



סיכום מפגש שולחן-עגול
מניעת זליגת מידע DLP
מאי 2014

מנחה
סיגל רוסיין

הקדמה

לקוחות נכבדים שלום,

תודה על השתתפותכם במפגש שולחן עגול Round Table בנושא DLP – מניעת זליגת מידע ארגוני.

מצ"ב סיכום עקרי הדברים שעלו במהלך המפגש. בסיכום זה מובאים עיקרי הדברים אשר עלו במהלך הדיון. אין בסיכום זה המלצה גורפת ללקוחות אלא מתן פרספקטיבה והצגה של ההתלבטויות

רוב הארגונים בשולחן העגול ציינו כי הם מכסים את דליפת המידע ע"י שימוש בטכנולוגיות כגון סינון ספאם במיילים וסינון תכני אינטרנט. הטמעת טכנולוגיות מסוג זה איננה מכסה את כל ערוצי דלף המידע היות ובשנים האחרונות ערוץ המובייל נחשב גם הוא כערוץ דליפת מידע רחב. על מנת למפות את מחזור החיים של המידע- עוד בטרם בחירת המוצר המתאים, נדרשים מנהלי אבטחת המידע יחד עם היחידות העסקיות בארגון לזהות את המידע הקיים, אופן ניהולו וניודו בארגון.

רוב פרויקטי DLP לא ממריאים בישראל. הסיבות לכך הינם הקושי בהגדרת המידע הרגיש בארגון, היכן הוא מאוחסן וערוצי השליחה של אותו מידע רגיש. ארגונים רבים התחילו בפרויקט DLP עקב מניעי רגולציה, תחרות בשוק, פגיעה במוניטין או עמידה בסטנדרטים של מבקרי ראיית חשבון. כמו כן, ארגונים רבים העלו בדיון את מודעות העובדים והלקוחות בנושא דלף המידע. ניתן לראות כי רוב הארגונים בשנה האחרונה העלו את רמת המודעות בנושא בעזרת לומדות, סרטונים וימי עיון, המדגישים את מהות אובדן/ גניבת מידע ארגוני רגיש. ישנם ארגונים שאף דיברו על נושא ההתרעה ע"י לקוח סמוי או הנדסה חברתית.

בנוסף חשוב לציין כי בדיון עלו טכנולוגיות נוספות בהן ארגונים עושים שימוש כגון: חסימת התקנים חיצוניים בעמדות קצה, סיווג מסמכים ע"י העובדים בעת יצירת המסמך, הצפנה של מחשבים ניידים בהתחברות מרחוק, היעזרות במוצרי הלבנה לבדיקת קבצים רגישים הנכנסים לארגון וכדומה.

לסיום, ישנם היבטים ארגוניים הכרוכים בהקמה ותפעול מערך DLP. יש ליצור תיאום בין פונקציות רבות בארגון כמו: הנהלת החברה, יועץ המשפטי, מנהלי אבטחת מידע, נציגי יחידות עסקיות וגורמי IT. לשם מיצוי הפוטנציאל הטכנולוגי במוצרים נדרשת פעילות הכנה תומכת בהטמעת המוצרים, המבוססת על מתודולוגיה מסודרת שתאפשר בניית חוקי זיהוי בהתאם לסוגי המידע הרגיש והתהליכים העסקיים המשפיעים על הארגון.

בברכה,

סיגל רוטין

תוכן עניינים

2	הקדמה
4	מהו DLP?
4	שלבי פרויקט DLP בארגון
8	הסיבות לכניסה לפרויקט
10	סוגיות טכנולוגיה בהטמעת מוצרי DLP
15	אחריות הפרויקט בארגון
16	מודעות עובדים בהקשר לפרויקט
17	סיכום
18	נספח מיוחד התייחסות ספקים ויצרנים לנאמר במפגש
18	התייחסות חברת בינת תקשורת מחשבים
19	התייחסות חברת מטריקס 2bSecure
19	התייחסות חברת סימנטק

מהו DLP?

What is DLP?

- DLP means different things to different people
 - * Data Loss Prevention
 - * Data Leakage Prevention
 - * Data Loss Protection
- DLP is always about protecting organization sensitive information.
- DLP technology is content aware
 - referred to as deep packet inspection, analyzes the payload contained within a file or session.
- DLP references data in one of three states
 - * Data in motion
 - * Data at rest
 - * Data in use

Source: <http://www.slideshare.net/technetbelux/data-leakage-prevention-22804526>



כל אחד מגדיר את המושג DLP באופן שונה, ויש המתייחסים אליו כשם כולל למוצרים הטכנולוגיים השומרים על סודיות המידע, החל מפתרונות הצפנה ועד להלבנת קבצים.

למעשה מערכות למניעת דלף מידע פועלות בזיהוי, ניטור ואבטחה של מידע העובר בתקשורת ומצוי במאגרי מידע וביחידות הקצה, בעזרת ניתוח עמוק של תוכן עם ממשק ניהול מרכזי.

שלבי פרויקט DLP בארגון

על מנת ליישם בצורה אפקטיבית מערכות DLP יש לשאול מספר שאלות משמעותיות:

- ✓ מהו המידע הרגיש/הסודי?
- ✓ היכן אותו מידע מאוחסן?
- ✓ מהם הערוצים דרכם המידע יכול לזלוג?
- ✓ במידה ויתרחש אירוע דלף מידע רגיש, באילו פעולות עלינו לנקוט?

מתוך: <http://www.digitalwhisper.co.il/files/Zines/0x1F/DW31-5-DLP.pdf>

1) ניתוח הסביבה העסקית והאיומים הקיימים (פנימיים/ חיצוניים).

שלב זה נועד למיפוי האיומים על הארגון. אם מדובר בארגון בטחוני, ככל הנראה שתהליכי אפיון מידע מסווג יהיו מורכבים יותר לעומת ארגון שכל מה שהוא מנסה לאבטח הם מספרי כרטיסי האשראי הנמצאים במאגרי המידע בארגון. בשלב זה נדרש למפות את האיומים, לרבות מי הם הגורמים היכולים לגרום לדלף מידע, מהם המניעים שלהם ומהי רמת היכולות של אותם גורמי איום.

2) סיווג המידע - הגדרת המידע הסודי/רגיש וסיווג לפי רמת רגישות.

בשלב זה נדרש להגדיר מהו המידע הסודי עליו רוצים לשמור. להלן דוגמאות למידע שעשוי להיות מוגדר בארגון כסודי:

- קניין רוחני.
- מידע הקשור לצנעת הפרט כגון מידע רפואי, פרטים אישיים ואף צבר של מידע.
- מידע פיננסי/עסקי.
- מידע השייך ללקוחות.
- מידע ביטחוני.
- מידע טכני אודות מערכות מידע בארגון שעשוי לחשוף חולשות אבטחה.

שיטות לביצוע תהליך סיווג מידע (DATA CLASSIFICATION):

- שיטה ידנית: קביעת תג סיווג עבור כל מסמך כחלק מתהליך יצירת המסמכים.
- שיטה אוטומטית: שימוש במערכת לומדת/מומחה לקריאת מידע ומתן תגי סיווג למידע באופן אוטומטי.

3) זיהוי ומיפוי מקומות אחסון של מידע סודי/רגיש.

מטרת פעילות זו הינה לענות על השאלה, היכן ממוקם המידע הרגיש? לצורך זה ניתן לעשות שימוש בכלי E-Discovery שלעתים הנם מודול במערכת ה-DLP. במהלך הפעילות, ימופו מקומות האחסון כגון:

- זיכרונות ניידים/מדיה
- בסיס נתונים
- שרתי קבצים
- שרתי אחסון/גיבוי/קלטות
- אמצעים ניידים - סולל אריים / מסופונים
- תחנות קצה

4) מיפוי וניתוח תהליכים עסקיים ומחזור החיים של המידע בארגון.

לאחר שבוצע מיפוי של המידע הרגיש ומקומות בהם הוא ממוקם, יש למפות את התהליכים העוברים על המידע. מידע יכול להיווצר בתחנת הקצה של המשתמש, לאחר מכן להישלח בדואר האלקטרוני בתוך הארגון, לעלות לשרתי קבצים או למערכות ניהול ידע, להיות מופץ שוב, ובכל שלב בזרימת המידע קיים סיכון של דלף. השלבים המקובלים במחזור החיים של מידע הנם:

- יצירת מידע
- הפצה
- שימוש
- תחזוקה/עדכון/עיבוד
- העברה לארכיון/גיבוי
- השמדה

5) מיפוי והערכת ערוצי הדלף הפוטנציאליים.

