1 אוקטובר, 2024

סט תנאים למפעל המחזיק במערכות בקרה ממוחשבות

1. בכל מערכת המכילה חומרים מסוכנים ואשר מנוהלת / מבוקרת ע"י מערכות מחשוב דוגמת מערכת בקרה ממוחשבת, מערכות ERP , מערכות MES וכל מערכת ממוחשבת אחרת אשר יש לה אפשרות להשפעה על החומרים המסוכנים במפעלים ינקטו הפעולות הבאות:

1.1 במידה ומדובר במערכת בקרה תעשייתית, יש להקפיד על ערכי סף נדרשים במערכת אשר כל שינוי מהם יתוקן ע"י מערכת הבקרה ומקביל תשלח הודעה (מייל או סמס או שניהם) אל אחראי המערכת במפעל וכן יודלקו חיווי אזהרה במערכת ה-HMI (מערכת אדם מכונה) אשר מנהלת / מבקרת את מערכת הבקרה.

1.2 ערכי הסף יוגדרו עבור כל ערך שיכול להיות קריטי עבור החומרים המסוכנים שנמצאים במערכת כגון: שינוי טמפרטורה, שינוי לחצים, שינוי ספיקות, שינוי ערכי PH וכל שינוי אחר שבמידה והוא לא מבוקר עלול לגרום לארוע חומרים מסוכנים.

1.3 לכל מערכת בקרה יוגדרו ערכים רצויים וערכי סף מקסימליים ומינימליים אשר חריגה מהם תגרום לבקר להעביר פקודות תיקון למערכת . ערכי הסף יוגדרו לכל פרמטר אשר יש לו השפעה על ארוע חומ"ס (כגון טמפ, לחץ, ספיקה, רמת PH וכל ערך אחר שיכול בערכי קיצון שלו לגרום לארוע חומ"ס)

1.4 למערכות הבקרה יוגדרו ערכי סף קיצוניים (תחתון ועליון) אשר יקובעו גם בקוד הבקר וכל חריגה מהם תייצר התראה חמורה באמצעות מייל , סמס או כל דרך אחרת שתאפשר העברת הודעה מיידית אל אחראי המערכת במפעל.

1.5 מערכת הבקרה תרשום לוגים על כל התהליך באופן רציף כולל שינויי קריטיים הנעשים במערכות הבקרה, וסטיות מהערכים הרצויים ומערכי הסף

1.6 כל היסטוריית הפעילות תשמר בבסיסי נתונים למשך פרק זמן של 5 שנים תגובה בגיבוי חם ובגיבוי קר

1.7 מערכת הגיבויים תיבדק אחת לחודש ע"י ביצוע שחזורים יזומים של מידע מגובה.

2. במידה וקיימת אפשרות להתחבר לבקר מרחוק ע"י חברה חיצונית המספקת תחזוקה / שירות, הגישה צריכה להיות מאובטחת ותכלול את הרכיבים הבאים:

2.1 גישת VPN אל חומת האש

2.2 הזדהות חכמה מבוססת לפחות 2FA מול ה-AD בשם משתמש חד - חד ערכי

2.3 שבירת הסשן המתחבר ככל האפשר

2.4 גישה לשרת טרמינל ברשת המנהלתית עם מינימום הרשאות.

2.5 גישה רק לשירות המבוקש דרך טרמינל נוסף ברשת התפעולית עם מינימום הרשאות למערכת הדורשת טיפול בלבד.

2.6 רצוי לשנות את הפורט ברירת מחדל בין 2 שרתי הטרמינל (מנהלתי ותפעולי)

3. בכל מערכת המנהלת / מבקרת חומרים מסוכנים יש לבצע את הפעולות הבאות

3.1 עדכונים שוטפים לבקר. יש לבצע עדכוני אבטחה תכנה וקושחה לבקר בצורה שוטפת לאחר בדיקתם בסביבת מעבדה

3.2 הקשחת עמדת HMI: יש לבצע הקשחה לעמדות HMI שיש להם גישה לבקרים . ההקשחה תבוצע ע"י BEST PRACTICE של מיקרוסופט (הורדת שירותים מיותרים, משתמשים מיותרים כגון משתמש GUEST וכל המלצה נוספת)

3.3 להסיר ככל האפשר משתמש ADMIN מקומי מתחנות HMI

3.4 סגירת התקנים חיצוניים אל תחנות HMI .

