BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank NL32ABNA0554706512
KvK 34121286

M +31 6 39 64 27 38
E rejo.zenger@bof.nl
W https://www.bof.nl

Hoogwaardige encryptie is essentieel voor onze economie en democratische vrijheid

Amsterdam
22 december 2015

De beschikbaarheid en de toepassing van hoogwaardige encryptie is essentieel voor de bescherming van onze digitale infrastructuur en communicatie, en daarmee niet alleen belangrijk voor onze democratische vrijheid maar ook van groot belang voor innovatie en economische groei.

De overheid moet daarom:

- de ontwikkeling van hoge standaarden voor encryptie stimuleren;
- de toepassing van hoogwaardige encryptie stimuleren en
- op geen enkele wijze die toepassing ondermijnen.

De Nederlandse overheid moet zich daarmee ook onthouden van het stellen van grenzen aan de maximale lengte van encryptiesleutels,[1] het bewust inbouwen van ingangen ten behoeve van de overheid (zoals 'achterdeurtjes'),[2] het verplicht toevoegen en afstaan van extra sleutels[3] of andere stappen die de ontwikkeling en toepassing van hoogwaardige encryptie in de weg staan.

Nederlandse economie heeft hoogwaardige encryptie nodig

De stimulering en toepassing van hoogwaardige encryptie bevordert het vertrouwen in onze digitale infrastructuur en communicatie. Het zorgt voor een goede bescherming van gevoelige persoonsgegevens, bedrijfsgeheimen en overheidsbelangen, en bemoeilijkt (economische) spionage.

De expliciete keuze voor hoogwaardige encryptie versterkt ook de internationale concurrentiepositie van Nederland. Afnemers zullen er waar mogelijk altijd voor kiezen hun gevoelige informatie onder te brengen bij bedrijven die hoogwaardige encryptie toepassen. Als Nederland de toepassing van hoogwaardige encryptie ondermijnt, betekent dit dat bedrijven die afhankelijk zijn van een sterke beveiliging van gevoelige informatie en communicatie naar het buitenland zullen uitwijken. Een land dat het gebruik van sterke encryptie stimuleert, versterkt zijn vestigingsklimaat.[4]

Het afdwingen van gebruik van encryptie van slechte kwaliteit brengt ook enorme lasten voor het bedrijfsleven met zich mee. Bedrijven moeten extra investeren om te kunnen voldoen aan de verplichte implementatie van bewust verzwakte technologie voor bepaalde markten. Internationaal opererende bedrijven zullen desondanks echter ook nog moeten investeren in sterke encryptie om zo te kunnen voldoen aan de eisen van afnemers in andere landen.

Deze investeringen remmen ook innovatie, omdat producten op voorhand aan meer eisen moeten voldoen.

Bovendien zet het een gevaarlijk precedent: als Nederland haar bedrijven dwingt om verzwakte encryptie toe te passen, zullen andere landen volgen. Als Nederland toegang wil tot de kwetsbaarheden in software van Chinese producenten, dan wil de Chinese overheid ook toegang tot kwetsbaarheden in de Nederlandse producten. Dat verhoogt de lasten van implementatie voor internationaal opererende Nederlandse bedrijven, maakt producten in eigen land kwetsbaarder en verhoogt het risico op (economische) spionage.

En dan is er ook nog de aansprakelijkheid in geval van misbruik. Het inbouwen van kwetsbaarheden betekent dat bedrijven moeten vertrouwen op de makers van de kwetsbaarheid. En wie is aansprakelijk als criminelen de op last van de overheid ingebouwde kwetsbaarheid misbruiken om eindgebruikers geld afhandig te maken of bedrijfsgeheimen te ontvreemden?

Ook Nederlandse overheid heeft baat bij hoogwaardige encryptie

Ook de Nederlandse overheid vertrouwt op hoogwaardige encryptie. De burger moet zoveel mogelijk digitaal belastingaangifte doen, de AIVD versleutelt haar staatsgeheimen, het leger vertrouwt op een goede bescherming van informatie om de risico's van militaire operaties te beperken en Nederlandse ambtenaren zouden zonder encryptie net zo goed achter open deuren kunnen onderhandelen met hun buitenlandse collega's.

