

/visie

Informatiebeveiliging

>>i've got nothing to hide, but everything to protect

Informatiesystemen spelen een cruciale rol in onze moderne samenleving. Uiteraard moeten die systemen goed worden beveiligd. Maar nog belangrijker is de vraag wat we erin opslaan en waarom. Privacy wordt het best beschermd door zo min mogelijk informatie te hebben.

Informatiebeveiliging als sluitstuk

Steeds meer bedrijven en instanties gebruiken informatiesystemen voor hun bedrijfsvoering. Van supermarkten tot ziekenhuizen en van banken tot de belastingdienst, overal liggen gegevens over ons opgeslagen; koopgedrag, ziektes, schulden en inkomsten.

Gevoelige informatie die we graag goed beveiligd hebben. In de wereld van informatiesystemen bestaat echter een merkwaardige paradox. Hoewel de beveiliging een onlosmakelijk onderdeel van elk informatiesysteem is, wordt het vaak niet integraal meegenomen in het ontwerp. Beveiliging komt dan pas tegen het einde om de hoek kijken. "Het huis is af. Nu nog een slot op de deur."

Deze scheiding tussen architectuur en beveiliging is traditioneel gegroeid. Bij het beveiligen gaat alle aandacht naar een gegeven informatiearchitectuur. Maar er wordt niet gevraagd waarom die architectuur is zoals hij is.

Privacy is het niet hebben van informatie

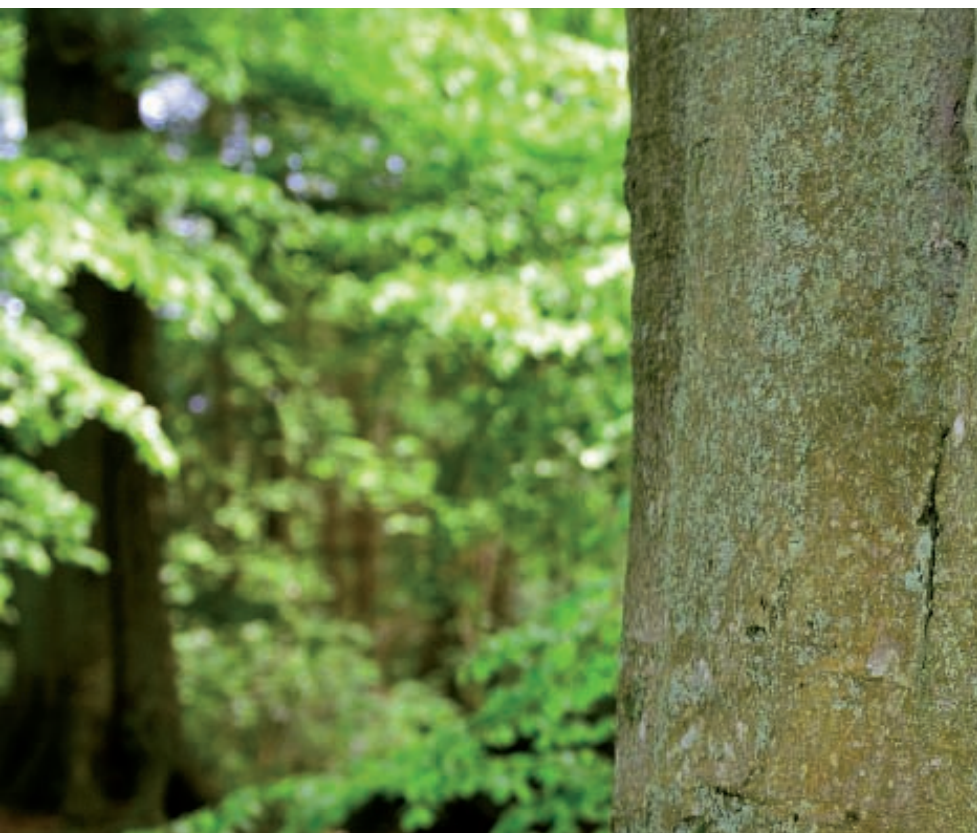
Bij privacy is het belangrijk om de 'waarom-vraag' juist al bij aanvang van een project te stellen. De kernvraag luidt: moet je die data überhaupt wel op die plek hebben? In het ideale geval heb je zo min mogelijk informatie om de privacy te waarborgen. Dikwijls worden dit soort vraagstukken niet meegenomen bij het ontwerp van een systeem. Ze worden doorgeschoven naar de implementatiekant. Zo ontstaan technische deeloplossingen met protocollen, wachtwoorden en fysieke beveiligingen. Allemaal achteraf, zonder vooraf goed over het concept na te denken.

