Dr.ir. O. Tettero *

Hoe zijn goede en veilige ICT-systemen te maken

'Hackers vinden lek in product X'. Informatie en Communicatie Technologie (ICT)-producten zijn regelmatig op deze wijze in het nieuws. Zijn die hackers zo slim of de producten zo slecht? Het blijkt dat het ontwerpen van veilige producten helemaal niet eenvoudig is. Dit artikel gaat in vogelvlucht in op de wijze waarop ICT-producten met adequate informatiebeveiliging zijn te ontwerpen. Wat zijn de problemen en de valkuilen? Waar moeten productontwerpers rekening mee houden tijdens het ontwerpen?

Organisaties kunnen tegenwoordig niet zonder informatiebeveiliging. Hun waardevolle informatie wordt verwerkt in ICT-systemen en dat brengt risico's met zich mee. Risico's zijn onder andere dat een document gewijzigd wordt zonder dat de auteurs dit weten of kunnen achterhalen, dat de inhoud van een document bekend wordt bij de verkeerde mensen en dat een computer met een document onbereikbaar wordt voor de auteur die net voor een deadline zit.
Het gebruik van ICT biedt voordelen, maar gelijktijdig maakt het organisaties en hun medewerkers kwetsbaarder voor storingen en onderbrekingen. Daarom is er behoefte aan beveiligde ICT-systemen die de kwetsbaarheid verminderen.

Systeemprestaties

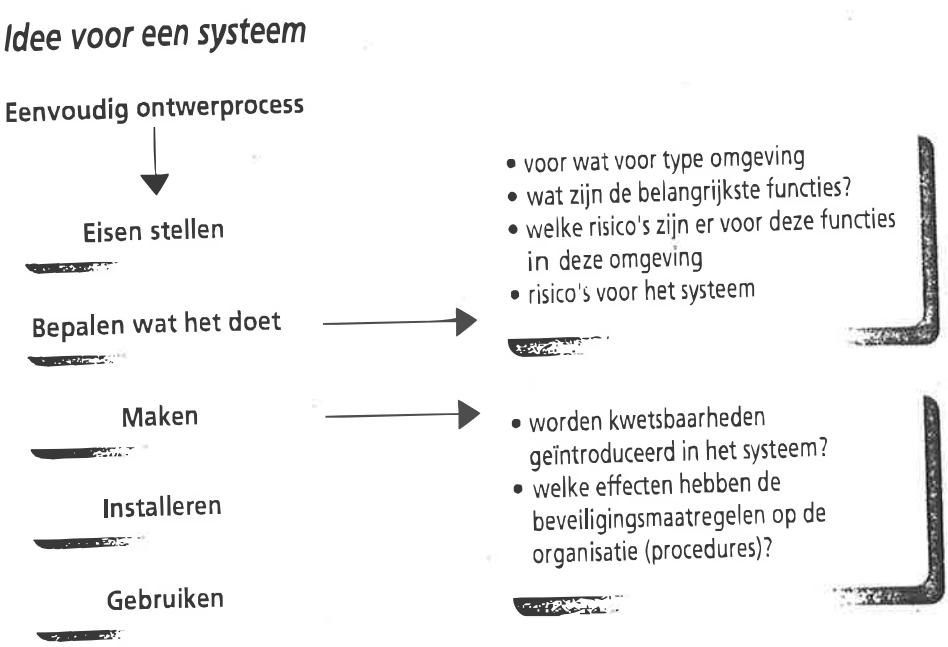
Ter bescherming tegen de kwetsbaarheden kunnen organisaties beveiligingsmaatregelen toevoegen aan hun bestaande ICT-systemen of een nieuw ICT-systeem aanschaffen dat al beveiligd is.
Nu blijkt de eerste mogelijkheid in de praktijk nogal moeilijk te zijn. Bovendien wordt op deze wijze de gewenste bescherming - het uiteindelijke doel van de hele exercitie - niet gehaald.
Ook vermindert toevoeging van beveiligingsmaatregelen de prestaties van het ICT-systeem. De uitwisseling van gegevens met een ander systeem gaat bijvoorbeeld trager, omdat eerst softwarematige vercijfering moet plaatsvinden. De beveiligingsmaatregelen gaan dan ten koste van de primaire activiteiten van de organisatie. Een ander gevolg is dat de beveiliging ingrijpt in de oorspronkelijk functionaliteit van het ICT-systeem. Beheer op afstand is bijvoorbeeld niet langer toegestaan. De reikwijdte van dit soort ingrepen is vaak niet onmiddellijk te overzien.
Direct al veilige ICT-systemen aanschaffen is overigens ook geen makkelijke optie. Immers, wat moet het systeem voor beveiliging bieden en welk vertrouwen rechtvaardigen de toegepaste maatregelen? Met name overheden en grotere bedrijven vertrouwen niet zomaar op de blauwe ogen van de productontwerpers. De systemen moeten dus langs een meetlat worden gelegd om te kijken of de beveiliging adequaat is.

