זליגת מידע: ניהול סיכונים ומניעת זליגת מידע במסגרת האפשרויות הכלכליות

הוכן על ידי: גיא פלטיאלי

הבעיה

בשנים האחרונות הקשיים שבמניעת אובדן מידע רגיש רק גברו בשנים האחרונות עבור ארגונים רבים. שיעורי המקרים בעלייה, האחריות של הארגונים גוברת, והסיכון שבגניבת זהות מחלחל לכל. הפגיעים ביותר הם התעשיות והארגונים שחייבים לפעול לפי תהליכים ופרוצדורות שכוללים רכישה, עיבוד, שמירה, העברה והריסה של מה שמומחי בטחון המידע מכני "מידע פיננסי אישי בר זיהוי" (Personally Identifiable Financial Informatio), ומידע בריאותי אישי בר זיהוי. באופן כללי, למידע מסוג זה מתייחסים כמידע אישי בר זיהוי (PII).

ה-PII הוא כל סוג של מידע רגיש ופרטי על הלקוח, שנמצא ברשות הארגון. כמה דוגמאות לכך כוללות: מספרי זהות, מידע על כרטיסי אשראי, מספר רישיון הנהיגה, ומידע רפואי הנוגע לאחד מעובדי הארגון או לאחד מלקוחותיו. בעת שבסיס הלקוחות ושירותי הארגון גוברים, כך גם עולה כמות מידע ה-PII. כאשר ארגון מעבד או מחזיק יותר מידע PII, כך הוא נמצא בסיכון רב יותר לזליגת מידע. זליגת מידע מתייחסת למצבים בהם מידע רגיש וחסוי דולף מתשתית הארגון, ויכול להיחשף באופן לא מאושר. צמצום הסיכונים שבניהול מידע כזה ולזליגתו, יכול להיות משימה יקרה מאוד.

ציות וזליגת מידע

למרבה המזל, בשל דרישות הציות התעשייתיות או הממשלתיות, חברות, ארגונים, ומוסדות מחויבים לפתור את הסיכונים הנוגעים לזליגת המידע. תעשיית כרטיסי האשראי מצייתת למצבור של דרישות אותן הציבו בתחילה חברות האשראי הגדולות. דרישות אלה דורשות מהישויות שהתהליכים ועסקאות האשראי יצייתו ל-12 חוקי בטחון מידע, כדי להגן על עצמן מפני קנסות כספיים. הדרישות הללו מחייבות את קיומן של בקרות, דוגמת פיירוולס המגנים על יישומי הרשת של הארגונים ומגבילים את הגישה למידע על כרטיסי האשראי; הקידוד של מידע שכזה בעת שהוא "במנוחה", כך שהוא יהפוך ללא קריא עבור המתקיף; וסקירה קבועה של האבטחה החברה על מנת להבטיח את הציות לתקנים הללו. הדרישות הללו מאפשרות את צמצום הסיכון שבזליגת המידע ואחריות הארגון.

דרישות ממשלתיות מסורתיות יותר, מספקות חוקים ורגולציות המכוונות באופן ישיר או באופן לא ישיר, למניעת זליגת המידע. ההגבלות של חוק הסארבנס-אוקסלי (SOX) דורשות מהארגונים להתמקד בפרקטיקות אבטחת המידע הטובות ביותר המוכרות כ-"Least Privilege Access". ה- Least Privilege Access קיימת כדי להגביל את החשיפה של המידע הרגיש רק לאלה שליש להם גישת Need-To-Know או Need-To-Have, על מנת שיוכלו לבצע את המשימות המוטלות עליהם.

למרות זאת, מספר רב של ארגונים אינו מחויב לרגולציות ממשלתיות או תעשייתיות. סוג הארגונים האלה, אשר ייתכן ואינו מחזיק מידע עסקי, יכולים להיות ישות פרטית חסרת בעלי מניות חיצוניות, וייתכן שאינה נתונה לדרישות ציות המונהגות ע"י התעשייה, דוגמת רגולציות ה- Health Insurance Portability and Accountability Act. למרות החיסרון הפוטנציאלי בדרישות ציות מנדטוריות, הארגונים הללו עדיין מנסים לשמור על חיסיון המידע של הלקוחות, מתוך ניסיון לשמור על המוניטין הארגוני שלהן, להציג את האחריות האתית שלהם, לשמור על אמון הלקוחות, ולהימנע מכל השלכה משפטית העוסקת באובדן המידע.