Anonieme Kilometerprijs

Wij zien het helaas nog steeds vaker fout dan goed gaan, maar gelukkig zie je ook goede voorbeelden waarbij de beveiligings- en privacyaspecten vanaf het prille begin zijn meegenomen. Zoals bij Kilometerprijs, die volop in de belangstelling stond, zij het vaak in negatieve zin. Uit oogpunt van beveiliging en privacy is dat ten onrechte. De essentie van kilometerheffing is: registreren hoeveel kilometer een auto op een bepaald type weg heeft gereden. Apparatuur in de auto berekent uit de GPS-coördinaten en de verschillende tarieven welk totaalbedrag verschuldigd is. Het rekenwerk gebeurt in de auto. Informatie als tijd en locatie komen de auto niet uit. Er gaan slechts een paar anonieme gegevens naar de overheid. Dit principe geldt ook in andere systemen: risico's met privacy zijn het makkelijkst en het best op te lossen aan de gebruikerskant. Zo zorgt de systeembouwer dat gevoelige informatie überhaupt niet beschikbaar komt.

Function creep

Vanuit technisch oogpunt kan het aantrekkelijk zijn om zo veel mogelijk informatie te vergaren en die vervolgens te combineren met zoveel mogelijk functies. Want je weet maar nooit wat je in de toekomst nog eens nodig hebt. Minimalisme is vaak niet aan technici besteed. Vanuit hun technische bevoegdheid streven ze juist naar meer mogelijkheden en functies. Helaas brengt dat ook risico's met zich mee, zoals we nu kunnen zien bij centrales voor telefoon en internet.

