Information Security On A Page

Koen Colpaert, CISO

July 20, 2020

Contents

1 Doel

Overzicht van de security en risk strategie op één enkele pagina met verwijzing naar de risico's, mogelijkeden, middelen en mensen van de organisatie met als doel deze strategie te communiceren naar de stakeholders. Verder bevat het document ook richtlijnen voor security architecten, ontwikkelaars en beheerders om tactische invulling te geven aan de strategische doelstellingen. Centraal in dit document is de onderlinge relatie tussen de organisatiedoelstellingen, technologische risico's en SRM maatregelen.

Dit document is geen afgewerkt eindproduct op zich en dient gebruikt te worden als startpunt voor verdere, diepgaande discussies over security en risk management. Het kan ook gebruikt worden als verantwoording voor inspanningen op het vlak van business continuity, herstelmaatregelen investeringen in technologie.

2 Aanpak

Op het hoogste niveau geeft dit document een overzicht van de samenhang tussen deze doelstellingen, risico's en maatregelen. Nadien worden de verschillende maatregelen inzake risicobeheersing besproken:

- Beschrijving van de specifieken relevante samenhang tussen risico's en organisatiedoelstellingen
- Mapping van de principes op de risico's
- Voorbereiding voor de tactische implementatie van het framework.

De strategie dient een antwoord te formuleren op de volgende aspecten:

- SRM verantwoordelijken moeten een goed inzicht hebben op de organisatiedoelstellingen
- SRM verantwoordelijken hebben de belangrijkste technologie-gerelateerde risico's voor de organisatiedoelstellingen in kaart gebracht
- De SRM-aanpak dient uitgewerkt te worden aan de hand van een veelvuldig gebruikt raamwerk en oplossingen bieden voor de geïndentificeerde risico's.

3 Informatie Strategie

3.1 Wie zijn we?

Centraal in dit onderdeel staat onze missie en visie als organisatie. Voor het departement Financiën en Begroting luidt de visie: "Het Departement Financiën en Begroting wil het financiële, fiscale, budgettaire en boekhoudkundige kenniscentrum van en voor de Vlaamse overheid zijn om zo van Vlaanderen een duurzaam financieel gezonde en performante regio te maken."

Om deze visie en missie te bereiken heeft DFB in het verleden zowel beleids- als organisatiedoelstellingen gedefiniëerd. Het SO heeft hieruit de belangrijkste gehaald om de doelstelling "het" kenniscentrum te worden en Vlaanderen als voorbeeldregio op de kaart te zetten waar te maken, specifiek vanuit het perspectief van security. Deze doelstellingen zijn:

- Houdbare openbare financiën realiseren in een Europees kader
- Een coherent fiscaal kader ontwikkelen
- Instaan voor het correct innen van belastingen
- Optimalisatie van de financiële situatie van de Vlaamse overheid
- Een efficiënte administratie zijn
- Kwalitatief en efficiënt archief-, documentatie- en informatiebeheer

3.2 Welke risico's hebben we?

De input voor dit onderdeel komt ideaal vanuit een risk assessment of vanuit het IT risicoregister. Gartner beveelt aan deze lijst kort en bondig te houden

wat ook aansluit bij de CISO insteek om doelstellingen te formuleren die op korte termijn tot haalbare resultaten kunnen lijden voor het SIEM/SOC-team en de visibiliteit naar de business te verhogen.

Duidelijk identificeerbare risico's zijn:

- Regelgeving en naleving
- Onvermogen om digitale bedrijfsprojecten bij te houden
- Risico opkomende technologie te missen
- Risico van derden
- Beschikbaarheid kritische systemen

3.3 Hoe pakken we ze aan?

Dit onderdeel bevat de grote lijnen van het risicobeheersingsprogramma. Er dient een duidelijke link te zijn met de risico's zowel als de organisatiedoelstellingen.

- Implementatie van een proactief risicobeheer
- Bescherming van onze informatie
- Implementatie van een robuust crisis- en incidentbeheer inclusief beheersmaatregelen
- Verbeteren van de beschikbaarheid en herstelbaarheid van de kritische systemen

4 Risico Landschap

Gebaseerd op de geïdentificeerde risico's en onze aanpak gaan we het nodige doen zodat we onze bedrijfsdoelstellingen kunnen bereiken en de risicoblootstelling beperken tot binnen de grenzen van onze risicobereidheid.

- **Regelgeving en naleving**: Als we ons niet aan de regels houden, zullen we boetes krijgen, een negatieve perceptie bij het publiek, hogere nalevingskosten krijgen en het vertrouwen verliezen van het politiek niveau..

- **Onvermogen om digitale bedrijfsprojecten bij te houden**: Als we de digitale doelen van onze organisatie niet kunnen ondersteunen, lopen we achter op de andere bestuursniveaus, krijgen we de reputatie dat we niet met de tijd (kunnen) veranderen, zien we hogere kosten als gevolg van een inhaalslag achteraf en verliezen we het vertrouwen van burger en politiek.

- **Risico opkomende technologie te missen**: Als we risico's negeren als gevolg van opkomende technologie die niet wordt begrepen of beheerd, zal dit ons ervan weerhouden te groeien als organisatie, waardoor we 'klanten' (burgers en politiek) van de volgende generatie verliezen die steun van deze nieuwe technologie zullen 'verwachten' en het gevaar van onbekende risico's laten toenemen.