הפרקטיקות העצמאיות הללו הן ראויות לכל שבח. מומחי אבטחה יכולים ללמוד רבות מארגונים שפיתחו שיטות הגנה רק כדי להגן על עצמם, ולא כדי לציית לחוק כלשהו. פעמים רבות, ארגונים הפועלים מחוץ לתחום השיפוט של הרגולציה הפדראלית או לציות התעשייתי, הם בד"כ ארגונים

קטנים עם מעט עובדים ורווחים נמוכים. למרות זאת, על אף גודלם, דרישות האבטחה או תהליכים עסקיים מסוימים, ישנן כמה נקודות מכשילות בהן הארגונים הקטנים מסתכנים בזליגת מידע, בדומה לסיכונים אליהם חשופות הישויות הגדולות. יותר מכך, כאשר פגיעות שכזו נוכחת, היא יכולה להתפשט לאורך הארגון, ולא להישאר רק ביחידה או המחלקה הפרטנית. משום כך, הפתרונות במסגרת האפשרויות הכספיות הללו, המיושמות באופן מוצלח בארגונים הקטנים, יכולים להיות יעילים באותה מידע גם בסביבות העסקיות הגדולות יותר.

פתרונות זולים

הצעדים זולים שיפורטו, קיימים כפתרונות אבטחה טקטיים וזולים, אותם יכולים לבחור ארגונים כדי ליישמם ולצמצם בעזרתם את הפגיעות התורמת לזליגת המידע. תהליכים כאלה הם זולים, ומיושמים בקלות. צעדים שכאלה קיימים כדי להשלים תוכנית אבטחה מקיפה יותר, אשר יכולה לכלול יישום של טכנולוגיות אבטחה, שכירת כ"א מנוסה באבטחה, או שכירת חברות לשירותי אבטחה; יחדיו, תהיה לכל אלה השפעה חיובית על עמדת אבטחת המידע הכללית של הארגון.

צעדים שכאלה יכולים להיות מיושמים כדי להשיג אבטחה, וכדי להשלים את מניעת זליגת המידע באמצעות הרתעה, גילוי, והגנה. אמצעי ההרתעה נועדו למנוע מתוקף פחות מקרי או אופורטוניסט מלנסות ולעקוף את האבטחה כדי לבצע עבירה. בקרות המאפשרות הרתעה - דוגמת מדיניות אבטחה מקיפה - הן ניהוליות בטבען. הרתעה יכולה להיחשב כמניעתו של תוקף בטרם המקרה. ההרתעה ממנפת את הניתוח המנבא, כדי ליצור בקרות אקטיביות.

הזיהוי מאפשר את גילויה של התקפה אפשרית המתבצעת ע"י תוקף מקרי יותר. דוגמאות להתקפה שכזו יכולות לכלול סריקת רשת או שכפול מוגזם מדי של מידע רגיש.כל פעולה שכזו יכולה לרמז על התנהגות עבריינית יותר. בקרות המסייעות בזיהוי הינן טכניות ופיזיות יותר בטבען. דוגמאות טכניות כוללות רישומי מערכת, מערכות זיהוי פריצות או ניסיונות כושלים לכניסה למערכת. מנגד, דוגמאות פיזיות כוללות את זיהויה של פעילות עבריינית פוטנציאלית ע"י כ"א מנוסה וערני. גילוי ממנף את יכולת התגובה של הארגון, כדי לשמר את ביטחון המידע הרגיש.

הגנה היא המניעה או הדיכוי של התקפות הנמצאות כבר בעיצומן, המופעלות ע"י תוקפים נחושים. דוגמאות להתקפות כאלה יכולות לכלול את ניסיונות החדירה לרשת הפנימית של הארגון, באמצעות ניחוש הסיסמא או ההסרה של תיעוד רגיש מהמתקנים של הארגון. גורמים התורמים להגנה יכולים להיות ניהוליים, טכניים או פיזיים. יכולות ההגנה מוגברות באמצעות קיומן של בקרות ניהוליות, דוגמת "תוכנית תגובה למקרים" מפותחת, "וצוות תגובה למקרים" מיומן ומגוון, כמו גם פיתוחן של תוכניות ניהול להתמודדות עם הפגיעות. בקרות טכניות נוספות המסייעות להגנה, כוללות פיירוולס מבוקרים ומעודכנים ושימוש בפתרונות קריפטוגרפים מוכחים בהתייחס לכל המידע הרגיש. בהמשך נציג כמה פתרונות להרתעה, גילוי והגנה.

מדיניות, תקנים, תהליכים, וקווים מנחים

מומחי אבטחה מנוסים צריכים להכיר ביתרונות של תיעוד טוב, ובייחוד, ביתרונות של תקנים ומדיניות יעילה ושלמה. המסמכים הללו נחשבים ל-"Must Have" בזירת האבטחה, בשל הדרישות הנמצאות תחת מגוון דירקטיבות הציות. למרבה הצער, כמה ארגונים מחזיקים מסמכים כאלה רק כדי "לסמן וי" לצורך ביקורת החשבונות, במקום לנהל את תקנות האבטחה ותהליכיה. אין זו תופעה חדשה.