Onze vrijheid bestaat bij gratie van hoogwaardige encryptie

Tot slot kan ook de Nederlandse burger niet zonder hoogwaardige encryptie. Het kunnen beschermen van digitale communicatie is essentieel voor zijn autonomie in een democratische rechtsstaat. Encryptie stelt burgers in staat informatie op te slaan en met anderen te communiceren, zonder inmenging van buitenaf. Daarmee is encryptie een fundamentele bouwsteen voor de vrijheid van meningsuiting en het respect voor de persoonlijke levenssfeer zoals vastgelegd in internationale verdragen als het Europees Verdrag van de Rechten van de Mens (EVRM).

Technisch: encryptie is niet slechts 'een beetje' te verzwakken

Als er niet onvoorwaardelijk wordt gekozen voor hoogwaardige encryptie, dan betekent dit dat er een weg wordt ingeslagen die haaks staat op de breed gevoelde noodzaak tot het beter beveiligen van ons digitale ecosysteem. Zulk beleid blokkeert zelfs het verder ontwikkelen van enkele vormen van sterke

encryptie, zoals daar waar gebruik wordt gemaakt van sleutels die per sessie gegenereerd worden.[5]

Daarnaast valt encryptie niet te verzwakken zonder nieuwe (additionele) kwetsbaarheden te introduceren. Een bewust ingebouwde kwetsbaarheid, zoals een backdoor, is niets anders dan extra functionaliteit waarmee de complexiteit van de software wordt vergroot. Complexiteit en veiligheid zijn omgekeerd evenredig aan elkaar: wie bewust een kwetsbaarheid inbouwt, bouwt potentieel onbewust nog meer kwetsbaarheden in.[6] Het gaat daarbij niet alleen om technische kwetsbaarheden. Als zo'n kwetsbaarheid breed geïmplementeerd moet worden, zijn er ook meteen vele ontwikkelaars bekend met die achterdeur. De extra functionaliteit vergroot bovendien het aantal manieren waarop de beveiliging doorbroken kan worden, de zogeheten 'attack surface'.

Een ingebouwde kwetsbaarheid kan bovendien door iedereen misbruikt worden. Het is namelijk technisch onmogelijk om een kwetsbaarheid zodanig in te bouwen dat enkel en alleen de Nederlandse opsporings- en/of geheime diensten er gebruik van kunnen maken.[7] Een in het geheim ingebouwde kwetsbaarheid wordt vroeg of laat ook misbruikt door kwaadwillenden.[8] De sleutels die op last van een overheid worden afgegeven en, onder de streep, toegang geven tot zeer veel en uiterst gevoelige informatie, zullen op zichzelf al een bijzonder aantrekkelijk doelwit zijn van kwaadwillenden.

Eenmaal ingebouwde zwakheden blijven ons decennia lang achtervolgen. Een aantal van de serieuze kwetsbaarheden die het afgelopen jaar in beveiligings-software zijn gevonden, zijn het gevolg van bewust en op last van overheden ingebouwde zwakheden in beveiligingssoftware.[9]

Een verbod op hoogwaardige encryptie is ten slotte niet te handhaven. Het aantal mogelijkheden van criminelen om zich aan de door de overheid opgelegde zwakheden te onttrekken, is oneindig.[10] Kennis van hoogwaardige encryptie is er al en verdere ontwikkeling en gebruik is niet tegen te houden. Het gevolg is dat enkel en alleen onschuldige burgers, bedrijven en overheden met zwakke encryptie opgescheept zitten.

Of zoals het motto van cryptograaf Phil Zimmermann luidt:

> "When crypto is outlawed, only outlaws will have crypto."

