

Veiligheid als uitgangspunt

Hoe OPS4 uw systemen, uw gegevens en uw bewijs beschermt

OPS4 bewaakt en onderhoudt de systemen waar uw organisatie op draait: SAP, databases, servers, hypervisors en netwerkapparatuur. Een hulpmiddel met dat bereik moet minstens zo goed beveiligd zijn als de systemen die het beheert. Deze folder legt zonder vakjargon uit welke maatregelen voor iedere klant in OPS4 zijn ingebouwd: niet als extra, maar als onderdeel van hoe het product werkt.

✓ Gescheiden

uw eigen omgeving, uw eigen sleutels

✓ Beheerst

MFA, rollen en goedkeuring

✓ Vastgelegd

een sluitend spoor van elke handeling

✓ Gecontroleerd

ondertekende updates, geteste releases

1 Uw eigen omgeving

- Iedere klant krijgt een eigen OPS4-omgeving: een eigen applicatie, database en eigen versleutelingssleutels. Niets wordt gedeeld met andere klanten.
- Een omgeving wordt leeg opgeleverd. Uw gegevens, gebruikers en instellingen zijn alleen van u.
- Geheimen die u in OPS4 invoert (wachtwoorden, priv sleutels, pincodes) worden versleuteld opgeslagen en na het opslaan nooit meer getoond.

2 Wie er binnenkomt

- Tweestapsverificatie met een authenticator-app, die een beheerder per gebruiker verplicht kan stellen.
- Optioneel een lijst met toegestane locaties: inloggen vanaf een onbekend adres moet eerst bevestigd worden. De controle gebeurt bij elk verzoek, dus een gestolen sessie werkt niet op een andere plek.
- Rechten per gebruikersgroep en per onderdeel: inzien of beheeren. Een automatisering uitvoeren is een ander recht dan haar beheeren.
- Het laatste beheerdersaccount kan nooit per ongeluk worden verwijderd of teruggezet.

3 Alles wordt vastgelegd

- Een audit-log van elke wijziging en elke handeling: wie, wat, wanneer en vanaf waar. Hij kan vanuit de applicatie niet worden aangepast of verwijderd en wordt twee jaar bewaard.
- Vastleggingen worden verzegeld in een hash-keten en buiten de omgeving tegengetekend, zodat latere manipulatie zichtbaar wordt. Uw auditor kan de keten zelf controleren.
- Een aparte toegangsl g van elke inlogpoging, ook de mislukte, direct zichtbaar in het menu.
- Gevoelige waarden worden in het spoor afgeschermd; het kan worden ingezien en ge xporteerd, nooit gewijzigd.

4 Agents die u kunt vertrouwen

- Agents op uw servers maken alleen uitgaand verbinding, versleuteld via HTTPS. Er hoeven geen poorten naar uw servers open.
- Updates van agents zijn digitaal ondertekend. Een agent controleert v  r installatie de handtekening bij het releaseregister van OPS4 en weigert de update als die niet klopt.
- Elke opdracht die een agent ontvangt, wordt eerst getoetst aan een strikte lijst van wat is toegestaan.

5 Automatisering onder uw regie

- Automatisering staat standaard uit. Ze moet twee keer worden toegestaan: bij de installatie van de agent, en per server in OPS4.
- Elke automatiseringstaak doorloopt een goedkeuringsstap en wordt stap voor stap gelogd, met het resultaat bewaard.
- Tijdens een taak gaat de server automatisch in onderhoud, zodat meldingen en serviceraportages kloppen.
- Grote wijzigingen, zoals een upgrade naar een nieuwe versie van het besturingssysteem, worden eerst getest op een afgeschermd kopie zonder netwerk, met een snapshot om naar terug te gaan.

6 Logbewaring (optioneel)

- De logs van uw servers worden bewaard in een archief dat eenmaal geschreven niet meer te wijzigen is: niemand kan ze aanpassen of verwijderen voordat de bewaartermijn verstreken is, ook een beheerder niet.
- Genummerde regels maken gaten zichtbaar, en struikeldraden slaan direct alarm als bijvoorbeeld een audit-log wordt geleegd of er een nieuwe beheerder verschijnt.
- Logs worden per bron en per maand versleuteld, zodat een specifiek deel vernietigd kan worden als de wet dat vraagt. Logs vernietigen kan altijd alleen met twee personen.

7 Koppelingen met uw andere systemen

- Koppelingen lezen via een apart leestoken, dat nooit iets kan wijzigen.
- Een leestoken werkt alleen vanaf adressen die u heeft toegestaan. Een lege lijst weigert iedereen.

8 Hoe wij OPS4 bouwen

- Elke release doorloopt de volledige geautomatiseerde testset voordat ze gebouwd kan worden, en wordt geleverd als genummerde, gecontroleerde release.
- OPS4 controleert zijn eigen onderdelen op bekende kwetsbaarheden, net zoals het dat voor uw servers doet.
- Beveiligingsreviews horen bij onze ontwikkelcyclus; bevindingen worden in het product opgelost, niet omzeild.
- AI-functies zijn optioneel en worden alleen op verzoek voor een omgeving aangezet.

Bewijs voor uw audits

OPS4 helpt u het bewijs te leveren waar kaders zoals ISO 27001 om vragen: wie er toegang had, wat er veranderde, wanneer systemen uit de lucht waren en waarom, of back-ups zijn gelopen en welke logs zijn bewaard. Serviceraportages bevatten een compliance-hoofdstuk dat dit samenbrengt.

Vragen over beveiliging, of een uitgebreide toelichting met uw security officer? Wij lopen het graag met u door.