Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Omgaan met insider threats

Good practices van Nederlandse organisaties

Publicatiedatum: 28 februari 2024

Toegestane verspreiding
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:CLEAR en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven op de website van het NCSC (https://www.ncsc.nl/onderwerpen/traffic-light-protocol)

Met TLP:CLEAR zijn er geen beperkingen om de informatie verder te delen.

Uw reacties zijn welkom op info@ncsc.nl

Inhoud

Introductie

Insiders kunnen een aanzienlijk cybersecurityrisico vormen voor uw organisatie. De impact van een insider threat kan verwoestend zijn. In tegenstelling tot cyberaanvallen van buitenaf, opereren insiders van binnenuit uw organisatie.

Een insider is een onzichtbare vijand die geautoriseerde toegang kan misbruiken om schade te veroorzaken. Hoe kunt u met deze onzichtbare vijand omgaan? We vroegen het aan de voorzitters en vicevoorzitters van de ISAC's waarbij het NCSC betrokken is. In deze publicatie delen we hun inzichten en good practices.

Het probleem van insider threats

Kwaadwillende insiders kunnen grote gevolgen hebben voor de digitale veiligheid van uw organisatie. Uit onderzoek van Ponemon blijkt dat incidenten met insiders geregeld voorkomen, het organisaties gemiddeld 77 dagen kost om een incident met een insider volledig onder controle te krijgen en de kosten daarbij aanzienlijk kunnen oplopen.[1]

Andere gevolgen van een incident met een kwaadwillende insider, zoals een breuk in onderling vertrouwen op de werkvloer, zijn moeilijk geldelijk uit te drukken maar raken ook uw organisatie.

Niet alle insiders zijn kwaadwillend

In deze publicatie richten we ons specifiek op kwaadwillende insiders, maar er bestaan ook andere categorieën van insider threats. Zo bestaat er ook de onbewuste insider. Dat is een persoon die, door onoplettend handelen, zijn organisatie onbewust blootstelt aan een cyberdreiging.

Een andere categorie van insiders zijn personen die bewust regels negeren. Ze kiezen er bewust voor om bepaalde beveiligingsrichtlijnen te negeren om, bijvoorbeeld, efficiënter te kunnen werken. Ze handelen daardoor onzorgvuldig, maar hebben niet direct kwade intenties tegenover de organisatie waarvoor ze werken.

Deze twee andere vormen van insiders behandelen we niet expliciet in deze publicatie, maar verdienen wel de aandacht bij een insider risicobeleid.

Een multidisciplinaire aanpak

Het vraagstuk omtrent insider threats raakt aan verschillende professionele disciplines, zoals fraudepreventie en organisatiepsychologie. In deze publicatie benaderen we insider threats vanuit een cybersecurityperspectief, toch is het raadzaam om in uw insider risicobeleid ook deze andere invalshoeken op insider threats mee te nemen. Een goede aanpak in het omgaan met insider threats is daarmee ook multidisciplinair.

Gehanteerde definities en methode

De definities in dit document over insider threats zijn overgenomen van het NCSC-UK.[2] Hierbij is een insider "elke persoon die geautoriseerde toegang heeft of eerder kennis heeft gehad van de middelen van de organisatie, inclusief mensen, processen, informatie, technologie en faciliteiten".

Insiders betreffen dus niet alleen de medewerkers van een organisatie, maar ook andere (tijdelijke) werknemers zoals personeel van partnerorganisaties, dienstverleners of leveranciers.

Een insider threat is "een persoon die de intentie heeft om schade aan een organisatie toe te brengen." We behandelen daarmee insider threats vanuit een intentioneel perspectief.

Toepassing van het NIST-raamwerk

Dit document is opgebouwd volgens het NIST-raamwerk.[3] In de afzonderlijke hoofdstukken behandelen we de functies uit het raamwerk en kijken daarmee naar preventieve en reactieve cybersecurity aspecten van het omgaan met insider threats.

Het vraagstuk omtrent insider threats, de bijbehorende definities en het NIST-raamwerk vormden de basis voor een workshop die het NCSC op 21 november 2023 heeft uitgevoerd met cybersecurityexperts van Nederlandse organisaties.

Het doel van deze sessie was om *good practices*[4] ten aanzien van insider threats te identificeren. Dit document is een resultaat van die sessie.

Doelgroep

Dit document is bedoeld voor CIO's, CISO's, BVA's en risicomanagers die zicht en grip willen krijgen op insider threats en betrokken zijn bij het opzetten van een insider risicobeleid.

Totstandkoming

Dit document is tot stand gekomen in een workshop met de voorzitters en vicevoorzitters van de ISAC's[5] waarbij het NCSC betrokken is.

In deze workshop zijn door de deelnemers good practices ten aanzien van omgaan met insider threats gedeeld. Ook de AIVD heeft deelgenomen aan deze sessie en heeft in de dialoog inzichten gedeeld over omgaan met insider threats. Het NCSC heeft de uitkomsten verrijkt en verwerkt in deze publicatie.

Dit is de tweede publicatie in een serie van documenten met good practices omtrent een cybersecuritythema. Eerder heeft het NCSC de publicatie "*Omgaan met risico's in de toeleveringsketen*" uitgebracht.[6]

Identify & Protect

Welke assets zijn een mogelijk doelwit van insider threats en hoe kunt u deze het beste beschermen? In dit hoofdstuk gaan we verder in op deze twee vragen.

