פתרונות חכמים להגנת מערכת המידע של הרשויות המוניציפאליות וארגונים אחרים

אלי סיסו, מנהל תחום אבטחת מידע, טלדור תקשורת גלאסהאוס

דמיינו לעצמכם שאתם מתעוררים בבוקר, מתלבשים ויוצאים לעבודה ברכבכם. באמצע הדרך, כתוצאה משיבוש במערכות הרמזורים, רמזורים אדומים הופכים לירוקים ומובילים לעשרות תאונות בין כלי רכב, תוך יצירת פקקי תנועה ענקיים בכל העיר. תיאור זה הינו חלק מסצינה בסרט ההוליוודי הג'וב האיטלקי. בסרט, האקר משתלט על מערכת בקרת התנועה בעיר לוס אנג'לס באמצעות שימוש בנקודה ציבורית של ה- WiFi העירוני, משתק את תנועת הרמזורים ויוצר פקק תנועה לשם ביצוע שוד. הסצינה המתוארת היא אומנם חלק מסרט אבל היא אינה רחוקה מהמציאות היומיומית המאפשרת השתלטות גורמים עוינים על מערכות העירייה.

בשנים האחרונות אנו חווים מלחמה מסוג חדש, המאיימת על ממשלות, ארגונים ומוסדות ציבור שונים. מלחמת הסייבר, שמימדיה גדלים עם השנים, חושפת ארגונים רבים לאיומים מגוונים בתחום אבטחת המידע והסייבר. רק לפני כשבוע, הזהיר האף בי איי שהאקרים הקשורים לקבוצת אנונימוס, הצליחו לחדור למחשבי הממשל ולגנוב מהם מידע רב. במזכר האף בי איי נכתב שההאקרים ניצלו פרצה בתוכנה של חברת אדובי כדי לבצע שורת פריצות שהחלו בדצמבר האחרון. לאחר מכן, הם הותירו "דלתות אחוריות" שיאפשרו להם לחדור שוב לאותם מחשבים בשלבים מאוחרים יותר.

הגנה על מאגרי המידע מפני גישה ושימוש של אנשים בלתי מורשים, היא דבר הכרחי וחשוב להתנהלות בריאה ויציבה של כל רשות, ארגון ועסק בכל ימות השנה. לאור הקדמה הטכנולוגית, כולם נדרשים להתאים עצמם למציאות החדשה שכוללת איומים מתוחכמים הרבה יותר מאשר בעבר. ההגנה מפני האיומים האלו באמצעות מערכות מתוחכמות הופכת להיות קריטית וחשובה לאין שיעור כאשר מדובר בשמירה על תפקוד יומיומי תקין של הארגון. האיומים הקיימים ברשויות מקומיות הם איומים ממשיים, הן לעירייה והן לתושבי העיר ולאזרחי המדינה. בהתממשותם עלולה להיפגע איכות חייהם של תושבי העיר שההגנה על מערכות המידע שלה אינה מספקת. רשויות מקומיות רבות, טרם הפנימו את האיום הממשי הקיים עליהן והן ממשיכות להפעיל מערכות בעלות פתרונות מסורתיים בלבד ולא בהכרח פתרונות סייבר המתאימים לתקופה המאתגרת בה אנו חיים.

במציאות של היום, מערכות שסורקות תכנים לצורך זיהוי קוד עוין אינן יעילות כנגד האיומים של הדור החדש. מערכות אנטי וירוס שמספקות רשימות שחורות של קודים עוינים גם הן אינן יעילות עוד, ומחקר ידני שנעשה ע"י אנשי מקצוע דורש השקעה עצומה במשאבים, שלא תמיד קיימים בידי הרשות. גם ציוד אבטחת המידע התשתיתי אינו מספק מענה אל מול האיומים החדשים. יש צורך במערכות מתוחכמות שיעמדו מול האיומים הללו, באופן יעיל ומהיר תוך שמירה על ביצועי מערכת ההפעלה והמחשוב.

