E-LOG

# Kdo vam krade kure?

**..S POMOČJO REŠITVE UČINKOVITEGA UPRAVLJANJA DNEVNIKOV E-LOG PODJETJA SIMT JE ZAGOTOVLJENA NE SAMO VARNOST PODATKOV, AMPAK TUDI SLEDLJIVOST POTENCIALNIH NEPRIDIPRAVOV..**

Po analizah največjih analitičnih hiš se 80 % varnostnih incidentov dogodi znotraj varnostnega okolja. Za izbris incidenta oziroma sledi incidenta je tako dovolj možnosti še v času, ko storilec deluje v okolju, še posebej, če ima napredno informacijsko znanje. Težava, ki jo zaznavamo, je, da sistemski skrbniki ne preverjajo dnevniških zapisov in takšnih dejavnosti ne morejo odkriti! To pa zato, ker so dnevniki navadno neurejeni, suhoparni ali celo nejasni.

V izogib tovrstnim tveganjem je podjetje SIMT po zgledu tujih varnostnih okolij ponudilo storitev E-log, ki omogoča velikim okoljem, da revizijske sledi v realnem času shranijo v zunanje specializirano in certificirano okolje. Dostop do njih pa brez možnosti sprememb omogoči samo pooblaščenim osebam naročnika.

Storitev je namenjena še posebej tistim, ki tako vrsto rešitev že uporabljajo interno, saj je mogoče vzporedno vzpostaviti še storitev, ki omogoča varnostnim delavcem izjemno hitro primerjavo notranjih in zunanjih revizijskih sledi ter posledično enostavno in učinkovito raziskovanje varnostnih incidentov.

## Upravljanje dnevniških zapisov

Upravljanje dnevniških zapisov (log manegment - LM) pomeni upravljanje oziroma obravnavanje velike količine računalniško ustvarjenih sporočil (log) in ga včasih poimenujemo tudi kot revizijska evidenca, revizijske sledi itd. LM zajema zbiranje, centralizirano shranjevanje, dolgoročno hrambo, analizo, kot tudi iskanje in poročanje.

LM v prvi vrsti uporabljamo zaradi varnosti sistema in omrežnih storitev pa tudi zaradi zagotavljanja skladnosti z veljavnimi predpisi.

Današnja varnostna in regulativna vprašanja se spotikajo ob dejstvo, da je Log Manegement za organizacije nuja. Pojavila se je namreč potreba po učinkovitem premagovanju znanih izzivov obvladovanja dnevniških zapisov in ostalih varnostnih zapisov, ki zagotavljajo varno zajete in shranjene informacije o dogodkih (SIEM), ne da bi zahtevali drago in zamudno implementacijo programske opreme.

V nedavnem poročilu, ki ga je objavil ameriški Nacionalni inštitut za standarde in tehnologijo, kot avtoritativno dokumentacijo za zahteve zvezne skladnosti s FISMA (Federal Information Security Management Act), so bili glavni izzivi obvladovanja upravljanja dnevniških zapisov:

- število virov, hitrost zapisovanja, starinski in neskladni formati dnevniških zapisov,
- zahteve po shranjevanju, varnost podatkov,
- zahteve po analizi in sposobnost povezovanja zapisov iz mnogih virov ter
- čas, ki ga porabi administrator, napor in stroški za vzdrževanje smiselnega upravljanja dnevnikov.

## Izboljšave z E-Log

Storitev E-Log daje prave odgovore na izzive obvladovanja dnevniških zapisov. Omogoča shranjevanje in raziskavo dejavnosti in dogodkov iz tisočih različnih virov dnevnikov celotnega okolja. Rešitev je v celoti skladna s standardi kot so SOX, PCI DSS, HIPAA in drugi z že vnaprej predpripravljenimi poročili v skladu z omenjenimi standardi.

E-Log omogoča spremljanje končnih uporabnikov, kot tudi administratorjev, z razlogom odkrivanja sumljivega obnašanja poskusov vdorov, vzpostavitve revizijske evidence, uveljavljanja odgovornosti nad administratorji, izvajanja boljših preiskav in forenzično analizo. Uporaba obvladovanja dnevniških zapisov kot storitve zmanjšuje čas, stroške in tveganja.

## Vodilne tehnologije

Tehnološka rešitev temelji na tehnologiji SenSage Event Data Warehouse, ki jo je mogoče zelo hitro implementirati, hkrati pa podpira več sto različnih konektorjev do različnih dnevniških virov. To tehnologijo uporablja prek 2000 ponudnikov storitev z veliko bazo zadovoljnih uporabnikov, kamor prištevamo tudi pomembne vladne subjekte. Zaradi široke baze strank je jasno, da so v SenSage na svoji dolgi karieri sodelovali s pomembnimi regulatornimi avtoritetami, kar uspešno prenašajo v produkte in na stranke.

## Na koga naj se obrnem glede upravljanja dnevniških zapisov?

Če ste tudi vi v skrbeh za svoje podatke in bi radi množico nepreglednih in suhoparnih dnevnikov uredili v pregledno entiteto, se nemudoma obrnite na podjetje SIMT, ki pri nas skrbi za zagotavljanje varno dislociranega shranjevanja dnevniških zapisov E–log. Zakaj SIMT? Ker je zaupanja vreden partner in ima za sabo že vrsto uspešnih projektov, o katerih smo v preteklih številkah že pisali in zagotovo še bomo tudi v prihodnje. (P.R.)

SIMT
UČINKOVITE SISTEMSKE REŠITVE

**SIMT, d. o. o.**
Industrijska cesta 9, 1290 Grosuplje
Tel.:+386 1 786 62 00
Faks: +386 1 786 42 02
E-pošta: info@simt.si
spletni naslov: www.simt.si