Inhoud

Voorwoord **9**

Inleiding: kies het risico **11**
Jij bent goud waard 12
Risico's inschatten 20

De belangrijkste stappen om te nemen **27**
Zinvolle maatregelen kiezen 28
Elementaire beveiligingsmaatregelen 34

Bescherming van persoonsgegevens **55**
Veranderingen in gedrag 56
Fysieke maatregelen 59
Handige tools en tips voor meer anonimiteit 61

Voor de echte diehard – een stap verder gaan **71**
Een andere desktop gebruiken 72
Een eigen server draaien 74
Een eigen cloud-omgeving opzetten 75

Bijlage: Nuttige sites **79**

Voorwoord

Beveiliging op internet wordt een steeds belangrijker thema voor mensen. Identiteitsdiefstal begint langzaam maar zeker een tastbaar probleem te worden: we horen steeds vaker dat persoonsgegevens worden gestolen, overheden onschuldige burgers blijken te bespioneren, criminelen miljoenen verdienen en dat de benodigde apparatuur of software toch niet zo betrouwbaar is als gedacht. Ondertussen is de informatiemaatschappij een gegeven, zijn social media een realiteit en speelt de cloud voor veel mensen een belangrijke rol in het dagelijks leven.

In dit boek helpen we je om je beter te wapenen tegen het gevaar dat van alle kanten lijkt te komen. Dat doen we niet alleen met praktische tips over welke tools nuttig zijn, maar ook met de nodige uitleg over beveiliging. Uiteindelijk moet je zelf nadenken over wat jij wel en niet wilt. Als je de belangrijkste mechanismen begrijpt, maak je vanzelf de keuzes die het best bij je passen. Niets is zwart-wit in beveiliging. Eigenlijk zijn we continu bezig met het maken van afwegingen tussen verschillende belangen. Dit boek helpt je daarbij. Het is geen kant-en-klare handleiding hoe tools werken. Daarvoor is de industrie te vluchtig en zijn er te veel verschillende apparaten. We helpen je de juiste richting te zoeken en zelf aan de slag te gaan. Beveiliging is namelijk nooit af.

Brenno de Winter, april 2014

Inleiding: kies het risico

1

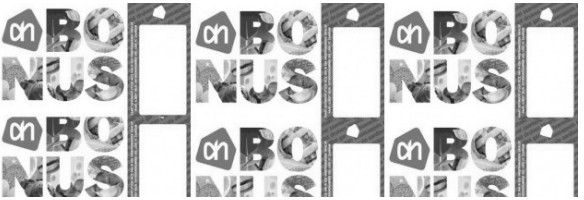
In de informatiemaatschappij waarin we leven, zijn onze gegevens geld waard. Dat begrijpen niet alleen bedrijven, maar ook criminelen en overheden. Daarom loont het aanvallen van onze systemen. Het vertrouwen op alleen leveranciers van software en hardware is niet langer goed genoeg, omdat niemand alomvattende bescherming kan bieden. We moeten ons dus bewust zijn van de risico's en daar maatregelen bij bedenken. Maar hoe brengen we de risico's in kaart en hoe werken beveiligingsmechanismen eigenlijk? In dit hoofdstuk staan we bij die vragen stil.

In dit hoofdstuk ontdek je:

- Hoe jouw informatie waarde heeft.
- Welke verschillende risico's er zijn.
- Hoe beveiligingsmechanismen werken.

Jij bent goud waard

In discussies over beveiliging klinkt vaak het argument dat mensen niet in jouw informatie geïnteresseerd zullen zijn. Maar het tegendeel is het geval: jij bent goud waard voor anderen. Facebook toont met de koop van Whatsapp, voor 19 miljard dollar, wat jouw contactenlijst en privéberichtjes waard zijn: 42 dollar per persoon. Voor een paar berichtjes, een contactenlijst en een gebruikerspatroon lijkt dat best veel geld. Maar netwerkinformatie is heel interessant voor bedrijven als Facebook. Sommige bedrijven zullen er grof geld voor over hebben om gedetailleerde informatie over jou te hebben. Dat is bijvoorbeeld het geval net voordat je een levensverzekering, hypotheek of andere belangrijke diensten afneemt.



