inventory information assets),** כגון: אתרים פיזיים, מידע דיגיטלי, חומרה, תוכנה, תקשורת, תהליכים וכו'. המיפוי כולל את הרכיבים הבאים: תיאור הנכס; הבעלים; מחזיק הנכס; רמת החיסיון הנדרשת; קריטיות בהיבטי שלמות, זמינות ושרידות; פוטנציאל הסיכון; וכו'.
4. **ביצוע סקרי סיכונים (Conduct information security risk assessment):** קביעת תהליך מובנה לסקירת סיכונים ולהערכתם; הגדרת קריטריונים לרמות סיכון קבילות; קביעת תכנית לסקר סיכונים; ביצוע סקרי סיכונים, זיהוי הסיכונים והערכתם; קביעת הגורם האחראי לניהול הסיכון ("בעל הסיכון"); וכו'.
5. **הכנת מסמך ישימות (Prepare statement of applicability) ותכנית לטיפול בסיכונים (Prepare risk treatment plan):** הגדרת מטרות בקרת המנא"מ ואמצעי הבקרה, החלטות על טיפול בסיכונים, הכנת תכנית לטיפול בהם, קבלת אישור מבעלי הסיכון על התכנית ועל הנכונות לקבל את הסיכונים השיוריים, וכו'.
6. **פיתוח תכנית ליישום המנא"מ (Develop ISMS implementation program):** הכנת תכניות מפורטות בכל תחומי המנא"מ, הכוללות: גורמים אחראים, משימות, משאבים, לוחות-זמנים, וכו'.
7. **יישום תכנית המנא"מ (ISMS implementation program):** הקצאת המשאבים הדרושים והמתאימים ליישום התכנית (כמות, כישורים, מודעות, וכו'), וביצוע הפרויקטים הנדרשים ליישום התכנית.
8. **בניית המנא"מ (ISMS),** ובכלל זה: מדיניות, נהלים, הוראות, טפסים, יומני תיעוד, יצירת מודעות, הדרכה, מבדקי אפקטיביות, מבדקי התאמה, וכו'.
9. **תפעול המנא"מ (ISMS operation artifacts):** יישום המנא"מ ובקרה תדירה על ביצועיה. כולל: עמידה ביעדים, תיעוד, התאמה לתהליכים מתוכננים, בקרת שינויים, בקרת תהליכי מיקור-חוץ, ניהול אירועים, פעילויות הדרכה ויצירת מודעות, וכו'.
10. **סקירת התאמה (Compliance review):** ביצוע סקרי התאמה על-פי רשימות תיוג (Check lists). הסקרים מוודאים את התאמת המנא"מ לדרישות המוגדרות, והם מפרטים את אי-ההתאמות. סיבות אפשריות לאי-התאמה: אי-התאמה לתקן, אי-התאמה למדיניות/לנוהל, או אי-התאמה ביישום הנוהל. נוסף על-כך, הסקרים מאפשרים לזהות הזדמנויות לשיפור.
11. **פעולות לביצוע התאמה (Corrective actions):** ביצוע פעולות מיידיות לתיקון אי-ההתאמה, זיהוי סיבות השורש של אי-ההתאמה וחקירתן לעומק, ביצוע פעולות מתקנות למניעת הישנות אי-ההתאמה, ובדיקת אפקטיביות הפעולה המתקנת. אם צריך, גם לקיים ביצוע חוזר של התהליך עד להבטחת ההתאמה המלאה.
12. **הערכה מקדימה למבדק ההסמכה (Pre-certification assessment):** ההערכה מוודאת את התאמת המנא"מ לדרישות התקן ומאתרת את הפערים ביניהן. זאת, לקראת מבדק ההסמכה החיצוני. הדו"ח המסכם של הערכה זאת כולל דרישות לביצוע התאמות, הנדרשות על-פי התקן.
13. **מבדק ההסמכה (Certification audit):** המבדק

> הקמת המנא"מ היא תהליך מובנה, שמטרתו ליצור מערכת אב"מ אפקטיבית להגנה על נכסי המידע, ויעילה במבחן של עלות-תועלת



בוחן את התאמת המנא"מ לדרישות התקן. המבדק מתבצע באמצעות גורם התעדה מוכר, כגון מכון התקנים הישראלי (מת"י). אם הארגון עומד בדרישות התקן, הוא זכאי לקבל תעודה, המעידה על תאימות המנא"מ לדרישות.

14. **מבדקי מעקב לבדיקת התאמת הארגון לדרישות התקן:** קבלת ההסמכה היא רק תחילת הדרך. נדרש לתפעל את המנא"מ ולהשקיע מאמץ מתמיד לשיפורה. המעקב על ביצועי המנא"מ ועל התאמתה לדרישות מתבצע דרך סקרי הנהלה, ומבדקים פנימיים וחיצוניים.

אבטחת המידע בארגון

אחד מעמודי התווך החשובים באב"מ הוא עצמאותו של האחראי לנושא בארגון. ברוב הארגונים, בעל התפקיד הוא מנהל אבטחת המידע הארגוני (Chief Information Security Officer) [CISO], המדווח ישירות למנכ"ל, לסמנכ"ל בכיר, או לקב"ט, וסמכויותיו נגזרות מוועדת ההיגוי.

אחריות המנהל כוללת: קביעת מדיניות אב"מ בארגון, סיווג המידע על-פי רמת הקריטיות בארגון, הערכת הסיכונים וניהולם, העלאת המודעות לאב"מ בארגון, הדרכות בנושא האב"מ, התאמת המנא"מ לדרישות רגולטוריות ולמדיניות ההנהלה, ליווי פרויקטים של הטמעת טכנולוגיות חדשות ושל שדרוג טכנולוגיות קיימות בהיבטי אב"מ, שיתוף פעולה עם הקב"ט, שיתוף ההנהלה בתכניות להבטחת ההמשכיות העסקית, וכו'.

