CERTIFICERINGSSCHEMA

INFORMATIEBEVEILIGING EN PRIVACY ROSA

Proces

DATUM	18 februari 2018
VERSIE	2.05
AUTEUR	Edustandaard werkgroep IBP

INHOUDSOPGAVE

1 INLEIDING

Het certificeringsschema bestaat uit onder andere een toetsingskader en een proces om een solide basisniveau van informatiebeveiliging en privacy te creëren van alle geleverde ict-toepassingen in de onderwijsketen.

De maatregelen in het toetsingskader zijn niet uitputtend. Er zijn altijd meer maatregelen die een organisatie kan treffen. Tevens houdt het toetsingskader niet expliciet rekening met het feit dat veel organisaties voor sommige activiteiten en producten een externe leverancier hebben (bijvoorbeeld een externe hosting partij of cloud-leverancier). In zo'n situatie dienen de maatregelen die relevant zijn voor die externe leverancier doorgezet te worden naar die externe leverancier en door de organisatie getoetst/gecontroleerd te worden.

Dit document beschrijft het proces hoe een organisatie het certificeringsschema toepast.

1.1 Continue verbetering

Het proces om aan de slag te gaan met het certificeringsschema is gebaseerd op de kwaliteitscirkel van Deming. Dit algemeen bekende verbeterproces is door elke organisatie te mappen op de bestaande verbetercyclus. De overeenkomstige processtappen zijn in dit document:

1. Voorbereiding (plan)
2. Classificatie en risicoanalyse (do)
3. Toetsen van maatregelen (check)
4. Verbeterplan (act)

1.2 Vastlegging

Om aantoonbaar te maken dat men aan het certificeringsschema voldoet, en om een minimale betrouwbaarheid te geven aan bijvoorbeeld een self-assessment, is het nodig om van dit proces de stappen en hun uitkomsten vast te leggen.

1.3 Benodigde personen en expertise

De volgende rollen zijn nodig bij de uitvoer van het proces:

- Eigenaar van de ict-toepassing; dit is de eigenaar van de ict-toepassing en vaak iemand uit de 'business'. Deze heeft inzicht in functionaliteit en prioriteiten van de organisatie.
- Eigenaar van de data; dit is vaak een proceseigenaar en vaak iemand uit de 'business'. Deze heeft een groot belang bij de bewerkte data.
- Technisch inhoudelijk specialist; dit is doorgaans een architect, ontwikkelaar of beheerder van de ict-toepassing. Deze heeft inzicht in de technische maatregelen.

- Specialist informatiebeveiliging; dit is doorgaans een security officer of ontwikkelaar met security-affiniteit.
- Procesbegeleider; dit is de persoon die het proces in goede banen leidt.

De combinatie van technische en niet-technische mensen zorgt voor een breed begrip en draagvlak in de organisatie om informatiebeveiliging en privacy verder op te pakken.

Bij de individuele stappen staat aangegeven welke van deze rollen nodig zijn. Het kan heel goed zijn dat in een kleine organisatie één persoon meerdere rollen vervult en dat de rol niet expliciet is vastgelegd.

Veel organisaties hebben baat bij het expliciet aanwijzen van een procesbegeleider. Deze kan namelijk boven de verschillende rollen uitstijgen zodat het certificeringsschema toegepast kan worden binnen een beperkt tijdsbestek en met geringe inspanning.

1.4 Externe partijen

De meeste organisaties maken voor een deel van hun ict-toepassingen of infrastructuur gebruik van externe partijen. Deze kunnen bijvoorbeeld servers hosten in een datacenter waar de organisatie zelf bij kan, of een virtuele oplossing zoals een cloud aanbieden.

In dat geval is het aan de organisatie om de maatregelen in het toetsingskader redelijkerwijs door te zetten naar die externe partij. Bijna alle externe partijen hebben hun eigen toetsingskaders waarmee ze aannemelijk maken dat ze de juiste maatregelen hebben getroffen. De organisatie kan dan middels de maatregelen in het toetsingskader controlevragen stellen en die antwoorden opnemen gebruiken als extra uitleg waar dat nodig is.

2 VOORBEREIDING

In deze fase wordt de voorbereiding getroffen voor de rest van de stappen. Het doel is om inzicht te krijgen in de ict-toepassing, de scope van het assessment en de gegevens die bewerkt worden door de ict-toepassing.

2.1 Scope

Maak een algemene beschrijving van de ict-toepassing en de verschillende componenten. Een voorbeeld is om een plaat te maken van de verschillende componenten van het systeem, welke partijen ermee werken, welke verbindingen er zijn met andere systemen, et cetera.

Deze plaat zal ook duidelijk moeten maken dat er grenzen zijn waar de invloed van de organisatie op de veiligheid van de ict-toepassing stopt. Bijvoorbeeld bij een verbinding naar een school heeft de organisatie wel invloed op haar kant van de koppeling, maar niet wat er vervolgens op de school achter zit.

