10 במרץ, 2014

סיכום מפגש 5 של קבוצת העבודה "תכן לאבטחת חסינות מערכות"

בנושא "פתרון בעיות בתנאי אי-וודאות"

ד"ר גדעון עקביה, ד"ר אביגדור זוננשיין, אבי הראל

בחלק הראשון של המפגש ד"ר גדעון עקביה הציג ניתוח אירוע של אש ידידותית משנת 1994. באירוע זה צמד מטוסי F-15 הפיל שני מסוקי Black Hawk שהיו בטיסה מנהלתית באזור האסור לטיסה בצפון עירק. הניתוח התייחס לכשלים רבים בהצטיידות, בתפקוד ובהתנהלות של צוות המסוקים, צוות מטוסי התקיפה, וצוות ה-AWACS (מרכז בקרה מוטס). הניתוח, המבוסס על השוואת ניתוחים של ננסי לבסון ושל סנוק, היה בשלש רמות: הפרט, הקבוצה והארגון. הכשלים העיקריים כללו:

- הגדרה דו-משמעית של גבולות האזור האסור לטיסה: המסוקים נהגו בשגרה להכנס לעיירה זחו, שנמצאת בתוך אזור הבטחון, במרחק 300 מגבולות האזור האסור לטיסה, מבלי להקפיד על נהלי תכנון ודיווח על כך.

- הגדרה דו-משמעית של כלי טייס: מסמכי תכנית הטיסות לא כללו פירוט טיסות מסוקים של חיל היבשה.

- הגדרה דו-משמעית של האחריות המנהלית והמבצעית בתכנון ובהטסת המסוקים: סטיה בהתנהלות בשגרה לעומת הנהלים הכתובים, בשיעור שעולה בהדרגה.

- הגדרה דו-משמעית של הגורם המאשר תקיפה: טייסי התקיפה פעלו על בסיס מידע חלקי ולקוי, מבלי שקיבלו אישור לכך ממרכז הבקרה.

- חוסר כשירות של צוות הבקרה במשימת איבחון מצבים חריגים: בעיית אמינות והתנהלות לא מסודרת בתהליך מעקב מרכז הבקרה אחר מיקום המסוקים

- חוסר כשירות של טייסי התקיפה ושל מרכז הבקרה וליקויים בנהלי התקשורת במשימת זע"ט

- אי התאמה של ציוד התקשורת ואי הקפדה על נהלי ההתקשרות

- עיגול פינות בתפקיד הזע"ט, עקב להיטות יתר של מטוסי התקיפה להגיע להישגים מבצעיים

- העדר אמצעי מיגון של המסוקים בפני תקיפה מהאוויר.

בחלק השני של המפגש, התנהל דיון בסוגיה של הפקת לקחים מאירוע כשל זה, ומאירועים אחרים של ירי על כוחותינו. הכוונה היתה לקיים דיון בגורמי כשל באירועי סיוע לגייסות, והתקלויות בין כוחות ידידותיים, וכן באפשרות לצמצם סיכונים כאלה בעזרת המדריך. היתה התחלה של דיון, שלא הסתיים. להלן הנושאים העיקריים שעלו בדיון.

סוגים של תאונת אש על כוחותינו

יש להבחין בין מצבים של טעות זע"ט (כמו בצפון עירק או בתאונת האימונים צאלים ב') לבין מצבים טעות בציון המטרה (כמו בתאונת האימונים צאלים א' או תאונת איפוס מציין המטרות באפגניסטן).

פירוק מודולרי של האירוע

תהליך הפקת הלקחים מבוסס על מודל הגבינה השוויצרית של ג'ימס ריזן, על פי מפשטים את תהליך הערכת החסינות על ידי בחינה של כל מנגנון הגנה בנפרד מהאחרים. בהקשר של המדריך לחסינות, אנחנו מבקשים לזהות ליקויים קריטיים, שעלולים לקרות במערכות דומות, ולהציע מנגנוני הגנה שיאפשרו להמנע מהליקויים הללו במערכות עתידיות.

הנושא של אש ידידותית הוא מורכב במיוחד, מכיוון שמדובר בו על שלש מערכות אוטונומיות, ועל המורכבות של תהליך התיאום ביניהם. במודל התגובה לאיום ההתייחסות אל כל מערכת ואל תהליך התיאום היא מיוחדת. במפגש זה התחלנו לדון בחסינות של מערכות המסוקים.

יגאל ציין שבניגוד למקרה המורכב של צפון עירק, בעייה זו קיימת גם בסיטואציות פשוטות, כגון בלחימה בשטח בנוי. לפיכך, ניתן להתייחס אל מרכיבים סצפיפיים של הבעיה, שישימים גם לכוחות היבשה.

