Auditdienst Rijk
Ministerie *van Financiën*

Onderzoek IT infrastructuur Leonardo

Datum 21 december 2015
Status Definitief
Kenmerk ADR/2015/1691

Weglak criteria WOB-verzoeken

B. de persoonsgebonden informatie (namen en telefoonnummers)
C. de bedrijfsvertrouwelijke informatie (uurtarieven, leverancier specifieke info, methoden e.d.)
D. de andere categorie gegevens die Ven) belangen kunnen schaden (beoordelingscriteria, positiebepaling/onderhandelingsinfo, kwetsbaarheden e.d.).

Colofon

Titel	Rapport van bevindingen IT- infrastructuur Leonardo
Bijlagen	
Bestemd voor	De directeur van de directie FEZ ministerie van V&J
Inlichtingen	Auditdienst Rijk Postbus 20201 2500 EE Den Haag

Criterium B

Inhoud

1 Infrastructuur onderzoek

Dit rapport bevat feitelijke bevindingen overeenkomstig NOREA Richtlijn 4401; specifieke werkzaamheden met betrekking tot informatietechnologie.

1.1 Opdrachtgever

De opdrachtgever voor dit onderzoek is de eigenaar van het systeem Leonardo. Dit is de directie DFEZ (Directie Financieel Economische Zaken) van het ministerie van Veiligheid en Justitie (V&J).

1.2 Object van onderzoek

Object van onderzoek is de IT-infrastructuur van de applicatie Leonardo waarin financiële gegevens verwerkt worden. Het beheer en de hosting van leonardo is belegd bij SSC-ICT. Het SSC-ICT is een shared service center dat voor acht ministeries werkt.

1.3 De overeengekomen werkzaamheden zijn uitgevoerd.

De randvoorwaarde voor het uitvoeren van dit onderzoek was de beschikbaarheid van een topologisch overzicht van de IT-infrastructuur van leonardo. Tijdens het opstellen en afstemmen van het plan van aanpak is gebruik gemaakt van een verouderde infrastructuurplaat, wat tot een niet juist beeld In de concept eindrapportage heeft geleid. In overleg met de opdrachtgever is na het uitbrengen van het concept rapport aanvullend onderzoek bij SSC ICT uitgevoerd aan de hand van actuele topologische overzichten. Dit onderzoek is op 10 december 2015 afgerond en heeft tot een significante aanpassing van het rapport geleid.

1.4 Onafhankelijkheid

De uitvoerende IT-audItors zijn in dienst van de Audit Dienst Rijk (ADR) van het ministerie van Financiën en daarmee niet afhankelijk van de opdrachtgever.

1.5 Doel van de opdracht

De integriteit van de gegevens in Leonardo is van groot belang voor de betrouwbaarheid van de financiële administratie. De systeemeigenaar van Leonardo, de DFEZ, streeft ernaar dat SSC-ICT over niet al te lange termijn een ISAE 3402-verklaring aan afnemers verstrekt ten einde de benodigde zekerheld te verschaffen dat de maatregelen die de betrouwbaarheid van de informatievoorziening moeten waarborgen getroffen zijn. Het doel van dit onderzoek is daarmee tweeledig, namelijk:

1. Nu eventuele risico's te onderkennen die de betrouwbaarheid van het financiële administratiesysteem bedreigen. Om dit doel te bereiken zijn onderzoeksvragen geformuleerd (zie hoofdstuk 2). Deze hebben betrekking op de getroffen beheersmaatregelen ten aanzien van de IT-infrastructuur van Leonardo die een bijdrage leveren aan de betrouwbaarheid van de gegevens In Leonardo.
2. De risico's die niet of onvoldoende worden afgedekt door maatregelen kunnen door het SSC-ICT worden meegenomen in het ontwikkeltraject naar de ISAE 3402-verklaring.

1.6 Beschrijving van de uitgevoerde specifieke werkzaamheden

Het onderzoek bevatte de volgende activiteiten: document studie, Interviews met medewerkers van SSC-ICT en deelwaarnemingen ter plaatse.