שלב זה נועד לתעדף ולמקד את יישום אמצעי ה-DLP והתהליכים הנלווים לערוצי דלף המסוכנים יותר. לדוגמא, בארגון בו קיימת הקשחה אפקטיבית של תחנות קצה מפני חיבור מדיה נתיקה, רצוי למקד את המאמצים סביב ניטור תוכן היוצא דרך הקישור החיצוני ולהיפך. ערוצי דלף אפשריים:

- ממשקים וקישורי רשת חיצוניים
- מדיה וזיכרונות ניידים
- מבקרי רשת מזדמנים (ספקים חיצוניים או עובדים זמניים המחברים יחידות קצה לרשת הארגונית באופן זמני).
- פקסים ומדפסות
- אמצעי מחשוב ניידים (עולם ה-Mobile)
- גורמים אנושיים

6) אפיון דרישות, בחירת מוצרים והטמעה, לרבות התאמה ועיצוב מדיניות, נהלים, תהליכי תגובה ואמצעים משלימים.

לצורך יישום אפקטיבי של מערכות ה-DLP נדרש לטפל בכלל היבטי אבטחת מידע הארגוני:

- נהלי עבודה והנחיות למשתמשים - הכנסת שינויים בנהלים הקיימים לגבי אופן ניהול המידע בארגון, כגון סיווגים ידניים, אופן העברת מידע לגורמים חיצוניים וכו'.
- תהליכי הטיפול באירועים - יישום מערכת DLP דורש התאמת תהליכי תגובה וטיפול באירועי הדלף, לרבות זמני תגובה של אנשי אבטחת מידע, שיטות תחקור האירועים, מזעור נזקים וביצוע חקירות. הדבר תלוי באופי הארגון וביכולות של צוות אבטחת המידע.
- אחריות ותפקידים - ייתכנו שינויים בהגדרות של בעלי תפקידים מסוימים, כגון מינוי בעלי תפקידים חדשים שיהיו אחראים על שלבים השונים במחזור החיים של מידע.
- תהליכי מחזור החיים של מידע בארגון - ייתכנו שינויים במחזור החיים של מידע, לדוגמא, הקפדה על קביעת תגי סיווג לכל מסמך בשלב היצירה. העברת/שיתוף מידע בתוך הארגון באמצעות מערכות ניהול ידע וכו'.
- נתיב ביקורת, לוגים וחיבור למערכות SIEM. לצורך שיפור יכולת תחקור אירועי דלף, נדרש לטייב את תקינות הלוגים במערכות נלוות Active Directory/DC.
- טיפול בערוצים סמויים - על מנת לוודא כי מירב ערוצי דלף מידע מכוסים ע"י מערכות DLP, נדרש לבצע התאמה של תהליכי עבודה וארכיטקטורת מערכות המידע באופן שלא יאפשר קיום ערוצים סמויים (לא מנוטרים). לדוגמא, הקשחת תחנות קצה מפני מדיה נתיקה, הגבלה של פרוטוקולי תקשורת הניתנים לטיפול ע"י DLP (חסימה של תוכנות Peer to Peer).

לאחר היישום - סקירה והערכה לצורך שיפור וייעול הביצועים של הפתרונות המיושמים.
במערכות DLP, בדומה למערכות ניטור אחרות, יש צורך בלימוד מתמיד ושיפור של איכות חוקי ניטור/משוואות בהתאם לאופי האירועים וכמות התראות השווא המיוצרות ע"י המערכת.

בשולחן עגול נערך דיון פתוח בבירור מצב השוק בנושאים הבאים:

- האם בכלל ניתן למנוע או לצמצם ניסיונות פגיעה וגניבה מכוונים של עובדים מתוך הארגון?
- אילו כלים אפקטיביים בטיפול בבעיית זליגת המידע מעובדים בארגון: חינוך? הדרכה? הרתעה?
- איך ניתן לפקח על מידע עסקי שעובר לשותפים עסקיים וספקים?
- מה התמריץ העיקרי להטמעת פתרונות כאלה ואחרים? (רגולציות, ריגול תעשייתי, שמירה על מוניטין ועוד?)
- איך ניתן להתמודד עם זליגת מידע בעידן הדיגיטלי: ניידות ומכשירים חכמים?
- האם ניתן להתמודד עם זליגת מידע דרך טיפול בתחנות הקצה? האם פתרונות EPS צריכים לשלב גם פתרונות DLP? (פגיעה בביצועים, בשלות הפתרונות).
- סיווג מידע כשלב ראשון לפרויקט DLP. איך לגשת לתחום? האם ארגונים הולכים לכיוון הזה?
- DLP – מה קורה בתחום? פתרונות חדשים, יצרנים והתפתחויות בתחום.
- הצפנה והקשחה - פתרונות להצפנה של אמצעים ניידים ונתיקים כאמצעי נוסף להתמודדות עם איבוד המידע. האם שימוש בפתרונות כאלה לא מסבך את חיי המשתמש? מה קורה אם מחשב נייד ננעל בטעות? האם הפתרונות הללו מתאימים לכל הסקטורים?
- DRM -נדבר על שימוש בפתרונות rights management והצפנה למיילים וקבצים בארגון כחלק מהצורך באבטחת המידע העובר בהם. מה חדש בתחום הזה? האם פתרונות אלה נותנים מענה מספק\משלים למניעת זליגת מידע?
- עמדות הלבנה\השחרה – נדבר נוסף למניעת זליגת מידע ומניעת פגיעה ברשת. מה קורה בתחום זה בקרב הארגונים השונים?

הסיבות לכניסה לפרויקט

אחד הלקוחות מספר כי הם נמצאים בפרויקט רגולטורי לסיווג מידע כבר חמש שנים; זהו פרויקט לא פשוט: יש לאתר איפה המידע הרגיש נמצא, להגדיר מהו מידע רגיש – למשל מידע לקוחות, לסווג את המידע ברמות של רגישות וכד'. לאותו ארגון יש הנחיות רגולטוריות מבחינת מהו מידע רגיש. בנוסף מעבר למידע הרגיש של הלקוחות יש להחליט מהו מידע רגיש עסקי, כלומר יש הבדל בהתייחסות בין שני סוגי המידע.

לקוח נוסף מציין כי הארגון מסתכל על נושא דלף המידע כדוגמת עובד עוין בתוך הארגון שרוצה להוציא מידע. אם הוא רוצה להוציא הוא יצליח בכל דרך, אך דלף מידע יכול להגיע ממקורות נוספים- למשל עובד שהוציא מידע החוצה בטעות וללא כוונה. בנוסף, דלף מידע יכול להיות מידע שיצא על מחשב נייד והמחשב אבד, מסופון של נהג שיצא החוצה ונחשף למתחרים בארגון ועוד. דלף מידע לא חייב להיות ישירות מהארגון. לגבי המדיניות, הארגון נעזר בגורם אחזקות- מידעים והוא קובע מדיניות ומסמן בארגון מהו מידע מסווג. בנוסף מחלקת מערכות מידע אחראית לאבטחת המידע הלוגי והטכנולוגי ומימוש הדברים בשטח. גורמי ביטחון אחראים לאכיפה ועושים את העבודה הקשה יותר. סך הכל ישנם שלושה גורמים שמעורבים בתהליך של DLP, וזה משפיע על תהליכים נוספים בארגון. העובדים עצמם לא פחות חשובים פה, ויש לעודד מודעות כדי שהעובדים לא יטעו ויבינו מה הם שולחים החוצה. יש כאן המון פסיכולוגיה, כמו למשל להגיד לעובדים כי מנטרים את מה שהם עושים, אך לא נסביר יותר מדי על מנת שהעובדים ייכנסו ללחץ ולפחד.

הלקוח טוען כי חייבים להתריע את העובדים בשילוב עם מודעות. הנושא שייך למחלקת הביטחון אם מדובר בגניבה של ציוד ארגוני או הוצאת קובץ וזה יכול להגיע לשימוע ואף פיטורין. בארגון אין רגולציה אלא יש ביקורות ראיית חשבון והארגון מחויב בנושא.

הסיבה של הארגון ללכת לפרויקט מסוג זה הינה הפחד שמידע ארגוני רגיש ייצא החוצה, במיוחד בעולם של מתחרים. במידה ומידע רגיש ייצא החוצה זה עלול לפגוע במוניטין הארגון בצורה משמעותית.

