Technologic Papers

אינטרנט לא חברותי

נכתב ע"י עו"ד יהונתן קלינגר

הקדמה

לפני בערך שבע שנים ניסחתי מניפסט הקורא לאינטרנט אלחוטי בחינם כשירות ציבורי; הסברתי את דעתי כי צריך לחייב את הממשלה לספק אינטרנט אלחוטי חינם לציבור, ולאפשר קיום בכבוד על ידי הפחתת עלויות, שיפור התשתיות ושיתוף. מאז ועד היום קרו הרבה דברים: קודם כל, מחירי הרשת ירדו בצורה משמעותית בגלל התחרות בשוק ורפורמות בשוק התקשורת. היום, אינטרנט ביתי (ספק ותשתית) עולה פחות ממאה שקלים בחודש, ומגיע בקצבים יותר מסבירים. שנית, הפתחות הרשתות הסלולריות גרמה לכך שיותר ויותר אנשים יהיו מחוברים לרשת באמצעות הטלפונים הסלולריים שלהם. אך, במקביל, קרו כמה בעיות: הראשונה היא שחרור תוכנות כגון Firesheep שגרמה לאדם הפשוט להבין כמה הוא חשוף, והשניה היא התפתחות של שירותים כמו WeFIFon , והאינטרנט החברתי של בזק, שמאפשרים שיתוף של החיבור הביתי.

בטקסט הקצר הזה, אני רוצה לדון בסכנות ובבעיות בשיתוף הרשת הביתית, ולהסביר מדוע דעתי לא השתנתה, אבל עדיין צריך למצוא פתרון טכנולוגי טוב יותר.

על מה כל הרעש?

קודם, נדון בנושא של FireSheep, שנדון לעומק כבר על ידי: כאשר אנחנו גולשים בחיבור אינטרנט אלחוטי שאינו מוצפן קורה משהו מיוחד: כל מי שמחובר לרשת יכול להתחבר ולראות בדיוק מה אנחנו מעבירים (עם חריגים קטנים, לא רלוונטי כרגע אבל), לאן אנחנו גולשים ואפילו לבצע התקפת Man In The Middle ולהעתיק את כל התעבורה שלנו. הדבר אומר שאם אני מתחבר באמצעות אחד השירותים החברתיים לרשת אלחוטית פתוחה, הרי שבאותו המקרה אני לא מצפין את המידע שלי, וכל אחד יכול לקרוא אותו. כלומר, אם נדבר לרגע על האינטרנט החברתי של בזק (למרות שהוא רק דוגמא, כי גם בחיבור אינטרנט במלונות יש בדיוק את אותה הבעיה): נניח שהתחברתי, הכנסתי את שם המשתמש והססמא שלי כדי לאמת את הזהות שלי, ואני גולש לנוחותי. מאותו רגע, כל מי שיתחבר לרשת (גם אם הוא לא יצליח לתת שם משתמש וססמא, אלא רק להתחבר אליה) יוכל לדעת מי אני, לאן אני גולש ואפילו לחטוף את ה-Cookies שלי ולהזדהות בשמי מול אתרים אחרים.

כלומר, השימוש ברשתות לא מאובטחות הוא מאוד בעייתי למשתמש הקצה: יש סכנות של פרטיות (כל אחד יכול לדעת לאן אתה גולש) ושל אבטחת מידע (כל אחד יכול לדעת מי אתה ואיך אתה מזדהה). זה הסוג הראשון של הבעיות; המינוי אולי פחות, אבל הסביר יותר. וזה הסוג שימנע מאנשים להשתמש בשירותי אינטרנט חברתי למינהם.

