AD Risk Analysis

In unserer Tätigkeit als Quest Software Consultant (PSO) durften wir im 2009 eine Risikoanalyse über eine sehr grosse ActiveDirectory Infrastruktur durchführen.

Ausgangslage

Der Kunde, eine internationale Detailshandelskette, betreibt sechs ActiveDirectoy Domänen, welche zu einem Forest mit ca. 50 Domänen gehören.
Um die Risiken des Herzstück der IT besser zu kennen und entsprechende Massnahmen treffen zu können, wurde die Firma Quest Software beauftragt eine Risikonalyse durchzuführen.

Projektinhalt

Die Analyse wurde mit den Complianceprodukten Intrust, Reporter und Spotlight for AD durchgeführt. Um eine rasche zusätzliche Absicherung der AD Datenbank zu ermöglichen, wurde der RecoveryManager for AD implementiert.
Die Implementation der Produkte konnte ohne Betriebsunterbrüche in die produktive Umgebung durchgeführt werden. Innert wenigen Tagen sammelten sich mehrere GB an Daten, welche durch die vielen vordefinierten Reports schnell ausgewertet werden kann.
Konfigurationsänderungen an Server, Sicherheitsverletzungen oder Bedrohungen innerhalb des Netzwerkes können so schnell und einfach ausgewertet und eliminiert werden.

Resultate

Da sich ein Derivat des Conficker Virus eingeschlichen hatte, musste als erstes ein System implementiert werden, dass fehlhafte Logins innert Minuten melden konnte. Bei rund 600 Domänencontrollern ist das mit Microsoft Boardmitteln unmöglich.
Intrust sammelte über seine Agents sämtliche Logdaten der Domänencontroller. Zudem wurde ein Realtime Alerting eingerichtet, welches eine Aufhäufung von fehlerhaften Logins per Mail und Webportal meldete. So konnte innerhalb von wenigen Stunden die Quelle eruiert und vom Antiviren Hersteller ein Pattern erstellt werden.
In erster Linie wurde eine Risikoanalyse erwünscht. Mit der Compliancelösung von Quest, konnte zusätzlich der Mehrwert aufgezeigt werden, indem Intrust sämtliche Sicherheitsverletzungen einer Infrastruktur aufzeigen kann. Nicht nur auf Domänencontrollern, sondern alle Arten von Server, auch Linux, Unix uws.