Federal Information Security Policy Guideline

Glossarium

21/11/2019

FISPDOC10 V1.0

Belangrijke opmerking: Dit document is een leidraad die het resultaat is van een samenwerking tussen informatiebeveiligingsexperts van de verschillende federale diensten (FOD, OIP, IPSS). De voorgestelde maatregelen worden beschouwd als minimummaatregelen die redelijkerwijs op een gemeenschappelijke manier van toepassing zijn op alle federale diensten. Deze zijn gebaseerd op internationale normen, goede praktijken op het gebied van informatiebeveiliging en de ervaringen van de deelnemers aan de FISP-werkgroep.

Indien strengere maatregelen vereist zijn voor een federale dienst omwille van reglementaire redenen of om andere formele en dwingende redenen, kan men ervan uitgegaan dat deze maatregelen voorrang hebben op de maatregelen die in deze gids worden beschreven.

FISP Werkgroep

.be

Inhoud van dit document

Oriëntatie van het document

Dit document maakt integraal deel uit van methodologie voor informatiebeveiliging binnen de Federale overheid (FISP project).

Veiligheidsdoel van het document

Het doel is consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten van FISP.

Toepassingsgebied

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle relevante definities gecentraliseerd in dit document.

Vrijwaring

Deze informatie mag niet individueel gebruikt worden als referentie documentatie. De lezer van dit document gebruikt dit document niet als vervanger van wetgeving of standaarden, maar als leidraad bij het nemen van de gepaste beveiligingsmaatregen.

Verantwoordelijkheden

Dit document is bestemd voor de informatieveiligheidsconsulent en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van federale overheid, voor de verwerkers van informatie (ook de onderaannemers van informatiesystemen) en andere belanghebbenden in verwante gebieden (bv. de documentenbeheerder).

Eigenaar

De eigenaar van dit document is de FISP-werkgroep.

Definities

A

Aanval: een poging om ongeautoriseerde toegang te krijgen tot bedrijfsinformatie. Die informatie te lezen, te stelen, te wijzigen, onbruikbaar te maken, of ongeoorloofd gebruik van de bedrijfsinformatie te maken.

Address spoofing: Techniek die het misbruik van IP adressen mogelijk maakt om firewall filters te omzeilen

Actieve sessie: Is een specifieke online omgeving waarin een gebruiker met zijn toepassing/transactie aan het werken is. Een gebruiker kan gelijktijdig in meerdere online omgevingen (of sessies) werken.

Analoge drager: Op een analoge drager worden gegevens op een niet-digitale manier opgeslagen. De meest voor de hand liggende analoge drager is papier.

AVG (GDPR): De algemene verordening inzake gegevensbescherming is een EU-wetgevingstekst die een nieuw rechtskader voor de verwerking van persoonsgegevens vaststelt.

Authentiek: wanneer een entiteit is wat het beweert te zijn.

Authenticeren: het authentiek, rechtsgeldig maken, vaststellen of het echt waar is. In de IT-context, wordt hier vooral mee bedoeld: het vaststellen van de juiste identiteit van een persoon of systeem dat zich aanmeldt bij een ander systeem om toegang te krijgen tot informatie. Garanderen dat een beweerde karaktertrek van een identiteit correct is.

B

Bedreiging: Potentiële oorzaak van ongewenst incident dat een systeem of organisatie schade kan toebrengen.

Bedrijfscontinuïteitsbeheer (Business Continuity Management : BCM) Bedrijfscontinuïteitsbeheer streeft ernaar om de bedrijfsprocessen (bedrijfsactiviteiten) te beschermen tegen onderbrekingen en om, wanneer er zich een onderbreking zou voordoen, te zorgen voor een positieve en effectieve reactie hierop.

Bedrijfsmiddel: Alles wat waarde heeft voor de organisatie (gebouwen, informatie, software, hardware,diensten maar ook mensen, vaardigheden,..).

Beheersmaatregelen: De maatregelen die getroffen worden om risico's te beheersen, kunnen bestaan uit een beleid, procedures, richtlijnen en werkwijzen of organisatiestructuren die administratief, technisch, beheersmatig of juridisch van aard kunnen zijn.

Beleid: de formeel uitgesproken inrichting van informatiebeveiliging en de intentie van de directie betreffende het omgaan met bedrijfsrisico's en de bescherming van de organisatie tegen informatiebeveiligingsrisico's.

Belgische privacywet: De wet van 30 juli 2018, die het GDPR implementeert en een aantal specifieke kenmerken voor België definieert.

Beschikbaarheid van informatie: beschikbaarheid waarborgt de toegankelijkheid en bruikbaarheid op verzoek van een bevoegde entiteit. M.a.w., beschikbaarheid garandeert dat de computersystemen beschikbaar zijn op het moment dat ze nodig zijn om de werkprocessen uit te voeren.

