Als alle informatie telt : een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties

Hafkamp, W.H.M.

Publication date
2008

8. Suggesties voor verder onderzoek

Het onderzoek naar kwetsbaarheden- en incidentenresponseprocessen had als belangrijke vooronderstelling dat grotere organisaties met op ITIL-gebaseerde ICT-beheerprocessen onvoldoende responsevermogen hebben om snel en effectief om te gaan met de permanente stroom aan kwetsbaarheden- en incidenteninformatie.

De voorgestelde referentiemodellen kunnen worden beschouwd als een eerste stap naar een adequate inrichting van kwetsbaarheden- en incidentenresponseprocessen binnen grotere ICT-organisaties. Om de responsecapaciteit van ICT-organisaties te optimaliseren wordt aanbevolen om nader onderzoek uit te voeren naar het verder automatiseren van twee processen:

Geautomatiseerd filteren, analyseren en volgen van kwetsbaarhedenberichten
- Het filteren van niet relevante kwetsbaarheden vergt nog steeds veel handenarbeid. Leveranciers van informatiediensten bieden weliswaar de mogelijkheid om ICT-configuratiebestanden van klanten te koppelen met hun informatiedienst, desondanks blijkt dat er nog teveel niet relevante berichten worden doorgestuurd aan de ICT-systeem- en netwerkbeheerders. Nader onderzoek is gewenst naar filters die op basis van configuratiegegevens en historiegegevens kwetsbaarhedenberichten doorlaten of tegenhouden.
- De huidige op ITIL georiënteerde beheertools zijn niet ingesteld voor tracking en tracing van kwetsbaarheden. Dit betekent dat organisaties die deze tools gebruiken ter ondersteuning van de ICT-beheerprocessen trucs moeten uithalen om de levenscyclus van kwetsbaarheden in een systeem vast te leggen en te kunnen volgen. Een voorbeeld van een dergelijke truc is de kwetsbaarheid, als ware het een incident, te registreren in de incidentendatabase. Nader onderzoek is gewenst naar de optimale vastlegging van kwetsbaarhedenberichten in een sterk geautomatiseerde ICT-beheerprocesomgeving.

Herkenning van incidenten
In paragraaf 7.4 is aangegeven dat aan ICT-beveiliging gerelateerde incidenten moeilijk te herkennen zijn. ICT-incidenten worden vaak als eerste telefonisch gemeld bij een (centrale) helpdesk. In feite voert de helpdesk de eerste analyse uit van een incident namens de beheerorganisatie. De helpdeskmedewerker besluit of en welke vervolgstappen nodig zijn. Helpdesks werken vaak met checklijsten aan de hand waarvan de helpdeskmedewerker probeert een beeld te krijgen van het gemelde incident. Bij een aantal organisaties worden helpdeskmedewerkers ondersteund door kennismanagamentsystemen waarin vraag- en antwoordscripts en historiegegevens zijn opgeslagen ter ondersteuning van het afhandelingsproces. Nader onderzoek is nodig om deze kennismanagementsystemen verder te ontwikkelen voor het herkennen van aan ICT-beveiliging gerelateerde incidenten.

Normenkader
Verder onderzoek is nodig om binnen de context van het ITIL-raamwerk een model te ontwikkelen voor het gestructureerd analyseren van ICT-incidenten en – problemen en normen te ontwikkelen voor de beheersing van kwetsbaarheden en incidenten. Het model dient de ICT-beheerorganisatie in staat te stellen bronoorzaken bij incidenten vast te stellen en structurele vervolgmaatregelen binnen vastgestelde tijdseenheden te implementeren.

Outsourcing
Het is onduidelijk wat het effect is van uitbesteden van (delen van) de ICT-dienstverlening op het kwetsbaarheden- en incidentenresponsevermogen van organisaties. Uit nader onderzoek moet blijken of de uitbesteding resulteert in een (mogelijke) verbetering of verslechtering van de termijnen voor security patching en de afhandeling van incidenten.