Identify

Welke assets[7] lopen mogelijk risico ten aanzien van insider threats?

GP[8] 1.1: Identificeer kritieke processen

Om te bepalen waar insider threats u mogelijk het hardst kunnen treffen, moet u eerst zicht hebben op uw kritieke processen. Kritieke processen zijn de processen die essentieel zijn voor het functioneren van uw organisatie. Deze worden vaak ook omschreven als uw "kroonjuwelen".[9]

- Maak bij het identificeren van kritieke processen gebruik van BIV-classificaties. Deze vertellen wat over een mogelijke impact op de beschikbaarheid, integriteit en/of vertrouwelijkheid van het proces en de gevolgen daarvan voor uw organisatie en haar belanghebbenden.
- Het in kaart brengen van kritieke processen kan met bestaande tools zoals bijvoorbeeld een Business Impact Assessment (BIA)[10].

GP 1.2: Incidenten met insiders kunnen plaatsvinden op alle organisatielagen

Insider threats kunnen zich manifesteren op alle lagen van uw organisatie. Zo kunnen insiders actief zijn van het hoogste besluitvormingsorgaan van uw organisatie tot aan het meest uitvoerende niveau.

GP 1.3: Insider threats kunnen ook voortvloeien vanuit leveranciers of partnerorganisaties

Insider threats kunnen voortkomen uit het personeelsbestand van uw leveranciers of organisaties waar u mee samenwerkt.

Werknemers van leveranciers of partnerorganisaties kunnen bijvoorbeeld toegang hebben tot uw systemen of data doordat ze tijdelijk werkzaam zijn in uw organisatie.

Het is daarom raadzaam inzichtelijk te hebben met welke organisaties u zakendoet en welke insider risico's daaraan verbonden zijn.

- Bepaal welke organisaties toegang of invloed hebben op uw kritieke processen. De mate van toegang of invloed op uw kritieke processen is een belangrijk uitgangspunt in het prioriteren welke organisaties, zoals leveranciers, het meeste aandacht behoeven.

  Breng daarmee in kaart hoe leveranciers en partnerorganisaties omgaan met insider threats en welke maatregelen ze getroffen hebben om uw processen en data te beschermen.
- Wees ervan bewust dat leveranciers en partnerorganisaties hun eigen organisatiecultuur hebben die van invloed is op het risico van insider threats. Zorg ervoor dat u een gevoel heeft bij uw meest belangrijke leveranciers en partners, en maak eventuele zorgen bespreekbaar.
- Leveranciers of partnerorganisaties kunnen daarnaast beïnvloed of verplicht

worden door buitenlandse autoriteiten om mee te werken met een inlichtingenoperatie.

Dit risico neemt toe als een leverancier of partnerorganisatie banden heeft met een land dat een bevestigd offensief cyberprogramma heeft dat gericht is tegen de Nederlandse belangen, zoals China, Rusland, Iran of Noord-Korea.

Zorg ervoor dat u, als u zakendoet met een buitenlandse organisatie zoals een leverancier, goed op de hoogte bent van eventuele insider risico's die daaruit kunnen voorvloeien. Het Dreigingsbeeld Statelijke Actoren van de AIVD, MIVD en NCTV vormt daarvoor een goed startpunt.[11]

Protect

Hoe kunnen assets vooraf beschermd worden tegen insider threats?

GP 1.4: Stel vooraf criteria op voor het beoordelen van signalen

Voorkom vooroordelen en cognitieve bias[12] in het benaderen van insider threats. Door een duidelijk proces te hanteren, waarin aandacht is voor het reduceren van vooroordelen en bias, beperkt u subjectiviteit in de beoordeling van signalen.

- Dit kunt u doen door vooraf een transparant en breed gedragen insider risicobeleid op te zetten in uw organisatie.
- Door bewustwording te creëren bij uw werknemers en organisatie kunnen blinde vlekken of mogelijke risico's in een vroeg stadium geïdentificeerd worden. Het helpt om bewust om te gaan met mogelijke vooroordelen en cognitieve bias.[13]
- Zorg ervoor dat de procedure duidelijk is hoe afwijkend en verdacht gedrag kan worden gemeld. Alleen zo komen signalen van afwijkend gedrag op de juiste plaats in uw organisatie terecht.

GP 1.5: Neem soft controls mee in uw insider risicobeleid

Soft controls zijn niet-tastbare maar wel gedrag beïnvloedende factoren die invloed hebben op de cultuur en werkomstandigheden in een organisatie. Soft controls kunnen ook gebruikt worden in een insider risicobeleid.

- Een belangrijke factor die de kans op insider threats verkleint, is een open bedrijfscultuur waarin problemen herkend en besproken worden. Door een veilige werksfeer te creëren waar mensen elkaar kennen en met elkaar in contact staan zullen insiders zich minder snel laten verleiden om afwijkende of verkeerde handelingen uit te voeren.
- Leidinggevenden hebben hierin een belangrijke rol. Ze kunnen insider threat-problematiek bespreekbaar maken en tijdig aandacht geven aan afwijkend gedrag. Door dit professioneel te doen, en volgens objectieve en transparante richtlijnen, dragen ze bij aan een veilige werksfeer en gezonde bedrijfscultuur.
- Stel daarnaast een gedragscode[14] op: Wat verwacht u van uw werknemers? Hoe gaat iedereen met elkaar om? Bij wie klop je aan als je afwijkend gedrag ziet of als je je zorgen maakt over een collega? Dit zijn een aantal voorbeelden van vragen die kunnen worden opgenomen in een gedragscode.

