digital whisper
Technologic Papers

פרסום חולשות - איך עושים את זה נכון?

מאת עו"ד יהונתן קלינגר

הקדמה

אז גיליתם פרצת אבטחה בשירות, תוכנה, מערכת, כור אטומי או מטוס סילון. המדריך הקצר הזה נועד עבורכם כדי להבין מהו תהליך Vulnerability Disclosure; תהליך אותו צריך לקחת כדי לגלות איך לפרסם פרצת אבטחה בצורה אתית, ושלא תגרום לכם לסיים את התהליך בכלא או בחובות קשים. שימו לב שבכל מקרה שבו גיליתם פרצת אבטחה משמעותית, אני ממליץ שתעזרו בעורך דין שיספק לכם ליווי צמוד לצורך הפעילות הזו, כיוון שלא אחת חברות שגילו על קיומן של פרצות ניסו לסתום אותן על ידי שימוש בעורכי דין שעמלו על השתקת חוקר האבטחה, ולא על ידי שימוש במתכנתים לתקן.

אז בוא נתחיל ב"מה לא לעשות אף פעם?"; כלומר, אם אתם הולכים לקרוא רק 200 מילים מהטקסט הזה, בבקשה תקראו את הפסקה הזו. אף פעם, אבל ממש אף פעם, אל תפנו לבד בצורה מזוהה לחברה שגיליתם אצלהם פרצה ותגידו להם "או שתשלמו לי מאה אלף שקלים או שאני מפרסם את פרצת האבטחה באינטרנט". מדוע? כי תהליך כזה עשוי להקרא "סחיטה באיומים"; והוא, על פי סעיף 428 לחוק העונשין, כזה: "... [ה]מאיים על אדם לפרסם או להימנע מפרסם דבר הנוגע לו או לאדם אחר, או מטיל אימה על אדם בדרך אחרת, הכל כדי להניע את האדם לעשות מעשה או להימנע ממעשה שהוא רשאי לעשותו, דינו - מאסר שבע שנים". כלומר, אם אני פונה לאדם מסוים, ואומר לו "אני יודע עלייך משהו, ואם תשלם לי אני לא אפרסם אותו", זו סחיטה באיומים.

לכן, המסקנה היא שאם גילית פרצת אבטחה, לבקש כסף עבור אי פרסום שלה זה פשוט הדבר הלא נכון לעשות. מכאן אפשר להתקדם לדיון ברצינות. המדריך הזה מבוסס על כמה טקסטים שחשוב שתקראו, בינהם המדריך של ה-EFF על נושאים שקשורים לחשיפת פרצות אבטחה, המדיניות של CERT בכל הנוגע לגילוי פרצות אבטחה, המדיניות של מיקרוסופט, ועוד כל מיני דברים שיוזכרו בהמשך.

למי המדריך הזה לא מיועד?

המדריך הזה גם לא מיועד לכל מיני חושפי שחיתות בעיני עצמם שחושבים שיהא זה אתי לפרסם פרצות Zero Day בפומבי בלי לתת לחברות את האפשרות לתקן את הפרצה, או לאנשים שרוצים לסחור בפרצות כאלו ולהרוויח כסף. המדריך הזה מיועד רק, ואך ורק, לאנשים שמעוניינים לדעת מה לעשות כאשר הם גילו פרצת אבטחה ולא רוצים להסתבך מבדרך שבה הם מגלים אותה לציבור ולאנשים הרלוונטיים.

עכשיו קחו בחשבון שיש עוד אנשים טובים שהמדריך הזה לא מיועד להם, וזה כאלה שמשתתפים בתכניות כמו Zero Day Initiative או Pwn2Own שמשלמות כסף טוב למי שכן מצליח למצוא פרצות. במצב כזה, יש הסכם מסחרי. גם בפרויקטים של קוד פתוח שמנוהלים עם Bug Tracker אפשר לדווח שם על הפרצות.

מתי אתה לא יכול בכלל לדבר על פרצות אבטחה שגילית?

התשובה הברורה היא כאשר יש לך הסכם סודיות עם החברה או כאשר היא המעסיק שלך. כלומר, אם אתה עובד במקום מסוים וגילית פרצת אבטחה, אתה צריך ללכת בצינורות המקובלים קודם כל. במצב שבו עובד יחליט לפרסם מידע של המעסיק שלו, אם הוא חתום על התחייבות לסודיות (וככל הנראה גם אם הוא לא), אשר עשויה לגרום לנזק למעסיק. בית הדין לעבודה פסק (בהקשר של סעיפי אי-תחרות, אולם) כי "תקנת הציבור היא שלא יהפוך העובד ל"סוס טרויאני" אשר בא בחצריו של מעסיקו - ויצא ממנו ונתח בידו" (עא 189/03 גירית נ' אביב).

