



Algemene Inlichtingen- en
Veiligheidsdienst

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties



Weerbaar tegen dreigingen van binnenuit

Herkennen en voorkomen

Inhoudsopgave

Voorwoord	3
Diverse typen <i>insiders</i>	4
Activiteiten die <i>insiders</i> kunnen ontplooiën	8
Wie zijn <i>insiders</i> binnen mijn organisatie?	9
Actoren	10
Het kritieke pad van de interne dreiging	11
Dreiging van binnenuit: herkennen en voorkomen	12
Een effectief <i>insider risk</i> -programma	14
Veelvoorkomende kwetsbaarheden in organisaties	17
Definities	22
Referenties	24
Notities	25

Voorwoord

Veel organisaties houden bij het nemen van maatregelen voor het beveiligen van hun informatie rekening met dreigingen van buitenaf, zoals hackers. Het risico dat van binnenuit komt, de interne dreiging, wordt vaak over het hoofd gezien. Interne dreiging is de dreiging die uitgaat van iemand die zijn kennis of autorisaties of positie gebruikt om bewust of onbewust schade toe te brengen aan de belangen van de organisatie waar diegene werkt.

Uit inlichtingenonderzoek van de Algemene Inlichtingen- en Veiligheidsdienst blijkt dat kwaadwillende inlichtingendiensten, de georganiseerde criminaliteit en extremisten er niet voor terugdeinzen om insiders in te zetten bij zowel publieke als private organisaties om hun doelstellingen te bereiken. Insiders zijn mensen die geautoriseerde toegang hebben tot de belangen die organisaties willen beschermen. Dit kan bijvoorbeeld gaan om informatie, het personeel of de fysieke en digitale systemen van organisaties.

Om insider-dreigingen tegen te gaan draagt de AIVD op basis van zijn inlichtingenpositie en unieke kennis bij aan het verhogen van de weerbaarheid van de overheid, vitale sectoren, kennisinstellingen en (delen van) het bedrijfsleven. Naast de beoogde bewustwording over insider-dreigingen, bevat deze brochure inzichten in maatregelen die helpen insider-risico's beheersbaar te maken.

De AIVD richt zich primair op insiders die, al dan niet aangestuurd door derde partijen, schade kunnen toebrengen aan de nationale veiligheid en/of de Nederlandse belangen. De adviezen en maatregelen in deze brochure zijn echter ook breder toepasbaar op insiders die onbewust schade aan hun organisaties veroorzaken.

Diverse typen *insiders*

Een insider is iemand die geautoriseerde toegang heeft tot te beschermen belangen zoals informatie, intellectueel eigendom, personeel of digitale en fysieke infrastructuur. Het kan ook iemand zijn die kennis heeft doordat hij eerder geautoriseerde toegang heeft gehad. Iedere persoon binnen een organisatie heeft de potentie om bewust of onbewust schade toe te brengen aan die organisatie en is daarmee een potentiële insider-dreiging die kan worden uitgebuit door tegenstanders. Dit noemen we actoren. Dat kunnen andere landen zijn, extremisten of criminele netwerken als zij daar kans toe zien.

Er worden verschillende typen insider-dreigingen onderscheiden, afhankelijk van de intentie en de aard van de acties van de insider. De meeste incidenten vinden plaats door niet-intentionele insiders. De impact van een actie van een intentionele insider is echter vaak groter.

Intentionele insider: Iemand die bewust schade toebrengt aan de organisatie waarvoor die persoon werkt of heeft gewerkt. We herkennen drie typen intentionele *insiders*.

1. Geïnfiltreerde insider

Een actor stuurt iemand uit eigen gelederen die een organisatie infiltreert door te solliciteren en aan de slag te gaan bij een organisatie.

Voorbeeld: Een inlichtingenofficier van een buitenlandse inlichtingendienst infiltreert een organisatie om de unieke kennis van deze organisatie te stelen en te delen met zijn inlichtingendienst.

Motivatie: De *insider* werkt in het belang van de actor waarvoor hij/zij werkt. Dit kan gaan om statelijke actoren zoals buitenlandse inlichtingendiensten, maar ook om criminele netwerken of extremistische groeperingen.

2. Zelf-initiërende insider

Iemand die uit eigen beweging ongeautoriseerde handelingen uitvoert die de belangen van de eigen organisatie kunnen beschadigen. Dit type *insider* kan ook uit eigen beweging toenadering zoeken tot een statelijke, extremistische of criminele actor om diens belang te behartigen en daarmee de belangen van de eigen organisatie te beschadigen.

