פותחים לך את התיק כשאתה נכנס לצ'ק פוינט / מורן סרף

מאמר לשבוע: 8.4.2003 – 15.4.2003

צ'ק פוינט והישראליות

צ'ק פוינט הפכה בשנים האחרונות למותג ישראלי. הירקן המשתמש עדיין בחשבונייה עם ניירות, אולי לא יודע להגיד שצ'ק פוינט היא חברת אבטחת מידע, אבל הוא יודע להגיד שיש שם הרבה מאד כסף, ו..כן שזה קשור למחשבים. לפני שמתחילות הפרסומות בערוץ שתיים במהדורת החדשות מראים לו לרגע את חמש המניות הישראליות הנסחרות בבורסה. שניה לפני שהוא קם לשירותים הוא רואה 'חץ למעלה' והרבה מספרים ליד המילה צ'ק פוינט. זה מספיק כדי שיבין שמשהו טוב קורה עם החברה הזאת והוא מרגיש גאה. זאת גם החברה שלו. הוא ישראלי והוא מכיר מישהו שמכיר מישהו שעובד שם. זה טוב.

ברדיו מדי פעם בגלי צה'ל יש פרסומות לתוכנית רדיו בנושאי כלכלה – 'פותחים לך את התיק כשאתה נכנס לצ'ק פוינט ?'. נכון – צ'ק פוינט זה מחסום באנגלית... ופותחים את התיקים במחסום... לא בטוח שהקשר לאבטחת מידע ולאופן הניהול המתוחכם נהירים לו – אבל זה לא משנה. כאמור – העיקר כאן זה תחושת הישראליות. זה התחיל איפשהו בצבא. מדובר בכמה חברים שהתחילו בקטן במרפסת של סבתא, והיום הם מצליחים בכל העולם... ובארה'ב. בכירי החברה מדברים עברית, והמוצר נכתב על ידי 'צבא קטן וחכם' ולא על ידי מפעל רב-מימדים. זה מה שכולנו מרגישים כשאנו מתארים את עצמנו. זוהי הישראליות.

בתקשורת מדי פעם מזמינים את בכירי החברה להגיב על המצב הכלכלי בארץ. על נושאים הנוגעים לבטחון אישי. החברה עוסקת הרי באבטחת מידע, אז למה שלא נשאל מה דעתם על השמירה בגני הילדים, האבטחה באל-על, או היכולת של טילי פטריוט להגן מפני טילים לא-קונבנציונאליים. 'הרווחתם הרבה מאד כסף בשנה שעברה ממכירת מוצרי אבטחת מידע, אולי תוכלו להציע לנו פתרון לקצבאות הסעד לזקנים בישראל ?'...

צ'ק פוינט הפכה לסממן להצלחה בכל תחום הקשור באופן כזה או אחר למילים שאנו מכירים הנוגעות לתחומי העיסוק של החברה. עכשיו נשאר רק להבין מה בדיוק הם עושים שם....

עובדות

חברת צ'ק פוינט קיימת כעשר שנים. תלוי את מי שואלים. תלוי איך סופרים.

מן היום שבו התחילו המייסדים בעבודה, מהיום שהונפקה בבורסה האמריקאית, מהיום שהפכה בעיני עצמה מחברת סטרט-אפ קטנה לחברה גדולה. התשובה הרשמית בכל אופן היא שהחברה קיימת משנת 1993.

החברה מונה כאלף ומאתיים עובדים. מרביתם בישראל. מרכז הפיתוח הוא בישראל, והמרכז הנוסף של החברה שוכן בארה'ב. הראשון ברמת-גן, והשני בקליפורניה. די בזה כדי לעורר גאווה. ניתן כמובן למצוא נציגים וסניפים קטנים של החברה במגוון רחב של מדינות נוספות בעולם.

המוצר הראשון שאותו ייצרה החברה – 'פיירוול-1' – הפך לסמל המזוהה עם החברה יותר מכל. בשנים האחרונות כבר זכתה החברה להוציא מגוון רחב של מוצרים נוספים הפונים לנישות רבות שאליהן לא פונה המוצר האמור, אך ככל הנראה לעד ייזכר מוצר האבטחה הראשון כסמלה של החברה. באתר החברה ניתן למצוא את מגוון הפרסים ותעודות ההוכרה שלהן זכתה החברה בעולם. אחד החשובים שבהם ככל הנראה הוא בחירת הפיירוול לאחד מן המוצרים המובילים של העשור שעבר (בשורה אחת עם ווינדווס NT, למשל). לוגו החברה הוחלף בשנה האחרונה, אך הציור המלווה אותו מלמד רבות על החברה. בשונה מן הציורים המלבניים, הטכנולוגיים, המוכרים, המלווים את מרבית חברות התוכנה המוכרות – סימלה של צ'ק פוינט דומה יותר לציור ילדים של מחשב ורשת בתוכו. יש בזה אמירה.

