Spor mistænkelig adfærd og tag sikkerhedstrusler i opløbet

Nøglen til at forhindre datalæk er at opdage mistænkelig brugeradfærd, inden sikkerhedsbruddet forekommer. Et stærkt teknologisk partnerskab mellem Microsoft og 2ndC gør det muligt øjeblikkeligt at spore trusler, reagere præcist og effektivt på angreb og automatisk blokere adgange til sensitive systemer direkte i 2ndC Compliance Suite.

Brugere er blevet et fristende mål for hackere, og både angrebenes hyppighed og raffinement stiger. Ifølge Microsofts seneste Security Intelligence Report voksede antallet af angreb på brugeridentiteter med hele 300 pct. fra 2016 til 2017.

Brugeroplysninger er nemlig hackernes hellige gral. I en undersøgelse af 905 phishing-angreb var langt størstedelen af angriberne (91 pct.) ude efter user credentials. Ligeledes sker hele 63 pct. af datasikkerhedsbrud, fordi hackere får adgang til virksomhedens IT-netværk gennem stjålne brugeroplysninger .

Beskyt virksomheden med datadrevet machine learning

Sandheden er, at der ikke findes uigennemtrængelige it-systemer. Hvis der sker brud på jeres sikkerhed, er der kun én måde, I hurtigt kan begrænse skaden: Spor bruddet hurtigt. Endnu bedre er det, hvis I kan opdage mistænkelig brugeradfærd, inden bruddet forekommer. 2ndC Compliance Suite er det ideelle værktøj. Det optimerer arbejdsgangene knyttet til bruger-, identitets- og adgangsstyring og er jeres garanti for, at de rette personer – og kun de rette – har adgang til de rette data og systemer.

Compliance Suite er er en add-on til Azure, så udbyttet af jeres Microsoft-investering maksimeres. Har I samtidig tildelt jeres brugere Office 365 Enterprise E5-licenser, beskytter Compliance Suite jer mod cybercrime via Microsoft Intelligent Security Graph (ISG). ISG trækker på enorme datasæt, og via machine learning og behavioral analytics kan systemet lynhurtigt opdage anormaliteter og identificere trusler, så I bliver opmærksomme på mistænkelig adfærd i realtid.

På baggrund af adfærdsevalueringen tildeler ISG alle brugere en numerisk trus-selsscore, der strækker sig fra ”low risk” til ”high risk”, alt efter, hvor risikabel deres adfærd er. Det gør det muligt øjeblikkeligt at spore mulige trusler og præcist reagere på interne og eksterne angreb.

[1] https://www.microsoft.com/en-us/security/Intelligence-report

[2] 2016 Data Breach Investigations Report - http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Beskyt jeres forretningskritiske systemer

Værn om vigtige data og ressourcer med risikoberegnet adgangsvurdering.

Beskyt jeres data mod brugerfejl

Udnyt indsigten i brugernes adfærd, og bliv opmærksom på risici, før de udfolder sig.

Spor angreb, før de volder skade

Afdæk mistænkelig adfærd og identificer trusler, før angrebet sker.

Kontakt 2ndC

CEO Jesper Bergstedt
E: jb@2ndc.dk
T: +45 3165 3444
www.2ndc.dk

2ndC
Kgs. Nytorv 8,3
1050 København K
2ndC.dk
info@2ndc.dk

Bloker automatisk adgangen til sensitive systemer

Compliance Suite er forbundet med Intelligent Security Graph, og anvender risikovurderingen til at definere regler for brugerrollerne. Ud fra jeres konsekvensvurdering af, hvilke systemer og applikationer, der er særligt sensitive, fastlægger Compliance Suite en grænseværdi, som brugernes trusselsscore ikke må overskride, hvis de skal bevare adgang.

En økonomidirektør ville f.eks. have ret til at oprette kunder, og ret til at udbetale fakturaer via ERP-systemet. Han bevarer dog kun retten til at udbetale fakturaer så længe hans trusselsscore ikke overstiger en på forhånd defineret værdi.

Hvis ISG vurderer, at økonomidirektørens brugeradfærd er mistænkelig og dermed opjusterer trusselsscoren, notificeres Compliance Suite med det samme og lukker automatisk for hans adgang til at udbetale fakturaer. Ved kun at spærre adgangen til de mest sensitive funktioner ved mistanke om et angreb, tillader det brugeren at fortsætte sit daglige arbejde, mens sikkerhedsrisiciene undersøges og afhjælpes.

Compliance Suite rapporterer øjeblikkeligt adgangsændringen til brugerens nærmeste leder, og registrerer i loggen, hvorfor og hvornår brugeren har mistet sin adgang samt, at lederen er adviseret. Dermed er I helt sikre på at leve op til gældende lovgivning – samtidig med, at I beskytter jer selv og jeres data mod forretningskompromitterende adfærd og angreb.

Microsoft Intelligent Security Graph (ISG) evaluerer risici på adskillige kriterier, men de hyppigste er:

- **Umulig rejseaktivitet.** Hvis en bruger anvender sin adgang i København og 10 minutter senere logger ind fra en lokation i Asien, bliver aktiviteten markeret som risikofyldt. Det ville være umuligt for enhver at bevæge sig fra den ene lokation til den anden inden for det tidsrum. Derfor er det sandsynligt, at brugeren er blevet kompromitteret.
- **Ukendte lokationer.** Baseret på de første ugers brugeraktivitet skaber systemet en vurdering af de lokationer, som brugeren sandsynligvis vil logge ind fra. Hvis et login forekommer fra en lokation, der ikke er i nærheden af de normale lokationer, markeres brugeren som en potentiel risiko.
- **Mistænkelige IP-adresser.** Systemet overvåger tendenser på tværs af jeres IT-miljø i realtid. Hvis der forekommer flere loginforsøg fra forskellige brugere, men fra den samme IP-adresse, bliver adressen automatisk markeret som en potentiel hacker. Kendte IP-adresser filtreres fra, mens trusler overvåges.

2ndC Compliance Suite registrerer ændringer i sikkerhedstallene og lukker for sensitive roller i systemerne, hvis det er nødvendigt.