[redacted]

26. 54

Van: WOC
Datum: 10.11.1998
Betreft: Nieuwe richtlijnen VS inzake export sterke cryptografische producten en de gevolgen voor Nederland.

Op 16 september kondigde de Amerikaanse overheid nieuwe richtlijnen aan voor de export van sterke cryptografische producten. Dit memo gaat in op de gevolgen voor Nederland.

Kern nieuwe beleid VS

Twee jaar geleden werd het voor VS-bedrijven mogelijk om producten met maximaal 56 bits DES crypto sleutels te ontwikkelen, indien daaraan een "key recovery faciliteit" zou worden toegevoegd. De gebruikte sleutels zijn dan achteraf opvraagbaar door (VS-) opsporings- en inlichtingendiensten.
De nieuwe richtlijnen impliceren dat nu deze 56 bits sleutels (in randapparatuur, PC's, software) op de markt kunnen komen waarbij de sleutels niet beschikbaar zijn voor opsporings- en inlichtingendiensten. Het breken van de codes kan met de huidige technische middelen geen dagen maar jaren duren. De Nederlandse overheid kan via bestaande rechtshulpverdragen hulp en inzage vragen. Het is tot nu toe echter onduidelijk of en hoe snel deze procedures werken.

Stand van zaken tot nu toe

Een groot deel van de cryptografische producten dat nu ter onderzoek wordt aangeboden, is afkomstig van Amerikaanse bedrijven. Tot eind 1996 mochten zij slechts software voorzien cryptografische beveiligingsfuncties exporteren indien de beveiliging vrij gemakkelijk te breken was; dit betekende in praktijk in minder dan 1 uur.
Daarna werd het mogelijk om iets sterkere softwareproducten te exporteren. In de praktijk kwam dat neer op producten met cryptosleutels met een maximale lengte van 40 bits. Het kraken van (bijvoorbeeld) een huidig Microsoft Word bestand van 40 bits duurt ongeveer 30 uur.

Gevolgen voor de operationele aanpak cryptografie

Het optrekken van de sleutelgrens tot 56 bits betekent bij de huidige techniek dat de kraaktijd van een bestand oploopt tot 224 jaar. *([65536 (=2^{16}) maal 30 uur, oftewel 224 jaar (40 bits = 30 uur, 41 bits 60 uur, 42 bits 120 uur etc.).* E.e.a. kan grote gevolgen hebben voor de opsporing van strafbare feiten en voor de informatiepositie van I&V-diensten.
Bijkomend gevolg van het gebruik van dit soort producten kan zijn dat het beveiligingsniveau voor bijvoorbeeld de telecomproducten in Nederland automatisch wordt verhoogd.

Amerikaans samenwerkingsverband operationele cryptoproblematiek
Opgemerkt dient te worden dat gelijktijdig met het bekendmaken van de nieuwe richtlijnen de FBI heeft aangekondigd het Technical Support Centre (TSC) nieuw leven in te blazen. Dit TSC (een Amerikaanse versie van ons Samenwerkingsverband aanpak Operationele Cryptoproblematiek) zou een kraakfaciliteit voor de Amerikaanse rechtshandhaving moeten worden.

Aanbevelingen

1. Het Samenwerkingsverband dient snelle voortgang te maken met het kunnen oplossen van 56-bits problemen.
2. De diensten in het Samenwerkingsverband dienen te onderzoeken hoe toegankelijk de VS key recovery faciliteit voor Nederland is. Het is tot nu toe onduidelijk of, en hoe snel de standaard procedures in zo'n geval zullen werken.
3. Onderzocht dient te worden of de Amerikaanse overheid wel in staat is om binnen een redelijke termijn van enkele dagen 56 bits cryptografische producten te ontsleutelen.