Unbreakable

Hackers nemen Ellison's handschoen op

Je hebt leugens, verdomde leugens en statistieken. En dan is er ook nog marketing. Zo werd de Titanic ooit als unsinkable aangeprezen. 'Unbreakable' noemde Oracle-chef Larry Ellison de 9i applicatieserver op de Comdex-conferentie in Las Vegas, medio november. Een boude uitspraak. Nog diezelfde dag slaagde David Litchfield van het Engelse beveiligingsbedrijf Next Generation Security Software erin Ellison's uitspraak te logenstraffen.

Met zijn presentatie in Las Vegas wilde Ellison vooral de clusterconfiguraties van 9i laten zien. Hoewel die demonstratie voor een breed publiek bestemd was en daarom inhoudelijk wat oppervlakkig, bevatte hij wel een goede uiteenzetting van de sterke punten van het nieuwe product, zoals het hanteren van failover en database redundantie. De toegang tot applicaties blijft zelfs ongehinderd bij uitval van meerdere servers. Ellison vertelde ook wat hij verder nog onder 'unbreakable' verstaat: "Het betekent dat je (9i AS- red.) niet kunt kraken, en dat je er niet kunt inbreken". IT'ers overal ter wereld gaven gehoor aan de uitnodiging van Ellison om Oracle's website te testen op onkraakbaarheid: het aantal aanvallen op de site vertienvoudigde binnen korte tijd van drieduizend naar dertigduizend per week. Voor het gros van de aanvallen werden tactieken aangewend die alleen tegen Windows NT gebruikt kunnen worden. Op de site van Oracle draait Oracle 9i echter onder Unix. Opvallend is dat Oracle-topman Jarvis beweert dat zelfs Microsoft voor de eigen site gebruik zou maken van Unix, omdat NT niet veilig genoeg zou zijn. Voormalig kraker Marc Maiffret, tegenwoordig chief hacking officer van beveiligingsbedrijf e-Eye, zegt dat zijn programmeurs maar vier uur nodig hadden om enkele zwakke punten in 9i te ontdekken. Deze stellen hackers in staat een denial of service-aanval uit te voeren. e-Eye heeft het recente, grote gat in Windows XP ontdekt.

> ***'Exchange server is just a bag full of viruses with a few notes in it.'***

De meest vergaande inbraak op 9i AS werd gepleegd op een Blackhat Security Briefing in Amsterdam. Volgens een bericht in Computable liet David Litchfield (zie het interview met hem verderop in dit artikel) zien hoe een niet goed ingestelde buffer door een kwaadwillende gebombardeerd kan worden totdat deze overloopt. Na deze buffer overflow kan men vervolgens van buitenaf code loslaten op de server. De buffer overflow trad op zonder enige vorm van authenticatie. Het systeem is dus kwetsbaar ongeacht password-bescherming. Op deze wijze kon Litchfield zich onbeperkte toegang tot de AS kon verwerven, en kreeg zelfs toegang tot de 9i database waarmee 9iAS verbonden was. De precieze techniek achter de inbraak kan en mag hier niet uit de doeken gedaan worden, omdat de meeste patches voor diverse veiligheidslekken van 9iAS (zie kader) nog niet beschikbaar zijn.
Beveiligingsresearchinstituten zoals Covert Labs van Network Associates, kwalificeren de lekken overigens op een high and medium risk level.
De "unbreakable"-premisse is geen op zichzelf staande boude uitspraak, zoals we die van Ellison met enige regelmaat gewend zijn. Oracle heeft een complete marketing-campagne op de vermeende onkraakbaarheid gestoeld – je zou bijna gaan denken dat Oracle het woord unbreakable als gedeponeerd handelsmerk wil gaan gebruiken. Hoe dan ook, met de "Unbreakable"-campagne wil Oracle significante veroveringen doen op de appserver-markt. Het heeft thans een magere acht procent van die markt in handen, even groot als het aandeel van Sun, maar ver achter IBM (15%) en BEA (18%). De appservermarkt is essentieel voor Oracle. Applicatieservers worden hoe langer hoe meer de achilleshiel voor het bouwen, deployen en integreren van webgebaseerde applicaties. Oracle beschouwt de applicatieserver als zijn derde 'core' product, na het databasevlaggenschip en de e-business suite met erp- en crm-tools.

