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

Hafkamp, W.H.M.

Publication date
2008

Bijlage 1 Vragenlijsten

Tabel 18 bevat de vragenlijst die is gebruikt ter ondersteuning van het onderzoek bij de banken. De lijst bevat in totaal vier subblokken, A1 tot en met A4. Het blok start met een uitleg van relevante begrippen en een schematische weergave van de scope van een mogelijke samenwerking. Vervolgens wordt een toelichting gegeven op de binnen het onderzoek gehanteerde definities en gevraagd of binnen de organisatie soortgelijke definities worden gehanteerd.

Blok A1 omvat vijf vragen over bronnen van kwetsbaarheden en incidenten. Daarbij is onderscheid gemaakt tussen externe en interne bronnen en menselijke en niet-menselijke bronnen, bijvoorbeeld scanners en detectors. Bij vraag vijf wordt nadere uitleg gevraagd over de frequentie van gebruik/inzet en de analyse en opvolging van de berichten.

In de daarop volgende twee hoofdvragen in blok A2 wordt gevraagd naar de wijze waarop het incident- en change managementproces binnen de bank is georganiseerd. De methodiek van ICT-beheer, inclusief incidentenafhandeling, komen hierbij aan bod. Bij het onderdeel change management wordt dieper ingegaan op de doorlooptijd van wijzigingen en het gehanteerde security patchbeleid.

Blok A3 met drie vragen gaat over het verloop van het calamiteitenproces. Gevraagd wordt naar het verschil tussen een incident en een calamiteit, de aanwezigheid van een calamiteitenplan en –organisatie en een kwantificering en kwalificering van in 2002 voorgekomen beveiligingsincidenten en -calamiteiten.

Het laatste blok, A4, bevat een drietal vragen en gaat in zijn geheel over het fenomeen Computer Emergency Response Team.

Tabel 18: Vragenlijst gevalstudie ‘Banken’

Blok A1	1. Ontvangt de organisatie alarmberichten over (nieuw ontdekte) kwetsbaarheden of aanvalsprogrammatuur van externe bronnen? a) wat is de bron (persoon, bedrijf, systemen)? b) hoe worden de berichten ontvangen? c) wie in de organisatie ontvangt/ontvangen de berichten? d) met welke frequentie en op welke wijze?
	2. Ontvangt de organisatie alarmberichten over (nieuw ontdekte) kwetsbaarheden of aanvalsprogrammatuur van interne bronnen (personen)? a) wat is de bron (persoon, bedrijf, systemen)? b) hoe worden de berichten ontvangen? c) wie in de organisatie ontvangt/ontvangen de berichten? d) met welke frequentie en op welke wijze?
	3. Welke detectietechnieken en/of tools gebruikt de organisatie voor: a) virusscannen? b) scannen op aanwezige kwetsbaarheden? c) intrusion detection? d) penetratietesten? e) overige?

	4. Op welke wijze wordt deze techniek ingezet: a) via een derde partij? b) via de eigen IT-afdeling? c) overige?
	5. Wat is de frequentie van inzet, hoe worden berichten ontvangen en wie is verantwoordelijk voor het analyseren en opvolgen van de resultaten/output voor de genoemde technieken?
Blok A2	1. Hoe verloopt een incident/problemproces (welke fasen worden onderkend)? a) welke ICT-beheerprocessen zijn in de eigen organisatie gedefinieerd en geïmplementeerd? b) wordt een methodologie[139] gevolgd? c) worden alle gemelde of geconstateerde beveiligingsincidenten behandeld conform het ICT-beheerproces?
	2. Hoe verloopt een change managementproces (welke fasen worden onderkend)?: a) wat is de gemiddelde doorlooptijd van een change op het systeem? b) wat is de gemiddelde doorlooptijd van een urgent (spoedeisende) change op het systeem? c) welke functionaris/sen dient/dienen de (urgent) change in? d) welke functionaris/sen is/zijn betrokken bij de besluitvorming m.b.t. de change (en met welke zeggenschap)? e) indien van toepassing: hoe ziet het patch- en/of vulnerabilitybeleid eruit? f) hoeveel patches 'vanwege security' zijn er uitgevoerd de afgelopen 6 maanden?
	1. Hoe verloopt het calamiteitenproces? a) wanneer eindigt een incident en begint een calamiteit? b) welke fasen worden onderkend in het calamiteitenproces? c) is er een calamiteitenplan en calamiteitenorganisatie?
	2. Welke communicatiestromen bestaan er gedurende een calamiteit? a) welke personen/onderdelen zijn betrokken en in welke hoedanigheid? b) leidt het hebben van wetenschap van een aanwezige kwetsbaarheid binnen de organisatie tot een incidenten- c.q. een calamiteitenmelding? c) indien nee, wat gebeurt er met deze informatie?

[139] Bijvoorbeeld Information Technology Infrastructure Library (ITIL).