Als informatie wordt aangevuld met andere gegevens, zijn de klantprofielen nog veel meer geld waard. Daarom heeft Albert Heijn tot twee maal toe een Bonuskaart geïntroduceerd. Want hoe nauwkeuriger jouw profiel is, hoe slimmer ze je kunnen verleiden vaker in de winkel te komen. In de onderwereld is dat mechanisme ook goed te zien. Voor minder dan een euro is een werkend creditcardnummer te koop, maar als er meer gegevens beschikbaar zijn en het gebruik eenvoudiger wordt, kan de prijs oplopen tot vele tientallen euro's. Met die informatie kan namelijk serieus geld worden uitgegeven en is oplichting effectiever. In een informatiesamenleving is jouw informatie gewoon goud waard!

Currence, het bedrijf dat het pinnen in Nederland regelt, wilde jouw gegevens gaan verkopen aan winkeliers. Zo valt er inzicht te krijgen in jouw koopgedrag en wordt duidelijk wanneer jij elders je geld uitgeeft. In een concurrerende wereld wil een winkel daar graag voor betalen. Aanleiding was dat het pinnen steeds goedkoper moet om de concurrentie het hoofd te bieden. Van die plannen werd afgezien toen klanten massaal boos reageerden.

En zelfs als jij als persoon niet interessant zou zijn, dan is jouw informatie het wel. Een mobieletelefoonprovider weet exact waar jij bent. Aangezien ze dat van heel veel klanten kunnen nagaan, weten ze ook precies waar het druk is. Er zijn al routeplanners die het aantal mobiele telefoons op een weg gebruiken om te voorspellen waar de files ontstaan. Voor die dienstverlening willen klanten dan weer betalen. Zo koop je indirect wat eigen informatie terug!

Bij phishing websites, die je verleiden om allerlei persoonlijke gegevens in te vullen, is de business lucratief. Niet

alleen geven onoplettende mensen allerlei nuttige informatie door, ook surfen ze op kwaadaardige websites, die kinderlijk eenvoudig je computer of mobiel vullen met bedenkelijke software. Op die manier is zelfs ná een bezoek de computer nog te misbruiken en kunnen documenten worden gestolen. Er zijn bedrijven die voor banken dit soort oplichterswebsites monitoren en proberen ze te stoppen. Dat lukt soms al binnen enkele uren, maar volgens experts zijn er dan met de oplichterstrucs al tonnen verdiend. Dus het stelen van e-mailadressen lijkt onschuldig, maar als een piepklein percentage in een oplichtersmail trapt, loont dit voor de criminelen enorm.

En sinds de onthullingen van Edward Snowden weten we dat inlichtingendiensten 52 miljard dollar per jaar verstoken. Voor slechts een fractie van dat bedrag worden clouddiensten van Facebook, Google, Microsoft en Apple gemonitord of afgetapt. Massale taps op internet lijken naast het afvangen van zakelijk verkeer ook op persoonlijke gegevens te zijn gericht. Slechts een fractie is vanuit terreurbestrijding te verklaren. Want Angela Merkel en de paus luister je om die reden niet af. Onze informatie is gewoon keihard geld waard ten behoeve van economische spionage en een vorm van controle. Bedrijven, criminelen en overheden hebben dus interesse in jouw informatie, want jij bent voor hen goud waard!

Beveiliging is een economie

Beveiliging is een economisch probleem. We horen vaak dat 100 procent beveiliging niet bestaat. Dat is waar, maar het dient ook vaak als dooddoener. Vaak is de bedoeling om falen daarmee goed te praten. Maar het klopt wel dat je nooit ieder risico kunt uitsluiten. Er moet altijd een balans worden gevonden tussen risico en maatregelen. Ook kan

het nemen van een maatregel andere beveiligingsrisico's introduceren. Het maken van back-ups helpt bijvoorbeeld tegen verlies van gegevens, maar brengt ook meteen risico's met zich mee. Wie bijvoorbeeld een harde schijf goed versleutelt, loopt het risico dat de data nooit meer toegankelijk is als het wachtwoord wordt vergeten.

Op het moment dat iets waarde heeft en we die waarde beseffen, gaan we onze bezittingen beter beschermen. Bewustzijn van de waarde helpt de beveiliging vooruit. Daarbij gaat het niet alleen om een economische waarde, maar bijvoorbeeld ook om een emotionele waarde. Precies dat mechanisme helpt niet bij informatiebeveiliging, omdat het vaak lastig is voor te stellen dat de informatie iets waard is.

