Beleidslijn informatieveiligheid en privacy

Logbeheer

(BLD LOG)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

Informatiesystemen en ICT-infrastructuur genereren log-informatie voor veel activiteiten, soms als normale statusmelding, soms als resultaat van een activiteit van een gebruiker of beheerder maar ook informatie als resultaat van onvoorziene omstandigheden of fouten.

Een log beschrijft wat er gebeurt in systemen. Tegenwoordig zijn de beschrijvingen van systemen soms zo gedetailleerd dat ze beschrijven waarom een gebeurtenis heeft plaatsgevonden. Logging stelt een organisatie in staat om transacties te volgen en te controleren. Veel computersystemen gebruiken logging om informatie op te slaan over foutsituaties en andere gebeurtenissen die aandacht behoeven van de gebruiker of beheerder. Een log kan geschreven worden in tekst bestanden maar ook in databank tabellen. De doelstelling van logging is het verzamelen en beoordelen van systeem data en waarschuwingen van bijvoorbeeld applicaties, netwerk infrastructuur, servers en desktops.

Logbeheer wordt dikwijls als een kostenpost gezien. Maar een goede logbeheeroplossing is vergelijkbaar met een verzekeringscontract: je hebt het nodig en je betaalt ervoor, maar je gebruikt het niet tot er een incident gebeurt. Goed logbeheer is ook meer en meer noodzakelijk om te kunnen voldoen aan wettelijke en regelgevende vereisten, bijvoorbeeld om een privacy-audit op een informatiesysteem uit te voeren. De vereisten die gesteld worden aan logbeheer worden zwaarder naarmate het belang hoger wordt[1].

Processen worden meer en meer geautomatiseerd en ook autorisaties vinden steeds vaker digitaal plaats. Door logbeheer te automatiseren, kan een organisatie grote schaalvoordelen realiseren, maar er zijn ook risico's. Als bij een volledig digitale log data verloren gaat, dan kan de organisatie niet meer terugvallen op papieren autorisaties of documenten. Een organisatie die logbeheer automatiseert zal moeten investeren in een goede veiligheid van data en een backup/herstelprocedure. Een ander aandachtspunt bij het automatiseren van logbeheer is het doorvoeren van de functiescheiding binnen geautomatiseerde systemen. Als de functiescheiding binnen de organisatie niet goed wordt verwerkt in de software, bijvoorbeeld door gebruik te maken van generieke (anonieme) gebruiker-accounts, dan kan een wijziging niet herleid worden naar een individueel persoon en is de waarde van logbeheer beperkt.

In dit document worden de beleidslijnen voor logbeheer beschreven.

[1] Zie hiervoor de beleidslijn omtrent data classificatie

2. Logbeheer

Elke organisatie onderschrijft de volgende beleidslijnen van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie.

1. De organisatie dient een formele procedure van logbeheer op te zetten, te valideren, te communiceren en te onderhouden.
2. De organisatie moet transacties, controlewerkzaamheden, activiteiten van gebruikers, uitzonderingen en informatieveiligheid- en privacy-gebeurtenissen/incidenten gestructureerd vastleggen in afzonderlijke logbestanden, zodat iedere handeling naar de brondocumenten herleid kan worden of uitgevoerde bewerking(en) gecontroleerd kan worden.
3. Logbeheer moet meegenomen worden vanaf het design tijdens de ontwikkeling of bij de bepalingen van aankoopcriteria van toepassingen of systemen om “security/privacy by design” te realiseren.
4. Elke toegang tot gegevens met gevoeligheidsklasse vertrouwelijk of hoger, moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving.
5. De interne klokken van alle informatiesystemen van de organisatie dienen gesynchroniseerd te worden met een overeengekomen nauwkeurige tijdsbron dat een betrouwbare analyse van logbestanden op verschillende informatiesystemen altijd mogelijk is.
6. De noodzakelijke tools moeten beschikbaar zijn of ontwikkeld worden om log gegevens te kunnen uit te baten en te laten analyseren door de geautoriseerde personen. Via de tools moet het mogelijk zijn om de logs snel, glashelder en eenvoudig te kunnen raadplegen.
7. Zoveel als mogelijk wordt systeemgebruik automatisch gelogd, als dit niet mogelijk is kan ook gebruik gemaakt worden van een manueel logboek door systeembeheerders.
8. Logbestanden dienen beschermd te worden tegen inzage door onbevoegden, wijzigingen en verwijderingen.
9. De logbestanden moeten gedurende een overeengekomen periode worden bewaard, ten behoeve van toekomstig onderzoeken en controles en in overeenstemming met wetgeving en regelgeving . In het bijzonder dienen de privacy logs minstens 10 jaar bewaard worden.
10. De kwaliteit van de privacy log dient een gepast antwoord te bieden om het gebruik te rechtvaardigen (al dan niet gebaseerd op een voorafgaandelijke autorisatie of machtiging). De log dient per verwerking een aanduiding te bevatten van wie wanneer over wie welke persoonsgegevens heeft verwerkt voor welke doeleinden en met welk resultaat (OK,NOK).
11. De raadpleging van logbestanden is altijd het voorwerp van een georganiseerde procedure binnen de organisatie met een historiek van de verzoeken die werden goedgekeurd/uitgevoerd of die werden afgekeurd.
12. Het resultaat van logbeheer moet regelmatig geanalyseerd, gerapporteerd en beoordeeld worden.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2004	JM Gossiaux	1.0	Eerste versie	26/03/2004	01/04/2004
2004	JM Gossiaux	2.0	Tweede versie	15/09/2004	01/10/2004
2005	JM Gossiaux	3.0	Derde versie	16/02/2005	01/03/2005
2005	JM Gossiaux	4.0	Vierde versie	03/11/2005	15/11/2005
2005	JM Gossiaux	5.0	Vijfde versie	10/11/2005	01/12/2005
2006	JM Gossiaux	6.0	Zesde versie	01/06/2006	01/07/2006
2017	M. Vael	V2017	Integratie EU GDPR	07/03/2017	07/03/2017
2018	Werkgroep policy	V2018	Aanpassingen retentietijden, type logs en samenstelling privacy logs	06/02/2018	01/01/2019