הסוגיה השניה, הבעייתית יותר, היא של הלקוח שבוחר לשתף את האינטרנט שלו. הדוגמא היא, שוב, של בזק, אבל היא לא רלוונטית אלא רק הדגמה. בזק טוענת כי החיבור באמצעות שם משתמש וססמא מאפשר לזהות את מי שהשתמש בשירות, אם היה שימוש לרעה כיוון שהמידע נאגר בשרתיה של בזק; אבל הדבר לא ברור ולא מצאתי דוקומנטציה מלאה של השימוש. אבל: נניח שאדם משתף את הרשת האלחוטית שלו, הרי שכל מי שמתחבר יכול להשתמש בה כדי לעשות פלאים לא חוקיים: החל מהורדה של חומר פדופילי, דרך שיתוף קבצים לא חוקי והרצת מניות, ועד פרסום טוקבקים בבלוגים שיהיו לשון הרע. אם יתקבל תזכיר חוק חשיפת גולשים שמאפשר לזהות גולשים אנונימיים, הרי שמה שיקרה כאן הוא מאוד בעייתי: דמיינו שאדם יקבל תביעה על סמך כתובת ה-IP שלו, וזאת כאשר הוא השאיר את הרשת שלו פתוחה למשתמשים.

אגב, במשפט הפלילי קיים כבר חוק נתוני תקשורת (חוק סדר הדין הפלילי (סמכויות אכיפה - נתוני תקשורת)) שמאפשר למשטרה ולעוד שורה של רשויות לקבל את המידע הזה, על זהות המשתמש. על סמך חוקים דומים, היו כבר טעויות בעבר בחו"ל. לדוגמא, בשנת 2011 אדם שהשאיר את הרשת האלחוטית שלו פתוחה נחשד בהורדת פורנוגרפיית קטינים; רק לאחר בדיקה פורנזית מעמיקה של המחשב שלו, התגלה שהוא דובר אמת, והדבר מעולם לא קרה.

זו, כמובן, לא אנקדוטה. גם בישראל היה סיפור דומה: בעניין עא 1806-09 רבקה פלח (בייבי פלוס) נ' שירותי בריאות כללית נדונה השאלה האם ראוי לחשוף גולש אנונימי. אותו מקרה קדם להחלטת בית המשפט העליון בעניין רמי מור שקבעה כי אין דרך חוקית לחשוף גולש (רעא 4447/07 רמי מור נ' ברק אינטרנט). אבל, שם קרה משהו מעניין: כתובת ה-IP אותה ביקשו לחשוף היתה שייכת לשירותי בריאות כללית; זו, מצדה, הסבירה לבית המשפט כי אין לה רישום של מי התחבר לרשת שלה. בית המשפט לא ממש היה קשוב, והורה לה לחשוף את המידע בכל מקרה. כך גם עשוי לקרות היום, במכשירי אינטרנט חברתיים.

אבל האחריות של מי שמפעיל את הרשת היא בעייתית: לדוגמא, בגרמניה בשנת 2010 התקבלה החלטה שבצורה אפקטיבית אוסרת על שימוש ברשתות פתוחות בדיוק בשביל הסיבה הזו: לזהות את כל מי שהתחבר. כלומר, השיטה הגרמנית היא שאם אי אפשר לזהות, אסור להתחבר בכלל לרשת.

שתי הבעיות המקבילות כאן: של העדר הפרטיות ושל הסכנות למפעיל הרשת ידועות לכל הצדדים, ולמרות זאת הם ממשיכים להפעיל רשתות. לכן, השאלה המעניינת היא מדוע אנשים ממשיכים להשתמש בהסדר הלא יעיל הזה ולא מחפשים פתרון טוב יותר, ומעבר לזה: מדוע חברות מסחריות כמו בזק או Fon

(שעכשיו טוענת שבזק העתיקה ממנה) ממשיכות לרכב על זה ולא מזהירות את גולשיהן מהסכנות? הפתרון לשאלה כזו אינו חד-משמעי, אבל נובע מהעדפה של נוחיות על גבי פרטיות, והיא בעיה שאנו חיים עמה כל היום.

