Abstract

Criminalitatea informatică este greu de investigat și efectuat, ceea ce a încurajat atacatorii cibernetici.Instrumentele de astăzi utilizate pentru detectarea breșelor dintr-un sistem utilizează tehnologii vechi pentru detectarea și eliminarea codului nesecurizat și cu scop răuvoitor înainte de a ajunge la infrastructura organizației. Modurile de abordarea tradiționale în securitatea cibernetică au fost eficiente în trecut dat fiind faptul că acestea se bazau pe apărarea perimetrului cu instrumente de detecție bazate pe semnătură. Astăzi, aceste instrumente nu mai fac față noilor tipuri de atac. Codul rău-intenționat, care permite ocolirea instrumentelor bazate pe semnătură, este disponibil tuturor atacatorilor. De cele mai multe ori, acești malware-uri sunt dezvoltați să exploateze vulnerabilități necunoscute ale unor software-uri instalate pe calculatoarele victimelor. Chiar dacă aceste vulnerabilități sunt descoperite și raportate, de-obicei, ia o perioadă lungă de timp până un patch este livrat de către furnizori și instalat de către organizații. Instrumentele precum managementul securității informației și al evenimentelor (SIEM) permit organizațiilor să consolideze datele de la mai multe dispozitive de securitate într-un singur sistem. Mai multe organizații au investit substanțial în infrastructură pentru a stoca informații legate de către log-ul evenimentelor ca parte din eforturile lor de susținere a securității. Unele organizații țin chiar înregistrări ale întregului trafic al rețelei pentru a detecta anomalii comportamentele precum descărcări bruște ale unor fișiere foarte mari. Însă, SIEM este eficient doar în mediile cu suficient personal și putere de procesare apropiate susținerii investigației și analizei. Mai mult, astfel de sisteme nu mai funcționează corect datorită cantității mari de date și analizei extrem de reduse. De cele mai multe ori, majoritatea datelor sunt pur și simplu arhivate. Instrumentele de analiză asupra cantităților mari de date și puterea de calcul ieftină a deschis noi oportunități în spațiul cibernetic. În timp ce atacatori își pot schimba instrumentele și abordările, modurile lor de operare rămân de cele mai multe ori aceleași. Această constanță comportamentală permite tehnologiilor de analiză de a detecta posibile atacuri rău-intenționate într-un timp mai scurt. Aceste sisteme iau în considerare profilul utilizatorului, comportamentul și normele de afaceri pentru a stabili pragurile în care evenimentele pot fi considerate anomalii. Instrumentele de securitate tradiționale funcționează folosind pattern-uri predefiniți și scenarii modelate în funcție de atacuri din trecut pentru a detecta și bloca comportamente suspicioase. Analiza datelor se poate raporta la cum un comportament normal zilnic arată și poate indica anomalii precum un calculator care brusc descarcă fișiere foarte mari. Utilizând modele matematice avansate, un mediu normal este modelat astfel încât activitățile care deviază de la cursul normal să se află între un interval statistic bine stabilit și să declanșează automat mecanismele de apărare. Ceea ce este considerat normal poate fi abstractizat până la nivelul de profil al utilizatorului. Pe baza modelelor matematice, utilizatorii sunt grupați în funcție de mai multe caracteristici și au o limită de bază care este stabilită pentru acel grup de utilizatori. Comportamentul rețelei care deviază de la caracteristicile grupului sugerează iregularități și investigații viitoare. În ciuda provocărilor privind normalizarea unor cantități atât de mare de informații de la surse dinamice și diferite, big data va juca întotdeauna un rol important în securitate. Prin incorporarea acesteia în programele de securitate, organizațiile creează un context mai bogat pentru minimizarea riscurilor și învață ceea ce este normal în activitatea unui anumit de tip utilizator, grup sau proces. Securitatea cibernetică este un proces constant de reacție la posibile amenințări în timp ce se adaptează la noi cerințe și nevoi ale unei organizații. Analiza în domeniul securității cibernetice poate îmbunătăți prevenția și poate reduce timpul între incident și detecție. Componentele cheie ale unui astfel de sistem sunt: sursele de date, mediul de stocare a datelor, interfața cu datele, motorul de analiză și prezentarea.