המשרד להגנת הסביבה
الوزارة لحماية البيئة
Israel Ministry of Environmental Protection

סייבר בתעשייה
המשרד להגנת הסביבה

הגנת מערכות ERP המשמשות לניהול חומרים מסוכנים

המשרד להגנת הסביבה
אגף חירום וסייבר, יחידת הסייבר בתעשייה

1. מבוא

מערכות ERP מנהלות מידע חשוב בארגונים רבים (מלאי, לקוחות, תהליכי מכירה, תהליכי ייצור, שירות לקוחות, חשבונאות ועוד) ולפיכך מהוות יעד מרכזי לתקיפה על ידי תוקפי סייבר הפועלים ממגוון מניעים – גניבת כספים על ידי שינויים בתהליכי החשבונאות, הפעלת נוזקת כופר על מערכות קריטיות, שיבוש תהליכי הארגון ממטרות לאומניות של פגיעה בכלכלת ישראל, מרצון לקצור תהילה בקהילת ההאקרים או ממניעים נוספים.

שיבוש רישומי מידע או תהליכים הנוגעים לחומרים מסוכנים (חומ"ס) עלול לגרום למספר רב של סכנות – אפשרות גניבה של חומ"ס או שליחתו לגורמים לא מורשים, שיבוש תהליכי ייצור ומתכונים באופן שיגרום לריאקציות מסוכנות ועוד.

מערך הסייבר הלאומי פרסם המלצות לנושא הגנת סייבר במערכות ERP ומומלץ לעיין בהן וליישמן.

מסמך זה מוסיף דגשים להגנת מערכות ERP אשר משמשות לניהול חומרים מסוכנים (פנקס הרעלים של הארגון), ניהול נתוני ייצור (כגון מתכונים) ו/או אשר בוצעה להם אינטגרציה מסוימת למערכות הייצור השולטות על או מבקרות חומרים מסוכנים, על מנת לעמוד בדרישות המשרד להגנת הסביבה הניתנות כתנאי בהיתר הרעלים, לרבות דרישות הגנת הסייבר המפורסמות במדריך הסייבר באתר המשרד להגנת הסביבה.

2. מיפוי תהליכים ומודולים

א) יש למפות את התהליכים בארגון הנוגעים לרישום תנועות חומ"ס / עדכון צריכה / שינוי מלאי החומ"ס של הארגון (פנקס הרעלים).

- מי נותני ההוראות.
- מי מבצעי השינויים במערכות המחשוב.
- באילו מסכים/מודולים של ה-ERP הם עושים זאת.

ניהול גרסאות

גרסה	כתב	אישר	מהות השינוי	תאריך
1.0	יוסי שביט ר' יחידת הסייבר בתעשייה	גלעד בן ארי ר' אגף חירום וסייבר	כתיבת המסמך	15.11.2020

- אילו מנגנונים קיימים בארגון למניעת טעויות הזנה (אישורי מנהל, השוואה מול רישום נייר, ביקורות תקופתיות של המלאי).
- אילו מנגנוני גיבוי מיושמים לנתונים אלה (בין אם באתר או בענן) למקרה של תקלה, שיבוש או מחיקה בזדון.

ב) במידה והארגון מוכר או מעביר חומ"ס הלאה לארגון אחר (לקוחות, מחסן לוגיסטי, מתקן לטיפול בפסולות וכו') יש למפות:

- כיצד ובאחריות מי מעודכנים נתוני הלקוח/הארגון המקבל חומ"ס.
- באילו מסכים/מודולים של ה-ERP עושים זאת.
- אילו מנגנונים קיימים בארגון למניעת טעויות במשלוח חומ"ס (למשל טעות הקלדה בכמויות, טעות בסימון החומרים או משלוח ללקוח שאין לו היתר רעלים).

ג) במידה ומערכת ה-ERP מנהלת גם מידע ייצור הקשור לחומרים מסוכנים כגון תכנון תהליכי ייצור ממוחשבים או מתכונים למוצרים יש למפות:

- למי יש גישה יום-יומית לצפייה/הפעלה.
- כיצד ובאחריות מי מבוצעים שינויים בתכנון הייצור/המתכונים במערכת.
- באילו מסכים/מודולים של ה-ERP עושים זאת.
- אילו מנגנונים קיימים בארגון למניעת טעויות - בדיקה/אישור תצורה או מתכון.
- אילו מנגנוני גיבוי מיושמים לנתונים אלה (בין אם באתר או בענן) למקרה של תקלה, שיבוש או מחיקה בזדון.

