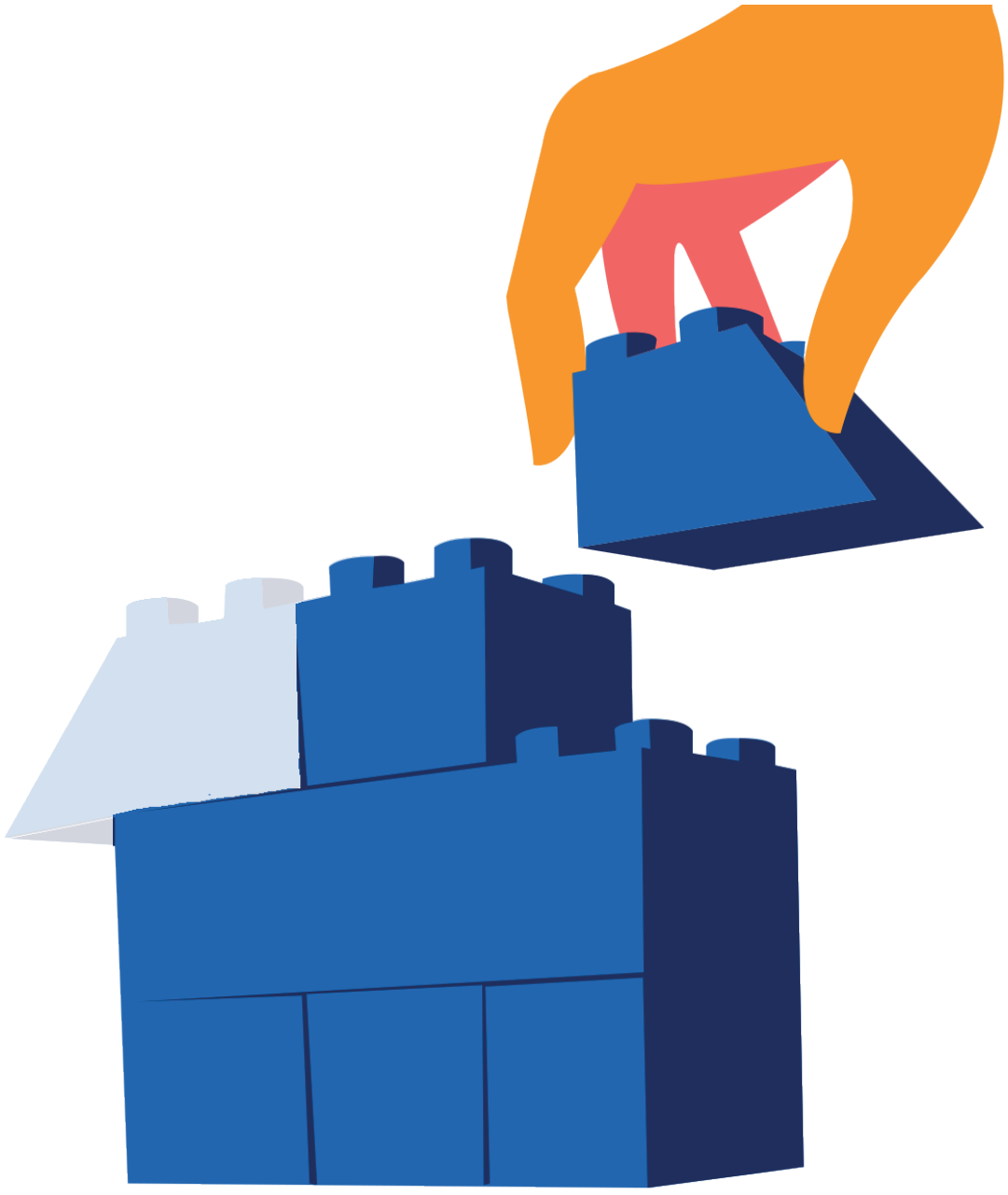
Audittrail
information security | privacy | quality | grc

BIC Building Blocks
Incidenten & Calamiteiten



INCIDENTEN & CALAMITEITEN

Als informatiebeveiliger voorkom je natuurlijk liever incidenten dan dat u ze moet oplossen en toch is er geen ontkomen aan. Want alle risicogerichte maatregelen ten spijt, vroeger of later zult u te maken krijgen met een informatiebeveiligingsincident of calamiteit. In deze whitepaper bespreken we de opzet van incidentmanagement en calamiteitenmanagement.

Incidenten/datalekken/calamiteiten

Informatiebeveiliging bestaat uit het borgen van drie pijlers: beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Een plotselinge of onverwachte verstoring van deze pijlers wordt een **informatiebeveiligingsincident** genoemd. Het gaat hierbij dus niet alleen om inbrekers of virussen op het netwerk, denk ook aan (stroom) storingen, het ontbreken van een backup of het verlies van documenten in de trein. Als bij dit soort incidenten persoonsgegevens betrokken zijn, is er (wellicht) sprake van een **datalek**. Wanneer de impact van het incident bijzonder groot is, spreken we ook wel van een **calamiteit**. Bij een calamiteit zijn processen zodanig verstoord dat het niet mogelijk is om werkzaamheden voort te zetten. Een veel genoemd voorbeeld is grote brand.