- **Risico van derden**: Als we ons uitgebreide ecosysteemrisico, het risico van de digitale toeleveringsketen en de uitgebreide risico's op het gebied van regelgeving en naleving niet effectief beheren, zullen aansprakelijkheid, afname van vertrouwen, gebrek aan zichtbaarheid en minder controle / zichtbaarheid leiden tot een lager vertrouwen in ons vermogen om bedrijfsrisico's te beheersen.

- **Beschikbaarheid van onze kritische systemen**: Als we niet op inzetten op het beschikbaar houden van onze systemen in alle omstandigheden, zullen we niet kunnen herstellen in geval van uitval, wat resulteert in verloren inkomsten (VLABEL), downtime, burgers die niet geholpen kunnen worden - kan intern, extern, per ongeluk of kwaadwillig zijn.

5 Risico Aanpak

In de vorige hoofdstukken lag de nadruk op de doelstellingen en de risico's, in dit onderdeel wordt voor het eerst naar de praktische kant van de zaak gekeken ('Hoe gaan we deze principes omzetten in de praktijk?'). Er dient ook op het vlak van security nagedacht te worden over een missie en visie en de nodige objectieven moeten worden uitgewerkt zodat we kunnen overgaan tot actie. Dit onderdeel is grotendeels gebaseerd op de 5 domeinen van het NIST CSF:

- **Identificeren**: Weten wat we hebben, wat belangrijk is en wat we doen.

- **Beschermen**: Nemen van efficiënte en effectieve beschermingsmaatregelen.
- **Detecteren**: Opsporen van die zaken die we niet tijdig konden voorkomen.
- **Reageren**: Prioretiseren en reageren op gedetecteerde incidenten.
- **Herstellen**: Zo snel als mogelijk/haalbaar alles terug in een operationele staat brengen.

6 SRM Doelstellingen

Missie

Het Security Office van Financiën en Begroting werkt samen met de entiteiten van departement en agentschap om systeem- en netwerkbronnen te beveiligen en de vertrouwelijkheid van informatie over en van burgers en organisatie te beschermen.

Visie

Om deze missie tot een goed einde te brengen zal het SO:

- Processen, procedures en richtlijnen ontwikkelen voor de bescherming van vertrouwelijke informatie
- Veiligheidsrisico's identificeren op het vlak van informatie en systemen en de nodige maatregelen nemen om de risico's te beperken tot het aanvaarde niveau
- Op basis van regelgeving en goede praktijken beveiligingsvereisten en baselines vastleggen en toezien op de naleving ervan
- In overleg met de andere entiteiten de beveiligingsproblemen en processen onderzoeken
- Een information security strategie en architectuur ontwikkelen in samenspraak met informatie- en applicatiebeheerders
- Erop toezien dat de nodige incident response en disaster recovery processen uitgewerkt zijn én worden toegepast
- Een antwoord formuleren op en oplossen van security incidenten
- Door toegepaste communicatie en opleiding de awareness bij alle betrokkenen verhogen

Hier wordt de onderlinge samenhang duidelijk tussen de principes, doelstellingen en de onderdelen van het raamwerk:

- Identificeren <> Implementatie van een proactief risicobeheer
- Beschermen <> Bescherming van onze informatie
- Detecteren <> Voorbereiden op nieuwe technologieën
- Reageren <> Verbeteren van de beschikbaarheid en herstelbaarheid van de kritische systemen
- Herstellen <> Implementatie van een robuust crisis- en incidentbeheer inclusief beheersmaatregelen

7 Relatie Tactiek-Strategie

In het laatste onderdeel van dit document wordt de link gelegd tussen de hoger niveaus en de tactische uitvoering.

- Identificeren > Weten wat we hebben, wat belangrijk is en wat we doen > Asset Management, Bedrijfsprocessen, Risk Assessment, Governance, Risk Management Strategie
- Beschermen > Stoppen wat we moeten stoppen; elementaire blokkering en aanpak > Identity management, Awareness, Data security, Informatiebeveiliging, Beveiligingstechnologie
- Detecteren > Snel, eenvoudig en efficiënt vinden wat we moeten stoppen > Anomalieën, incidenten, monitoring
- Reageren > Response planning, analyse, beperking, verbeterprocessen, communicatie
- Herstellen > Terugkeer naar een goede staat, lessen trekken en streven naar continue verbetering > herstelplannen, communicatie

Om het raamwerk optimaal te benutten, moeten we deze processen implementeren die ons zullen helpen schaalbare, herhaalbare gedragspatronen en acties op te bouwen om ons beveiligings- en risicobeheerprogramma in de loop van de tijd te verbeteren.

8 Lijst afkortingen

Afkorting	Verklaring
CISO	Chief Information Security Officer
CSF	Cyber Security Framework
DFB	Departement Financiën en Begroting
NIST	National Institute of Standards and Technology
SIEM	Security Information and Event Management System
SO	Security Office
SOC	Security Operation Center
SRM	Security and Risk Management
VLABEL	Vlaamse Belastingdienst

9 Lijst bronnen

- G00368015-Toolkit: Information Security Strategy on a Page - Link
- DFB Ondernemingsplan 2016 - Link