Tactisch beleid Logging

Datum: 09 April 2021

Materieel toepassingsgebied

Dit document beschrijft het tactische beleidskader voor logging ten aanzien van het vastleggen van systeemgebeurtenissen en gebruikershandelingen. Dit document is een uitwerking van het Strategisch Beleidskader Informatieveiligheid Gemeente Den Haag en beschrijft specifiek de principes met betrekking tot het creëren, bewaren en beoordelen van logbestanden, inclusief de toegang tot loginformatie en de naleving van dit beleid.

Binnen de kaders van dit tactische beleid dienen operationele maatregelen te worden getroffen rondom logging door de betrokken applicatie-, systeem- en proceseigenaren.

Formeel toepassingsgebied

Het beleid is van toepassing op:

- Alle medewerkers van Gemeente Den Haag en externen die werkzaamheden verrichten voor de gemeente en ten behoeve van hun werkzaamheden toegang behoeven tot digitale informatie;
- Alle leveranciers van ICT-voorzieningen van de gemeente die ten behoeve van ondersteuning toegang nodig hebben tot de informatie(-systemen).

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO), v1.04:

- 9.4.4.2 Het gebruik van systeemhulpmiddelen wordt gelogd.
- 12.4.1 Gebeurtenissen registreren.
- 12.4.1.1 Eisen wat een logregel minimaal moet bevatten.
- 12.4.1.2 Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
- 12.4.1.3 De omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen.
- 12.4.1.5 De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd.
- 12.4.2 Beschermen van informatie in logbestanden.
- 12.4.2.1 Er is een overzicht van logbestanden die worden gegenereerd.
- 12.4.2.2 Ten behoeve van de loganalyse is op basis van risicoafweging de bewaarperiode van de logging bepaald.
- 12.4.2.3 Er is een audit procedure die toetst op het ongewijzigd bestaan van logbestanden.
- 12.4.2.4 Oneigenlijk wijzigen of verwijderen van loggegevens worden gemeld als beveiligingsincident.
- 12.4.3 Logbestanden van beheerders en operators.
- 12.4.4 Kloksynchronisatie.
- 16.1.7.1 De bewaartermijn van gelogde incidentinformatie is minimaal drie jaar.

Doel

Dit document heeft tot doel om verantwoordelijkheden vast te stellen en te waarborgen dat de verschillende aspecten van logging zijn ingericht conform de uitgangspunten en maatregeldoelstellingen uit het Strategisch Beleidskader voor informatieveiligheid. Op basis van dit beleid worden operationele procedures opgesteld voor log review-processen, evenals voor het behandelen van exceptions.

Indien om stringente redenen afgeweken moet worden van de kaders van dit beleid kan er in overleg met de IA security keten beoordeeld worden of de voorgestelde afwijking goedgekeurd kan worden en voor welke tijdspanne deze afwijking voort kan duren. De beoordeling van de voorgestelde afwijking vindt plaats op basis van een expliciete risicoafweging.

De gemeentelijke informatiebeveiligingsbeleidsregels met betrekking tot logging zijn

1. Logging algemeen

Informatiesystemen en ICT-infrastructuur genereren loginformatie. Een log beschrijft wat er gebeurt binnen systemen. Goed loggen is een eis uit de BIO, noodzakelijk om te kunnen voldoen aan wettelijke eisen en om bijvoorbeeld een audit op een systeem te doen. De eisen die gesteld worden aan logging worden zwaarder naarmate het belang hoger wordt. Op basis van het hieronder beschreven tactische beleid worden de kaders geschetst waarbinnen concrete maatregelen worden genomen voor logging en controle binnen de gemeente. In een log wordt het volgende weergegeven, de zogenaamde vijf W's:

- Wat gebeurde er?
- Wanneer gebeurde het?
- Waar gebeurde het?
- Wie was betrokken?
- Waar komt het vandaan?

Binnen de gemeente wordt onderscheid gemaakt tussen twee soorten logbestanden: technische logging en audittrail logging. Technische logging wordt uitgevoerd met als doel de controle van systeemgebruik vast te stellen of vast te stellen of informatiesystemen correct worden gebruikt, goed worden beheerd en functioneren conform de gestelde eisen in bijvoorbeeld een SLA. Audittrail logging bevatten de activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen. Op basis van de logbestanden worden rapportages opgesteld die periodiek beoordeeld worden. Met betrekking tot de rollen en verantwoordelijkheden hieromtrent kan worden verwezen naar paragraaf "rollen en verantwoordelijkheden".

2. Logbestanden

Logbestanden bevatten, voor zover relevant:

a) Gebruikersidentificaties
b) Systeemactiviteiten
c) Datum en tijdstippen van de gebeurtenis
d) Details betreffende de handeling van de gebeurtenis
e) Identiteit van de apparatuur en de systeemidentificatie
f) Registratie van al dan niet geslaagde pogingen om toegang tot het systeem te verkrijgen
g) Registratie van al dan niet geslaagde pogingen om toegang te verkrijgen tot informatiebronnen
h) Systeemconfiguratieveranderingen
i) Het gebruik van speciale bevoegdheden, waaronder het gebruik van een beheeraccount
j) Het gebruik van systeemhulpmiddelen
k) Geopende bestanden
l) Netwerkadressen en -protocollen
m) Afgegeven alerts
n) (De)activering van beschermingsmaatregelen, waaronder antimalware software, IDS en IPS.
o) Verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd.