אחד הלקוחות העדיף לספר פחות על טכנולוגיה, אלא יותר על מהו מידע רגיש ואיך להתכונן לפרויקט מסוג זה. משמעות פרויקט דלף מידע הינה פחות טכנולוגית, הכוונה כי יש הכנה מרובה לפני. עיקר המידע בארגון הינו מידע עסקי (סוג מידע שלא רצוי שידלוף החוצה) ומידע רגיש שמתייחס לצנעת הפרט- לקוחות חיצוניים. היום שם ות. מוגדר כמידע רגיש. הארגון כפוף לרגולציה של רמות- רשות משפט וטכנולוגיה. מזה שנה הארגון מנסה להיכנס לנושא צנעת הפרט. הפעילות היא לא טכנולוגית עדיין היות ואין כרגע תקציב. הרבה לקוחות טענו כי כמה שלא תאבטח את הארגון עדיין מי שרוצה להוציא את המידע יצליח להוציא אותו. הארגון מחליט להתמקד בכלל המידע שצריך לדעת- מי שצריך לדעת יודע על אותם קבצים רגישים. למשל, ישנם קבצים מסוימים שרק קבוצה מורשת יודעת עליהם ומה החשיבות אם ייצאו החוצה, אחרת זה נזק תדמיתי. בארגון אין הרבה עובדים שחשופים ורואים את אותם קבצים, למעט מי שיצר אותם. הארגון ניעזר בכספות וירטואליות של סייבארק כדי להעביר קבצים בין סניפים והן נפתחות בזמן ובמועד שנקבע.

לקוח נוסף מספר כי לגבי החוקה בנושא DLP הנושא עלה להנהלה והכל אושר על ידם. הארגון הסביר להנהלה בדיוק מה משמעות נושא דלף מידע. כיום בתהליך טיוב ושדרוג החוקה אנשי האבטחה מאד משולבים עם אנשי הביזנס והצרכים שלהם בנושא. אחד הלקוחות טוען שהIT צריך

להוביל פרויקט מסוג זה וזו בעיה מבחינת המעורבות של יחידות עסקיות. העבודה הקשה היא לעקוב אחרי המידע, ולא מדובר רק על הטכנולוגיה אלא גם על תהליך ארגוני, סוג של "האח הגדול".

לקוח נוסף מספר כי לארגון יש ביקורות בנושא ISOX של רואי חשבון, אך הארגון לא כפוף לרגולציה כלשהי. כל נושא הביטחון עבר למערכות מידע. בחשיבה האסטרטגית החדשה של הארגון מחלקת האבטחה בונים תוכנית חדשה להנהלה לעשות פעילות בנושא דלף המידע, כאשר DLP יהיה במקום הראשון בעקבות מקרים פנימיים שקרו בארגון. הלקוח מציין כי חשוב לבנות את התהליך מול הנהלה ומול הביקורות הפנימיות. חשוב להראות להנהלה איך ניתן לגנוב מידע עם סקרי סיכון חיצוניים וכמה האקרים מתוחכמים בנושא. השנה הארגון צריך לעבור למערכת DLP. לצורך כך עירבו את מחלקת הביקורת הפנימית בתקווה כי שיתוף פעולה זה יצור דרך טובה יותר להעלות את הנושא להנהלה ולקבל את ברכת הדרך. אבטחת המידע תפעיל לחץ על מקבלי החלטות הנוכחות בארגון, בין אם זה CFO או היחידות העסקיות. בעבר מי שהיה אחראי לפרויקט מסוג זה היה מנהל אבטחת המידע והאינטגרטור של המוצר. הארגון לא מסוגל מידע אלא עושה איסוף במקביל של כל האזורים בהם המידע הרגיש יושב, אך זה לא מספיק. בזמן שהמערכת הייתה למעלה היה תהליך בו פעם ברבעון קבוצת מנהלי היחידות העסקיות היו יושבות יחד לאיסוף מידע ורענון היכן המידע יושב.

לקוח נוסף מספר כי כיום הם נמצאים בפרויקט הטמעת DLP כבר 8 חודשים עם סימנטק ברמת תחנות gateway. הם נמצאים בשלב הניטור ועדיין לא התחילו אכיפה. הלקוח מציין כי ראו דברים יפים ברשת, למרות שלא הניבו תוצאות. למשל, הארגון איתר קובץ שיצא החוצה והכיל כרטיסי אשראי עם ספרות הביטחון וטלפונים של לקוחות. הארגון עשה חקירה מעמיקה בנושא ומסתבר כי חלק מהלקוחות בקובץ הינם לקוחות הארגון. הקובץ יצא עקב טעות אנוש של אחד ממשתמשי הארגון. התחלת הפרויקט והמניעים לכך הגיעו מצד הנהלה גם בעקבות אותו קובץ שדלף. התהליך התחיל במיפוי של נכסי המידע בארגון, תיקיות רשת של מחלקות או עובדים, אנשי מפתח בארגון, חוקיות מסוימת (אם קובץ מכיל מספר ת.ז. נחשב חשוד) והתאמת חוקים כדי להוריד את false positiven ולצמצם אותו.

לקוח נוסף מספר כי רואה את התהליך הזה כפרויקט משמעותי בתחום אבטחת המידע. כאשר ניגשים לפרויקט מסוג זה חייבים להתחיל ממיפוי הנכסים. הארגון התחיל תהליך כזה והמיפוי הוא די טוב. חשוב לקבוע חוקים בהתאם לרגולציות וההיבטים עסקיים אליהם הארגון כפוף. בלי מיפוי הנכסים ואיפה המידע יושב אין טעם להתחיל פרויקט מסוג זה או לנטר. הטכנולוגיה לא פותרת את נושא הDLP. מה שדחף את הארגון להתחיל פרויקט כזה היא הרגולציה וכך התחילו להגדיר מסמך מדיניות למי מותר להוציא מידע ואיך. חשוב תמיד לתת חלופות להעברת מידע ולא רק לחסום הכל. עושים המון עבודת הכנה בנושא עם המוצר שנבחר - WEBSense, והכל קשור גם בהיבט התקציבי. היות והפרויקט מורכב הוא יכול להיתקע הרבה על false positive. אין לשכוח את הגברת המודעות בנושא ולהעביר זאת למשתמשים. גם זה סוג של אמצעי הפחדה. אין אדם שיושב רק על הנושא הזה, ישנה השתתפות של מחלקת האו"ש והIT - אבטחה בפרויקט. גם ההיבט המשפטי עלה, בעבר לא היתה מודעות לנושא הפרטיות והיום חשובה מאד השקיפות בפרויקט.

לקוח נוסף המגיע ממחלקת הביטחון בארגון מספר כי אצלם שיחות על כרטיסי אשראי נחשבות כמידע רגיש. הארגון מפוקח ע"י רגולציה של רא"ם ומשרד התקשורת. התשתית הארגונית מחולקת לשניים: מערכת IT ומערכת הנדסה. כתוצאה מהמבנה המורכב הזה ישנם 3 גופי אבטחה: גוף אבטחה בתוך מחלקת תשתיות, גוף אופקי הכולל גם את נושא הDLP וגוף אבטחה היושב ברשת

ההנדסה. הארגון התחיל לעבוד עם WEBSense לפני 7 שנים לשם ניטור דוא"ל. למידת הכלי, מה עובר או נכנס לארגון ואילו סוגי מידע עוברים לקחה כשנה-שנתיים. לפני 3 שנים הארגון החל לחסום ולנטר כל דבר שהוגדר כמידע רגיש. במסגרת ועדת היגוי ופורום אבטחת מידע, שמתקיימים באופן קבוע, הוגדר מה המידע הרגיש. המיפוי והגדרת המידע התמקד במידע על לקוחות בגלל צנעת הפרט והיות שהארגון מבוסס על פרטים אלו. הלקוח מתאר כי לפני כשנתיים-שלוש הגדירו מדיניות אבטחת מידע (מה מותר להוציא, למי מותר, סוגי מידע), וחילקו את הארגון לאוכלוסיות ברמת התפקידים. בכל חטיבה עסקית יש נאמן אבטחת מידע (רפרנט) שעבור כל שינוי מחלקת אבטחת המידע נעזרת בו. בהמשך למיפוי מגדירים חוקים למשל, חטיבות עסקיות ששולחות כל הזמן מידע רגיש ללקוחות- מחלקת אבטחת המידע רוצה לבקר בזמן אמת מה יוצא מהארגון. המטרה היא שמידע שיוצא יעבור עין נוספת ולא דווקא מסיבות של אבטחה או ביטחון בארגון. לכן, קישרו את מערכת WEBSense ל-AD של הארגון וכל מייל שיוצא מהיחידות המורשות נבדק בעזרת מנהל המחלקה. המנהל בודק מה עובד רשאי לשלוח ומאשר בהתאם, כך שעובד לא יכול לשלוח מידע רגיש באופן עצמאי. הנושא המשפטי התחיל עוד לפני הכנסת ה-DLP בארגון; הארגון הקים פורום התייעצות עם היועץ המשפטי בו הוחתמו כל העובדים, כולל סעיפי פירוט מלא מה מותר ומה אסור לאבטחת מידע. חשוב לציין כי באותה תקופה לא היה ועד עובדים שיכל להקשות על פרויקט מסוג זה.

