IMPLEMENTATIE GEGEVENSBEVEILIGING EN ICT BELEID IN KADER VAN DIGID

Aanleiding

Begin 2012 heeft Logius, de beheerder van DigiD, aangekondigd dat alle afnemers van DigiD jaarlijks een beveiligingsassessment moeten uitvoeren. Dit assessment heeft tot doel de beveiliging van de door DigiD ontsloten webomgeving van afnemerorganisaties te toetsen. De nadruk daarbij ligt zowel op het IT-gerelateerde deel (netwerken, ICT infrastructuur, hardware en software) als op de organisatie, werkwijzen en procedures die worden gehanteerd. Het assessment moet vóór 1 januari 2014 met positief resultaat zijn uitgevoerd.
Vanaf dat moment is een jaarlijks assessment verplicht. De basis voor het assessment wordt gevormd door de normen die zijn uitgegeven door Logius. Logius op haar beurt baseert zich op de beveiligingsrichtlijnen die door Nationaal Cyber Security Center (NCSC) zijn gesteld t.a.v. de beveiliging van webomgevingen bij de overheid.

De uitvoering van de assessments dient te worden gedaan door een erkende EDP auditor. Om het resultaat van het assessment bij voorbaat zo goed mogelijk te laten zijn is het relevant om het bestaande beleid, de daarvan afgeleide procedures en werkwijzen te evalueren. Dat kan voorafgaand aan het uit te voeren assessment, maar het is ook mogelijk om dat te doen aan de hand van de resultaten van een pre-audit die door een erkend EDP auditor is uitgevoerd.

Noodzaak voor goed uitgewerkt IT-beleid

Informatie en Communicatie Technologie (ICT) speelt in veel organisaties een cruciale rol. Het niet beschikbaar zijn van cruciale IT-systemen of –faciliteiten heeft een directe invloed op de bedrijfvoering van uw organisatie. Daarom is het van belang dat de wijze waarop deze systemen in uw bedrijfsvoering zijn ingepast en de processen die zij ondersteunen goed worden uitgewerkt en beschreven. Wij hanteren daarvoor standaarden als ISO en ITIL.

Naar aanleiding van recente inbreuken op gegevensbestanden en IT-systemen van overheidsdiensten zijn door de Nederlandse overheid stringente maatregelen genomen die het ongeoorloofd gebruik en de integriteit van deze bestanden en systemen moeten zekerstellen. Eén van die maatregelen is het uitvoeren van een jaarlijks assessment op de gegevensbeveiliging in het kader van DigiD.

DigiD assessment in 10 stappen

Vanuit de praktijk hebben wij een 10 stappen plan ontwikkeld. Dit plan zorgt ervoor dat de organisatie, die DigiD als afnemer gebruikt, het assessment met positief resultaat kan afleggen. Als afnemer van DigiD kunt u deze 10 stappen grotendeels in eigen beheer uitvoeren.

TASCLINX B.V., Postbus 77 , 5240 AB Rosmalen
Gerbrandyborch 18, 5241 HK Rosmalen
Tel : +31 (0)88. 890.8900
Internet www.tasclinx.com

Het bespaart echter nogal wat tijd en capaciteit wanneer u, zeker bij de eerste keer gebruik maakt van onze expertise om het assessment voor te bereiden en uit te voeren.
Wanneer u eenmaal een positief resultaat heeft geboekt, dan hoeft u als afnemer alleen te zorgen dat het beleid, de procedures en de uitvoering daarvan blijft voldoen aan de normen van Logius. Onze aanpak is erop gericht om de afnemerorganisatie zo te instrueren dat zij in de komende jaren het assessment zelfstandig en dus zonder externe ondersteuning kan uitvoeren.

- Stap 1 Breng alle relevante onderdelen in kaart
- Stap 2 Maak een plan
- Stap 3 Neem de controlelijst en voer een zelfevaluatie uit
- Stap 4 Corrigeer eventuele afwijkingen
- Stap 5 Maak een afspraak met een erkende EDP auditor
- Stap 6 Laat het assessment door de auditor uitvoeren
- Stap 7 Laat de penetratietest uitvoeren
- Stap 8 Corrigeer de eventuele tekortkomingen
- Stap 9 Finale toets door EDP auditor
- Stap 10 Stuur rapport in naar Logius

