Geheimen doorgesluisd door vergissing bij domeinnaam

Info ministerie publiek door foutje ambtenaar

door Bart Olmer

AMSTERDAM, maandag

Politiek gevoelige en geheime operationele informatie kan simpel op straat komen te liggen door slordig typende ambtenaren van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

De ambtenaren typten per ongeluk in mailtjes 'minbkz.nl' als maildomein, in plaats van het correcte 'minbzk.nl'. De foute domeinnaam 'minbkz'.nl' was in handen van securitybedrijf Fox-IT. Het securitybedrijf en het ministerie onderzochten samen of 'typosquatting' een reeel (spionage)gevaar is. De uitkomsten waren verbijsterend: in achttien weken tijd werden op het valse domein 271 gevoelige e-mailberichten ontvangen.

Het BZK-ministerie is onder meer verantwoordelijk voor de geheime dienst AIVD.

Typosquatting is gebaseerd op het feit dat mensen zich wel eens vergissen bij het typen van een domeinnaam. De 'typosquatter' zet een website op waarvan het adres slechts heel weinig verschilt van het adres van een populaire website. Alle internetgebruikers die dezelfde typefout of vergissing maken, komen terecht op de website van de typosquatter.

Beleid

Bij de proef van Fox-IT en het ministerie kwamen berichten binnen met uiterst gevoelige informatie: „De afzenders bestonden uit medewerkers van het ministerie, burgers, bedrijven en andere overheden. De berichten waren afspraakverzoeken, beleidsinhoudelijke zaken, facilitaire zaken, nieuwsbrieven, uitnodigingen, privécommunicatie en sollicitaties. Met name 'beleidsinhoudelijke zaken' bevatte informatie die men niet graag in verkeerde handen ziet. Bij een beperkt aantal was er zelfs sprake van politiek gevoelige dossiers", aldus Johri Maat, senior-adviseur bij het ministerie van Binnenlandse Zaken, en Fox-IT-specialist Francisco Dominguez Santos.

Volgens de deskundigen is deze vorm van spionage spotgoedkoop: het registreren van een domeinnaam kost maar een tientje. Daarmee is een gigantische 'stofzuiger' gecreeerd die handig misbruik maakt van typefoutjes.

Storing

„Ook informatie uit de categorieën 'afspraakverzoeken' en 'facilitaire zaken' kon door kwaadwillende lieden worden misbruikt. Zo kan een kwaadwillende een storingsmelding gebruiken door zich als storingsmonteur voor te doen en zo een organisatie binnen te dringen. Deze praktijktest toonde aan dat typosquatting niet alleen een theoretisch risico is. De belangrijkste maatregel is dat organisaties zelf 'lookalike' domeinnamen registreren, zodat anderen er geen misbruik van kunnen maken", aldus de deskundigen.

De foute domeinnaam is inmiddels aan de overheid overgedragen.