  Bedenk hierbij ook wat u van werknemers verwacht wanneer ze bij u de dienst verlaten. Hoe verwacht u dat ze omgaan met de vertrouwelijke informatie waar ze toegang tot hebben gehad?

GP 1.6: Werk aan een goede netwerkarchitectuur

Een goede netwerkarchitectuur is belangrijk in de bescherming tegen meerdere dreigingen, waaronder ook insider threats. Alhoewel een insider al toegang heeft tot het netwerk kunt u door een goede netwerkarchitectuur nog steeds de impact van een insider threat beperken. Dit kunt u doen door:

- **De implementatie van "Ethical Walls".** Dit zijn maatregelen die ervoor zorgen dat gebruikers geen toegang tot data krijgen wanneer dit zou leiden tot een conflict of interest.
- **Het gebruik maken van data loss protection systemen.** Dit draagt eraan bij dat gevoelige data niet zomaar de systemen of het netwerk kan verlaten.
- **Het toepassen van zero trust-principes**. Hierdoor zorgt u ervoor dat uw organisatie weerbaarder wordt tegen aanvallen die van binnenuit uw organisatie worden uitgevoerd.[15]
- **Het toepassen van fysieke segmentatie**. Wie krijgt er bijvoorbeeld toegang tot de serverruimte? En hoe houdt u hier toezicht op?

GP 1.7: Niet iedereen heeft toegang nodig tot alle informatie

Medewerkers hebben vaak geen toegang nodig tot alle beschikbare informatie in een organisatie. Leg vast welke medewerkers tot welke informatie toegang nodig hebben. Denk hierbij in principes zoals *need to know*, *need to have*, en *least privilege*.

- Ook is het waardevol inzichtelijk te maken wat voor gedrag u verwacht per type gebruiker. Door vervolgens gebruikerslogs te monitoren kan afwijkend gedrag worden waargenomen.
- Het is belangrijk transparant te zijn over monitoring richting medewerkers en ze hierover geïnformeerd te houden.

GP 1.8: Ontwikkel een screeningsbeleid en wees daar transparant over

Door het screenen van personeel kunnen eventuele insider risico's inzichtelijk worden gemaakt. Een screening van (nieuwe) werknemers is anderzijds een zwaar middel om in te zetten. Maak een afweging of een screening een proportioneel middel is in het omgaan met insider threats en of een screening voor alle of specifieke functies benodigd is.

- Bepaalde eigenschappen van een werknemer kunnen bijdragen aan een verhoogd insider risico. Als een werknemer schulden heeft, of zeer negatief spreekt over uw organisatie, zijn dat risicofactoren.
- Zorg voor een goede juridische grondslag van uw screeningsbeleid, zeker ook wanneer u een externe organisatie de opdracht geeft een screening uit te voeren.
- Wees transparant over uw screeningsbeleid t.a.v. specifieke functies. Wees ervan bewust dat een screening ongewenst een drempel kan opwerpen om te solliciteren op een specifieke functie.
- Bepaal vooraf een *expectation of privacy* en bespreek dit met medewerkers. Hierin kan bijvoorbeeld staan welke informatie een werkgever kan inzien en wat er van werknemers wordt verwacht. Uw screeningsbeleid voor specifieke functies kan hier ook in worden opgenomen.
- Alleen vooraf een screening uitvoeren is soms niet voldoende. Door een screening periodiek uit te voeren blijft u zicht houden op medewerkers op vertrouwelijke functies.
- U hoeft een screening niet zelf uit te voeren. Er zijn organisaties gespecialiseerd in het ontwerpen en uitvoeren van een screeningsbeleid voor vertrouwelijke functies.

Detect

Hoe kunnen insider threats tijdig worden herkend? In dit hoofdstuk gaan we verder in op mogelijke detectiemaatregelen die u kunt treffen om malafide insiders te herkennen.

Een uitdagende kwestie

Het herkennen van insider threats is uitdagend. Een insider threat heeft raakvlakken met cyber of ICT-gerelateerde incidenten en fraude incidenten. Ook kunnen insider threats overal in de organisatie voorkomen en kunnen, zeker indien niet goed aangepakt, zorgen voor een organisatie brede crisissituatie.

Uit de gesprekken met de voorzitters en vicevoorzitters van de ISAC's blijkt dat in veel gevallen er wisselende afdelingen verantwoordelijk zijn voor het afhandelen van dit soort incidenten.

- In sommige gevallen draagt een afdeling risk en/of compliance de verantwoordelijkheid, waar in andere gevallen deze verantwoordelijkheid ligt bij een integriteits- of fraudecoördinator.
- Daarnaast komen meldingen, signalen en incidenten vaak niet bij elkaar terecht bij een centraal punt. Hierdoor ontbreekt organisatie breed overzicht en kunnen verbanden moeilijk worden gelegd.
- Dit onderstreept de noodzaak van een multidisciplinaire aanpak in uw insider risicobeleid, ook bij het detecteren van malafide insiders.

Detect

Hoe kunnen insider threats tijdig worden herkend in uw organisatie?

GP 2.1: Zorg voor een gedeelde norm

Om te kunnen bepalen welk gedrag afwijkend is, moet u ook een begrip van normaal gedrag hebben. Deze norm kunt u vervolgens gebruiken bij het toetsen op afwijkend gedrag.