הפקת לקחים מאירועים קודמים

יש להבחין בין שני סוגי וועדות תחקור: לצורך הפקת לקחים או לצורך הצבעה על אשמים. **ישראל** העיר שהבעיה עולה לעתים קרובות במשחקי מלחמה, ולא ברור כיצד מפיקים מאירועים אלו את הלקחים. **גדעון וראובן** העלו את הצורך במיסוד התהליך של הפקת לקחים, בסטנדרד של תחקור תאונות בתחום התעופה, ובחשיפה של המסקנות לציבור. **אילן** הסביר שקיימים תהליכי תחקור מסודרים, אבל הממצאים לעתים קרובות מסווגים.

ארכיטקטורה לאבטחת חסינות

יישום הפתרונות לאבטחת חסינות מבוסס על עקרון האילוצים שהוצע על ידי ננסי לבסון. הישום הוא על ידי הוספת יחידות מאפשרות למערכת לבקר את עצמה. הוצגה ארכיטקטורה של מערכת חסינה שמיישמת את עקרון האילוצים בתכן מערכת. במערכת החסינה, פעולות של תפעול תקלות הן חלק בלתי נפרד מהארכיטקטורה. לפיכך, הארכיטקטורה המוצעת כוללת את המרכיבים הבאים:

- היחידה הפונקציונאלית – השינוי הוא שהיחידה צריכה לדווח על מצבה
- יחידת התפעול השגרתי – בדרך כלל נהוג להתייחס אליה כאל ממשק התפעול
- יחידת איתור חריגים – מיישמת מודל של ההתנהלות השגרתית, עוקבת אחר התנהלות היחידה הפונקצינאלית, משווה את המצב בפועל למצב על פי מודל ההתנהלות השגרתית, ומעבירה מידע על חריגות ליחידת ההתרעות
- יחידת ההתרעות – מיישמת עקרונות מתחום התפיסה, על מנת להבטיח שהמפעילים יבחינו במצב החריג ויזהו את רמת הסיכון
- יחידת הפיקוח – מיישמת עקרונות מהתחום של קבלת החלטות, על מנת להבטיח אוטומציה במצבי לחץ, ושיקול דעת כשהמצב מאפשר זאת. יחידת הפיקוח היא ספציפית לכל תת מערכת.
- יחידת התפעול בחירום – מיישמת תהליכים של איתור תקלות, והנחיה לגבי התגברות על התקלות.

המדריך כולל הנחיות להגדרת דרישות לכל אחת מהיחידות באופן שהמערכת המורחבת תוכל להבטיח חסינות. כל אחת מיחידות המערכת החסינה יכולה לכלול מפעילים ומרכיבים אוטומטים. אופן הקצאת התפקידים תלוי ביכולות המכונה לסייע למפעיל. בדרך כלל, תפקיד המכונה הוא להציג מידע למפעילים באופן שיאפשר להם לקבל החלטות נבונות.

עופר ורן הציעו שההגדרות תהיינה כך שהמכונה תאפשר למפעיל גם פעולות חריגות. בדוגמא של צפון עירק, המשמעות היא שהמכונה תאפשר למפעיל להזמין "אש על כוחותינו".

הארכיטקטורה מוצגת במדריך בכתובת
http://resilience.ergolight-sw.com/Guide-v4/Design/Architecture.htm

זיהוי ההפרעה

זיהוי ההפרעה לתהליך התפעול השגרתי תלוי בנקודת המבט. מנקודת מבט המסוקים, מדובר בהפרעה חיצונית. מנקודת מבט מטוסי התקיפה, ההפרעה היא של טעות תפעול. מנקודת המבט של מערך ההגנה, ההפרעה היא תקלת תקשורת. במדריך, ההתייחסות לכך היא בנושא הגדרת ההפרעות, בכתובת
http://resilience.ergolight-sw.com/Guide-v4/Terms/Disturbances.htm

זיהוי האיום

במודל התגובה לאיום, הבעיה תלויה אף היא בנקודת המבט. מנקודת מבט המסוקים, הבעיה היא של סיכול האיום. מנקודת מבט מטוסי התקיפה, הבעיה היא של זיהוי האיום. מנקודת המבט של מערך ההגנה, הבעיה היא של גילוי ואיבחון המצב החריג.

בעיית ההתמצאות

הנוהל של תלות במידע מגורם מתאם (מרכז הבקרה המוטס) אינו עומד במבחן המציאות. **שוש** הביעה ספק לגבי התועלת שבנוהל עדכון המידע במרכז הבקרה. **רן וגדעון** העלו טיעון שלעתים תמונת המצב של מרכז בקרה אינה משקפת את המציאות, והיא גורמת להטעיה. לעתים הנזק עלול לעלות על התועלת. **אביגדור** העלה תמיהה מדוע לא הוגדר תנאי של קשר ישיר בין מטוסי התקיפה לבין המסוקים.