Wij hebben tijdens de voorstudie op basis van de aangeleverde documentatie een risico-inschatting gemaakt van de infrastructurele risicofactoren die het meest van invloed zijn op Leonardo. Hierbij is de voor de Rijksoverheid geldende BIR [1] normeringen gehanteerd, waarbij de auditvragen zijn geconcretiseerd aan de hand van critica! security controls, zoals beschreven door het SANS institute [2].

De 20 *critica/ security controls* van het SANS institute beschrijven de belangrijkste beveiligingsmaatregelen die van belang zijn in een IT-landschap. Het is gebaseerd op de risico's die SANS door middel van eigen onderzoek en enquêtes in beeld brengt. De SANS top 20 is een wereldwijde toonaangevende bron van informatiebeveiliging en risico-inventarisering.

Met het beperkte beeld van het IT-infrastructuurlandschap van Leonardo is in het plan van aanpak een keuze gemaakt van de volgende risico's van de SANS top 20 die wij relevant achten voor dit onderzoek. De andere onderdelen van de SANS top 20 zijn ook relevant maar op basis van de documenten die wij bij het schrijven van het plan van aanpak overhandigd gekregen hebben, is het onderzoek beperkt op onderstaande negen controls. Deze risico's zijn uitgewerkt in onderzoeksvragen voor de verschillende componenten van de IT-Infrastructuur.

Nr	Beschrijving	SANS nrs.
1	Een volledig overzicht van hard en software	1 2
2	Een 'secure' configuratie van de Inrichting van de componenten	3
3	De wijze van het monitoren van punt 1 en 2	1, 2
4	De continue monitoring van kwetsbaarheden van infrastructurele componenten zoals aangeven door leveranciers en security researchers	4
5	Data recovery: mogelijkheid tot herstel van dataverwerking	8
6	Gecontroleerde beheerderstoegang langs elk onderdeel van het logisch pad (incl. OTAP en monitoring poortenJ	12
7	Boundary defences traffic control en last managed component.	13
8	Audit logs maintenance monitoring en analyze	14
9	Account monitoring en controL	16

De beantwoording van bovenstaande onderwerpen is opgenomen in hoofdstuk 2 van dit rapport.

1 BIR: Baseline Infonnatlevoorzlenlng Rijk
2 http://www.sans.org/critical-security-controls/ The Critical Security Controls focuses first on prioritizing security tunetlens that are effective against the latest Advanced Targeted Threats, with a streng emphasis on "What Works" • security cantreis where products, processes, architectures and servlees are In use that have demonstrated real world effectiveness.

1.7 Geen assurance-opdracht

Het uitgevoerde onderzoek betreft specifieke overeengekomen werkzaamheden. Dit betekent dat hier geen assurance wordt verstrekt en geen zekerheid wordt verstrekt. Wij geven geen algemeen oordeel, maar rapporteren bevindingen en risico's op basis van het gehanteerde referentiekader. Dit betekent voorts dat indien wij andere (aanvullende) werkzaamheden of een assurance-opdracht zou hebben uitgevoerd, wellicht andere onderwerpen zouden zijn onderzocht en gerapporteerd.

1.8 Verspreiding

Deze rapportage wordt verstrekt aan de opdrachtgever. Het rapport is besproken met degenen die bij de totstandkoming betrokken zijn geweest. Het is aan de opdrachtgever het rapport verder te verspreiden.

1.9 Hoor/wederhoor

Bij de bespreking van het concept rapport is door SSC-ICT aangegeven dat niet alle relevante evidence initieel was aangeleverd. De ADR heeft daarom aanvullend onderzoek gedaan en de resultaten hiervan verwerkt in deze rapportage.