1 De Amerikaanse overheid beperkte tussen het aflopen van de Tweede Wereldoorlog en de jaren negentig de export van encryptiesleutels langer dan 40 bits. Andere landen moesten het maar doen met zwakkere vormen van encryptie: goed genoeg om betrekkelijk veilig te winkelen op het internet, maar zwak genoeg voor de geheime diensten om de encryptie ongedaan te maken. Deze beperking werd uiteindelijk opgegeven, mede uit angst voor negatieve consequenties voor de economische groei.

2 Soms ook 'frontdoor' of 'backdoor' genoemd.

3 Bekend als 'golden keys', 'key escrow', 'key recovery' en 'trusted third-party encryption'.

4 Er zijn verschillende bedrijven die, bijvoorbeeld naar aanleiding van het conceptwetsvoorstel voor de herziening van de Wet op de inlichtingen- en veiligheidsdiensten, zich uiterst negatief hebben uitgelaten over het vestigingsklimaat. Telecomprovider Voys zegt bijvoorbeeld: "If you value your customers privacy don't start your startup in the Netherlands [...]".

5 Een concreet voorbeeld is 'forward secrecy', een techniek waarbij de sleutels na gebruik zo snel mogelijk worden vernietigd. Gestolen sleutels zijn onbruikbaar om eerdere of latere communicatie te onderscheppen. Als de overheid de maker dwingt een extra sleutel op te nemen, zodat de overheid de communicatie altijd kan ontsleutelen, is het voordeel van "forward secrecy" ongedaan gemaakt.

6 In de jaren negentig introduceerde de Amerikaanse overheid een achterdeur, de Clipper Chip, die in allerlei systemen ingebouwd moest worden. Cryptograaf Matt Blaze toonde aan dat deze bewust ingebouwde kwetsbaarheid zelf ook weer een kwetsbaarheid bevatte.

7 De apparatuur van de Amerikaanse fabrikant Cisco bevatte een bewust ingebouwde kwetsbaarheid, bedoeld om (Amerikaanse) opsporings- en geheime diensten toegang te geven tot het internet-verkeer dat via deze apparatuur werd afgehandeld. Die functionaliteit bleek lek en door kwaadwillenden te misbruiken.

8 In Griekenland werd de functionaliteit die bedoeld was voor het door opsporingsdiensten afluisteren van telefoonverbindingen misbruikt door kwaadwillenden. Die konden op die manier de gesprekken van meer dan honderd parlementariërs en hooggeplaatste ambtenaren afluisteren. Het misbruik van de kwetsbaarheid begon ergens in de zomer van 2004 en werd pas in de daarop volgende lente ontdekt. Een meer recent voorbeeld is Google's interface waarmee zij de opsporings- geheime diensten toegang gaf tot gegevens van haar klanten. Die 'achterdeur' werd misbruikt door de Chinese geheime dienst om te zien of haar spionnen op de radar van de Amerikaanse overheid stonden.

9 De restricties op de export van encryptietechnologie in de jaren negentig zorgen vandaag de dag nog voor problemen. Hoewel uiteindelijk, bijna twee decennia geleden, de exportbeperkingen opgegeven werden, is de ondersteuning in de software voor die zwakke vormen van encryptie (om begrijpelijke redenen) nooit verwijderd – maar wel vergeten. Enkele maanden geleden werd duidelijk dat die code door kwaadwillenden misbruikt kon worden. Onderzoekers ontdekten twee kwetsbaarheden, bekend als FREAK en Logjam, waardoor schijnbaar versleutelde verbindingen niet langer versleuteld waren.

10 Zie ook "You can't backdoor a platform" van Jonathan Mayer. Als, bijvoorbeeld, de overheid eist dat Google er voor moet zorgen dat telefoons met het Android-besturingssysteem van een backdoor voorzien zijn, dan zou Google daar aan tegemoet kunnen komen door de encryptie van de harde schijf in de telefoon te verzwakken. Maar dat laat applicaties van derden op de telefoon ongemoeid. Ten einde ook daarin te kunnen voorzien zou Google ook elke applicatie op haar platform moeten beoordelen. Maar daarmee voorkomt Google nog niet dat een gebruiker een applicatie via een andere app store installeert. Dat is een wedstrijd die niet te winnen is.