הערות ראשוניות של התאחדות התעשיינים

טיוטת המשרד להגנת הסביבה בנושא הגנת הסייבר:
"הוראות לעמידה בתנאי היתר רעלים בתחום ההגנה על מידע וסייבר. גרסה 0.9"

המשרד להגנת הסביבה (הג"ס) מתעתד להוסיף פרק הגנה על הסייבר בהיתר הרעלים בשנים הקרובות. מטרת התוכנית הינה להגן על מערכות המפעלים מפני מתקפות סייבר, העלולות להביא לפגיעה בסביבה או בבריאות הציבור וחיי אדם. החל מ 2018 מתכנן המשרד להגנת הסביבה להכניס לתוכנית מספר מפעלים בדירוג A, ובהמשך יכנסו לתוכנית בהדרגה כלל המפעלים בארץ. לאור זאת, הועברה טיוטה ראשונית, לא מחייבת, מטעם משרד הג"ס להערות התאחדות התעשיינים: "הוראות לעמידה בתנאי היתר רעלים בתחום ההגנה על מידע וסייבר - גרסה 0.9". גרסאות מתקדמות יותר יועברו להתייחסות המפעלים.

הרקע למסמך מועיל במתן המסגרת הכללית והצורך בהגנת מערכות הסייבר.

הערות כלליות

1. הנחיצות להתמודד עם איומי סייבר ברורה, אולם יש לוודא כי תוכנית הפיילוט שתחל ב 2018 תתנהל בצורה ממוקדת ויעילה תוך גיבוש מסקנות והסכמות ענייניות. על כן, מוצע להמתין עם הליך הכנסת דרישות ממפעלים עד אשר יסוכם המתווה באופן מסודר, ולאחר שנבחנו ההשלכות שלו על התעשייה.
2. ביצוע הוראות המסמך כולל תכנון עבודה על שלביה, הקצאת משאבים ליישום, ויישום. על לוחות הזמנים לביצוע להיות ישימים ומתואמים ישירות עם כל עסק, תוך התחשבות ביכולותיו. יש ליצור מנגנון המאפשר שיג ושיח ומונע קביעה חד צדדית.
3. במטרה שהטמעת ההגנה תבוצע באופן מיטבי ולאורך זמן, רצוי לפעול לחשיפת אנשי מקצוע בתעשייה להכיר את נושא הגנה על מידע וסיכול איומי סייבר ומערכות ההגנה, ולתת להם כלים לתכנן ולתפעל אותן בצורה נאותה. יש לשקול אמצעים כגון חוברות הדרכה זמינות, סרטוני הכשרה, סדנאות, בנוסף לחברות ייעוץ. חשוב לא להשית את האחראיות לחברות ייעוץ חיצוניות ולתת כלים מעשיים לפחות לתעשיות שמסוגלות לכך.
4. בעיקר, יש לוודא שקיימת אפשרות שהמפעל, לפחות להגדרת צרכים ראשוניים, יוכל להסתייע בעזרי לימוד מהמשרד להגנת הסביבה בהתאם לאמור בפגישה המקדימה. מבין משימותיה, ולפי ההגדרות הנכללות במסמך, על יחידת הסייבר ללוות באופן מקצועי ושוטף ולתת מענה לפניות מקצועיות בהתאם למאפיינים של העסקים וכתלות בהשתנות איומי הסייבר בזמן. זהו נדבך חשוב מאוד ונחוץ למניעת אירועי חומ"ס. יש לוודא שאכן ממשיך להתקיים גם כשהתוכנית תפעל בצורה סדירה. המטרה היא לתת סביבת עבודה תומכת למפעלים שתאפשר להם לאמץ פתרונות מתאימים ולהימנע מראש מצעדי אכיפה.

5. מיפוי הסיכונים במפעל נעשה באמצעות שילוב בין הערכות: (1) רמת הנזק, משתנה **I**, (נספח ג') ו – (2) רמת חשיפת הארגון לחומ"ס, משתנה **P**, (נספח ד'). שני משתנים אלו מסוכמים לפי נוסחא לצורך קבלת הנחיות פעולה (פרק 9).
   א. יש לחדד את ההסבר על אופן ביצוע הערכת הסיכונים גם ברמה הפרטנית של כל פרמטר וכיצד מקבלים/מחשבים אותו וגם ברמת הצורך בסכימה לפי נוסחא. כרגע זה אינו בהיר דיו מהמסמך עצמו.
   ב. נדרשת הבהרה לגבי מכלול הפעולות שיש צורך לבצע בהתאם למיפוי הסיכונים שהתקבל (נספח ה'). האם הרשימה המלאה רלוונטית למפעלים בדרוג הגבוה (דרוג 4). הכוונה שהפלט המדוייק יצא בהתאם לתשובות של המפעלים על שאלות רמת הנזק (I) ורמת החשיפה (P) אינה ברורה דייה.
6. מוצע להדגיש במבוא כחלק מההתייחסות לתמונה הרחבה יותר של איומי הסייבר, שיקולים עקרוניים (לא מחייבים) שחשוב שהמפעל יהיה מודע אליהם מעבר לשיקולים הקשורים בחומרים מסוכנים.

הערות פרטניות

התייחסויות לסוגיות נקודתיות ושאלות הבהרה מצורפות כהערות עריכה על-גבי המסמך עצמו.

לסיכום, הצורך בהגנת סייבר ברור ומובן. על מנת לקדם הגנה מיטבית ומניעת אירועי חומ"ס לאורך זמן יש לקדם את זמינות המידע לתעשייה ולתת כלים מעשיים לתפעול מיטבי באופן שוטף וזמין.