מעבר לכך, בהתחשב בכך שעובד אשר מועסק בחברה חייב בנאמנות למעסיק, הרי שאלא אם מדובר במקרים בהם ישנה סכנה ברורה ומיידית לציבור, הרי שהעובד כלל אינו יכול לפרסם מידע החוצה (וראו סיכום יפה ב-EarthWeb, Inc. v. Schlack, 71 F. Supp. 2d 299 - Dist. Court, SD New York 1999, שדן בעיקר בסוגיית האי-תחרות).

מעבר לכך, אם אתה עובד עבור חברה ומספק שירותי תוכנה כאשר יש לך חובת סודיות, כדאי מאוד שתבדוק את ההסכמים ותתיעץ עם עורך דין לפני שאתה ממשיך בגילוי פרצות אבטחה.

איך לדווח על פרצת אבטחה?

אז קודם כל השאלה איך מדווחים על פרצת אבטחה. מתחילים את השאלה בשאלת משנה של האם לדווח קודם לציבור או קודם לחברה הנפגעת. התשובה לכך, בדרך כלל, היא שכל עוד אין סכנה מוחשית לחיי אדם או למערכות מחשב קריטיות בכך שהפרצה לא תחשף עכשיו, וכל עוד אין חשש שהפרצה כבר בשימוש של אחרים, כדאי לשקול קודם כל להתחיל עם החברה הנפגעת.

כאן צריך להחליט אחד משלושה דברים: או לפנות לבד, ובעילום שם, או לפנות בשמך המלא, או לפנות באמצעות גורם מתווך (כמו עורך דין). בלי קשר לאיך שהחלטתם לפנות, צריך לוודא שהתווך עד לחברה הנפגעת הוא לאדם הנכון בחברה. במצב כזה, כדאי לא להתחיל ב"גיליתי פרצת אבטחה, היא כך וכך, וזהו" אלא להתחיל בלהציג את עצמכם (בין אם על ידי המוניטין שלכם או על ידי מסמכים אחרים) ולספר על התחום שהבעיה נמצאת בו, לוודא שהאדם שהגעתם אליו הוא האדם הנכון בארגון (ולא כזה שידליף החוצה) ולראות שהוא אמין.

אחר כך, אני ממליץ, כדאי להחליף מפתחות PGP בין הצדדים. מדוע? כי אם פרצת האבטחה היא באמת רגישה, אז לא כדאי שמישהו בדרך יוכל לקרוא את הפרצה, נכון?

אחרי שמעבירים את הפרצה, כדאי לשמור על קשר עם החברה ולשאול אם אפשר לעזור.

חשוב מאוד, בשלב הזה, לא לעשות שני דברים: (1) לא לבקש כסף על גילוי הפרצה, ו(2) לא לבקש גישה לעוד מערכות כדי לחפש פרצות נוספות.

עכשיו, כדאי מאוד לחכות ולראות איך אפשר לעזור.

כמה זמן לחכות?

השאלה היא "לחכות למה?". אם לא קיבלתם תשובה להודעה הראשונה (זו שאין בה את הפירוט של הפרצה) בתוך שבוע, אני מציע שתבדקו אם היא בכלל הגיעה ליעד, ונסו שוב. הסיבה לכך, היא שאתה לא רוצה ללכת ולשחרר פרצה לעולם בלי שבדקת שהסיבה היתה שההודעה שלך נפלה לתיקיית הספאם של מישהו אחר.

עכשיו, אם הגעתם לשלב השני (שלחתם פרצה) ולא שמעת או ראיתם כלום במשך חודש, אז אולי כדאי להתחיל לנג'ס.

אם הגיעו 45 ימים, שזה המועד שרוב שאר החברות מציינות במדריכים שלהן (וזו הסיבה היחידה לדבוק לכך) ואף אחד לא ענה לכם (אחרי שפירטתם את הפרצה, לא לפני) אז אולי כדאי שתשקלו לעשות משהו אחר.

אחר כך, אם לא נתנו לי תשובה, איך לפרסם?

