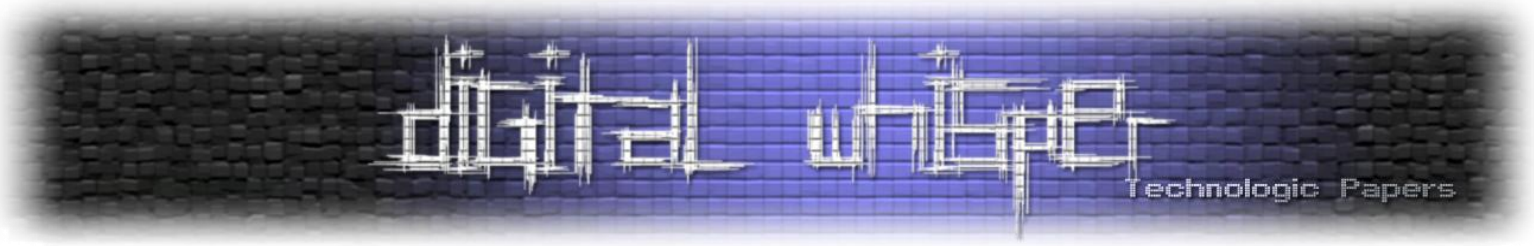

הענן והמידע שלך

מאת עו"ד יהונתן קלינגר

הקדמה

על סף יומן של המכונות התבוניות, מחשוב ענן מביא לעידן חדש בעיבוד מידע. מחשוב ענן, ככלל, הוא שם סל למספר שירותים שונים, החל מאחסון מרוחק, שירותי עיבוד ומחשוב ושירותי מכונות וירטואליות. המשותף לכל שירותים אלה, כאשר הם פועלים בקונפיגורציית "ענן", הוא שהם אינם מאוחסנים, בהכרח, בנקודה מרכזית אחת אלא בדרך כלל מבוזרים סביב מספר מקומות שונים, כאשר המטרה היא לצור שרידות והסתלמות גבוהה. כך, לדוגמא, עסק קטן יכול להקים את אתר האינטרנט שלו ולדעת שאם הביקוש לכח מחשוב יגדל, שירותי הענן יוכלו לגדול יחד עמו. בצורה אחרת, כל אדם יכול להשתמש בשירותי גיבוי מרוחק על מנת לשמור את המידע שלו בצורה שתשרוד גם אם מחשבו יאבד, ויכול גם להשתמש באחד מעשרות השירותים המאפשרים לו להפעיל מחשבים וירטואליים על מנת לבצע פעולות חישוביות.

הענן כיום מחזיק יותר ויותר מידע, כאשר בעלי המידע ונשואי המידע מאבדים שליטה פיזית עליו. אם בעולם הישן המודל היה שמידע על נשוא המידע מוחזק על ידי ספק השירותים, אשר עיבד את המידע והביא אותו למשתמש הקצה, מודל הענן מאפשר לספק השירות להחזיק את המידע עבור משתמש הקצה בחצרים של צדדים שלישיים. לצורך הדגמה קצרה כאן, אנו נשוחח על שירות Dropbox כדוגמא, אבל היכן שדרופבוקס כדוגמא תכשל, נעבור למקומות אחרים.

בקצרה, דרופבוקס הוא שירות גיבוי ושיתוף קבצים אשר מגבה את המידע שלך על שרתי Amazon's S3 ברקע ובצורה אוטומאטית; דרופבוקס מאפשרים לך, אם יש לך מספר מחשבים, לחלוק תיקיות בין המחשבים האלה; ואם אתה עובד עם מספר אנשים, הרי שהם מאפשרים לך לחלוק תיקיות עם אותם אנשים, כאשר כל שינוי מתעדכן אוטומאטית אצל כל הצדדים. דרופבוקס יושבת על כר פורה של פוטנציאל ועשויה להניב 100 מיליון דולר בהכנסות השנה וגייסה לא מעט כסף. השירות, שבניגוד לחלק ניכר מהמתחרים, מאפשר סנכרון בין מערכות הפעלה שונות ובין מכשירים שונים, לרבות אפליקציה סלולרית שמאפשרת גישה לקבצים.

דרופבוקס גם משמשת לשימושים לא סטנדרטיים, החל משימוש משני לשיתוף קבצים, דרך החלפת מערכות Subversion ואפילו בתור מערכת מעקב. אלא, שכשאשר אתה מתקין את דרופבוקס, אתה משתמש לפחות בספק שירותי ענן (CSP) נוסף ואתה כפוף לתנאים שלו.

