TLP:GREEN

SOC SECURITY POLICIES

Monitoring & Detectie – Readiness Assistance

Factsheet versie 1.4

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot netwerken, systemen en (gevoelige) informatie.

Monitoring- en detectiediensten zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om monitoring- en detectiediensten effectief in te kunnen zetten zijn er diverse onderwerpen die binnen een organisatie moeten zijn ingericht. Dit document "Security Operations Center en Security Policies" geeft organisaties houvast bij het opstellen van kaders en beleid voor inrichten van een Security Operations Center (SOC).

Achtergrond

VSSR levert verschillende kennisproducten die aansluiten bij de SOC Readiness Quickscan. In dit document worden handvatten geboden voor Security Operations, aansluitend bij het strategisch onderwerp "Informatiebeveiligingsbeleid" uit de SOC Readiness Quickscan.

Doelgroep

VSSR biedt met dit document handvatten voor de Chief Information Security Officer (CISO) bij het opstellen van het informatiebeveiligingsbeleid voor (het goed functioneren van) een Security Operations Center (SOC).

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
1.0	14-12-2023	Initiële versie
1.1	29-2-2024	Weergave document complexiteit opgenomen
1.2	11-9-2024	TLP Markering opgenomen
1.3	19-6-2025	Bijlage I vervangen door Word template
1.4	9-6-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
SOC Security Policy template	Zie "SOC Security Policy Template (Word)"
Voorbeeld Policies (SANS)	Information Security Policy Templates | SANS Institute
CSF-policy richtlijnen (NIST)	NIST-CSF-Policy-Template-Guide.pdf (cisecurity.org)
Producten Informatiebeveiliging & Privacy (VNG)	Producten Informatiebeveiliging & Privacy - Informatiebeveiligingsdienst
Leidraad Coordinated Vulnerability Disclosure	Leidraad Coordinated Vulnerability Disclosure | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)
Readiness Quickscan (VSSR)	https://www.ncsc.nl/soc/het-vertrekpunt-voor-een-soc#:~:text=SOC%20Readiness%20Assistance
SOC Strategische Aanbevelingen (VSSR)	https://www.ncsc.nl/soc/het-vertrekpunt-voor-een-soc#:~:text=SOC%20Readiness%20Assistance

1.3 Definities

Voor alle termen en begrippen verwijst dit document naar het online Woordenboek - Cyberveilig Nederland.

2 Kaders en Beleid

Een Security Operations Center (SOC) is het organisatieonderdeel dat zich richt op de dagelijkse technisch operationele kant van informatiebeveiliging en houdt zich specifiek bezig met zaken als kwetsbaarhedenbeheer, bescherming tegen malware, detectie van inbraken, monitoring en opvolging van meldingen en incidenten.

Het is voor een SOC van groot belang dat een organisatie aan een aantal randvoorwaarden voldoet. Het informatiebeveiligingsbeleid vormt hiervoor de basis. Het beleid, dat is uitgezet door de directie, biedt de juiste handvatten voor de organisatie om kaders en richting te geven. Zonder mandaat vanuit de directie is het inrichten van informatiebeveiliging vrijwel onmogelijk. Voor het opzetten van een SOC is dit niet anders. Veel van de grondslagen voor het opbouwen van een succesvol SOC liggen in het beleid van de organisatie. Dit is onderkend in de eerste control in de Baseline Informatiebeveiliging Overheid (BIO, hoofdstuk 5).

BIO	BBN	Control	Verantwoordelijke
5.1.1	1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Sturing door directie

Tabel 1 BIO referentie in relatie tot kaders en beleid

3 Beleid

De BIO geeft nadrukkelijk aan dat beleid dient te worden geformuleerd en dat dit beleid frequent moet worden herzien. Maar wat moet er nu precies in het beleid staan? Voor een SOC is het van belang dat er een aantal beleidsregels (hierna genoemd: policies) voor verschillende onderwerpen zijn geformuleerd. Relevante SOC-security policies zijn benoemd in Tabel 2 SOC relevante security policies. Dit overzicht geeft houvast maar is niet uitputtend. Waar mogelijk is in de tabel een BIO verwijzing opgenomen. De daadwerkelijke tekst in de BIO is in sommige gevallen heel summier en in andere gevallen redelijk specifiek. Om dit verschil enigszins te ondervangen, is in de kolom "Inhoud" een aantal belangrijke onderwerpen opgenomen om houvast te bieden. Bekijk voor de eigen organisatie goed wat van toepassing is, waarbij verschillende (of alle) onderwerpen mogelijk in één document kunnen worden gebundeld.