Ondanks alles heeft Ellison gelijk, wanneer hij zegt dat Oracle qua veiligheid er beter voorstaat dan IBM en Microsoft. Maar 'unbreakable' is natuurlijk onzin, of beter gezegd: het is net zolang waar totdat iemand het tegendeel bewezen heeft – in dit geval dus maar een paar uur. Beveiliging is een voortdurend gevecht tussen jagers en gejaagden, met een open einde. Absolute veiligheid bestaat niet, en dat weet Ellison beter dan geen ander. De 'unbreakable'campagne is daarom een vrij dubieuze zaak, waarvan het de vraag is of die zich niet tegen Oracle zal keren. Erger is misschien, dat een aantal Oracle klanten zo'n uitspraak letterlijk zullen nemen. Wie volkomen vertrouwt op de veiligheid van een server, zal verzuimen maatregelen te nemen en maakt zich daarmee juist kwetsbaar. Ook in dat opzicht zou de campagne wel eens een averechts effect kunnen sorteren.

Tijdens Oracle Apps World op 17 januari in Amsterdam, bleek dat Ellison in de recente gebeurtenissen geen aanleiding zag van koers te veranderen. Op een vraag over het memo van Bill Gates over veiligheid, volgde een amusante aanval op Microsoft ('Exchange server is just a bag full of viruses with a few notes in it.') en een exposé over de veiligheid van Oracle. Over de manier waarop hackers en beveiligingsexperts op 'Unbreakable' hadden gereageerd, zweeg Ellison echter in alle talen.

'Uitspraak van Ellison is gevaarlijk'

Oracle neemt veiligheid wel serieus

David Litchfield is beveiligingsexpert en degene die Ellison's uitdaging op de meests spectaculaire manier beantwoord heeft. Was de 'Unbreakable'-uitspraak de directe aanleiding?
Litchfield: 'In feite wel. Toen ik dat hoorde, dacht ik, dat is nogal een uitspraak, unbreakable, dat kan niet kloppen. Ik heb een exemplaar van Oracle Application Server en van de database van hun site gedownload en nog diezelfde dag vond ik de meeste van de problemen die nu erop wachten om gerepareerd te worden.'

Vindt hij zo'n uitspraak van Ellison nu verstandig?
Litchfield: 'Het is erg gevaarlijk om dat te zeggen, en het had waarschijnlijk niet gezegd mogen worden. Oracle probeert met die marketingcampagne waarschijnlijk te zeggen: Oracle is veiliger dan al zijn concurrenten op het gebied van databaseservers. Oracle heeft veertien onafhankelijke veiligheidsevaluaties laten doen en heeft ze gehaald, geen van Oracle's concurrenten kan op iets dergelijks wijzen, ik denk dat Microsoft SQL Server er één heeft en DB2 geen enkele. Die campagne is er meer om hun toewijding aan veiligheid te laten zien dan om te beweren dat Oracle 9i echt 'unbreakable' is. Hoewel Larry Ellison ongelukkigerwijze juist precies dat gezegd heeft: "You cannot break in." Maar ik denk dat het idee achter de campagne eigenlijk meer is te zeggen, dat ze ergens aan gecommitteerd zijn.'