בעיות שעלולות לצוץ מאימן מדיניות רק לשם הציות כוללות:

מדיניות פזרנית: דרישות מוגזמות מדי, מעבר ליכולות הארגון. מדיניות לא שלמה: התמקדות בציות ולא באבטחה; חוסר כיוון. מדיניות מתנגשת: נובעת מחוסר ארגון או מחוסר ריכוז.

בעוד שפזרנות יכולה שלא להשפיע ישירות על זליגת המידע, היא לפעמים מקשה על ארגונים לציית למדיניות שלהם עצמם. סוגי מדיניות לא שלמים או מתנגשים הם מאתגרים יותר למניעת זליגת המידע. כדי להשיג הצלחה באבטחה, חשוב לארגון לספק חזון וגישה ברורים ושלמים, אשר צריכה להתאים למדיניות ולתקנים, וחשוב לא פחות גם לאכוף אותו. כל הליקויים במדיניות שצוינו קודם לכן, עלולים ליצור בלבול ולהוביל לאי-ציות למטרות הארגוניות.

כמו המדיניות, חשובים גם התהליכים והקווים המנחים של הארגונים. חוסר השלמות, שלא לדבר על קיומם, של מסמכים שכאלה אינם נבדקים פעמים רבות ע"י הדירקטיבות הרגולאטוריות, אך הם חשובים מאוד לציות. תהליכים וקווים מנחים מסייעים לכ"א העוסק באבטחה וגם לאלה שאינם עוסקים בה, במילוי המטרות שהוצבו ע"י המדיניות והתהליכים. ההנהלה הבכירה של הארגון, מנהלי התהליך ועובדי האבטחה, צריכים לעבוד יחדיו על מנת לבסס ולשמור על תהליכים וקווים מנחים המקלים על הצלחת האבטחה של פעילויות הארגון, כמו גם כדי לבסס ציות למדיניות רחבה יותר. השתתפות בפיתוח, אכיפה, ושמירה של תיעוד שכזה הינה עדות למחויבות הארגון לתפקוד המלווה במתן תשומת לב ושקדנות, באשר להגנת ה-PII.

ארגונים צריכים לפעול לפי פרקטיקות האבטחה הטובות ביותר, גם אלו הכלליות וגם אלו המוגדרות לתעשייה, ולכלול אותם בפיתוח התיעוד הארגוני (מדיניות, תקנים, נהלים וקווים מנחים). תיעוד צריך להיות מבוקר בצורה מרכזית ולהיות זמין לכל העובדים המתאימים ולהנהלה. בנוסף, בקרת החשבונות הפנימית או יחידת אבטחת המידע, צריכות לבקר את הבקרות המנהליות באופן קבוע כדי להבטיח את הציות.

בשנת 2007, ה-IT Policy Compliance Group, פרסמה תוצאות של מחקר אשר תיעד 16 סיבות מובילות לאבדן מידע. הסיבה שדורגה שנייה, המתרחשת פעם בכל ארבע מקרים, זוהתה כ-"הפרת מדיניות". בהתחשב בהשפעה השלילית של הפרות מדיניות, ההנהלה צריכה לכלול הגבלות מדיניות המתארות את ההשלכות הטמונות באי-ציות; ליישם מנגנונים מנהליים, פיזיים וטכניים, כדי לזהות את ההפרות; ולאכוף את ההגבלות הללו באופן קבוע.

נעילת המידע

אבטחת המידע רגיש או אבטחת האמצעים המאפשרים גישה למידע הזה, היא לעתים הצעד הראשון ליצירת סביבה המועדת פחות לזליגת מידע.

תדפיסים של התיעוד הם בדרך כלל האופן הרגיש ביותר לגניבה פיזית או לשכפול או מחיקה לא מורשית של המסמכים מהעסק. ישנם כמה אמצעים בעזרתם ארגון יכול להבטיח את ההגנה על תדפיסי התיעוד. אמצעי מקובל מאוד - ואחד שלא מנוצל כיאות - לביצוע המשימה, הוא אמצעי שכבר זמין מאוד: מנעולים. מקומות עבודה רבים מלאים בארוניות ובמגירות שנועדו לשמירת תדפיסים של התיעוד. לכן, אנשי האבטחה צריכים לשמור על שימור מרבי בחלל האחסון הזמין הזה, כמו גם על מנגנוני הנעילה.