Policy	Doel	Inhoud
Incident Melding en Response (BIO-16.1)	Vaststellen hoe de organisatie omgaat met beveiligingsincidenten in het algemeen en cyber security-incidenten in het bijzonder.	– Rapporteren; – Registreren; – Classificeren; – Afhandelen; – Reactietijden; – Escaleren; – Verantwoordelijkheden medewerkers.
Kwetsbaarheden beheer (BIO-12.6)	Vaststellen hoe de organisatie omgaat met het inzichtelijk maken, vastleggen, rapporteren en mitigeren van kwetsbaarheden.	– Scannen (inzichtelijk maken) – Vastleggen; – Rapporteren; – Verhelpen; – Oplostijden; – Verantwoordelijkheden en eigenaarschap.

Policy	Doel	Inhoud
Responsible Disclosure[1]	Vaststellen hoe de organisatie omgaat met externe meldingen van beveiligingslekken.	– Externe publicatie beleid; – Hoe te melden; – Reactietijden; – Opvolging; – Beloningsbeleid; – Verantwoordelijkheden; – Security.txt.
Security Logging en Vastlegging (BIO-12.4)	Vaststellen welke gegevens betreft IT-systemen op welke manier moet worden vastgelegd en waar de data dient te worden aangeleverd.	– Verantwoordelijkheden en eigenaarschap; – Welke logdata type dient te worden vastgelegd (Server audit log, DNS, DHCP, Firewalls, enz.); – Wat vast te leggen (welk type audit events: authenticatie, autorisatie, netwerk toegang, firewall blok events, enz.); – Inhoud van een audit regel (ook wat niet mag worden vastgelegd, zoals passwords); – Waar vast te leggen; – Retentie periode; – Bescherming van audit gegevens; – Toegang tot de data; – Tijdsynchronisatie eisen.
Continue Monitoring (BIO-12.4)	Vaststellen hoe de organisatie wil monitoren op mogelijke beveiligingsincidenten.	– Wat te monitoren (scope); – Verantwoordelijkheden; – Wanneer te monitoren (openingstijden SOC); – Afhandeltijden; – Rapportage; – Verantwoordelijkheden IT/proces eigenaren.
Acceptable use (BIO-12.2 en 13.2)	Vaststellen wat verantwoordelijkheden en verwacht gedrag is betreft het gebruik van Internet en email binnen de organisatie.	– Verantwoordelijkheden medewerker; – Wat mag wel/niet; – Welk ongewenst gedrag dient te worden gemeld; – Malware bescherming; – Melding verdachte e-mails (Phishing); – Gebruik privé email; – Privacy betreft email en Internetverkeer; – Monitoring door de organisatie; – Wat wordt geblokkeerd (welke Internetwebsite categorieën); – Opslag (email) data.
Detectie (BIO-12.4/13.1)	Vastleggen hoe gebeurtenissen moeten worden vastgelegd en bewijs wordt verzameld.	– Welke detectiemethoden moeten binnen de organisatie worden gebruikt; – Hoe en waar moet detectie zijn geregeld; – Aanleveren log data voor monitoring.
Internet DMZ-componenten (BIO-13.1)	Vaststellen wat de eisen zijn t.a.v. de beveiliging van componenten die in het DMZ staan. NB: omdat het DMZ een buffer vormt tussen Internet en het interne netwerk en direct is blootgesteld aan het Internet, vereisen de componenten	– Welke (cloud) services mogen worden gebruikt; – Eisen betreft dataversleuteling voor diensten; – Beveiligingseisen voor platform inrichting; – Monitoringeisen; – Detectie-eisen; – Auditpolicy-eisen; – Logdata aanlevering;

[1] Leidraad Coordinated Vulnerability Disclosure | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