Beveiligde ruimten: Ruimten die fysiek beschermd zijn (bijv. data centers).

C

CISO: CISO staat voor Chief Information Security Officer. Deze maakt deel uit van het topmanagement. Definieert namens het topmanagement het informatiebeveiligingsbeleid en organiseert en stuurt de informatiebeveiliging van de organisatie in overeenstemming met de behoeften en de risicobereidheid van de organisatie.

Cloud computing: Cloud computing is het via het internet beschikbaar stellen van hardware, software, informatie, bestanden en gegevens. Zie het document, “FISP – Cloud beveiliging”.

Cloud Backup: Cloudback-up, of cloud computerback-up, verwijst naar het maken van back-ups van data naar een externe, cloudgebaseerde server. Bij deze vorm van cloudopslag worden cloudback-ups opgeslagen in en zijn deze toegankelijk via meerdere verspreide en verbonden resources, die samen een cloud vormen.

Cloud Backup Service Provider: Een derde partij die voor klanten cloudgebaseerde databack-upservices en -oplossingen beheert en distribueert vanuit een centraal datacenter.

Cloud Broker (Tussenpersoon): Een entiteit die relaties met meerdere clouddienst-providers aangaat en onderhoudt. Fungeert als tussenpersoon voor clouddienst-klanten en clouddienst-providers, waarbij voor elke klant de beste provider wordt geselecteerd en diensten worden gemonitord.

Cloudburst: Cloud bursting is een techniek die door hybride clouds wordt gebruikt om waar nodig aanvullende resources te leveren voor private clouds. Als de private cloud de verwerkingskracht heeft om zijn workloads aan te kunnen, wordt de hybride cloud niet gebruikt. Dit is wat in werking treedt wanneer uw cloud een storing of beveiligingslek heeft en uw data niet beschikbaar is. De term cloudburst wordt op twee manieren gebruikt, zowel negatief als positief:

- Cloudburst (negatief): het falen van een cloud computing-omgeving vanwege het onvermogen om met een piek in vraag om te gaan.
- Cloudburst (positief): de dynamische inzet van een softwaretoepassing, die normaliter op interne computingresources werkt, in een openbare cloud om een piek in vraag aan te pakken.

Cloudcenter: Een datacenter in de “cloud” die gebruik maakt van op standaarden gebaseerde gevirtualiseerde componenten als een datacenter-achtige infrastructuur die zijn infrastructuur huurt.

Cloud Database: Een database die voor clients via de cloud toegankelijk is en die door servers van een cloud database-provider on-demand aan gebruikers wordt geleverd via internet. Ook wel Database-as-a-Service (DBaaS) genoemd. Cloud-databases kunnen cloud computing gebruiken om geoptimaliseerde schaalbaarheid, hoge beschikbaarheid, multi-tenancy en effectieve resourcetoewijzing mogelijk te maken.

Cloud Management: Software en technologieën die ontworpen zijn voor het uitvoeren en monitoren van toepassingen, data en diensten die zich in de cloud bevinden. Cloudmanagement-tools helpen ervoor te zorgen

dat de cloud computing-resources van een bedrijf optimaal werken en goed communiceren met gebruikers en andere services.

Cloud Migratie: Het proces van het verhuizen van alle of een deel van de data, toepassingen en diensten van een bedrijf, van on-site locaties achter een firewall naar de cloud, waar de informatie on-demand via internet kan worden geleverd.

Cloud-Oriented Architecture (Cloud-georiënteerde Architectuur) of COA: Een term die bedacht is door Jeff Barr van Amazon Web Services. Beschrijft een architectuur waarin toepassingen fungeren als diensten in de cloud en andere toepassingen in de cloudomgeving bedienen. Een architectuur voor IT-infrastructuur en softwaretoepassingen die zijn geoptimaliseerd voor gebruik in cloud computing-omgevingen. De term is nog niet wijdverspreid en, zoals in het geval van de term “cloud computing” zelf, bestaat er geen algemene/algemeen aanvaarde definitie of specifieke beschrijving van een cloudgeoriënteerde architectuur.

Cloud Platform: De “middelste” laag van de Cloud Pyramide die een computing-platform of framework (bijv. .NET, Ruby on Rails of Python) levert als dienst of stack. Controle is alleen mogelijk over het platform of framework, maar niet op een lager niveau (serverinfrastructuur). Voorbeelden hiervan zijn: Google AppEngine of Microsoft Azure.

Cloud Portability (Overdraagbaarheid): In cloud (computing)-terminologie betekent de term “cloud portability” de mogelijkheid om toepassingen en bijbehorende data te verplaatsen van de ene cloudprovider naar de andere – of van openbare naar private cloudomgevingen. Zie ook Vendor-lock-in.

Cloudprovider: Een serviceprovider die klanten opslagruimte of softwareoplossingen biedt via een openbaar of privé netwerk.