גילוי דעת

עד לפני שנה עבדתי בחברת צ'ק פוינט. השנתיים בחברה היו עבורי מן החשובות והמהנות שהיו לי בעולם התוכנה. עבדתי בתור המדריך של אנשי הפיתוח. קרי – כאשר אנשי הפיתוח נדרשו לידע מסויים, בדרך כלל ידע שקשה יותר לרוכשו בקורסים הרווחים בשוק, שעניינו טכני הרבה יותר, והוא נוגע לפרטים הפנימיים בהם מעורבת הארכיטקטורה של המוצר – היו הללו פונים לאחד מן

מהיכרות החברה אם כן ניתן לומר דבר אחד בוודאות: הרשמים שתיארתי לגבי אופייה המצליחני של החברה בידי הקהל הרחב - נכונים. זה לא רק רושם שיש לגבי הקומקום, זה גם מה שיש בתוכו. מרבית המיתוסים המצליחנים שדבקו בחברה נשענים על אמיתות מוצקות. זהו אחד מאותם מקומות שעונים על הציפיות מהם.
זה היה 'המסביב'. עכשיו הגיע הזמן לפנות לאימי.

פרק בשביל אמא

יותר מהכל חשוב לי במאמר הזה להסביר לאמא שלי – שידעה משך שנתיים שאני עובד בצ'ק פוינט, וידעה לספר על כך בגאווה לירקן שלה – מה בדיוק עושים שם. את שני המשפטים שניתנים בכל כתבה על צ'ק פוינט היא כבר קראה. אני לא בטוח שזה עוזר לה להבין מה זה בדיוק פיירוול. תוכנת הגנה. בסדר. אז מה הם עושים שם כל כך הרבה שעות ביום ? הגיעה העת לספק תשובה.

הדוגמא השכיחה בקורסי אבטחת מידע לשימושו של פיירוול היא כאותו שומר סף בכניסה למועדונים.

השומר עומד לצד הדלת ובידו רשימה. מגיעה בחורה. השומר מביט בה במבט חטוף, ומביט בדף שבידו. כתוב שם: 'בחורה בעלת שער אדום, עיניים ירוקות, המגיעה מנתניה – הכנס', 'בחורה בעלת שער שחור, עיניים ירוקות, המגיעה מתל-אביב – אל תכניס', 'בחור שמן, מקריח, נמוך, המגיע מאשקלון – הכנס'. וכך הלאה.
השומר מביט בבחורה. היא בעלת שער אדום, עיניה ירוקות. הוא שואל מניין היא מגיעה ?' – 'נתניה'. – 'את מוזמנת להיכנס'.
השומר עוקב אחר הרשימה שבידו ומזהה אחד אחד את כל המנסים לעבור דרכו. לצד כל אדם המופיע ברשימה בתיאור זה או אחר מופיע ההרשאה – להכניס או לא. אם הגיע השומר לתחתית הרשימה ולא מצא כל חוק החל על האדם שלמולו, הוא בוחר בכלל ברירת המחדל – לא להכניס.
הפיירוול פועל בדרך דומה. אדם מסויים נדרש ראשית להגדיר אוסף – לפעמים גדול ביותר – של כללים כאלו. מידע שמגיע מרשת האינטרנט, נכנס לתוך הארגון שלי, ומנסה לפנות לשרת הדואר – חסום, מידע היוצא מתוך הארגון שלי – העבר, וכך הלאה. הפיירוול ניצב בתווך בין הארגון כולו ובין העולם החיצון – לרוב האינטרנט – ובודק כל פיסת מידע המנסה להיכנס, *או לצאת*. לא אחת משתמשים ארגונים בפיירוול גם כדי לחסום את הגישה החוצה מן הארגון. שומר הסף יכול גם למנוע את היציאה מן המועדון. 'בחור שרירי וחסון, הגר במטולה, נושא את נגיף ה- SARS - אל תאפשר לו לצאת.