Ondersteuning Tasclinx
Tasclinx is al een aantal jaren actief in het implementeren van complexe IT-systemen en –applicatie bij overheidsorganisaties. De ontwikkeling en uitwerking van beleid en procedures is daarvan een integraal onderdeel. Vanuit deze ervaring zijn wij goed op de hoogte van de actuele eisen en regelgeving m.b.t. Informatiebeveiliging en de wijze waarop deze vorm gegeven moet worden in het bedrijfsbeleid van uw organisatie. Wij kunnen ondersteuning leveren gedurende het gehele traject van DigiD assessment. Deze ondersteuning bestaat doorgaans uit:

1. Het opzetten en eventueel voeren van projectmanagement inclusief ontwikkeling van het plan van aanpak, selecteren van en afstemmen met EDP-auditor t.a.v. planning en uitvoering van het feitelijk assessment.
2. Uitvoeren en/of begeleiden van de zelfevaluatie.
3. Inventariseren en beschrijven van de bestaande situatie.
4. Controle van beleid, procedures en regelgeving aan de hand van normenkader van Logius en NCSC.
5. Uitwerken resp. aanpassen en vastleggen van beleid en procedures (governance deel) in een maatwerk ICT-beleidsdocument.
6. Verzorgen van rapportage aan Logius.

Afhankelijk van de beschikbare capaciteit, kennis en ervaring bij uw organisatie kunnen onderdelen van de hiervoor vermelde ondersteuning meer of minder uitgebreid zijn.

Planning en capaciteit
De doorlooptijd van een compleet assessment traject bedraagt onder gemiddelde omstandigheden ca. 10 tot 12 weken, exclusief eventuele herstelacties. De doorlooptijd is mede afhankelijk van de beschikbaarheid van sleutelfunctionarissen en de EDP-auditor.
Bij de afnemerorganisatie zijn doorgaans betrokken:

- de verantwoordelijke functionaris voor IT,
- één of meer applicatiebeheerders,
- één of meer systeembeheerders (mede afhankelijk van de gebruikte infrastructuur),
- een of meer leveranciers (mede afhankelijk van de gebruikte applicaties, wijze waarop provisioning van webomgeving en hosting is geregeld).

Onder gemiddelde omstandigheden vereist de uitvoering van een assessment in totaal ca. 40 manuren verdeeld over de genoemde functionarissen.

Uitvoering
Wanneer u kiest voor een volledig ondersteuning door Tasclinx dan leveren wij de volgende producten:

1. Een volledige uitgewerkte beschrijving (in schema's en tekst) van uw IT-infrastructuur die relevant is voor het DigiD assessment.
2. Een volledig uitgewerkt IT-beleidsdocument dat voldoet aan het normenkader van Logius, resp. NCSC. Dit document kan dienen als kerndocument voor uw ICT-beleid en informatieveiligheidsbeleid.
3. Een uitgewerkt overzicht van concrete aanbevelingen en adviezen t.b.v. de organisatie om voorbereid te zijn op de toekomstige (zwaardere) informatiebeveiligingsassessments.

Wanneer u (delen van) het bovenstaande al heeft uitgewerkt, dan blijft de inzet van Tasclinx doorgaans beperkt tot toetsing van de uitgewerkte documenten en waar nodig (beperkte) aanpassing. Daarmee worden ook de kosten van externe inzet beperkt.

De uitvoering van het feitelijk assessment dient te geschieden door een geautoriseerde EDP-auditor. De activiteiten die Tasclinx uitvoert zijn gescheiden van de activiteiten van de auditor. De enige relatie is dat beiden werken vanuit het zelfde normenkader.
Het is van belang om tijdig de EDP auditor in te schakelen. Dat kan op het moment dat u de zogenaamde zelfevaluatie heeft uitgevoerd en eventuele afwijkingen of omissies heeft aangepast in overeenstemming met het normenkader. Uiteraard kunnen wij u bij de opzet en uitvoering daarvan ondersteunen.

Kosten
Voor de uitvoering van de ondersteuning dient u rekening te houden met ca. 3-6 adviesdagen, afhankelijk van de status van de huidige IT-infrastructuur, stand van zaken m.b.t. uitwerking van het beleid en de afstemming met leveranciers, providers en overige specialisten.
Voor samenwerkingsverbanden van gemeenten en/of waterschappen hanteren wij een speciaal (gereduceerd) tarief.