Voorbeeld: Een medewerker van een organisatie heeft grote financiële problemen. Om zijn schulden af te lossen verkoopt de medewerker op eigen initiatief geheime documenten aan een buitenlandse inlichtingendienst.

Motivatie: Dit kan variëren van financieel gewin, wraakgevoelens en ideologische overtuigingen tot een verlangen om te concurreren met de organisatie.

3. Gerekruteerde insider

Iemand die al werkzaam is binnen een organisatie wordt gerekruteerd door een actor. Dit kan zowel een intentionele insider als een niet-intentionele *insider* zijn. Iemand kan bewust meewerken met een actor, maar soms wordt iemand zo goed bespeeld dat diegene bijvoorbeeld informatie prijsgeeft zonder zich hiervan bewust te zijn. De gerekruteerde insider kan dus ook onder de categorie niet-intentionele *insider* vallen.

Voorbeeld: Een crimineel netwerk rekruteert een medewerker van een groot verhuurbedrijf om informatie over klanten te verkrijgen. Het criminele netwerk gebruikt deze informatie voor criminele doeleinden.

Motivatie: Dit kan variëren van omkoping, chantage, en sociale manipulatie of bedreigingen tegen henzelf of hun dierbaren.

Niet-intentionele insider: iemand die onbewust schade toebrengt aan de organisatie waarvoor die persoon werkt of heeft gewerkt. Dit kan bijvoorbeeld doordat deze persoon in zijn of haar werk onzorgvuldig, onwetend of security-vermijgend is.

We herkennen drie typen niet-intentionele insiders:

1. Onwetende insider

Door onvoldoende kennis te hebben of onvoldoende overzicht te hebben over de gevolgen van hun acties, kunnen medewerkers onbewust hun organisatie beschadigen.

Voorbeeld: iemand die per ongeluk op een linkje in een phishing-mail klikt en daardoor zonder het zelf door te hebben de organisatie beschadigt.

2. Onzorgvuldige insider

Door onzorgvuldig te werk te gaan kunnen medewerkers onbewust schade toebrengen aan hun organisaties.

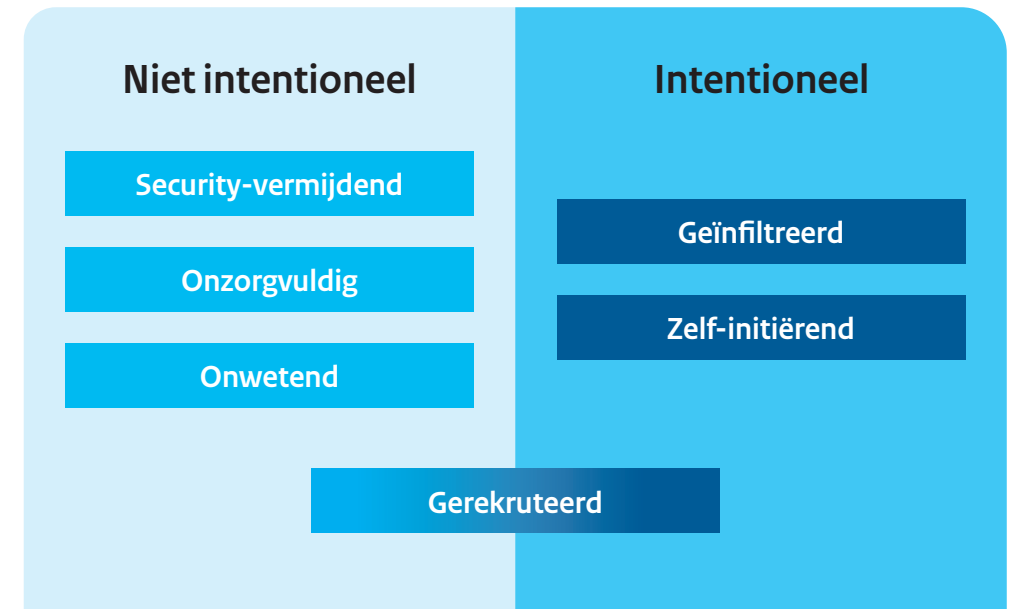
Voorbeeld: iemand die onzorgvuldig met zijn of haar spullen omgaat en zo vertrouwelijke documenten in de trein achterlaat.

3. Security-vermijdende insider

Dit is iemand die de regels wel kent, maar besluit om zich er niet aan te houden bij het uitvoeren van zijn of haar werkzaamheden. De security-vermijdende insider heeft niet bewust het doel om schade aan zijn/haar organisatie toe te brengen maar dit kan wel een effect zijn van het negeren van de geldende beveiligingsmaatregelen.