Cloud Provisioning: De implementatie van de cloud computing-strategie van een bedrijf, waarbij meestal eerst wordt geselecteerd welke applicaties en services in de cloud worden bewaard en welke on-site achter een firewall of in een private cloud blijven. Cloud provisioning omvat ook het ontwikkelen van processen voor interfacing met cloud-applicaties en -diensten, evenals audits en monitoring van wie toegang heeft tot en gebruikmaakt van resources.

Cloud Beveiliging: Dezelfde beveiligingsprincipes die van toepassing zijn op on-site computing zijn ook van toepassing op cloud computing-beveiliging.

Cloud Servers: Gevirtualiseerde servers met Windows- of Linux-besturingssystemen die worden geactiveerd via een webinterface of API. Cloud Servers gedragen zich op dezelfde manier als fysieke servers en kunnen worden beheerd op administrator- of rootniveau, afhankelijk van het servertype en de Cloud Hosting-provider.

Cloud Serverhosting: Cloud serverhosting is een vorm van hosting waarbij hostingdiensten via internet on-demand beschikbaar zijn voor klanten. In plaats van te worden aangeboden door een enkele server of virtuele server, worden cloud serverhostingdiensten geleverd door meerdere verbonden servers die samen een cloud vormen.

Cloud Service Architectuur of CSA: Een term die bedacht is door Jeff Barr van Amazon Web Services. De term beschrijft een architectuur waarin toepassingen en toepassingscomponenten fungeren als diensten in de cloud, die andere toepassingen binnen dezelfde cloudomgeving bedienen.

Cloud Sourcing: Outsourcing van opslag of profiteren van een ander type clouddienst. Het outsourcen van sommige IT-activiteiten naar goedkopere clouddiensten. Voorbeeld: data back-up

Cloud Opslag: Een dienst waarmee de klant data kan opslaan door deze via internet of een ander netwerk over te brengen naar een extern opslagsysteem dat door een derde partij wordt onderhouden. Cloudopslag betekent "Dataopslag online in de cloud", waarbij bedrijfsdata opgeslagen wordt en toegankelijk is d.m.v. meerdere verspreide en verbonden resources die samen een cloud vormen.

Cloud Testing (Testen): Het uitvoeren van load- en prestatietests op de via de cloud computing aangeboden toepassingen en diensten – met name de toegankelijkheid van deze diensten – om optimale prestaties en schaalbaarheid onder uiteenlopende omstandigheden te garanderen.

Control (Maatregel): Middelen voor het managen van een risico. Meestal is dit een technische of organisatorisch beveiligingsmaatregel. Hieronder vallen ook het bedrijfsbeveiligingsbeleid, procedures, richtlijnen en best practices.

D

Data: Elektronische informatie verwerkt door of opgeslagen op informatiesystemen.

Data at rest (DAR) of inactieve data: Data die digitaal opgeslagen ligt op een fysieke of virtuele drager; Opslagmedia, externe gegevensdragers, tapes en virtuele opslagmedia. De vormen van opslag kunnen zijn: bestanden, databases, archieven, off-site back-ups. Opslaglocaties kunnen zijn: fysieke en virtuele servers, (Mobiele) werkstations, Mobiele toestellen, Appliances.

Data in de cloud: Het beheren van data in de cloud vereist databeveiliging en privacy, evenals controle over het verplaatsen van data van punt A naar punt B. Het omvat ook het beheer van dataopslag en resources voor grootschalige dataverwerking.

Data in motion (DIM): Data die overgedragen wordt via een privaat, publiek of bedrijfsnetwerk, onafhankelijk van de drager, bekabeld en draadloos

Data in use (DIU) of actieve data: Data aanwezig in geheugen, dat actief verwerkt wordt of tijdelijk opslagen (technische caching) tijdens de verwerking door een proces of toepassing.

Disaster Recovery (Rampherstel) of DR: DR is de mogelijkheid om toegang te herstellen tot archieven, data, hardware en software, zodat na een ramp belangrijke bedrijfsactiviteiten kunnen worden hervat. Denk hierbij aan rampen in uw faciliteit (bijv. brand in het gebouw, bomdreigingen), lokale rampen (bijv. stroomuitval, overstromingen, aardbevingen) en regionale rampen (bijv. orkanen [orkaan Katrina was ruim 800 km breed], storingen in het elektriciteitsnet). De kosten voor garantie dat u activiteiten kunt hervatten nemen doorgaans toe naarmate de afstand en het aantal disaster recovery-centra toeneemt. Dit is vaak samengebracht met Business Continuity.

Declassificatie: Het wegnemen van de eerder aan informatie toegekende classificatie, waardoor de betreffende informatie vrij toegankelijk wordt.