Sancties
Logius stelt als eis dat voldaan moet zijn aan het minimum pakket eisen (28) vóór 31 december 2013. Het niet (tijdig) voldoen aan de eisen van het normenkader van Logius betekent onherroepelijk afsluiting van het gebruik van DigiD.

Referenties
Specialisten van Tasclinx zijn in de voorbije jaren veelvuldig betrokken geweest bij de ontwikkeling en implementatie van complexe IT-systemen. Beleidsontwikkeling en –implementatie op IT-gebied vormt daarvan een integraal onderdeel. Desgewenst verstrekken wij u een of meer referenties waarbij u de kwaliteit van onze dienstverlening kunt nagaan.

Over TASCLINX
Tasclinx is een netwerk-gebaseerde adviesorganisatie. De onderneming werkt met 3 productlijnen: het ontwikkelen en implementeren van complexe ICT programma's en projecten, de levering van e-HR diensten en de ontwikkeling, implementatie van social media marketing. Tasclinx is actief voor zowel publieke als private organisaties. In de afgelopen jaren is Tasclinx rechtstreeks betrokken geweest bij de ontwikkeling en implementatie van een aantal regionale belastingsamenwerkingsverbanden.

Meer informatie?
Wilt u geheel vrijblijvend advies of nadere informatie? Neem contact met ons op voor een afspraak. Een oriënterend gesprek kost u niets en helpt u gericht bij het bepalen van wat u moet en kunt doen.

TASCLINX B.V., Postbus 77 , 5240 AB Rosmalen
Gerbrandyborch 18, 5241 HK Rosmalen
Tel : +31 (0)88. 890.8900
Internet www.tasclinx.com

Bijlage Voorbeeld uitwerking IT-beleid

Bij de uitwerking van uw IT-beleid hanteren wij een standaard indeling. Deze indeling is indicatief en kan uiteraard worden aangepast aan uw specifieke situatie, wensen en eisen.

Versiebeheer
Verspreidingsoverzicht

1. **Inleiding**
   - a. Beoogde doelstellingen
   - b. Definitie van gegevens- en informatiebeveiliging in organisatie X
   - c. Leeswijzer
   - d. Gebruik
2. **Organisatie**
   - a. Taken, bevoegdheden en verantwoordelijkheden
     - i. Vaststelling beleid
     - ii. Taak- en rolverdeling
     - iii. Bevoegdheden en verantwoordelijkheden
     - iv. Wijzigingen
   - b. Processen
   - c. Producten en diensten
3. **Autorisatie**
   - a. Autorisatiebeleid en de vastlegging daarvan
   - b. Wijzigingen
   - c. Inpassing nieuwe werknemers
   - d. Vertrek uit dienst van werknemers
   - e. Tijdelijke werknemers
   - f. Leveranciers
   - g. Overige aspecten m.b.t. autorisatie
4. **IT-infrastructuur, systemen en applicaties**
   - a. Het IT-landschap (schema)
   - b. Systemen
     - i. Data
     - ii. Telefonie
   - c. Applicaties
     - i. Frontoffice
     - ii. Mid- en backoffice
     - iii. Basisregistraties
     - iv. Kantoorautomatisering
     - v. Bedrijfsvoering
     - vi. Overige
   - d. Gegevens
     - i. Opslag, w.o. hosting
     - ii. Uitwisseling, w.o. ontsluiting (basis)gegevens t.b.v. derden/externe gebruikers
   - e. Technische infrastructuur
     - i. Netwerken
     - ii. Componenten
       1. Servers
       2. Clients
       3. Randapparatuur
       4. Overige
5. **Beheer en ontwikkeling**
   - a. Beheer
     - i. Productie
     - ii. Test
   - b. Ontwikkeling
   - c. Wijzigingen
6. **Risicomanagement**
   - a. Gebruik risico-analyse methodiek
   - b. Inventarisatie belangrijkste risico's en de daartegen genomen maatregelen
7. **Beveiligingsmanagement**
   - a. Beleidsdoelstellingen
   - b. Wettelijke verplichtingen
   - c. Preventie
   - d. Handhaving
   - e. Controles en audits
   - f. Beveiliging applicaties en data
   - g. Beveiliging technische infrastructuur
   - h. Toegangsbeveiliging
   - i. Sleutelbeheer
8. **Continuïteitsmanagement**
   - a. Calamiteiten
   - b. Back up en uitwijk
9. **Overige aspecten**