תגובה למטה הסייבר – מוצגת בפני חברות הסייבר במכון היצוא

א. מנהלה

מטה הסייבר שפרסם את סדרת ההגבלות החדשות הציג שני מועדים שאינם חופפים למתן תגובות. במכתבו של רועי ירום מופיע תארים 3.3.16 ואילו בתוכן המסמך עצמו מופיע תאריך 7.2.16. לכאורה טעות סופר בפועל חשוב מאד לוודא מהו התאריך הנכון על מנת לייצר תהליך תגובה ולא סתם מסמך תגובה.

תהליך תגובה כולל קודם כל מפגש עם מטה הסייבר על מנת לבחון מהם הנושאים הניתנים להגמשה ורק לאחר מכן להוציא מסמכים ולפעול להשגת ההגמשות. אם המועד הוא 7.2.16 למעשה אין מספיק זמן למצות תהליך של תגובה.

ב. חיבוק הדוב

אין ספק שמטה הסייבר הוא בעל הברית הטוב ביותר של מרבית חברות הסייבר בישראל. ההכרזות האחרונות שהיו בכנס שנערך בבורסה רק הוכיחו עד כמה ניתן להבנות מתוך התמיכה של מטה הסייבר. אבל, מטה הסייבר אינו חברה עיסקית ואינו יכול לראות את הדברים מראיתו של המפתח והיצואן. ואכן המחויבות של מטה הסייבר בהגבלות החדשות ממחישה עד כמה זה עלול להיות חיבוק דוב.

כל חברת סייבר מתמודדת עם 2 בעיות שיווקיות כבדות: למצוא את הלקוח הראשון ולמצוא את הלקוח הראשון מחוץ לישראל.

זרועות הביטחון השונות של ישראל היו במשך שנים הבחירה המוצלחת של הלקוח הראשון (או בין הראשונים). ההגבלות החדשות יוצרות מצב שבו אם זרועות הביטחון יהיו הלקוח הראשון הם גם יהיו הלקוח האחרון משום שלאחריו כל יצוא יהפוך לבלתי אפשרי.

ג. OPEN SECURITY

ההתמודדות בפשעי ובפוגעני הסייבר היא כבר מזמן לא נחלתה של חברת סייבר כזו או אחרת וגם לא של מדינה כזו או אחרת. המגמה הרווחת בקרב חברות הסייבר היא לשתף מידע ולזהות חולשות כדי שכולם יוכלו להתגונן בצורה מיטבית. כל אחד בהתאם לכלים שלו. הדבר משותף לכל החברות הישראליות מצ'קפוינט ועד לאחרון הסטארטאפים שעדיין לא נרשם ברשם החברות. כולם מעונינים לשתף מידע כדי להתחרות בעיצוב ופיתוח הכלים ולא בזמינות המידע. דווקא החברות הצעירות הן אלו שמציפות כלים ודרכים חדשות לזיהוי חולשות ופוגענים ולאחר מכן כלל החברות יכולות להתמודד איתם.

ד. ואסנאר

אמנם ישראל היא אחת מ-41 המדינות שחתמו על ההסכם המקורי (שההגבלות החדשות אמורות להרחיב אותו). אבל לא ברור שזו חזות הכל. במקור הכוונה היתה למנוע זליגה של פתרונות התקפה כדי ש"תוקף לבן" לא יהפוך ל"תוקף שחור", אבל בפועל גם לכלי תקיפה יש ערך א) בפיתוח כלי הגנה ב) בביצוע בדיקות חדירה לאירגונים.

יש למצוא דרכים לרגולציה של השימוש בכלים אלו. אבל מניעת השיווק שלהם היא חרב פיפיות: בה בשעה שהמחקר והפיתוח של כלים אלו ידעך כתוצאה מאי-כדאיות כלכלית, כל אותם "תוקפים שחורים" ימשיכו לפתח את האמצעים שלהם ויסכנו עוד יותר את העולם. כמו כן, חברות ומדינות שלא יקבלו עליהן את ההסכם ייהנו מיתרון עסקי בלתי הוגן.