כמו בכל אמצעי זהירות אחרים, הסגל צריך לקשור בין היישום של אמצעי האבטחה עם אובדן היצרנות. בהינתן שצוות האבטחה יכול להפגין את יכולתם לבצע את המשימות הבאות במהירות, וללא הפרעה, הסגל להשתכנע עד ליישם את אמצעי ההזהרה הבאים:

- זיהוי הסגל הדורש גישה לתיעוד ספציפי.
- בקרה בהפצת המפתחות.
- שמירת מפתחות גיבוי זמינים.

במאמר שפרסם, טוד פארו, הציע כמה עצות לאבטחת התיעוד הפיזי והגבלת הגישה לכל מידע PII רגיש, מפני תוקפים נחושים המנסים לבצע גניבת זהות או הונאה. בין שאר ההצעות שלו, פארו

מזכיר לקוראים שגם אם מנגנוני הנעילה שולבו לתוך הארגון, המשתמשים צריכים להימנע מפעולות מסוימות שיכולות להפחית את היעילות של מערכות כאלה ולאפשר למשתמשים להערים על בקרות האבטחה. כהרחבה למאמר, המשתמשים וצוות האבטחה צריך:

- להימנע מלהשאיר את המפתחות שלהם (או הצירופים) בשטחי אחסון גלויים דוגמת:
  - § מגרות שולחן לא נעולות.
  - § מתחת למקלדות או המסכים.
  - § קבועים לתחתית השולחן.
- הימנעות מהצגת מידע הנוגע למנגנוני הנעילה אשר יכולים לאפשר לתוקף ללמוד כל מידע באשר לתפקוד המנגנון.
- בדיקת המנעולים ווידוא כי אלו המיושמים נבחנו וקיבלו ציון טוב ע"י מכוני התקנים.
- הצבת מנגנוני הנעילה לבדיקה ארגונית ווידוא כי לא ניתן לעקוף את המגבלות הללו.

לבסוף, מבלי להתייחס לפרסומת של יצרני המנעולים, המנעולים בטוחים או ברי-הגנה רק לתקופת זמן מסוימת. אם מנעול יכול לעמוד בפני שבוע אחד של התקפה, אין טעם לבדוק אותו פעם בשנה. למנגנוני נעילה צריכים להתווסף מנגנוני בקרה, דוגמת סיורי אבטחה, או התקנת מצלמות במעגל סגור.

סיווג המידע

סיבה נפוצה לשימוש להוגן במידע היא חוסר הבנה מערכתית באשר למשמעות המידע, הרלבנטיות שלו לחומרים אחרים, או הרגישות הכללית שלו. לכן, הארגונים צריכים ליישם תקני סיווג מובנים ואחרים, המעודדים את העוסקים במידע להתייחס למידע רגיש ברמת הכבוד והבטיחות הנדרש.

סיווג המידע נחשב פעמים רבות לאבן הפינה, או הדרישה המוקדמת לפרקטיקות ניהול הסיכונים המוצלחות. בנוסף לניהול המידע, הסיווג מספק להנהלה הבכירה את המידע החיוני לקבלת ההחלטות הנוגעות לביטחונם של פרטי מידע או נכסים רגישים. נכסים הנתונים לסיווג המידע יכולים לכלול שרתי קבצים, שרתי רשת, מאגדי מידע או רשת אחסון אזורית. נכסים אחרים החומקים לפעמים מהדירוג המקובל הם דיסקים וכונני USB.

סיווג מידע או נכסים יכול להיקבע בכמה דרכים. כאשר מתייחסים ל-PII, הארגון יכול לייעד את דרגת הסיווג הגבוהה ביותר לאותן פיסות מידע שרגישות ביותר ללקוחות (דוגמת מספרי זהות, ומספרי כרטיסי אשראי). אובדן מידע שכזה בפורמט לא מקודד, נקשר בד"כ להפרת דרישות ציות, לעלויות דיווח, ולנזק במוניטין או במותג.

גישה אחרת יכולה להיות בהקצאת דרגות הסיווג בהתבסס על ניתוח ההשפעה העסקית הרשמית (BIA). תהליך זה יסייע בזיהוי נכסים ומידע שהם הקריטיים ביותר לארגון, יוביל את ההחזרה המועדפת של מערכות המחשוב, ואת שחזור התהליכים העסקיים הקריטיים, כחלק מאסטרטגיה רחבה יותר.

כדי למנוע זליגת מידע, ארגונים צריכים לאמץ מודל לסיווג מידע המתאים לפעילויות שלו. כל מידע שנשמר צריך להיות מזוהה, ויש לצפות מראש דרגת הנזק שיכולה להיגרם אם המידע יאבד.