- Wat voor uw organisatie normaal gedrag is, is afhankelijk van uw organisatiecultuur, de kernwaarden, de volwassenheid van uw organisatie en in welke mate de organisatie al gedwongen wordt om aan bepaalde regels, wetten en (normen)kaders te voldoen.
- Bepaal ook op welke aspecten van gedrag u een norm wilt bepalen. Voorkom dat u door uw normeringen ongewenst individuele vrijheden van uw medewerkers beperkt.

  Voorbeeld: Als een medewerker 's nachts plotseling grote hoeveelheden data op een USB-stick zet, is dat een indicatie van afwijkend gedrag dat een relatie kan hebben met een insider threat.

GP 2.2: Verlaag de drempel om melding te maken van een verdachte situatie

Zorg ervoor dat medewerkers eenvoudig een melding kunnen doen van een verdachte situatie. De drempel om een melding te doen van een verdachte situatie en dit bespreekbaar te maken kan hoog zijn.

- Zorg dat leidinggevenden weten hoe ze met een melding moeten omgaan en dit vertrouwelijk op te pakken.
- Zorg ervoor dat er een duidelijk loket is waar werknemers met hun melding terecht kunnen, ook als dit niet de leidinggevende is. Dit kan ook een algemeen loket zijn voor een "melding voorval".

- Koppel ook aan uw organisatie terug wat er met meldingen is gebeurd. U hoeft hierbij niet in detail te gaan, maar u laat wel zien serieus en vertrouwelijk om te gaan met gemaakte meldingen.

GP 2.3: Train uw medewerkers

Zorg ervoor dat uw medewerkers op de hoogte zijn van uw integriteitsbeleid, welke gedragsregels er zijn, wie de vertrouwenspersoon is, dat er een klokkenluidersregeling is en waar die te vinden is. Dit kan onderdeel uitmaken van een onboarding programma voor nieuwe medewerkers.

GP 2.3.1: Specifieke training voor medewerkers

- Laat medewerkers ervaren welke risico's omtrent insiders er bestaan op de werkvloer. En hoe ze vanuit hun functie kunnen bijdragen aan het herkennen van kwaadwillende insiders.
- Maak ook bekend welke sleutelfuncties extra gevoelig zijn voor een insider threat, denk hierbij aan functies met meer (beheer)autorisaties, hogere mandatering of bevoegdheden.
- Leer medewerkers hoe ze het beste kunnen reageren op een verdachte situatie en daar melding van kunnen maken.

GP 2.3.2: Specifieke training voor leidinggevenden

- Geef leidinggevenden de mogelijkheid om een training te volgen om mensen op de werkvloer aan te spreken op afwijkend gedrag.

  Door een goede band met hun team hebben leidinggevenden een belangrijke rol in het voorkomen en tijdig herkennen van insider threats. Maak ook duidelijk wat u hierin van leidinggevenden verwacht.

- Weet hoe er binnen de organisatie wordt omgegaan met meldingen, onderzoeken en de consequenties voor de betrokkene die het onderwerp van een onderzoek is. Oefen dit ook met elkaar periodiek, zowel op procesniveau als de vaardigheden die nodig zijn om met een melding om te gaan.

GP 2.4: Breng gevoelige momenten in kaart

Bepaalde gebeurtenissen kunnen invloed hebben op de manifestatie van een insider threat.

- **Onrustige periodes:** Zo kan het voorkomen dat een malafide insider ervoor kiest misbruik te maken van een onrustige periode in een organisatie in de veronderstelling dat er dan verminderd toezicht is. Denk hierbij aan vakanties, feestdagen of transitieperiodes en personeelswisselingen.
- **Triggering events:** Ook kunnen gebeurtenissen aanleiding vormen voor een insider om over te gaan op malafide acties. Denk hierbij aan een aangekondigde reorganisatie, een naderend einde van een (arbeids)contract of een lopende ontslagprocedure.

GP 2.5: Maak detectie mogelijk

Afwijkend gedrag kan ook door technische maatregelen gedetecteerd worden.[16] Denk hierbij aan het herkennen van afwijkend gedrag op systemen, onverklaarbare datastromen of eigenaardige autorisaties voor medewerkers.

- Om dit te kunnen doen, zijn goede logging en afdoende bewaartermijnen noodzakelijk. Deze logs kunnen worden gebruik om afwijkingen in gedrag te detecteren en, bij een eventueel incident, te herleiden wat de oorzaak van het incident is.

- Ook logging kan onderhevig zijn aan maximale bewaartermijnen. Houd hier rekening mee.
- Detectie kan op meerdere punten in een netwerk plaatsvinden. Door mogelijke aanvalspaden van een kwaadwillende insider uit te werken kunnen verschillende punten in een netwerk geïdentificeerd worden voor detectie. Bepaal per punt op welke indicatoren kan worden gedetecteerd.

GP 2.6: Deel uw ervaringen en inzichten met partnerorganisaties

Het is waardevol van andere organisaties te leren over insider threats en hoe daarmee om te gaan. Vanwege de gevoeligheid omtrent het thema blijft veel informatie binnenskamers, ook vanwege angst voor reputatieschade en gezichtsverlies. Toch kan het delen van ervaringen u helpen om effectiever om te gaan met insider threats.