ה-CISO מתמודד עם איומים חיצוניים (גורמים עוינים, מתחרים עסקיים, וכו') ופנימיים (משתמשים במערכות התקשוב), העלולים לפגוע בנכסי המידע של הארגון. ההתגוננות מאיומים אלה כוללת שלושה היבטים: טכנולוגיה, תהליכים ומשתמשים.

להלן דוגמאות לגורמי סיכון בהיבטים אלה:

- טכנולוגיה: טעויות בכתיבת אפליקציה או בבדיקתה; עדכוני מערכת הפעלה, שאינם מספקים הגנה מלאה; הגנה חלקית מתוכנות זדוניות (מערכות התגוננות לא עדכניות); וכו'.
- תהליכים: הגדרות לא נכונות של תהליכים עסקיים; פרצות ונקודות תורפה בתהליכים עסקיים; שימוש בשרתים שאינם מוקשחים; טבלאות משותפות לתהליכים שונים, שיש צורך להפריד ביניהן; פרופילי הרשאות לא מעודכנים; וכו'.
- משתמשים: תמימות המשתמש (קורבן לשימוש בזהות גנובה), סקרנות (כניסה למאגרי מידע ללא היתר), זדון (מעילות והונאות), חוסר מודעות (אי-הקפדה על הנחיות), טעויות אנוש (אי-תשומת לב), וכו'.

טיפול מיטבי באיומי אב"מ מחייב גישת אבטחה פרואקטיבית (משפיעה באמצעות יוזמה), הכוללת את מעגלי האבטחה הבאים:

1. **מניעה:** מודעות אצל עובדי הארגון וקידום ההרתעה.
2. **גילוי:** זיהוי האיום, פענוח חיוויים והתרעות על האיום.
3. **הגנה:** מיגון הקשחות ואמצעי התגוננות מתוכנות מזיקות.
4. **תגובה:** ניהול אפקטיבי של אירועי אבטחה, וביצוע פעולות חיוניות להקטנת נזקים.
5. **תיקון הנזקים:** החזרת המצב התקין, וביצוע פעולות להבטחת ההמשכיות העסקית.

בדיקת המנא"מ והערכתה

בדיקת המנא"מ באה לקבוע את התאמתה לדרישות התקן, לבחון את אפקטיביות המנא"מ, ולזהות הזדמנויות לשיפור. הבדיקה כוללת מבדקים (חיצוניים ופנימיים), הנערכים על-פי קווים מנחים לעריכת מבדקים במערכות ניהול (ת"י ISO 19011). הבדיקה מתבצעת על-פי תכנית מבדקים תקופתית, המפרטת את מטרותיו של כל מבדק, היקפו, מועדו, איזו יחידה ארגונית נבדקת, מה הם הנושאים המוגדרים לבדיקה, וכו'.

הערכת המנא"מ אפשרית על-פי כמה מודלים, ולדוגמה:

- סיווג רמת הבגרות/הבשלות של המנא"מ, על-פי מודל להערכת התהליכים בארגון (Capability Maturity Model Integration) [CMMI]***, ולדוגמה:
  - רמה 1: ניהול "אד-הוק" (תגובתיות ו"כיבוי שריפות" במקום תכנון מראש).
  - רמה 2: קיימת תבנית לניהול חלק מן התהליכים בארגון.
  - רמה 3: התהליכים הארגוניים מוגדרים, מתועדים ומתוקשרים לגורמים הרלוונטיים.
  - רמה 4: התהליכים מנוטרים, נמדדים ומנוהלים כמותית.
  - רמה 5: התהליכים מנוהלים בצורה מיטבית, והפעילות מתמקדת בשיפור מתמיד.
- סיווג רמת ההתאמה של המנא"מ, על-פי מודל של ציון משוקלל במבדק, ולדוגמה:
  - סיווג ראוי לציון (Notable): הציון המשוקלל הוא בטווח של 0-5 נקודות שליליות;
  - סיווג קביל (Acceptable): הציון המשוקלל הוא בטווח של 6-14 נקודות שליליות;
  - סיווג לא קביל (Unacceptable): הציון המשוקלל הוא 15 נקודות שליליות ויותר.

הניקוד ניתן על-פי המפתח הבא: אי-התאמה קריטית (Critical Observation): 4 נקודות שליליות, אי-התאמה משמעותית (Major Observation): 2 נקודות שליליות, ואי-התאמה קלה (Minor Observation): נקודה שלילית אחת.

לדוגמה: אם במבדק נמצאו 2 אי-התאמות משמעותיות ו-5 אי-התאמות קלות (סה"כ: 9 נקודות שליליות), הרי סיווג רמת ההתאמה של המנא"מ הוא קביל.

לסיכום, בעידן המודרני, המידע הוא אחד מן המשאבים החשובים של הארגון, שנדרש להגן עליו, כדי למנוע נזק אפשרי ולהבטיח את ההמשכיות העסקית לטווח-ארוך. לכן, הקמת המנא"מ על-פי תקן ISO 27001 היא כלי אפקטיבי ויעיל למימוש הגנה זו. ■

> ה-CISO מתמודד עם איומים חיצוניים (גורמים עוינים, מתחרים עסקיים, וכו') ופנימיים (משתמשים במערכות התקשוב), העלולים לפגוע בנכסי המידע של הארגון

*** המודל פותח באוניברסיטת קארנגי-מלון (Carnegie Mellon), המחזיקה בסימן רשום עליו, והיא אף רשמה פטנט עליו.