Tip: sommige organisaties kiezen om de eerste keer niet elke applicatie in detail te analyseren, maar ze te groeperen in typen applicaties. Daardoor kunnen detailanalyses van specifieke applicaties leren van voorgaande analyses en kost het toepassen van het certificeringsschema elke opeenvolgende keer minder inspanning.

2.2 Inventarisatie van de data

Inventariseer welke gegevens er bewerkt worden door de ict-toepassing en in welke componenten de gegevens worden bewerkt. Maak daarbij gebruik van een classificatie die onderscheid maakt tussen ten minste openbare gegevens, gegevens voor interne medewerkers, persoonsgegevens en bijzondere persoonsgegevens.

2.3 Werkvorm en betrokkenen

In deze fase zijn de volgende mensen betrokken:

- Eigenaar van de toepassing
- Eigenaar van de data
- Technisch inhoudelijk specialist (optioneel)

2.4 Werkvorm, resultaat en tijdsbesteding

De werkvorm van deze fase is voornamelijk bureauwerk.

Het resultaat van deze fase is een gezamenlijk gedragen overzicht van de toepassing. Deze hoeft vooralsnog niet perfect te zijn, maar scheelt een hoop tijd in de volgende fase. Het is zonder overzicht lastig om iedereen op dezelfde lijn te krijgen.

De geschatte tijdsbesteding is 4-8 uur, verdeeld over twee of drie personen.

3 CLASSIFICATIE EN RISICOANALYSE

Het doel is om bewustzijn te creëren van de informatiebeveiliging van de ict-toepassing door inzicht te krijgen in de classificatie en mogelijke risico's.

3.1 Classificatie

Maak gebruik van het hulpmiddel voor classificatie van het certificeringsschema en bepaal het volgende:

- Wat zijn de (zeer) privacygevoelige gegevens in het systeem?
- Wat moet de beschikbaarheid van de ict-toepassing zijn?
- Wat moet de integriteit van de ict-toepassing zijn?
- Wat moet de vertrouwelijkheid van de ict-toepassing zijn?

Tip: bij het kiezen van een niveau is het soms illustratief om te denken in de volgende analogie: niveau Laag is de lokale boekhandel, niveau Midden is een commerciële instelling, niveau Hoog is een bank. Daarboven is nog het niveau van de geheime diensten, maar dat gaat voor de onderwijssector te ver en daarom is deze niet opgenomen in het certificeringsschema. Voor de gemiddelde toepassing (zonder bijzondere persoonsgegevens) zal niveau Midden het meest geschikt zijn.

3.2 Risicoanalyse

Inventariseer wat de meest voorname/actuele risico's actueel zijn. Dit kan door bijvoorbeeld na te lopen welke incidenten er de afgelopen jaren zijn geweest of door het bespreken van zogenoemde 'dreigingsbeelden' die door het NCSC (https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland) of SURF (Cyberdreigingsbeeld 2016) jaarlijks worden uitgegeven.

3.3 Betrokkenen

In deze fase zijn de volgende mensen betrokken:

- Eigenaar van de toepassing
- Eigenaar van de data
- Technisch inhoudelijk specialist
- Specialist informatiebeveiliging (optioneel, zie 3.4)

3.4 Werkvorm, resultaat en tijdsbesteding

De werkvorm van deze fase is een workshop/discussie/overleg. Het is aan te bevelen deze te laten begeleiden door een specialist in informatiebeveiliging. Deze houdt dan het proces in de gaten en geeft waar nodig inhoudelijke sturing of extra achtergrondinformatie.
Het resultaat van deze fase is een vastgelegde classificatie van de ict-toepassing op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid. Bijvangst van de workshop is bewustzijn van de informatiebeveiliging en voornaamste risico's van de ict-toepassing.

De geschatte tijdsbesteding is 4 uur per aanwezige van de workshop en een additionele 2 uur voor de procesbegeleider voor de vastlegging en uitwerking van de resultaten.

4 TOETSEN VAN MAATREGELEN

In deze fase wordt daadwerkelijk gekeken naar de getroffen maatregelen in de ict-toepassing. Deze worden vergeleken met de maatregelen in het toetsingskader.

4.1 Vergelijk maatregelen met toetsingskader

Loop het toetsingskader langs per aspect van informatiebeveiliging (beschikbaarheid, integriteit, vertrouwelijkheid) en bepaal dan voor elk aandachtsgebied welke maatregelen de organisatie heeft getroffen.

Bepaal hoe de maatregelen zich verhouden tot de maatregelen van het betreffende niveau in het toetsingskader.