הסיווג צריך להיות מזוהה בבירור, והמדיניות או התקנים המתייחסים לסיווג המידע צריכים להיות מבוקרים ונאכפים באופן קבוע.

הגבלות השימוש ברשת

אחסון וסיווג בטוחים של התיעוד הם רק דרך אחת מתוך כמה, בעזרתן יכולים ארגונים למנוע הסרה לא מאושרת של מידע ו-PII, וזהו רק צעד אחד לקראת ההגנה של המידע הזה. מידע הקיים בפורמט לוגי ומאוחסן בבסיסי מידע או מערכות עדיין יכול להיות בסיכון, ללא קשר ליישום בקרות האבטחה הפיסיות.

מבלי להשקיע סכומים גדולים של שעות עבודה או כספים לצמצום פגיעותן של מערכות ההפעלה והיישומים, ישנן כמה בקרות שנמצאות בתחום תקציב ה-IT של הארגון, אותן ניתן ליישם כדי לצמצם את הסיכון או האפשרות שזליגת מידע תנבע מתוך מכאניקה גרועה או קונפיגורציות גישה. בקרות כאלו יכולות לכלול את ההגבלות הבאות:

- הודעות מייל יוצאות.
- נגישות לאינטרנט
  - § בלוגים.
  - § גישה לאי-מייל (דוגמת Yahoo, Hotmail, G-mail).
  - § שירותי הודעות (AIM, Windows Messenger, Yahoo Messenger).
  - § שיחות צ'אט.
- שימוש במערכות USB.
- גישה לשורת הפקודה.
- תפקודיות ה-FTP/SFTP.
- eFax.

אם הפריבילגיות הללו אינן מוגבלות, הן יכולות להתיר למשתמשים העבריינים להוציא מידע רגיש מהתחום בו הם אמורים להישאר. בתחילה, המשתמשים צריכים להיות מוגבלים מכל פריבילגיות שכאלה ועליהם להראות כי הפעילות שלהם דורשת הרשאות שכאלה. צוות האבטחה צריך לדון על הגבלות הרשת עם ההנהלה הבכירה לפני היישום, ולאחר שפעילות כזו אושר קודם לכן תחת מדיניות שכן היא עשויה להשפיע לרעה על תפקוד הרשת. למרות זאת, הרשאות רשת נרחבות צריכות להיות מוכרות כזירות אפשריות לזליגת מידע, ויש לפקח עליהן.

ניהול היחסים עם הספקים

חששות באשר לזליגת המידע אינן מוגבלות רק למידע המעובד, המאוחסן והמנוהל בארגון, אלא שיש לתת את הדעת גם לכל המידע אליו הארגון האחראי. במאמץ להגן על מידע שכזה, ארגונים צריכים לבחון את ההסכמים החוזיים שלהם עם צדדים שלישיים באופן קבוע, על מנת להבטיח שהצדדים הלו מחוייבים לתנאי השירותים המאובטחים. ארגונים צריכים גם להבטיח את הביטחון של המידע שלהם, באמצעות השתתפות בהערכה או ביקורת של הספקים שלהם, כדי שיוכלו להבטיח שהבקרות מיושמות בהתאם להסכמים החתומים.

בנוגע לבקרות שהספקים צריכים ליישם, הארגונים צריכים לדרוש גישה מוגבלת למידע שלהם. משמעות הדבר היא התקנתן של ארוניות, מגירות ודלתות נעולות, עם גישה מבוקרת לחומרים רגישים, שימוש בכרטיסי מפתח, ושימוש בסיסמאות "חזקות". אלו רק כמה הצעות ליצירת סביבה בטוחה יותר לאחסון מידע. מטרת האחסון הבטוח היא, כמובן, להבטיח ולשמור על האמון, הזמניות,

והחיסיון של המידע הרגיש. דוגמא לשיטה "יקרה" להבטחת האחסון הבטוח יכולה להיות התקנת בקרות גישה ביומטריות.

אך גישה למידע רגיש היא רק חלק אחד מבעית זליגת המידע. ארגונים צריכים להיות מודעים לנושאים הסובבים את זליגת המידע בכל ההיבטים של מחזור החיים של המידע. לא מספיק לאבטח את המידע בזמן שהוא נשמר; מאבטח מידע טוב יבטיח שהמידע ייוצר באופן בטוח, שתינתן לו דרגת סיווג נכונה, לפי תקני הסיווג; ושהוא יישמר או יושמד בהתאם לרמת הסיווג.