חוק המספרים הגדולים

את המונח Shoulder Surfing לא צריך להסביר. מדובר על התנהגות שבה אדם אחד מציץ למסך של חברו שנמצא בקרבתו, וזאת רק כיוון שאותו אדם אינו מאבטח את מסך המחשב שלו בצורה ראויה והמסך בוהק מספיק. כולנו מודעים לבעיה הזו ולכן גם כולנו מכירים את תסמין "הפרחה ברכבת" שמדברת על הסודות האישיים ביותר שלה בטלפון הסלולרי בקולי קולות. כולנו יודעים שאם אנחנו עושים משהו במרחב ציבורי, אין לנו ממש יכולת לשלוט על מה שאחרים מגלים, אבל אנחנו עדיין עושים את זה. לכן, לעיתים תמצאו בבתי קפה פגישות סתרים, אנשים שעובדים על פרויקטים מסווגים או מאובטחים, בגידות של בני זוג ועוד. ההנחה שלנו היא שאף אחד לא מחפש מידע, ולכן הוא לא מעניין.

מה שאנחנו לא יודעים (או רוב האנשים לא יודעים) זה שהיכולת לכרות מידע קיימת. כלומר, לאף אחד באמת אין רצון להכנס לחשבון ה-Facebook שלך. זה לא מעניין אף אחד איפה אחיך נפש בסוף השבוע, ואיפה האקסית מהתיכון מבלה היום; אבל: בקבוצה גדולה יחסית זה כן מעניין, כי המידע המצטבר מאפשר לבצע פעולות רבות. אנשים לא מניחים שאפשר לצבור כך את המידע ושאפשר להשתמש בו, ולכן הם מתעלמים. בדרך כלל, כאשר אני מציג לאנשים את הסכנות בגלישה ברשת לא מאובטחת, הם אומרים לי "אז מה יש לי כבר לפחד מזה?" כאילו אין להם מידע פרטי.

מנגד, בעלי בתי הקפה שמשאירים רשתות פתוחות (או בכלל עסקים, מקומות בילוי, לימודים וכדומה) אינם מודעים לסיכונים המשמעותיים: רובם אינם מבינים שאפשר בקלות יחסית לנסות להטיל עליהם אחריות על שיתוף קבצים שנעשה במסגרת המתחם שלהם, או יותר מזה: שיכול להיות שפעילות לא חוקית שמבוצעת מאצלהם תוביל לפגיעה בפרטיות של כל הגולשים שם.

יש פתרון?

עכשיו, איך פותרים את בעיית המודעות הזו, כאשר מנגד יש קמפיין של 'רשת חברתית' שמעודד שימוש ברשתות לא מוצפנות? הרי הפתרון של "לפרוץ כדי להוכיח" הוא לא חוקי ולא יעיל; לא תמיד אדם יודע שהחשבון שלו נפרץ. הפתרון צריך להיות גמול למי שמאבטח את הרשת שלו, ומייצר ענישה חלקית לרשתות לא מאובטחות. בתיאוריה, הפתרון עבורי, בתור אזרח, היא להתחבר הביתה באמצעות SSH כאשר אני מגיע לרשת לא מאובטחת, ואת המשך החיבור לעשות דרך הבית. הסיבה לכך? חיבור כזה

מאבטח את התקשורת ומונע ממי שיושב לידי להאזין לי. החסרון? כמובן, שאם אתה יודע להגדיר פרוקסי בבית, אתה כנראה לא צריך לקרוא את המאמר הזה. פתרון נוסף הוא להשתמש בתוסף הדפדפן HTTPS Everywhere שמכריח חלק ניכר מהאתרים הגדולים לעבוד בצורה מאובטחת. אבל עדיין: לא מדובר על פתרון מושלם. מעבר לזה? אין הרבה דרכים לשמור על עצמך.

הפתרון בצד השני, של בתי הקפה שנותנים אינטרנט בחינם, הוא להרים Firewall עצמתי ובעייתי, שיחסום כל תעבורה שהיא לא סטנדרטית. כלומר, לפגוע ביכולת של הלקוחות לבצע פעילות של שיתוף קבצים, התחברות לשירותי FTP או P2P, הורדות מאסיביות שמפרות זכויות יוצרים. הבעיה היא, שגם פתרון כזה הוא לא הרמטי: הוא לא מונע ממני לכתוב תגובה מבישה באתר חדשות שמוציאה לשון הרע, או פוגעת בפרטיות, והוא לא מונע בצורה הרמטית את האפשרות שמישהו יוריד חומר פורנוגרפי מהרשת. לכן, גם שימוש כזה הוא בעייתי.