Voorbeeld: iemand die uit gemakzucht bewust vertrouwelijke gesprekken voert op plekken die niet daarvoor geschikt zijn. Door bijvoorbeeld in het openbaar vervoer met collega's te spreken over bedrijfsgevoelige of staatsgeheime informatie.

Motivatie: Haast, gemakzucht, onoplettendheid, nalatigheid, een gebrek aan kennis of begrip van de risico's kunnen er allemaal toe leiden dat een insider onbedoeld schade toebrengt aan een organisatie.



Activiteiten die *insiders* kunnen ontplooiën

De belangrijkste schadelijke activiteiten door *insiders* die de AIVD onderscheidt, zijn:

Spionage

Het onrechtmatig verkrijgen van vertrouwelijke informatie, kennis of technologie om deze voor eigen doeleinden te kunnen gebruiken.

Voorbeeld: Een inlichtingendienst die een insider gebruikt om vertrouwelijke informatie te verkrijgen over militaire technologie.

Beïnvloeding

Het beïnvloeden van processen en/of personen in het voordeel van de actor.

Voorbeeld: Een insider lekt informatie van zijn organisatie om de publieke opinie te sturen of de strategische koers van zijn organisatie te beïnvloeden.

Sabotage

De positie van de organisatie wordt verzwakt door bijvoorbeeld fysieke schade toe te brengen, processen te verstoren, imagoschade te creëren of financiële schade toe te brengen.

Voorbeeld: Een vijandige inlichtingendienst gebruikt een insider die werkzaam is binnen een nutsbedrijf om de infrastructuur van een land te saboteren.

Corruptie

Het misbruik maken van toegekende bevoegdheden of macht voor persoonlijk gewin. Actoren kunnen corruptie bij insiders gebruiken om hun doel te bereiken. In het bedrijfsleven leidt corruptie tot schade aan bedrijven doordat bijvoorbeeld bedrijfsgeheimen of financiële middelen worden misbruikt. In de publieke sector leidt het tot aantasting van de integriteit van de overheid, doordat corrupte ambtenaren handelingen kunnen uitvoeren die schade kunnen toebrengen aan individuele burgers of de samenleving als geheel.

Voorbeeld: Een crimineel netwerk heeft informatie nodig over een rivaal en gebruikt een corrupte insider in de publieke of private sector om informatie over de rivaal te verkrijgen. Na het verkrijgen van bijvoorbeeld een woonadres wordt deze informatie gebruikt door het criminele netwerk om de rivaal te bedreigen.

Wie zijn *insiders* binnen mijn organisatie?

Bij *insiders* wordt vaak alleen gedacht aan de vaste medewerkers van organisaties. Medewerkers zijn de personen die werkzaam zijn binnen de organisatie en toegang hebben tot de organisatorische assets, zoals personen, gebouwen, informatie, netwerken en systemen. Ook moet gedacht worden aan medewerkers die op afstand werken en (mogelijk) vanaf daar bij alle systemen en informatie kunnen. Denk hierbij aan medewerkers die vanuit huis of vanuit het buitenland werken of in een langdurig ziekteverlof zitten.

Houd er echter ook rekening mee dat naast de vaste medewerkers ook andere mensen in uw organisatie dezelfde mate van toegang kunnen hebben tot uw organisatie. Zij moeten ook als insider worden beschouwd. Hieronder staan enkele voorbeelden van mensen die ook als *insiders* moeten worden aangemerkt binnen organisaties:

Ex-medewerkers

Personen die vroeger werkzaam waren binnen de organisatie en nog steeds kennis hebben van en mogelijk toegang hebben tot organisatorische assets, zoals medewerkers, gebouwen, informatie, netwerken en systemen van een organisatie.

Bezoekers

Personen die de organisatie bezoeken en toegang hebben tot organisatorische assets.

Leveranciers

Personen die producten of diensten leveren aan de organisatie en toegang hebben tot organisatorische assets. Denk hierbij aan IT-onderaannemers of softwareleveranciers.

Contractanten

Personen die door de organisatie worden ingehuurd en toegang hebben tot organisatorische assets. Denk hierbij aan freelancers of interim-managers.

Stagiairs of studenten

Personen die stagelopen of onderzoek doen binnen de organisatie en toegang hebben tot organisatorische assets.