ארגונים צריכים לא רק להבטיח שכל שלבי ארגון המידע מתאימים לפרקטיקות האבטחה בתחום הארגון, אלא גם שהפסקים והשותפים האחרים ימלאו את אותן הדרישות גם כן. הסכמים חוזיים צריכים להתחדש, וההערכות יבוצעו כדי להבטיח שבקרות אבטחה טובות יישומו באופן הולם.

ניתוח תנועה

ישנן כמה טכנולוגיות מסחריות מוכחות המספקות ל-IT הארגונית ולמחלקות האבטחה, את הכלים הדרושים להם כדי להעריך את תבניות התנועה, ניטור הגישה, דיווחי הפרות המדיניות הארגונית, וזיהוי ומניעת מקרים של זליגת מידע.מובילי שוק מניעת זליגת המידע כוללים את Vericept ו-Vontu. יישום הפתרונות הללו, מאפשר לארגונים להגביר את פוטנציאל הזיהוי והמניעה של הזליגה. למרות זאת, אם רכישת המוצרים הללו עולה על יכולות הארגון, ישנם כמה פתרונות רשת בחינם המאפשרים זיהוי של זליגת מידע, למרות שהכלים הללו עושים ברמה פחותה יותר.

ללא ספק, ישנם כמה חסרונות בשימוש בתוכנות חופשיות או במאגרים פתוחים. בהשוואה לכלים המסחריים, הכלים החופשיים אינם מקבלים את אותה התמיכה, גם בהיבט התמיכה ובהיבט פתרון הבעיות. פעמים רבות, כלים חופשיים חסרים את הממשק הגראפי אליהם מומחי ה-IT כבר התרגלו. כלים מסחריים מאפשרים למומחי ה-IT והאבטחה לבזבז פחות זמן בשורות הפקודה, ולהשקיע יותר זמן בפתרון הבעיות.

למרות זאת, עבור ארגון עם תקציב מצומצם, הכלים החופשיים הללו הינם אלטרנטיבה טובה. לכלים יש את היכולת לזהות אינדיקטורים רבים לזליגת מידע בנוגע לפעילויות רשת מסוכנות (כמו אלה שהוזכרו קודם לכם, דוגמת הבלוגים). בנוסף, הכלים החופשיים יכולים לזהות התנהגויות עברייניות אחרות, תקשורות חיצוניות שאינן יזומות לצדדים לא מורשים, זהו בד"כ סימן לחדירה למערכת.

הקביעה האם פתרון חופשי מתאים לארגון, נתונה להחלטת ההנהלה, עובדיה והמדיניות המוגדרת שלה. היתרונות והחסרונות של הכלים המסחריים והחופשיים נתונים לויכוח, אך עבור ארגון עם תקציב אבטחה או IT מוגבל, ההחלטה להפעיל טכנולוגיה חופשית היא פשוטה.

שימוש במידע "דבש"

שיטה זולה לזיהוי זליגת מידע אותה יכולים ליישם ארגונים בגדלים שונים, היא מספר בסיסי נתונים ארגוניים או מאגרי מידע עם מידע "דבש". מידע דבש הוא מידע לא מוגדר הנמצא בקרב מידע ארגוני לגיטימי. דוגמא למידע דבש יגולה להיות ההוספה של כתובת אי-מייל שאינה קשורה לעובד בארגון או ללקוח, בתוך בסיס הנתונים של כתובות האי-מייל הלגיטימיות. משום שהשימוש או התפוצה של הכתובת הזו יהיה נתון לפיקוח, קבלת האי-מייל או הפרסום של מידע הדבש, יהיה סממן לאבדן מידע.

אך השימוש במידע דבש אינו מוגבל רק לכתובות האי-מייל. מנהלי צוות הפיתוח יכולים לבחור לאכלס את בסיס המידע שלהם או ספריות הקבצים בהליכי יישום של קוד מקור שאינו משרתים כל מטרה פרט מזיהוי מקרי זליגה. קוד שכזה יכול להפוך לזמין בספריות הזמינות למשתמשים או במהלך שיתוף קבצים הדורש גישה מיוחסת. במקרה כזה השימוש בקוד הזה מציין גם את הזליגה ואת

השימוש הלא הולם במידע רגיש, אלא גם השימוש הנרחב והלא מאושר בפריבילגיות או בחסרונות של פרקטיקות ניהול הזיהוי של הארגון.

