

## **Persbericht: Met DriveLock is forensisch onderzoek kinderspel**

Datum: 17 juli 2007

Van: Louis Koppes

Ingeval van een vertrouwelijke informatielek via mobiele dragers moet forensisch onderzoek leiden tot informatie over wie er lekte, wanneer er is gelekt en welke vertrouwelijk informatie er is gelekt of zelfs is gestolen. De bewijslast ligt bij de organisatie.

De nieuwste versie 5.0 van DriveLock biedt nu deze gevraagde mogelijkheid. 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.

DriveLock 5.0 helpt daarmee ook in het bereiken van compliance met wet- en regelgeving, door auditmogelijkheden van alle administratieve acties zoals veranderingen aan white lists of aan toegangsrechten.

DriveLock is software voor het beveiligen van computerpoorten, voor het selectief autoriseren van randapparaten en van applicaties en voor het versleutelen van vertrouwelijke informatie op verwijderbare opslagmedia. De bekendste licentienemer in de Benelux is - na een Europese aanbesteding - het Nederlands Ministerie van Defensie.

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 deblokking 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.

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.

In alle gevallen kost het met DriveLock slechts enkele seconden om antwoorden te krijgen op forensisch vragen.

Het september (2006) nummer van LAN Magazine staat uitgebreid stil bij de werking van DriveLock versie 4.0

CenterTools Software GmbH uit Duitsland is de fabrikant van DriveLock en wordt in de Benelux markt exclusief vertegenwoordigd door UBM Global.

Meer informatie op [www.drivelock.nl](http://www.drivelock.nl) en [www.drivelock.be](http://www.drivelock.be)

Contactpersoon: Louis Koppes

Telefoonnummer mobiel:

+31 6 53 38 21 56

Telefoonnummer UBM Nederland:

0492 523 7780

E-mail:

netherlands@ubm-global.com

Telefoonnummer UBM België:

014/704537

E-mail:

belgium@ubm-global.com