ה. פיקוח על חולשות

עידוד איתור חולשות עשוי להדמות כעידוד האקרים. בפועל, תהליך איתור החולשות בשוק בפרטי והמסחרי הוא מהלך החוסך לחברות ולארגונים סכומי כסף לא מבוטלים. לדוגמא, החוקרים הפרטיים שמצאו דרכים לחדור למכוניות BMW חסכו לחברה מילונים הן בתביעות של לקוחות והן במאמצי איתור. כך שאפילו אם התשלום עבור חשיפת הפרטים הייתה בעלת אופי חתרני, התשלום הוא שבר אחוז מהנזק שהיה עשוי להגרם לחברה.

איתור החולשות הוא לרוב גם מהלך מקדים לפיתוח כלי התגוננות ולכן שיתוף המידע (והסחר בו) הוא חיוני לקיומה של התעשייה.

יש מקום לבחון רגולציה מתאימה במיוחד לחולשות שנחשפו במשותף עם גורמי בטחון, אבל בהחלט חשוב להמשיך ולאפשר לגורמים עסקיים לספק מידע על חולשות.

ו. שיתופי פעולה

העידכון המקומם ביותר הוא ביחס לפיתוחים שהותאמו למערכת הבטחון לצורך הגנת סייבר. הכללה גורפת של כלל זה עשויה למנוע מחברות ישראליות להציע את פתרונותיהם להגנת הסייבר. מערכת הביטחון תמיד מבקשת שיפור קטן כזה או אחר ומאותו רגע הפיתוח כולו נגוע במעורבות בהגנת סייבר ומכאן חסומה דרכו ליצוא. צריך למצוא כאן דרכים דומות לדרכים שדנות בפיתוח IP (קניין רוחני) משותף.

ז. יכולות פורנזיות

קיימות מספר חברות ישראליות שההגבלות בגרסתן הנוכחית היא מכת מוות עבורן. לדוגמא חברת CELLBRITE. מוצרי החברה מופצים ברחבי העולם ומסתמכים על הנסיון שהחברה צברה אצל הלקוחות המקומיים שלה קרי משטרה וכוחות הבטחון.

ח. לסיכום

Cyber Together כארגון שיתופי של חברות הסייבר מתייצבת לימין מכון היצוא בדיאלוג עם מטה הסייבר מתוך מטרה לצמצם את המגבלות ולעגן את הדברים ברגולציה פנימית ובבקרה משותפת לחברות, למטה הסייבר ולמכון היצוא.

מטה הסייבר איננו "צד שכנגד". נהפוך הוא, מטה הסייבר הוא קטליזטור להתפתחותן של חלק מחברות הסייבר בישראל. אבל חובה על הגורמים העסקיים ומכון היצוא לשמור על האיזון העדין בין ההגבלות הגורפות לפריצת השערים. בדרך של דיאלוג נוכל לשמור על המובילות הישראל במוצרי סייבר מבלי לפגוע בחוסנה של ישראל בתחום זה.

פיקוח על הייצוא – רקע ומגמות מחו"ל

- ישנן 41 מדינות בהסכם הפיקוח [מתוך כ-200 מדינות בעולם]. כלומר, מי שלא יישם את ההסכם יקבל יתרון תחרותי.
- 125 חברי קונגרס חתמו על עצומה שנשלחה ליועצת לביטחון לאומי של ארה"ב עם בקשה לבחון את הפיקוח על הסייבר מתוך חשש שפיקוח כזה יפגע במחקר ובחוסן הלאומי של ארה"ב. **https://goo.gl/1O73dZ**
- במאי 2015 הונחה בארה"ב הצעת טיוטא לפקח על תוכנות מעקב ופריצה [" **intrusion and surveillance items**]. במקור ההצעה הייתה של בריטניה בניסיון לפקח על חברת גמא.
- הטענה העיקרית של כל החברות היא שהנוסח המוצע הוא כללי מידי ומכסה למעשה גם את תעשיית ההגנה ומוצריה, ולא באופן מסויים סט סופי של כלים מוגדרים.