Logbestanden bevatten in geen enkel geval gegevens (zoals wachtwoorden) die tot een doorbreking van de beveiliging kunnen leiden.

In voorkomend geval kunnen logbestanden gevoelige gegevens en/of persoonsgegevens bevatten, zoals gebruikersnamen of inlogaccounts. In dergelijke gevallen wordt hierbij ook met de relevante regelgeving omtrent privacy rekening gehouden te worden. Logbestanden bevatten in géén geval persoonsgegevens uit systemen van de Gemeente Den Haag zelf. Gebruikersnamen of useraccounts worden expliciet wel opgenomen in de logbestanden. Uitzonderingen in het kader van wet- en regelgeving zijn mogelijk hierop (denk aan protocollering BRP).

3. Registratie van logbestanden

De gemeente gebruikt verschillende soorten mechanismen voor logging die naast elkaar voorkomen. De gemeente streeft er echter naar om het aantal soorten te beperken, zodat een goed overzicht van de informatie kan worden gemaakt.

Voor zover mogelijk wordt logging centraal opgeslagen. Dit ter vergemakkelijking van de bescherming van de logbestanden, analysedoeleinden en het te beperken van de grootte van de opslag op productiesystemen.

Er wordt gecontroleerd op de opslagcapaciteit van logbestanden. Hiervoor is een grenswaarde per opslagmedium vastgesteld. Het bereiken van deze grenswaarde leidt tot een registratie daarvan en een alarmering van de beheerorganisatie.

Indien een opslagmedium voor logbestanden onbereikbaar of niet beschikbaar is gaat er een melding uit naar de beheerorganisatie.

4. Toegang tot loggegevens

Aangezien logbestanden zeer gevoelige informatie kunnen bevatten dient elke toegang of toegangspoging tot de logbestanden gelogd te worden. Uitschakelen van het loggen van toegang tot logbestanden moet niet mogelijk zijn. Een uitzondering wordt uitsluitend voorzien voor een benadering van de logbestanden die buiten de reguliere applicatie om op systeemtechnisch niveau herstelwerkzaamheden (correcties) verrichten aan de logging en of de logging-programmatuur. De actie dat het loggen wordt uitgezet, moet daarbij gelogd worden.

5. In- of uitschakelen van logging

Het in- of uitschakelen van logging geeft een wijziging weer in het loggingbeleid. Het in- of uitschakelen van logging moet altijd worden gelogd. Bij het in- of uitschakelen van de logging wordt de proces- of systeemeigenaar direct geïnformeerd over deze handelingen.

6. Bescherming van logbestanden

Logbestanden worden beschermd tegen oneigenlijke wijzigingen, verwijderingen of pogingen daartoe. Bij (het vermoeden van) een oneigenlijke wijziging, verwijdering of poging daartoe wordt de proces- of systeemeigenaar direct geïnformeerd over deze handelingen. Tevens worden de logbestanden met regelmaat beoordeeld op onregelmatigheden. Waar mogelijk wordt dit gedaan door middel van triggers of automatische alarmering. Logbestanden zijn louter toegankelijk voor geautoriseerde gebruikers en zijn read-only. Gebruikers van beheeraccounts hebben geen toestemming of (technisch of anderszins) de mogelijkheid om logbestanden van hun eigen activiteiten te wissen of deactiveren.

7. Exception handling

Er zijn gedocumenteerde operationele procedures voor het behandelen van uitzonderingen en hoe deze beoordeeld worden indien deze gevonden zijn gedurende de logcontrole.

Het onderzoeken van uitzonderingen en de behandeling daarvan wordt gedocumenteerd in een logboek, inclusief de op de uitzonderingen uitgevoerde acties.

Het logboek bevat mogelijk de volgende onderdelen voor elke registratie van een uitzondering:

a) Datum/tijd/tijdzone waarop de registratie in het logboek werd gestart.
b) Naam en functie van de persoon betreffende de registratie in het logboek.
c) Waarom wordt gestart: loguitzondering (gekopieerd uit de logaggregatie tool of uit het oorspronkelijke logbestand), ervoor zorgen dat de gehele log wordt gekopieerd, in het bijzonder de tijdstempel ervan (wat/wanneer/waar, et cetera).
d) Gedetailleerde beschrijving waarom de regel in het logboek niet routine is en waarom deze analyse wordt uitgevoerd.
e) Informatie over het systeem:
    a. Host naam
    b. Operating System (OS)
    c. Naam van de toepassing
    d. IP-adres(sen)
    e. Locatie(s)
    f. Eigenaarschap (indien bekend)
    g. Belang van het systeem (indien gedefinieerd en van toepassing)
    h. Informatie over Patch Management status, Change Management status, et cetera
f) Informatie over de gebruiker die in de logging gevonden is (indien van toepassing).
g) Gevolgde procedure en gebruikte tools, gemaakte screenshots et cetera.
h) Onderzoek acties die zijn uitgevoerd en uitgezet.
i) Mensen waarmee contact is geweest gedurende het onderzoek.
j) Bepaalde impact gedurende de analyse.
k) Aanbevelingen voor acties en genomen maatregelen (indien nodig).