- De belangrijkste vereiste om kennis onderling te delen is vertrouwen. Zorg dat mensen elkaar kennen en weten te vinden. Een ISAC is een voorbeeld van een gremium waar mensen elkaar treffen en een vertrouwensband kan ontstaan, waardoor vervolgens kennis en ervaringen vertrouwelijk kunnen worden gedeeld.[17]
- Volg bij het uitwisselen van ervaringen een vaste structuur. Bespreek bijvoorbeeld modus operandi: Hoe is de insider te werk gegaan? Hoe is het incident aan het licht gekomen? En hoe is er gereageerd op het incident? Deze informatie kan anderen helpen in het omgaan met insider threats.

GP 2.7: Werk samen en spreek verwachtingen uit

U staat niet alleen in het herkennen van insider threats.[18] Verschillende afdelingen en/of organisaties in uw keten kunnen bijdragen in het herkennen van malafide insiders.

- Zo kan een onderzoek van een accountant of een IT-auditor ook leiden tot het herkennen van afwijkend gedrag van een medewerker.
- Ook toezichthouders, kennisautoriteiten en opsporingsinstanties kunnen kennis en expertise delen over insider threats. Zo kunnen waargenomen trends in een sector leiden tot concrete detectiemaatregelen in een organisatie.

Respond & Recover

"Het is niet de vraag of, maar wanneer u te maken krijgt met een insider threat."[19] In dit hoofdstuk gaan we in op hoe u kunt reageren op een incident met een insider threat en hoe u vervolgens van de gevolgen kan herstellen.

Respond

Hoe kan u reageren op een incident met een malafide insider?

"Het gaat om mensen. De insider is de boef, maar ook de collega"[20]

GP 3.1: Omgaan met insider threats is mensenwerk

Een incident met een insider threat heeft impact op de werkvloer. Naast dat een incident met een insider threat overeenkomsten heeft met algemene aspecten van cybersecurity incidenten, spelen sociale elementen hierin een belangrijke rol. Immers, u of uw collega's hebben te maken gehad met een vertrouwensbreuk: Een collega of bekende blijkt mogelijk een malafide insider zijn. Dat heeft invloed op het onderlinge vertrouwen en werkplezier op de werkvloer.

- Wees ervan bewust dat deze sociale aspecten van belang zijn in uw reactie op het incident. Emoties als verdriet, boosheid of medelijden – afhankelijk van de motivatie en het type incident – kunnen al gauw de boventoon voeren. Ga daar gepast mee om.
- Tegelijkertijd is snelheid geboden in uw reactie op een malafide insider, hoe langer het duurt om te reageren des te groter de schade.[21]
- Realiseer dat beide aspecten uw besluitvorming kunnen beïnvloeden. Geef daarom ruimte aan die emotie en houd er rekening mee dat ook de ervaren urgentie en tijdsdruk uw besluitvorming kunnen beïnvloeden. Dit kunt u doen door vooraf ontwikkelde plannen en protocollen te gebruiken in uw reactie.

GP 3.2: Laat u bijstaan in uw reactie door een externe partner

Er bestaan organisaties die zich specialiseren in insider threat-problematiek en forensisch onderzoek naar een mogelijk misdrijf.

Deze organisaties kunnen u adviseren en ondersteunen in de reactie op een insider. Zeker als uw organisatie niet beschikt over de expertise om goed te reageren op een insider kan het inzetten van een externe partner wenselijk zijn.

Deze externe partner kan mogelijk toegang krijgen tot vertrouwelijke informatie. Zorg er daarom voor dat u een goede juridische grondslag heeft voordat u een externe partner betrekt bij een incident. Laat u tijdig juridisch informeren en neem deze juridische implicaties vooraf al mee in uw insider risicobeleid.

GP 3.3: Handel voortvarend en in afstemming met belanghebben

Het reageren op incidenten met insiders is complex en uitdagend. Voor een adequate reactie is betrokkenheid van diverse belanghebbenden nodig. Denk bijvoorbeeld aan HR, uw juridische afdeling en de directie. Afstemming en een goede samenwerking

tussen deze belanghebbenden is nodig om gebalanceerd en effectief op te treden.

- Bereid vooraf een incidentprocedure voor waarop u kunt terugvallen bij een incident. Neem hier ook escalatiemogelijkheden in mee. Bespreek ook de mogelijkheid tot het formeren van een incidentteam.
- Haastig reageren op een insider threat, zonder directe belanghebbenden te informeren, is risicovol. Betrek, indien mogelijk, de belangrijkste belanghebbenden in uw reactie.

  U kunt tijd winnen door tijdelijke maatregelen te nemen die minder ingrijpend zijn, maar wel risico's mitigeren. Denk bijvoorbeeld aan het tijdelijk bevriezen en isoleren van een gebruikersaccount.
- Er kunnen diverse oorzaken achter een incident met een insider liggen. Een medewerker die uit wrok samenspant met een criminele actor vergt een ander type reactie als een leverancier die onder de druk van chantage toegang heeft gegeven tot uw systemen. Dit heeft invloed op hoe u moet reageren.
- In uw besluitvorming kunt u gebruik maken van het BOB-model (beeldvorming, oordeelvorming, besluitvorming). Hierdoor voorkomt u overhaaste beslissingen en krijgt u er een scherper beeld bij welke partijen betrokken moeten worden om te komen tot een gepaste reactie.

GP 3.4: Stem uw handelen af op beschikbare informatie

"Het op orde hebben van processen helpt bij het reageren op een malafide insider. Zo voorkomen we dat emoties de overhand nemen en een gepaste reactie in de weg zitten."[20]

Op het moment dat actie op de insider threat vereist is, is er doorgaans nog niet een volledig beeld van de omvang en toedracht van een incident. Emoties en de wens om de dreiging snel in de kiem te smoren, kunnen de overhand nemen in een reactie.

