



Patching

Microsoft brengt dinsdag een nieuwe patch uit die een twee weken geleden verspreide probleempatch (MS06-015) moet repareren. Een deel van de Windows-gebruikers heeft diverse problemen ondervonden na installatie van die patch.

Veel applicaties en omgevingen bestaan uit code, waarvan de kern soms jaren oud is. Telkens wordt hier weer wat bijgeschreven of gewijzigd, vaak onder tijdsdruk, vanwege de concurrentie. Hierdoor ontstaat vaak vanuit het gezichtspunt van security een "lappendeken". Telkens weer worden er nieuwe exploits geconstateerd. Het aantal uit te brengen patches door leveranciers neemt alleen maar toe.

Beheerders kunnen de grote toename van security patches nog nauwelijks bijbenen. Zo bracht Microsoft in 2005 in totaal 55 security patches uit, terwijl Oracle 81 security patches uitbracht. Gartner heeft becijferd dat de kosten voor het patchen zo'n 300 dollar per server per patch kost. Dit vanwege het enorme tijdrovende karakter van het testen van nieuw patches.

Veel organisaties lopen daarom achter met het installeren van nieuwe patches. Hackers weten dat, waardoor organisaties kwetsbaar zijn voor aanvallen.

Vaak wordt vertrouwd op de firewall met intrusion detection systemen. Verder heeft met een Demilitarized Zone en denkt men dat het interne data center met de kwetsbare systemen (relatief) veilig is voor aanvallen van buiten af.

In de praktijk valt dit vaak tegen. Organisaties zijn met hun bedrijfsgegevens en hun applicaties meer en meer gekoppeld aan elkaar. Bedrijfsinformatie moet overal beschikbaar zijn. Applicaties moeten met elkaar kunnen communiceren. Hierdoor is het aantal toegangspaden tot applicaties enorm toegenomen en ook complexer geworden.

Pach management blijft van cruciaal belang in het beveiligen van de kwetsbare systemen.

Een mogelijke oplossing is het aanbrengen van een zgn. "patch proxy". Dit houdt in dat er een patch wordt aangebracht, zonder een installatie op de applicatie server. Een patch proxy is een stuk software wat het verkeer tussen clients en server van de betreffende applicatie controleert. Er kan in de sessie worden gekeken (statefull inspection), waarbij de poging om een exploit te gebruiken wordt herkend.

Het grote voordeel van deze aanpak boven het installeren van nieuwe patches is de tijd die het kost om nieuwe patches, die op de applicatieserver worden aangebracht te testen in combinatie met alle andere applicaties.

De technologie van de "patch proxy" is nog erg nieuw. Verwacht wordt echter dat dit een grote vlucht zal nemen.

Bronnen: "Painless patching", Tim Greene; "Riders on the Storm", G.L. Ness.

Secure Connection brengt PDA2L-remarks uit.

Secure Connection heeft een nieuwe versie van "Process Dependency Analysis Tool" (PDA2L) uitgebracht.

In deze versie is het mogelijk om per vraag "evidence" toe te voegen. Op deze manier wordt het hele proces rond het uitvoeren van een analyse met PDA2L inzichtelijker voor de auditor.

Er kan in een organisatie bijvoorbeeld worden besloten om inschattingsvragen altijd te voorzien van een toelichting op de gemaakte keuze.

Er kan een uitdraai worden gemaakt van alle antwoorden, inclusief "evidence".

De nieuwe versie is vanaf heden leverbaar.

Met deze nieuwsbrief zal tevens een brochure van PDA2L-remarks worden toegestuurd.



Actueel

Oracle beperkt rechten databasebeheerder

Oracle is bezig met een nieuwe add-on die "Oracle Database Vault" heet. Hiermee is het mogelijk om de rechten van database administrators te beperken.

De database administrators kunnen dan nog steeds hun taken uitvoeren, maar hun rechten zijn meer gespecificeerd.

Oracle Database Vault biedt de mogelijkheid om precies aan te geven wie toegang heeft tot welke gegevens. Op deze manier wil Oracle een versie leveren, waarmee men compatible kan zijn met de Sarbanes Oxley wetgeving.

De beperking van de toegang van DBA'ers tot de data wordt met behulp van encryptie van de data verkregen.

Oracle komt tevens met secure backup, waarbij de data op backuptapes tevens wordt encrypt.

Tenslotte bevat de Database Vault ook mogelijkheden voor auditors om rapportages uit te draaien.

Bron: www.eweek.com