

Artikel Security professionals willen meer management rapportages

Door Redactie security.nl op donderdag 13 december 2007 16:06

Security professionals willen meer bezig zijn met het rapporteren aan het management, het opleiden van gebruikers en het uitvoeren van oorzaak-gevolg analyses. Zo'n zeven procent van de tijd zijn security professionals bezig met het opleiden van andere werknemers binnen de organisaties, en tien procent van de tijd gaat naar het opstellen van een incident response, het inlichten van het management en uitvoeren van oorzaak-gevolg analyses. Meer dan de helft van de tijd is men kwijt aan het dichten van beveiligingslekken en het oplossen van real-time incidenten.

85% van de security en privacy professionals had de afgelopen 12 maanden met een incident te maken, en bij 63% ging het om meerdere incidenten, tussen de 6 en 20 gevallen. Niet verwonderlijk, want meer dan de helft zegt dat trainingen aan het personeel slechts eenmalig gegeven worden of op een ad hoc basis plaatsvinden. Het volledige rapport van Deloitte & Touche en het Ponemon Institute is op [deze pagina](#) te vinden.

UBM Global: met CenterTools DriveLock Basic en DriveLock Security Reporting Center bieden veel managementrapportage en –informatie.

DriveLock Basic

DriveLock maakt het eenvoudig voor systeembeheerders en onderzoekers om gebruikersactiviteiten te traceren. Een exclusieve applicatielog en uitgebreide event messaging geven de mogelijkheid om de informatie te krijgen over wat er in het netwerk en op de computers met randapparaten is gebeurd.

Om een organisatie tegen haar onwetende medewerkers te beschermen biedt DriveLock een inhoudsfilter. Deze filtert / blokkeert ongeautoriseerde via randapparaten inkomende en uitgaande bestand extensies of file typen, of inhoud van de bestanden.

Om de organisatie tegen haar wetende medewerkers te beschermen heeft DriveLock audit- en schaduwmogelijkheden:

Auditing

- *Logt acties met randapparaten*
- *Logt dataoverdracht, lees en schrijfactiviteiten van en naar verwijderbare opslagmedia en randapparaten met een schijf*
- *Heeft geavanceerde log mogelijkheden voor*
 - » *Configuratieveranderingen (inclusief veranderingsdetails)*
 - » *Gebruik management console*
 - » *Tijdelijke deblokkering van een agent*
 - » *Gebruik van agent remote control*
 - » *Encryptie events*
 - » *Opstarten of blokkeren van een applicatie*
 - » *Netwerkconfiguratie veranderingen*

Schaduw

- *Een schaduwkopie kan worden gemaakt van alle bestanden van en naar verwijderbare opslagmedia en randapparaten met een schijf*
- *Limitering mogelijk tot de eerste paar regels van het bestand*

- *Uitsluiting mogelijk voor een lijst van file extensies*

Indien een DriveLock licentienemer besluit om de schaduwfunctionaliteit te gaan gebruiken is het advies om eerst de ondernemingsraad en de werknemers te informeren.

De hierboven beschreven basisfunctionaliteiten van DriveLock, samengevoegd met de DriveLock Security Reporting Center (add on), maken forensische analyse heel eenvoudig.

DriveLock SRC

Met DriveLock SRC is het nu mogelijk events te traceren tot aan de corresponderende white list entries (lijst met autorisatieregels).

Voor verdere onderzoek en analyse met DriveLock SRC kunnen DriveLock events worden bekeken door gebruikmaking van flexibele filters met zoek- en groeperingcriteria. Vervolgens is er de mogelijkheid de resultaten te exporteren en te printen voor verdere analyse, verwerking, rapportage of bewijsvoering. Hierbij heeft de organisatie keuze uit een persoonlijk rapport met alleen toegang voor de huidige gebruiker, of een opgeslagen rapport met toegang voor andere gebruikers gebaseerd op configuratie instellingen overeenkomstig het informatieveiligheidsbeleid van de organisatie.