Hackers worden steeds crimineler

Interview met Mary Ann Davidson

Mary Ann Davidson is chief security officer voor Oracle Corporation. Zij bezocht dit voorjaar de conferentie van de Oracle Gebruikersclub Holland. Voor Optimize en Gerard Uiterwaal van Motiv een uitgelezen kans om met haar gedachten te wisselen over de achtergronden van het security-beleid van Oracle.

Wordt er in de VS anders tegen informatiebeveiliging aangekeken dan in Europa?

Davidson: 'Er wordt in de Verenigde Staten en Europa op twee totaal verschillende manieren naar security gekeken. In de Verenigde Staten wordt er voornamelijk naar security gekeken vanwege de regelgeving. De laatste jaren zijn er een groot aantal wetten aangenomen op het gebied van informatiebeveiliging. De bekendste daarvan is ongetwijfeld Sarbanes-Oxley, een wet die aan de ene kant CEO's persoonlijk aansprakelijk stelt voor gebreken op het gebied van security en aan de andere kant harde eisen stelt aan het vastleggen wie, wat, wanneer heeft gedaan. Deze wet is grotendeels te vertalen in specificaties op het gebied van security van bedrijfsinformatiesystemen. Volgens een recent onderzoek noemen 21 procent van de bedrijven in de VS regelgeving als de belangrijkste reden voor security maatregelen. Daarbij moet eigenlijk nog worden opgeteld het aantal bedrijven dat Sabanes-Oxley specifiek noemt (15 procent).

In Europa leeft het begrip privacy van oudsher meer dan in de Verenigde Staten. Hier worden zelfs de begrippen privacy en security nog wel eens verward. Terwijl privacy slechts één van de aspecten van security is. Overigens groeien de beide werelden wel naar elkaar toe. Het nut van de uitgebreidere vorm

Adv Array Informatieanalyse

wordt echter ook in Europa steeds duidelijker, al is het alleen al door internationals met vestigingen in de VS. Anderzijds wordt privacy ook steeds meer een issue in de VS. Een voorbeeld hiervan is de Californische wet SB 13/86. Hierin worden bedrijven verplicht, je op de hoogte stellen indien aan jouw gerelateerde persoonlijke informatie openbaar gemaakt wordt.'

Vertrouwenspositie

In de Nederlandse security-praktijk wordt er veelal naar geïnformeerd of het mogelijk is om dba-werk te doen zonder toegang te hebben tot de business-data. De achtergrond van deze vraag is dat allerlei standaarden terecht geëist wordt dat een gebruiker alleen toegang mag hebben tot die data die noodzakelijk is voor zijn functioneren. Toegang tot business-data is voor dba-werk niet noodzakelijk.

> ***'In Europa leeft het begrip privacy van oudsher meer dan in de Verenigde Staten'***

Davidson: 'Een dba bekleedt een vertrouwenspositie en mag best gescreend worden. Allerlei eisen die puur uit de theorie komen, mogen best wel aan de praktijk getoetst mogen worden. Je moet echter niet alleen naar de theorie kijken, maar vooral naar waar je je tegen beschermen wilt. Baseer hierop je maatregelen. Eén van deze maatregelen kan zijn encryptie van data in de database. Als dit gebruikt wordt om je te beschermen tegen kwaadwillige dba's moet je er wel voor zorgen om de sleutels buiten de database te bewaren en te managen. Een andere, meer gebruikelijke manier om dezelfde bescherming voor elkaar te krijgen is de 'two person rule': zorg ervoor dat alle dingen die kwaad kunnen niet door een persoon alleen kunnen worden uitgevoerd. Een derde manier is 'trust but verify': leg met uitgebreide auditing alle belangrijke handelingen van een dba vast.'

In het verlengde daarvan ligt ook een consultancy-dienst die Oracle vooralsnog alleen in de VS aanbiedt: selective auditing.
Davidson: 'Deze dienst bestaat uit een fraaie GUI met daarin ondergebracht een op de lokale applicatie toegespitste oplossing met generic audit, fine grain audit en flash back query als gebruikte technieken. In de GUI is het bijvoorbeeld mogelijk om naar gebruikers te kijken en hierop in te zoomen. Met behulp van de flashback query is het mogelijk om te achterhalen wat de gebruikers bekeken hebben.'

Op het OGH-seminar is de uitspraak gedaan dat Oracle de 'leading company' wil zijn op het gebied van security.
Davidson: 'Dat is op twee manieren te interpreteren: enerzijds wil Oracle een leider zijn in het bouwen van producten met een goede ingebouwde security. Oracle heeft de afgelopen jaren veel geïnvesteerd om security in te bouwen in het ontwikkelingsproces. We maken daarbij gebruik van specifiek op security toegesneden programmeerstandaarden specifiek voor security. We laten de software evalueren door interne en externe instanties. We hanteren criteria op het gebied van security waaraan releases moeten voldoen, voordat ze uitgebracht mogen worden.'