Voor al deze typen incidenten geldt dat het oplossen ervan veel werk met zich meebrengt en mogelijk zeer kostbaar is. Om snel te kunnen handelen bij verstoringen en om herhaling te voorkomen is het van belang om incidentmanagement goed in te richten.

INCIDENTMANAGEMENT

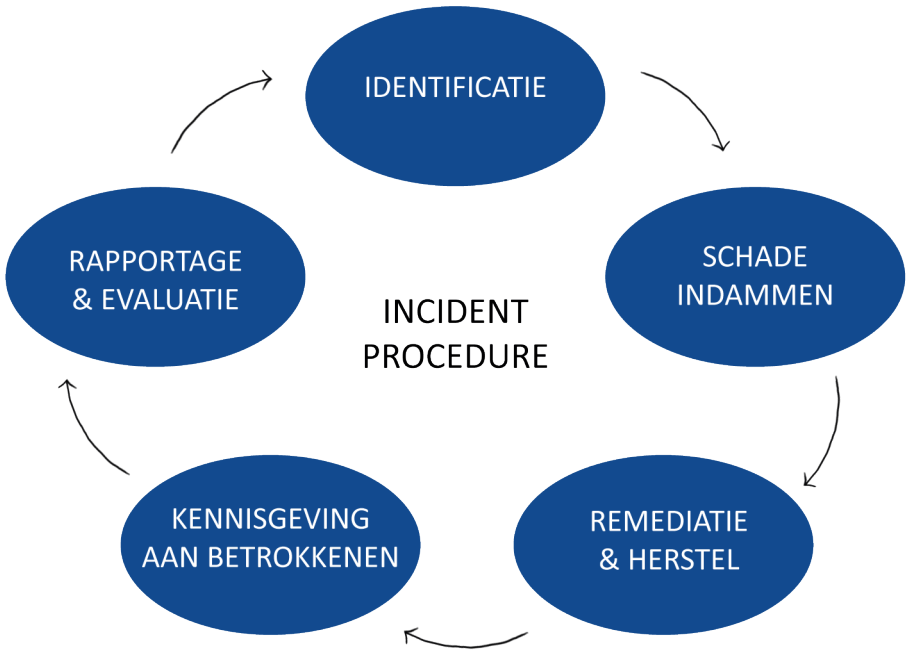
Incidentmanagement is meer dan alleen een datalekprocedure. Het richt zich niet alleen op het oplossen van incidenten, maar ook op het herkennen en oplossen van kwetsbaarheden en het lering trekken uit incidenten zodat ze niet nogmaals voorkomen. Naast reactieve maatregelen (een maatregel die gaat lopen op het moment dat het incident heeft plaatsgevonden), zoals een incidentprocedure, is het ook mogelijk (en wenselijk) om detectieve maatregelen (het herkennen van incidenten op het moment dat ze plaatsvinden) in te zetten binnen je incidentmanagement. Interne controle is hier een goed voorbeeld van.

Interne controle

Door een structurele controle van logging en andere aanpassingen in informatiesystemen zijn abnormale situaties sneller te herkennen. Denk bijvoorbeeld aan de trend in wachtwoordwijzigingen. Over het algemeen kennen organisaties twee pieken in het jaar waarop werknemers wachtwoorden veranderen: na de zomervakantie en na de kerstvakantie. Velen zijn er even uit geweest en zijn de wachtwoorden simpelweg vergeten. Is er opeens op een ander moment in het jaar een piek in wachtwoordherstelaanvragen? Dan zou dit een reden voor een onderzoek kunnen zijn. Is er opeens helemaal geen piek meer? Dan wordt het misschien tijd om de post-itjes onder de toetsenborden nog eens te controleren. Inzicht in logging kan zo helpen in het opsporen van informatiebeveiligingsincidenten. Voor alle incidenten die ontsnappen aan de logging is een incidentenprocedure van essentieel belang.

Incidentprocedure

Een incidentenproces bestaat uit een aantal vaste stappen, die ook goed zijn beschreven in de BIO, de baseline voor de Nederlandse overheid:



Audittrail
information security | privacy | quality | grc

INCIDENTMANAGEMENT

Identificatie

De procedure start met een incident. Zoals hierboven genoemd kunnen deze incidenten naar voren komen uit detectieve maatregelen. Voor overige incidentmelding bent u afhankelijk van de organisatie. Een hele organisatie ziet meer dan 1 informatiebeveiliger en daarom is het trainen van de mensen om u heen essentieel. Het start met een vraag waaraan vaak voorbij wordt gegaan: weten medewerkers een incident te herkennen? En als ze dan een incident herkennen, kunnen (en weten) ze deze ergens te melden? Bij het ontwikkelen van een incidentenprocedure, is dit misschien wel het onderdeel waar het meeste tijd in gaat zitten. Hoeveel medewerkers denken bij informatie die niet voor hen beschikbaar is: 'Och, dan probeer ik het later nog eens,' of: 'dat zie ik morgen wel.'