Denial of service: Een situatie waarin een computersysteem onbedoeld niet beschikbaar is voor de verwachte dienstverlening.

Derde partij: Persoon of organisatie vreemd aan de organisatie, die niet als contractpartij bij een overeenkomst betrokken is.

Digitale drager: Wanneer gegevens op een elektronische manier opgeslagen worden (een representatie van de gegevens in een binaire omzetting) spreken we van een digitale drager.

Distributielijst: Een distributielijst is een de lijst van personen aan wie een document geheel of gedeeltelijk verstuurd of gecommuniceerd mag worden. Personen kunnen fysieke individuele personen zijn of groepen van personen die zich door een specifiek verifieerbaar kenmerk onderscheiden.

DPO: dit staat voor Data Protection Officer ook genaamd de functionaris voor gegevensbescherming.

DPIA: dit staat voor Data Protection Impact Assessment ook genaamd de gegevenbeschermings-effectenbeoordeling.

E

Eigenaar van informatie (informatie-eigenaar): Informatie moet toegekend worden aan een 'eigenaar' die kennis heeft van het gebruik en de waarde van de informatie voor de organisatie, nodig om het classificatieniveau van de informatie te bepalen.

Encryptie: De bescherming van uw informatiemiddelen d.m.v. het transformeren van informatie (onbewerkte tekst) op een manier die het voor iedereen onleesbaar maakt (versleutelde tekst), behalve voor degenen die over een sleutel beschikken.

EU GDPR: European General Data Protection Regulation

Event logging: Dit is het verzamelen van systeem- en gebruikersactiviteiten, system events, fouten en ook gebeurtenissen die de informatiebeveiliging betreffen.

Externe cloud: Openbare of private clouddiensten die buiten de organisatie, door een derde partij worden geleverd. Een cloud computing-omgeving die zich buiten de organisatiegrenzen bevindt.

F

Faciliteiten voor het gebruik van informatie: iedere vorm van een informatiesysteem, service of infrastructuur die gebruikt wordt om informatie op te slaan, te bewerken en te beheren en de fysieke middelen en locaties dienen daarvoor aanwezig te zijn.

FISP: Federal information security policy

Forensisch (onderzoek): Met betrekking tot rechtszaken, gerechtelijk onderzoek.

Fysieke perimeter: Een fysieke perimeter is een fysieke barrière, die verhindert dat ongeoorloofde personen deze barrière binnendringen. Het bestaan van een fysieke perimeter gaat dus samen met het verlenen van toegang aan bevoegde personen. Dit kan op verschillende manieren, bijv. door een sleutel of een badgesysteem. In het

kader van dit beleid wordt ervan uit gegaan dat de fysieke perimeter afdoende beveiligd is tegen indringing door onbevoegden.

G

Gecompromitteerde sleutel: Een sleutel waarvan niet gegarandeerd kan worden dat deze enkel geautoriseerd gebruikt kan worden.

Gebruikers van informatiesystemen: Alle interne en externe medewerkers, geautomatiseerde diensten en applicaties en externe partijen (bv. andere organisaties) en klanten (bv. personen, ondernemingen, instellingen).

Gegevensbeschermingseffectbeoordeling: analyse van onderdelen van processen en het effect dat een onderbreking van activiteiten daarop kan hebben .

Gegevensbeschermingsautoriteit: elke EU-lidstaat moet een of meer toezichthoudende autoriteiten oprichten om toezicht te houden op de toepassing van de verordening en moet het contactpunt zijn voor elke vordering van de betrokkene.

Gegevensverantwoordelijke : Dit is een natuurlijke of rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt.

Gegevensverwerker : Dit is een natuurlijke of rechtspersoon die uitsluitend op basis van een schriftelijke overeenkomst persoonsgegevens verwerkt voor rekening van de verantwoordelijke voor de verwerking.

Geprivilegieerde toegangsrechten: De toegangsrechten die benodigd zijn om wijzigingen binnen het RBAC-model uit te voeren of om systeemwijzingen uit te voeren (systeembeheer).

Gestandaardiseerde interfaces: Clouddiensten zouden gestandaardiseerde API's moeten hebben, die instructies geven over hoe twee applicatie- of gegevensbronnen met elkaar kunnen communiceren.

Gevoelige gegevens: Gevoelige gegevens zijn die gegevens die door de eigenaar van de gegevens als dusdanig geclassificeerd worden. Algemeen beschouwd mogen gevoelige gegevens niet aan het publiek gecommuniceerd worden maar uitsluitend aan de betrokken persoon of onderneming. In functie van de classificatie zijn deze gevoelige gegevens duidelijk gedefinieerd, zijn er gebruiksregels gedefinieerd, en worden zij slechts gebruikt door een relatief beperkte groep van de medewerkers.