Actoren

De AIVD ziet op basis van inlichtingen een insider-dreiging uitgaan van verschillende actoren. De belangrijkste actoren die de AIVD vanuit zijn inlichtingenonderzoek onderscheidt:

Statelijke actoren

Landen met een offensief programma tegen Nederland of de Nederlandse belangen ondernemen in het geheim activiteiten die de nationale veiligheid bedreigen en de democratische rechtsorde kunnen ondermijnen. Goede diplomatieke relaties tussen landen hoeven heimelijke activiteiten niet uit te sluiten. In veel gevallen is het moeilijk de scheidslijn tussen statelijke en niet-statelijke actoren te onderscheiden. Uit onderzoek van de AIVD komt onder meer naar voren dat sommige criminele netwerken structureel actief zijn voor statelijke actoren in het uitvoeren van geweld. Naast geweld kunnen diefstal van kennis en intellectueel eigendom ook tot de activiteiten van statelijke actoren behoren.

Extremisten

De AIVD ziet soms gevallen waar mensen met een extremistisch gedachtegoed werkzaam zijn binnen organisaties met te beschermen belangen voor de staat. Van daaruit kunnen deze personen bewust of onbewust schade toebrengen aan de betreffende organisatie en de democratische rechtsorde.

Criminele netwerken

Criminele netwerken maken gebruik van insiders om via hen informatie te verkrijgen en/of handelingen te verrichten die van nut kunnen zijn voor hun criminele activiteiten. Denk hierbij aan het op afstand houden van de overheid en het plannen van geweld tegen belangendragers van de democratische rechtsorde.

Het kritieke pad van de interne dreiging

Een insider-incident ontstaat door een samenloop van omstandigheden. Een insider-dreiging is niet terug te brengen naar een vaste set aan persoonskenmerken of situaties. Om het insider-risico goed te kunnen duiden moet een organisatie de context van de medewerkers en de eigen organisatie kennen. Daarnaast moet de organisatie in staat zijn te reflecteren op het eigen handelen om zo het risico op insider-gedrag te beheersen.

Om beter inzicht te krijgen in de factoren die invloed kunnen hebben op insider-incidenten is het model 'Het kritieke pad naar een insider risico' ontwikkeld door Shaw en Sellers (Shaw & Sellers, 2015). Dit model beschrijft hoe medewerkers via een bepaald kritiek pad geleidelijk afglijden, met het risico dat zij uiteindelijk overgaan tot het uitvoeren van schadelijke activiteiten.

'Het kritieke pad naar een insider risico' stelt organisaties in staat om incidenten te evalueren. Ook biedt het concrete handvatten voor een risico- en maatregelanalyse om risico's inzichtelijk te maken en maatregelen te bepalen om deze risico's te beheersen.

Dreiging van binnenuit: herkennen en voorkomen

Organisaties kunnen te maken krijgen met interne dreigingen, zoals (bedrijfs) spionage, diefstal of het lekken van informatie, fraude, corruptie, *insider trading*, sabotage, misbruik van middelen, agressief gedrag en (politiek) activisme. Zulke incidenten komen zelden uit het niets; vaak zijn er (zichtbare) gedragingen en factoren die hieraan voorafgaan. Door die tijdig te herkennen en juist te handelen, kunnen risico's worden beperkt.



Bron: Shaw, E., & Sellers, L. (2015). Application of critical-path method to evaluate insider risks. Defense Personnel and Security Research Center (PERSEREC).

Een effectief *insider risk*-programma

Om insider-risico's te verminderen is een effectief insider risk-programma nodig. Een insider risk-programma is een doorlopend programma dat een groot deel van de bedrijfsvoering raakt. In dit hoofdstuk zijn principes uitgewerkt die kunnen leiden tot een effectief insider risk-programma.

De principes zijn uitgewerkt onder de structuur van het NIST-cybersecurity 2.0 framework (National Institute of Standard and Technology, 2024).

Dit framework gaat uit van de volgende factoren:

Bestuur

Op basis van strategie wordt beleid gemaakt. Op dat beleid wordt toezicht gehouden.

Identificeren

Het identificeren en in kaart brengen en begrijpen van de risico's.

Beschermen

Het treffen van maatregelen om risico's te beheersen.

Opsporen

Het detecteren van dreigingen die zich manifesteren rondom de bedrijfsmiddelen.

Reageren

De manier waarop de organisatie reageert op de dreiging die zij waarneemt.

Herstellen

Het herstellen van de belangen die zijn geraakt door een incident.

Onderstaande lijst is niet uitputtend maar geeft een eerste indicatie waarmee u aan de slag kunt gaan.

Besturen

Een effectief insider risk-programma:

- definieert rollen en verantwoordelijkheden voor insider risk-management door de juiste expertise en capaciteiten te borgen op zowel technisch, juridisch, HR, privacy als psychologisch vlak;
- stelt insider-risicobeleid op;
- zorgt voor toezicht op het insider-risicobeleid;
- moet op de juiste juridische grondslag zijn gebaseerd.