3.5 עמדות ה- HMI יהיו במצב קריאה בלבד, לצורך ביצוע שינוי ע"י מורשים בלבד תידרש הזדהות נוספת.

3.6 יש להשתמש בעמדות ה- HMI בגרסאות מערכת הפעלה שלא פג תוקפן כולל ביצוע עדכונים שוטפים (אם אין אפשרות לעדכון דרך האינטרנט יש לבצע עדכונים עיתיים ידניים)

3.7 יש לדאוג לאנטי-וירוס מעודכן על כל מחשבי ה- HMI ורצוי ליישם בהם פתרון EDR .

3.8 גישה לעמדת ה-HMI תהיה בסיסמא מורכבת (לפחות 8 תווים, מורכבות של 3 מתוך 4 תווים במקלדת : אותיות גדולות, אותיות קטנות, מספרים ותווים מיוחדים)

3.9 הקפצת שם משתמש וסיסמא עם שינוי ערכים של SET POINT או ערכים קריטיים אחרים הקשורים לפעילות הבקר.

3.10 במידה וקיימים LOCAL PANEL (מסכים מובנים במערכת הבקרה) ברחבי המפעל יש להעביר אותם למצב קריאה בלבד . ככל האפשר גם לבצע נעילה פיסית של גישה לאותם מסכים ללא מורשים.

3.11 נעילת ארון הבקרים. ארון הבקרים חייב להיות נעול, יש להציב ככל האפשר מצלמה בסביבת ארון הבקרים

3.12 הסרת כבלי תקשורת מיותרים בארון התקשורת.

3.13 נעילת חדר בקרה וביצוע בקרת גישה למורשים בלבד, יש להציב ככל האפשר מצלמה בחדר הבקרה .

3.14 מומלץ לשקול הצבת דיודה חד כוונית שתגן פיסית על גישות חיצוניות אל רשת התפעול

3.15 יש לבצע מיפוי של כל התהליכים המנהלים / מבקרים חומרים מסוכנים במפעל, ורכיבי המחשוב / הבקרה המרכיבים כל מערכת. יש לעדכן מיפוי זה אחת לרבעון

4. הגנה על מערכת ERP אשר מנהלת / מבקרת חומרים מסוכנים

4.1 מיפוי תהליכים ומודולים

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

4.1.2 יש למפות מי נותני ההוראות במפעל ומי מבצעי השינויים במערכות המחשוב המנהלות מבקרות חומרים מסוכנים ובאילו מסכים/מודולים של ה-ERP הם עושים זאת.

4.1.3 יש לבדוק אילו מנגנונים קיימים במפעל למניעת טעויות הזנה (אישורי מנהל, השוואה מול רישום נייר, ביקורות תקופתיות של המלאי).

4.1.4 אילו מנגנוני גיבוי מיושמים לנתונים אלה (בין אם באתר או בענן) למקרה של תקלה, שיבוש או מחיקה בזדון.

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

4.1.5.1 כיצד ובאחריות מי מעודכנים נתוני הלקוח/הארגון המקבל חומ"ס.

4.1.5.2 באילו מסכים/מודולים של ה-ERP עושים זאת.

4.1.5.3 אילו מנגנונים קיימים בארגון למניעת טעויות במשלוח חומ"ס (למשל טעות הקלדה בכמויות, טעות בסימון החומרים או משלוח ללקוח שאין לו היתר רעלים).

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

4.2.1 למי יש גישה יום-יומית לצפייה/הפעלה.

4.2.2 כיצד ובאחריות מי מבוצעים שינויים בתכנון הייצור/המתכונים במערכת.

4.2.3 באילו מסכים/מודולים של ה-ERP עושים זאת.

4.2.4 אילו מנגנונים קיימים בארגון למניעת טעויות - בדיקה/אישור תצורה או מתכון.

4.2.5 אילו מנגנוני גיבוי מיושמים לנתונים אלה (בין אם באתר או בענן) למקרה של תקלה, שיבוש או מחיקה בזדון.

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

4.3.1 הצגת הנתונים המועברים והאם כוללים נתונים הקשורים לחומ"ס.

4.3.2 יש לפרט באיזה פורמט/פרוטוקול, באיזה חיבור רשת או אופן העברת קבצים.