4.2 Noteer resultaten

Noteer op welke wijze de organisatie voldoet of afwijkt:

- Voldaan; wanneer de organisatie de maatregelen in het toetsingskader treft.
- Niet voldaan; wanneer de organisatie (nog) niet voldoet aan de maatregelen genoemd in het toetsingskader.
- Alternatieve maatregel; wanneer de organisatie van mening is dat door een alternatieve maatregel alsnog het gewenste beveiligingsniveau gehaald wordt.

Vastlegging van de resultaten is nuttig voor de interne communicatie en een eventuele externe toetsing. Leg bewijsmateriaal vast op basis waarvan het resultaat bepaald is.

4.3 Werkvorm en betrokkenen

In deze fase zijn de volgende mensen betrokken:

- Technisch inhoudelijk specialist
- Eigenaar van de data
- Eigenaar van de toepassing (optioneel)
- Specialist informatiebeveiliging

4.4 Werkvorm, resultaat en tijdsbesteding

De werkvorm van deze fase is een workshop/discussie/overleg. De specialist informatiebeveiliging is nodig om het nut van alternatieve maatregelen te toetsen.

Het resultaat van deze fase is een overzicht van voldane maatregelen (comply) en afwijkingen (non-comply of explain).

De geschatte tijdsbesteding is 4 uur per aanwezige van de workshop en een additionele 4 uur voor de procesbegeleider voor de vastlegging, uitwerking en eventuele navolging ten behoeve van de uitwerking.

5 VERBETERPLAN

In deze fase worden de afwijkingen meegenomen in het bestaande verbeterproces. Dit kunnen aparte processen zijn in de organisatie omdat de maatregelen zowel processen, software en infrastructuur raken.

5.1 Prioriteer de verbeteringen

Bepaal welke verbeteringen niet op zich kunnen laten wachten. Op deze manier kunnen urgente verbeteringen direct gepland worden.

Bepaal welke aanvullende maatregelen passen in de bestaande tijd en middelen. Op deze manier ontstaat een roadmap voor de verbeteringen op korte en langere termijn.

5.2 Plan de verbeteringen

Bepaal wie wat wanneer gaat uitvoeren. Leg vast wanneer de eerstvolgende controle plaatsvindt.

Afwijkingen zijn niet altijd binnen afzienbare tijd op te lossen of kosten een significante investering. Ook kunnen er andere complicaties zijn. Een veelkomende complicatie is dat een oud legacy-systeem wordt gebruikt, maar dat dat oude systeem binnen afzienbare tijd wordt afgesloten. De best practice is om in dat geval aan te geven:

- op welke termijn het systeem wordt afgesloten,
- welke aanvullende maatregel(en) je neemt om de informatiebeveiliging en privacy in de tussentijd te beschermen.

5.3 Werkvorm en betrokkenen

In deze fase zijn de volgende mensen betrokken:

- Technisch inhoudelijk specialist
- Specialist informatiebeveiliging
- Eigenaar van de toepassing (optioneel)
- Eigenaar van de data (optioneel)

5.4 Werkvorm, resultaat en tijdsbesteding

De werkvorm van deze fase is voornamelijk bureauwerk.

Het resultaat van deze fase is een plan van aanpak die wordt aangeboden aan de eigenaar van de toepassing en eigenaar van de data. Hierin staat beschreven welke maatregelen op welke wijze worden genomen. Doordat deze door de eigenaar van de toepassing en eigenaar van de data wordt goedgekeurd, is er betrokkenheid van de ‘business’ bij het oppakken van informatiebeveiliging.

De geschatte tijdsbesteding is 4-8 uur, verdeeld over de betrokkenen.

6 AANDACHTSPUNTEN

6.1 Tips bij de uitvoering

Gebaseerd op de eerste toepassingen van het certificeringsschema zijn er de volgende aandachtspunten:

- Een goede begeleiding van het proces en een deel van de inhoud is nuttig. Hiervoor is een specialist op het gebied van informatiebeveiliging wenselijk.
- Discussie met alle betrokkenen draagt bij aan de beeldvorming en bewustwording rondom informatiebeveiliging. De eigenaar van de toepassing en de eigenaar van de data verlenen hun goedkeuring aan het plan van aanpak, waardoor betrokkenheid is van de 'business' bij de informatiebeveiliging is gewaarborgd.
- Focus op de eigen toepassing en wat binnen de eigen invloedssfeer ligt. Breng de verantwoordelijkheden binnen en buiten de organisatie in kaart en bespreek deze waar nodig met de ketenpartners.

6.2 Feedback

Het certificeringsschema is een baseline gebaseerd op best practices. De technologie en informatiebeveiliging gaan steeds verder vooruit. Daarmee moet het certificeringsschema per definitie mee met de tijd en de techniek.

Geef daarom terugkoppeling van de toepassing van het certificeringsschema door aan Edustandaard. Zij zorgen ervoor dat deze wordt opgepakt in de roadmap voor het beheer en de doorontwikkeling van het certificeringsschema.