2 במרץ, 2017

מילון מונחים בתחום של טעויות אנוש

כתב: אבי הראל

בישיבה היום הועלה הצורך להכין מילון מונחים שישמש לתקשורת בין מהנדסי גורמי אנוש לבין מהנדסי פיתוח מדיסציפלינות אחרות בכלל, ומהנדסי מערכת בפרט.

במסגרת פיתוח המדריך לאבטחת חסינות בפני טעויות מפעיל הגדרנו מונחים שנועדו לפתור בעיות באופני המינוח המקובלים. מוצע בזאת לדון במונחים הללו, ולבחון את התאמתם לעולם המושגים של חברי קבוצת העבודה.

מושגי יסוד

ראשית, כדאי להבחין בין המושגים שימוש ותפעול, ובהתאם בין המשתמש והמפעיל.

המונח שימוש הוא פונקציונאלי, והוא מתייחס אל תפוקה וניצול בפועל של התועלת הפוטנציאלית של המערכת. המשתמש הוא האדם שנהנה מהפונקציות.

המונח תפעול הוא תהליכי, והוא מתייחס אל הפעילות הדרושה להבאת הפונקציה אל המשתמש. המפעיל אינו נהנה מהפונקציות, אבל הוא אחראי לכך שהמשתמש יהנה מהן.

במערכות פשוטות, כגון מוצרי צריכה, המשתמש הוא גם המפעיל, אבל לא כן במערכות מורכבות. במדריך לאבטחת חסינות קיים תרשים שמדגיש את ההבדל בין המושגים הללו:

http://resilience.har-el.com/Guide/Models/Extended-system/index.htm

הערה: יש מקום להרחיב את הדיון במושגי היסוד ולכלול מושגים הקשורים בתמיכה טכנית, תחזוקה, הדרכה וכיו"ב.

מהי טעות?

המושג "טעות" הוא רב משמעי, כאשר המשמעות היא סובייקטיבית, ותלויה בציפיות. הטעות היא מצב של חריגה משמעותית מהציפיות.

הציפיות הן כדלקמן:

- הציפיות של המפעיל הן שהמפתח יבין את כוונת המפעיל ויתכנן את המערכת בהתאם
- הציפיות של המפתח הן שהמפעיל יבין את כוונת המפתח ויפעל בהתאם
- הציפיות של בעלי העניין הן שהביצועים של המערכת יהיו מיטביים, והנזקים בגין כשל יהיו מזעריים.

חריגה היא משמעותית אם היא מצדיקה תחקור, בפועל, תנאי זה מתקיים אך ורק כאשר נפגע האינטרס של בעלי העניין. בהתבסס על ההגדרה של הולנגל משנת 1980, ההגדרה המוצעת למונח "טעות" היא כדלקמן:

הגדרה: פעילות במהלך תפעול מוגדרת כטעות אם בעקבותיה נגרם נזק לבעלי העניין ברמה שמצדיקה תחקיר.

של מי הטעות?

בכל מצב טעות יש גורמים רבים המעורבים בו:

- תנאים קיצוניים בתפעול, כגון, תקלה ברכיב
- ליקוי בתכן שמאפשר את יצירת הנזק
- קושי של המפעיל למנוע את הנזק
- מחדל של ההנהלה בתחום ההדרכה, הבטיחות ומנגנון הפקת לקחים.

בתהליך תחקור אופייני, ההנהלה נדרשת להסבר גורמי הכשל, ולכוונותיה לגבי מניעת כשל חוזר. בדרך כלל ההנהלה מתקשה לספק את ההסברים ולשכנע שהכשל לא יחזור: אין לה שליטה בתנאים הקיצוניים, אין לה אפשרות מעשית להתעמק בטכנולוגיה, להכנס לעובי הקורה בעבודת ההנדסה, ולהתעמת עם המהנדסים, ולכן ההנהלה נוהגת לייחס את הטעות למפעילים.

המדריך לחסינות בפני טעויות תפעול כולל סטטיסטיקות של ייחוס הטעויות למפעיל, בדף:

http://resilience.har-el.com/Guide/Terms//Error/index.htm

לימוד מטעויות

מקיום תהליך של הפקת לקחים משתמעת הודאה באחריות ההנהלה לכשל. בתהליך אופייני של הפקת לקחים, ההנהלה מתקשה להצביע על הגורמים שיכולים למנוע את האירוע הבא, או לשכנע את בעלי העניין להשקיע משמעותית במניעת אירועים דומים. בכדי לסבר את האוזן, ההנהלה נוקטת בצעדים ראוותניים במישור האישי. בדרך כלל הקרבן הוא המפעיל, שמתקשה לשחזר את מהלך האירועים ולהצדיק את התנהגותו בכל שלב. זוהי הסיבה העיקרית מדוע הטעות מיוחסת דווקא למפעיל, יותר מאשר לכל גורם אחר. ייחוס הטעות למפעיל מאפשרת להנהלה להמנע מדיון בתהליך הפקת לקחים. המונח "טעות מפעיל" נועד בראש וראשונה לשרת את האינטרס של ההנהלה, להסיט את הדיון ממחדלים למישור האישי.