מיקרוסופט

https://oversight.house.gov/wp-content/uploads/2016/01/Goodwin-Microsoft-Statement-1-12-Wassenaar.pdf

- פגיעה בפיתוח תוכנות הגנה - ההגדרה של intrusion software definition אם תשאר כמו שהיא, תפגע בפיתוח יישומים נגד-מעקב ותשפיע לרעה על היכולת לגלות פגיעויות. זו הגדרה שעוסקת בשיטות נפוצות וחיוניות בעולם התוכנה המשמשות לא רק תוכנות שעלולות לשמש ככלי תוכנה זדוני. למעשה, טכניקות אלה משמשות מוצרי אבטחת מידע, תוכנת ניהול מרחוק, אנטי וירוס, תוכנות לניטור העסק ומערכות הפעלה.
- פגיעה בחדשנות - מהנדסי מיקרוסופט הביעו חשש כי, אם יישום, יצירת עדיפות בפגיעויות יחד עם חוקרי אבטחה במרכז תגובת האבטחה של מיקרוסופט, הערכת תוכנות זדוניות ב-Microsoft Malware Protection או פיתוח כלים עם צוותי פנימיים יכול להיות תרגיל מעיק וגוזל זמן של בירוקרטיה ממשלתית, תיעוד , טפסים, ולא חדשנות.

- פגיעה ביכולת התגובה של צוותי הגנה - אנחנו רוצים שלחוקרים וחברות הגנה תהיה אפשרות להגיב בזמן אמת לאיומים. בזמן בו כולנו מחפשים להעצים את מגיני הסייבר ולספק להם הכלים ויכולות שהם צריכים, אנחנו לא יכולים לקחת צעד משמעותי אחורה.
- הסתמכות על הגדרות טכנולוגיות צרות במקום על יצירת נורמות התנהגות - הגדרה מופשטת מידי של תוכנת פריצה. במקום לנסות ולהגדיר פיקוח "תפור" שימנע כביכול ייצוא של תוכנות מעקב כמו של האקינג טים, צריך לשנות את הדיון שיתבסס על נורמות, ולא על הגדרות טכנולוגיות.
- פגיעה בתערוכות סייבר בישראל - ביפן כבר בוטלה תערוכת סייבר אחת בגלל שחברות עסקיות פחדו שחשיפת מוצרים תעבור על חוקי ווסנאר [Pwn2Own Tokyo].
- פגיעה באבטחת תשתיות המדינה - היכולת של מיקרוסופט להגן על מוצרים שמשמשים את תשתית ה-IT של ארה"ב תפגע.
- פגיעה במליוני לקוחות מיקרוסופוט בארה"ב ובעולם - למיקרוסופט לא תהיה יכולת להגן על מוצרים הנמצאים אצל מליוני לקוחות בעולם ובארה"ב.
- הפיקוח ישפיע על מספר תחומים בהם מעורבת מיקרוסופט , PT, Malware Research - Vulnerability Testing , Security Tools, Application Compatibility, Interoperability and Work-Arounds, Information Sharing, Supporting Customers, Engaging the Security Community ו-Automated Exports and Re-Exports .
- פגיעה בשיתוף מידע בינלאומי - חלק מהפעילות של מיקרוסופט כולל העברת מידע בנוגע לקוד זדוני עם מדינות שונות, לעיתים בצורה אוטומטית בזמן אמת וללא אדם בלופ.
- התמודדות עם מספר משטרי פיקוח בעולם - כחברה בינלאומית מיקרוסופט צריכה להתמודד עם רגולוצייה של הרבה מדינות. ולכן, ארה"ב צריכה להגיע להסכמה בינלאומית עם כמה שיותר מדינות לפיקוח צר ככל הניתן מאשר להשאיר את הפיקוח כמו שהוא היום בצורה מופשטת.
- העדר אחידות בפיקוח בעולם - בעוד ארה"ב [וישראל] ימנעו שימוש מסוים בתוכנה, מדינות אחרות מיישמות את הפיקוח בצורה שונה וייתכן כי אותו שימוש מסוים יהיה לגיטימי עבורן. בגלל זה דיון סביב שימוש בתוכנות מעקב צריך להעשות על הקווים של נורמות התנהגות [ולא טכנולוגיים]. נורמות בסייבר המגבילות את הסכסוך הפוטנציאלי ברשת צפויות להביא יותר יכולת חיזוי, יציבות וביטחון לקהילה הבינלאומית.