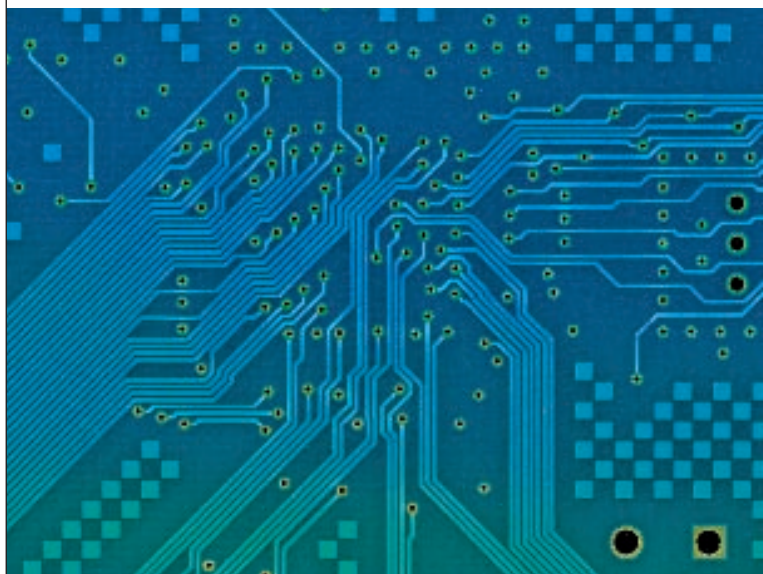


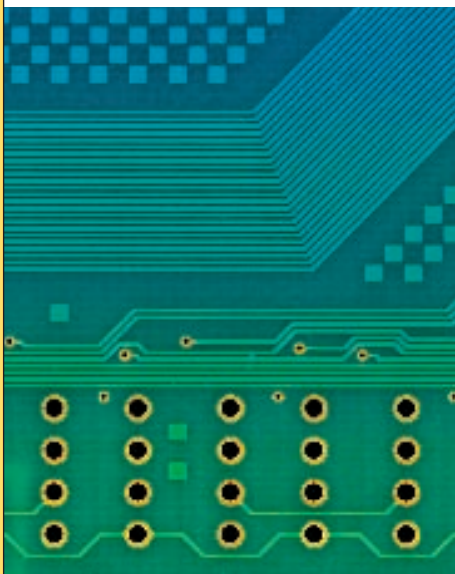
Ontwerpers van nieuwe (digitale) telecomcentrales bouwden opslagfunctionaliteit in. Dat was handig om de kwaliteit van het eigen systeem en netwerk te analyseren. Gegevens werden zes weken bewaard en dan verwijderd. De opslag werd niet geanonimiseerd, want het was toch alleen maar voor eigen technische analyses. De overheid vond die bewaarde informatie wel handig voor opsporingsdoeleinden: “daar kunnen we criminelen mee lokaliseren en opsporen.” Zo ontstaat function creep: ingebouwde functies worden later voor andere toepassingen gebruikt of misbruikt.



>>welke informatie opslaan?

Inmiddels is Nederland wereldwijd nummer één in het gebruik van telefoontaps. Bovendien stelt Europese wetgeving telecomproviders verplicht om 6 maanden alle gegevens van alle gebruikers te bewaren. Het is natuurlijk de vraag of deze wettelijke ruimte achterwege was gebleven als de technische mogelijkheden ontbraken. Maar dankzij de ruime functionaliteit van moderne telefooncentrales, is deze inbreuk op onze privacy nu mogelijk.





Wat is informatiebeveiliging?

Kortom, als de informatie er is, is de verleiding groot om het te gebruiken. Dus zorgt een verstandige ontwerper ervoor dat een systeem zo min mogelijk informatie nodig heeft. En die informatie behoeft uiteraard een goede beveiliging qua beschikbaarheid, integriteit en geheimhouding. Daarbij draait het om het totale systeem waar de informatie doorheen gaat: zowel opslag als transport van data.

Beschikbaarheid

Voor de Kilometerprijs zou elke auto permanent zijn route vastleggen. Het GPS-signaal moest dus altijd en overal beschikbaar zijn. Ook de kastjes in de auto's moesten het altijd doen. De communicatie met de backoffice was minder kritisch. Als die verbinding wegvalt, houdt het kastje zijn gegevens vast om het later nog eens te proberen. Het oplossen van deze vragen rond beschikbaarheid vereist een goed totaaloverzicht. Hoe werken alle deelsystemen met elkaar samen? Wat gebeurt er als er één systeem uitvalt? Hoe herstelt zich dat? Dat is system engineering.

Integriteit

Integriteit draait om de juistheid van gegevens. Kloppen de getallen die ik uitlees, zijn ze actueel, volledig, niet gemanipuleerd en van de vermelde bron? Belangrijke vragen voor elk informatie-systeem, maar zeker voor systemen die ondersteunen bij het nemen van belangrijke beslissingen. Vliegtuigen en schepen moeten blind kunnen vertrouwen op meetgegevens. Door meetresultaten te bewaren in een "data log" kan manipulatie worden aangetoond, daarnaast kan een uitspraak worden gedaan over de integriteit. De gebruiker kan hiermee zien (en bewijzen) wat er is gebeurd. De opslag van gegevens dient hier als bewijslast, maar ook om in geval van problemen te kunnen analyseren wat er mis ging. In de zwarte doos van een vliegtuig levert dat onontbeerlijke informatie op. Dit soort systemen lijken qua werking op financiële systemen. Een bank wil elke transactie kunnen herleiden van betaler tot ontvanger. Bancaire systemen zijn per definitie niet met het oog op privacy gebouwd. Integendeel, hun beveiliging werkt door betalingen te volgen en te analyseren. Wat betaalt de klant met zijn creditcard, welke bedragen en aan welk soort winkels of bedrijven? Als daar iets vreemds tussen zit, merkt de bank het meteen. Zo bestrijden banken fraude. Ze zullen hun gegevens niet snel misbruiken. Een bank geniet vertrouwen en wil dat behouden.