Identificeren

Een effectief *insider risk*-programma:

- werkt risico-gebaseerd op basis van een doorlopend risicomanagementproces;
- brengt de te beschermen belangen zoals kritieke diensten, processen en assets in kaart en richt zich op de dreiging die verschillende typen insiders hiervoor kunnen vormen.

Beschermen

Een effectief insider risk-programma zorgt voor een robuust securitylandschap door de organisatie te verdedigen tegen insider-dreigingen met:

- technische maatregelen zoals netwerkbeveiliging, segmentatie, encryptie en Identity en Access Management en forensic readiness;
- fysieke maatregelen zoals risico-gebaseerde compartimentering van werkgebieden op basis van het need-to-be-principe, en multifactorauthenticatie voor fysieke toegang tot gevoelige werkgebieden;
- organisatorische maatregelen zoals beveiligingsbeleid, gedragscodes, een clean desk policy, bewustwording bij medewerkers en leidinggevendenden over zorgwekkend gedrag bij collega's, een sociaal fonds, een zichtbare en benaderbare vertrouwenspersoon, ethisch en betrokken leiderschap en een sterke veiligheidscultuur;
- personele maatregelen zoals een screeningsbeleid voor nieuwe en bestaande werknemers, periodieke herhaalscreenings en het uitvoeren van een antecedentenonderzoek voor medewerkers in functies met toegang tot gevoelige gegevens of locaties.

Leestips

- In 2024 is de NCSC publicatie 'Omgaan met insider threats, good practices van Nederlandse organisaties' uitgebracht. In deze publicatie zijn de te nemen maatregelen omtrent insider threat in meer detail onder de structuur van het NIST-framework uitgewerkt. Voor dit stuk is input van de AIVD gebruikt.
- In 2026 heeft het NCSC het artikel 'Omgaan met insider threats' gepubliceerd. Ook in deze publicatie zijn de te nemen maatregelen omtrent insider threat verder uitgewerkt onder de structuur van het NIST-framework. Voor dit stuk is input van de AIVD gebruikt.

Opsporen

Een effectief insider risk-programma detecteert afwijkend gedrag en spoort risico's op door gebruik te maken van:

- duidelijke meldprocedure voor zorgwekkend gedrag bij medewerkers;
- fysieke controle van werknemers door middel van bijvoorbeeld visitaties bij het in- en uittreden van de gebouwen van een organisatie;
- het toepassen van protective monitoring;
- het gebruik van technische detectiemiddelen zoals bijvoorbeeld User and Entity Behavior Analytics (UEBA) software en Security Information and Event Management (SIEM) software.

Reageren

Een effectief insider risk-programma:

- ontwikkelt en onderhoudt een incident response- en communicatieplan gericht op insider risk en investeert in de juiste expertises voor onderzoek en opvolging;
- zorgt voor noodprocedures met duidelijke afspraken over governance;
- zorgt voor noodprocedures om rechten in te trekken. Zo kunnen bij incidenten digitale en fysieke toegangsrechten abrupt worden ingetrokken en kunnen bedrijfsmiddelen meteen worden ingenomen;
- zorgt voor een proces om meldingen te maken van insider risk-casuïstiek bij de AIVD wanneer de verdenking bestaat dat er sprake is van een statelijke dreiging;
- zorgt voor een proces om aangifte te doen bij de politie in het geval van strafbare feiten;
- ondersteunt medewerkers met beheersbare risicofactoren voor insider-gedrag door bijvoorbeeld hulp aan te bieden aan medewerkers met schulden.

Herstellen

Een effectief *insider risk*-programma:

- heeft herstelplannen om snel te kunnen herstellen van incidenten;
- heeft een procedure waarmee incidenten worden geëvalueerd en processen en maatregelen worden verbeterd.

Veelvoorkomende kwetsbaarheden in organisaties

Veel publieke en private organisaties hebben nog te weinig maatregelen getroffen om zichzelf te beschermen tegen kwaadwillende insiders. Uit inlichtingenonderzoek van de AIVD blijkt dat kwaadwillende insiders systeemkwetsbaarheden binnen organisaties weten te benutten en zo bijvoorbeeld aan gevoelige informatie kunnen komen. Hieronder staan veelvoorkomende praktijkvoorbeelden van de kwetsbaarheden die de AIVD in inlichtingenonderzoek is tegengekomen bij organisaties in Nederland, zonder deze te herleiden naar een specifieke bron of organisatie.