Identity Management

Als gevolg van deze inspanningen heeft Oracle op dit moment dan ook negentien certificaten op het gebied van security. Mary Ann is er zo van overtuigd dat ze er zeker van is dat ze geen business verliezen op security issues: 'Als security belangrijk is voor je, koop je Oracle.' Anderzijds is Oracle nu ook begonnen met een specifiek security-product: Identiteit management.
Davidson: 'Dat is het enige security-product dat gevormd wordt door business-software. Met het inzetten van identiteitsmanagement kun je de business verbeteren. Terwijl producten als firewalls en anti-virus software alleen maar ervoor zorgen dat je geen of minder last hebt van problemen van buitenaf. Veel andere security-producten, zoals firewalls en anti-virus software zijn preventie- of band-aid producten. Ze zijn noodzakelijk omdat je in een onveilige wereld leeft, maar identity management is daarmee niet minder noodzakelijk. Identity management is business-software omdat het een waardevol onderdeel is van je infrastructuur, zelfs zonder dreigingen. Dingen als single sign-on leveren kostenbesparingen op bij je helpdesk, minder telefoontjes. Het zorgt ervoor dat je applicaties sneller kunt opleveren. Het helpt bij het voldoen aan regelgeving zoals Sarbanes-Oxley. Als je moet aangeven hoe je beveiliging in elkaar zit en wie toegang heeft tot wat, is het veel gemakkelijker dat dit op één plaats zit in plaats van in achtendertig applicaties en dan nog steeds op een andere manier. Het levert ook betere security op doordat je beter in staat bent om iemand in één keer alle benodigde rechten te geven en, misschien nog belangrijker, weer af te kunnen nemen, zonder dat er ergens iets blijft hangen. Zonder dat ik nu een premature productaankondiging zou willen doen, is een logische aanvulling op dit product een meer omvattende vorm van auditing. Denk dan aan het sturen van de auditing door business-criteria in plaats van technische criteria.'

Hashes

Over het algemeen wordt het als een zwakte van de Oracle-authenticatiemethode beschouwd, dat eenzelfde user/wachtwoord-combinatie in alle verschillende databases dezelfde pass-

word-hash oplevert. Dit geeft een hacker die password-hashes heeft gevonden namelijk de mogelijkheid om offline met behulp van een password-cracker te proberen de hash te kraken. Omdat dit offline gebeurt, is het niet te traceren.
Davidson: 'Password-hashes zijn niet zomaar te vinden en er moet zorgvuldig mee omgegaan worden. Anderzijds is het erg moeilijk om bestaande functionaliteit te wijzigen, ook al gaat

'Alleen al economisch gezien is het zinvol om meer aandacht aan security te besteden'

het om zoiets technisch als password-hashes. Het klopt inderdaad dat de voorgestelde oplossingen, zoals het afhankelijk laten zijn van een machine-id dan wel de database-id gevolgen zouden hebben voor een product zoals de stand-by database en zelfs ook voor zoiets als het terugzetten van een back-up na een calamiteit op een andere machine.'
Het korte antwoord, dat ze overigens niet expliciet geuit heeft, luidt dan ongetwijfeld ook dat dit op korte termijn niet veranderd zal worden.

Security holes

Davidson ziet security in het verlengde van betrouwbaarheid:
'Oracle-databases moeten beschouwd worden als een deel van de infrastructuur, en als zodanig bovenal betrouwbaar. Als je een gebouw inloopt denk je ook nooit:
Will I get the blue building of death this morning, is the door going to be frozen and will it have to be rebooted?'

De business case voor het investeren van geld in security vereist enige toelichting:
Davidson: 'Je hoort vaak dat klanten niet bereid zijn om te betalen voor goede security. Klanten betalen nu in feite ook, maar dan voor slechte security, al is dat dan niet in de vorm van licentiekosten. Als we nu een tool aanschaffen die security-holes voor ons vindt, gaat dit ons nu geen besparing opleveren. Alle holes die we vinden moeten opgelost worden en dat kost alleen maar geld. Een ander plaatje krijg je als je kijkt vanuit het perspectief van over twee jaar. Dan is het om twee redenen goedkoper om de problemen nu op te lossen in plaats van later. Geld wordt steeds duurder, waardoor een investering nu goedkoper is dan een investering later. De effecten hiervan zijn door te rekenen met wat in de economie heet *discounted cash flow analysis*. Een tweede effect is dat een gemiddeld stuk software op steeds meer plekken gebruikt wordt, waardoor het veranderen hiervan ook steeds duurder wordt. Als je het allemaal doorrekent, is het alleen al economisch gezien zinvol om meer aandacht aan security te besteden, ook al lijkt het in eerste instantie alleen maar geld te kosten.'

Trends

Tenslotte, wat zijn de trends op het gebied van security?
Davidson: 'Eerst de positieve wijzigingen. Deze hebben vooral betrekking op de aandacht die het gebied security op dit moment (vooral in de Verenigde Staten) krijgt. Dit is bijvoorbeeld af te lezen aan het aantal boeken over een onderwerp als 'security coding practices' verschenen is. Vier jaar geleden was hier nog geen boek over te krijgen. Ook waren er geen seminars op dit gebied, terwijl ik er alleen al dit jaar drie of vier heb bijgewoond. Ook tools op het gebied van security-scanning zijn een relatief nieuw fenomeen. In zijn algemeenheid wordt er ook meer gekeken naar de echte onderliggende problemen. Maak producten zoals Oracle beter, het is tenslotte infrastructuur.
Een negatieve wijziging met op de lange duur een grote impact is echter dat de aard van de hackers aan het veranderen is. Vroeger was het een meestal een beetje nerd-achtig persoon, die het er alleen maar ging te bewijzen dat zijn virus virieler was dan dat van de anderen. Volgens een recent onderzoek is tachtig procent van de 'malware' tegenwoordig geschreven met een crimineel oogmerk. Uit hoofde van mijn functie krijg ik nog wel eens inlichtingen die niet voor de openbaarheid bedoeld zijn. Daaruit blijkt dat het steeds vaker voorkomt dat software als 'trojan horses' specifiek voor een doelwit geschreven worden. Het oogmerk is dan om gegevens van concurrenten te verkrijgen. Deze software is moeilijk door generieke scanners te ontdekken.'

Gerard Uiterwaal is Oracle- en security expert en werkzaam bij Motiv.
Fotografie: Dré de Man