הסמנטיקה של גורמי הכשל

ייחוס הכשל למפעילים, הענשתם על תקלה שהיא במהותה מערכתית, פוגעת בתהליך הפקת הלקחים. דוגמאות מוכרות מהספרות כוללות:

1. מתחום התעופה: בסלון אוירי בשנת 1988 באלזס שבצרפת התרסק מטוס איירבאס 220 בשירות AF, שהיה הדגם הראשון עם טייס אוטומטי, בגלל טעות בתכן (הגנת יתר בפני הזדקרות). התקלה נחקרה, אבל תהליך התיקון לא יושם, עד לתאונה בבנגאלור בהודו בשנת 1990, שאירעה בנסיבות דומות.

2. מתחום הכורים הגרעיניים: בכור Davis Besse שבאוהיו היתה בשנת 1977 תקלה בשסתום שחרור הלחץ בכור ההיתוך. ההנחיות להתמודדות עם התקלה היו שגויות, אבל הצוות הצליח לאתר את התקלה למרות ההוראות השגויות. המידע על כך לא הועבר לתחנת הכח ה"אחות" TMI שבפנסילבניה. פעולת תיקון בלתי מוצלחת בתכן הפריעה לדיאגנוסטיקה של התקלה, והשאר היסטוריה.

הענשת המפעילים גורמת לנזק נוסף, והוא פגיעה בנכונות העובדים לשתף פעולה עם ההנהלה בענייני בטיחות, והעלמת מידע שעלול להביא להאשמתם. בשנים האחרונות קיימת מגמה של הגנה על המפעיל בדרך של תחיקה. דוגמא לכך היא חוק התעופה הנורבגי, שאוסר להעניש את מי שמדווח על בעית בטיחות.

בשנים האחרונות קיימת מגמה להשתמש המונח "טעות שימוש" במקום "טעות משתמש". מגמה זו מעוגנת בתקינה במערכות רפואיות, אבל לא מעבר לכך (https://en.wikipedia.org/wiki/Use_error). יש בכך מענה חלקי, כי לכאורה, מהנדסי הפיתוח הופכים לשותפים לאשמה. בפועל, כל עוד הדיון הוא במונחים של אשמה, האשמה רובצת עדיין על המפעילים, מאחר שאין להם כלים להתמודד מול הכלים של המהנדסים.

מינוח קונסטרוקטיבי

המונח "טעות" בהקשר של מהלך האירועים הוא הרסני. הוא כולל בחובו האשמה, שפוגעת בתפקוד המערכת. יש להחליף אותו במינוחים שמתייחסים למצבי כשל, במקום לתפקוד המפעילים או המשתמשים.

עקרון: אין לייחס את הטעות לפרסונה כלשהי. יש לייחס אותה לסיטואציה התפעולית בלבד.

במדריך לחסינות בפני טעויות יש אפיון של שני מצבים בהם נהוג לייחס את הטעות למפעיל:

- פעולה חריגה, שאינה תואמת את ציפיות המפתחים, בין אם במתכוון או בשוגג, נקראת "החטאה". ההתמודדות עם החטאות היא בעזרת נגזרת גורמי אנוש של חוק מרפי: אם המערכת מאפשרת החטאה, במוקדם או במאוחר המפעיל יחטיא. To err is human!. מניעת הטעות מתאפשרת על ידי מנגנון הגנה בפני הפעלה בטעות.

- כשל בהתמודדות עם מצב בלתי מוכר של המערכת נקרא "מבוכה". ההתמודדות עם מבוכה היא בעזרת סמנטיקה שמייחסת את האירוע למצב שהוא בלתי מוכר למפעיל. את המבוכה ניתן לייחס לחוסר מידע או למידע לקוי למפעיל, לייצוג המידע באופן שאינו תואם את ציפיות המפעיל, לבעיית זמינות של פקדים שהופעתם תלויית מצב וכיו"ב. מינוחים שמכוונים לנסיבות הכשל הם קונסטרוקטיביים, ומאפשרים תהליכים של הפקת לקחים (הדגמה במדריך: http://resilience.har-el.com/Guide/Models/Confusion/index.htm).

הצעת מינוח: ניתן להשתמש במונח "טעות" בהקשר של פריטי התכן. דוגמאות של מינוחים ראויים:

- טעות במידע
- טעות בהצגת המידע
- טעות במיקום פקד
- טעות בעיצוב פקד
- טעות ביצור התרעה
- טעות במידע בהתרעה
- טעות בהדרכה
- טעות בהוראות ההפעלה.

לשימושכם,

אבי הראל