תהליכי הטמעה של מוצרים טכנולוגיים

מאת: אמיתי דן

הקדמה

מאמר זה נכתב מתוך כוונה להביא את הקורא להסתכל על כשלים שיטתיים ממבט רחב, וזאת לאחר בחינה של מקרים ודוגמאות בצורה ממוקדת ונקודתית.

לאחר בחינה ושקלול של מקרים שונים מתחומים מגוונים שבהם טכנולוגיות הוטמעו במהירות מתוך כוונה להפיק רווחים בטווח הקצר, או לחלופין לקצר את הליכי הפיתוח היקרים הבנתי שיש צורך בהסתכלות רחבה על הליכי הפיתוח וההטמעה של מוצרים שונים, וזאת עקב ההשלכות של הכשלים כאשר הם מופיעים.

כשלים שיטתיים הנם האיום הגדול ביותר מאחר שההשלכות שלהם עלולות להיות קריסה של מערכות דיגיטליות (באג 2000 שלא התרחש) ובפזה אחרת- אסון ורסאי וכשלים של שיטות שלמות אחרות שקשה מאוד לבצע להן Recalling עקב הפופולריות והתפוצה שצברו.

המאמר לא מתמקד בתחום של אבטחת המידע - מוצרים בתחום זה הנם מוצר לכל דבר ועניין ולכן נרוויח מההסכתלות הכללית.

פיתוח מוצרים

תפוצה רחבה וגלובלית של מוצר, וההטמעה שלו בחיי היום יום של אנשים או הליכים (כמו הליכי ייצור) הנם מדדים שבהם אדם פשוט יכול להשתמש ולהבין שיש הצלחה למוצר מסויים. כהמשך לכך פעמים רבות המטרה של עסק הינה הפצה של המוצר, ומכירה שלו וכמה שיותר מהר.

דוגמה מוכרת בה משתמשים כשבאים להראות את התחום היא המקרה בו ניתנה הנחיה לייצר מכוניות בעלות חלקי חילוף בעלי בלאי גבוה (Ford), וזאת מאחר שנוצר מצב שבו אין תקלות ומאחר שאין כשלים נוצר רצון לייצר כאלה לצורך גרימה ללקוח לחזור ולרכוש מכונית חדשה.

לגבי המכוניות, נראה שהיום ישנם מקרים רבים של Recalling דווקא בגלל תקלות מסכנות חיים, ולא מדובר עוד על ייצור מכונית עם בלאי גבוה או נמוך אלא ייצור של מכוניות שיעמדו בסטנדרטים קפדניים של בטיחות.

דוגמת המכוניות מעניינת מאחר ששם נוצר מצב שבו הוגדר מחדש מדד ההצלחה, וממצב של ייצור של כלי רכב בעלי חלקים איכותיים ללא בלאי, המצב החדש להגדרת ההצלחה היה ייצור מכוניות איכותיות שיוחלפו באחרות לאחר זמן מסויים עקב בלאי טבעי. מצב זה נוצר כאמור עקב מכירה של מוצר טוב מידי שאיננו מתכלה.

אני בוחר בדוגמה זו מאחר שלפיה ניתן ללמוד שהגדרת המושג הצלחה הנו דבר שניתן לשחק בו בהתאם לאינטרס של כל אחד מהצדדים (הלקוח/היצרן) ולכן ניתן לראות שבזמן שהיצרן רואה ככשל את העובדה שהמוצר מחזיק מעמד לאורך זמן, הרי שמבחינת הלקוח ההשלכות של דבר זה הנן קבלת מוצר בעל חיי מדף קצרים יותר.

כפי שציינתי בפתיחה מאחר שמטרת היצרן הנה למכור כמה שיותר, הרי שמחלקת הפיתוח הנה מחלקה שבה המשאבים הנם כאלה שלרוב לא ניתן לראות את הרווחים שלהם באופן מיידי על החברה.