Organisatorische inbedding

Toch gaat de voorkeur uit naar integratie van beveiliging in het ontwerp van ICT-systemen. Softwareontwerpers kunnen beveiligingsmaatregelen namelijk al toepassen voordat het systeem gebruikt gaat worden. Helaas blijkt dit slechts zelden op systematische wijze te

Management-summary
Organisaties willen hun waardevolle informatie in ICT-systemen beschermen. Veel systemen bieden daarvoor onvoldoende bescherming. Ontwerpers beschouwen beveiliging namelijk als lastig en veronachtzamen dit aspect daarom tijdens het ontwerpen van een ICT-systeem. Het is mogelijk om veiliger systemen te bouwen wanneer beveiliging wordt geïntegreerd in het realiseren van de primaire functionaliteit. Van belang hierbij is dat in een zo vroeg mogelijk stadium bepaald wordt wat het systeem, gegeven de gevoeligheid van de verwerkte informatie, aan beveiligingsfuncties moet bieden en wat het in geen geval mag doen. Ten tweede moet tijdens de realisatie van de functionaliteit stelselmatig worden geanalyseerd of met een bepaalde ontwerpkeuze de beveiligingsdoelstellingen worden gecompromitteerd.

* Olaf Tettero is gepromoveerd aan de Universiteit Twente. Bij het Telematica Instituut te Enschede (1994 - 1998) heeft hij een deel van het onderzoek hiervoor uitgevoerd. Sinds 1998 werkt hij bij de Evaluatiefaciliteit voor Informatiebeveiliging van TNO FEL.



Figuur 1. Beveiligingsspecifieke onderwerpen in een ontwerpproces.

gebeuren. Een reden hiervoor is dat de aandacht gericht is op de primaire functionaliteit van de software. En dat is een voornamelijk technische aangelegenheid.

Organisatorische inbedding

Adequate technische beveiliging staat of valt echter met een goede organisatorische inbedding. Hoe is het sleutelbeheer geregeld? Hoe vaak moeten sleutels worden gewisseld? Wie mag dat doen? Welke processen in een organisatie werken niet meer als er sleutels kwijtraken? Juist aan deze organisatorische inbedding schenken ontwerpers traditioneel weinig aandacht. Zij gaan er ten onrechte van uit dat hun systemen per definitie voor een keurige omgeving bedoeld zijn. Het gedrag van de gebruikers en processen die interactie hebben met het systeem wordt dus correct gedefinieerd.
Vanuit beveiligingsoogpunt is echter vooral het eventuele minder correcte gedrag van belang. Een ontwerper die niet vanuit dit perspectief werkt, zal tijdens het ontwerpproces niet alle noodzakelijke beschermingsmaatregelen identificeren. Beveiliging wordt bovendien nog eens als lastig ervaren en komt ook nog eens boven op de complexiteit van de primaire functionaliteit. Om die primaire functionaliteit binnen de randvoorwaarden van tijd en geld te kunnen opleveren wordt genoegen genomen met uitstel en veronachtzaming van de beveiligingsfunctionaliteit.

Houvast voor beveiliging

Het is belangrijk dat beveiliging wordt meegenomen in het ontwerpproces, dat het vanaf het begin de aandacht heeft en dat uitstelgedrag vermeden wordt. Dit maakt het noodzakelijk om beveiliging te integreren in het ontwerpproces.
Ontwerpers blijken echter binnen de huidige manier van werken onvoldoende houvast te hebben om systemen te bouwen die adequate functionaliteit bieden en ook nog veilig zijn.
Nu kan het ontwerpproces op drie niveaus houvast bieden. Het eerste niveau is dat van de activiteiten. Welke activiteiten moeten uitgevoerd worden om beveiliging adequaat tijdens het ontwerp mee te nemen en op welk moment in een ontwerpproces kunnen deze activiteiten het beste worden uitgevoerd?
Het tweede niveau is de rolverdeling. Wie zijn betrokken bij het uitvoeren van de activiteiten en welke expertise moeten deze mensen in huis hebben?
Het derde niveau zijn de hulpmiddelen. Welke hulpmiddelen hebben de ontwerpers nodig bij het uitvoeren van de activiteiten? Deze drie niveaus geven overigens nog niet aan op welke wijze beveiliging moet worden meegenomen.

