9 ביולי, 2016

ניהול סיכונים משניים בתפעול מערכות

במסגרת מפגש קבוצת העבודה – ניהול סיכונים – יו"ר ד"ר משה ויילר

כתב: אבי הראל[1]

מהם סיכונים משניים

בתהליך של אבטחת חסינות מערכת בפני סיכוני תפעול אנחנו מוסיפים לתכן המערכת עזרי חסינות, כולל חיישנים, אינדיקטורים, תהליכים, אלגוריתמים וכיו"ב, שמטרתם להפחית את הסיכונים על ידי מניעה ועל ידי איתור המצב החריג בעוד מועד.

סיכונים משניים אלו הם סיכונים לתקלות ולטעויות בתפעול עזרי החסינות. במקרים מסויימים (שיודגמו במהלך המפגש) הסיכונים המשניים עלולים לעלות על הסיכונים אותם העזרים הללו נועדו למנוע (להלן, הסיכונים המקוריים) . המדריך לאבטחת חסינות מציג מתודולוגיה לאבטחת חסינות המבוססת על מודל של כשל בתפעול מערכות. פרק מרכזי במתודולוגיה זו עוסק בסיכונים הנובעים מיישום פתרונות למניעת סיכונים אחרים. [2]

דוגמאות

- בטיסת **AF296** של איירבאס **A320**, מעטפת ההגנה נגד הזדקרות מנעה מהטייס לנסוק בתום החליפה מעל השדה
- בטיסת **AF 447** של איירבאס **A330**, הניהוג הועבר אוטומטית מאוטומטי לידני, למרות שהטייסים לא הבינו את התרחיש
- בטיסת **China Airlines 140** הטייס האוטומטי "תיקן" את פקודת הטייסים, ומנע את ביצועה
- כמעט-תאונה בכור הגרעיני **Davis Besse** נגרמה כתוצאה מתקלה בשסתום בטיחות שנתקע
- התאונה במפורסמת בכור הגרעיני **TMI** נגרמה כתוצאה מתקלה באנדיקציה למצב שסתום הבטיחות שנוסף בעקבות הפקת לקחים מהכמעט-תאונה ב-**Davis Besse**

[1] אודות אבי הראל - http://avi.har-el.com/

[2] גירסא ראשונה של מושגי היסוד והאפיונים שלהם מופיעה במדריך לאבטחת חסינות מערכות (http://resilience.har-el.com/).

שאלות של ניהול סיכונים בנושאי בטיחות

במפגש זה ננסה לאפיין את ההבדלים בין סיכוני תפעול משניים לבין הסיכונים המקוריים.

- כיצד מעריכים את הסיכונים בגין עזרי בטיחות ומשווים בין פתרונות שונים
- האם ניתן להגדיר עלות של סיכון, בהשוואה לעלות של תוספת עזרי בטיחות
- האם ניתן להגדיר כללים ליישום עזרי בטיחות.

דוגמאות

- השוואת הסיכונים של טעות מכונה לעומת טעות אנוש בהטסה
- השוואת הסיכונים של "התמכרות" לעזרי בטיחות, לעומת התועלת שלהם
- השוואת הסיכונים של פתרונות שונים עבור מגוון של מאפיינים של ממשקי הפעלה
- השוואת התועלת לעומת הסיכון של פרמטרים שונים בנושא התרעות, כגון טעויות אלפא ובטא בערכי סף התרעה שונים.