מדינת ישראל
הוועדה לאנרגיה אטומית

רשב"ט
היחידה לרישוי ובטיחות

מתודולוגיה להגנה על אמצעי בטיחות מפני מתקפות טכנולוגיות

כנס חשמל ואנרגיה 2024

ניר עדי, רז שני, אברהם ברם

תוכן ההצגה

- מבוא
- המתודולוגיה המוצעת
- דוגמה עקרונית

מבוא

רקע

- התהליך הבסיסי של הערכת סיכונים כולל התייחסות לשני מרכיבים:

סיכון = חומרה X הסתברות

- הערכת החומרה מתבצעת בהתאם לגורם הסיכון **ללא תלות בגורם המעורר** (טעות אנוש, כשל ציוד או חבלה)
- הערכת הסיכון לכשלים טכניים או לטעויות אנוש מתבצעת על בסיס **תקנים או ידע מצטבר בארגון**

רקע

- קשה להעריך הסתברות של מתקפה טכנולוגית כגורם מעורר
- ההסתברות לתקיפה תלויה בגורמים שבעיקרם אינם הסתברותיים
  - הזדמנות
  - מוטיבציה של התוקף (גניבת ידע, גרימת נזק וכו')
  - יכולת טכנית

המוטיבציה

- ההערכה של מרכיב ה"הסתברות" בהערכת הסיכון היא מורכבת וסובייקטיבית
- טעות בהערכת ההסתברות עלולה להביא להערכת חסר של הסיכון – בעייתי במקרים שבהם הנזק חמור במיוחד
- נוצר צורך לגבש שיטה המפרידה את המרכיבים ה"סובייקטיביים" מהערכת הסיכון

הרעיון המרכזי

- השיטה המוצעת מתבססת על עקרון מתחום בטיחות התוכנה
- ע"פ עיקרון זה את ההסתברות להתרחשות האירוע מחליפה הקריטיות הבטיחותית של אמצעי הבטיחות
- קריטיות זו מבוטאת באמצעות "רמת השליטה" של האמצעי על מניעת התממשות הסיכון

המתודולוגיה

המתודולוגיה

רמות החומרה - כור

רמת חומרה	תיאור
1	פגיעה בתפקוד מערכת בטיחות ברמה 1 (Safety Category 1) ו/או נזק לרכיבי הליבה המלווה בשחרור של חומרים רדיואקטיביים בכמות העולה על גבולות המנה השנתיים לעובדים ו/או לאיש מן הציבור
2	נזק לרכיבי הליבה ללא שחרור כלל של חומרים רדיואקטיביים או עם שחרור מזערי שאינו עולה על גבולות המנה השנתיים לעובדים ו/או לאיש מן הציבור
3	כשל של רכיב בודד במערכת בטיחות (פגיעה בהגנה לעומק) או במערכת תומכת בבטיחות (Safety Related System) ללא שחרור של חומרים רדיואקטיביים
4	חריגה לא משמעותית מתנאי פעולה נורמליים, ללא פגיעה במערכות הבטיחות או במערכות הבקרה

רמות החומרה - מתקנים

רמת חומרה	רמת חשיפה לעובד	רמת חשיפה לאיש מן הציבור
1	≥ 1000mSv	≥ 100mSv
2	≥ 100mSv	≥ 10mSv
3	≥ גבול המנה	≥ גבול המנה
4	< חסם המנה	< חסם המנה

רמות השליטה

הגדרה	רמה	תיאור
אוטונומי	1	התרחשות אירוע הבטיחות תלויה באופן מלא ובלעדי בפעולה או במחדל של אמצעי בטיחות ללא אפשרות מוגדרת מראש לגילוי ולהתערבות ע"י ישות חיצונית בלתי תלויה. לחילופין, יש אמצעי בטיחות יתירים אך האמצעים היתירים הינם זהים.
אוטונומי למחצה	2	התרחשות אירוע הבטיחות תלויה באופן מלא ובלעדי בפעולה או במחדל של אמצעי בטיחות אך מוצג מידע בטיחותי למפעיל המחייב תגובה מיידית (Time Sensitive) שלו. לחילופין, יש אמצעי בטיחות יתירים אך הם פגיעים באופן דומה למתקפה טכנולוגית.
יתיר לבטיחות	3	התרחשות אירוע הבטיחות תלויה באופן מלא ובלעדי בפעולה או במחדל של מספר אמצעי בטיחות שאינם פגיעים באופן דומה למתקפות טכנולוגיות.
משפיע על בטיחות	4	אמצעי הבטיחות מייצר מידע בעל אופי בטיחותי שנדרש לצורך קבלת החלטות ע"י המפעיל אך לא נדרשת פעולת מפעיל או שהיא אינה Time Sensitive למניעת אירוע הבטיחות

קביעת רמת המאמץ - CLOR

	רמת החומרה			
רמת השליטה	1	2	3	4
1	לא קביל	CLOR-1	CLOR-3	CLOR-4
2	CLOR-1	CLOR-2	CLOR-3	CLOR-4
3	CLOR-2	CLOR-3	CLOR-4	CLOR-4
4	CLOR-3	CLOR-4	CLOR-4	CLOR-4

