LinkedIn: Linke soep

wolfman, 2013-14-03

Wat als een wildvreemde al uw vrienden en zakelijke relaties eens ging mailen. Uit naam van u. Zelfs een mail met onschuldige inhoud zou leiden tot een hoop verwarring en tijdsverlies. Gelukkig gebeurt dat niet zomaar. Toch bestaat het gevaar wel degelijk. Enige tijd geleden lagen inloggegevens van LinkedIn op straat, en miljoenen gebruikers werden opgeroepen hun wachtwoord te veranderen. Hoe kan zoiets gebeuren, en hoe voorkomen we het?

Hashed wachtwoorden

Wat is er precies gebeurd? Het is gebruikelijk om wachtwoorden op te slaan in een database. Dit zijn dan veelal hashed wachtwoorden. Definitie van een hash is een onomkeerbare, wiskundige omrekening. De gebruiker geeft een wachtwoord op, de applicatie-database hashes dit wachtwoord en de database zoekt naar overeenkomstige hashes.

Het wordt veel gebruikt voor de opslag van wachtwoorden, in certificaten en om de oorspronkelijkheid van documenten te borgen. En hoewel er zwakke plekken zijn, blijft het terugrekenen lastig. Laat ik voorop stellen dat het al een veel betere manier is dan wachtwoorden in gewone tekst opslaan. Dat is eigenlijk de deur openzetten en vragen wie er een kijkje wil komen nemen.

In geval van inbraak zoals bij LinkedIn is niet exact duidelijk hoe het is gebeurd, maar hackers hebben de hashes kunnen bemachtigen, niet de eigenlijke wachtwoorden. De vraag is kunnen ze er wat mee, en hoe kun je het voorkomen?

Zout in de wonden - Salted hashes

Kan men iets beginnen met gestolen hashes? Jazeker! Er circuleren zogeheten RAINBOW crack tabellen op internet die een zeer grote hoeveelheid vooraf berekende hashes bevatten. Grote kans dat de juiste ertussen zit.

De oplossing ligt volgens LinkedIn in ‘Salted’ hashes. Dit is een wachtwoord-hash gekoppeld aan een willekeurige sleutel per gebruiker. Zo zijn vooraf berekende hashes niet zomaar te gebruiken.

Het stopt niet bij LinkedIn

Nu hebben hackers dus een wachtwoord en waarschijnlijk een login-naam, wat bij LinkedIn een e-mailadres is. Hoeveel mensen gebruiken voor LinkedIn een op zichzelf staand adres? En hoeveel mensen gebruiken het wachtwoord nergens anders? Een beetje hacker haalt alle informatie via Google bij elkaar.

Stop hackers vóór de database

Wanneer hackers de database hebben bereikt, hoe deze ook is opgebouwd is er al veel te veel fout gegaan vooraf. De echte oplossing ligt in het blokkeren van dergelijk verkeer middels een gelaagde beveiliging van firewalls en IPS. Deze oplossingen hebben echter geen idee welke kwetsbaarheden op applicatieniveau aanwezig zijn. Een perfect geconfigureerde firewall en IPS met alle recente patches aan boord zijn niet in staat om aanvallen op applicatieniveau te stoppen. De reden hiervoor is dat traditionele firewalls en IPS-en dergelijk verkeer als legitiem beschouwen. Dan kun je er natuurlijk voor kiezen om SSL te gebruiken voor een veilige verbinding tussen gebruiker en webserver. Het probleem hier is dat een firewall het SSL-verkeer alleen maar kan doorlaten omdat hij niet in versleutelde pakketten kan kijken. Een IPS zou dit wel moeten kunnen, maar dient dan wel te beschikken over de private keys.

Beveiliging niet ten koste van performance

Inspectie van SSL-verkeer door IPS gaat meestal ten koste van de performance, met als gevolg dat veel organisaties ervoor kiezen om SSL-verkeer ongemoeid door te laten naar de webserver. Ook SSL-verkeer kan worden misbruikt waardoor het bypassen van de beveiliging weer makkelijker wordt. Om webapplicaties en gerelateerde databases echt te beschermen dient een application aware oplossing te worden geïntroduceerd, een zogenaamde webapplicatie firewall. Een dergelijke oplossing is in staat om SSL-verkeer te offloaden, ook bij grotere volumes, zonder dat dit ten koste gaat van de performance. Daarnaast beschermt hij tegen gevaren die gericht zijn tegen de applicatie zoals SQL injection, cross site ccripting en cross site forgety. De meest voorkomende bedreigingen voor webapplicaties staan gepubliceerd als OWASP top 10 (www.owasp.org). Een goede webapplicatie firewall maakt gebruikt van een combinatie van het positief en negatief security model. Bovendien is hij in staat om ook SOA-omgevingen te beschermen en levert protectie tegen het lekken van data.

Gehashte wachtwoorden of klantgegevens hoeven dus helemaal niet op straat te komen liggen, met alle kosten en reputatieschade tot gevolg. Een goede webapplicatie firewall is in staat om applicaties en databases te beschermen, hoge beschikbaarheid te leveren en in staat een goede gebruikerservaring te leveren. Waarom zou beveiliging van uw applicatie ten koste moeten gaan van de performance!?

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com