H

Handleiding: hiermee bedoelt men richtlijnen die men als adviseren dient te beschouwen. Ze moeten niet per se op die manieren opgevolgd worden. Het zijn hulpmiddelen die een bepaalde richting geven aan een werkwijze.

Hoge risico omgeving: Omgevingen die een hoger risico lopen op vlak van informatieveiligheid. Bv. omgevingen die een gegevenstrafiek genereren over een publiek netwerk (zoals VPN verbindingen).

Hybride cloud: zie het document, "FISP – Cloud Beveiliging".

I

IAAS: Infrastructure As A Service – Zie het document, "FISP – Cloud Beveiliging".

IAM: Identified Access Managent – Zie het document, “FISP – IAM en PAM”.

ICT Continuïteitsbeheer: ICT Continuïteitsbeheer verzekert dat vereiste informatie- en communicatietechnologie en diensten weerbaar zijn en kunnen hersteld worden tot op vooraf gedefinieerde niveaus, én binnen tijdschalen zoals vereist door de business. ICT Continuïteitsbeheer ondersteunt het overkoepelend Bedrijfscontinuïteitsbeheerproces (Business Continuity Management (BCM)) van een organisatie.

Identiteitsbeheer: Het beheer van persoonlijke identiteitsgegevens, zodat toegang tot computerresources, toepassingen, data en diensten op de juiste manier wordt gecontroleerd.

Informatie: Informatie is een bedrijfsmiddel dat, zoals elk ander belangrijk bedrijfsmiddel, gepast beschermd/beveiligd moet worden. Informatie kan verschillende vormen aannemen, zoals geschreven, gedrukte, elektronische of gesproken informatie. Als informatie wordt opgeslagen in een computersysteem, wordt er meestal verwezen naar data.

Informatiebeveiliging: het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Daarbij kunnen ook andere eigenschappen zoals authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid een rol spelen.

Informatiemiddel: alle elementen/middelen die bij het creëren, ontvangen, verwerken, opslagen, verdelen, verzenden, dupliceren, en vernietigen van informatie van waarde zijn voor de organisatie; informatie die kan opgeslagen worden op verschillende informatiedragers en in verschillende informatiesystemen.

Informatieveiligheidsgebeurtenis: Een waargenomen verandering in de normale werking van een systeem, omgeving, proces of persoon, die gerelateerd is aan een mogelijke inbreuk van het informatieveiligheid, het falen van controle maatregelen, een voordien nog onbekende situatie die relevant kan zijn in het kader van informatieveiligheid.

Informatieveiligheidsincident: Een of meerdere niet gewenste informatieveiligheidsgebeurtenissen met een significante kans om de dienstverlening van de organisatie te verstoren en de informatieveiligheid in gedrang te brengen.

Informatieveiligheidsincidentmanagement: processen voor het opsporen, rapporteren, beoordelen, beoordelen, beantwoorden, behandelen en leren van, en het leren van informatieveiligheidsincidenten.

Informatieveiligheidsmanagement: Alle gecoördineerde activiteiten die richting geven aan het beleid van een organisatie ten aanzien van risico’s. Risicomanagement omvat normaal gesproken risicoanalyses, het nemen van beveiligingsmaatregelen, het accepteren van risico’s tot een bepaald niveau en het communiceren van risico’s binnen de organisatie.

Informatiesystemen: Alle netwerken en ICT systemen, inclusief applicaties, onder het beheer van de organisatie.

Informatieveiligheid: Informatieveiligheid is het beschermen van informatie tegen een breed scala van dreigingen. De integriteit, vertrouwelijkheid en beschikbaarheid van informatie zijn drie aspecten die hierin centraal staan.

Inherent risico: de waarschijnlijkheid dat een negatieve impact zich zal voordoen wanneer er geen beschermingsmaatregelen genomen worden

Integriteit van informatie: Integriteit gaat over de eigenschap van nauwkeurigheid en volledigheid. Het gaat er om te waarborgen dat de informatie betrouwbaar is en dat er geen ongeautoriseerde modificatie van informatie is.

Interne gegevens: alle gegevens waarvan het gebruik beperkt moet worden tot binnen de eigen organisatie. Deze gegevens zijn niet bestemd voor publieke bekendmaking zonder voorafgaande goedkeuring door een bevoegd personeelslid van de organisatie.

Intrusion Detection System (IDS): Een geautomatiseerd systeem dat pogingen of voorvallen van niet geautoriseerde toegang tot een informatie systeem of netwerk detecteert.

Intrusion Prevention System (IPS): Een geautomatiseerd systeem dat pogingen of voorvallen van niet-geautoriseerde toegang tot een netwerk blokkeert.

IP of internet Protocol: IP definieert de manier waarop datapakketten, ook wel datagrammen genoemd, tussen bestemming en bron worden verplaatst. Technisch gesproken kan dit worden gedefinieerd als het netwerklaagprotocol in de TCP/IP-communicatieprotocolsuite.