Belangrijke aspecten

Voor het verwerken van beveiliging in het ontwerp zijn vijf aspecten van belang. Als eerste is dat integratie. De voor beveiliging vereiste activiteiten moeten worden geïntegreerd in de activiteiten die nodig zijn om de primaire functionaliteit van een systeem te verkrijgen. Dit stelt de ontwerper in staat om een balans te vinden tussen primaire functionaliteit en beveiligingsfunctionaliteit.
Het tweede aspect is het vasthouden van de aandacht. De voor beveiliging noodzakelijke activiteiten moeten terugkeren in alle fasen van het ontwerp of invloed hebben op die fasen. Zo blijft het mogelijk tijdens het ontwerp de beveiliging te identificeren en af te wegen tegen de primaire functionaliteit.
Aspect drie is het afstemmen van de beveiliging op het abstractieniveau van een ontwerp. Wanneer de systeemconcepten voor de primaire functionaliteit zich op een ander abstractieniveau bevinden dan de beveiliging kunnen namelijk geen afwegingen gemaakt worden ten opzichte van de beveili-

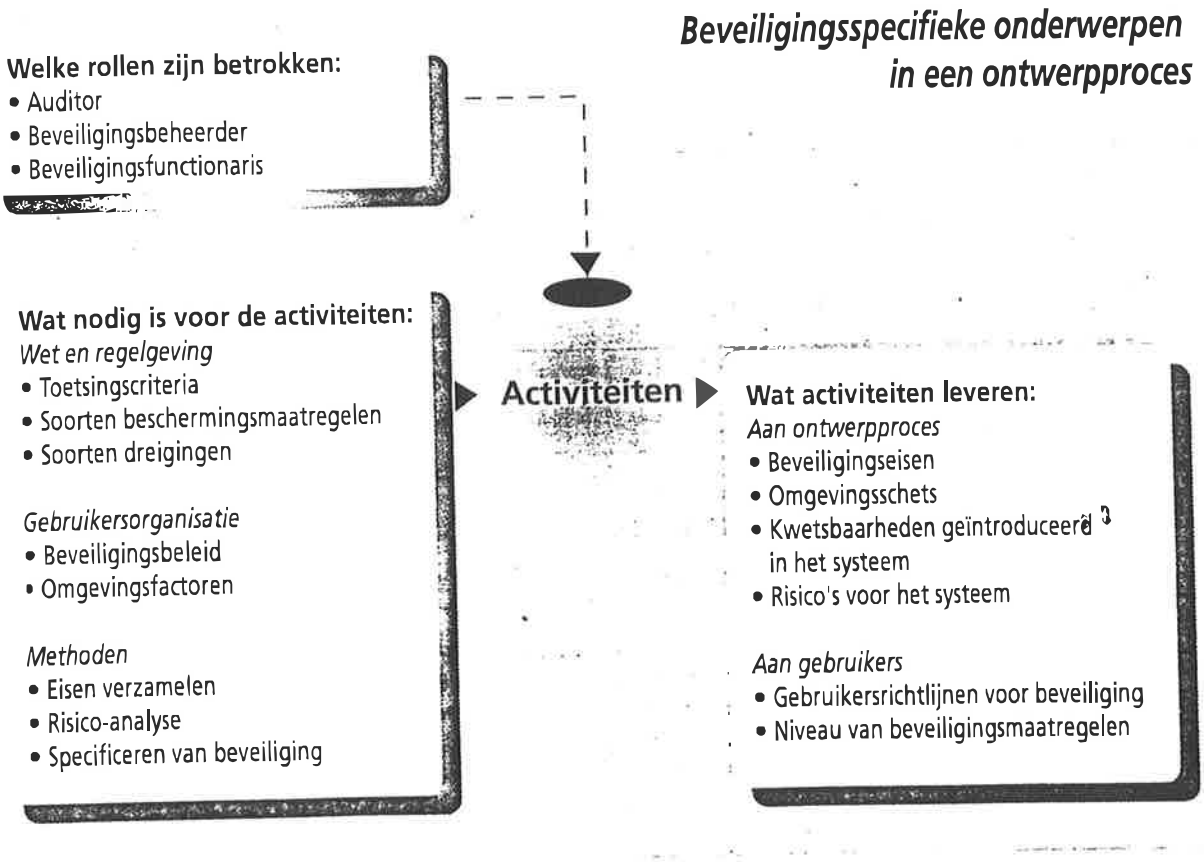
gingsfunctionaliteit. Het zou grofweg neerkomen op het 'even aanplakken van een vercijferboxje'.
Op de vierde plaats is het van belang om het ICT-systeem niet als geïsoleerd technisch systeem te beschouwen. Naast technische zijn namelijk ook organisatorische, procedurele en menselijke kenmerken van belang. Beveiliging is sterk gelieerd aan dit soort kenmerken. Het beïnvloedt ze, maar wordt er zelf ook door beïnvloed.
Tot slot is de overdracht van beveiligingskennis aan het ontwerpproces van belang om het mogelijk te maken een volledige verzameling van beveiligingseisen te definiëren.