כיום, כל עובד בכל ארגון מחזיק דיסק און-קי אישי ועושה בו שימוש להעלאת והורדת קבצים למחשבי הארגון המאובטחים. בכך הוא מאפשר הרצת קבצים מסוכנים בעלי קוד עוין אף מבלי לשים לב לכך. גם גלישה באינטרנט במחשבי הארגון עשויה להיות מסוכנת ולהוביל לכניסה של קודים עוינים לרשת. קושי ממשי הקיים בכל ארגון ורשות הוא זיהוי קוד עוין שנכנס לרשת ונמצא בהיחבא וכן, מניעה מאותו קוד לפעול ברשת ולפגוע בה. חברת טלדור, מתמקדת בפתרונות אבטחת מידע של הדור הבא, משקיעה בהכשרת צוות אנשי האבטחה בדיסציפלינות הנדרשות לניטור וניתוח הרשת.

אלי סיסו

התקופה בא סמכנו על מוצרים ויצרנים שיספקו בבלעדיות את המענה עברה.

כיום יותר מתמיד יש צורך בהכשרת אנשי האבטחה במשימות שונות מהעבר, סקירה של הרשת, ניטור, ניתוח, הדרכות עובדי הארגון ועוד. דוגמאות להטמעת פתרונות הדור הבא של חברת טלדור, מערכת בקרה ה- Security Analytics המזהה כל דבר חריג שקורה ברשת ומזהירה את הארגון מפניו ומערכת Sandbox, מריצה את הקבצים, קודם כל בסביבה מאובטחת, ורק אם הקבצים נקיים ואין בהם קוד עוין הם עוברים לרשת. המערכת יוצרת הטעיה עבור הקובץ, שחושב שהוא רץ במערכת ההפעלה הרגילה ולא באזור מאובטח.

לאחרונה, צצים סטארטאפים חדשניים בתחום הסייבר, המאפשרים זיהוי וטיפול איכותי בגורמים המסכנים את טכנולוגיות המידע של ארגונים ורשויות מקומיות. טלדור עוטפת את פתרונות הסטארטאפים המתקדמים כחלק מהפתרון הכולל שהיא מציעה ללקוחותיה. לדוגמא Advanced endpoint security הוא סוכן שיודע לאבחן כיצד המערכת צריכה לפעול וכך ניתן יהיה לזהות את מה שלא פועל בה כראוי. דרך נוספת וחדשנית לזיהוי מתקפות ואיומים היא יצירת HoneyPot, דהיינו מלכודת דבש. יצירת המלכודת נעשית ע"י יצירת אזור חשוף ברשת שנראה כמו רשת פעילה וימשוך אליו את כל הגורמים העוינים שבפועל יתקפו בסביבה וירטואלית. באמצעות פעולה זו, הארגון והרשות יכולים לזהות את הגורם המתקיף, ולסמן אותו כגורם עוין.

הגנה נוספת על טכנולוגיות המידע ניתן למצוא בשירותי ענן בעולם הסייבר. שירותי הענן מאפשרים זיהוי Botnet, הלא הוא סוס טרויאני חכם, שמתחבר לשרת בצורה סמויה ונשלט מרחוק ע"י האקר הנותן פקודה להפעלתו. במידה וארגון מגלה שהוא חשוף ל- Botnets ומעוניין לזהות איזו תחנה בשרת נגועה הוא יכול לבחון זאת באמצעות שליחת ה- Log, המצוי בציוד אבטחת המידע התשתיתי (כגון Firewall), אל הענן שינתח אותו וימפה את מיקומו המדויק.

הפתרונות המוצגים, אינם פתרונות מלאים, אך הם בוודאי ממלאים את הצרכים הבסיסיים של הרשות. רשות שלא תדאג להגן על אבטחת המידע שלה, תמצא את עצמה בפני התקפות סייבר שעשויות, ביום מן הימים, לשתק אותה באופן מוחלט. חברת טלדור, בוחנת באופן שוטף פתרונות חדשניים בתחום הסייבר, כאלו שיבטיחו לכל רשות מוניציפאלית ביטחון מירבי.

Taldor
we deliver IT
GlassHouse
INFRASTRUCTURE::OPTIMIZED