- Maak een onderscheid tussen feiten en aannames in uw analyse. Neem actie op basis van de voor u beschikbare feiten en wees terughoudend in het handelen op aannames.
- *Playbooks* en responsplannen kunnen u helpen in het gepast reageren op een insider threat. Deze helpen u om de aandacht te leggen op het uitvoeren van het proces, in plaats van te handelen op emotie.

GP 3.5: Reageer gepast op een insider threat

GP 3.5.1: De reactie binnen uw organisatie

Een goede reactie binnen uw organisatie op een malafide insider vereist doorgaans een multidisciplinaire aanpak. Hierin houdt u rekening met ook juridische, technische of beleidsmatige aspecten die een rol spelen bij een incident met een insider. Overweeg in uw reactie de volgende maatregelen:

- **Isoleer de insider**. Isoleren kan door bijvoorbeeld de gebruikersaccounts van de insider te bevriezen dan wel te blokkeren, zodat de insider geen toegang meer heeft tot uw systemen en data.
- **Onderzoek de insider.** Soms is het nodig om meer informatie te verzamelen over de toedracht, motivatie en de reikwijdte van een mogelijk incident met de insider. Denk hierbij aan het verzamelen van bewijsmateriaal met behulp van monitoring en logging.
- **Confronteer de insider**. Dit vraagt om ervaren en getrainde medewerkers die deze confrontatie in goede banen kunnen leiden. Zorg altijd voor hoor en wederhoor. En houdt gedurende het

gehele proces subsidiariteit en proportionaliteit in het oog bij uw reactie.

- **Communiceer richting uw organisatie over het incident.**[22] Tegen de tijd dat reactie op de insider threat vereist is, ligt het voor de hand dat er al verhalen over de insider de ronde doen. Met oog voor de omstandigheden en de beschikbare informatie kan het communiceren richting de eigen medewerkers nodig zijn. Let er hierbij wel op dat louter intern communiceren niet bestaat. Interne is doorgaans ook externe communicatie (zie ook GP3.5). Denk daarom ook in deze fase al na of er richting klanten, (toe)leveranciers en andere belanghebbenden moet worden gecommuniceerd.

GP 3.5.2: Maak melding van het incident

- **Maak melding van het incident**. Melden kan bij de daartoe bevoegde instanties. Vitale aanbieders en aanbieders van essentiële diensten hebben een meldplicht voor ernstige digitale veiligheidsincidenten bij het NCSC.[23]

  Doe aangifte bij de politie in het geval van verdenking op strafbare feiten.[24] Doe melding bij de Autoriteit Persoonsgegevens in het geval van een datalek waarbij gevoelige gegevens gelekt zijn.[25] Bij vermoedens van betrokkenheid van statelijke actoren kan contact worden opgenomen met de AIVD.[26]

  Door uw melding of aangifte kan verdere schade door een incident worden voorkomen. U draagt daarmee bij aan een digitaal veilig Nederland.

- **Overweeg juridische stappen**. Het kan nodig zijn om over te gaan tot juridische stappen. Een aangifte kan leiden tot strafrechtelijk onderzoek, maar daarnaast kunnen ook civielrechtelijke, bestuursrechtelijke, of tuchtrechtelijke stappen een optie zijn. In sommige gevallen kan ook een integriteitscommissie een uitkomst bieden. Ook hier geldt dat dit afhangt van de ernst en oorzaak van de insider threat.

Recover

Hoe kan uw organisatie herstellen en leren van een incident met een malafide insider?

GP 3.6: Herstel van de kwetsbaarheid

Herstel van de gecompromitteerde systemen en data is de eerste prioriteit nadat de insider threat is afgewend. Daarnaast moet duidelijk worden welke oorzaken ten grondslag lagen aan de insider threat.

- Ga na hoe het incident heeft kunnen plaatsvinden. Waren er maatregelen die niet hebben gewerkt? Of heeft u belangrijke informatie gemist waardoor de insider niet tijdig is waargenomen? Door het uitvoeren van een goede evaluatie kunt u herstellen en leren van een incident.
- Wees beducht op een overreactie op een incident. Een incident met een insider kan een grote indruk achterlaten. Sommige risico's zijn echter moeilijk weg te nemen of, in het geval van zeer ingrijpende maatregelen, is het middel erger dan de kwaal.

GP 3.7: Communiceer over een incident

Een incident met een insider kan zorgen voor reputatieschade voor uw organisatie. Door open te communiceren over een incident en uw reactie daarop behoudt u vertrouwen van uw klanten, (toe)leveranciers en andere belanghebbenden.

- Een belangrijke voorwaarde voor open communicatie is dat vooraf wordt nagedacht over de doelgroepen die moeten worden benaderd, waarbij wettelijke verplichtingen, belangen,

informatiebehoeftes en reputatierisico's centraal staan. Dit kunt u doen in een crisiscommunicatieplan.

GP 3.8: Heb oog voor het rouwproces

"*Als crisisteam loop je vaak twee fasen van rouwen voor. Jij kunt de insider al de rotzak vinden, terwijl de medewerkers nog in ontkenning zitten. Zorg daarom voor een goede debrief en biedt ruimte en nazorg.*"[20]

Cyberincidenten hebben naast technische en financiële schade ook een grote impact op medewerkers.[27] Incidenten met insiders voegen daar nog een extra dimensie aan toe: de dader is immers voor sommigen een bekende. Iemand waar mee is samengewerkt, waar vertrouwen in is gesteld en waar misschien wel lief en leed mee is gedeeld.

