

Gevolgen internetinbraak Diginotar

07/09/11 - Nadat bekend werd dat ingebroken was op de systemen van certificatenleverancier Diginotar, heeft Binnenlandse Zaken het vertrouwen opgezegd en het bewind over het bedrijf overgenomen.

Na onderzoek is gebleken dat een groot aantal valse certificaten is uitgegeven. Certificaten zijn nodig om te kunnen waarborgen dat het internetverkeer veilig verloopt. Zij dienen ter identificatie van websites (het zogenaamde slotje) en beveiliging van verkeer tussen computers onderling. Omdat niet duidelijk is welke certificaten van Diginotar nog te vertrouwen zijn en welke niet, is het vertrouwen in álle Diginotar certificaten verloren gegaan. Alle Diginotar certificaten moeten daarom worden vervangen. Deze oproep is afgelopen weekend al breed gecommuniceerd, onder meer via de website van VNO-NCW en MKB-Nederland (www.vno-ncw.nl; www.mkb.nl).

Microsoft update

Vandaag komt Microsoft met een update van de software. Deze update kan mogelijk gevolgen hebben voor het serververkeer in onze sector. Dit speelt in ieder geval in de overheidssector - die veelvuldig gebruik maakte van dit certificaat -, maar mogelijk ook bij sommige sectoren uit het bedrijfsleven. Op verzoek van de Nederlandse overheid wordt deze update daarom in Nederland niet automatisch doorgevoerd. Bedrijven krijgen de keuze deze update direct in te voeren of nog uit te stellen totdat zij hun DigiNotar certificaat hebben vervangen.

Aanbevelingen voor ondernemers

1. Bedrijven die gebruik maken van DigiNotar certificaten dienen deze zo snel mogelijk te vervangen.

Certificatiedienstverleners waar u op kunt overstappen zijn (zonder voorkeur):

- KPN/Getronics: tel. 0320-217300, email pki@getronics.com
- ESG: tel. 0495 566355, email info@csp4.eu
- Quo Vadis: tel. 030-2324320, email info.nl@quovadisglobal.com

Bedrijven die gebruik maken van DigiNotarcertificaten en daarover vragen hebben, kunnen terecht bij hun softwareleveranciers. Met vragen over de vervanging van certificaten kunt u ook terecht bij Logius (www.logius.nl)

2. Per bedrijf dient een keuze te worden gemaakt of de Microsoft update nu of op een later moment moet worden geïnstalleerd. Bij deze keuze moeten bedrijven niet alleen bekijken of zij zelf DigiNotarcertificaten hebben, maar ook bezien of bedrijven in de keten deze certificaten gebruiken. Wij adviseren u hierbij te letten op de communicatie van Microsoft (www.microsoft.nl) en de rijksoverheid (www.rijksoverheid.nl)

Elektronische aangifte ondernemers:

Met de Belastingdienst, het ministerie van Financiën, ICT~Office, diverse softwareleveranciers en belastingconsulenten, is intensief overleg gevoerd over de elektronische belastingaangifte van ondernemers. In verband met de het belang van dit proces, is onderzocht of dit proces in stand te houden is. Tijdens het overleg is vastgesteld dat de systemen waarmee ondernemers direct of via hun intermediair aangifte doen ook in deze situatie op dit moment kunnen blijven functioneren. Het systeem kent voldoende

aanvullende waarborgen voor een veilige aangifte. Alle betrokken partijen zijn overeengekomen dat de situatie de komende tijd nauwgezet wordt gemonitord. Ook wordt met de betrokken partijen afgesproken dat wanneer aangiftes door certificaatfouten te laat of niet aankomen, de Belastingdienst hier coulant mee om zal gaan.

Vervolg

Over de gevolgen voor andere sectoren vindt op dit moment intensieve analyse plaats door overheid en betrokken bedrijfsleven. Zodra deze resultaten bekend zijn worden deze per sector gepubliceerd. Ten behoeve van dit onderzoek verzoeken wij u om de problemen waar u in de praktijk tegen aanloopt inzake deze valse certificaten, [hier](#) te melden. VNO-NCW en MKB Nederland houden voortdurend de vinger aan de pols en zullen u via de websites van VNO-NCW en MKB Nederland op de hoogte houden van nieuwe ontwikkelingen. Wij adviseren u de communicatie van de rijksoverheid (www.rijksoverheid.nl) over Diginotar in de gaten te houden en uw systeembeheerders op deze informatie te wijzen.