1.10 Dossiervorming

De opdracht wordt uitgevoerd als een onderzoeksopdracht in overeenstemming met de bij de ADR geldende kwallteitsrichtlijnen en de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. De beroepsregels voor auditors stellen voorwaarden aan het omgaan met vertrouwelijke gegevens (geheimhoudingsplicht). In het elektronische dossier van de ADR wordt alle evidence van het onderzoek opgenomen.

2 Beschrijving van de feitelijke bevindingen

Zoals vermeld in het plan van aanpak geven wij in deze rapportage antwoord op de volgende negen vragen:

Op welke wijze:

1. wordt een overzicht bijgehouden van de hardware en software?
2. worden / zijn de componenten ingericht?
3. vindt monitoring van deze componenten plaats?
4. vindt continue monitoring van kwetsbaarheden plaats?
5. is data-recovery ingericht?
6. is beheerdertoegang ingeregeld?
7. zijn de 'boundary defences' geregeld?
8. vindt er onderhoud, monitoring en analyse van de loggegevens plaats?
9. vindt account monitoring en control plaats?

In dit hoofdstuk zijn de antwoorden op deze negen deelvragen in paragrafen gegroepeerd. Per paragraaf zijn de volgende elementen weergegeven:

1. De deelvraag uit het Plan van Aanpak
2. Toelichting, gebaseerd op de beschrijving van het risico door het SANS. Deze toelichting moet de lezer inzicht geven in de urgentie van de vraag
3. Opzet: hoe zijn de maatregelen ontworpen?
4. Bestaan: hoe is dit risico in de werkelijkheid geadresseerd door SSC-ICT?
5. Eventuele restrisico's

2.1 Op welke wijze wordt bij SSC-ICT een overzicht bijgehouden van de hardware en software? *{subvragen 1-4}*

SANS toelichting

Aanvallers zoeken voortdurend naar nieuwe kwetsbaarheden binnen een systeemlandschap. Voorbeelden van kwetsbaarheden zijn de toepassing van verouderde software (met bekende beveiligingslekken), onjuiste inrichting van de netwerkzonering, onjuist geconfigureerde systemen of onjuist geplaatste componenten zoals firewalls.

Een randvoorwaarde om te beoordelen of de IT-infrastructuur voldoende is beveiligd is een accuraat inzicht in de beoogde opzet van de IT-infrastructuur (de architectuur) en een accuraat inzicht in de werkelijk geconfigureerde hard-[3] en software[4]. Zonder deze kennis is het niet mogelijk de genomen beveiligingsmaatregelen in hun context te beoordelen.

3 Hardwareregistratie: Dit zijn de processen en instrumenten die worden gebruikt om bij te houden, te controleren en/of voorkomen dat alleen geautoriseerde netwerkapparaten (computers, netwerkcomponenten, printers, iets met IP-adressen) op basis van een CMDB-verbinding mogen maken met het netwerk.

4 Softwareregistratie: Dit zijn de processen en instrumenten die worden gebruikt om bij te houden, te controleren en/of voorkomen of er een correcte installatie is en gebruik van software op computers op basis van een inventaris van goedgekeurde software.

Opzet
Tijdens het onderzoek hebben we overzichten ontvangen van de inrichting en opzet van Leonardo. We hebben vastgesteld dat deze documenten sinds de in beheer name van Leonardo door SSC ICT in 2013 vijf maal zijn geactualiseerd.

Criterium C

Voor de vastlegging van hard- en software zijn diverse registraties in gebruik zoals [redacted] De processen zijn vastgelegd in [redacted] en door DEKRA volgens de ISO 9001en ISO 27001norm gecertificeerd.

