

Voortaan veilig in de cloud

Toen begin september pikante foto's van grote beroemdheden uitlekten, bleek dat je danig moet oppassen met het opslaan van gegevens in de iCloud van Apple. Hoe veilig is de cloud en zijn er veiligere alternatieven?

Door Yannick Fritschy

1 Hoe konden zoveel foto's tegelijkertijd uitlekken?

Vanwege de omvang van het schandaal waren veel mensen bang dat de centrale beveiliging van iCloud was gekraakt. Binnen enkele dagen na het privacy-schandaal haastte Apple zich echter te melden dat het uitlekken van de foto's geen gevolg was van een breuk in het veiligheidssysteem. Uit veertig uur onderzoek bleek dat de foto's niet tegelijkertijd uit de cloud waren gevist, maar dat de hackers ze gedurende een lange periode afzonderlijk hadden verzameld door de individuele accounts van de beroemdheden te kraken. Een centraal lek zou tot een nog veel grotere stroom aan gegevens hebben geleid. Marko van Eekelen, hoogleraar softwaretechnologie aan de Open Universiteit Nederland en universitair hoofddocent aan de RU Nijmegen, ziet

dat bij dergelijke geavanceerde beveiligingssystemen niet snel gebeuren. 'Spionagediensten van de NSA zijn daar misschien toe in staat, maar voor een particuliere hacker is dat buitengewoon moeilijk', zegt hij.

2 Is het makkelijk om een persoonlijke account te hacken?

Vaak wel. Vlak voor het uitlekken van de naaktfoto's maakten hackers al gebruik van een onvolkomenheid in de Apple-app *Find my iPhone*. Computerprogramma's konden via de *bruteforcing*-methode onbeperkt wachtwoorden invullen, totdat ze het juiste hadden gevonden. Inmiddels heeft Apple daar een stokje voor gestoken door in te stellen dat je niet meer dan vijf keer een verkeerd wachtwoord mag opgeven. Toch zijn er nog genoeg andere manieren om een persoonlijke code te achterhalen. Bijvoorbeeld via phishing-mails: mails in naam van een officiële instantie die je vragen je wachtwoord prijs

te geven. Ook de beveiligingsvragen, die je helpen als je je wachtwoord bent vergeten, zijn vaak te kraken. Uit het oogpunt van gebruiksvriendelijkheid zijn dat eenvoudige vragen, zoals de meisjesnaam van je moeder of je eerste huisdier. Maar zeker in het geval van beroemdheden ligt het antwoord op zulke vragen vaak op straat.

3 Kun je jezelf beschermen tegen hackers?

Informatici raden in ieder geval aan een sterk, lang en regelmatig veranderend wachtwoord te hanteren, dat je niet al voor andere applicaties gebruikt. Volgens Van Eekelen is het gevaar dan al grotendeels weg. 'Als het wachtwoord onmogelijk te raden is, doordat het uit verschillende niet bij elkaar passende onderdelen bestaat, kan een hacker weinig beginnen', zegt hij. Daarnaast is het handig om laptops en andere apparaten zelf ook met een wachtwoord te vergrendelen en het besturingssysteem up-to-date te houden.



De hele wereld zag plotseling compromitterende privéfoto's van Rihanna. Eén troost: dit overkwam haar niet als *only girl in the world*.
MARC SCHILLER

Om echt veilig te zijn, kun je bij veel diensten, zoals Google, Microsoft en ook Apple inmiddels, tweestapsverificatie instellen. Dat houdt in dat je na het inloggen nog een tweede code moet invoeren, die je ontvangt op een ander apparaat, bijvoorbeeld je telefoon. 'Dat biedt momenteel de beste bescherming tegen hackers', zegt Van Eekelen. Veel mensen zijn echter te laks om tweestapsverificatie in te stellen, of willen hun telefoonnummer niet prijsgeven. Van Eekelen: 'Het zou goed zijn als clouddiensten dat standaard invoeren. Nu geven ze de gebruiker heel veel opties, maar die zijn niet allemaal even veilig.'

4 Zijn er goede alternatieven voor de grote clouddiensten?

Van Eekelen: 'Ik verwacht dat mensen vaker een externe harde schijf zullen gebruiken. Het gemak van de cloud blijft echter bestaan, en ik denk niet dat dit kleine schokje daar veel verandering in

zal brengen.' Maar een tussenvorm is in opkomst. De laatste tijd ontwikkelen steeds meer bedrijven software voor decentrale cloudopslag. Het programma BitTorrent Sync richt zich bijvoorbeeld op het synchroniseren van gegevens op verschillende apparaten, maar dan wel alleen je eigen apparaten. Daarnaast biedt ownCloud, zoals de naam al aangeeft, een stukje cloud dat je helemaal zelf beheert. Deze diensten moeten het tot dusver qua gebruiksvriendelijkheid en opslagruimte nog ruimschoots afleggen tegen de traditionele cloudgiganten, maar als gegevens uit de grote cloud blijven regenen zouden ze de komende jaren sterk aan terrein kunnen winnen.

5 Kunnen we de cloud voortaan maar beter vermijden?

In het geval van privacygevoelige informatie is het zeker verstandig om goed na te denken over waar je die opslaat. Informatici raden aan om automatische

synchronisatie met clouddiensten uit te schakelen, zodat niet elke naaktfoto meteen in de cloud terechtkomt. Je eigen harde schijf kun je eveneens beveiligen, en bovendien is de kans veel kleiner dat hackers daar gaan zoeken. 'Sommige mensen zijn bang dat hun harde schijf makkelijk te kraken is, maar die kun je ook met een wachtwoord vergrendelen of zelfs volledig versleutelen,' zegt Van Eekelen. 'Het is vergelijkbaar met geld. Je kunt het prima in je portemonnee bewaren in plaats van op de bank, maar dan moet je je portemonnee niet uit je zak laten steken.'

Daarnaast is het goed om te beseffen dat als je dan toch iets in de cloud opslaat, je vanzelf een deel van de controle erover verliest. Van Eekelen: 'Je kiest er dan voor om foto's niet in je eigen kast, maar in die van je burens te bewaren.' ■

Meer informatie

Een oratie van Marko van Eekelen op de Open Universiteit is te zien op youtu.be/CgYW1yf6gmY.