איך עושים את זה ?
הטכנולוגיה – אך שהיא נראית מסובכת לרבים – מושתתת על עקרונות פשוטים למדי. צורות התקשורת באינטרנט היום בנויות על פרוטוקולים מאד מסודרים של מידע. קשה מאד לחרוג מן הפרוטוקולים ולהיות מסוגל לדבר עם מישהו. כל שעל הפיירוול לעשות הוא להכיר את מרבית הפרוטוקולים הקיימים, ולדעת לחלץ מתוכם את הפרטים הנוגעים למידע שאותו הם נושאים. בדרך כלל הפרטים המעניינים ביותר דומים לפרטים הנמצאים על חבילת דואר. כתובת המקור, כתובת היעד, שם המען, שם השולח, תוכן החבילה. די באוסף מצומצם ביותר של פרטים כדי להיות מסוגל לאתר את החוק המדוייק שניסחו מבעוד מועד ולהחליט אם להעביר את החבילה – אם לאו.
זהו מוצר אחד של החברה. מוצר הדגל. מתברר שכבר לא די במוצר כזה בעולם האבטחה של ימינו. העולם מורכב מדי.
העסק מסתבך. תחילה הספיק לנו להשאיר את הרעים בחוץ ואת הטובים בפנים. שומר הסף הפריד בינינו ובינם. אנחנו כאן – הם שם.
עכשיו אין זה מספיק. רבות מן החברות – כאמור, צ'ק פוינט היא דוגמה לכך מחזיקות במגוון רחב של מסונפות. מרכז בקליפורניה, ומרכז בישראל. עכשיו נניח שעובד החברה בקליפורניה רוצה להעביר מידע לישראל. אם נאפשר את הכניסה על ידי התרת הכניסה לארגון אנו מאפשרים מחד למישהו להתחזות לברנש מקליפורניה, וגרוע מכך – אנו מאפשרים לכל אחד להיות מסוגל להזיק למידע מקליפורניה עת הוא עושה את דרכו לארגון. לא די בכך ששני המועדונים מוגנים על ידי שומר סף. אנחנו צריכים גם שחבילה כלשהי הנשלחת ממועדון אחד לאחר לא תיזוק בדרך. אם הברמן בלילנבלום שולח וודקה לברמן באלנבי – אנחנו צריכים להיות בטוחים שבדרך אף אחד לא מהל את זה במים – רחמנא ליצלן.

מה נעשה. נשלח את הוודקה כשהיא נעולה. כל דבר שייצא ממועדון אחד ויישלח אל האחר יינעל על ידי שומר הסף האחד, וייפתח על ידי שומר הסף השני. זהו העיקרון הבסיסי של VPN – רשת אישית מאובטחת .

ה-V מוסיף אך המושג 'וירטואלית' – הרשת לא חייבת להיות כזה שהיא באמת אישית. מספיק שבאופן וירטואלי היא אישית, נוכח האבטחה שנשכין בה, כדי שהיא תהיה טובה לנו. אם ישתמשו שני השומרים ברשות הדואר של ישראל, אבל יוסיפו מנגנון הגנה משלהם לחבילות בדרך הרי שהם משתמשים ברשת שבבסיסה אינה מאובטחת לצורכם, כדי לממש מעליה את האבטחה שלהם.

איך עושים את זה ?

הצפנה. שומר הסף – הפיירוול מכיל עתה מרכיב נוסף היודע להצפין את המידע היוצר מן הארגון. כאמור, כל מידע שנכנס ויוצא מן הארגון עובר תמיד דרכו בדרך. הוא אוסף את המידע הזה ומצפין אותו. עתה כשעובר המידע באינטרנט בדרכו אל היעד בצידו השני של הגלובוס איש אינו מסוגל להביט בו.

הוודקה בהכרח לא תימהל.

למעשה ההגדרה הנכונה של VPN היא כזו שלא די לה בכך שהמידע עשה את הדרך כאשר הוא לא פוענח על ידי איש, אלא גם בכך שאם הוא שונה – ולו במעט – נוכל מייד לדעת שנעשה כזה שינוי, ושהמקבל יוכל לוודא שמקור המידע הוא אכן מקור לו ציפה. אנחנו רוצים שאם הוודקה נפתחה בדרך – נוכל מייד לראות שהפקק אינו חתום, ולדעת שהיא עשויה להיות מהולה, ואנחנו רוצים לוודא שמקורו של בקבוק עלום שאנחנו מקבלים הוא אכן המועדון השכן, ולא מדובר בבקבוק חתום שנשלח אלינו מן המועדון המתחרה, כשהוא חתום, אך מכיל תרכיז אחר.

