"ב-CyberArk הגדרנו את המשתמשים האלה, שקרויים משתמשים פריבילגיים, כאתגר האבטחה הגדול ביותר. לשם כך עלינו תחילה לזהות את אלה שעלולים להוות דלת אחורית למערכות המיחשוב של הארגון, לשמר אותם - כלומר, לדאוג להחליף להם סיסמה באופן סדיר, ולנהל אותם נכון כדי להשיב את השליטה לאנשי התשתיות", הוסיף.

מזור דיבר בנוסף על התהליך לאיתור השימוש לרעה בסמכויות של משתמשים פריבילגיים. "יש לכך מספר שלבים: ראשית - בידוד מלא בין המחשב של המשתמש לבין המערכת באמצעות שרת פרוקסי. השלב השני - הקלטת כל הפעילויות - מסכי כניסה למערכת, הודעות והתראות, ובשלב השלישי - שימוש במערכת פרו אקטיבית לזיהוי איומים ולזיהוי אנומליות בשימוש".

"דוגמה לאנומליות כאלה היא שעות כניסה שאינן שעות העבודה הרגילות במערכת; פעילות חוצת משמרות; משתמש שניגש פתאום למערכות רבות יותר מאשר מספר המערכות שהוא נכנס בשימוש השוטף שלו, גם אם מותר לו להיכנס לכל המערכות הללו, ועוד. כל האנומליות נכנסות למערכת הבקרה וכל אנומליה כזו מקבלת ניקוד".

מערכת שמנטרת פעילות משתמש באמצעות וידיאו

אריק קשה, מנהל מכירות אזורי ב-ObserveIT, תיאר מערכת המנטרת את פעילות המשתמש באמצעות וידיאו. היא מאפשרת ניתוח מהיר של אירועים, בצורה קלה להבנה הרבה יותר מאשר שימוש בלוגים.

"יש למערכת שלנו יכולות הקלטה, ניטור וחיפוש. מאחר שיש בה גם את אפשרות ההקלטה בווידיאו וגם את המטה-נתונים (מי נכנס, מתי ולאן), מנהל אבטחת המידע יכול לראות בדיוק מה קרה באותו סשן", הוסיף.

"ההקלטה בווידיאו חכם מאפשרת לדעת שלב אחרי שלב מה נעשה", ציין קשה. "מכיוון שאנחנו לא רק מקליטים זמן המתנה אלא רק מצלמים את המסך כל פעם שהמשתמש מקליק על המקלדת או העכבר. הווידיאו צורך מעט מקום. שנית, אנחנו מאנדקסים כל פעולה כדי שנדע לזהות אותה בהמשך. כך נוכל לזהות כל שלב בפעילות המשתמש ואם היא לא מתאימה לדפוס שלו, המערכת מתריעה וניתן בקלות לנתח את הפעילויות".

"גם המערכת של ObserveIT עוקבת אחרי משתמשים פריבילגיים, ואחת ההנחיות שלה היא לדרוש מהם להיכנס בסיסמה פרטית ולא בחשבון אדמין", אמר.

"מנהלי אבטחת מידע משתלבים בליבת העסקים בחברה"

"שוק אבטחת המידע משתנה ורואים יותר ויותר מנהלי אבטחת מידע משתלבים בליבה העסקית של החברה, בפרויקטים שהיא מבצעת. הם מתקרבים לצד של הלקוחות ומבינים שאבטחת מידע לא יכולה לפגוע בחוויית המשתמש ולא יכולה לגרום לאיטיות. הם חייבים לספק אבטחת מידע במהירות החדשנות העסקית של הארגון", כך אמרה **הילה מלר**, מנהלת האסטרטגיה של CA באירופה לתחום אבטחת המידע.

לדבריה, "אנשי אבטחת המידע צריכים פתאום לדבר בשפה אחרת, במונחים עסקיים. השינוי הזה מחייב את מנהלי אבטחת המידע להיות מכוונים יותר לצדדים העסקיים ופחות לצדדים האופרטיביים הטכניים של עולם אבטחת המידע".

אריק קשה

היא עמדה על פן נוסף שבו מרגישים, לדבריה, שינוי בשוק, בכל הקשור לאבטחת מידע. "זהות המשתמש נהיית מרכיב חשוב במעגלי אבטחת המידע, מאחר שהארגונים מחויבים, בגלל צרכים עסקיים ותחרותיים, להיפתח לעולם החיצון, לענן, למוביליטי, ל-BYOD, לרשתות החברתיות", אמרה מלר. "כשעובדים בארגון פתוח, זהות המשתמש היא מרכיב האבטחה המרכזי. פיירוולים פחות חשובים והגנה על תחנות קצה פחות חשובה, כי רוצים לאפשר למשתמשים את הכול".

> הילה מלר: "כשעובדים בארגון פתוח, זהות המשתמש היא מרכיב האבטחה המרכזי. פיירוולים פחות חשובים והגנה על תחנות קצה פחות חשובה, כי רוצים לאפשר למשתמשים את הכול"

"מרכיב חשוב בשרשרת אבטחת המידע הוא לדעת מי המשתמש ומה הרקע שלו", הוסיפה. "ניתן לקבל בעזרת הידע הזה החלטות מושכלות, למשל האם לפתוח או לסגור גישה, או באיזו רמה לספק אותה".

הילה מלר

מלר דיברה גם על האינטרנט של הדברים וציינה ש-"מדובר בדבר חדש שעלינו להתכונן אליו. אנחנו, ב-CA, כבר לא מסתכלים רק על משתמשים אנושיים אלא גם רואים שחלק גדול מזרימת המידע מגיע מ-API, כלומר - מרכיבים חכמים שמתחברים לרשת. בעולם הזה אי אפשר לבנות אסטרטגית אבטחת מידע כוללת שמתייחסת רק לצד האנושי של הסיפור, חייבים לכסות גם את ה-API".

"קיימות טכנולוגיות שיודעות לנהל ולאבטח מפניו", אמרה. "ל-CA, לדוגמה, יש מוצר שיודע לנתח את כל תעבורת ה-API בארגון, שמאפשר לטפל בהרשאות הגישה ובכך למנוע סיכונים שקשורים לחשיפת הארגון החוצה באמצעות API."

המקרה של Target

ישי ורטהיימר, דירקטור אבטחת מידע ב-KPMG סומך חייקין, סיפר על אירוע חמור בתחום שהתרחש בארצות הברית בסוף השנה שעברה: האקרים נכנסו למחשב של חברה קטנה המספקת מקררים לכמה מסניפי רשת המרכולים הענקית Target והצליחו דרכם להגיע לסיסמאות גישה לרשת עצמה. באמצעות הסיסמאות הללו הם התחברו לקופות ומשכו בזמן אמת כל את נתוני הפס המגנטי בכל העברה של כרטיס אשראי שבוצעה בהן. בדרך זו הם גנבו 40 מיליון פסים מגנטיים שאפשרו לשכפל את הכרטיסים. לאחר מכן הם מכרו את אותם הכרטיסים ברשת והרוכשים יכולים היו לצאת למסעות קניות על חשבון הלקוח או, אם הוא שם לב לבעיה, על חשבון חברת כרטיסי האשראי.

יצוין כי בנוסף ל-40 מיליון הכרטיסים נגנבו באותה הפריצה 70 מיליון פרטים אישיים של לקוחות Target. לדברי ורטהיימר, "מלבד היקף הפריצה, מה שחמור במקרה הזה הוא שחברת אבטחת המידע זיהתה שיש בעיה, אך המנהלים לא התייחסו לכך, רק לאחר כחודש, כשמומחי