

CS R07 Richtlijn logging

Uitgegeven door	RWS/CIV
Vertrouwelijkheidsniveau	RWS Ongeclassificeerd
Datum	27 mei 2016
Versie	1.0

Logging is vanuit de Baseline Informatiebeveiliging Rijksdienst (BIR) vereist en hierbij ligt meer de nadruk op het vastleggen van de gebruikershandelingen binnen applicaties. Dit moet men ook meer zien als logging vanuit de auditbehoefte. De logvereisten die vanuit de BIR afgeleid en vertaald zijn, staan beschreven in paragraaf 2.6 van de Cybersecurity Implementatierichtlijn Objecten RWS.

De eisen en diepgang aan logging worden zwaarder naarmate het belang hoger wordt. Zo is loginformatie vanuit de verschillende ICT en ICS/SCADA systemen die onderdeel uitmaken van de IA van essentieel belang om zicht te hebben op de beschikbaarheid en integriteit van deze apparaten. De focus op logging binnen de IA ligt meer op het systeemgedrag en -activiteiten. Is het systeem beschikbaar, werkt het systeem of component nog integer en is er een storing of onderhoud nodig etc.

Het doel dat wordt nagestreefd met het loggen van IA systemen heeft dan ook meer betrekking op het waarborgen van de beschikbaarheid en de integriteit van de IA door:

- Het verzamelen, analyseren en reageren op status info van de ICT en ISC/SCADA deelsystemen binnen de IA.
- Het ontdekken van menselijke fouten of systeem fouten, zoals fouten bij de bediening, maar ook het ontdekken van indringers in systemen.
- Het ontdekken van corruptie van data of programmatuur
- Het ondersteunen van onderzoek na een incident

Om de doelstelling van logging van IA systemen vorm te geven dienen de volgende maatregelen uitgevoerd te worden.

1. Een syslog server inrichten die de syslog events verzameld en toegankelijk maakt voor analysedoeleinden en automatische waarschuwingen.
2. De syslogserver dient voorzien te worden van malware protectie, hardening, logging van de activiteiten op de server zelf (toegang, config/systeemaanpassingen en kopieer acties).
3. De syslog server dient de syslog data te forwarden naar de RWS SIEM oplossing. Voor de benodigde netwerkverbinding dienen de NNV aansluitvoorwaarden in acht te worden genomen.
4. De syslogserver en syslog database is alleen toegankelijk voor geautoriseerden.
5. De syslog database kan niet gewijzigd of vernietigd worden door beheerders.
6. Het openen van een nieuw logbestand maar ook het verwijderen ervan dient te worden gelogd.
7. De bewaartermijn van de syslog database moet instelbaar zijn met een minimum van een maand.
8. Op aangeven van Opdrachtgever wordt de syslog database langer bewaard.
9. De syslog database dient zodanig ingericht te worden dat deze via het RWS netwerk toegankelijk is voor het Security Operations Centre van RWS.
10. De ICT en ICS/SCADA systemen die ingezet worden voor het Systeem dienen de syslog gebeurtenissen door te geven aan de syslogserver voor vastlegging in de syslog database.
11. Het ICT of ICS/SCADA deelsysteem binnen de IA dat de logregel veroorzaakt staat vaak niet in de logregel zelf, in dat geval moet de syslog server deze toevoegen aan de opgenomen logregel.

12. Om meldingen goed te kunnen correleren is het essentieel dat tijdsynchronisatie (NTP) is ingericht. Niet alleen de logserver dient te worden geconfigureerd op een tijdserver, maar ook alle aangesloten componenten zoals PLC's welke logregels genereren op de logserver.
13. Indien mogelijk dient Transport Layer Security (TLS) via TCP op poort 6514 gebruikt te worden (RFC 5425). Indien dit niet mogelijk is omdat de gebruikte apparatuur dit niet ondersteund, kan gebruik gemaakt worden van UDP port 514 voor transmissie naar de logserver.
14. Voor zover de ICT en ICS/SCADA systeemcomponenten hierin voorzien dienen de volgende events aangeleverd te worden aan de syslogserver:

Event:	Omschrijving:
Log In	Succesvolle login (lokaal of op afstand)
Manual Log Out	Gebruiker logt zelf uit
Timed Log Out	Uitloggen door voor-ingestelde tijd (time-out)
Value Forcing	Handmatig aangepaste waarde (overschrijving)
Configuration Access	Download van de PLC configuratie naar datadrager
Configuration Change	Upload van de PLC configuratie naar de PLC
Firmware Change	Nieuwe firmware installatie op de PLC
ID/Password Creation or Modification	Creatie of modificatie van een gebruiker of wachtwoord
ID/Password Deletion	Wissen van een gebruiker en wachtwoord in de PLC
Audit Log Access	Toegang tot de logbestanden in de PLC
Time/Date Change	Datum/Tijd aanpassing van de PLC
Unsuccessful Login Attempt	Onjuiste inlog poging op de PLC
Reboot	Herstart van de PLC
Attempted Use of Unauthorized Configuration Software	Ongeautoriseerde poging tot toegang van de PLC configuratie
Invalid Configuration or Firmware Download	Ongeldige configuratie of firmware download
Unauthorized Configuration or Firmware File	Ongeautoriseerde configuratie of firmware bestand
Unexpected Time Signal Out of Tolerance	Onverwachte tijd/datum wijziging
Invalid Field Hardware Changes	Ongeldige hardware aangesloten

Formaat syslog.

<timestamp> <IP> <Host> <facility> <Severity level> <message>

Voorbeeld:

<Oct 14 2015 22:09:12> <10.1.2.40> <123> <auth> <Alert> <Attempted Use of Unauthorized Configuration Software>

waarbij:

<timestamp> bij default tijd in het formaat `date "+%b %d %Y %H:%M:%S"`, zoals hierboven.

<IP> IP adres van het device, bijvoorbeeld 10.1.2.40

<Host> hostnaam of ID van het busdevice, in dit voorbeeld "123" in geval van een computer de hostnaam van de computer.

<facility> soort log gebeurtenis, bijvoorbeeld: kern, user, auth, syslog

<Severity level> bijvoorbeeld Emergency, Alert, Critical, Error, Warning

<message> het syslog bericht, bijvoorbeeld: Attempted Use of Unauthorized Configuration Software