4.3.3 עם אילו הרשאות ניגשות המערכות החיצוניות לנתונים במערכת ה-ERP.

4.3.4 אילו מנגנונים קיימים למניעת טעויות במידע המתקבל למערכת.

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

4.4.1 הנתונים המועברים.

4.4.2 פקודות להפעלת תהליכי ייצור.

4.4.3 באיזה פורמט/פרוטוקול, באיזה חיבור רשת או אופן העברת קבצים.

4.4.4 מי נותני ההוראות להפעלת תהליכי ייצור או מעבירים נתונים לייצור ממערכת ה-ERP.

4.4.5 באילו מסכים/מודולים של ה-ERP עושים זאת.

4.4.6 אילו מנגנונים קיימים בארגון למניעת תקלות (הפעלת תהליך ייצור בשגגה או כשמצב המכונות אינו נכון, וידוא הנתונים המתקבלים מה-ERP בייצור)

4.5 המלצות להגנת מערכת ה-ERP

4.5.1 <u>הרשאות</u>

4.5.1.1 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 – מומלץ שתמנע ממנו הגישה למודולים או המסכים הקשורים לחומרים מסוכנים.

4.5.1.2 יש לוודא כי המערכת אוכפת הרשאות הפעלת תהליכים / דיווח צריכת חומ"ס / העברת נתונים לייצור / קבלת נתונים ממקורות חיצוניים למי שהוסמך לכך באופן אישי.

4.5.1.3 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.

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

4.6 <u>אכיפת תהליכי מניעת טעויות ותקלות</u>

4.6.1 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.

4.7 <u>מעקב ותיעוד</u>

4.7.1 יש לתעד נסיונות גישה למערכת ה-ERP מרחוק (מחוץ למתקן), נסיונות כושלים או לא מורשים להתחברות של משתמשים או מערכות.

4.7.2 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.

4.7.3 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

4.7.4 ניתן ליישם במערכת ה-ERP דוח היסטוריית שינויים לנושא החומרים המסוכנים שירכז את כל התיעוד הנ"ל לבדיקה תקופתית.

4.8 <u>זיהוי משתמשים</u>

4.8.1 מומלץ כי משתמשים בעלי הרשאות להפעלת תהליכים או ביצוע שינוי בתהליכים או בנתונים יזהו באמצעות הזדהות חזקה (MFA).

4.8.2 באם משתמש מתחבר מרחוק - מומלץ ליישם כלים להצפנת החיבור, וידוא בטיחות המחשב המתחבר.

4.9 <u>אינטגרציה למערכות מידע וייצור</u>

4.9.1 במידה ומבוצע חיבור רשתי בין מערכת ה-ERP למערכות הייצור העושות שימוש או מסכנות חומ"ס, יש להקפיד על דרישות הפרדת הרשתות וסינון הקישור כמפורט במדריך הסייבר.

4.9.2 יש לתעד את הפעלת/העברת נתונים לקווי הייצור ויוזם הפעולה.

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

4.10 <u>גיבוי</u>

4.10.1 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').

4.10.2 יש להגדיר ממונה לתהליך הגיבוי ולתרגלו בשחזור מגיבוי.

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

4.11.1 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.

4.11.2 יש להגדיר וליישם תהליכי עדכון מעה"פ, תשתיות תוכנה, אפליקציה ואנטיוירוס בתדירות מינימלית של פעם ברבעון.

4.11.3 יש להימנע משימוש בתוכנות השתלטות מרחוק (VNC, TeamViewer, AnyDesk, DameWare וכו') ולעשות שימוש בהתחברות טרמינל מאובטח בלבד (RDP, SSH).

4.12 יש ליישם הגנות על עמדות הניגשות למערכת ה-ERP (PC, Thin Client), ראה המלצות מערך הסייבר.

ניהול גירסאות המסמך

גירסא	תאריך	מחבר	מאשר	מהות השינוי
0.99	1.10.2024	יוסי שביט – ר' יחידת הסייבר בתעשייה		כתיבת המסמך
1.0	31.12.2024	יוסי שביט – ר' יחידת הסייבר בתעשייה	לילך פדלון – ר' המערך הלאומי לחומ"ס וחירום	סבב עידונים ותיקונים