- Herkent u onderstaande kwetsbaarheden bij uw eigen organisatie?
- Beantwoord de beoordelvingsvraag en ga na wat uw organisatie kan doen om deze kwetsbaarheden te beheersen.
- Inventariseer welke stappen u kunt ondernemen om uw organisatie weerbaar te maken tegen insiders.

Fictief voorbeeld:

Binnen een bedrijf wordt bij HR een melding gemaakt over een medewerker van de afdeling financiën die zichzelf toegang heeft verschaft tot documenten over het fabricageproces van het bedrijf. Een andere medewerker van het bedrijf had al eerder bij haar eigen leidinggevende haar zorgen geuit over ander zorgwekkend gedrag van deze medewerker. Omdat de signalen niet op een centrale plek verzameld worden en niet in samenhang bekeken kunnen worden, herkent het bedrijf de casus niet als een insider risk en worden er geen tijdige, adequate maatregelen genomen.

Fictief voorbeeld:

Een medewerker van een bedrijf wordt op zijn verjaardag aangesproken door zijn buurman. De buurman vertelt dat hij door zijn recente verhuizing helaas het adres van zijn oude studievriend is verloren. De buurman vraagt tussen neus en lippen door of de medewerker even in het klantenbestand van het bedrijf waar hij werkt het adres van zijn studievriend kan opzoeken zodat hij weer eens in contact kan komen. Door het pas doorlopen bewustwordingsprogramma van het bedrijf, herkent de medewerker deze ongewenste situatie. De medewerker gaat niet mee in het verzoek en maakt er een melding van bij zijn bedrijf.

Categorie	Kwetsbaarheid	Beoordelvingsvraag
Signalering en melding	Signalen van mogelijk kwaadwillend handelen worden onvoldoende vastgelegd of niet centraal vastgelegd en geanalyseerd. Soms ontstaat een compleet beeld pas als alle signalen van afwijkend gedrag in samenhang worden bekeken. Daarom is het extra belangrijk om ook de signalen vast te leggen die niet direct geduid kunnen worden.	Worden alle signalen (ook onduidelijke of kleine incidenten) centraal vastgelegd en in samenhang geanalyseerd om dreigingen te herkennen?
	Medewerkers weten niet waar of hoe zij verdachte situaties veilig kunnen melden. Vooral in kleine organisaties is anoniem meldingen kunnen doen een aandachtspunt.	Weten medewerkers waar zij vertrouwelijk en anoniem een melding kunnen doen?
	Na directe bevraging van insiders binnen integriteitsonderzoeken nemen zij vaak ontslag. Met het ontslag stopt ook vaak het integriteitsonderzoek. Signalen uit dat onderzoek worden daarna vaak niet goed uitgezocht, vastgelegd en gedeeld, wat jobhopping buiten of binnen de organisatie faciliteert.	Wordt bij integriteitsonderzoeken waarbij de medewerker de organisatie verlaat, de dossiervorming geborgd? Is er een mechanisme om jobhopping tussen organisaties of organisatieonderdelen te voorkomen?

Categorie	Kwetsbaarheid	Beoordelvingsvraag
Cultuur en bewustzijn	Er is binnen organisaties onvoldoende bewustzijn over de insider-dreiging op de organisatie vanuit criminele, statelijke of extremistische actoren.	Is er een structureel bewustwordingsprogramma aanwezig voor zowel medewerkers als leidinggevenenden over insider-dreigingen die relevant zijn voor de organisatie?
	Binnen veel organisaties bestaat een lage meldingsbereidheid vanwege loyaliteitsconflicten.	Is de organisatiecultuur zodanig dat medewerkers zich veilig voelen om meldingen te doen, ook als dit onderlinge loyaliteit raakt?
	Er ontstaan risico's door vermenging met of beïnvloeding door criminele netwerken, statelijke actoren en extremisten via de sociale omgeving van medewerkers.	Is er bewustwording over de risico's die voortvloeien uit de vermenging van de sociale omgeving en het werk van medewerkers? Weten medewerkers wat ze moeten doen wanneer iemand ze probeert te beïnvloeden?
	Computers worden niet vergrendeld bij het verlaten van de werkplek, waardoor accounts misbruikt kunnen worden.	Hebben medewerkers de discipline om computers te vergrendelen bij het verlaten van de werkplek en wordt hierop toegezien?

