Relevante beleidsregels logging

Bijlage 1 bij bepalingen informatiebeveiliging voor leveranciers

1. Logging

1. Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen binnen informatiesystemen en IT-infrastructuur behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
2. Een logregel bevat minimaal:
    a. Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
    b. De gebeurtenis;
    c. Waar mogelijk de identiteit van het werkstation of de locatie;
    d. Host naam;
    e. Operating System (OS);
    f. Naam van de toepassing;
    g. IP-adres(sen);
    h. Locatie(s);
    i. Het object waarop de handeling werd uitgevoerd;
    j. Het resultaat van de handeling;
    k. De datum en het tijdstip van de gebeurtenis.
3. In een logregel worden nooit gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, etcetera). In de logregel mogen ook geen overige persoonsgegevens worden opgenomen uit systemen van de SWO zelf (wel gebruikersnamen of inlog accounts).
4. Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren bij voorkeur aangesloten op een Security Information and Event Management systeem (SIEM) of geschikt om op een later moment aan te sluiten op een SIEM. Hiermee worden (gecorreleerde) meldingen en alarmoproepen aan de beheerorganisatie gegeven. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.
5. Controle op opslag van logging: 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).
6. De volgende gebeurtenissen worden in ieder geval opgenomen in de logs:
    a. Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instellingen: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore;
    b. Gebruik van functies voor functioneel applicatiebeheer, zoals het wijzigingen van configuraties en instellingen, release van nieuwe functionaliteiten, ingrepen in gegevenssets (waaronder databases);
    c. Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren van gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels;
    d. Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatie-bevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van Security Services);
    e. Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens het uitvoeren van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of -systemen);

   f. Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders;
   g. Online transacties. Hierbij wordt gelogd: het bericht-ID, datum en tijd, aanroepend en verzendend systeem en -proces.
7. Logfaciliteiten en informatie in logbestanden worden beschermd tegen inbreuk en onbevoegde toegang;
8. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log;
9. Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten;
10. Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden;
11. De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden zal daarbij altijd het ‘vier ogen’ principe toegepast worden;
12. De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden;
13. Bij een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn van de relevante loginformatie minimaal drie jaar;
14. Het goed functioneren van de logging wordt continu gemonitord voor essentiële systemen.
15. Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.