

Proces voor afhandeling informatiebeveiligingsincident CSIRT (Nov. 2015)

Het Computer Security Incident Response Team van de KNAW (CSIRT-KNAW) registreert, coördineert en volgt de afhandeling van informatiebeveiligingsincidenten binnen de KNAW. Het CSIRT kan adviseren bij de oplossing van zo'n incident, maar lost zelf geen incidenten op. Het oplossen van een incident is een taak van de technisch beheerders in overleg en samenwerking met de functioneel verantwoordelijken.

Als een melding binnenkomt bij CSIRT-KNAW worden de volgende stappen doorlopen:

- 1) Identificatie
- 2) Indammen en vaststellen schade
- 3) Herstel activiteiten
- 4) Evaluatie en rapportage

Bij elke stap speelt communicatie met betrokkenen een belangrijke rol.

In de tabel is sprake van een CMT (Crisis Management Team). Het CMT zal de coördinatie overnemen bij een urgent incident met grote impact (crisis). Als een instituut geen CMT heeft dan worden de Contactpersoon Informatiebeveiliging en eventueel lokale technisch beheerders benaderd. Deze worden geacht waar nodig hun instituutsleding te betrekken (en zo een "ad hoc" CMT te vormen). Alles is afhankelijk van het type incident en waar het zich heeft voorgedaan. De procedure wordt jaarlijks met CSIRT-KNAW en betrokkenen (management, CIB, functioneel en technisch beheerders) geëvalueerd en zo nodig aangepast.

Uitwerking:

Stap	Inhoud activiteit	Betrokkene
0	Melding komt binnen via csirt@knaw.nl , 088-0034600 of anders. CSIRT-leden communiceren hooguit met de betrokkenen en zeker niet met de media.	CSIRT, betrokkenen
1	Identificatie	
1.1	Stel vast wat de melding inhoudt: welke mensen, infrastructuur, systemen en/of gegevens zijn getroffen of lopen gevaar.	CSIRT, melder,..
1.2	Bepaal ernst van de melding: urgentie en impact. Urgent: - Schade wordt snel groter als niet wordt ingegrepen. Grote impact: - Gevoelige (persoons)gegevens zijn getroffen - Grote groepen medewerkers/gebruikers zijn getroffen - Risico op publiciteit - Risico op grote financiële of wetenschappelijke schade Midden impact: - Geen persoonsgegevens getroffen - Een of enkele systemen functioneren niet, enkele gegevens bestanden, beperkte groep gebruikers - Beperkte schade Lage impact: - Spam, duidelijk herkenbare phishing, een enkele virusbesmetting, ..	CSIRT i.o.m. melder, eventueel functioneel beheerder systeem
1.3	Communiceer: Urgent en grote impact: - Met Information Security Officer (ISO) en Crisismanagementteam (CMT) instituut/bureau/I&A. Bij ontbreken crisismanagementteam: contact met CIB en technisch beheer - Als het persoonsgegevens betreft wordt de Functionaris gegevensbescherming betrokken i.v.m. eventuele melding bij	CSIRT, ISO, CMT, Technisch beheerders

Proces voor afhandeling informatiebeveiligingsincident CSIRT (Nov. 2015)

	cbp. Dit loopt verder via "procedure datalekken" Urgent en midden impact: - Met ISO en technische- en zo mogelijk functionele beheerders van getroffen instituut/afdeling Niet urgent en impact laag: - Met technische beheerders van getroffen instituut/afdeling	
2	Indammen en vaststellen schade	
2.1	Bepaal aan de hand van ernst en omvang van het incident of het crisis management team wordt ingeschakeld of dat dit incident op het niveau beheerders (functioneel/technisch) wordt afgehandeld. Urgent en grote impact: - Crisis Management Plan (Instituut/Bureau/I&A) treedt in werking Urgent en midden impact/Niet urgent en kleine impact: - Technisch beheerders betreffende instituut onderzoeken incident eventueel met ondersteuning CSIRT, ISO en centrale ict-specialisten	Crisis Management Team (CMT), technisch beheerders, functioneel beheerders, ISO
2.2	Technisch beheerders treffen maatregelen Urgent en grote impact: - Crisismanagementteam stuurt technisch oplosteam aan, eventueel advies/ondersteuning vanuit CSIRT Urgent en midden impact/Niet urgent en kleine impact: - Technisch beheer neemt maatregelen om impact te verminderen. (Bv: uit zetten services, afsluiten deel internetverkeer, afkoppelen werkstations..) en onderzoekt onderliggende oorzaken probleem: bv: kwetsbaarheden op systeem of applicatie niveau. Eventueel advies vanuit CSIRT	CMT, Technisch beheerders i.o.m. gebruikersorganisatie (functioneel beheer, proceseigenaar)
2.3	Overleg met juridische zaken en of communicatieafdeling Urgent en grote impact: - CMT volgt crisismanagementplan Urgent midden impact / niet urgent, lage impact: - Bij vermoeden misdrijf: Overleg met hoofd juridische zaken over juiste reactie en eventuele aangifte. Schakel eventueel forensisch digi-expert in voor veiligstellen bewijs; - Bij mogelijk publiciteitsgevoelige zaken overleg met communicatieafdeling	CMT, ISO, Juridische zaken, afdeling communicatie.
3	Herstel activiteiten	
3.1	In alle gevallen - Technisch beheer herstelt onderliggende problematiek (patches, bug-fixes, updates, toegangsrechten,.. en andere acties die de kwetsbaarheid verhelpen)	Technisch beheer
3.2	CMT of Technisch beheerders melden afhandeling incident bij CSIRT	Technisch beheer
4	Rapportage & Evaluatie	
4.1	Urgent en grote of midden impact - Bij persoonsgegevens: Informeren Functionaris Gegevensbescherming over oplossing problematiek, eventueel ondersteuning melding CBP - Melder informeren over oplossing incident - Lessons learned benoemen en vastleggen	CSIRT