Bestaan
Wij hebben gedurende het onderzoek het bestaan van de systemen uit de aangeleverde architectuuroverzichten kunnen vaststellen. Door de beheerders *van* SSC-ICT is door middel van screenprints uit diverse beheersystemen een beeld geschetst van de infrastructuur die ten behoeve van Leonardo wordt ingezet:

Criterium C

- Hardware zoals netwerkcomponenten (switches, reuters, load balancers), servers (applicatie-servers, database-servers), storage (SAN);
- Software (OS, [redacted]), virtualisatie software ([redacted]), applicatiesoftware (bv. [redacted] database, middleware), beheertooling ([redacted]

Criterium C

Door de netwerkbeheerder is aangegeven dat er een preventieve control in de *vorm* van een netwerkauthenticatie protocol via poorten op een lokaal netwerk [redacted] is ingericht waarmee ongeautoriseerde toegang tot het netwerk wordt voorkomen.

Criterium D

Tijdens de bestaansvaststelling van de infrastructuur is vastgesteld dat er van de [redacted] servers één niet In de CMDB aanwezig was. [redacted]

Restrisico

Criterium D

[redacted]

2.2 Op welke wijze worden *1* zijn de Leonardo componenten ingericht bij SSC-ICT? *[subvragen 5-12]*

SANS toelichting
Deze onderzoeksvraag heeft tot doel inzichtelijk te maken welke processen en tools de IT-organisatie gebruikt om componenten veilig te configureren. Dit is belangrijk omdat standaard configuraties van hard- en software in de regel niet veilig zijn. Zo wordt het aanvalsoppervlak van een systeem vergroot als poorten onnodig open staan, fabrieksaccounts en wachtwoorden nog actief zijn, verouderde en kwetsbare protocollen (denk aan de Hartbleedbug) In gebruik zijn etc.

Het ontwikkelen van configuratie settings met de juiste security eigenschappen is een complexe taak, waarbij door de vele configuratiemogelijkheden snel een fout

wordt gemaakt. Zelfs een sterke Initiële configuratie moet worden bijgehouden en bewaakt om de beveiliging up to date te houden.

Opzet

Door de architect van Leonardo is aangegeven dat Leonardo ten opzichte van de bij de start van dit onderzoek overhandigde overzichten is vernieuwd, uitgebreid en verbeterd. Wij hebben tijdens ons onderzoek actuele en afgestemde ontwerpen van het nieuwe ontwerp ingezien.

Door SSC-ICT is aangeven dat er een project loopt om de security baselines in te richten. De verwachte opleverdatum hiervan is Q2 2016.

Bestaan

Criterium C

[redacted] servers:

Er een shellscript waarmee de inrichting van [redacted] servers (incl. de aanwezige beheeraccounts) door een beheerder kan worden gecontroleerd. Deze controle vindt momenteel plaats ten behoeve van de 1e oplevering van een server. Deze controle wordt (nog) niet periodiek over in productie zijnde servers uitgevoerd.

Criterium C

[redacted] wordt via [redacted] geïnstalleerd. De softwarepatches worden via het [redacted]. De securitybaseline van de [redacted] wordt ieder kwartaal geüpdatet op basis van nieuwe informatie van de leverancier. Deze nieuwe baseline vormt het uitgangspunt om de servers te patchen.

Criterium D

[redacted]

[redacted] servers:

1. Er is een lokaal administratoraccount voor het geval de AD faalt en toch toegang moet worden verkregen tot de server. De beheerder verklaart dat de wachtwoorden van deze lokale beheeraccounts in een digitale kluis zijn opgeslagen en alleen bij calamiteiten worden gebruikt.

2. De beheerder heeft verklaard dat [redacted] servers volgens een standaard inrichtingsdocument worden ingericht. Dit inrichtingsdocument is getoond. Bij de inspectie van een [redacted] server is getoond dat het patchlevel op [redacted] stond.

Criterium D

[redacted]

SSC-ICT volgt de securitybaselines van de leveranciers. De implementatie hiervan gaat volgens planning per kwartaal.

Criterium D

[redacted]

Tijdens de bestaansvaststelling op 10 december is een securityscan door het SOC [redacted] uitgevoerd. Hierbij is vastgesteld dat er [redacted].

Criterium D

[redacted] kwetsbaarheden aanwezig zijn.