Eisen

Hoe zijn de vijf aspecten te realiseren binnen het ontwerpproces? Hiervoor bestaan weer zeven beveiligingsspecifieke activiteiten. De belangrijkste rollen en hulpmiddelen die bij deze activiteiten meespelen, staan in figuur 1.
Om te bepalen wat voor beveiliging een systeem vereist, moet de ontwerper weten in wat voor soort omgeving het terecht komt. Is het systeem bedoeld voor een militaire omgeving waarin al veel beveiligingsmaatregelen zijn genomen of gaat het naar een e-commerce-omgeving waarvan niet bekend is wie de klanten zijn en welke intenties die hebben? Van belang voor het vaststellen van de beveiligingseisen zijn de systemen zelf, de gebruikers, de fysieke omgeving en de geldende procedures.
Natuurlijk heeft elk systeem te maken met bepaalde risico's. In hoeverre hiervoor maatregelen nodig zijn hangt af van de omgeving en de primaire functionaliteit. Wanneer in de omgeving procedurele of organisatorische beveiligingsmaatregelen zijn genomen, hoeven deze niet nog eens overgedaan te worden in het ICT-systeem. De primaire functionaliteit bepaalt welke waardevolle informatie het systeem verwerkt. Wanneer deze informatie zonder het systeem verwerkt wordt, zullen er bepaalde risico's zijn. Hoe liggen die risico's bij het nieuwe systeem?

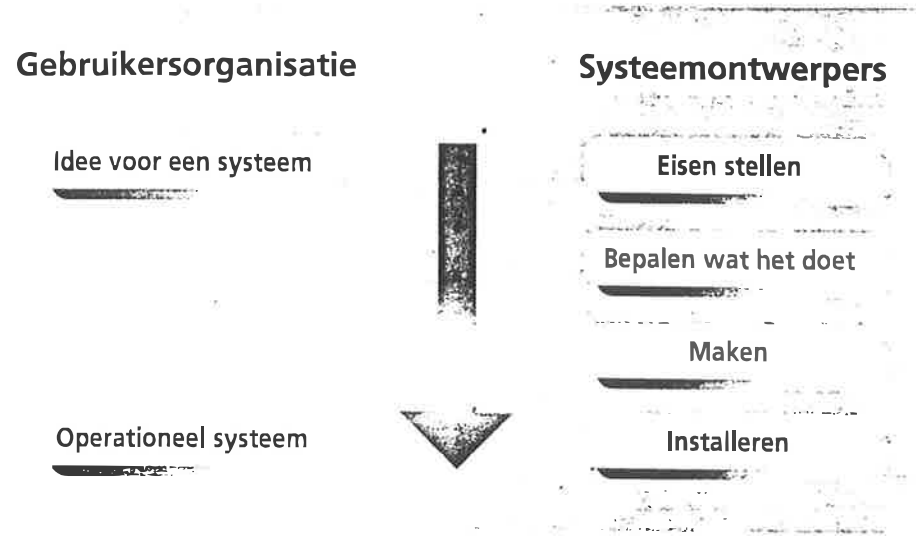
Uitgangspunten

Een ontwerpproces staat of valt met de gedefinieerde uitgangspunten, ofwel de systeemeisen. Identificatie van beveiligingseisen moet daarom in het begin van het ontwerpproces plaatsvinden. In figuur 2 is het definiëren van eisen in een ontwerpproces gepositioneerd.