VMware

https://goo.gl/XO3Uzn

- פגיעה ביכולת לחקור פגיעויות בקוד ולשתף את הממצאים. זה יוביל לפגיעה בהגנה של המוצרים ושל הלקוחות.
- החברה משתפת נתונים עם מספר רב של יישויות בארה"ב ומחוצה לה. דרישות הפיקוח יעמיסו תקורה על החברה ויפריעו לה לשתף מידע בזמן אמת כדי למנוע התקפות. זה יתן להאקרים יתרון שידעו שידינו קשורות בהמתנה לרישיון ייצוא.
- בחלק מהמקרים שארעו בשנה האחרונה, החברה הייתה שותפה למחקר של התקפות עם חברות אירופאיות אשר דרש שיתוף של קוד זדוני. שיתוף זה אפשר למהנדסים של החברה לפתח במהירות טלאים.
- בחלק מהמקרים המהנדסים של החברה מפתחים בעצמם קוד זדוני כדי להדגים פגיעויות במוצרי החברה לצורך מחקר, הדגמה ואימון.
- אנחנו מקבלים מידע לגבי איומים לא רק מתחומי ארה"ב , אלא מהרבה מקומות נוספים בעולם. ואנחנו צריכים את הגמישות להגיב בזמן אמת למידע שמגיע אלינו. גם אם ארה"ב תתקן את מדיניותה כאן מבית, זה לא יאפשר לנו להמשיך ולקבל מידע לגבי איום קריטי ממקורות מחוץ לגבולותינו.

סימנטק

https://goo.gl/tqm8f0

- פגיעה ביכולת לשתף מידע אודות פגיעויות וקוד זדונה. לפתח מוצרי הגנה ולספק פתרונות בזמן אמת.
- זה לא פיקוח על מספר סופי של כלים מסויימים, אלא על כל עולם הסייבר. זה יפגע בכלכלה, בלקוחות האמריקאים ויתן יתרון נוסף להאקרים.
- הגבלה על מעבר של מידע.
- מחקר אבטחה מקוון יקוצץ. הפיקוח מעכב מפתחים וחוקרים בבדיקת מוצרים ורשתות ושיתוף מידע טכני על נקודות תורפה חדשות מעבר לגבולות.
- הזמינות של כלי הגנה בסייבר תהיה מוגבלת, כפי שהשלטון מגביל את היצוא של טכנולוגיות אבטחה מקוונות, אפילו לחברות בנות של חברות אמריקאיות בחו"ל.
- שיתוף הפעולה ושיתוף המידע יפגע. הפיקוח רואה את כ"מיוצא" כאשר הוא משותף עם אנשים שאינם אמריקאים, גם אם הם עובדים באופן פיזי בחברה כאן בארה"ב.
- תוכנת תקיפה דומה בבסיסה לתוכנות הגנה [אותן טכנולוגיות ו/או מנגנונים משמשים הן את ההתקפה והן את ההגנה].
- זה לא עניין של הגדרה טכנולוגיות או של רשימות כלים, אלא של צורך לזהות את הכוונה של המשתמש בכלי. [לכן מיקרוסופט טענה שוונסנאר צריך לעסוק בקביעת נורמות].
- אין יכולת מעשית לשלוט ולפקח על תוכנות פריצה ומעקב . ולכן ההסכם משתמש בהגדרות מופשטות שמכניסות את כל כלי ההגנה, השיטות והטכנולוגיות לתוך אותה קטגוריה.
- העדר יכולת לחקור פגיעויות יום-אפס ולשתף אותן או מידע לגביהן עם חוקרים אחרים בעולם, יפגע ביכולת לפתח כלי הגנה בפני איומים המתבססים על פגיעויות אלו.
- הפיקוח יפגע ביכולת של חברות תשתיות קריטיות להתגונן באופן אקטיבי בשל פיקוח על כלי PT. חברות אלו מבצעות התקפות דמה על הרשתות שלהן לצורך זיהוי חורים בהגנה ותיקון שלהם כאקט מונע.
- במקום פיקוח, ארה"ב יכולה לשים משקל על החוק הפלילי ועל סנקציות כלכליות. אלו כלים טובים יותר להרתיע מפני שימוש לא נורמטיבי בקוד תוכנה.