אחסון משותף, מחשוב משותף, שליטה משותפת [כלומר: הבעיה]

כעת, למי יש שליטה על המידע שלך? מדיניות הפרטיות של דרופבוקס מעידה ש"דרופבוקס משתפת פעולה עם ממשלות ורשויות אכיפת חוק וגורמים פרטיים על מנת לאכוף ולציית לחוק. אנו נגלה כל מידע אודותייך לממשלה או רשות אכיפת חוק או גורמים פרטיים כאשר אנו, לפי שיקול דעתנו הבלעדי, נאמין שהדבר נחוץ או הולם כדי להשיב לטענות או הליכים משפטיים". כמו כן, ממדיניות הפרטיות של Amazon S3 מסבירה ש "אנו משחררים מידע על החשבון ומידע פרטי אחר כאשר אנו מאמינים ששחרור זה הולם כדי לציית לחוק; לאכוף את תנאי השימוש שלנו והסכמים אחרים". כלומר, הן אמאזון והן דרופבוקס יצייתו לרשויות אכיפה ויספקו מידע אם צו בית משפט יאמר להן לעשות כן. בכלליות, זה דבר טוב.

אלא, שלעיתים הכלליות הזו לא ממש שורדת. הבה נקח דברים ברפופורציה. נאמר שאני יצרן לימונדה ולי יש סוד מסחרי: המתכון; אני מאחסן אותו בתיקיית הדרופבוקס שלי, כיוון שאני נדרש לתת גישה למספר עובדים ואני רוצה גיבוי מאובטח. כעת, המתחרה הגדול ביותר שלי רוצה גישה למתכוני הלימונדה. הוא ניגש לבית המשפט עם עורך דין סביר ומקבל צו אנטון פילר (צו המרשה לו לתפוס את נכסי, בין אם מוחזקים על ידי או על ידי צד שלישי, כיוון שהחשש הוא שאני אבריח אותם אם אגלה על המשפט); הצו ניתן על סמך טענותיו שאני גנבתי את המתכון ובית המשפט פוסק, במעמד צד אחד כי דרופבוקס צריכה לתת לו גישה לקבצים שלי. זה נעשה כיוון שטענות המתחרה שלי היו שדרופבוקס עצמה מחזיקה את הקבצים. דרופבוקס מקבלת עותק מהצו ולא יודעת כיצד לנהוג: היא לא מסוגלת להבין האם אני הבעלים המקורי של הקובץ או גנבתי אותו ולכן היא מספקת גישה לקובץ למתחרה שלי: צו הוא צו.

ישנם שני הבדלים משמעותיים במקרים בהם אני אוחז במידע וכאשר ספק השירותים אוחז בו, וככאלה ההבדלים מסבירים את הבעייתיות בשימוש באחסון בענן למידע רגיש: (1) אם אני הייתי מחזיק את החומר, הרי שהוצאה לפועל של כל צו היתה חייבת להעשות בידיעתי על קיומו של הצו כיוון שהקבצים היו מאוחסנים בחצרי ותחת שליטתי [לעניין זה, ראה לדוגמא את רע"א 1810/10 PCIC נ' קפלן, בו ספק שירותי אירוח נתבקש לחשוף תוכן של דואר אלקטרוני של אחד מלקוחותיו בלי ידיעתו]; (2) לספק השירותים יש אדישות רציונאלית לחשיפת המידע שלי, שכן אם לא יעשה כן הוא עשוי להיות אחראי על תוכן המידע. בתי משפט בישראל פסקו במספר מקרים כי השתתפות פעילה ואינטרס באי הסרת תוכן

לאחר ידיעה מקימה אחריות בנזיקין לתוכן הקבצים [כך, לדוגמא, א 176992/09 אתי אברמוב נ' אביב פרנקל, א 32986/03 בושמיץ נ' רפואה]. כלומר, אם אתה מפרסם מידע בענן, אתה בסיכון שהמידע הזה עשוי להיות בשימוש על ידי צדדים אחרים.

השאלה היא האם הדבר אפשרי? כלומר, האם אותו ספק שירותי ענן יכול לגשת לקבצים שלך. בוא נאמר, שעל פי חוק, תנאי השימוש של דרופבוקס מתירים שימוש כזה של ספק השירותים וספקי שירותים אחרים (כמו גוגל) כבר נדרשו לגלות כתובות IP של משתמשיהן (א 4854/07 ברלומנפלד נ' גוגל) וחסמו גישה לחשבונות במקרים אחרים. מעבר לכך, דרופבוקס עיצבה (ונראה את דרופבוקס, כזכור, כדוגמא) את הארכיטקטורה, יש לה את היכולת לשחזר את הקבצים שלי ואת סמאתי, כך שהיא תמיד יכולה לעקוף את מנגנוני האבטחה המקובלים.