כפי שניתן להניח, ישנם כמה אמצעים שבעזרתם מנהל רשת יכול לחקור את הזליגה של מידע דבש. שיטה אחת תהיה להפעיל פיקוח מתמשך או תקופתי על משאבי הרשת. הדבר יכול לכלול את הפריצה הפשוטה ביותר למנוע חיפוש או השימוש בסקריפטים אוטומטים על מנת לחדור למשאבי הרשת. לא חשוב איזו שיטה מיושמת, העיקר הוא שהאדם האחראי לפעילויות החיפוש יזכור לחפש לא רק באינטרנט, אלא גם בפרסומים מוטמנים וערוצי תקשורת אחרים דוגמת, IRC. כמובן, השיטה הזו יכולה להיות מופעלת גם על מנת לזהות את השימוש או הפרסום של מידע לגיטימי.

שיטת החקירה השנייה תהיה לפקח או לעצב סביבת התרעה לשימוש במידע דבש. אם נשתמש בדוגמת האי-מייל שהוצגה קודם לכן, מנהל הרשת יהיה אחראי לגישה התקופתית של חשבון הדבש ויבטיח שתיבת ההודעות הנכנסות אינה מכילה חומרים מצד-שלישי. אם התיבה אכן קיבלה הודעה מציידי כישרונות או מתחרים, תהיה זו עדות שספריית האי-מייל הארגונית נמצאת בסיכון. כדי להמשיך את אמצעי הפיקוח והגברת יכולת הזיהוי של מידע דבש, ארגונים בהם האבטחה מפותחת יותר יכולים לבחור לעצב את מערכות זיהוי או מניעת החדירה, כדי לזהות חתימות ספציפיות הקשורות למידע דבש. אזהרה מוקדמת יכולה להיות במיטבה, באמצעות השימוש ב- Host-Based Intrusion Detection System (HIDS) הקיימת במערכת המאחסנת מידע דבש, או באמצעות הצבת חיישן Network-Based Intrusion Detection System(NIDS) בקרבה למערכת הזאת.

בעוד שקוד המקור וספריות האי-מייל חשובות לארגון, אם הארגון אחראי לאחזקה ולאחסון של ה-PII, האבטחה של מידע שכזה צריכה להיות באחריות מנהלי הרשת וההנהלה הבכירה. לאחר הגילוי של מידע דבש, האחריות לבדיקת הזליגה יכולה להיות של צוות התגובות של הארגון. בהינתן טבעו של השימוש במידע דבש, הארגון יכול לבחור גם להשתמש במיקור חוץ, על מנת לחקור את הזליגה, או אפילו לפנות לרשויות החוק. להנהלה הבכירה צריכה להיות תוכנית מוכנה לניהול מידע דבש, כמו גם תוכנית תגובה לניהול זליגת המידע הזה, משום שהגילוי הזה יכול לגרום לבלבול בקרב הארגון ובקרב אנשים חיצוניים לו המחזיקים מידע שכזה.

השפעה ארגונית

היישום של פתרונות זולים אליהם התייחסנו קודם לכן במאמר, הוא התחלה טובה להגבלת הסיכונים שבזליגת המידע, וללקיחת ההחלטות הארגוניות לקראת שמירה על פרטיות; למרות זאת, בשום אופן לא ניתן יהיה לשמור על המידע הארגוני רק באמצעות יישומם של אלה. ארגון יהיה צריך להשקיע כדי שיוכל לשמור על הפרטיות ועל הביטחון הכולל של המידע. ההשקעות צריכות לכלול, אך לא להיות מוגבלות רק לנושאים הבאים:

- שכירת מומחי אבטחה מנוסים.
- הכשרה בנושאי אבטחה לסגל האבטחה הקיים.
- הכשרה בסיסית בנושאי אבטחה ומודעות לכל העובדים.
- בקרות גישה.
- ניהול זהויות הגישה.
- רכישה ויישום של טכנולוגיות אבטחה מוכחות:
  - § כ זליגת מידע.
  - § אכיפת מדיניות.

§ מערכות לזיהוי/מניעת חדירה.

§ אנטיוירוס.

§ פתרונות קידוד.

• שדרוג האבטחה הפיזית.

משום שכמה מהפתרונות הללו יהיו יכולים להיות יקרים לכמה ארגונים בעלי תקציב IT נמוך, אלטרנטיבה אחת המאפשרת יישום הדרגתי יותר היא השימוש בצד שלישי אמין, אשר יכול להעריך באופן תקופתי של "נוף הפגיעות". הערכת צד שלישי אינה פתרון ארוך טווח לארגון בתקציב מצומצם; אך הניסיון הארגוני, המחויבות לאבטחת המידע, והיכולת להיות עצמאי הן בד"כ הסיבות להערכה שלמה, מקיפה, ולא משוחדת של עמדת האבטחה הנוכחית של הארגון.