השאלה 'איך לפרסם?' היא שאלה שאין לה תשובה חד-משמעית. התשובה בדרך כלל היא "בזהירות", או "בזהירות מרובה". המחשבה צריכה להיות שאם יש דרך שאפשר לפרסם בה בלי לסכן אנשים קיימים, אז כדאי לעשות זאת. בואו נקח לדוגמא את החשיפה של ISE מלפני מספר חודשים, שמצאה מספר פרצות אבטחה רציניות בראוטרים. הדוגמא כאן היא בכוונה דוגמא קיצונית, כי ISE צרפו להדגמה שלהם קוד להרצה בכל אחד מהראוטרים כדי לחשוף את פרצות האבטחה עצמן, לדוגמא לראוטר הביתי שלי, יש לשלוח קוד HTML ולבצע השתלטות באמצעות CSRF, להפעיל אדמיניסטרציה מרוחקת ולתת גישה לשרת ה-FTP על הראוטר.

עכשיו, הדוגמא הזו היא רעה במיוחד כי היא מספקת בתוך החשיפה כבר את הקוד כדי לנצל את הפרצה.

דוגמא הרבה יותר טובה לאיך כן צריך לחשוף היא כזו שמספקת Proof of Concept, בה ניתן לראות את הפרצה, ניתן להבין איזו חולשה נוצלה, אבל אין בהכרח את הקוד המחייב כדי להשתמש בה. כלומר, אם אתה כמו קוסם טוב על הבמה, שלא מגלה את הטריק שלו למרות שכולם יודעים מה השיטה, אתה יכול גם למזער נזקים. דוגמא נכונה (לפחות חלקית) היא הדרך בה פורסמה פרצת האבטחה בחייגנים של Samsung לאחרונה. החוקר הצליח להדגים כיצד הפרצות עובדות וזאת בלי להציג בפני הציבור את קוד המקור; הדבר אפשר תיקון מהיר של פרצת האבטחה בלי לסכן את הציבור יותר מדי.

זכור, המטרה שלך כחוקר אבטחה היא לא לאפשר לאחרים להשתמש בפרצות האבטחה, אלא לגרום לכך שהן יסגרו. הסיבה היחידה שצריכה לגרום לך לפרסם פרצות אבטחה היא אם החברה שמנהלת את המוצר לא הסכימה לתקן פרצת אבטחה לתקופה מסוימת, עד כדי כך שזה מסכן את הציבור.

אם דורשים ממני לחתום על הסכם סודיות, מה לעשות?

ובכן, כאן השאלה היא מה המטרה שלך. אם המטרה שלך היא ליידע את הציבור ולוודא שהתקלה תעלם, אז ככל הנראה שלחתום על הסכם סודיות לא יהיה אופטימאלי אלא אם הפרצה תסגר. אם הפרצה נסגרה, ואתה נדרש לחתום על הסכם סודיות, כדאי מאוד שתוועץ בעורך דין.

אם אתה מרגיש שמנסים לרמוז לך בעדינות שאם לא תחתום אז ככל הנראה צפויה נגדך תביעה, אז ברור שהגיע הזמן להתייעץ עם עורך דין.

בגדול, חתימה על הסכם סודיות אינה דבר פסול: היא נועדה להבטיח את האינטרס של החברה שמידע כזה לא יגיע למתחריה ולא יגיע למי שרוצה לפגוע בחברה. אבל, צריך לזכור שכל עוד אתה לא עובד של החברה, ואתה עושה את מה שאתה עושה מתוך תפישה של טובת הציבור, אז צריך לשקול את השיקולים האלה בזהירות.

ומה אם אני רוצה כסף?

בגדול? הולך לחפש מדריך אחר. כלומר, היו מקרים שחוקרי אבטחה קיבלו כמה שקלים על מציאת פרצות; והיו מקרים שהם הועסקו אחר כך, אבל צאו מנקודת הנחה שאם אתם רוצים למכור פרצת אבטחה אז יש שווקים הרבה פחות הגונים לכך.

אז בואו נסכם

בשלב הראשון לפנות לחברה, בצורה מנומסת ולהציע את העזרה בפתרון. לא לבקש כסף, אף פעם, לא משנה מה, גם לא אם זה נראה לכם לגיטמי. אם לא עונים, לנסות שוב, אולי במקום אחר, אולי בטלפון. אם הכל מצליח, נהדר. אחרי שזה קרה, ואחרי שהכל בטוח תוקן, תפרסמו מה שאתם יכולים או רוצים, וגם אז בזהירות. אם לא הצלחתם לשכנע אותם לתקן, אז חכו לפחות 45 ימים, דברו עם עורך דין ותבדקו איך אפשר לחשוף בזהירות.