מצב זה הנו הכר הפורה לגידול כשלים שיטתיים מאחר שכאשר מייצרים מוצר הרצון הוא לקבל מוצר עובד, וברגע שיש אחד כזה כל עיקוב בהמשך הליכי הייצור הסדרתיים ולאחר מכן ההפצה יוצר מצב של הפסדים מיידים לחברה.

עקב כך שהייצור מואץ והבדיקות למניעת כשלים לא תמיד נעשות כראוי, וגם אם כן הרי שהבדיקות שנעשות הנן מול הכשלים הידועים לנו עד כה (עמידה בתקנים לאבטחת מידע או בטיחות), ולא בדיקה של המוצר מול כשלים שאינם מוכרים הרי שנוצר פתח ליצירה של כשלים שבמקרה שיהיו שיטתיים הרי שהנזק העתידי על החברה יהיה גבוה וכואב.

הטמעת מהירה של מוצרים ושיטות

מאחר שהייצור או ההטמעה של המוצרים מתמקד פעמים רבות במוצר ולא בכשלים החיצוניים או הפנימיים שמאיימים עליהם, נוצר מצב של טמינת הראש בחול והתמקדות לא נכונה בייצור עצמו, ולחלופין בהטמעת השיטה ופחות בבחינה של הסיכונים שלה.

החשיבה הטבעית של בני האדם בזמן היצירה הנה חיובית ולכן נוצר מצב שבו ניתן לראות שההטמעה של המוצר לאחר הפיתוח שלו הפכו להיות ממוקדי שיווק, ואחוז ההשקעה במניעת הכשלים מסתכם במה שחובה לעשות לפי חוק.

אני טוען שההבנה שייצור נכון משמעותה הטמעה של הליכי ההגנה על המוצר כבר בזמן הפיתוח שלו, ולא רק בחינה של עמידות המוצר לאחר סיום הייצור.

מוצרים פיזיים

כאשר ישנו כשל שיטתי במוצר פיזי פעמים רבות הצעד שיידרש הנו Recalling וזאת במיוחד לאור המצב כיום שבו חברות מוחרמות כאשר מתברר שהן הסתירו אינפורמציה על הכשל, או שפרסמו אותו מאוחר מידי. מוצרים פיזיים לרוב מאופיינים בחברה שעומדת מאחוריהם ולכן קל יהיה למצוא את האחראי לתקלה ולתבוע אותו במידת הצורך.

הבעיה החמורה יותר הנה כאשר יצרנים רבים מתחילים לייצר מוצר שלאחר ההטמעה השיטתית שלו ללא בדיקה של כלל הסיכונים נוצר מצב שבו מתברר שהוא עלול לאיים על הצרכנים. כדוגמה לכך ניתן לראות את הטלפונים הסלולריים שלמרות כל האיומים שפורסמו לאורך השנים, בלתי ניתן למנוע את הנזקים של הקרינה שלהם, אם אכן קיימת כזו ומאחר שההטמעה שלהם כה רחבה הסיכוי שיתמודדו אתה בהצלחה מעורר סימני שאלה על הסיכוי שלנו כמשתמשים כצרכנים וכחברה להתמודד בהצלחה עם ההשלכות של המצב החדש, שבו יש בעיה שהפיתרון שלה הוא לא להשתמש במוצר יותר כפי שאנו רגילים כיום.

לא נראה לי שניתן כיום לתבוע את ממציא השיטה של השיחות הסלולריות, וגם אם כן, האם ראוי מוסרית לתבוע את מי שהמציא מוצר שכה רבים משתמשים בו?

מוצרים פיזיים ממוחשבים

כאשר מדובר במוצר פיזי שהכשל השיטתי שלו משלב חומרה ותוכנה אנו נקבל מצב שבו יש להחליף חלקים, ובו בזמן לעדכן תוכנה. דבר זה הנו כאב ראש לוגיסטי מאחר שצריך פיזית להגיע אל המוצר ולהקדיש לו זמן יקר ומשאבים כלכליים לא צפויים.

במצב זה ניתן לראות שוב שההצלחה של המוצר שהתפתח גלובלית מהווה את הגורם לכך שהעלויות של התיקון שלו הנן יקרות פי כמה ממוצר שהתפוצה שלו הנה מקומית.