ITIL: staat voor Information Technology Infrastructure Library. Dit is een reeks van de beste praktijkoplossingen en concepten als referentiekader voor het inrichten van beheersprocessen binnen een ICT-organisatie.

K

Kritieke IT- of informatiesystemen: Op basis van een risico analyse moet bepaald worden of een IT- of informatiesysteem als kritiek beschouwd moet worden. Kritiek dient beschouwd te worden vanuit het belang van een IT- of informatiesysteem in het vrijwaren van vertrouwelijkheid, integriteit of beschikbaarheid van gegevens en IT dienstverlening.

Kritieke zone/ ruimte/ apparatuur: Elke organisatie zal op basis van een Business Impact Analyse moeten bepalen welke ruimtes het meest risicovol en bijgevolg kritiek zijn. Men zal hierbij ook gebruik maken van de BIV klasse: Beschikbaarheid, Integriteit en Vertrouwelijkheid.

Kritische toepassingen: Zonder de kritische toepassingen is een organisatie niet in staat om de dagdagelijkse activiteiten uit te voeren.

L

LAN: Een groep computers en bijbehorende apparaten die een gemeenschappelijke communicatielijn of draadloze verbinding delen en meestal de resources van één processor of server delen binnen een klein geografisch gebied (bijv. binnen een kantoorgebouw).

Logische perimeter: Een logische perimeter is een barrière op het niveau van informatiesystemen, die verhindert dat ongeoorloofde personen of applicaties deze barrière binnendringen. Het bestaan van een logische perimeter vereist dus het verifiëren van de identiteit, het controleren van de autorisatie en het filteren van de gegevens.

M

Mobiele apparaten: De verzamelnaam voor smartphones, tablets, notebooks en laptops.

Mobile device management (MDM): Software die het mogelijk maakt om apparaten op afstand uit te schakelen, informatie te wissen of te blokkeren in geval van diefstal of misbruik

Multi-Tenant: Multi-tenant is een in cloud computing gebruikte term voor het beschrijven van meerdere klanten die dezelfde openbare cloud gebruiken.

Multitenancy: Multitenancy is het op dezelfde fysieke hardware hosten van eigendom van verschillende bedrijven, dat bestaat uit meerdere systemen, applicaties en/of data. Multitenancy komt voor op de meeste cloudgebaseerde systemen.

N

Naleving: Niet-naleving van deze beleidslijnen kan ernstige veiligheidsrisico's met zich meebrengen met betrekking tot de vertrouwelijkheid, integriteit en beschikbaarheid van (gevoelige) gegevens, en het imago en reputatie van de organisatie. De vaststelling dat het beleid en de bijhorende procedures niet gerespecteerd worden, kan leiden tot sancties of zelfs juridische vervolging.

O

Openbare Cloud: zie het document, "FISP – Cloud Beveiliging".

Openbare Cloudopslag: Een vorm van cloudopslag waarbij de onderneming en de opslagserviceprovider gescheiden zijn en data buiten het datacenter van de onderneming opgeslagen wordt.

Operationeel informatiebeheerder: Een operationele beheerder van informatie is een persoon, of een departement, aangeduid door ofwel de organisatie of door de proceseigenaar, die verantwoordelijk is voor het implementeren en operationeel beheren van de nodige beveiligingsmaatregelen in functie van het classificatieniveau bepaald door de proceseigenaar. In de praktijk kan een operationele beheerder van informatie bijvoorbeeld een ICT systeembeheerder zijn, een toepassingsontwikkelaar, een verantwoordelijke voor gebouwenbeheer, enz.

Opslag: het bewaren van gegevens op een drager (opslagmedium). Vanuit de opslag kan een verwerking gebeuren.

Overeenkomst: Schriftelijke afspraken tussen de organisaties en een derde partij over werken, leveringen en diensten die geleverd worden door derde partijen aan de organisatie en/of omgekeerd.

P

PAAS: Platform As A Service – Zie het document, FISP – Cloud beveiliging.

PAM: Privileged Access Management – Zie het document, FISP – IAM en PAM

Patch: een aanpassing/update van ofwel een bestaande software op basis van een programmacode ter correctie en/of verbetering van zwakheden of fouten, ofwel van netwerkapparatuur en/of netwerkbekabeling.

Permissies: bepalen welke acties de gebruiker kan uitvoeren in een applicatie of systeem.

Persoonsgegevens: de persoonsgegevens zijn elke informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon ("betrokkene"); als identificeerbare natuurlijke persoon wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer, een identificatienummer, locatiegegevens, een online-identificatienummer of een of meer specifieke factoren die kenmerkend zijn voor de fysieke, fysiologische, genetische, mentale, economische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Preventieve actie: Dit is een maatregel genomen om een incident te voorkomen (o.a. firewall en antivirus maatregelen).