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- SANS, “Information Logging Standard”, Juni 2014, 4 blz.
- NIST, “Guide to computer security log management”, September 2006, 72 blz.

Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
- http://www.isaca.org/cobit
- http://cee.mitre.org/

Bijlage C: Richtlijnen voor veilig logbeheer

Hierna volgen richtlijnen voor de organisatie om een degelijk logbeheer uit te voeren.

Verantwoordelijkheden omtrent logbeheer

De verantwoordelijkheid voor het organiseren van informatieveiligheid en privacy ligt steeds bij de organisatie die eigenaar is van de informatieverwerkende toepassing (de verwerkingsverantwoordelijke) . Deze verantwoordelijkheid houdt voor de eigenaar van de toepassing de noodzaak in om te zorgen voor de implementatie van een georganiseerde procedure inzake informatieveiligheids- en privacy-logbeheer.

Als het gaat over een toepassing met gedeelde verantwoordelijkheden (gezamenlijke verwerkingsverantwoordelijken), dan is elke partner-organisatie medeverantwoordelijk voor de implementatie van logbeheer.

Indien informatieverwerkende opdrachten aan derden (verwerkers) worden toevertrouwd, dan kan de organisatie de verantwoordelijkheden en verplichtingen omtrent logbeheer vastleggen in een Service Level Agreement (SLA) of in een contract, maar de derden dienen steeds de gepaste organisatorische, procedurele en technologische maatregelen te treffen conform de geldende wetten en regelgevingen.

Organisatie van logbeheer

De organisatie van logbeheer moet een traceerbaarheid van de gebruikte persoonsgegevens garanderen: de gebruikte toepassingen, de verrichte bewerkingen en de gebruikte informatie garanderen. Zij moeten de link garanderen tussen de gebruiker en de gebeurtenis.

De organisatie van logbeheer omvat ook de uitvoering van alle taken die borg staan voor een duurzaam beheer van alle logbestanden gedurende de levenscyclus van de log.

Bijzondere aandacht wordt besteed aan de volgende aspecten:.

1. de beveiligde inzameling,
2. de bewaring en de archivering in een bruikbaar formaat en op bruikbare dragers die elk risico op vervalsing tot een minimum beperken,
3. de alarmprocedure wanneer belangrijke feiten zoals de onmogelijkheid om de logbestanden te traceren, aan het licht worden gebracht,
4. de controle naar de integriteit van de geïmplementeerde maatregelen,
5. de beheerprocedures.