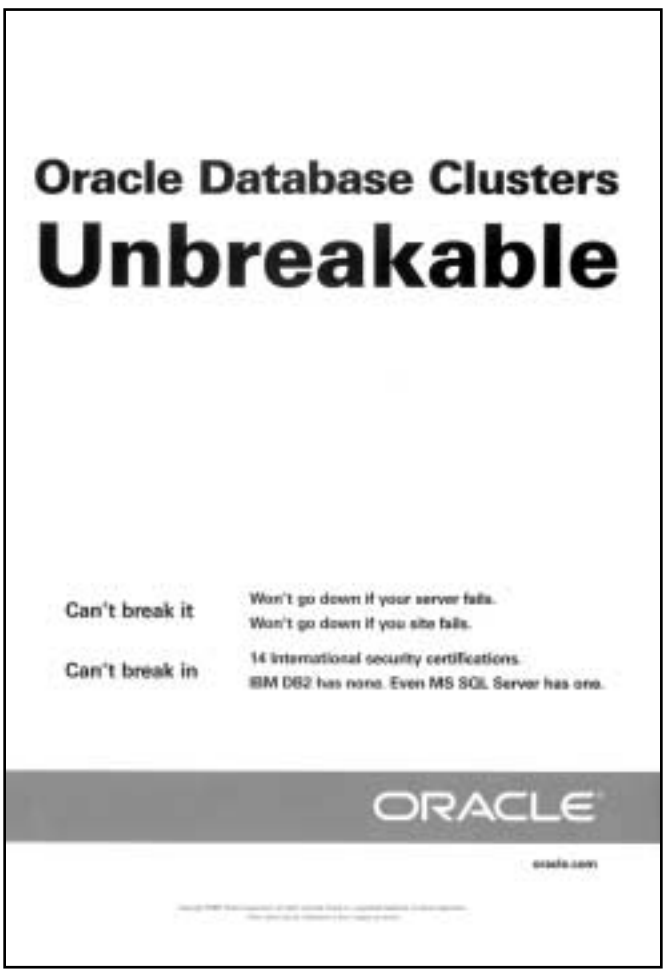
Ergens aan gecommitteerd zijn, en ergens ook daadwerkelijk goed in zijn, is natuurlijk iets heel anders. Denkt u dat Oracle werkelijk zoveel veiliger, of zoveel minder onveilig is dan de anderen?
Litchfield: 'Ik zou niet willen zeggen, dat het veiliger is dan de anderen. Wat ik wel zou willen zeggen, is dat Oracle fijngevoeliger controle toelaat op het gebied van security dan veel van de database concurrenten. Maar in staat zijn security te controleren is niet hetzelfde als kwetsbaarheid op het gebied van veiligheid. Kwetsbaarheid en veiligheidsmanagement zijn twee geheel verschillende zaken en alle databases hebben in de kern van de zaak hun eigen unieke problemen. MS SQLServer heeft buffer overruns, Oracle heeft soortgelijke problemen. Zij zijn allemaal kwetsbaar voor hetzelfde type aanvallen en problemen. Maar zoals ik al zei, Oracle laat zeer zeker fijngevoeliger controle over security toe, met name van zijn logins.'

Oracle heeft zeker een grote klus voor de boeg, wanneer iemand een groot beveiligingslek vindt

De artikelen die ik gelezen had, waren een beetje onduidelijk over wat u precies gedaan heeft. Ik begrijp dat u dat ook niet precies kunt vertellen voordat de patches uit zijn. U heeft de buffer overflow gebruikt om op een gegeven moment commando's door te geven, maar bent u zover gekomen dat u complete controle over de database had?
Litchfield: Ja. Ik zal proberen het problemen te beschrijven zonder te veel details prijs te geven. Door gebruik te maken van de bugger overrun (of één van de buffer overflows waarover ik kan spreken, want deze is gepubliceerd en de patch is verkrijgbaar) aan het Oracle web front-end, ben je in feite door elke firewall heen. Je zit nu als het ware op de webserver, vandaar kun je een aanval op de Oracle database beginnen. Ik kan nu niet ingaan op de details daarvan, maar in feite kan ik dan zonder identificatie met de database server machine connecten en remote control over die server krijgen. Als je doel de Oracle database back-end server is, is het duidelijk dat je vanuit Internet de webserver in de tang moet nemen. We kunnen de webserver bewijsbaar kraken. Het wachten is nu op de patch voor de volgende aanval, zodat ik daar meer over kan vertel-

len. In ieder geval stelt die me in staat controle te krijgen over de database backend server. Dat is bewijsbaar. Het spijt me dat ik het niet duidelijker kan zeggen, maar ik kan nu eenmaal niet de volledige details prijsgeven.'