סדר עדיפויות ומדידה

בעוד שהשיטות היעילות להרתעה, גילוי והגנה יכולות להיות מיושמות, ארגונים צריכים מבנה מוכן לתיעוד ומעקב אחרי זליגות, כמו גם אחרי ההתקדמות שלהם לקראת פיתרון. בנוסף, הערכות זליגת מידע יכולות לטמון בחובן, מגוון של טכניקות לגילוי פגיעות. בהתייחס לצורך שבמבנה כזה ובטבע ההערכה, ארגונים יכולים לבחור בגישה המביאה בחשבון את המדידה וסדר העדיפויות של הפגיעויות, בהתבסס על המיקוד הטכני שלהן, כמו גם על היחס עלות/משאבים המתאפשר לתיקון כל פגם.

לעתים נדירות יצליח ארגון לתאר באופן ברור את היחס שבין העלות ויכולת הטכנית. כתוצאה מכך, ההנהלה הבכירה תתקשה להמשיג את היתרונות והערך של יזמות אבטחה מסוימות, כאשר הן יושוו לאחרות. למרות זאת, תקשורת טובה עם ההנהלה הבכירה תשפיע באופן נרחב, אם לארגון יהיו (1) מתודולוגיה מבוסס וגישה להערכת הפגיעויות. (2) מאגר מרכזי לאחסון ולשמירת ידע המתייחס לאפשרות הזליגה. (3) מודלים מבוססים לתקשורות בנושאי זליגת מידע (4) בסיס לייחוס עלות הניצול למול קבלת הפגיעות.

בהמשך להחלטה ליישם יוזמות שנועדו לתקן את הפגיעות לזליגת מידע, ההצלחה של יזמות כאלה תועצם באופן משמעותי באמצעות התמיכה המתמשכת מצד ההנהלה הבכירה. בשל כך, חשוב מאוד שהארגונים יספקו שיטת מדידה מתמשכת והולמת להנהלה, כדי שזהו תוכל להכיר באבני הדרך שהשיג צוות האבטחה, או להקצות משאבים כדי לתמוך בהשלמה הטכנית של יזמות כאלה.

בעת שסוגי הפגיעות לזליגת מידע שונים מארגון לארגון, חשוב שמבנה הדיווח המדיד יימצא, כדי להדריך ולשלוט ביזמות זליגת מידע,וכדי להעצים ולמנף באופן יעיל את הזמן של ההנהלה הבכירה. כדי להשיג זאת, ולהתייחס באופן מדויק לחששות של הצדדים המעוברים, המדידה של זליגת המידע צריכה להיות מרוכזת ומגובשת, כשהם עולים בדרגות ומגיעים להנהלה הבכירה.

נושאים למחשבה

כאשר דנים בשאלה האם מניעת זליגת המידע היא במסגרת האפשרויות הכלכליות, או לא, הארגונים צריכים לשקול את השאלות הבאות:

האם אנחנו יכולים לסבול את סיכוני זליגת המידע מבלי שייגרם נזק משמעותי ללקוחות שלנו?

האם אנחנו יכולים לסבול את סיכוני זליגת המידע מבלי שייגרם נזק משמעותי למוניטין שלנו?

האם אנחנו יכולים לסבול את סיכוני זליגת המידע מבלי שייגרם נזק משמעותי לעובדים שלנו?

האם אנחנו יכולים לסבול את סיכוני זליגת המידע מבלי שייגרם נזק משמעותי לשורה התחתונה שלנו?

היכולת לממן את הפתרונות שהוצגו במסמך זה ישתנו מארגון אחד למשנהו, אך לרוע המזל, גם המשאבים הקשורים לפעילויות צמצום הסיכונים הזולות ביותר, עלולות להיחשב ע"י מנהלים בכירים כיקרות מדי.

לעתים קרובות מדי, ההנהלה הבכירה מאמינה שהפתרון יהיה יעיל רק אם הוא יישום באופן מלא ובמהירות באמצעות הקדשת המשאבים המקסימאלית. אך במקום זאת, יזמות האבטחה והיישום של פרקטיקות אבטחה, התהליכים והטכנולוגיה, צריכות להיחשב כחלק מתהליך שדומה יותר למרתון. צעדים נלקחים בהדרגה כדי להשלים כמה מטרות, להבטיח איכות, ולספק אבני דרך להשלמת תבנית ההתקדמות של הארגון.

הכרת כמה מהשיטות הזולות יותר לצמצום זליגת המידע, פיתוח גישה למדידה, לתיעדוף, לדיווח ולשילוב הידע הזה בהבנה שאבטחה הא תהליך שישפר באופן ניכר את יכולתו של הארגון לעשות רציונליזציה למימון, להשתמש ולהקצות באופן טוב יותר את תקציב המניות, ולשפר באופן דרמטי את מצב האבטחה בארגון.