Kwaliteit van logbeheer

In het logbeheer van privacy logs moeten minimaal de volgende zes vragen beantwoord kunnen worden:

1. Welke activiteit had plaats? (Wat) (operatie)
2. Wanneer gebeurde de activiteit? (Wanneer) (Datum/tijd)
3. Wie voerde de activiteit uit? (Welke organisatie) (Wie)
4. Met welk systeem gebeurde de activiteit? (Hoe) (Applicatie ID)
5. Op welk object voerde de activiteit iets uit? (Over wie) (De betrokkene van de verwerking)
6. Wat was het resultaat/de status van de activiteit? (Gelukt / mislukt)

De volgende informatie is zeer wenselijk bij privacy logs :

7. Het waarom? (Detail van de activiteit / finaliteit)
8. De end-of-life datum van de log (Retention time)
9. Welke transactie aan de hand van uniek nummer? (Wat) (Transaction ID)

Log verplichtingen

a. Een organisatie dient een formele procedure van logbeheer op te zetten, te valideren, te communiceren en te onderhouden:

1. een werkend log systeem,
2. de controle op de naleving van de procedure en op de inhoud van de logbestanden,
3. het beheren, het bewaren, het archiveren en het verwijderen van de informatieveiligheids- en privacy-logbestanden na het verstrijken van de bewaarduur ervan,
4. de beslissing om de loggegevens op te nemen in het continuïteitsplan van de organisatie,
5. de gecontroleerde toegang tot de loggegevens.
6. de organisatie moet als eigenaar van de toepassing de informatieveiligheids- en privacy-logbestanden voorzien en beheren. Bijvoorbeeld op het niveau van de transactionele monitor, het besturingssysteem, het beheersysteem van de machtigingen, het beheer en de bijwerking van de gegevensbanken
7. de organisatie moet periodiek controles verrichten om de naleving van de maatregelen die op haar betrekking hebben te vergewissen.
8. elke gebruiker van een toepassing van de sociale zekerheid of van een toepassing die mogelijk wordt via de sociale zekerheid als knooppunt binnen het netwerk van de Sociale Zekerheid moet worden ingelicht over het feit dat er logbeheer geschiedt en over de doelstelling ervan.

b. De gebruiker van de sociale zekerheid is verplicht de instructie en de procedures na te leven die in de sociale zekerheid of binnen andere netwerken van toepassing zijn

c. Voor de toepassingen op de portaal van de sociale zekerheid en van eHealth wordt de basisdienst voor logbeheer gebruikt

Elke aanvraag tot gebruik van een alternatieve procedure ten opzichte van logbeheer moet grondig worden gemotiveerd en gerechtvaardigd bij de organisatie die eigenaar is van de toepassing.

Automatisering van logbeheer

Bij de automatisering van logbeheer spreekt men dikwijls bij veiligheid logbestanden over SIM (security information management), SEM (security event management) en SIEM (Security Information and Event Management).
Op technisch vlak bestaan er een aantal goede praktijken, bijvoorbeeld over welke protocols je gebruikt, op welke manier je je logbestanden verstuurt en ontvangt, enzovoort. De processen rond logbeheer zijn niet eenvoudig: het is niet zomaar alle logbestanden van de servers naar de centrale logbeheeroplossing sturen en laten analyseren. Er zijn veel gegevensbronnen die irrelevant zijn. Daarom moet eerst gekeken worden naar welke gegevensbronnen er beschikbaar zijn en welke daarvan relevant zijn. Wat niet relevant is, wordt niet gecentraliseerd.
Van de relevante gegevensbronnen worden voorbeelden gemaakt die formeel omschrijven welke gebeurtenissen er moeten gebeuren om een extra actie te activeren. De behoeften van de organisatie zijn cruciaal bij logbeheer automatisering.

Definities en retentietijd

- Technical / infrastructurele logs :

Logs aangemaakt voor het technische analyseren en het technisch herstellen van ICT assets . Wenselijke retentietijd 6 maanden tenzij er andere wettelijke bepalingen zijn die een langere bewaartermijn voorzien.

- Business logs (transactionele logs) :

Logs aangemaakt voor het analyseren en het herstellen van business transactionale systemen . Wenselijke retentietijd 2 jaar tenzij er andere wettelijke bepalingen zijn die een langere bewaartermijn voorzien.

- Veiligheids logs :

Logs aangemaakt met als doel om beveiligingsgebeurtenissen en -incidenten te detecteren en / of te analyseren. Wenselijke retentietijd 5 jaar tenzij er andere wettelijke bepalingen zijn die een langere bewaartermijn voorzien..

- Privacy logs :

Logs aangemaakt om te voldoen aan en te beantwoorden op privacy regelgeving. Retentietijd zie hfst. logbeheer.

Bijlage D: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	
Organisatie van de informatieveiligheid.	
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	**Ja**
Leveranciersrelaties	
Beheer van veiligheidsincidenten	**Ja**
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	**Ja**

***** EINDE VAN DIT DOCUMENT *****