לאור זאת מובנת השאלה האם מוקדשת מספיק מחשבה בזמן פיתוח מוצרים לכשלונות הבלתי צפויים שלהם.

תוכנת Skype

תוכנת סקייפ נבנתה כך שכאשר משתמש נכנס אליה נשמרים הנתונים שלו במחשב האישי לצורך חיסכון של זמן בסנכרון מול שרתי החברה בזמן ההתחברות למערכת, ומאחר שנתוני כל המשתמשים נשמרים על המחשב ללא הצפנה נוצר מצב שבו יומן שיחות ונתונים רגישים אחרים כמו הודעות אישיות נשמרים על המחשב.

מאחר שתפיסה זו שבה נתוני הלקוח נשמרים גם על שרתי החברה וגם על המחשב האישי שלו המשיכו עם החברה לאורך זמן, הרי שגם כאשר הוטמעה התוכנה במכשירים אחרים (Skype Wifi Phone, Smart Phones), התפיסה של החברה נשמרה ולאור זאת גם נשמרו הכשלים שלה כשיטת עבודה.

מאחר שניתן לגשת לנתוני הלקוח הנשמרים ללא אופציית שינוי וללא כל סיסמה נוצר מצב שבו ניתן היה לגשת לנתוני לקוח מכל מחשב שאליו התחבר. במצב זה לקוח שבחר להשתמש בתוכנת סקייפ בקפה אינטרנט השאיר את כל ההיסטוריה של החשבון שלו, ואנשי הקשר יחד עם ההודעות ששלח ויומן השיחות במחשב הציבורי.

גם במחשבים שבהם ישנו מחיקה של נתונים חדשים בכל הפעלה של המחשב נתוני התוכנה לא נמחקו, והלקוח מצד שני לא יכל למחוק מתוך התוכנה את נתוניו האישיים שנשמרו על המחשב, ואילו הגדרות המחשב מנעו ממנו לגשת בצורה ישירה לתיקייה שבה הנתונים מאוכסנים (דבר שניתן היה לעקוף ע"י גישה לתיקיות דרך חיפוש ממוקד במחשב, או עקיפת הגדרות הניהול).

מספר שנים לאחר מכן החברה הטמיעה את התוכנה במכשירים חכמים, וכך שוב ניתן היה לגשת לפרטים של הלקוח דרך התוכנה שנוהגת לשמור נתונים ללא הגנה ותוך הצפנה חלקית במידה וקיימת. (נסו לגשת לתיקיות של התוכנה במכשיר החכם שלכם).

פיילוט של חברת דואר ישראל

חברת דואר ישראל הכניסה לפיילוט בשנת 2008 מתקנים אוטומטיים לחלוקת חבילות. הבעיה במתקנים אלו היתה שלקוחות הופנו למתקנים תוך שימוש בברקוד בלבד כמזהה לצורך איסוף החבילה. למרות שבמתקנים הייתה אופציה של הכנסה של קוד אישי בנוסף להצגת הברקוד של ההודעה מהדואר על חבילה, נוצר מצב שעקב כך שמדובר בפיילוט לא נמסרו ללקוחות קודים אישיים וכך כל אדם שהחזיק בהודעה מהדואר יכל לקבל את החבילה, וזאת ללא שימוש בקוד אישי.

מאחר שניתן לגנוב בקלות את ההודעות על דואר רשום ניתן היה בקלות לאסוף גם את החבילה עצמה. ממקרה זה ניתן להבין שבזמן פיילוט יש חלון זמן אופטימלי לביצוע חדירות למערכות ולכן כדאי לאטום תקלות מראש ומצד שני ניתן למצוא בעיות רבות במערכות רגישות דווקא בזמן הפיילוט שלהן.

<u>חדירה שיטתית לאתרים דרך נתונים חד חד ערכיים</u>

ישנם נתונים אישיים שכאשר הנם מופיעים במערכות ניתן להשתמש בהם כדרך שיטתית לחדירה קלה לאתרים שפרסמו נתונים רגישים של לקוחות או עובדים. הכלל הוא שככל שהנתון יותר ייחודי מציאה שלו באתר אינטרנט לאחר סריקה שלו תביא למציאת נתונים רגישים נוספים.