>>communiceer open en volledig naar gebruiker

Geheimhouding

Bij geheimhouding is het zaak om de informatie alleen toegankelijk te laten zijn voor daartoe bevoegde personen en systemen. Geheimhouding draait dus vooral ook om organisatie. Wie heeft er toegang tot gevoelige informatie en hoe voorkomen we dat onbevoegden toegang tot deze informatie krijgen?

Beveiligingstechnologie

Om de integriteit en geheimhouding van signalen of communicatie te beschermen bestaat een breed scala aan cryptografische technieken. Zo'n techniek versleutelt de informatie, zodat niemand er onderweg bij kan. De ontvanger heeft een sleutel om de informatie te ontsluiten. Hij kan tevens zien of er onderweg met de gegevens is gerommeld. Digitale sleutels kunnen bijvoorbeeld komen uit een PKI-certificaat. PKI staat voor Public Key Infrastructure, een wereldwijde techniek die mensen en machines voorziet van een digitaal paspoort (PKI-certificaat) en een eigen sleutel. Gespecialiseerde bedrijven zoals VeriSign geven PKI-certificaten uit. Zij zijn de vertrouwde derde partij in dit proces van versleuteling, een soort 'sleutelkoning' van internet. Overigens biedt een digitaal paspoort geen absolute zekerheid, het kan net als een gewoon paspoort vervalst worden.

Restrisico's

Hoe goed je ook beveiligt, er blijven altijd restrisico's. Een 100% veilig systeem bestaat nu eenmaal niet. De restrisico's zullen organisatorisch moeten worden opgevangen zodra ze optreden. Denk hierbij aan wie er verantwoordelijk is en of de organisatie dan besluitvaardig is qua handelen en communicatie. Dit betekent dat er naast techniek ook gepland moet worden in de vorm van overdachte scenario's en processen om eventueel additionele technologie in te passen.

Communicatie

De gehackte OV-chipkaart krijgt in de media alle aandacht. Misschien omdat journalisten niet weten wat er precies speelt. Het grote publiek krijgt zo echter een vertekend beeld van nieuwe technologie. Een probleem dat ook de Kilometerprijs parten heeft gespeeld. Technisch steekt de Kilometerprijs goed in elkaar, maar in de communicatie naar de burger is het nodige misgegaan. De burger krijgt verplicht te maken met nieuwe, onbekende technologie. Onbekend maakt onbemind en techniek vinden we eng. Zeker als we denken dat onze privacy in het geding is.

Anderzijds bellen en surfen we ons suf zonder over privacy na te denken. Maar zodra de overheid ons ergens toe verplicht, staan we op scherp. Privacy en informatiebeveiliging liggen gevoelig, dus moeten overheid en bedrijven juist daarover goed en overtuigend communiceren. Met de juiste timing: op een zelf gekozen ogenblik naar buiten treden, met een consistent verhaal en duidelijke antwoorden op alle vragen. Wees ook eerlijk over restrisico's. "Gezien de stand van de techniek en organisatie kunnen we nu dit en ook niet meer dan dit."

Vertrouwen en reputatie

Een goed project kun je vernietigen met slechte communicatie. Door gebrekkige communicatie is het vertrouwen in de Kilometerprijs geschaad. De communicatie kwam te laat en was reactief, als antwoord op negatieve vragen. Wie in de publieke opinie het vertrouwen verspeelt, wint dat niet terug met een briljante technische oplossing. Vertrouwen ontstaat door communicatie, niet alleen met de burger, maar ook met bedrijven en tussen bedrijven onderling, dus met alle stakeholders.