- Er moet om die reden ruimte zijn voor een rouwproces. Het is goed dit te realiseren, temeer omdat dat de betrokkenen in het crisis- of responsteam wellicht al in een andere fase van rouwen zijn beland als de medewerkers daarbuiten.[28]

GP 3.9: Evalueer en leer

Een belangrijk component van herstellen van incidenten met insiders is het vergroten van de weerbaarheid. Incidenten zijn immers het moment waarop in de praktijk getoetst wordt hoe goed uw voorbereidingen zijn geweest. Welke procedures hebben gewerkt en waar bestaat nog ruimte voor verbetering?

- Hiervoor is het nodig om tijdens het incident nauwkeurig te documenteren welke stappen zijn ondernomen. Identificeer naderhand leerpunten die betrekking hebben op de gehele keten van bescherming, detectie, reactie tot herstel.
- Deze input kunt u gebruiken om uw respons en herstelplannen te verbeteren. Bovendien kunnen deze inzichten ervoor zorgen dat u in de toekomst malafide insiders beter kunt identificeren en detecteren.
- Overweeg een hot debrief uit te voeren met uw crisisteam direct nadat het incident onder controle is. Hierin kunt u de eerste geleerde lessen bij uw crisisteam ophalen en ook ruimte geven aan eventuele emoties en frustraties.

GP 3.9.1: Maak gebruik van crisisoefeningen en simulaties

Evalueren en leren kan ook na het doorlopen van een tabletop oefening. Door een scenario met een incident door een kwaadwillende insider te doorlopen krijgt u inzichtelijk of uw organisatie met dit type incident om kan gaan.

- In een tabletop oefening kunt u in relatieve rust procedures en crisisplannen doorlopen. Dit geeft u ook de mogelijkheid eventuele verantwoordelijkheden en verwachtingen tussen afdelingen en medewerkers te bespreken.
- Bespreek in een tabletop ook uw communicatieplan bij een incident met een malafide insider. Bespreek daarin het type boodschap dat u bij zo'n incident wilt afgeven en via welke kanalen u dit beoogt te doen.

Govern

Hoe zorgt u ervoor dat uw insider risicobeleid goed aansluit bij uw organisatiedoelstellingen en besluitvorming? In dit hoofdstuk gaan we verder in op bestuurlijke aspecten die belangrijk zijn mee te nemen in uw insider risicobeleid.

Govern

Hoe zorgt u ervoor dat uw insider risicobeleid goed aansluit bij uw organisatiedoelstellingen en besluitvorming?[29]

GP 4.1: Laat u juridisch adviseren

Een aanpak ten aanzien van insider threats kan juridische implicaties hebben. Zorg voor het overgaan op maatregelen dat deze in overeenstemming zijn met geldende wet- en regelgeving.

Het invulling geven aan een screeningsbeleid, zoals omschreven onder GP 1.8, kan bijvoorbeeld juridische vragen oproepen. Zorg dat u vooraf duidelijk inzichtelijk heeft of maatregelen juridisch haalbaar zijn.

GP 4.2: Zorg voor toezicht op uw insider risicobeleid

Een insider risicobeleid kan gevolgen hebben voor de privacy van uw medewerkers. Het is daarom ook belangrijk dat er onafhankelijk toezicht wordt gehouden op dit insider risicobeleid.

Voor medewerkers is het belangrijk om te weten dat er zorgvuldig met vertrouwelijke gegevens wordt omgegaan, en dat er niet meer gegevens worden vergaard dan noodzakelijk.

Een onafhankelijke commissie, waarin vertegenwoordigers van verschillende belangengroepen uit uw organisatie kunnen deelnemen, kan toezien op de uitvoering van een insider risicobeleid en of dit aansluit bij uw ethisch kader.

Meer lezen?

De fraudedriehoek

In het omgaan met insider threats kan ook geleerd worden van aangrenzende vakgebieden zoals accountancy en fraudepreventie. Een van de daar gebruikte concepten is de fraudedriehoek, waarin drie factoren staan die nodig zijn om fraude te kunnen plegen.

"Frauderisicobeheersing: Aanbevelingen voor bestuurders en toezichthouders", Koninklijke NBA, 2022

NCSC-UK: Reducing data exfiltration by malicious insiders

Ook het NCSC-UK besteed uitgebreid aandacht aan het omgaan met insider threats. Op hun website staan adviezen en aanbevelingen om het risico van data exfiltratie door insider threats te verkleinen.

"Reducing data exfiltration by malicious insiders", NCSC-UK, 30 juni 2022

Het MICE-model

MICE is een afkorting voor de indicatoren *Money*, *Ideology*, *Coercion* en *Ego*. Het MICE-model kan organisaties helpen bij het nadenken over maatregelen en manieren hoe insider threats tijdig gedetecteerd en voorkomen kunnen worden.

Charney, David L., and John A. Irvin. "The psychology of espionage." Intelligencer: Journal of US Intelligence Studies 22 (2016): 71-77.

NPSA: Reducing Insider Risk

De Britse *National Protective Security Authority* heeft een toolbox uitgebracht over hoe om te gaan met Insider Risks. Deze toolbox bevat naast adviezen over hoe om te gaan met insider threats, ook inzichten over hoe hierover te communiceren en dit te trainen in een organisatie.