אבי הציג אנקדוטה מנסיונו האישי כקצין טיווח ארטילרי במוצב הר דב. באירוע זה, אחת התצפיות זיהתה תנועה באזור המוצב, והפעילה תאורה. בדיעבד, התברר שהתאורה הפריעה לפעילות של כוחותינו. מאנקדוטה זו ניתן ללמוד על הצורך לקבוע נהלים לתיאום בקשר ישיר עם האחראי על הגזרה. יש להבחין בין מצבי שגרה, בהם הדגש הוא על התמצאות, לבין מצבי חירום, בהם הדגש הוא על פעולה מהירה.

ניתן ליישם את העקרון הזה גם בנושאי זע"ט באזור אסור לטיסה. התניה כזו, לו הוגדרה בנהלים, היתה אוסרת על המסוקים לצאת לדרך כל עוד לא היה קשר ישיר עם מטוסי התקיפה האחראים על הגזרה. מרכז הבקרה המוטס צריך לאסוף מידע במצב שגרה, ובמצב חירום הוא צריך לצאת מהמעגל. במונחים של STAMP, התיאום בקשר ישיר יוגדר כתנאי ליציאה לפעולה.

גדעון הצביע על קושי מעשי ליישם התניה של קשר ישיר בזמן מלחמה. במקרה של צפון עירק, היתה התניה כזו, אך היה קושי בישום.

מגננה

גלעד העלה את הבעיה של מצב בו אין קשר עם הסביבה. **רון** הזכיר שקיים פתרון של מערכת חירום פורצת תדרים.

עלתה השאלה של עלות-תועלת בישום פתרונות ל"א למצבי מתקפה על ידי כוחותינו. בהקשר זה **גדעון** העלה שאלה לגבי הנזק האפשרי של פתרונות אד-הוק לבעיה ספציפית. ייתכן מצב בו אילוץ המערכת לפעול בדרך נתונה יגביל את האפשרות להתמודד עם מגוון של בעיות שצריך לפתור ביומיום.

פתרונות בתחום הארגון

יגאל הציע להגדיר אחריות אישית מלאה של המפקד על כל האופרציה, כולל היבטי בטיחות. **גדעון** הביא נימוקים של פגיעה ביכולת המבצעית בסיטואציות בהן המפקד נדרש לעקוב אחר הפרטים, והעלה על נס את הנוהג המקובל של האצלת סמכויות לדרגי הביצוע.

שוש הציעה להדגיש את נושא ההדרכה והאימון. **מאיר** העלה את נושא אחריות המפקד ליישום ההדרכה.

תרבות בטיחות

המטרה היא להביא לכך שהתוקף יבדוק היטב האם קיימת סכנה לכוחות ידידותיים. זאת, על ידי העלאת הסיכון בסיטואציה נתונה למודעות. **אביגדור** העלה על נס פעילות של עמותת אור ירוק שהביאה להפחתה בשיעור התאונות של פגיעה בילדים בנסיעה לאחור.

ניהול סיכונים

נערך דיון האם המודל המקובל של ניהול סיכונים ישים. **אמנון** העלה טיעון של עלות-תועלת, במצב של משאבי פיתוח מוגבלים.

נערך דיון בנושא של האפשרות להעריך את הנזקים או את ההסתברות לאירועים חריגים. במקרה של ברבורים שחורים, בודאי שהמודל של ניהול סיכונים אינו ישים, מכיוון שמדובר במצבים שהם בלתי צפויים, ולכן לא ניתן להעריך את הנזק שלהם או את ההסתברות להם. גם במקרה של ברבורים אפורים, קשה ביותר להעריך את הנזק, וההערכות לוקות באי וודאות חמורה. דוגמאות לכך הן הטעויות הגסות בהערכת הנזק האפשרי של מתקפת אל-קאידה או של הצונמי באוקיינוס השקט.

סיכום

במפגש זה לא הספקנו לדון נושאים חשובים אחרים בתחום של קבלת החלטות בתנאי אי-וודאות, ומיוחד בתחום של ירי על כוחותינו. בכוונתנו לקיים דיון בנושאים הללו בהמשך.

רון חזר על הצעתו מהמפגש הקודם, להזמין לקבוצה הרצאה בנושא אינטראקציה אדם-מכונה. חברי הקבוצה מוזמנים להציע נושאים או מרצים נוספים.