יש המשך

כפי שתיארתי בעיה נוספת שיש צורך לפתור אותה לבד מן הצורך הבסיסי להגן על המועדון שלנו מפני העולם הרחב – קיימות עוד מגוון רחב של תופעות וצרות שנובעות מן ההגנה. נהוג לטעון בעולם האבטחה שנוחות וקלות שימוש במוצרים האבטחה הן תחליפיות להגנה שמספקים המוצרים. ככל שההגנה טובה יותר – כן קשה יותר להפעיל את המערכת, מכיוון שיש מגוון רחב של פרמטרים שיש להתייחס אליהם. מכיוון שצ'ק פוינט נותנת היום מענה בעזרת מגוון רחב של מוצרים נוספים שאותם לא הזכרתי למרבית בעיות אבטחת המידע הקיימות, גם כמות המוצרים ומורכבותם רק הולכת וגדילה. מה קורה אם יש לנו מועדון שהשומרים בו מתחלפים בתדירות רבה, כיצד נוכל למנוע מצב בו המערכת תפעל לאט ביותר נוכח ריבוי החלופות ? מה קורה כאשר יש לך אדם שאינו נמצא במועדון אחר, מוגן על ידי שומר סף, הרוצה לשלוח לך וודקה. אתה רוצה לאפשר לו זאת – אבל אין לך שומר שיעטוף את החבילה במערכת ההגנה. מה תעשה אם יש לך רשת של מאות מועדונים – כאשר על חלקם חלים חוקים שונים שיש לאכוף אותם במקביל? מה קורה כאשר שומר אינו יכול לעבוד עוד – האם תוכל להשאיר את המועדון פתוח, תוך שימוש בשומר אחר שמייד ייכנס לפעולה, ויכיר את רשימת כל החוקים ? נניח שארעה פריצה לאחד המועדונים – האם ניתן ללמוד על מאפייניה בעזרת תיעוד המאורעות שקדמו לה ? מה קורה כאשר אדם שלפי החוקים רשאי להיכנס נושא עימו דבר-מה שאותו לא נרצה להכניס ? מה עם בעלת השער האדום, והעיניים הירוקות מנתניה מחזיקה בתיק שלה פצצה ? האם התנאים יאפשרו לה להיכנס עכשיו ? אולי נרצה שהשומר יוציא את הפצצה, ורק אז יאפשר את הכניסה.... בקיצור – שיבדוק את התיק כשנכנסים לצ'ק פוינט.

עולם אבטחת המידע הוא רחב. ככל שהטכנולוגיה מתפתחת יותר הופך השוק לגדול ומורכב יותר. טלפונים סלולריים מאובטחים, רשתות ביתיות מאובטחות, טלויזיה מאובטחת. כל דבר שמתחבר היום לעולם צריך בשלב זה או אחר להיות מאובטח. עתידה של צ'ק פוינט נראה מאובטח גם הוא.

הפן הישראלי ביותר, אולי, ברעיון של צ'ק פוינט הוא בעצם העובדה שהקשר אסוציאטיבי העצוב בין מוצר החברה והקורות במערכת האבטחה של ישראל. העובדה שבכל יום אנו שומעים על הקורות במחסומים – הצ'ק פוינט. העובדה שבדיקת התיק בכניסה לקניון היא הדוגמא הראשונה שניתן להציע כאלגוריה לבדיקות שעושה הפיירוול. למעשה – במובן הפשוט ניתן לומר שמרבית הישראלית בילו שעה זו או אחרת בצ'ק פוינט. במחסום ארז, או מסביב לירושלים. כולנו יודעים להסתכל על החוקים שניסחו לנו ולהחליט לפיהם עם לאפשר את הכניסה או לאו. זוהי הישראליות. עשרה חודשים אתה כותב פיירוול, וחודשיים אתה בעצמך פיירוול.

לפחות נקווה **שבנקודה** (Point) מסויימת כל אחד יזכה גם לראות משהו מהצ'ק.