אבדן הריכוזיות

כפי שאנו רואים, כאשר מדברים על ספקי שירותי ענן אנו יודעים שהשליטה חייבת לעבור משחקן אחד למספר שחקנים מבוזרים, כאשר לכל אחד יש את היכולת לעבד את המידע. היכולת הזו דרושה כי כל אחד מספקי השירות צריך גישה לקבצים על מנת לספק את השירותים לשמם הוא נשכר. על פניו, ספק שירותי הענן נחשב כגורם צד שלישי שמחזיק את המידע או מעבד אותו, לצורך טיפול בהנחיות הפרטיות, הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים הוציאה טיוטת הנחיות מסוימת על עיבור מידע במיקור חוץ שספק אם רוב שירותי הענן עומדים בה.

על פי ההנחיות, אם אנו מחזיקים מידע רגיש על צדדים שלישיים, וחלק ממנו מאוחסן בענן עלינו לברר שספק שירותי הענן מציית למדיניות פרטיות ששומרת על המידע הפרטי של אותם צדדים. לדוגמא, אם אני עורך דין, עליי ליידע את דרופבוקס שאני עורך דין ושכל המידע שנמצא בתיקיית הדרופבוקס שלי מוגן על ידי חסיון עורך-דין: לקוח כך שאם יתקבל צו אנטון פילר אלה יסרבו למסור את המידע ויגנו עליי. מעבר לכך, עליי לוודא שספק שירותי הענן לא יגלה מידע, פרטי, אישי או רגיש לכל גורם שלישי בלי הסכמתי.

להגן על עצמך מספק שירותי הענן

כיצד אדם יכול להגן על עצמו מספקי שירותי ענן? בצורה תיאורטית, יש מספר הצעות לאחסנה מוצפנה בענן, לדוגמא "Cryptographic Cloud Storage" [ע"י Kamara et al], ואפילו פתרונות יותר מעשיים כמו Tahoe-LaFS, אלא שהם עדיין לא אומצו על ידי השוק העסקי. ההצעות התיאורטיות טרם מומשו ועדיין לא

ראינו דרך הגיונית כדי להצפין מידע על הענן. ההצעה של קאמרה וחבריו היא, בכלליות, ש"לפני שמידע מועלה לענן, אליס משתמשת במעבד המידע כדי להצפין ולקודד את המסמכים לצד המטא-מידע שלהם (תגים, זמן, גודל וכדומה) ואז היא שולחת אותן לענן. כשהיא רוצה להוריד מספר מסמכים, אליס משתמשת ב-TG כדי לייצר טוקן ומפתח שפותח את ההצפנה".

אופציה טכנולוגית נוספת שמוצעת היא להצפין את כונני המכונה הוירטואלית או להשתמש במערכות מוצפנות כמו SFZ להצפנה בענן. האופציה השלישית היא להשתמש בתוכנת הצפנה כמו TrueCrypt על האחסון בענן שלך (כמו דרופבוקס); אלא, שפתרון מסוג זה עשוי להיות מאוד בעייתי כיוון שדרופבוקס לא יכולה לגשת למערכת הקבצים שלך ויכולה לא להיות מסוגלת אלא לגבות את כלל הקבצים בכל פעם ששינוי קטן ביותר מוכנס לקובץ; מה גם שפתרון מסוג זה לא יאפשר שחזור של קובץ בודד אלא של כלל מערכת הקבצים.

גישה שונה יכולה להיות על ידי Secret Sharing. Secret Sharing (שיתוף סוד) היא גישה קריפטוגרפית בה הגישה למידע מוגבלת רק למצב בו מספר אנשים מתוך מספר גדול יותר מעוניינים לגשת; כך, לדוגמא, אפשר לאחסן את המידע על מספר שרתים שונים כאשר לכל שרת יש חלק מהקובץ (או חלק מהמפתח הקריפטוגרפי בלבד) (כך מוצע, לדוגמא, על ידי Recursive Secret Sharing for Distributed Storage and Information Hiding [ע"י Parakh et al])

אלא, שפתרונות מסוג זה הם תיאורטיים גם כן ועדיין לא יושמו בארגונים או שירותי אחסנה כחלק אינטגרלי מהשירותים שלהם (אולי חוץ מזה).

פתרונות

כעת עלינו לדון בפתרונות גם כן. אנו צריכים לקיים מערך קשיח של כללים להגדיר מערכת אחסון בענן כמוטת פרטיות: הדרישות שלנו היא שספק שירותי הענן יאפשר:

- אינטגרציה תמידית לקבצים, גם באופליין וגם באונליין.
- אינדקס וחיפוש בקבצים.
- שיתוף הקבצים או חלק מהם עם גורמים שלישיים.
- דיווח מלא על כל גישה לקבצים, הן מורשית והן לא מורשית.