פתרון אחר הוא להפעיל שירות מעקב, שפותר אולי את הבעיה הראשונה (של שימוש לרעה ללא אחריות) אבל מגדיל את החשיפה לבעיה השניה (פגיעה בפרטיות): כלומר, אם בית קפה מסוים יעקוב אחר כל הגולשים שלו, וישמור מידע כמו כתובת MAC (הכתובת הפיסית של כרטיס הרשת), מידע מזהה אחר כמו שם המשתמש בפייסבוק וכדומה, זה ירתיע אנשים מלעשות שימוש לא ראוי, אבל זה גם ירתיע אנשים מלהשתמש ברשת, בהתחשב בכך שהמידע הזה נשמר.

כלומר, אין ממש דרך הרמטית להגן על רשת אלחוטית בכל אחד מהצדדים, ומדובר על הסכם של אמון: אותו הסכם של אמון שנובע מכך שכשלקוח מגיע למסעדה ומזמין מזון, לא מבקשים ממנו לשלם מראש. מניחים שאם הוא הגיע, התיישב והזמין, אז יש לו את הכסף. ההנחה הזו בעייתית: היא בעייתית כי הנזק מאי תשלום חשבון (שיכול להגיע לכמה מאות בודדים של שקלים, במקרה הרע ביותר) אינו מתקרב בסדרי גודל לנזק האפשרי שיכול להגרם משימוש לרעה ברשת האלחוטית.

האמון הזה מבוסס על פיסות מידע שאנחנו חושבים שיש לנו: אדם שמשלם בכרטיס אשראי מותיר אחריו פיסת מידע קטנה של זהות, כך גם מצלמות 'אבטחה' שמותקנות באותו בית קפה. אבל מה קורה כשהאדם כלל לא מגיע לבית הקפה, אלא יושב בדירה למעלה ומשתמש בחיבור האינטרנט של בית הקפה כדי לצרוך תכנים לא חוקיים או פורנוגרפיה קשה? האם במצב כזה בית הקפה חי מאותו אמון? אני בספק.

לסיכום

הפתרון צריך להיות אחר: או להגדיר נקודות חיבור כאלה כ'ערי מקלט', כמו אתרי תוכן גולשים, או לסגור אותן לגמרי. הגדרה כערי מקלט משמעה כי כל תחנה שתסומן כתחנת אינטרנט פתוחה לא תהיה אחראית לשימושים שנעשים בה בדיוק כמו שאתר כמו תפוז אינו אחראי לתוכן בפורומים. במצב כזה, יחסכו מראש ההליכים המשפטיים, אבל העולם ידע שכל נזק שיגרם משם עשוי להשאר ללא סממן.

אבל זה בדיוק כמו בעולם האמיתי: גם בעולם האמיתי יש מקרים שלא מותירים ראיות, שלא ניתנים לפענוח. האקר תמיד יכול לקפוץ דרך חמישה או שישה מחשבים בדרך ולא להתגלות (ומה לעשות, ההצגה בסרטים הוליוודים של הדרך בה מזהים אותו אינה ממש נכונה).

וזו בדיוק הבעיה שצריך לטפל בה: עד עכשיו יש לנו לא מעט אנשים שמנצלים לרעה: גם אם הם עומדים בצד ואף אחד לא מכיר אותם; הבעיה היא שכשנותנים אינטרנט חברתי, או שכשמשתפים את הרשת, אף אחד לא יודע בדיוק מה קורה שם. את הסכנות האלה אנשים שוכחים, ואומרים "מה כבר יקרה לי". ואם לא יהיו אנשים שיזכירו להם את הסכנות, אנחנו נשאר בבעיה.