

ניהול סיכוני תפעול על פי המודל לאבטחת הסינות מערכות

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

כתב: אבי הראל

ניהול סיכונים

ניהול סיכונים זהו תהליך אופטימיזציה דינאמית, המבוסס על בחינה והערכה שוטפת של הסיכונים שבישום חלופות שונות.

תהליכי ניהול סיכונים עוסקים באופטימיזציה, שמטרתה למזער את הסיכונים. השיטה לניהול סיכונים מבוססת על חישוב התוחלת של הסיכונים השונים, על בסיס שיערוך של הנזק והסבירות של הסיכונים. ניתן לנסח זאת בנוסחה

$$\text{Solution} = \min_{h \in \{\text{Hazards}\}} \Sigma \text{Risk}(h)$$

הסיכונים נבחנים מנקודת מבט שונות של בעלי העניין במערכת: המפתחים, הלקוחות, והמפעילים. במפגש זה ננסה לאפיין את ההבדלים בין תהליכי ניהול סיכונים מנקודות המבט השונות.

ניהול סיכונים בפיתוח

העניין העיקרי של מהנדסי מערכות בניהול סיכונים הינו הצלחת הפיתוח. דהיינו, מדובר בשלב מוקדם בחייה המערכת. הסיכונים הינם סיכוני פיתוח: טכנולוגיה, משאבי אנוש, זמינות רכיבים, אמינות ...

תהליכי ניהול סיכונים בהנדסת מערכות מיועדים להפחית את הסיכונים לאורך חיי המערכת. התהליכים ה"מסורתיים" מתמקדים בשלב קריטי במחזור החיים של הפרויקט, שלב הפיתוח, והם נועדו לשפר את הסיכוי לכך שפיתוח המערכת יסתיים בהצלחה.

בהנחה שניתן להעריך את הנזק בגין הסיכונים, ולהעריך או למדוד את סבירותם החישוב של סיכון הוא על ידי:

$$\text{Risk}(h) = \text{ExpectedValue}(\text{cost}) = \Sigma (\text{Pr}(h) \times \text{Cost}(h))$$

תיאורטית, ניתן להעריך כל אחד מהסיכונים, ולהשוות את הסיכון המצטבר על פי הנוסחה לעיל.

ניהול סיכונים בתפעול

ניהול סיכונים בתפעול מערכות עוסק בשלב אחר בחיי המערכת, דהיינו, בהפעלתה אצל הלקוח. הסיכונים הינם סיכוני עלות ונזקים ללקוח: בגין תקלות וטעויות בתפעול. בשלב זה הסיכונים הם שונים, והם כוללים נזקים בגין תקלות, טעויות תפעול, פעולה בלתי מתואמת בין מכלולים וכיו"ב.

הנושא של סיכוני תפעול הוצג בשנת 2010 במסגרת קודמת של קבוצת עבודה זו (<http://avi.har-el.com/heb/Articles/Operational-Risk-Management.pdf>). מאמר זה מאפיין את ההבדלים בין סיכוני תפעול לבין סיכוני פיתוח, ולהסיק לגבי ההבדלים בניהול שני סוגי הסיכונים הללו. המאמר מדגים מדוע תהליך ניהול הסיכונים בפיתוח אינו ישים למצב התפעול, ומציג את הדרישות לניהול סיכונים בתפעול.

שיערוך הנזק בגין תקלה

האירועים המהווים סיכון בפיתוח מוכרים ברובם היטב, וניתן לצפות אותם ולהעריך את הסתברותם. המצב הוא דומה כאשר מדובר בתקלות בצידוד בשלב התפעול. הערכות סבירות התקלות נעשות בפרויקטים תחת הכותרת של אבטחת אמינות, במונחים של MTBF. הבעיה היא שהנזק בשלב התפעול תלוי בסיטואציה הספציפית. המדד בו נהוג להשתמש הינו עלות התיקון, כגון, במונחים של MTTR. הבעיה היא במקרים חריגים, בהם המפעילים נכשלו בזיהוי התקלה, וכשלוון זה הסתיים בתאונה. הבעיה היא שאותה פעולה, שבדרך כלל נחשבה ללגיטימית, או שגרמה לנזק זניח, במצבים מסויימים מסתיימת באסון.