Fictief voorbeeld:

Een medewerker van een organisatie zit thuis in een langdurig ziekteverlof. De medewerkers zijn al maanden niet op kantoor geweest en herstellen langzaam. In tussentijd start de medewerker zijn werklaptop op en downloadt gevoelige data die hij te koop aanbiedt aan een crimineel netwerk om zijn gokschulden af te lossen. De collega's en leidinggevende van deze medewerker hebben door het langdurige ziekteverlof van de medewerker geen goed zicht op de medewerker en hebben niet door dat hij nog bij gevoelige data kan.

Fictief voorbeeld:

Bij een bedrijf blijken gegevens te zijn weggelekt. Intern onderzoek laat zien dat deze gegevens op een intern netwerk van het bedrijf staan waar alleen medewerkers toegang toe hebben. Omdat het bedrijf de logging van (digitale) handelingen van medewerkers op systemen slechts enkele dagen bewaart, kan het bedrijf niet onderzoeken wie de gegevens heeft opgezocht in het systeem. Het bedrijf kan daardoor niet achterhalen wie de gegevens heeft gelekt. De insider kan aan het werk blijven in de organisatie en blijft dus een risico vormen.

Categorie	Kwetsbaarheid	Beoordelvraag
Screening en werkplek	Medewerkers werken soms in complete sociale isolatie waardoor de organisatie de grip op hen verliest. Denk aan thuiswerken, een langdurig ziekteverlof of langdurig werken vanuit het buitenland.	Worden de risico's van werken in isolatie (zoals thuiswerken of werken vanuit het buitenland) beoordeeld en gemonitord?
	Er vindt onvoldoende controle plaats op (herhaal)screenings van medewerkers.	Worden personeelsscreenings bij kritieke functies niet alleen bij aanvang gedaan, maar ook periodiek herhaald?

Categorie	Kwetsbaarheid	Beoordelvraag
Toegang en monitoring	De principes van need-to-know, need-to-be, en need-to-use worden onvoldoende toegepast.	Worden autorisaties strikt toegekend op basis van de noodzaak voor de specifieke werkzaamheden (need-to-know/use/be)? Wordt toegang tot gevoelige processen beheerst door medewerkers niet meer rechten te geven dan zij nodig hebben om hun functie uit te voeren?
	Maatregelen als het vier-ogenprincipe of functiescheiding worden onvoldoende toegepast.	Worden processen die een hoog risico op fouten of fraude met zich meebrengen, zodanig ingericht dat een handeling nooit door één persoon alleen kan worden voltooid (vier-ogenprincipe)? Worden uitvoerende en controlerende taken strikt gescheiden gehouden (functiescheiding)?
	Onvoldoende aandacht voor het aanpassen van rechten bij functiewisseling, uitdiensttreding of langdurige ziekteverloven waarin de medewerkers niet aan het werk zijn.	Worden autorisaties, rechten en plichten van medewerkers direct aangepast bij een functieovergang of uitdiensttreding? Wordt er (periodiek) gecontroleerd of de autorisaties van medewerkers nog aansluiten op hun werkzaamheden?
	Er vindt onvoldoende vastlegging plaats van handelingen in systemen. De bewaartermijn van de logging is vaak te kort. Daarnaast wordt er weinig actief gemonitord.	Worden handelingen in systemen voldoende gelogd en worden de logs lang genoeg bewaard voor effectief onderzoek? Wordt er gemonitord op het gebruik van systemen met technieken als User en Entity Behaviour Analytics?

Definities

Criminele netwerken

De georganiseerde misdaad maakt zich schuldig aan ondermijning van de overheid en bedrijven. Als criminele actoren een dreiging vormen voor de nationale veiligheid en hun activiteiten leiden tot ondermijning van de democratische rechtsorde heeft de AIVD de taak daar onderzoek naar te doen.

Extremisten

Het uit ideologische motieven bereid zijn om niet-gewelddadige en/of gewelddadige activiteiten te verrichten die de democratische rechtsorde ondermijnen.

Forensic readiness

Forensic readiness is de paraatheid van een organisatie om digitaal sporenonderzoek te kunnen (laten) doen bij een cyberincident (NCSC, 2025a).

Insider

Iemand die uit functionele overweging geautoriseerde toegang of kennis heeft (of had) van de organisatie, waaronder personeel, gebouwen, informatie, systemen en netwerken. Iedereen binnen de organisatie is een insider.

Insider risk

Dit is de impact vermenigvuldigd met de kans van een insider threat. Om dit type risico goed te kunnen beheersen, dient het opgenomen te zijn in het integrale risicobeheersingsproces van een organisatie. Gezien de complexiteit die vaak gepaard gaat met het beheersen van dit specifieke risico, adviseert de AIVD om hiervoor een insider risk-programma in te richten.