Criterium D

[redacted]

Restrisico

Criterium D

[redacted]

2.3 Op welke wijze vindt monitoring van deze componenten plaats

SANS toelichting

Deze onderzoeksvraag heeft tot doel inzichtelijk te maken op welke wijze de IT-infrastructuur ten behoeve van Leonardo wordt gemonitoord, teneinde ongeautoriseerde mutaties te detecteren.

Criterium C

[redacted]

Opzet

Uit beantwoording van de deelvragen door SSC-ICT komt naar voren dat de componenten van Leonardo worden gemonitord:

Criterium C

1. netwerk componenten
2. systemen met ;
3 systemen met .

Criterium D

Bestaan

Criterium C

Het SSC-ICT heeft aangegeven dat monitoringtool) op basis van door de leverancier aangeleverde securitybaselines systemen monitort. Dit zal in de toekomst worden uitgebreid voor de bewaking .

Criterium D

Restrisico

2.4 Op welke wijze vindt monitoring van kwetsbaarheden plaats bij SSC-ICT?

[subvragen 13 - 15]

SANS toelichting

Deze vraag heeft tot doel inzichtelijk te maken welke processen en middelen de organisatie gebruikt om kwetsbaarheden In de veiligheid van de configuraties van de netwerkapparaten, servers en opslag ten behoeve van Leonardo te controleren, voorkomen en/of corrigeren. Het belang van deze monitoring is gelegen In het feit dat beheerders worden geconfronteerd met een constante stroom van software updates, security adviezen en berichten over kwetsbaarheden van leveranciers en het Nationaal Cyber Security Center (NCSC) of andere bronnen. Aanvallers beschikken echter over dezelfde Informatie. Zij kunnen de tijd benutten tussen het publiceren van kwetsbaarheden en het daadwerkelijk doorvoeren van correcties voor het plaatsen van een gerichte aanval. Organisaties die niet scannen op kwetsbaarheden en onveilige software configuraties niet proactief adresseren lopen een gerede kans op gecompromitteerde computer systemen.

Opzet

Criterium D

Door SSC-ICT is aangegeven is dat er tools zijn waarmee de kwetsbaarheid van softwareversies en configuraties onderzocht kan worden.

Criterium C

Bestaan

Tijdens het interview met SSC-ICT te Zoetermeer heeft de vertegenwoordiger van het Security Operations Center (SOC) aangegeven dat scanners dagelijks controleren op verdachte patronen. Deze kwetsbaarhedenscanners worden dagelijks voorzien van nieuwe patrooninformatie.

Criterium C

Door het SOC is een toelichting gegeven op de mogelijke scanmogelijkheden. Eén daarvan is de kwetsbaarhedenscan waarbij een zeer gedetailleerd overzicht wordt gegeven van de kwetsbaarheden van een server. Het SOC geeft aan Leonardo systemen uitsluitend te controleren en te rapporteren vanuit de security organisatie.

Criterium D

Wij beschouwen het continue monitoren van de kwetsbaarheden in hard- en software en configuratie een randvoorwaarde voor een veilige dienstverlening.

Restrisico

Criterium D

2.5 Op welke wijze is data-recovery ingericht? *[subvragen 16, 17]*

SANS toelichting

Dataherstel is belangrijk omdat aanvallers na een succesvolle inbraak vaak braakschade in de vorm van aangepaste programma's of gemuteerde data veroorzaken. Zonder een betrouwbare data herstel mogelijkheid kan het erg moeilijk zijn betrouwbare data te herstellen en alle sporen van aanvaller te verwijderen. De organisatie moet daarom een (nood}plan met bijbehorende middelen hebben om een data-recovery beheerst uit te kunnen voeren. Daarnaast bestaat de kans dat data onbedoeld onbruikbaar Is doordat een server op een andere manier defect raakt.

Opzet

Aangegeven door SSC ICT is dat er een project bestaat om business continuity management in te richten om te kunnen uitwijken. De verwachte opleverdatum van dit project is Q1 2016.

