TLP:GREEN

INTERNET FACING KRITISCHE KWETSBAARHEID

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 op 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.
- **Besluitvorming en communicatie:** Voor elk escalatieniveau is vastgelegd welke belanghebbende geïnformeerd moeten en waar besluitvorming plaatsvindt.
- **Rollen en verantwoordelijkheden:** Voor elk escalatieniveau ligt vast wie lid is van het respons-team, inclusief primaire en back-up contactpersonen en hun rollen.
- **Escalatieprocedures:** Er is beschreven wanneer en hoe er geëscaleerd moet worden naar hoger management of andere teams.
- **Playbook-activatiecriteria:** Het IR-plan heeft duidelijke triggers die aangeven wanneer een specifiek playbook moet worden geactiveerd.

2. Voorbereiding:

- **Identificeer Aanvalsoppervlak:** Bepaal welke diensten, applicaties, systemen, etc, toegankelijk zijn vanaf het Internet.
- **Differentieer op basis van kriticiteit:** Bepaal hoe kritiek publiek-toegankelijke systemen zijn om de impact van risico's en kwetsbaarheden goed in te kunnen schatten.
- **Evalueer Risico's:** Inventariseer per omgeving 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. Houd hierbij rekening met mogelijke doorlooptijd van patching, het ontbreken van de juiste dreigingsinformatie, en het falen van processen. m.a.w. Implementeer het "layered defense" principe zodat bij het (tijdelijk) ontbreken van patches (de eerste en primaire security laag)
- **Implementeer maatregelen:** Na identificatie van maatregelen voor risico's en het opnemen in de architectuur, dienen deze geïmplementeerd te worden.
- **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. Beheersen van kwetsbaarheden:

- **Beleid:** Beschrijf een helder beleid waarbij het onder andere duidelijk wordt wie welke verantwoordelijkheden heeft met betrekking tot kwetsbaarheden en de ernst ervan. De organisatie dient een assetmanagement, kwetsbaarhedenmanagement, en patch management beleid te hebben.
- **Implementeer specifieke beveiligingstools:** Implementeer tools voor kwetsbaarhedenscanning, assetmanagement en patchmanagement om de detectie- en herstelprocessen te automatiseren.
- **Scan en rapporteer:** Implementeer regelmatige scans op kwetsbaarheden, vergelijk de resultaten met eerdere scans om vooruitgang en nieuwe bevindingen te onderscheiden, en rapporteer de bevindingen zodat.
- **Risicobeheersing:** leg belangrijke bevindingen vast in een risicoregister zodat, binnen de kaders van het risicobeheersingsbeleid, risico's worden onderkend en afgehandeld.

3 Draaiboek

1. **Detectie en Analyse**
   - **Verzamel dreigingsinformatie:** Blijf continu op de hoogte van gevonden kwetsbaarheden (omdat er lang niet altijd direct patches of scan-signatures voor zijn).
   - **Scan en Detectie update:** Richt een proces in dat op basis van dreigingsinformatie scan- & detectie-signatures implementeert om tijdelijke gaps op te vangen.
   - **Identificeer de kwetsbaarheid:** Gebruik beveiligingsmonitoring en kwetsbaarheidsscanners om actieve bedreigingen of kwetsbare systemen te detecteren.
   - **Verzamel informatie:** Leg details vast over de kwetsbaarheid, zoals de ernst ervan, de getroffen softwareversies en eventuele Indicators of Compromise (IOC's).
   - **Risicobeoordeling en rapportage:** Gebruik een methodologie zoals Stakeholder-Specific Vulnerability Categorisation (SSVC) om de ernst van de kwetsbaarheid binnen uw omgeving te bepalen en volg bestaand beleid en bijbehorende procedures om kritieke bevindingen direct te rapporteren en escaleren.

2. **Inperking, Uitroeiing en Herstel**
   - **Isoleer getroffen systemen:** Isoleer gecompromitteerde of kwetsbare systemen onmiddellijk van de rest van het netwerk om laterale verplaatsing door een aanvaller te voorkomen.
   - **Verzamel en bewaar bewijsmateriaal:** Verzamel en bewaar bewijs voor forensische analyse om de omvang van de inbreuk te begrijpen.
   - **Traceer het aanvalspad:** Onderzoek goed hoe de uitbuiting van de kwetsbaarheid heeft kunnen plaatsvinden. Dit geeft mogelijk inzicht in mogelijkheden om extra maatregelen op het aanvalspad te introduceren om tijdelijk de aanval te mitigeren.
   - **Blokkeer aanvallen:** Onderzoek de mogelijkheid om aanvallen te blokkeren voordat ze bij het doelwit zijn aangekomen (bijvoorbeeld in een Firewall of Intrusion Prevention Systeem of Web-Application Firewall).
   - **Verwijder de dreiging:** Maak eventueel geïnfecteerde systemen schoon en verwijder de kwetsbaarheid, bijvoorbeeld door een patch of beveiligingsupdate toe te passen.
   - **Beveilig het systeem:** Neem maatregelen om ervoor te zorgen dat de kwetsbaarheid niet opnieuw kan worden misbruikt, zoals het opnieuw configureren van getroffen systemen of het versterken van beveiligingsmaatregelen.
   - **Test:** Zodra de doelsystemen zijn hersteld, test dan of de potentiële aanval, behorend bij een kwetsbaarheid, inderdaad ineffectief is op basis van de genomen maatregelen.
   - **Herstel systemen:** Breng getroffen systemen veilig weer online.
   - **Monitor systemen:** Controleer herstelde systemen nauwlettend op tekenen van herinfectie en aanvalspogingen om zeker te zijn van de veiligheid.

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 en identificeer of het kwetsbaarhedenbeheer-proces of patchmanagement-proces kunnen worden verbeterd.
   - **Playbooks en verdedigingen bijwerken:** herzie processen, plannen, dit draaiboek, architectuur en de beveiligingsmaatregelen 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