סוגיות טכנולוגיה בהטמעת מוצרי DLP

אחד הלקוחות מספר כי הפעילות הינה פעילות כללית של מחלקת אבטחת מידע, אין פעילות שוטפת מול ההנהלה או ועדת היגוי לאותו פרויקט DLP. אבטחת מידע יצרה מהלך ראשוני מול ההנהלה על מנת לגרום למודעות בנושא, אך אין פעילות שוטפת בנושא מול ההנהלה. הלקוח מציין כי התהליך קשה, ארוך, דורש זמן ומשאבים. צריך להגדיר את המידע בכל מערכת, למפות אותו, להתעסק עם false positive ועוד. באותו ארגון מנטרים בינתיים את המידע במייל ובתוכן האינטרנט בעזרת הכלי WEBSense.

הארגון לאט לאט מתקדם הלאה, בצורה הדרגתית וחוסם מידע רגיש נוסף כמו מידע רפואי וכד'. מבחינת חסימת התקנים לא מורשים בעמדות קצה ישנה חסימה, למעט התקנים מורשים לפי מה שהוגדר, וברור כי אין שליטה מלאה על כל המידע איך יוצא החוצה ולאן. זו מגבלה שחייבים להבין אותה בתהליך מסוג זה. הבעיה העיקרית בהתמודדות עם דלף מידע (אחרי שהוא קורה) היא להבין מאיפה זה הגיע, ערוצי הפצת המידע רבים וקשה לשלוט בהם. ברגע שיש חשד לדלף מידע יש תחרות באותו מגזר וכולם מחפשים מידע כמו חוקרים חיצוניים. אם יש חשד, קשה מאד לאתר מאיפה דלף המידע היות והארגון חשוף לשותפים, ספקים חיצוניים, גורמי צד ג', לקוחות ומתחרים. כיום הארגון משקיע המון מאמץ בכלי חיתוך של המון מערכות על מנת להבין האם מידע יכול לדלוף, מאיפה ובאילו מצבים.

לקוח אחר טוען כי אם המשתמש חכם ויודע לנצל מנגנון אחר (מניפולציה) הוא יכול להוציא מידע בכל דרך שהיא וזו בעיה רצינית. בנוסף, קשה גם לגלות אם באמת יצא מידע רגיש ולאן הופץ. אם עובד או אורח חיצוני בתוך הארגון רוצה להוציא מידע- קשה לעצור אותו, זה בשליטתו. צריך לעשות בקרה אם הצליחו להוציא את המידע, ולא רק מניעה מלכתחילה. הארגון גם מתעסק בתחום ההלבנה בקבצים הנכנסים לארגון, ובהשחרה לא מתעסקים. מידע שיוצא החוצה מולבן ללקוחות ושותפים.

לקוח נוסף מספר כי הם מתעסקים גם בנושא ההלבנה ופרויקט DLP בצורה מצומצמת, אבל משתדלים לסגור כמה שיותר דרכים של הוצאת מידע החוצה. הארגון חוסם אמצעים נתיקים בעמדות קצה, יש נהלים ברורים בנושא וזה לא חל על כל הארגון. יש מחלקות שהן מעין VIP, שאצלם אין חסימה היות והם צריכים להוציא מידע החוצה בצורה זמינה, נגישה ומהירה כמו DISK ON KEY ו- CD לצרכי עבודה בלבד. חשוב למפות את כל כניסות המידע פנימה לארגון ויציאות החוצה, ולהפוך לצורה סטנדרטית ככל האפשר באמצעות כלים לשליחת מייל מוצפן או כספות להעברת קבצים בצורה מוצפנת, ולאחר מכן לנטר את מה שיצא החוצה.

אם רוצים להוציא מידע החוצה קשה לנטר זאת תוך כדי מניפולציה על המידע שיוצא בין אם זה הצפנה או פורמט שונה ממה שהכלים יודעים לנתח. המערכות לא עולות על כל סוגי הקבצים, דבר המצריך ביצוע מניפולציות שונות על הקבצים ולוקח המון זמן. השאלה היא איך מנטרים מידע שיוצא החוצה, וזו פעולה לא קלה אך אפשרית. כמובן שצריך לשים בקרות איפה שניתן כמו כרטיסי אשראי, ת.ז, כרטיסי חשבון וכדומה, כאשר בדר"כ הבקרות נמצאות ביציאה ב-GATEWAY. אין הוצאה של לפטופים מחוץ לארגון וחזרה פנימה, כך שאין צורך בהצפנה שלהם. יש בארגון סיווג מידע אך לא נעשה בפועל באופן גורף, כיוון שזה מאד קשה.

יש הבדל בין סיווג המידע לסימון המידע- סיווג ברמת רגישות של מידע כמו מידע בריאותי. כל הסיווג מצריך אישור מהנהלה. לא מסמנים את המידע כי זה יותר בעייתי וממתג אותו. יש הבדל בין רגולציות שונות שמחייבות לסמן את המידע או רק לסווג אותו. חשוב להדגיש כי חוק הפרטיות ומידע בריאותי מסווגים בארגון. מיפוי המידע לוקח זמן ועבודה ידנית. נושא המודעות חשוב פה, לא רק של מפתחים אלא כל הארגון לדעת איזה מידע מותר להוציא ואיך, ואם כן רוצים להוציא מידע איזה תהליכים ארגוניים צריכים לעבור. הארגון חוסם היום כניסת התקנים חיצוניים והתקנות של ענני אחסון חיצוניים כגון דרופבוקס, SKYDRIVE ועוד. אי אפשר לחסום ב-100% כי עדיין יש אנשי מפתח בארגון שזקוקים לתחנות עם גישה של DISK ON KEY. כל מי שרוצה להכניס מידע לארגון חייב לעבור דרך עמדת הלבנה- הרצה במקום ניטרלי ולבדוק מה קורה. בתחום של הלבנה יש בעיה מבחינת קבצי התקנה EXE שקשה לסרוק אותם ולגלות בעיה בהם- מעין SANDBOX בצד.

הלקוח מסביר כי מניעת דלף מתחילה הרבה לפני: מי ניגש למידע- הרשאות. כאשר אדם ניגש למידע זה 80% מהדלף. אם אדם מגיע למידע שהוא לא אמור להגיע עקב הרשאות שגויות אז יש לטפל במעטפת ההרשאות. הארגון עושה שימוש במערכת ניטור הרשאות- ורוניס ואנומליות, NAC פורטנוקס התקנים שמחברים לארגון. בנוסף, הארגון מצפין את המחשבים הניידים במידה ואובדים בעזרת safeguard, ישנה חסימת התקנים חיצוניים בעמדות קצה, אך יש ציבור שלם של עובדים שמחברים התקנים מוצפנים שמערכות מידע נתנו להם והם עדיין בפיקוח. מערכות מידע דורשים מהעובדים בצריבה של CD לעבור דרך הביטחון לאישור. בעזרת WEBSense מונעים מהמידע לצאת החוצה ומנטרים מה יוצא בארגון, חוסמים גישה לאחסון בענן, חוסמים מיילים ענניים כמו GMAIL ובנוסף מנטרים את עולם המובייל (כולל אפליקציות ארגוניות, מיילים וכל מה נשאר על הניידים בעת גניבת מכשיר). כיום הארגון נמצא בפייולוט עם NATIVEFLOW- הגנת המידע במובייל. בינתיים מאבטחים את נושא המיילים. מעל כל זה יש את פרטיות העובד וחובה להיזהר פה: מי מעורב, על מה מחתימים את העובדים, האם מסתכלים בתיבת המייל של העובד, מה עובד העלה ברשתות חברתיות וכו'. דוגמא נוספת- כאשר עובד מגיע לשימוע האם מותר לארגון לציין בשימוע כי בדקו לעובד במייל הארגוני שלו, אחרת זו עילה לתביעה. בארגון לכל עובד יש אופציה לגלוש למייל פרטי שלו מהמובייל, והמייל הארגוני הוא רק לשם עבודה, וה-IT יכול לבדוק אותו במידה

והתגלה חשש כלשהו. אין ניטור על המייל הפרטי, הפייסבוק או המובייל הפרטי של העובד- זה נחלת הפרט והארגון חייב להבין את זה. גם פייסבוק חסום בעיקר אלא בגלל פרודוקטיביות עובד. מערכות מידע אחרים לכל מידע שעובר בארגון ושם יש הכי הרבה תשומת לב.