Criterium D

Bestaan

Tijdens het interview Is door het SSC-ICT is aangegeven dat van alle systemen een 'full backup' een 'incremental backup' en online archive wordt gemaakt. Van de virtual machines worden snapshots gemaakt. Deze werkzaamheden vloeien voort uit

Criterium C

8

de SLA-afspraken. Restore wordt alleen op verzoek van de klant getest. SSC-ICT heeft geen SLA afspraken om periodiek de restore capaciteit te testen. Aangegeven is dat tijdens het actualiseren van de ontwikkel-, test- en acceptatie (OTA) omgevingen gebruik gemaakt wordt van productie back-ups. Dit is vastgelegd in de clone procedure.

Naast back-ups is er ook redundantie van de verwerkingscapaciteit ingebouwd in Leonardo. Dit blijkt uit de Landschaptekening Leonardo en de daarbij gegeven uitleg

Criterium D

Criterium D

Restrisico

2.6 Op welke wijze is beheerdertoegang ingeregeld? *[subvragen 18 t/m 26]*

SANS toelichting

Het misbruik van administratorrechten is de primaire methode voor aanvallers om toegang te krijgen tot een systeemomgeving. Methodes hiervoor zijn phishingmails of het raden van administratorwachtwoorden op basis van eerder buitgemaakte gegevens.

Criterium D

Opzet

In opzet maakt SSC-ICT gebruik van een apart beheernetwerk ( ). Wij hebben een overzicht van dit netwerk ontvangen hoe dit netwerk is ingericht.

Criterium D

Bestaan

Wij hebben middels een deelwaarneming ter plaatse vastgesteld dat het beheerdernetwerk wordt gebruikt om d.m.v. toegang te krijgen tot de servers. Hierbij is aangegeven dat uit een afgeschermd netwerkdeel (VLAN) bestaat met een eigen Active Directory [9] authenticatie. Voorts is aangegeven dat maandelijks ter verificatie aan de teamleiders een overzicht wordt gezonden van de geautoriseerde gebruikers, waarbij de teamleiders moeten controleren of de rechten van de beheerders nog overeenstemmen met hun taken.

Criterium D

Verder bleek dat de beheerders van de servers lokaal worden geautoriseerd

9 Active Directory is een directoryservice waarmee beheerders rechten en instellingen in het netwerk kunnen beheren. Active Directory slaat instellingen in relatie tot een file of computer op in een database.

Criterium C

De [redacted] beheerders worden via de Active Directory geautoriseerd. Er is lokale noodgebruiker, waarvan het wachtwoord in de (digitale) kluis ligt.

Criterium D

Restrisico
Door de ingerichte beheerprocessen rondom het toekennen, wijzigen en verwijderen van beheerdersaccounts en de maatregelen om het beheerdersnetwerk [redacted]) te beschermen achten wij het risico laag dat adminstratoraccounts worden misbruikt.

2.7 Op welke wijze zijn de boundary defences ingeregeld? [subvragen 27 t/m 31]

SANS toelichting
'Boundary defences' (bescherming van de koppelvlakken) hebben tot doei te voorkomen dat informatie ongecontroleerd de bedrijfsomgeving verlaat. Om deze datastroom te beheersen wordt een architectuur van firewalls, proxies, demilitarised zones en intrusion detection systems (zowel inbound als outbound) ontworpen en onderhouden.

Opzet
Uit de actuele architectuurplaat kan de inrichting van de koppelvlakken zoals firewalls, routers, loadbalancers, packet shapers en demilitarised zones worden afgeleid binnen de justitie-net omgeving.

Bestaan
Het netwerk is gesegmenteerd in VLAN's[10] met behulp van routers. Met de firewalls wordt het verkeer tussen de VLAN's beheerst.

Wij hebben de inrichting van het netwerk vastgesteld. De netwerkbeheerder heeft laten zien hoe pakketten vanaf de werkplek naar Leonardo verstuurd werden. Dit kwam overeen met de tekening van het netwerk.