ד) במידה ול-ERP ישנם ממשקים של ייצוא/ייבוא נתונים אל מערכות מידע חיצוניות (אתר אינטרנט, פורטל ספקים/לקוחות וכו') יש למפותם:

- הנתונים המועברים והאם כוללים נתונים הקשורים לחומ"ס.

ניהול גרסאות

גרסה	כתב	אישר	מהות השינוי	תאריך
1.0	יוסי שביט ר' יחידת הסייבר בתעשייה	גלעד בן ארי ר' אגף חירום וסייבר	כתיבת המסמך	15.11.2020

- באיזה פורמט/פרוטוקול, באיזה חיבור רשת או אופן העברת קבצים.
- עם אילו הרשאות ניגשות המערכות החיצוניות לנתונים במערכת ה-ERP.
- אילו מנגנונים קיימים למניעת טעויות במידע המתקבל למערכת.

ה) במידה ובוצעה אינטגרציה של ה-ERP אל מערכות הייצור יש למפות את האינטגרציה שבוצעה:

- הנתונים המועברים.
- פקודות להפעלת תהליכי ייצור.
- באיזה פורמט/פרוטוקול, באיזה חיבור רשת או אופן העברת קבצים.
- מי נותני ההוראות להפעלת תהליכי ייצור או מעבירים נתונים לייצור ממערכת ה-ERP.
- באילו מסכים/מודולים של ה-ERP עושים זאת.
- אילו מנגנונים קיימים בארגון למניעת תקלות (הפעלת תהליך ייצור בשגגה או כשמצב המכונות אינו נכון, וידוא הנתונים המתקבלים מה-ERP בייצור)

3. <u>המלצות להגנת מערכת ה-ERP</u>

א) <u>הרשאות</u>

- יש לוודא כי המערכת אוכפת הרשאות צפייה בנתונים הקשורים לחומרים מסוכנים למי שנדרש לכך על פי פרופיל תפקידו (מנהל ייצור, איש רכש), מי שתפקידו אינו מצריך גישה – עדיף שתמנע ממנו אף הגישה למודולים או המסכים הקשורים לחומרים מסוכנים.
- יש לוודא כי המערכת אוכפת הרשאות הפעלת תהליכים / דיווח צריכת חומ"ס / העברת נתונים לייצור / קבלת נתונים ממקורות חיצוניים למי שהוסמך לכך באופן אישי.
- יש לוודא כי היכולת לשנות מלאי חומ"ס (פנקס רעלים), סימוני חומ"ס, עדכון לקוחות מקבלי חומ"ס, שינוי מתכונים או תהליכי ייצור מוגדרת לאחראי הרעלים של הארגון בלבד.

- יש לתקף את רשימת בעלי ההרשאות לפעולה/שינוי בתדירות רבעונית, ולהסיר עובדים שעזבו, עברו תפקיד וכדומה.

ב) <u>אכיפת תהליכי מניעת טעויות ותקלות</u>

- יש לוודא כי במערכת ה-ERP מיושמות אינדיקציות / חתימות / אישורים לפי העניין לתהליכי מניעת הטעויות והתקלות. למשל, אם אחראי רעלים צריך לאשר הזמנת חומ"ס של מנהל רכש, התהליך צריך להיות משוקף במערכת, לדוגמה באמצעות הקפצת חלונית אישור או משלוח התרעה לאישור ביצוע הפעולה. אם משתמש מנסה להפעיל תהליך ייצור ממערכת ה-ERP, הפקודה תתבצע רק לאחר קבלת אינדיקציית אישור למוכנות לביצוע מרצפת הייצור. אם לפני הוצאת משלוח יש תהליך וידוא זהות המקבל, כמויות החומר, סימונים, התאמה לתעודת משלוח וכו', יש לשקף זאת במערכת בתהליך מתאים.