Zorg dat medewerkers een loket hebben om incidenten te melden en denk vooraf goed na over de informatie die nodig is om het incident te kunnen beoordelen. Start met een logboek op het moment dat het incident is gemeld. Dit gaat helpen bij het verdere onderzoek én bij de evaluatie achteraf.

Schade indammen

Na de melding is het van belang om schade zoveel mogelijk te beperken. Een incident kan eenmalig zijn (het verlies van informatie) of nog steeds gaande (cyberaanval). Om mogelijkheden voor forensisch onderzoek zo groot mogelijk te houden wordt aangeraden om devices niet compleet af te sluiten, maar bijvoorbeeld de netwerkverbinding te verbreken.

Remediatie en herstel

Is de eerste branden zijn geblust is het van belang om het incident te onderzoeken en na te denken over stappen voor het herstel van het incident. Wie zijn betrokken bij het onderzoek? Vaak is dit organisatieafhankelijk en ook nog eens incidentafhankelijk. Denk naast de usual suspects als ICT (zowel intern als extern) of Bedrijfsvoering ook eens aan het betrekken van communicatiespecialisten en directie/RvB.

Bij onderzoek en herstel zijn een aantal afwegingen essentieel om te maken: 1. Zijn er persoonsgegevens betrokken bij het incident en is er dus kans dat dit lek ook een datalek is? Mocht dit het geval zijn, dan is het zaak de privacy officer of FG te betrekken. Zij kunnen ervoor kiezen een voorlopige melding te doen bij de Autoriteit Persoonsgegevens. 2. Is er een externe partij nodig om het incident te onderzoeken? Wanneer een forensisch onderzoek gewenst is, dan zal de externe partij snel ingeschakeld moeten worden. Het is aan raden om al vooraf na te denken over derde partijen die zouden kunnen helpen bij uw incidentmanagementproces.

Kennisgeving aan betrokkenen

Mocht het incident een datalek betreffen, dan is de kans aanwezig dat het lek ook aan betrokkenen gemeld dient te worden. Maar ook zonder datalek is het aan te raden goed te communiceren over incidenten, niet alleen intern maar mogelijk ook naar externe stakeholders.

Rapportage en evaluatie

Als de bedrijfsvoering weer loopt en het incident is afgehandeld is het tijd voor evaluatie en rapportage. Dankzij het incidentenlogboek is het proces goed gedocumenteerd en kunnen eventuele lessons learned worden aangepast in de procedure. Bewaar alle informatie over het incident goed en loop periodiek alle incidenten na: zijn er patronen te ontdekken?

Rapportage is afhankelijk van de ontvanger. Bespreek verwachtingen met stakeholders bij de inrichting van incidentmanagement en stem rapportages hierop af.

Audittrail
information security | privacy | quality | grc

CALAMITEITENMANAGEMENT

Een incidentenproces is vaak niet voldoende om ook calamiteiten op te lossen. Bij een calamiteit is het zaak de bedrijfsvoering zo snel mogelijk te herstellen en kritische bedrijfsprocessen te beschermen. Toch wordt een bedrijfscontinuïteitsplan vaak als een 'moetje' gezien dat niet altijd up-to-date wordt gehouden. Toch biedt zo'n plan goede houvast, niet alleen intern maar ook in de regierol naar externe ICT leveranciers toe. Immers zijn de interne afspraken over uitval, uitwijk, en hersteltijd ook zaken die vastgelegd dienen te worden in SLA met deze leveranciers.

In de BIC staan goede punten genoemd om aandacht aan te besteden in het continuïteitsplan. Denk daarnaast ook eens aan de volgende punten:

- Waar staat het continuïteitsplan opgeslagen? Is het wel beschikbaar op het moment van een calamiteit?
- Hetzelfde geldt voor essentiële telefoonnummers. Zijn deze beschikbaar op het moment dat de telefooncentrale uitvalt?
- Zijn uitval- en hersteltijden besproken met alle stakeholders en is hier akkoord op? Tijdens een calamiteit zijn uiteenlopende verwachtingen niet gewenst.
- Is er nagedacht over communicatie op het moment van calamiteit? Laat de afdeling communicatie meedenken over de wijze waarop gecommuniceerd kan worden, zowel intern als extern.

Contactgegevens
Audittrail
Sisalbaan 5a
2352 AE Leiderdorp

KantNoord
Winschoterdiep 50
9723 AB Groningen

071 - 747 71 71
BBB@audittrail.nl

Audittrail
information security | privacy | quality | grc