Figuur 2. Aandachtspunten voor beveiliging in een ontwerpproces.

Om beveiligingseisen te kunnen definiëren is een aantal vragen van belang over het type omgeving, de belangrijkste functies en de risico's. De eisen voor beveiliging dienen te zorgen voor een balans tussen de risico's met betrekking tot de primaire functionaliteit, de doelen van de organisatie en de omgeving waarin het systeem gaat werken.
Een probleem hierbij is de vraag of de beveiligingsdoelen volledig zijn voor het systeem. Bestaande informatie (checklist) is daarom nodig om risico's en functionaliteit te bepalen. Om een goed beeld te krijgen is het aan te raden om een model van de risico's te maken. Vanuit beveiligingsperspectief is het belangrijk dat in dat model niet alleen staat wat het systeem moet doen (ook op beveiligingsgebied) maar ook wat het systeem niet moet doen. We noemen datgene wat het systeem niet mag doen de verboden-functionaliteit. Een voorbeeld is het verlenen van toegang aan een niet geïdentificeerde gebruiker.



Randvoorwaarden

Gedurende het bouwen van een systeem maken ontwerpers allerlei keuzen. Kan een beheerder auditrecords op afstand uitlezen of moet dit lokaal? Het zijn overigens niet altijd beveiligingsoverwegingen die de keuze bepalen. Maar door te definiëren wat een systeem niet mag, krijgen de ontwerpers een middel in handen waarmee zij tijdens het maken van het systeem kunnen analyseren of het ontwerp ten aanzien van de beveiliging nog steeds de goede richting op gaat.[4]
Op een gegeven moment in het ontwerpproces worden maatregelen bedacht om aan bepaalde beveiligingseisen te voldoen. Dit zijn technische maatregelen, die vaak alleen functioneren onder organisatorische randvoorwaarden. Toegangscontrole wordt bijvoorbeeld beïnvloed door mensen die van functie veranderen.
Ook documentatie is van belang. Het password is de meeste gebruikers wel bekend. Maar andere beveiligingsvoorzieningen, zoals een firewall, hebben vaak ook nog allerlei specifieke autorisatiemogelijkheden. De beheerder moet over goede documentatie beschikken om te kunnen bepalen hoe dergelijke beveiliging geregeld is.

Evaluatie

Aan het einde van een ontwerpproces wordt getest of het systeem doet wat in de eisen stond. Voor de beveiliging gebeurt dit ook. Daarbij moet dan wel zeker zijn dat de verbodenfunctionaliteit niet in het systeem aanwezig is. Bijvoorbeeld om te kunnen bewijzen dat documenten gewijzigd worden, bevat een zeker systeem beveiligingsfunctionaliteit om activiteiten in dat systeem te loggen. De logische test is om te kijken of wanneer iemand toegang krijgt tot een document dit in de log-file is terug te vinden. Maar er zijn meer soorten vragen die bij het testen van deze beveiligingsfunctionaliteit een rol spelen, zoals: 'als de log-file vol is, wat gebeurt er dan met de volgende activiteit die gelogd moet worden?', 'Is het mogelijk dat de log-file wordt verwijderd door willekeurige gebruikers?'; 'Is het mogelijk dat iemand gegevens uit de log-file haalt of wijzigt zonder dat dit ontdekt kan worden?'
Een rigoureuze aanpak om op dit soort vragen een antwoord te krijgen is een beveiligingsevaluatie. In zo'n evaluatie wordt naast normale testen en penetratietesten, geanalyseerd of het ontwerp en code op elkaar en op de eisen aansluiten, of het ontwerpproces van voldoende kwaliteit is ten aanzien van het configuratiemanagement, de gebruikte hulpmiddelen en technieken, life-cycle model en of de documentatie aansluit bij het product en er adequaat in beschreven staat hoe het product veilig moet worden gebruikt. ■

Dit artikel is geschreven naar aanleiding van het proefschrift Intrinsic Information Security: Embedding security issues in the design process of telematics systems door Olaf Tettero (Uitgegeven door het Telematica Instituut, Mei 2000, ISBN 90-75176-22-8, http://www.telin.nl/dscgi/ds.py/Get/File-8274). Met dank aan Dirk-Jan Out, Jeroen Schot, Marten van Sinderen en Eddie Michiels.