לקוח אחר מספר כי דלף המידע יכול להיווצר לאו דווקא ע"י אותם יוצרי המידע אלא גם ע"י יועצים/ ספקים חיצוניים המעורבים במידע. היות וישנם הרבה סניפים קשה לאבטח את המידע ויש מודעות נמוכה לכך בסניפים. לפעמים לא אדם אחד יוצר את הקובץ אלא כמה עובדים עליו והם חתומים עליו. יש לציין כי צוות אבטחה מבצע ביקורות על מסמכים רגישים, מבקר את הסניפים, המערכות והעובדים.

בנוסף, יש מידע רגיש של לקוחות שנחשב צנעת הפרט וזו בעיה אמיתית. מספיק שמזכירה יוצרת קובץ אקסל עם לקוחות כולל שם ות.ז וזה נחשב מידע רגיש. קשה לשים אמצעים טכנולוגיים ובקורות בכל מקום. הארגון פועל הרבה בנושא מודעות עובדים למשל, כל מכרז שיוצא מפוקח ומבוקר. הארגון מעביר הנחיה לכל הסניפים והכי חשוב לספקים חיצוניים. כל מכרז עובר דרך צוות אבטחה שנותן הנחיות לכל מכרז. הארגון עושה שימוש ב-DLP של מקאפי, המימוש רק בשלבי התחלה ועדיין לא יושם. כמו כן, יש שימוש ב-WEBSense לסינון תכנים ומניעת שימוש באחסון בענן.

ארגון אחר מספר כי הקבצים מסווגים ע"י המידען הראשי, אשר מחליט על כל פיסת מידע בארגון. גם ביחידות הארגוניות יש בעלי מידע האחראים על המידע במחלקות שלהם. המידען מגדיר ומסווג את המידע והכל עובר דרכו- כל מידע חדש או פרויקט חדש שנוצר בארגון. הסיווג מבוצע בצורה ידנית ולא אוטומטית, כאשר המידען מגדיר קטגוריה ומה עובר דרכה. הארגון ניסה להטמיע secureislands אך פרויקט זה נכשל, היות וקשה לחנך עובדים לסווג מידע בעצמם, תרבותית זה לא עובר. המערכת מצוינת אך זו בעיה. הלקוח מאמין כי יש להצפין את המידע, וליישם מדיניות על המידע כמו גם COVERTIX. אם כל עובד יסווג מסמך הוא ייקבע סיווג ברירת מחדל שהוא הכי חזק, וייווצרו המון false positive, וזו בעיה. המידען הכתיב את המדיניות והוא בקשר עם השיווק שמודעים לכל יצירת מידע רגיש, כאשר בסופו של דבר האחריות היא של העובד.

נראה כי ספקים מדליפים המון מידע ואין להאמין להם, היות והם עובדים עם מספר לקוחות. יש בארגון כל כך הרבה מידע והמידע המסומן יכול להיות אחוז מהארגון שזה המידע הרגיש. יש דגש רב על חינוך עובד ובדיקות ידניות- אגף הביטחון מטפל בתחקיר ואכיפה של אירועים. זה עוזר להעביר את המסר לעובדים על חשיבות דלף מידע. יש גישה שאומרת שצריך להצפין כל דבר: גישות, DB, מידע, מובייל ועוד, אך זו בעיה כי צריך לאפשר לארגון להמשיך לתפקד מבחינה עסקית.

לקוח נוסף בא מתחום הסייבר ואבטחת מידע בארגון ומספר כי הארגון נמצא באמצע תהליך רחב של ניטור רשתות ופעילות הרשת. יש להם מערכת DLP מוטמעת של סימנטק יותר משנה וכרגע נמצאים לקראת שדרוג המוצר וטיוב חוקה. כיום מנטרים מיילים, העברת המידע החוצה לאינטרנט והעברת מידע להתקנים לא מאושרים. הלקוח טוען כי לדעתו מערכת DLP זו מערכת יוריסטית שמנסה להתמודד עם דלף מידע משני כיוונים: עובד/משתמש פנימי שעשה טעות או גורם זדוני נאיבי. חשוב- צריך להתייחס ולשים דגש לנושא הכוונה היות והכל מתחיל שם, בכוונה של הצד השני להדליף מידע. לצערנו, יש בעיה ללא פתרון אמיתי! בתהליך זה ישנה מעורבות בארגון הן מצד ההנהלה והן מצד היחידות עסקיות. ישנו ניטור של דלף מידע גם בהקשרים עסקיים וגם בהקשרים טכנולוגיים (אלגוריתם מסוים שפותח). הלקוח מציין כי ההסתכלות בנושא דלף מידע צריכה להיות יותר רחבה גם בהקשרים של מובייל. DLP הוא למעשה כלי שאמור לשרת תהליך, והתחום מאד

רחב: קבלנים חיצוניים, עובדים שמחברים מהבית, מובייל ועוד. הארגון כפוף ל-SOX, והתהליך התחיל לפני קצת יותר משנה סביב פעילות פנימית שלהם בנושא סייבר ואבטחה. כיום יש חצי משרה של אדם המתעסק בנושא DLP ואחראי לניטור ותחזוקה של המערכת כולל טיוב חוקה. בנוסף, לפטופים נעזרים בהצפנה של BITLOCKER, כולל סינון ספאם ותכנים.

לקוח אחר מספר כי היה להם מוצר עד לא מזמן בנושא דליפת מידע שנקרא VERDASY. הלקוח מציין כי המוצר היה מעבר למוצר זליגת מידע אלא יותר access control ברמת LAN והארגון עשה בו שימוש בשלושה רבדים. רובד ראשון, עובד שרוצה לעשות משהו זדוני אבל הוא לא מתחכם. הרובד שני, היה לעלות את מודעות העובדים לטעויות שהם עושים, והשימוש נעשה פה ברמה יומיומית. הרובד האחרון, הלקוח מציין כי אין תחליף הולם בנושא זה לחקירות ברמה גבוהה. כמה שהמוצר טוב זה גם היה עקב האכילס שלו. המוצר יושב ממש ב-CORE של הארגון ומערכות המחשוב ובתוך ה-LAN בתחנות קצה – המוצר היה כל כך חזק וידע לעשות המון חקירות ברמת נתונים, עד שזה הפך לבעיה. הבעיה התגלתה במעבר לווינדוס 7 ושידרוג גרסאות של לפטופים, וכאן הארגון נתקל בבעיות עם המוצר. היו בעיות טכניות עם המוצר והבעיה הכי קשה הייתה אצל היצרן כאשר התחלפו הנהלות וכבר לא היה ניתן לדבר מולם. גם האינטגרטור בארץ נעלם והארגון נאלץ לנטוש את המוצר.

כיום מאד קשה למצוא למוצר תחליף, אף מוצר לא עושה חקירות ברמה גבוהה כזו. במהלך השנים האחרונות הייתה למידה ארוכה של תהליכים ארגוניים שעזרו להטמיע את נושא ה-DLP. למשל, עובד שמוציא כמויות של מידע מאד רגיש ממחלקה מסוימת USB וקשור למחלקה אחרת. אחרי החקירה ומעקב אחר העובד נראה דפוס ההתנהגות שלו והאבטחה עירבו את יחידת הבטחון אשר בדקו את הנושא והבינו כי העובד רצה לחזור לאחד התפקידים באותה המחלקה ולכן, למד המון מידע משם. בעקבות מקרה זה ועוד רבים, הארגון הבין כי יש בעיית הרשאות ויש לעשות סדר בנושא. מדובר פה בפרויקט שלקח המון זמן לסדר את כל ההרשאות הארגוניות כולל fileservers. הצליחו לעשות אותו כמה שהיה קשה. זה תהליך שעזר להם מאד בעולם ה-DLP. בנושא המודעות ישנה החלטה ארגונית לא לחסום התקנים חיצוניים בעמדות קצה וכאן נעשתה המון מודעות בנושא. ההחלטה תקפה גם בנושא העברת מיילים החוצה למייל אישי וכאן גם ישנו מעקב ומודעות עובדים בנושא.