Policy	Doel	Inhoud
	veelal meer beveiliging dan andere componenten.	– Patch-beleid; – Eisen bij uitzonderingen en bijbehorende verantwoordelijkheden; – Change managementbeleid.
Bescherming tegen Malware (BIO-12.2)	Vaststellen hoe de organisatie wordt beschermd tegen malware aanvallen en wat hierbij het verwacht gedrag van medewerkers is.	– Aanwezigheid anti-malware software op end-points, servers, mailservers, proxy-servers, enz. – Pattern update policy; – Hoe de organisatie (geautomatiseerd) handelt bij non-compliance; – Verantwoordelijkheden medewerkers en systeem/proces eigenaren; – Wat wordt verwacht van medewerkers; – Monitoring op infectie-notificaties.
Software-installatiebeleid (BIO-12.6)	Vaststellen wat wel/niet mag t.a.v. het installeren van software op eindgebruiker werkplekken en wat de organisatie hierin doet.	– Wat mag wel/niet; – Hoe kan toegang verkregen worden tot bepaalde software en voor welke doeleinden; – Wat doet de organisatie om dit af te dwingen; – Monitoring van applicatie gedrag door de organisatie; – Uitzonderingen.
Server security	Vaststellen van de standaard inrichting van server componenten t.a.v. security.	– Registratie-eisen; – System hardening; – Configuratie eisen en bijbehorende compliance verificatie eisen; – Auditing-, logging- en monitoring eisen; – Verantwoordelijkheden systeem-/proces eigenaar; – Vastlegging en afhandeling van uitzonderingen.
Toegang/Externe toegang (BIO-9.1)	Vaststellen wat de eisen zijn t.a.v. toegang en externe toegang tot het netwerk van de organisatie.	– Wie krijgt wel/niet toegang; – Hoe toegang verkregen kan worden voor verschillende partijen (medewerkers, derde partijen, enz.); – Eisen betreft data versleuteling; – Authenticatie-/autorisatie- en logging beleid; – Eisen betreft het component waarmee toegang wordt verkregen (bijv. eigenaarschap component, aanwezigheid antivirussoftware, Split-tunnel configuratie, enz.); – Aanleveren data voor monitoring; – Wat wordt gemonitord door de organisatie.
Verwijderbare media	Vaststellen van de eisen t.a.v. het gebruik van verwijderbare media om data lekken en malware infectie te beperken.	– Door de organisatie genomen risicobeperkende beveiligingsmaatregelen; – Verantwoordelijkheden eindgebruiker; – Monitoring van gedrag; – Welke data wel/niet op mediadragers mogen staan.
Account en wachtwoord policy	Vaststellen hoe wachtwoorden en gebruik van 2-factor authenticatie binnen de organisatie is ingericht.	– Welke type accounts mogen voor welk doel worden ingezet; – Configuratie instellingen inclusief: wachtwoordlengte, complexiteit, lock-out-eisen, frequentie van wijziging, enz.; – Verantwoordelijkheden eindgebruiker;

Policy	Doel	Inhoud
		– Eisen betreft 2-FA; – Gebruik van wachtwoordkluis; – Gebruik van accounts met hoge privileges; – Gebruik van speciale accounts voor noodprocedures.

Tabel 2 SOC relevante security policies

Afhankelijk van het type policy, komen een aantal zaken regelmatig terug in de verschillende beleidsdocumenten:

- Wat mag wel/niet en wat dwingt de organisatie hierin af;
- Wat is de verantwoordelijkheid van de eindgebruiker;
- Welke mate van privacy heeft een medewerker;
- Naar welke data kijkt de organisatie;
  (Bijvoorbeeld data dat het gedrag van medewerkers weerspiegelt)
- Wie heeft toegang tot logdata.

Dit zijn belangrijke componenten voor een goed functionerend SOC. Niet alleen omdat dit weergeeft welke logdata beschikbaar is, maar ook omdat medewerkers rechten en plichten hebben. Dat de organisatie naar bepaalde data kijkt, moet (contractueel) nadrukkelijk kenbaar worden gemaakt, omdat dit anders mogelijk inbreuk maakt op het recht op privacy. Om zeker te zijn dat de juiste zaken worden opgenomen in de verschillende policies kan het lonen om de juiste juridisch expertise in te zetten.

4 Policy inhoud

Na het vaststellen van het beleidskader is de volgende stap het opstellen van de individuele beleidsdocumenten per onderwerp. Hiervoor kan onderstaande structuur worden gehanteerd.