Privacy by Design: Het principe van privacy by design, vermeld in de AVG, vraagt van elke organisatie om vanaf het begin van elk project of proces passende veiligheidsmaatregelen te nemen om de persoonsgegevens te bewaren en te beschermen.

Privacy Risk Assessment (PRA) : zie gegevensbeschermingseffectbeoordeling

Private cloud: zie het document, “FISP – Cloud Beveiliging.

Private Cloud Beveiliging: Een private cloud-implementatie is bedoeld om veel van de bezwaren tegen cloud computing-beveiliging weg te nemen. Omdat een private cloud-setup veilig in de bedrijfsfirewall is geïmplementeerd, blijft deze onder controle van de IT-afdeling.

Private Cloudopslag: Een vorm van cloudopslag waarbij bedrijfsdata en cloudopslagresources zich zowel binnen het datacenter van de onderneming als achter de firewall bevinden.

Procedures: ondersteunen de specifieke beleidsdocumenten door de desbetreffende beleidslijnen om te zetten naar specifieke operationele taken (hoe er beveiligd moet worden).

R

Recovery Point Objective (RPO): De maximale periode waarin het aanvaardbaar is om data te verliezen.

Recovery Time Objective (RTO): Het tijdbestek na uitval van een systeem waarin systemen en data moeten worden teruggezet naar een eerder vastgesteld punt.

Rechten van de betrokkene (AVG): Elke betrokkene heeft nieuwe rechten en kan aan elke organisatie vragen om zijn/haar rechten toe te passen. Dit omvat het recht op Informatie en toegang tot persoonsgegevens; Correctie en uitwissing van de gegevens; Bezwaar tegen direct marketingpraktijken; Bezwaar tegen geautomatiseerde besluitvorming en profilering; Overdraagbaarheid van de gegevens.

Relatiebeheer: Het beheren van de relatie met een derde partij die toegang heeft (of zal verkrijgen) tot informatie en/of informatiebedrijfsmiddelen van de organisatie, en/of informatie en/of informatiebedrijfsmiddelen aanlevert (of zal aanleveren) aan de organisatie.

Restrisico (residual risk): Het risico dat overblijft nadat beveiligingsmaatregelen genomen zijn. Het is vaak onmogelijk om risico’s volledig uit te sluiten, het is meestal wel mogelijk om risico’s tot een aanvaardbaar niveau terug te brengen. Het kleine geaccepteerde risico is het rest risico.

Risico: de kans (“waarschijnlijkheid”) dat een bepaalde bedreiging zich voordoet met een welbepaalde impact (“ernst”) tot gevolg.

Risicobeheer: Gecoördineerde activiteiten om een organisatie sturing te geven en te bewaken met betrekking tot risico’s.

Risico-evaluatie: Het geheel van procedures dat er toe strekt om risico’s te identificeren, analyseren en evalueren.

Risicobeoordeling: Proces waarin het ingeschatte risico wordt afgewogen tegen vastgestelde risicocriteria om te bepalen in welke mate het risico en/of de omvang ervan aanvaardbaar of verdraaglijk is.

Risicoprofiel: het resultaat van de risico analyse van de organisatie. Binnen de risico analyse worden - op basis van de impact en waarschijnlijkheid van bedreigingen op vlak van informatieveiligheid - de risico’s bepaald. Alle risico’s samen vormen het risicoprofiel van de organisatie.

Role-based access control (RBAC): Een methode waarmee op een effectieve en efficiënte wijze toegangscontrole voor informatiesystemen kan worden ingericht, waarbij gebruikers gekoppeld worden aan voor-gedefinieerde bedrijfsfuncties, die bestaan uit diverse rollen, waarvan elk een specifieke set permissies heeft.

Roleigenaar: Verantwoordelijke voor een rol in het RBAC-model, bestaande uit een specifieke set permissies en gekoppeld aan één of meerdere functies.

S

SaaS : Software As A Service - Zie het document – “FISP – Cloud beveiliging”

Security Incident en Event management (SIEM): Een term voor software producten en diensten die data over gebeurtenissen en incidenten, die een invloed op de veiligheid kunnen hebben, verzamelen in een centraal overzicht en deze analyseren.

Security Incident Response Team (SIRT): Team van medewerkers dat moet optreden wanneer er bepaalde informatiebeveiligingsincidenten zich voordoen. In functie van het type informatiebeveiligingsincident kan dit team telkens uit verschillende personen bestaan.

Service Level Agreement (SLA): Een contractuele overeenkomst waarin een serviceprovider het serviceniveau, de verantwoordelijkheden, prioriteiten en garanties m.b.t. beschikbaarheid, prestaties en andere aspecten van de service, definieert.

Serviceprovider: Het bedrijf of de organisatie die een openbare of private clouddienst levert.