Restrisico's

Criterium C

De WAN verbindingen worden afgenomen van [redacted] Uit de netwerktekening blijkt dat deze verbinding is versleuteld [redacted]

10 Een Virtual LAN of Virtual Local Area Network (VLAN) is een type virtueel netwerk. Een VLAN wordt gerealiseerd op de datalinklaag. Op deze wijze kunnen logisch gescheiden netwerken gerealiseerd worden die fysieke hardware zoals switches en bekabeling delen.Jn een fysiek netwerk kunnen verschillende VLAN's naast elkaar bestaan.

Criterium C

[redacted]

2.8 Op welke wijze vindt maintenance, monitoring en analyse van de auditlogging plaats? *[subvragen 32 t/m 36]*

SANS 14 Toelichting

Loginformatie bevat vaak waardevolle informatie over mogelijke inbraakpogingen in systemen. Omdat deze informatie vaak niet actief wordt geanalyseerd kunnen aanvallers lange tijd gebruik maken van een kwetsbaarheid, zonder te worden gedetecteerd.

Opzet

Het [redacted] is bezig de securitymonitoring in te bedden in de reguliere beheerprocessen. De technische tooling hiervoor is aanwezig en ingericht. Door de betrokken disciplines ([redacted] worden de relevante logbestanden [redacted] geanalyseerd.

Criterium D

Bestaan

Het SOC houdt zich ondermeer bezig met de volgende taken:

- Monitoren Ir-infrastructuur op dreigingen
- Analyseren van kwetsbaarheden
- Rapportage naar securitymanagement

De verzameling en monitoring van logbestanden vindt door het [redacted] plaats met behulp van [redacted]. Momenteel bevindt zich al een groot deel van de systemen in deze [redacted] omgeving. Volgens SSC-ICT is de migratie van alle logbestanden naar [redacted] nog niet afgerond. Volgens SSC ICT is dit gepland voor QI 2016. Alle beheerde servers en netwerk apparatuur zijn al aangesloten als dit van toepassing is. [redacted]

Criterium C

Criterium D

Restrisico

[redacted]

Criterium D

2.9 Op welke wijze vindt account monitoring en control plaats? *[subvragen 37 t/m 40]*

SANS toelichting

Gebruikersaccounts van medewerkers die vertrokken zijn, kunnen worden misbruikt door andere personen. Aanvallers maken vaak gebruik van bestaande inactieve gebruikersaccounts om zich voor te doen als legitieme gebruikers. Zo maken zij hun gedrag minder zichtbaar voor de netwerk beheerders. Niet verwijderde accounts van tijdelijk personeel of ex-werknemers worden vaak misbruikt voor dit doel.

Opzet

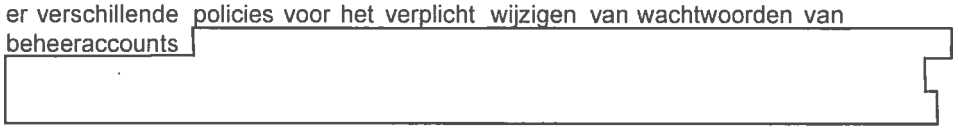
Maandelijks ontvangen de teamleiders van SSC-ICT een overzicht van de verleende autorisaties aan beheerders in hun team. De teamleiders moeten controleren of de

rechten van de beheerders nog overeenstemmen met hun taken. Accounts kunnen maximaal één maand actief blijven. Vertrokken medewerkers kunnen geen gebruik maken van hun accounts aangezien ze geen fysieke toegang tot de panden meer hebben en hun Active Directory account is afgesloten.

Bestaan

Wij hebben een voorbeeld van dergelijk maandelijks overzicht ingezien. Tevens zijn er verschillende policies voor het verplicht wijzigen van wachtwoorden van beheeraccounts

Criterium D



Restrisico

Criterium D

De Audit Dienst Rijk, ADR,
namens deze,

Criterium B