Blok A3	3. Hoeveel beveiligingsincidenten zijn er bij u in de organisatie in de periode 1 januari 2002 tot en met 31 december 2002 geweest (conform uw definitie)? a) hoeveel van deze incidenten kregen het predikaat 'calamiteit'? b) onder welke categorie viel het incident of de calamiteit?: 1) dienstontzegging; 2) ongeautoriseerde toegang; 3) ongeautoriseerde wijziging van bevoegdheden of (klant)informatie; 4) ongeautoriseerde verwijdering; 5) aanwezigheid van een voor ICT-beveiliging relevante kwetsbaarheid; 6) geef in termen van uren aan hoe lang de kortste, langste en de gemiddelde doorlooptijd van een calamiteit was; 7) wat zijn in generieke zin mogelijke verbeterpunten?
Blok A4	1. Indien van toepassing: waaruit bestaat het CERT-team (aantal, kwaliteit/hoedanigheid)? a) hoe is de bemensing gerealiseerd (7*24 uur)? b) hoe is het team gesitueerd binnen de organisatie? c) welke formele en informele relaties heeft de CERT?
	2. Is er een CERT-policy gedefinieerd en zo ja, hoe ziet deze eruit? a) hoe ziet het Operational Framework eruit? b) wat is de gemiddelde tijdsduur tussen de initiële melding van een incident en de 'constituency advisory' n.a.v. de melding? c) waaruit bestaat de constituency[140] van de CERT?
	3. Welke bron(nen) gebruikt de CERT? a) welke (soort) hulpmiddelen gebruikt de CERT voor de analyse van gemelde incidenten? b) welke (soort) functionarissen worden betrokken bij de analyse van gemelde incidenten
Blok B	Acht vragen met betrekking tot de mogelijke interbancaire samenwerking in een ISAC[141].
Blok C	Eén vraag met betrekking tot prioriteitsstelling bij invoering.
Blok D	Eén vraag met betrekking tot kosten/baten.

[140] Constituency = totale gebruikersgemeenschap, doelgroep.
[141] ISAC staat voor Information Sharing and Analysis Center.

Tijdens het onderzoek bij de computer security incident responseteams van SURFnet, Radboud Universiteit en Rijksuniversiteit Groningen is gebruik gemaakt van de eenendertig vragen uit tabel 19. De vragen zijn verdeeld over zeven categorieën.

Tabel 19: vragenlijst gevalstudie 'Computer Emergency Response Teams'

Historie	1. Wat was de datum van oprichting?
	2. Wat was de ontstaansreden?
	3. Wat was de doelstelling bij oprichting?
	4. Wat was de doelgroep?
Activiteiten	1. Wat zijn de hoofdtaken?
	2. Wat zijn de neventaken?
	3. Geef een incidentoverzicht vanaf 1-1-2000: a) aantal; b) type / aard; c) ernst; d) opvolgingsinspanning.
Organisatie	1. Wat is de relatie met de ICT-organisatie?
	2. Wat is de relatie met de helpdesk/overige specialisten?
	3. Hoeveel medewerkers heeft het CERT?
	4. Is er sprake van een parttime- of fulltimetaak?
	5. Type medewerker (opleiding/ervaring)?
	6. Wordt een consignatierooster gehanteerd?
Procedures	1. Hoe ziet het Operational Framework eruit?
	2. Hoe kunnen incidenten worden aangemeld?
	3. Geef een beschrijving van de coördinatie en vastlegging van incidenten.
	4. Geef een beschrijving van de afhandeling en terugkoppeling van incidenten.
	5. Welke onderzoeksmethodieken gebruikt CERT?
	6. Worden oplossingen (bijvoorbeeld patches) zelf getest?
Hulpmiddelen	1. Welke hardware wordt gebruikt?
	2. Welke software wordt gebruikt?
	3. Welke (standaard)tools worden gebruikt?
	4. Worden eigen tools ontwikkeld?
Contacten intern	1. Wie is de constituency?
	2. Wat wordt gecommuniceerd?
	3. Welke communicatiemiddelen worden gebruikt?
	4. Waaruit bestaat de 'disclosure policy'?
Contacten extern	1. Onderhoudt de CERT (inter)nationale contacten?
	2. Zijn deze contacten formeel of persoonsgebonden?
	3. Is de CERT lid van FIRST en TERENA[142]?
	4. Zijn er formele contacten met: a) politie; b) jusitie; c) Internet serviceproviders; d) overige.

[142] TERENA = Trans-European Research and Education Networking Association.

Tabel 20 bevat een aantal vragen die zijn gebruikt ter ondersteuning van het onderzoek binnen het Korps Landelijke Politiediensten en de analyse van het kastje-incident bij een van de Nederlandse banken.

Tabel 20: vragenlijst gevalstudie 'Korps Landelijke Politiediensten'

KLPD	1. Geef een definitie van cybercrime.
	2. Op welke wijze en waar kan aangifte van cybercrime worden gedaan?
	3. Hoe wordt bij de aangifte het strafbare feit vastgesteld?
	4. Welke bewijsmateriaal is vereist bij cybercrime[143]?
	5. Welke overige eisen zijn van belang met betrekking tot de 'Chain-of-Evidence'?
	6. Hoe verloopt in grote lijnen het proces van digitaal en/of Internetrechercheren bij de Nederlandse politie?
Bank ABCD	1. Hoe en waar kwam de eerste melding binnen?
	2. Welke stappen zijn ondernomen door de IT afdeling, veiligheidszaken, overige afdelingen?
	3. Is er binnen veiligheidszaken een formeel incidentenafhandelingsproces?
	4. Is er een speciale taskforce ingericht?
	5. Hoe is het interne onderzoek op hoofdlijnen verlopen?
	6. Welk bewijsmateriaal is verzameld?
	7. Hoe is de 'chain-of-evidence'bewaakt?
	8. Wanneer (na hoeveel tijd) is aangifte gedaan bij politie en door wie?
	9. Waar is aangifte gedaan?
	10. Hoe heeft de politie dit opgepakt?

[143] Uitgaande van 'cybercrime in enge zin'.