שימוש במערכות קבצים מוצפנת עונה על שלושה מתוך ארבעה הקריטריונים: גישה, אינדקס ודיווח. אלא, שכדי לחלוק את המידע עם צדדים שלישיים הגישה למערכת הקבצים צריכה להיות מנוהלת על ידי ספק

שירותי הענן (במיוחד לצורך שיתוף קבצים ראו: Secure, Dependable and High Performance Cloud Storage [ע"י see Y unqi Ye et al]) הפתרון האחר הוא להצפין כל קובץ בצורה שונה (עם מפתחות סימטריים לכל קובץ, כך שאין בעיה עם שיתוף של הקובץ); אלא, שבשיטה כזו אנו מאבדים אחד מהקריטריונים: או שלא נוכל לחפש בקבצים או שנצטרך להחזיק מאגר מרכזי של מפתחות. לכן, כדי לקבל מערכת מוצפנת אנו עומדים בפני משוכה קשה למדי.

עדיין, אם נניח, שההצפנה היא סימטרית ושכל מתחם משותף בין משתמשים מקבל מפתח סימטרי שונה, אנו לא יכולים להגדיר את הפתרון כאינטגרציה תמידית, כיוון שכדי להפוך קבצים מפרטיים לציבוריים צריך לבצע את ההמרה במחשב של המשתמש ולא על השרת (כמו כן, אנו עדיין צריכים שרת מפתחות שיטפל במידע).

לכן, אם נקח את הפתרון של עדי שמיר לשיתוף סוד (How to share a secret [ע"י Shamir]) שאגב מצליח בשני עמודים להסביר בעיה כל כך מסובכת על ידי פתרון אלגנטי, משהו שחריג ונדיר בתחום של מדעי המחשב) ולצורך הפתרון נגדיר את הסף היעיל לגישה למפתח כשותף סוד אחד (1), אנו נגדיר את התיקיות המשותפות כבעלות שלושה מפתחות קריפטוגרפיים (אחת לתיקיה אשר תשותף על ידי מישהו ואחד לכל משתמש) בצורה כזו שכל משתמש יוכל לכתוב לתיקיה ולקרוא ממנה בצורה אינטואיטיבית ללא כל בעיה, הן אונליין והן אופליין, היא יוכל לחפש ולייצר אינדקס באמצעות מפתח ההצפנה שלו (והמפתח השיתופי) ולשתף את המידע עם כל גורם שלישי.

יישום של מערכת שיתוף סוד מסוג זה (שעדיין לא נבדקה בפועל) עשויה לייצר פרטיות מוגברת וגמישות של שיתוף המידע דרך רשתות ומשתמשים.

הפתרון היחיד שקרוב לכך הוא הפתרון שמוצע על ידי Tahoe-LaFS, ונמצא בפיתוח [ערך ויקיפדיה]; היישימות של השירות עדיין אינה מוחלטת, והוא מבוסס על אחסון על ידי משתמשי הקצה (ובכך מייצר ענן לא מבוזר) ולא אצל ספקיות אחסון רבות. במצב כזה, הוא לא עומד בדרישות השרידות הרציניות לדעתי (אלא אם יאחסנו אותו אצל ספקית אחסון רצינית אחת לפחות).

מסקנות

טרם הוטמע פתרון טכנולוגי לבעיה המשפטית האמיתית של פרטיות במתחם המעונן מול ספקי השירות. האבדן הלא דרוש של שליטה כאשר מידע מאוחסן בענן, במיוחד על מידע רגיש במיוחד, הוא צפוי עקב הגבלות ארכיטקטורה, כח מחשוב ועיבוד, רוחב פס ובעיות שונות.
פתרונות מעשיים קיימים ודורשים טרחה מועטה, כאשר מודל מבוסס הצפנה יכול להיות מיושם במהרה כדי לאפשר אחסון של מידע על שרתים מרוחקים (לדוגמא, ענן) כאשר ספק השירות לא יכול לגשת לקבצים אך בעל המידע יכול לשתף אותו עם צדדים שלישיים אחרים.

אלא, שעד ליום זה לספקי השירות יש תמריץ שלילי כיום שמונע מהם לספק שירותים מסוג זה, בין היתר בעקבות עלויות רבות יותר, חוסר שליטה על הנעשה בחצריהם ועוד סיבות רבות. סביר להניח שעד שנושא זה לא יגיע לבית המשפט או עד שעסק גדול דיו לא יאלץ לנייד את המידע שלו לענן, אנו לא נראה פתרון טכנולוגי יישים וסופי.