

# סיכום מפגש מספר 2 של קבוצת העבודה, תכן לחסינות - 26 במאי, 2013

**חברי הקבוצה מתבקשים להתייחס לסיכום זה:** האם הוא מבטא היטב את מהלך המפגש והנושאים שעלו בו, והאם הסיכום מקובל עליהם.

**בדברי הפתיחה** חזר ד"ר אביגדור זוננשיין והזכיר לנו את המוטיבציה לדין מקצועי בנושא חסינות מערכות, את יעדי הקבוצה, ואת דרך פעולת הקבוצה. חסינות המערכת קשורה לנושא של טעויות אנוש, וניתן למנוע טעויות רבות בתכן מערכתי. מוביל פעילות הקבוצה, אבי הראל, הכין אתר אינטרנט שכתובתו <http://resilience.ergolight-sw.com> הכולל:

- גירסא אינטראקטיבית של מודל החסינות
- גירסא אינטראקטיבית של המדריך לתכן לחסינות
- מאגר אירועים של כשל מערכתי
- מידע על קבוצת העבודה ועל פעילותה.

הכוונה היא לבחון את תוקף המודל והמדריך בעזרת האירועים, ולשפר אותם במידת הצורך. העבודה מתבצעת במסגרת מחקר במרכז גורדון להנדסת מערכות בטכניון. כמו כן חבר קבוצת העבודה, גלעד סלע, התחיל בעבודת מסטר בנושא בפקולטה לתעשייה וניהול בטכניון ויסייע לקבוצת העבודה. **חברי הקבוצה מתבקשים לתרום לבנק האירועים מנסיונם האישי.**

**בחלק הראשון** של המפגש הרצה ד"ר אלון סנה-אור על הגורמים המשפיעים על חסינות, עם הדגמה לגבי שתי תאונות מפורסמות של כלי טיס בזמן המראה:

- התאונה של מטוס הקונקורד, שהסתיימה בהתרסקות
- התאונה של מטוס איירבאס שנחת ללא מנועים על נהר ההאדסון.

במוקד ההרצאה היה הנושא של התייחסות לאורך זמן לנושא התקלות, והשפעתה על יכולת התפקוד בשעת משבר. כמו כן עלה לדיון הנושא של העלות העקיפה של אבטחת בטיחות, כאשר מדובר בפגיעה בתפעול. נושא זה עלה בהקשר של זמינות הטכנולוגיה לאיתור גורמי סיכון של להקת עופות, וההמנעות מישום הטכנולוגיה, משיקולי רווח והפסד. בנוסף, נערך דיון קצר בשאלה של אחריות קברניט המטוס בבחירת הפתרון מבין מספר חלופות.

**בחלק השני** של המפגש הציג אבי הראל את אתר האינטרנט והדגים את שיטת התיקוף בעזרת ניתוח האירוע של תאונת TMI. האיום שהודגם בניתוח האירוע היה של איום סמוי, סגירת מערכת הגיבוי של קירור הכור. בנסיון לתקף את המודל ואת המדריך הסתבר שרמת הפירוט בהתייחסות לאיומים סמויים אינה מספקת, ויש צורך בתוספת פירוט בנושא זה. חברי הקבוצה הביעו תהיות בנושאים הבאים:

- הגישה של המודל והמדריך לאבטחת חסינות היא איכותית. יתכן שיש מקום להוסיף אלמנטים כמותיים.
- בשאיפה, רצוי שההנחיות במדריך תהיינה מיושמות בתקנים
- מההדגמה לא ברור כיצד מהנדסי מערכת אמורים להשתמש במדריך
- פיתוח המדריך על בסיס מאגר האירועים הוא בגדר חכמה לאחר מעשה, וראוי להתייחס לתוקף של מדריך כזה.

**בהמשך למפגש**

תכנית עבודה דינאמית עודכנה בהתאם להערות חברי הקבוצה, וניתן לעיין בה באתר, בכתובת  
<http://resilience.ergolight-sw.com/plan.htm>

תכנית למפגשים הקרובים:

- **רון צורן** הכין מצגת של מספר אירועים המדגימים את ישום מודל החסינות, ויצג אותה במפגש הבא.
- **אבי הראל** יציג את הדרך שקישור בין המודל, המדריך ומאגר האירועים
- **אלון סנה-אור** יוסיף את האירועים שהציג למאגר הנתונים ויצג את המסקנות לגבי תוקף המודל והמדריך מניתוח האירועים
- **אבי הראל** יציג את השיפור במודל ובמדריך בעקבות ניתוח האירוע של תאונת TMI.
- **רון צורן** יוסיף את האירועים שבמצגת שלו לבסיס הנתונים
- **גלעד סגל ואבי הראל** יציגו את האירועים שהכניסו לבסיס הנתונים.
- המשך דיון בתרומה הפוטנציאלית של המדריך. חברי הקבוצה מתבקשים להעביר את התרשמותם, הערותיהם והצעותיהם כולל **אירועים מנסיונם האישי**, אל אבי הראל לכתובת [ergolight@gmail.com](mailto:ergolight@gmail.com)