אחד הלקוחות מספר כי אצלהם הרשתות מנותקות לגמרי ולכן נושא דליפת מידע בטעות פחות רלוונטי לארגון. בארגון קיימות תשתיות השחרה והלבנה בין הרשתות הפנימיות וכן המידע שיוצא החוצה. תשתיות אלה מאפשרות לארגון לשלוט איזה מידע יוצא החוצה ומאיזה מערכות ספציפיות. בארגון יש פתרונות לחסימת התקנים בעמדות קצה אך חשוב לציין כי אין הרבה התקנים מאפשרים לעובדים. למשל, התקני USB חסומים לגמרי. כמו כן, ישנם תהליכי עבודה מוגדרים בארגון בנושא זה בהם כן מאפשר התקנים עם דרישות מיוחדות ואישורים. מה שכן עובר לסביבת האינטרנט מהארגון הינו מידע עסקי שמותר לחשוף. עקב הפרדת רשתות ברורה בארגון והתמודדות עם מידע עסקי ברשת האינטרנט, אין כרגע בהגדרה פתרון ארגוני לנושא דלף המידע או פרויקט DLP. הארגון נמצא יותר בהטמעה של פרויקטים בעולם סיווג מסמכים DRM. כמו כן, הלקוח מציין כי הם מתחילים פיילוט בנושא "דרופבוקס" ארגוני ברשת האינטרנט עם מוצר אמריקאי בשם אקסליום. בנוסף, התחילו פרויקט בנושא MDM להגנה על המובייל ובעולם האינטרנט יש להם כספות של סייבארק. נושא של זליגת מידע הארגון מתמודד עם כוונות של זדון ויש בקרות בכל מקום. המידע מיורט ברשת האינטרנט במידה ויוצא. חשוב להבין כי בנושא המובייל אורחים לא נכנסים לארגון עם

סמארטפונים לשם מניעת דלף מידע. יש היום פתרונות לנעילת המצלמה במובייל בעת כניסה לארגון וכדומה.

כל הפתרונות הללו מובילים לכך שנושא ה-DLP לא נמצא בפוקוס מהותי בארגון אלא יותר על ניטור ובקרה אחרי המידע שמסתובב ברשת האינטרנט. למשל, אנשי שיווק שעושים שימוש בדרופבוקס או במיילים אישיים זה בעייתי לחסום. בעקבות כך נמצא הפתרון של "דרופבוקס" פנימי להעברת קבצים. הארגון נמצא בתחילת פרויקט של סיווג מסמכים DRM ובוחן מוצרים כגון secure islands או COVERTIX. עדיין לא התחילו למפות את כל סוגי הנכסים בארגון ולמצוא את כל החוקים האפשריים לסיווג מידע. כיום סיווג מידע מתבסס על העובדים עצמם. המטרה היא שהמערכת תיקח את סיווג המידע הידני שבוצע ע"י העובדים ויקבע פוליטי על המידע לאורך כל הדרך. כיום ישנם 4-5 עובדים בנושא של "דרופבוקס" וסיווג מידע. בארגון יש לפטופים ברשת האינטרנט אך המידע מוצפן בעזרת BITLOCKER. מה לגבי יעצים חיצוניים שנכנסים לארגון? לעובדים יש מודעות לנושא בהקשר של אורחים חיצוניים. ישנה הקפדה בארגון לעמדות אינטרנט מרוחקות ונהלי בטחון בנושא למניעת טעויות אנוש.

לקוח נוסף מציין כי בארגון ישנו "דרופבוקס" ארגוני שנקרא sharefile של סיטריקס שמשמש להעברת קבצים גדולים ומחובר ל-DLP הארגוני כדי לדעת מי שלח ולאן שלח. כמו כן, ישנה הצפנת ניידים והתקנים חיצוניים בעזרת מוצר SAFEND. יש מוצר NAC של חברת FORESCOUT למניעת דלף של חיבור לא מורשה פנימה לארגון. נושא ההלבנה והשחרה נמצא בבחינה בארגון. האחריות לפרויקט DLP הינה בתוך אבטחת מידע ואינטגרטור חיצוני שמגיע פעמיים בשבוע. לקוח אחר טוען כי אבטחת מידע לא חייבים לשבת על מערכת כזו ולנטר כל מידע שעובר אולי דווקא גורם עסקי או או"שי בנושא עדיף.

לקוח נוסף המגיע ממחלקת אבטחת מידע מספר כי הארגון שוקל להיכנס לפרויקט DLP. לדעתו הפרויקט מורכב מאד לא מבחינה טכנולוגית אלא מבחינה משפטית. נושא ניטור וצפיה בחומר רגיש בעייתי גם מכיוון ועד העובדים. נושא ה-DLP לא מטופל בארגון. הארגון מדבר על נושא דלף המידע המון אך מצד שני יש המון מערכות אבטחה ונראה כי כל הנישיות סגורות. לא היו מקרים של דליפת מידע. השאלה היא מהו מידע רגיש בארגון, היות והארגון ציבורי כל המידע באינטרנט. המידע הרגיש פה יכול להיות מידע עסקי ששייך לשיבות דריקטוריון. יש למפות מקור מידע וליצור ערוצי העברת מידע בתוך הארגון שהם בטוחים. כיום יש הלבנה והשחרה בארגון. רוב ערוצי העברת המידע מוצפנים. אין לפטופים של הארגון ואין הפרדה של מכשירי מובייל פרטיים או עסקיים היות ועושים שימוש ב-GOOD. הארגון לא חוסם USB אבל מאפשרים לעשות שימוש רק ב-USB ארגוני שעבר סריקה לא משהו זר. במידה וזה USB חיצוני יש שימוש במערכת הלבנה לסריקת ההתקן.

אחריות הפרויקט בארגון

אחד הלקוחות מספר כי הפעילות תחת אבטחת מידע כחלק מהפעילות השוטפת, יש עובד בצוות האחראי לזה כחלק משאר תפקידיו. הארגון הגדיר לעצמו שלבים בפרויקט. כיום, רוב המידע הרגיש שעובר במייל ובאינטרנט מנוטר. לפני הניטור הלקוח מציין כי היו המון זמן בתהליך של למידה מהניטור ומעקב כדי להבין מי הגורמים שעובדים מולם ומקבלים מידע ארגוני רגיש ושם יש לכוון הצפנה של התווך במקום להצפין את האימייל או הקבצים. כמו כן, הלקוח מספר כי הם התחילו בתהליך של חסימה שמאד רגיש ומחייב הרבה תשומת לב ולכן עושים זאת בצורה מאד מדודה. כרגע הם מתרכזים אך ורק בחסימת כרטיסי אשראי והתהליך מתנהל יפה.

לקוח אחר מספר כי יש צוות אחראי בארגון לנושא הלבנה כולל אחריות למידע שיוצא או נכנס לארגון- 3 איש. זהו צוות תפעולי תחת אגף תשתיות. גם צוות SOC אחראי לניטור, בקרה ותגובה בנושא מידע שיוצא החוצה. אם יצא מידע החוצה זה עולה בסוף לתחקור צוות אבטחת מידע.

לקוח אחר שבא ממחלקת הביקורת מספר כי אצלם הארגון עם מערכת של VERDASYS ויש מחלקה ספציפית לתחום ה-DLP. אנשי אבטחת מידע באותו ארגון הגיעו גם לדיון וסיפרו כי בנושא זה מוקצים 2 אנשים בארגון. כל האיפיון של המוצר היה חוקה כללית שהוגדרה למידע רגיש כולל איפיון ספציפי עם איפיון ספציפי לחטיבות השונות. למעשה עברו כל חטיבה ואפיינו את המידע הרגיש בה. מי שמגדיר את הפוליסי זה מחלקת אבטחה תחת תשתיות וניטור המידע הרגיש מתבצע ע"י בקרת ה-SOC. כרגע רק מנטרים ולא חוסמים – הנושא בדיונים עצם העובדה שהמידע רגיש. יש הרבה FALSE POSITIVE ומנסים לצמצם. בנוסף, התקני USB חסומים כמעט בכל מקום, יש מעט חריגות. בארגון יש עמדות הלבנה. נושא העבודה מרחוק מול גורמים חיצוניים מתבצע עם כספות של סייבארק. יש לארגון פתרון פיתוח עצמי בנושא מעבר של מידע רגיש באופן חד פעמי ישנה הצפנה חד פעמי של המייל דרך רכיב באטלוק.

