

Bestuurders stelen 1,1 miljard aan bedrijfsgeheimen via USB-stick

Door Redactie security.nl op donderdag 15 november 2007 12:42

Twee Koreaanse topbestuurders van een elektriciteitsbedrijf hebben voor 1,1 miljard euro aan bedrijfsgeheimen meegenomen toen ze bij de concurrent gingen werken. De twee bestuurders van STX Heavy Industries werden vrijdag door politie aangehouden. Toen ze nog voor Doosan Heavy Industries & Construction werkten namen ze meer dan 900 documenten, waaronder blauwdrukken van zeer belangrijke technologieën, via USB-sticks mee naar huis.

Toen ze al voor STX werkten zouden ze voormalige collega's de opdracht hebben gegeven om als spion te fungeren. De waarde van de documenten wordt op 1,1 miljard euro geschat, maar volgens Doosan zou de werkelijke waarde veel hoger liggen, omdat het jaren in de ontwikkeling van de technologieën heeft gestoken. STX ontkent de wet te hebben overtreden, toch daalde de waarde van de aandelen afgelopen vrijdag.

UBM Global: 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.

DriveLock biedt 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.

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*

Schaduwen

- *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.