8. Burgers

In voorkomend geval hebben burgers recht op inzage in hun gegevens (burgerdossier). In het verlengde daarvan hebben zij het recht te weten wie toegang tot hun burgerdossier hebben gehad. De logging van de toegang moet hiertoe ondersteuning bieden. De logging die een burger te zien krijgt, mag alleen betrekking hebben op het eigen burgerdossier.

In bepaalde gevallen willen burgers kunnen nagaan wie welke gegevens in het burgerdossier heeft genoteerd of gelezen. In het bijzonder kan dat het geval zijn wanneer de burger daarvoor aanwijzingen heeft gegeven of beperkingen kenbaar heeft gemaakt in een toestemmingsprofiel. Daarmee wordt afgeweken van generieke autorisatieprotocollen, waarin de geldende regels voor toegang tot de gegevens zijn vastgelegd. Wettelijke kaders beschrijven de minimumsituatie van de gevallen waarin deze wensen van de burger, dan wel diens gemachtigde of wettelijke vertegenwoordiger, moeten worden gehonoreerd.

De logging moet kunnen worden getoetst aan het autorisatieprotocol en het toestemmingsprofiel zoals die ten tijde van de actie van kracht waren.

Om dit mogelijk te maken moet in de logging met betrekking op een burgerdossier worden opgenomen:
- op welke gegevensgroep of compartiment van het burgerdossier de gebeurtenis betrekking had;
- welk autorisatieprotocol is toegepast;
- welk toestemmingsprofiel gold.

9. Kloksynchronisatie

De Gemeente Den Haag maakt gebruik van een atoomklok, door middel van een radiotijdsein, als referentietijdsein voor logsystemen. Relevante componenten van de Gemeente Den Haag worden gesynchroniseerd met de atoomklok

10. Bewaartermijn logbestanden

Logbestanden zijn minimaal een half jaar beschikbaar voor onderzoek. Logbestanden worden maximaal 2 jaar bewaard. Mocht het informatie systeem betrekking hebben op de gezondheid van burgers en het de kenmerken heeft van een medisch dossier is de bewaartermijn m.i.v. 01-01-2020 20 jaar

Indien er (het vermoeden van) een informatiebeveiligingsincident is wordt de bewaartermijn van de logbestanden minimaal drie jaar.

Logging die van relevantie is voor de jaarrekeningcontrole wordt voor het gehele betreffende kalenderjaar bewaard, of ten minste tot na afloop van de betreffende jaarrekeningcontrole.

11. Controle van logbestanden

Als er wordt gelogd, maar niemand kijkt ernaar, dan is loggen zinloos om uit te voeren. Om die reden is het voor de gemeente belangrijk om actief controles uit te voeren op de verzamelde logs. Het vol lopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt ook gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld een logserver die niet bereikbaar is).

Er zijn binnen de gemeente procedures vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten wordt regelmatig beoordeeld. Zoveel als mogelijk wordt systeemgebruik automatisch gelogd, als dit niet mogelijk is kan ook gebruik gemaakt worden van een logboek door bijvoorbeeld beheerders.

Indien er bij de controle van de logbestanden zich uitzonderingen voordoen worden deze verder behandeld conform 7. Exception handling.

Bij het vermoeden van oneigenlijk gebruik van de informatiesystemen door medewerkers moet de controle te alle tijden door of in samenwerking met een integriteitscoördinator worden uitgevoerd.

12. Rollen en verantwoordelijkheden

Binnen de gemeente wordt vastgesteld welke persoon en/of rol verantwoordelijk is voor het opstellen van de rapportages over de logbestanden en de beoordeling hiervan. Gezien de decentrale organisatie van logging wordt per type logging vastgesteld wie in welk team verantwoordelijk is voor de logging (werkplekbeheer, databases, etc.).

De proces-/systeemeigenaar is verantwoordelijk voor de naleving van het tactische beleid logging en de operationele toepassing ervan. De ISO's adviseren over de te treffen beveiligingsmaatregelen bij de toepassing van logging. IDC/a is verantwoordelijk voor het beschikbaar stellen van de kennis en technologie ter ondersteuning van de uitvoering van het beleid.

De CISO is verantwoordelijk voor de controle op het beleid en een controle op een juiste uitvoering van het beleid door de gemeente (Beleidscontrole). De CISO kan hiertoe een auditor opdracht geven.

Jaarlijks dient de beoordeling van dit beleid plaats te vinden, door een onafhankelijke partij, die gespecialiseerd is in informatiebeveiliging. Tussentijdse controles kunnen plaatsvinden door de interne accountantsdienst van de gemeente zelf. De bevindingen en verbeteringen zijn onderdeel van de jaarlijkse controle door een onafhankelijke partij.