אחד הלקוחות מספר כי אצלם בארגון הרשת יותר מתירנית אין הפרדה בין רשתות. יש רשת אחת והשימוש די חופשי באינטרנט לכל העובדים. הארגון לא חוסם סוגי אחסון חיצוני או דוא"ל בענן כמו GMAIL, אלא בעיקר רק חסימת אתרים כמו פייסבוק שלא פתוח לכולם. בנוסף, ישנה בדיקה של קבצים שנכנסים ויוצאים מהארגון. כל נושא המידע הרגיש עובר דרך כספות. יש הרבה מידע לקוחות רגיש בארגון. בארגון רוב המידע הוא מידע תפעולי שנמצא בבסיסי נתונים. יחסית לארגונים אחרים לארגון יש מעט מאד מידע שהוא נמצא בקבצים. אצלם הכי פחות חשוב הוא המידע העסקי, היות והכל מפורסם אלא מידע לקוחות פרטי רגיש. בכל זאת, הארגון מאד מוטרד מנושא דליפת מידע למשל, מצבים בהם יש התכתבות במיילים על לקוח, או התייעצות לגבי לקוח. יש מצבים בו מוציאים קובץ ממערכות תפעוליות עם המון מידע פרטי של לקוחות (מידע גולמי) ולאחר עיבודים רבים יוצא סוג של גרף לשיבת הנהלה. אז איך מגנים על זה? כאשר המקור של הקובץ מאד רגיש? הארגון עובד עם עובדים החיצוניים דרך גישה מרחוק מאובטחת- סטריקט TERMINAL SERVER. לאותו עובד חיצוני יש DB-בסיס נתונים קטן אצלו והוא מוצפן במידה וצריך אותו. הארגון לא כל כך מתקדם כמו ארגונים אחרים בדיון, כרגע נמצא בפילוט בנושא התקנים ניידים חיצוניים בעמדות קצה, תוך חצי שנה לסיום. אופי העבודה בארגון לא מחייב שימוש בהתקנים ניידים אך בכל זאת יש להגן פה. הלקוח מתחבט בשאלה מהו מידע רגיש בארגון, מתי זה לגיטימי ומתי לא, איך מגדירים פוליסי (מדיניות) כזה. כמו כן, הלקוח מרגיש כי נושא המודעות ולומדות לעובדים לא מספיק, לדעתו יש פה חוסר הצלחה.

מודעות עובדים בהקשר לפרויקט

אחד הלקוחות מספר כי עשו קמפיין מודעות בנושא זליגת מספרי כרטיסי אשראי מחוץ לארגון והעובדים מודעים לנושא. אין הרבה false positive, הכמות נמוכה. כמובן שחוסמים מיילים עם אזכורים של כרטיסי אשראי כתוצאה מתקן PCI וגם הרגולציה אליה כפופים.

לקוח נוסף מספר כי עבודת המודעות חזקה והארגון מאמין כי ממשיכים להגיד לעובדים כי מנטרים את המידע שלהם, זה לא מספיק עקב פסק דין פרטיות. לכן, הארגון הוציא מדיניות חדשה לשימוש מחשב כולל יועץ משפטי שאומרת כי עושים הפרדה לסביבה עסקית ופרטית. לעובדים יש אפשרות להסתכל בתיבת הדואר האישית ואין חסימה אך ישנה הבנה והפרדה בין הסביבות. עדיין אם יש חשד כלשהו למעילה/גניבה וכדומה כאן יש זכות לאבטחה להסתכל בתיבות דואר הארגוניות של העובדים. בנוסף, הארגון חסם ברמת וובסאנס קטגוריות של אחסון בענן חוץ מיחידה אחת בארגון שקיבלה אישור מיוחד לשימוש בדורפבוקס. כרגע אין פתרון הולם לנושא הדורפבוקס מבחינת DLP. יש להם הדרכות מודעות וימי קליטה כולל לומדה לעובדים. הלומדה מתרעננת פעם בשנה.

לקוח נוסף מציין כי בארגון יש הפרדת רשתות ורשת האינטרנט נפרדת לחלוטין, יש עובדים עם 2 מחשבים. אחד הגורמים באותו ארגון קשור לנושא המודעות. בארגון עושים המון בנושא מודעות בכל ערוץ אפשרי החל מהדרכות, עובדים חדשים בסניפים שונים, ימי עיון חוזרים ומידע בפורטל ומיילים בנושא. הארגון מפיץ לומדה וסרטונים בנושא בעקבות אירועים חריגים של עובדים, הרצאות מתוקשבות לעובדים. בארגון רצה לעשות תרגיל בהנדסה חברתית (לקוחות סמויים) אך הבעיה פה היא ועד העובדים. אחד הלקוחות מעלה כי נושא האורחים הסמויים פיזית או טלפונית בארגון בעל השפעה נהדרת על הארגון ובכלל על ההנהלה. באותו ארגון יש הגנה על שומרי מסך ושליטה עליהם. בארגון יש קוד אתי לגבי חיסיון מידע, מעין אמנה לגבי רשתות חברתיות- מה מותר ומה אסור איך מזדהים, תגובה בפורומים בשם הארגון, הוצאת מידע ברשתות חברתיות. אין סינכרון של מייל למחשב פרטי או טלפון פרטי של עובד.

כמו כן, הארגון עושה שימוש במוצר GOOD אך ורק לאנשים מורשים. כמו כן, יש שימוש בטאבלטים בדרג ההנהלה ומעבירים קבצים דרך כספות. חשוב להתייחס למידע שקיים באינטרנט והוא לגיטימי, המערכות שקיימות בארגון מעבירות לכל לקוח את המידע שלו עם הזיהוי שלו כדי שלא יהיה דלף מידע גם מכיוון האינטרנט והלקוחות. הארגון מנסה לחנך לקוחות גם לא להתחבר ממקומות לא רצויים כי גם שם יכולה להיות זליגת מידע. גם ספקים שמקבלים מידע מהארגון, אבטחת מידע עושה אצל אותו ספק וביקורת כדי לוודא שעומד בסטנדרטים של הארגון. רק ספקים מורשים לקבל מידע רגיש.

לגבי נושא סיווג מידע ידנית עפ"י המשתמש זו בעיה. היות ואם נותנים למשתמשים לסווג הם יחמירו עם עצמם כי הם בעלי האחריות. הם תמיד כאשר המשתמש מקבל את האחריות, הוא מפחד יותר ויחמיר עם עצמו.

לקוח נוסף מציין כי משקיע המון במודעות דרך לקוח סמוי ששולח לקבלת מידע דרך ספקים, סניפים, נציגי שירות. הארגון מדמה את סוחט/גונב המידע בכל הנקודות והמוקדים ומנסים להוציא מידע רגיש כמו פירוט שיחות. כך הארגון בודק את הטמעת הנוהל בשטח לגבי לקוח סמוי. כמו כן, הארגון מתקן את הנוהל אם צריך במידה ויש יותר מדי כישלונות והנציגים נופלים. בארגון יש לומדה שפותחה פנימית שמרכזת את כלל הנחיות ודרישות אבטחת מידע. התוכנה אינטראקטיבית וממוחשבת כולל

שאלות לעובדים. היא נערכת אחת לשנה לכל העובדים ולכל עובד שנכנס לחברה. בהמשך הארגון מחלק ערכת אבטחה הדרכה לכל עובד שנכנס. יש הדרכות בנושא אבטחה והשנה עושים שבוע אבטחת מידע עם מיתוג והדרכות בנושא. נכון שיש בעיה עם תקציב אבל מנסים כמה שיותר להשתמש במה שיש בארגון – סלוגן שממציאים בנושא. במוקדי השירות יש סיטריקס והם סגורים להוצאת מיללים החוצה או אינטרנט. הכל מנותק בעמדות ולכן שם אין מערכת DLP. נושא דליפת מידע יכול לבוא גם מכיוון ההדפסה ובארגון יש ניטור על זה לפי כרטיסי עובד.

סיכום

כיום בעידן הדיגיטלי בו מידע נע באופן דינמי בתוך הארגון ומחוצה לו, ארגונים צריכים להתמודד עם דלף מידע ולשמור על סודיות המידע הארגוני כדי לשמור על מוניטין הארגון ולעמוד ברגולציה הכפופים אליה.

ראינו כי דלף מידע יכול לנבוע מסיבות שונות כמו: טעויות אנוש, תחרות בשוק וריגול, תקלות טכניות, עובדים ממורמרים, אובדן מחשבים ניידים השייכים לארגון ומכילים מידע רגיש, החדרת תוכנות זדוניות וריגול דרך אמצעים נתיקים וכדומה.

ארגונים רבים מטמיעים מספר מערכות לצורך מניעת דלף מידע אך לא כולם עושים הכנה מקדימה לנושא. כתוצאה מכך המערכות הטכנולוגיות לא ממצות את כל הפוטנציאל שלהן לכסות את כל ערוצי הדלפת המידע. על מנת להטמיע בצורה אפקטיבית מערכת DLP בארגון יש להיערך ראשית ולבצע תהליכים ארגוניים יחד עם ההנהלה והיחידות העסקיות בהגדרת המידע הרגיש.

נספח מיוחד התייחסות ספקים ויצרנים לנאמר במפגש

התייחסות חברת בינת תקשורת מחשבים

איש קשר: פלביו מנטלמכר CTO, flavio@BYNET.CO.IL, 052-5528093

חברת טיטוס www.titus.com הינה החברה המובילה בעולם לסווג מידע בלתי מובנה, מסמכים, דואר אלקטרוני וסוגים רבים אחרים של קבצים.