"Reducing Insider Risks", National Protective Security Authority, 2023

CISA: Insider Threat Mitigation

Ook het Amerikaanse CISA heeft een uitgebreide handleiding gepubliceerd over hoe om te gaan met insider threats. Deze handleiding bevat daarnaast ook meerdere aanvullende uitreikstukken met aanbevelingen en adviezen op dit thema.

"Insider Threat Mitigation", CISA, 2023

The Critical Pathway to Insider Risk Model

In dit artikel van Mark Lenzenweger en Eric Shaw gaan ze verder in op het CPIR-model. Dit is een model dat ingaat op gedragsfactoren die helpen bij het tijdig inzichtelijk krijgen van insider risico's. Dit artikel bespreekt voornamelijk de gedragsdimensie bij insider problematiek.

Lenzenweger, M. F., & Shaw, E. D. "The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions", Counter-Insider Threat Research and Practice, 2022

Integriteit in de praktijk

In dit document gaat het Huis voor Klokkenluiders in op hoe een organisatie intern onderzoek kan doen naar een vermoedelijke misstand

"Integriteit in de praktijk", Huis voor Klokkenluiders, 01 april 2020

Referenties

[1] https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/

[2] https://www.ncsc.gov.uk/guidance/reducing-data-exfiltration-by-malicious-insiders

[3] https://www.nist.gov/cyberframework

[4] Good practices in dit document zijn werkwijzen, gebruiken en methodes die vanuit praktijkervaring effectief blijken in het benaderen van een vraagstuk.

[5] ISAC staat voor Information Sharing and Analysis Centre (ISAC). Dit is een overlegvorm over cybersecurity waarin organisaties uit dezelfde sector gevoelige en vertrouwelijke informatie uitwisselen over incidenten, dreigingen, kwetsbaarheden en maatregelen.

[6] "Omgaan met risico's in de toeleveringsketen; Good practices van Nederlandse organisaties", NCSC, 15 augustus 2023

[7] Assets zijn, in cybersecurity-termen, informatie of digitale systemen die van waarde zijn voor een organisatie. Voorbeelden zijn: intellectueel eigendom, een klantendatabase, personeelsinformatie en dergelijke

[8] In dit document duiden de we verschillende door de deelnemers geïdentificeerde *good practices* aan met "GP".

[9] Kroonjuwelen zijn informatie en informatiesystemen die het allerbelangrijkst zijn voor een organisatie. Het heeft grote gevolgen voor de organisatie als men niet meer bij deze informatie kan komen wanneer men dat wil. Of als de informatie niet meer klopt, of als die ongewild bij anderen terechtkomt.

[10] https://csrc.nist.gov/pubs/ir/8286/d/final

[11] https://www.rijksoverheid.nl/documenten/rapporten/2022/11/28/tk-bijlage-dreigingsbeeld-statelijke-actoren-2

[12] Cognitieve bias zijn denkfouten die voortkomen uit de manier waarop mensen informatie verwerken en interpreteren. Deze denkfouten kunnen verschillende oorzaken hebben die daaraan ten grondslag liggen.

Voor meer informatie over cognitieve bias, zie:

"Psychology of intelligence analysis", Richards J. Heuer, Jr., 1999

[13] "Strategies for Addressing Bias in Insider Threat Programs", Intelligence and National Security Committee, 2022

[14] Ook de Rijksoverheid heeft een gedragscode. Hierin staan ook passages over het zorgvuldig omgaan met vertrouwelijke informatie en het tegengaan van datalekken.

https://www.rijksoverheid.nl/documenten/richtlijnen/2017/12/01/gedragscode-integriteit-rijk-gir

[15] "Bereid u voor op zero trust", NCSC, 18 augustus 2021

[16] https://insights.sei.cmu.edu/documents/1260/2016_005_001_454627.pdf

[17] "Samenwerking in een ISAC", NCSC, bezocht op 23 juni 2023

[18] https://www.pwc.nl/nl/spotlight/assets/documents/pwc-spotlight-uitgave-2021-4.pdf

[19] Zie voor een overzicht van omvangrijke insider threat incidenten deze blog: https://www.mandiant.com/resources/blog/insider-threat-impact-studies

[20] Uitspraak van een deelnemer tijdens de sessie.

[21] Ponemon. The Cost of Insider Risks Global Report 2023. https://www.dtexsystems.com/resource-ponemon-insider-risks-global-report/

[22] Zie ook onze publicatie over crisismanagement en crisiscommunicatie bij digitale incidenten: https://www.ncsc.nl/documenten/publicaties/2022/maart/4/aandachtspunten-crisismanagement-en-crisiscommunicatie

[23] https://www.ncsc.nl/contact/wbni-melding-doen

[24] https://www.politie.nl/aangifte-of-melding-doen/

[25] https://www.autoriteitpersoonsgegevens.nl/datalek-melden

[26] https://www.aivd.nl/contact

[27] Zie The Human Consequences of Ransomware Attacks (isaca.org)

[28] Kübler-Ross, E., & Kessler, D. (2009). The five stages of grief. In Library of Congress Catalogin in

Publication Data (Ed.), On grief and grieving (pp. 7-30)

[29] Dit hoofdstuk is later toegevoegd door het NCSC op basis van de resultaten uit de eerdere hoofdstukken en ontvangen feedback van verschillende deelnemers.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

maart 2024

TLP:CLEAR