Systeemeigenaar: Verantwoordelijke voor een of meerdere informatiesystemen onder het beheer van organisatie.

Systemen van gebruikers: Alle systemen die toegekend zijn aan een individuele gebruiker en uitsluitend gebruikt worden door deze persoon.

T

Token: Een authenticatiemiddel dat gebruikt wordt om de identiteit van de gebruiker te controleren. Een token bestaat meestal uit reeks cijfers die onderdeel uit maken van een wachtwoord. (bv. token die burgers zelf kunnen aanvragen, de elektronische token die aan de medewerkers van de organisatie verstrekt wordt).

Transactie: Een transactie is een automatische uitwisseling van data tussen IT systemen zonder tussenkomst van een gebruiker. Vb. uitwisseling van data met andere overheidsinstellingen.

Transport: Onder fysiek transport van gegevens wordt het verplaatsen van de drager (dus zowel analoge als digitale opslagmedia) bedoeld of het verplaatsen van de apparatuur waarin deze drager zou geïntegreerd zijn. Impliciet is er dan automatisch ook sprake van mobiele opslagmedia. Onder elektronisch transport wordt het kopiëren of het behandelen van dat via een telecommunicatienetwerk bedoeld. Bij elektronisch transport gaat het uitsluitend over digitale gegevens. Eigen aan elektronisch transport is dat men niet het opslagmedium zelf, maar een kopie van de data verplaatst.

Twee-factor authenticatie (TOTP): Een authenticatie methode die gebruik maakt van een combinatie van twee verschillende manieren om de identiteit van de gebruiker te bevestigen (bv. Geld afhalen door gebruik te maken van een bankkaart en een pincode).

Toegangscontrole: middelen om ervoor te zorgen dat de toegang tot activa geautoriseerd is en beperkt is op basis van bedrijfs- en veiligheidseisen.

U

UPS: UPS staat voor Uninterruptible Power Supply. Dit is de noodstroomvoeding die in werking treed wanneer de gebruikelijke primaire voeding uitvalt.

V

Veiligheidsconsulent: een functie verantwoordelijk voor het onderhoud en ontwikkeling van de beveiligingsstrategie van de organisatie en dit in overeenstemming met de geldende wetgeving en de minimale normen waarop de organisatie zich baseert. Hij/zij rapporteert verplicht formeel één keer per jaar aan de directie

Veiligheidsmatrix: Een model dat gebruikt wordt voor het beheren van de toegangsrechten op basis van de permissies, rollen en functies voor applicaties.

Vendor lock-in: Afhankelijkheid van een bepaalde cloud-leverancier en problemen bij het overstappen van de ene leverancier naar de andere, vanwege een gebrek aan gestandaardiseerde protocollen, API's, datastructuren (schema) en servicemodellen.

Vernietiging: zeker stellen dat elk spoor van data of informatie op een gegevensdrager verdwenen is, of de gegevensdrager zelf in voldoende mate vernietigd is, en de data of informatie van dezelfde bron niet terug zichtbaar of leesbaar kan gemaakt worden. Vernietiging van bijvoorbeeld documenten kan door versnippering, of door het verzamelen in speciale 'containers'. De inhoud van deze containers wordt door een gespecialiseerde firma vernietigd. Vernietiging van originele gegevens kan uitsluitend met medeweten van de eigenaar en rekening houdend met de wettelijke bepalingen die erop van toepassing zijn. De actie van de vernietiging moet het voorwerp uitmaken van een autorisatie.

Vertrouwelijkheid van informatie: Eigenschap dat informatie niet beschikbaar wordt gesteld of wordt ontsloten aan onbevoegde personen, entiteiten of processen.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (Bron AVG).

Verwerking: elke bewerking of elk geheel van bewerkingen met betrekking tot informatie, al dan niet uitgevoerd met behulp van geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.

Verwerkingsverantwoordelijke: De verwerkingsverantwoordelijke bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt. Als uw organisatie dus beslist “waarom” en “hoe” persoonsgegevens moeten worden verwerkt, is zij de verwerkingsverantwoordelijke (Bron AVG).

Virtual Private Cloud (VPC): Een private cloud die bestaat binnen een gedeelde of publieke cloud.

Documentbeheer

Historiek

Datum	*Auteur*	*Versie*	*Omschrijving wijzigingen*
28/10/2019	BOSA	v0.1	Eerste draft
05/11/2019	BOSA	V0.2	Toevoeging begrippen. O.a. CISO, data in rest,… Verwijdering van link met andere beleid
21/11/2019	FISP workgroup	V1.0	Publieke verspreiding

Goedkeuringen

Datum	*Approver(s)*	*Versie*
21/11/2019	FISP FISP workgroup	V1.0

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/mnm_minimale_normen_definities.pdf
- IEC 27000:2018
- “Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002”, Van Haren Publishing.