תרומתה המכרעת של TITUS הוא בשינוי התרבות הארגונית וזאת מהסיבה שיוצר המסמך יודע ומבין מה המידע שיש במסמך.

המערכת תסייע למשתמש לסווג את המסמך בצורה נכונה בעזרת מספר כלים אוטומטיים.

בהמשך להרבה התייחסויות בשולחן העגול בנושא חשיבות וקריטיות הסיווג של המידע לביצועי מערכות ה-DLP טיטוס מקיימת שיתופי פעולה עם חברות ה-DLP המובילות ובעצם משמשת בהרבה מקרים "מאפשר" (enabler) של התקנות DLP.

כפי שצוין על ידי מספר משתמשים סווג המידע מאד קריטי לביצועי ה-DLP. בטיטוס מאמינים כי הסיווג צריך להתבצע ע"י יצרן המידע בעזרת שורה תוכנה ידידותית שעוזרת לסווג ולהימנע מטעויות אך בסופו של דבר הרעיון להכניס שינוי תרבותי בארגון (כפי שלא מעט ארגונים ציינו בסיכום) שבו ליצרן המידע יש אחריות לסווגו.

יש להדגיש ש-96% מדלף המידע נובע מטעויות אנוש או מטעויות תהליכיות.

ברגע שבוצע הסיווג תוכנת טיטוס דואגת להכניסו כ-Meta-Data למסמך או לדואר האלקטרוני וכל תכנה אחרת (כדוגמת DLP) יכולה לקרוא את המידע ולהשתמש בו כדי לקבל החלטות ולשפר דיוקים.

רבים ממשמשי טיטוס, (לטיטוס מעל 650 לקוחות ו 3.5 מיליון משתמשים בעולם) קנו את התוכנה כדי לגרום למערכות ה-DLP שלהם לעבור ממוד monitoring למוד חסימה ובעצם לנצל את ההשקעה שנעשתה בארגון ברכישת מערכת DLP שללא הסיווג פשוט לא הביאה תועלת משמעותית.

טיטוס נותנים מענה לבעיית ה false positive המאוד שכיחה בישומי DLP שהוזכרה רבות בשולחן העגול.

לסיכום, לחברת TITUS תרומה ופתרון מאד משמעותיים הטיפול בבעיות המרכזיות שקיימות והוזכרו שמונעות הצלחה בהטמעת מערכות DLP.

חברת אינציו טכנולוגיות הינה המפיצה הרשמית של המוצר בישראל וחברת בינת תקשורת ביצעה את ההסמכות הנדרשות והיא משווקת מוסכמת של המוצר, לחברה מעל ל- 18 אנשים טכניים בתחום אבטחת המידע והסייבר אשר מסוגלים לטפל ולסייע ללקוחותינו להטמיעו.

התייחסות חברת מטריקס 2bSecure

איש קשר: שגיא זלינגר Sagi.Zelinger@2bsecure.co.il 054-6500277

על מנת למפות את מחזור החיים של המידע - עוד בטרם בחירת המוצר המתאים, נדרשים מנהלי מערכות המידע ומנהלי אבטחת מידע לזהות את המידע הקיים ואת אופן ניהולו וניודו בארגון. על כן, עליהם לענות ראשית על שאלות מהותיות כגון: מהו מידע סודי? היכן הוא מאוחסן? מה הם הערוצים דרכם המידע עלול לזלוג? ולבסוף, אלו פעולות יינקטו אם וכאשר יתרחש אירוע של דלף מידע סודי?

חברות נדרשות להתייחס להיבטים ארגוניים הכרוכים בהקמה ותפעול של מערך ה-DLP. בין היתר, נדרש תיאום בין פונקציות רבות בארגון, כגון: הנהלת החברה, מנהלי אבטחת מידע, היועץ משפטי, גורמי ה-IT, נציגי היחידות העסקיות, ועוד.

כיום, כבר קיימת הכרה בכך שארגונים המעוניינים בהטמעת מוצרים למניעת דלף מידע שתוצאותיהם מורגשות לטווח ארוך, לא יכולים להסתפק בהתקנת כלים טכנולוגיים בלבד אשר רק מפקחים ומסננים תוכן ב"ערוצים יוצאים" ופועלים על בסיס חוקי זיהוי חריגות תוכן כפי שנקבעו ע"י היצרנים, לדוגמה חוקי זיהוי מספרי כרטיסי אשראי.

לשם מיצוי הפוטנציאל טכנולוגי, נדרשת פעילות הכנה תומכת להטמעת המוצרים, המבוססת על מתודולוגיה מובנית ומסודרת שתאפשר בניית חוקי זיהוי בהתאם לסוגי המידע הרגיש והתהליכים העסקיים המשפיעים עליו. פעילות מתודית זו תאפשר התמודדת אפקטיבית עם מקרים של דלף מידע ואף הפחתת דיווחי סרק רבים, שאופייניים לפתרונות הטכנולוגיים העוסקים בזיהוי חריגות.

התייחסות חברת סימנטק

איש קשר: רון כהן Ron.Cohen@symantec.com 054-6227703

להלן התייחסות לנקודות במסמך מתוך הניסיון שלנו בשוק אצל לקוחות כגון ECI, הדסה, אסותא, משרדי ממשלה, אורבוטק, בנק איגוד, 888 ועוד רבים ...

1 – בהתייחס לסעיף (3.5) – לקוחות רבים מזהים את תחנת הקצה כמוקד דליפת המידע בעוד שבדרך כלל המוקד העקרי הוא בדואר אלקטרוני, כך שהתחלת פרויקט בדואר אלקטרוני גם יעילה יותר מבחינת הכסוי, גם תורמת יותר מבחינת לימוד תנועת המידע בארגון וגם זולה יותר לפתיחת פרויקט הן מבחינת המחיר, זמן ועלויות יישום.

2 – בהתייחס לסעיף (5) ראוי לציין כי הגורם האנושי אחראי באחוזים גבוהים בפעולת הוצאת המידע לא כדי לגרום נזק אלא דווקא כדי לשפר את פעילות הארגון. (נושא זה מוזכר ראשון בסיכום אך כלל לא בפתיחה)

3 – בהתייחס לסעיף (6) כמות האירועים המוצפים ע"י מערכת ה-DLP חייבת להיות קטנה ביותר (אירועים בודדים לשבוע עד חודש) אחרת המערכת הופכת להיות נטל.

לקוחות. מוזכר אובדן ציוד – הפתרון לנושא זה הוא הצפנת הדיסק ולא DLP

מוזכר נושא הסברה לעובדים – במקרים רבים רצוי לבצע את ההסברה שלא דרך המוצר, ולא דרך חסימות או הקפצות מסכים במוצר שבפועל מדריכות את הלקוח איך "לעקוף" את המוצר. (עמוד 10 למטה)

עמוד 11 מוזכר מושא ההרשאות – סימנטק רואה בנושא חשיבות גבוהה ביותר ולכן גם מציפה את הרשאות של הקובץ במסגרת האירוע וגם מאפשרת ניתוח ושליטה בהרשאות דרך ה Data insight שהוא רכיב ב DLP המתממשק עם מערכות אחסון Windows, NetApp, EMC ועוד, וממפה את נושא ההרשאות ביחס לבעלי המידע ולאירועי אבטחת מידע.

עמוד 12 – בעיית סווג מידע – כדאי להזכיר טכנולוגיות כגון VML המאפשרות ניתוח טקסטואלי אוטומטי של טקסטים וזהו ברמה גבוהה של מידע טקסטואלי כגון קוד מחשב, מסמכי אפיון וכד'.

בעמודים רבים מוזכרים מוצרי AGENT כגון Secure Island, Verdasys (עמוד 13 לדוגמא) ואחרים חלקם עם סיפורי כישלון, דבר שאינו מפליא מכיוון ש DLP חייב להיפתר בכל השכבות ולא רק ברמת התחנה.

ניכר כי קיימת אי הבנה בין מספר פתרונות ברמת תשתית כגון חסימת התקנים, NAC שממוקדים בתשתית בעוד שפתרון ופרוייקט DLP מתחיל ומסתיים בתוכן.

לסיכום:

- DLP מיועד לעיתים קרובות להתמודדות עם העובד המעוניין "לעזור" או העובד הממורמר ולא רק עם "גנבי" מידע.
- קיים בלבול בשוק בין מוצרי NAC, הצפנה, ו Device Control ונושא ה DLP – כנראה בגלל שקל יותר ברמה האירגונית להתמודד עם בעיית תשתית ולא עם מיפוי וחסימת תכנים.
- על פתרון DLP אירגוני לתת מענה איכותי לכלל המרכיבים ומומלץ להתחיל ביישום מדורג שתחילתו באפיק זליגה מרכזי שהוא דואר אלקטרוני.