Steeds meer bedrijven zijn aanwezig op Internet, dat betekent ook dat steeds meer bedrijven een potentiële kwetsbaarheid hebben opgebouwd. Wordt er wel genoeg aandacht aan security besteed in het licht van die toename?
Litchfield: 'Mijn ervaring is dat er de laatste jaren zeer zeker een grote toename is geweest in mensen die bezorgd zijn over security. Deze proberen ook stappen te nemen om hun veiligheid te vergroten. Het zou vanzelfsprekend beter kunnen zijn, meer mensen zouden zich er mee bezig kunnen houden, maar



aan de andere kant zijn mensen nu met de economische slechtere tijden aan het bezuinigen op veiligheidsbudgetten. Dat is erg stom, nee niet stom, dwaas, want het is bewezen dat het uitgeven van geld voor security de cost of ownership van een bepaald project omlaag kan brengen. Een voorbeeld: wanneer je een beveiligde webserver met een niet-beveiligde webserver vergelijkt, zal de eerste alle niet noodzakelijke services disabled hebben, terwijl ze op de andere server gewoon doorlopen. De beveiligde server heeft meer CPU power en meer geheugen beschikbaar en kan meer web-requests afhandelen, terwijl de andere kostbare CPU-cycli verspilt met niet noodzakelijke services. Veiligheid wordt niet serieus genoeg genomen, dat ben ik met u eens, maar de situatie is zeker veel beter dan een paar jaar geleden..'

Wat kun je doen wanneer iemand eenmaal de database binnen is?
Litchfield: 'Ten eerste: onkwetsbaarheid kun je alleen bereiken op een bepaald moment in de tijd, je kunt alle kwetsbaarheden van een systeem verwijderen en dan is op dat moment die machine veilig. Maar zo gauw iemand een nieuwe bug vindt die consequenties heeft voor de veiligheid, wordt die machine onveilig. Je kunt dicht bij de absolute veiligheid komen, wanneer je het relateert aan het kennisniveau van dat moment. Zo gauw er echter een nieuwe kwetsbare plek gevonden wordt, kan die machine weer volkomen veilig zijn. Die ene bug kan complete controle over die computer mogelijk maken. Je kunt dus honderd procent veiligheid bereiken, maar alleen voor een heel kort moment.'

Het is een voortdurend spel van jagers en slachtoffers?
Litchfield: 'Precies.

Zijn er dingen die je kunt doet, ervan uitgaande dat iemand op een bepaald moment zal inbreken?
Litchfield: 'Er zijn 1001 manieren om in te breken en 1001 dingen die je kunt doen, het is moeilijk om dit in het kort te bespreken. Dat is onder meer afhankelijk van het soort bedrijf in kwestie. Ook wanneer je weet dat er ingebroken is, kun je allerlei dingen doen. Je kunt die inbraak aan de politie doorgeven, ik noem maar wat. Maar er zijn duizenden andere dingen die je zou moeten doen. Bijvoorbeeld: kun je de data nog vertrouwen? Dat kost natuurlijk vrij veel geld. In plaats van zoiets te laten gebeuren, zou je nu de noodzakelijke stappen moeten zetten om te voorkomen dat zoiets gebeurt.'

Waarom duurt het zo lang voordat de patches klaar zijn?
Oracle draait op zestig verschillende besturingssystemen, dus ze moeten ieder van die systemen checken om te zien of het probleem daar optreedt. Dan moet men weer terug naar oudere versies die nog steeds ondersteund worden. Dan moeten de patches nog geschreven worden en gestest, om te controleren of ze geen neveneffecten hebben. Oracle heeft zeker een grote klus voor de boeg, wanneer iemand een groot beveiligingslek vindt. Een leverancier als Microsoft, die alleen patches schrijft voor een paar besturingssystemen, zou in staat moeten zijn veel sneller een patch uit te brengen. Maar ze zijn ongeveer even snel.'

Redactie Optimize