Insider threat

De mogelijkheid dat een werknemer, een collega of ander persoon met toegang tot een organisatie, onbedoeld of opzettelijk schade aanricht aan de organisatie door middel van misbruik van toegang of bevoegdheden. Insider threat, ook wel de interne dreiging, kan een ernstige bedreiging vormen voor de continuïteit van een organisatie, en kan leiden tot financiële verliezen en/of reputatieschade. In sommige gevallen kan insider threat zelfs een bedreiging vormen voor het welzijn en de veiligheid van het personeel.

Need-to-be

Het uitgangspunt dat een persoon alleen fysieke of digitale toegang heeft tot een omgeving wanneer dit noodzakelijk is voor de uitvoering van zijn of haar werkzaamheden (Rijksoverheid, 2026)

Need-to-know

Het uitgangspunt dat een persoon alleen kennis neemt van of toegang heeft tot bepaalde informatie wanneer dit noodzakelijk is voor de uitvoering van zijn of haar werkzaamheden (Rijksoverheid, 2026)

Need-to-use

Het uitgangspunt dat een persoon alleen fysiek of digitaal gebruik kan maken van middelen (zoals apparatuur, hardware of software) of informatie wanneer dit noodzakelijk is voor de uitvoering van zijn of haar werkzaamheden (Rijksoverheid, 2026)

Protective monitoring

Dit is een methode om insider risk vroegtijdig te ontdekken. Bij protective monitoring worden gedrag (zowel fysiek als digitaal), omstandigheden en mate van toegang van werknemers geanalyseerd. De opgedane kennis over dit gedrag wordt gecombineerd tot een risicoscore die aangeeft hoeveel risico een organisatie loopt door het gedrag van een medewerker. Op basis van deze risicoscore kan een organisatie onderzoek doen naar potentiële kwaadwillende insiders.

Security Information & Event Management software

Security Information & Event Management (SIEM) software is in staat om log-informatie vanuit verschillende bronnen te interpreteren en te correleren naar wat zich binnen en rondom het netwerk afspeelt op gebied van cyberaanvallen en andere beveiligingsincidenten (NCSC, 2025b)

Statelijke actoren

Buitenlandse inlichtingen- en veiligheidsdiensten worden ook wel aangeduid als statelijke actoren. De motieven van statelijke actoren lopen uiteen, maar aangenomen mag worden dat deze actoren over de capaciteiten, middelen en intenties beschikken om (heimelijk) schade toe te brengen aan onze nationale veiligheid, economische veiligheid en democratische rechtsorde.

User and Entity Behaviour Analytics (UEBA) software

UEBA-software verzamelt een baseline van het gedrag van gebruikers (de mens die de systemen gebruikt) en entiteiten (zoals bijvoorbeeld servers, firewalls of databases). Als gedrag niet binnen het normale patroon van deze gebruiker of entiteit valt, kan er gealarmeerd worden.

Referenties

1. Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025). *Dreigingsbeeld Terrorisme Nederland* 2025. <https://www.nctv.nl/site/binaries/site-content/collections/documents/2025/12/09/dtn-december-2025-dtn-december-2025.pdf>
2. Nationaal Cyber Security Centrum. (2024). *Omgaan met insider threats*. <https://www.ncsc.nl/identiteits-en-toegangsbeheer/omgaan-met-insider-threats>
3. Nationaal Cyber Security Centrum. (2025a). *Forensic readiness*. <https://www.ncsc.nl/incidenten-en-herstellen/forensic-readiness>
4. Nationaal Cyber Security Centrum. (2025b). *SOC inrichten, begin klein*. <https://www.ncsc.nl/soc/soc-inrichten-begin-klein>
5. Nationaal Cyber Security Centrum. (2026). *Omgaan met insider threats*. <https://ncsc.nl/identiteits-en-toegangsbeheer/omgaan-met-insider-threats>
6. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. <https://doi.org/10.6028/NIST.CSWP.29>
7. Rijksoverheid. (2026). *Algemene beveiligingseisen voor Rijksoverheidopdrachten 2026*. <https://open.overheid.nl/documenten/a13699d9-fcf4-43ef-b282-ec9519e9b81/file>
8. Shaw, E., & Sellers, L. (2015). *Application of the Critical-Path Method to Evaluate Insider Risks*. *Studies in Intelligence*, 59(2), 41-48. <https://www.cia.gov/resources/csi/static/Application-of-Critical-Path-1.pdf>

Notities

[illegible]

Notities

[illegible]

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010 | 2500 EA Den Haag
aivd.nl

oktober 2026