שיערוך השכיחות של תקלות

מרבית התאונות מיוחסות לגורם האנושי, ובמיוחד בטעויות בתפעול. מדובר בפעולות בלתי צפויות, בעיקר כמצבים של חוסר תיאום בין מכלולים במערכת. ברמה התיאורטית, לא ניתן למדוד את השכיחות של תקלה שעדיין לא קרתה. כיום, עדיין לא פותח מודל שמאפשר להעריך את השכיחות של פעולות בלתי צפויות.

האחריות להפחתת הסיכונים

כשמדובר בפיתוח, האחריות המקצועית להפחתת הסיכונים היא בביורור של מהנדסי המערכת. כאשר מדובר בתפעול, מדובר באחריות במשותף, של המפתח ושל המפעיל. המפעיל מצפה שהמפתח יחזה את כל מצבי הכשל האפשריים, וימנע אותם במידת האפשר, או יתמוך בפעילות של הפחתת הנזק. המפתח מצדו מצפה שהמפעיל ישכיל להתמודד עם האיומים, ומתקשה לחזות את המצבים בהם המפעיל אינו מתמודד עם האיומים.

נושא האחריות הינו קריטי להפחתת סיכונים. הנושא נדון במסגרות שונות של אקלים בטיחות ושל תרבות בטיחות. אקלים בטיחות מתייחס לשיתוף העובדים וההנהלה במניעת תאונות. זהו מצב אידיאלי, שמתעלם מהמציאות של התנהגות אנושית תחת איום של אשמה ברשלנות. תרבות הבטיחות מתייחסת להמנעות מאשמה, על מנת לאפשר מיצוי התחקירים של מצבי תאונה וכמעט-תאונה.

גורם הזמן

המונח מתייחס אל הזמן מהיווצרות האיום ועד למימוש. גורם זה מופיע בנוסחאות של ניהול סיכונים קלאסי כאילוץ של הפרויקט, אבל לא כמאפיין של האיום. כשמדובר בסיכונים תפעוליים, גורם הזמן הוא קריטי. התכן להפחתת סיכונים צריך להבטיח גילוי מוקדם ככל האפשר של האיום, ותהליכים מהירים של איתור תקלות, כאשר הפעילות היא בתנאי לחץ מנטאלי.

המידע על האיום

לגורם הזמן יש משמעות מיוחדת לגבי ההתנהגות בתגובה לאיום, מכיוון שהוא משפיע על היכולת להעריך נכונה את המצב, ולבחור את אופן התגובה ההולם. בתגובה להתרעות בתפעול, גורם הזמן מתייחס אל המידע למפעילים לגבי הזמן הנותר עד למימוש האיום (זמן החסד). מידע זה חיוני לבחירת התגובה המתאימה למסגרת הזמן בו המפעיל יכול להשפיע על התוצאה.

איכות ההתרעה

כאשר מדובר באיום במהלך פיתוח, תפקיד ההתרעה הוא להסב את תשומת לב המפתחים לבעיה. ההתרעה לא צריכה לרמז על הפתרון. בניגוד לכך, כשמדובר בסיכונים בתפעול, בתנאים של לחץ זמן, ובמיוחד במצב של סיכוני מרובים בו-זמנית, ההתרעה צריכה להנחות את המפעיל להערכת הסיכונים השונים, על מנת שיתמקד בפעילות הנדרשת להפחתת הסיכונים.

התרעות טורדניות

מדובר בהתרעות כלליות, התרעות שווא, התרעות תזכורת וכיו"ב. כשמדובר בתהליך הפיתוח, ההתרעות הללו אינן מהוות בדרך כלל גורם הסחה משמעותי. למפתחים יש זמן די והותר לסנן את הרעשים, ולזהות את העיקר. בניגוד לכך, כשמדובר בסיכונים בתפעול, התרעות טורדניות גורמות להסחת דעתו של המפעיל מהתפקיד העיקרי. במקרים רבים, במקרה של ריבוי בהתרעות טורדניות, המפעיל לומד להתעלם מההתרעות. תאונות רבות נגרמו כתוצאה מכך שהמפעיל לא זיהה שמדובר בהתרעת אמת. במקרים קיצוניים, כגון במצבי חירום, המפעיל משתיק או מנטרל את מערכת ההתרעות, על מנת למנוע את ההפרעה. בהמשך, הוא עלול להחמיץ מקרים של התרעת אמת.