Organisaties werken volgens de economie

Dat het voornaamste aspect van beveiliging economie is, maakt het ook een belangrijk stuurmiddel. Bij veel banken in de Verenigde Staten is internetbankieren met weinig meer dan gebruikersnaam en wachtwoord beveiligd. De aansprakelijkheid is zo geregeld dat deze bijna altijd bij de klant ligt. Voor een bank is er dan ook weinig aanleiding om veel aan beveiliging te doen. In Nederland ligt een groot deel van de verantwoordelijkheid bij de banken, waardoor zij ook financieel risico lopen. Daardoor loont het daadwerkelijk energie te steken in de beveiliging van de toegang tot het systeem. Nu de houding van de banken meer en meer verandert en jij ook risico gaat lopen, willen de banken jouw gedrag beïnvloeden.

Een ander voorbeeld is wetgeving die bedrijven verplicht om melding te maken wanneer er persoonsgegevens zijn gelekt. Door de aandacht en de vrees voor reputatieschade

worden bedrijven voorzichtiger, en zal er sneller worden besloten geld te investeren in beveiliging. De economie dwingt dan tot actie, omdat reputatie ook een waarde vertegenwoordigt. In de Verenigde Staten werd wetgeving geïntroduceerd om beursgenoteerde bedrijven te verplichten de administratie op orde te hebben. Verantwoordelijken riskeren celstraf. Dat stukje economie is voor de organisaties reden genoeg om fors te investeren in een accurate administratie en het strikt hanteren van regels.

Bedenk dat organisaties altijd hun eigen economie voorop hebben staan. Het beschermen van jouw gegevens is alleen interessant omdat het alternatief slechter is: weglopende klanten of problemen met de wetgever. Wees realistisch en bedenk dat altijd slechts het minimale aan beveiliging zal worden gedaan. Is een dienst gratis, dan moet de economie anders worden gevoed. Dat kan zijn via advertenties, het doorverkopen van gegevens of het voorzien in een behoefte zoals het nastreven van een maatschappelijk doel. Denk daarom altijd na welke diensten je gebruikt en wat de (privacy)voorwaarden zijn. Statements als 'wij houden ons aan de Wet bescherming persoonsgegevens' zijn doodoeners. Iedereen hoort zich aan de wet te houden!

Aanvallers hacken economisch bewust

Ook criminelen hebben bij het hacken economische bedoelingen. Natuurlijk kunnen bepaalde mensen een bewust doelwit van aanvallers zijn, maar in veel gevallen gaat het gewoon om het stelen van waarde. Of je nou Jan, Piet of Klaas heet, maakt dan niet zo veel uit. Het gaat erom om met zo min mogelijk moeite zo veel mogelijk geld te verdienen. Als een crimineel dus iets wil bereiken, zal deze voor de weg van de minste weerstand kiezen. Door jezelf te

beveiligen tot een niveau dat net iets beter is dan dat van andere mensen, nodig je criminelen uit jou met rust te laten.

Zie het als twee appartementen naast elkaar met beide een schitterende stereo, televisie en dure juwelen die voor inbrekers zichtbaar zijn. Het eerste appartement heeft een alarminstallatie, strips op de deuren en goede sloten. Het andere heeft al die maatregelen niet. Waar denk je dat een dief zal inbreken? Mocht je het doelwit van een gerichte aanval zijn (dus iemand moet per se jou hebben), dan helpt beveiliging wel iets, maar deze zal uiteindelijk tekort schieten. De economie is dan immers een andere: ze moeten jou hebben. Voor de meeste criminaliteit geldt dat gelukkig niet.

Uit de documenten van Edward Snowden – over het inbreuk maken op privacy door de Amerikaanse National Security Agency – wordt duidelijk dat massaal spioneren relatief goedkoop is. Het is haalbaar gebleken om een profiel van zo'n beetje iedere wereldburger te maken. Daarbij kunnen ook de inhoud van berichten en zelfs telefoongesprekken goed bewaard worden. Op zich is dat geen vreemd verschijnsel als je beseft dat diensten voor video en foto's uit de advertentie-inkomsten enorme hoeveelheden data kunnen genereren en opslaan. Wie zich beter beveiligt en meer communicatie afschermt, zal vanzelf buiten de standaard spionage gaan vallen. Als de Amerikanen dan iets over je willen weten, moeten ze gerichte en dus duurdere aanvallen gaan uitvoeren. Daarmee loont massale spionage niet meer. Beveiligen helpt dus om risico's te verkleinen, maar zal nooit alles oplossen.