Voor het opstellen van beleidsdocumenten is een SOC Security Policy Template beschikbaar.

Onderwerp	Doel
Introductie	Korte introductie over de policy.
Doel	Het doel van de policy, waarom is het belangrijk voor de organisatie.
Scope	Op welke individuen/organisatieonderdelen is de policy van toepassing.
Beleidsregel	Dit onderdeel beschrijft puntsgewijs het daadwerkelijke beleid.
Compliance	- Compliance toetsing - Compliance uitzonderingen - Disciplinaire maatregelen bij –non-compliance
Gerelateerde documenten	Verwijzingen naar gerelateerde policies, standaarden, processen, enz.

Tabel 3 Policy-onderwerpen

5 Standaarden

Naast de verschillende beleidsstukken is het verstandig om voor een aantal onderwerpen ook standaarden te definiëren. Een standaard is een specifieke uitwerking van een policy die van toepassing is op een specifiek type component of specifieke groep van componenten in het IT-landschap. Deze uitwerkingen beschrijven hoe het doel component dient te worden ingericht zodat het duidelijk is voor de IT-beheerder hoe e.e.a. in detail kan worden uitgevoerd. Deze beschrijvingen zijn nodig om uniformiteit te garanderen en om uitzonderingen vast te kunnen leggen.

In Tabel 4 Standaarden zijn een aantal standaarden genoemd die van belang kunnen zijn voor het goed functioneren van een SOC. Deze lijst is niet uitputtend, dus bepaal voor de eigen organisatie wat van belang is. Als de standaarden goed worden beschreven en doorgevoerd in de organisatie dan zou het SOC de juiste log data op een uniforme wijze moeten krijgen aangeleverd.

Standaard	Doel	Inhoud
Informatielogging standaard	Voorschrift voor het logformaat waarin data bij het SOC dient te worden aangeleverd en hoe.	- Aanleveringsmethode (bijv. syslog); - Eisen betreft data-versleuteling; - Aanleverformaat (bijv. OSCF of CEF); - Tijdzone-configuratie; - Locatie op het netwerk waar de data aangeleverd dient te worden.
Server/Endpoint OS auditstandaard	Voorschrift voor het configureren van server audit-faciliteiten. Notitie: Deze standaard zal per besturingssysteem moeten worden gemaakt.	- Event types: DNS, DHCP, IIS, Security; - Event-categorieën: toegang, wijzigingen, privileges, systeem, enz.; - Generieke configuratie instellingen; - Configuratie-instellingen om de data te genereren.
Server Applicatie audit standaard	Voorschriften voor de instellingen voor de logging van specifieke applicaties die op servers aanwezig kunnen zijn. NB: Deze standaard zal per applicatie (DNS, DHCP, Web Server, Active Directory, LDAP, enz.) moeten worden gemaakt.	- Event categorieën; - Generieke configuratie instellingen; - Configuratie instellingen om de data te genereren.
Netwerkcomponenten-audit standaard	Voorschriften voor de inrichting van netwerkcomponenten.	- Event categorieën; - Generieke configuratie instellingen; - Configuratie instellingen om de data te genereren.

Tabel 4 Standaarden

6 Tot slot

Het opzetten en formuleren van een informatiebeveiligingsbeleid is een omvangrijk traject. De hier genoemde beleidsonderwerpen en bijbehorende standaarden zijn onderdeel van een uitgebreidere set aan organisatie brede beleidsdocumenten zoals bedoeld in de BIO, sectie 5.1. Na het formuleren van het beleid dient dit ook te worden onderhouden en waar nodig te worden herzien naar gelang de organisatie verandert, zoals bedoeld in de BIO, control 5.1.2. Voor het formuleren van de verschillende beleidsstukken is het telkens van belang om te kijken naar de doelstellingen voor het SOC en naar de implementatie-roadmap[2] . Zorg elke keer dat de beleidsstukken zijn uitgewerkt die van belang zijn voor het implementeren van de volgende fase van het SOC.

[2] Meer informatie over het opzetten van een SOC-roadmap is te vinden in kennisdocument "SOC Strategische Aanbevelingen (VSSR)"

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

December 2023