TLP:GREEN

SUPPLY CHAIN ATTACK

Incident Response – Draaiboek

Best Practice versie 1.1

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	18-11-2025	Initiële versie
V1.1	2-7-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
NIST SP 800-61 Rev. 3	SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile | CSRC
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Voorbereiding

1. **Randvoorwaarden:**
   Zorg dat de organisatie beschikt over een algemeen incident respons (IR-) plan waarin verschillende zaken zijn gedefinieerd:
   - **Incidentclassificatie:** Er zijn criteria opgesteld om incidenten te classificeren op basis van type (supply-chain, phishing, ransomware, datalek, etc.) en ernst (kritiek, hoog, middel, laag, informatief) voor het prioriteren van incidenten en bijbehorende respons.
   - **Rollen en verantwoordelijkheden:** Er is vastgesteld wie de leden van het respons-team zijn, inclusief primaire en back-up contactpersonen en hun rollen.
   - **Escalatieprocedures:** Escalatie procedures, paden, contactpersonen en beslismomenten zijn helder beschreven en bekend binnen de organisatie.
   - **Playbook-activatiecriteria:** Het IR-plan heeft duidelijke triggers die aangeven wanneer een specifiek playbook moet worden geactiveerd.

2. **Voorbereiding:**
   - **Evalueer Risico's:** Inventariseer per leverancier wat de potentiële risico's zijn en identificeer maatregelen (bijvoorbeeld op basis van SANS 18 critical security controls of de NIST 800-53 controls.
   - **Architectuur:** Neem de maatregelen op via (Security) Architectuur met betrekking tot de leverancier en in bredere zin.
   - **Implementeer maatregelen:** Na identificatie van maatregelen voor risico's en het opnemen in de architectuur, dienen deze geïmplementeerd te worden.
   - **Bepaal een baseline:** Bepaal hoe de normale activiteiten tussen uw organisatie en haar leveranciers eruitzien om afwijkingen gemakkelijker te detecteren.
   - **Beveiligde ontwikkelprocessen:** Bescherm systemen die betrokken zijn bij ontwikkeling, bouw en implementatie tegen ongeautoriseerde toegang.
   - **Handhaaf toegangscontroles:** Implementeer sterke multi-factor authenticatie voor waardevolle targets en kritieke systemen.
   - **Test de beveiliging:** Neem regelmatig de tijd om de risicobeperkende maatregelen en detectie van afwijkingen te testen. Gebruik de testresultaten voor verdere verbetering.
   - **Train personeel:** Voer trainingsoefeningen en simulaties uit om ervoor te zorgen dat het team het draaiboek effectief kan uitvoeren onder druk.

3. **Breng ketens in beeld:**
   - **Processen:** Inventariseer de (kritische) processen binnen de organisatie vast en stel de eigenaar vast.
   - **Ketens:** Inventariseer de bredere ketens bij de verschillende processen en bekijk welke externe partijen hierbij betrokken zijn.
   - **Leveranciers/klanten:** Wie zijn de leveranciers en klanten binnen de ketens en hoe kan je ze bereiken voor cybersecurity gerelateerde zaken?
   - **Contracteigenaarschap:** Wie zijn voor deze leveranciers/afnemers de contracteigenaren binnen de organisatie? Zorg dat deze informatie bij incidenten direct beschikbaar is.

3 Draaiboek

1. **Detectie en Analyse:**
   - **Verzamel dreigingsinformatie:** Blijf continu op de hoogte van gevonden kwetsbaarheden met betrekking tot fabrikanten en leveranciers van gebruikte componenten.
   - **Monitor op afwijkingen:** Monitor actief netwerkverkeer en systeemgedrag op ongebruikelijke activiteiten.
   - **Isoleer aangetaste pipelines:** Isoleer verdachte pipelines onmiddellijk, trek toegangstokens van leveranciers in en stop downstream builds om verdere verspreiding te voorkomen.
   - **Neem contact op met de leverancier(s)/afnemer(s):** Neem bij externe softwareontwikkeling contact op met de softwareleverancier zodat deze onderzoek kan doen, deze kan herstellen en patches en/of software-updates kan leveren.
   - **Verzamel bewijs:** Maak geheugendumps, logs en versie statussen om bewijs te bewaren voor forensische en juridische doeleinden.
   - **Traceer het aanvalspad:** reconstrueer de hoofdoorzaak van de aanval, identificeer injectiepunten en begrijp hoe de dreiging zich heeft verspreid.

2. **Inperking, Uitroeiing en Herstel:**
   - **Beperk de verspreiding:** isoleer getroffen systemen (maak eventueel gebruik van het stekkermandaad) en trek alle gecompromitteerde leverancierstoegangstokens in.
   - **Terugdraaien naar bekende goede versies:** herstel de software of systemen naar een vertrouwde staat om schadelijke code te verwijderen. Zorg voor snelle verzending van ondertekende patches naar alle downstreamgebruikers.
   - **De dreiging uitroeien:** verwijder de dreiging van getroffen systemen en beveilig de omgeving.

3. **Communicatie:**
   - **Stakeholders informeren:** informeer relevante interne teams, externe partners, klanten en regelgevende instanties.
   - **Transparantie behouden:** zorg voor tijdige en waarheidsgetrouwe updates, zelfs wanneer informatie onzeker is.

4. **Post-incident en geleerde lessen:**
   - **Voer een post-mortem uit:** voer een objectieve beoordeling uit om te identificeren wat er mis is gegaan en hoe het incident is afgehandeld.
   - **Playbooks en verdedigingen bijwerken:** herzie het incidentresponsplan, beleid, processen, architectuur, beveiligingsmaatregelen, implementatie, dit draaiboek en andere relevante zaken op basis van de geleerde lessen.
   - **Deel bedreigingsinformatie:** deel relevante indicatoren (IoC's) en tactieken, technieken en procedures (TTP's) met branchegenoten.

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)

November 2025