עקרונות לקביעת רמת המאמץ

- רמת המאמץ תיגזר מהחמור מבין כל השילובים של רמת שליטה וחומרת אירוע
- יש לשאוף לתכן המחייב את רמת המאמץ הנמוכה ביותר (3 או 4 אם ניתן)
- השילוב של רמת חומרה 1 ורמת שליטה 1 **אינו קביל** ומחייב שינוי תכן
- ניתוח המציג צורך בהגנה ברמת CLOR2 מחייב אישור פרטני מהגורמים המוסמכים

קטגוריות של אמצעי הגנה נדרשים

- תכן מערכתי
- אבטחה פיסית
- הקשחת תקשורת ורשת
- הקשחת רכיבי מערך הבקרה
- אבטחת רכיבים מתוכנתים ורכיבי קצה
- ניהול משתמשים והרשאות
- ניטור
- שרשרת אספקה

דוגמה ליישום המדורג

#	אמצעי הגנה	נדרש ב-CLOR			
		1	2	3	4
3	**הקשחת תקשורת ורשת**				
3.1	מניעת התפשטות וגישה של משתמש/קוד זדוני בין סגמנטים ברשת	+	+	+	
3.2	מניעת התפשטות וגישה של משתמש/קוד זדוני בתקשורת לרכיבי המערכת	+	+		
3.3	אבטחה קריפטוגרפית של פרוטוקולי התקשורת בין רכיבי המערך	+			

דוגמה – מתקן הקרנה

מתקן הקרנה

- שפופרת הקרנה בתוך תא עופרת
- אמצעי הבטיחות
  - מפסק סריקה / טלוויזיה במעגל סגור
  - מפסקים – מפסק סף (דלת), מפסק חירום
  - התרעה – נורות, צופר, שילוט
  - בקר הבטיחות
  - גלאי קרינה
- מערכות בטיחות כלליות (אש, רפואה וכו')

ארכיטקטורת הבטיחות העקרונית

- בקר הבטיחות **מונע הפעלת הקרינה במקרה שדלת תא ההקרנה פתוחה** ע"פ חיוויים מגלאי הקרינה ומפסקי הסף
- מערכת גלאים נפרדת **מתריעה במקרה של גילוי קרינה** מחוץ לתא
- מפסקי חירום מאפשרים **הפסקת החשמל למתקן** במקרה הצורך

רמת החומרה

- אירוע הבטיחות – הפעלת הקרינה כאשר הדלת פתוחה
- רמת החומרה
  - במקרה של אדם בתוך התא – רמת חומרה 2
  - במקרה של אדם מחוץ לתא – רמת חומרה 3

רמת השליטה של הבקר

- הבקר מאפשר או מונע אספקת חשמל למתקן ההקרנה על פי התניות מוגדרות מגלאי הקרינה ומפסקי הסף
- גלאי הקרינה מחוץ לתא מדווחים לגורם פיקוח חיצוני
- במקרה של תקלה בבקר, נדרשת התערבות של גורם חיצוני להפסקת המתח ע"י לחיצה על אחד ממפסקי החירום

רמת השליטה של הבקר

- רמת השליטה של הבקר במקרה זה - 2

אוטונומי למחצה	**2**	**התרחשות אירוע הבטיחות תלויה באופן מלא ובלעדי בפעולה או במחדל של אמצעי בטיחות אך מוצג מידע בטיחותי למפעיל המחייב תגובה מיידית (Time Sensitive) שלו.** **לחילופין, יש אמצעי בטיחות יתירים אך הם פגיעים באופן דומה למתקפה טכנולוגית.**

קביעת רמת המאמץ

- רמת השליטה 2, רמת חומרה 3 או 2 (תלוי תרחיש)

	רמת החומרה			
רמת השליטה	1	2	3	4
1	לא קביל	CLOR-1	CLOR-3	CLOR-4
2	CLOR-1	CLOR-2	CLOR-3	CLOR-4
3	CLOR-2	CLOR-3	CLOR-4	CLOR-4
4	CLOR-3	CLOR-4	CLOR-4	CLOR-4

דוגמה ליישום המדורג

#	אמצעי הגנה	נדרש ב-CLOR			
		1	2	3	4
3	**הקשחת תקשורת ורשת**				
3.1	מניעת התפשטות וגישה של משתמש/קוד זדוני בין סגמנטים ברשת	+	+	+	
3.2	מניעת התפשטות וגישה של משתמש/קוד זדוני בתקשורת לרכיבי המערכת	+	+		
3.3	אבטחה קריפטוגרפית של פרוטוקולי התקשורת בין רכיבי המערך	+			

סיכום

- הוצגה שיטה להגדרת דרישות להגנה מפני מתקפה טכנולוגית של אמצעי בטיחות ע"י:
  - זיהוי אמצעי בטיחות החשופים למתקפה טכנולוגית
  - דירוג האמצעים ע"פ הקריטיות שלהם לבטיחות
  - קביעת רמת מאמץ ע"פ הקריטיות
  - הגדרת אמצעי הגנה בהתאם לרמת המאמץ הנדרשת

תודה!