לדוגמה: הסבירות שאדם יפרסם מספר טלפון שלו באתר אינטרנט הינה גבוהה, אך לעומת זאת מספר תעודת זהות הנו נתון שאם נמצא חברה שמפרסמת אותו באתר האינטרנט שלה (לרוב באתרים לא גלויים), אנו נמצא לרוב נתונים רגישים נוספים על לקוחות אחרים, וכנראה גם פרצות נוספות. חיפוש באינטרנט של תעודות זהות מקומיות יכול להביא בקלות למציאה של פרצות אבטחה וזאת מאחר שנתוני תעודת הזדהות הנם חד ערכיים, ואם נמקד את החיפוש באתרים ישראליים נגיע לתוצאות מעניינות (שילוב של מנוע חיפוש חכם ומאגר מידע כדוגמת אגרון).

<u>פיילוט של מערכת לווין בנקאית</u>

בזמן הטמעה של מערכת בנקאית לביצוע פעולות מרחוק במערכת מחשב מובנת, היה חלון זמן שבו לא נדרש קוד אישי ולכן כרטיס אשראי בנקאי היה כלי לביצוע פעולות ללא הגנה על הלקוח.

<u>טלפון ציבורי להתקשרות לבנק מהסניף</u>

שיטה שאומצה על ידי בנקים רבים, שבה ניתן היה להתקשר לבנק מהבנק עצמו תוך שימוש בטלפון סטנדרטי שממנו ניתן היה לבצע פיענוח קל של תעודת הזהות והסיסמה בעזרת הקשה על כפתור החיוג החוזר, ולאחר מכן חדירה לחשבון הבנק של הלקוח האקראי האחרון.

<u>שיטה לשימוש בדיסקים להעברת נתונים בריאותיים</u>

במערכות בריאותיות רבות ישנה שיטה שבה הפציינטים מקבלים את נתוניהם האישיים (בדיקות רנטגן) על גבי דיסקים ולאחר מכן נותנים אותם לבדיקה של גורם נוסף (רופא אישי). ניצול של שיטה אנושית זו

יכול להביא למצב שבו תהיה החדרה קלה למערכת הבריאותית על ידי דיסק נגוע שיוחדר למחשבי קופת החולים. (שיכפול דיסק דיגיטלית וחיצונית תוך ותוספת סוס טרויאני)

הסקת מסקנות

משקלול של הדוגמאות שהזכרתי ניתן להבין שבזמן פיילוט ניתן לתקוף בקלות מוצרים טכנולוגיים רבים ולכן ראוי לתת את הדעת להגנה טובה יותר על מוצרים בשלב קריטי זה. בנוסף כאשר ישנו כשל של שיטה שמאומצת על ידי גורמים רבים תיקון שלה לא יסתכם מ-Recalling של מוצר אחד אלה בטיפול שיטתי ומערכתי בשיטה כולה.

מבחינת כשלים איתור של כשל שיטתי במערכות גלובליות יהיה מטרה נעלה, אך מעבר לכך איתור של מוצר שבו יש כשל משולב של חומרה ותוכנה שהוטמעה בחברות רבות ומיוצרת על ידי יצרני חומרה שונים או אז הפתרון לכשל יהיה מסובך ויתכן שיבחרו להתעלם ממנו עקב העלויות הרבות.

דוגמת הדיסקים במערכת הבריאות הנה דוגמא לשיטה אנושית שניצול שלה לרעה יכול להיות בעייתי במיוחד, ולכן יש לשים לב גם לחיפוש של כשלים בשיטות פעולה אנושיות לא פחות מחיפוש של כשלים במערכות שגורמי אנוש יצרו.

על הכותב

אמיתי דן חוקר סוגיות אבטחה תוך התמקדות בכשלים של מערכות פיזיות ,וזאת מתוך מטרה לספק לכשלים אלו פתרונות במידת האפשר.