ניהול גרסאות

גרסה	כתב	אישר	מהות השינוי	תאריך
1.0	יוסי שביט ר' יחידת הסייבר בתעשייה	גלעד בן ארי ר' אגף חירום וסייבר	כתיבת המסמך	15.11.2020

ג) <u>מעקב ותיעוד</u>

- יש לתעד נסיונות גישה למערכת ה-ERP מרחוק (מחוץ למתקן), נסיונות כושלים או לא מורשים להתחברות של משתמשים או מערכות.
- יש לתעד כל הפעולות הקשורות לחומרים מסוכנים – שינוי רמות מלאי, קבלת והוצאת משלוחים, הפעלת תהליכי ייצור, שינוי מתכונים וכו'. התיעוד יכלול זיהוי המשתמש והעמדה ממנה בוצעה הפעולה, במידה והצריכה אישורים גם את זהות המאשר.
- ניתן להטמיע מערכות אבטחת מידע המזהות אנומליות בהתנהגות משתמשים (גישה בשבת בלילה, ביצוע פעולות רבות בתוך דקה) ולתת להן גישת קריאה לתיעוד הנ"ל כדי למצוא בו גם התנהגות חריגה, במידה וקיים בעסק SOC ארגוני מומלץ לנטר את מערכת ה-ERP בצורה קפדנית.
- ניתן ליישם במערכת ה-ERP דוח היסטוריית שינויים לנושא החומרים המסוכנים שירכז את כל התיעוד הנ"ל לבדיקה תקופתית.

ד) <u>זיהוי משתמשים</u>

- מומלץ כי משתמשים בעלי הרשאות להפעלת תהליכים או ביצוע שינוי בתהליכים או בנתונים יזהו באמצעות הזדהות חזקה (MFA).
- באם משתמש מתחבר מרחוק - מומלץ ליישם כלים להצפנת החיבור, וידוא בטיחות המחשב המתחבר.

ה) <u>אינטגרציה למערכות מידע וייצור</u>

- במידה ומבוצע חיבור רשתי בין מערכת ה-ERP למערכות הייצור העושות שימוש או מסכנות חום"ס, יש להקפיד על דרישות הפרדת הרשתות וסינון הקישור כמפורט במדריך הסייבר.
- יש לתעד את הפעלת/העברת נתונים לקווי הייצור ויוזם הפעולה.

ניהול גרסאות

גרסה	כתב	אישר	מהות השינוי	תאריך
1.0	יוסי שביט ר' יחידת הסייבר בתעשייה	גלעד בן ארי ר' אגף חירום וסייבר	כתיבת המסמך	15.11.2020

- במידה ומבוצע שימוש במדיות לשם כך יש להשתמש במדיות ייעודיות, ולבצע סריקת נוזקות למדיה (הלבנה) בעת כל שימוש.

ו) <u>גיבוי</u>

- יש להגדיר תהליך גיבוי מלאי החומ"ס, התהליכים, המתכונים, והיסטוריית השינויים בהם למדיה חיצונית ייעודית או שרות מחשוב חיצוני/ענני בתדירות התואמת את קצב שימוש מכירת החומרים בארגון (שבועית, חודשית וכו').
- יש להגדיר ממונה לתהליך הגיבוי ולתרגלו בשחזור מגיבוי.

ז) <u>הקשחת שרתים, תחנות עבודה, גישה לשירותי ענן / SaaS</u>

- הקשחת שרתים מקומיים (On Premise) וענניים - יש להגדיר תצורת שרת מינימלית התומכת בהרצת האפליקציה, ומנטרלת שירותי מערכת שאינם נחוצים, מונעת חיבורי רשת שאינם נחוצים, מגדירה הרשאות ריצה מינימליות (יש לוודא שהאפליקציה אינה רצה בהרשאות מנהל מקומי או מנהל דומיין) וכו'. ראה המלצות מערך הסייבר וכן ניתן להיעזר בהמלצות יצרני מעה"פ ותשתיות האפליקציה.
- יש להגדיר וליישם תהליכי עדכון מעה"פ, תשתיות תוכנה, אפליקציה ואנטיוירוס בתדירות מינימלית של פעם ברבעון.
- יש להימנע משימוש בתוכנות השתלטות מרחוק (VNC, TeamViewer, AnyDesk, DameWare וכו') ולעשות שימוש בהתחברות טרמינל מאובטח בלבד (RDP, SSH).
- יש ליישם הגנות על עמדות הניגשות למערכת ה-ERP (PC, Thin Client), ראה המלצות מערך הסייבר.

ניהול גרסאות

גרסה	כתב	אישר	מהות השינוי	תאריך
1.0	יוסי שביט ר' יחידת הסייבר בתעשייה	גלעד בן ארי ר' אגף חירום וסייבר	כתיבת המסמך	15.11.2020