WHITEPAPER VEILIGHEID BIJ SPEAKAP

Zo waarborgen we de vertrouwelijkheid, integriteit en beschikbaarheid van informatie

Versie 4.3 - April 2026

speakap

Inhoudsopgave

Inleiding

Vandaag de dag is informatiebeveiliging cruciaal voor iedere moderne SAAS-organisatie. Bij Speakap vonden we altijd al dat klanten de baas horen te zijn over hun eigen data. Dat betekent dat de bescherming van data bovenaan onze prioriteitenlijst staat. Wij vinden de toegenomen aandacht voor deze onderwerpen in het nieuws en in de maatschappij dan ook een goede ontwikkeling voor organisaties en consumenten.

Informatiebeveiliging is altijd een belangrijk onderdeel geweest van alle processen bij Speakap. Naarmate de organisatie en de de klantenlijst groeide, ontstond de behoefte aan een formeel Information Security Management System (ISMS).

De afgelopen jaren hebben we procedures en beleid vastgelegd, zodat we regelmatige checks en audits kunnen uitvoeren om de veiligheid te waarborgen. Daarnaast hebben we onze systemen en assets nagelopen en hebben we specifieke personen specifieke, gedocumenteerde verantwoordelijkheden toegekend. Tot slot hebben we een risicobeoordelingsprocedure ingevoerd die ons helpt om gericht verbeteringen door te voeren op het gebied van informatiebeveiliging.

Het hebben van een ISO 27001 compliant managementsysteem helpt ons om te voldoen aan de wet- en regelgeving zoals AVG, maar het verzekert ons er ook van dat we voldoen aan onze contractuele verplichtingen met klanten en leveranciers.

Op de volgende pagina's vind je een samenvatting van alle organisatorische en technische maatregelen die Speakap heeft genomen in relatie tot informatiebeveiliging.

> ***Onze risicogebaseerde aanpak stelt ons in staat om de informatiebeveiliging continu te verbeteren in gebieden waar het ertoe doet.***

Bart van Wissen
CTO

Beveiliging van de applicatie

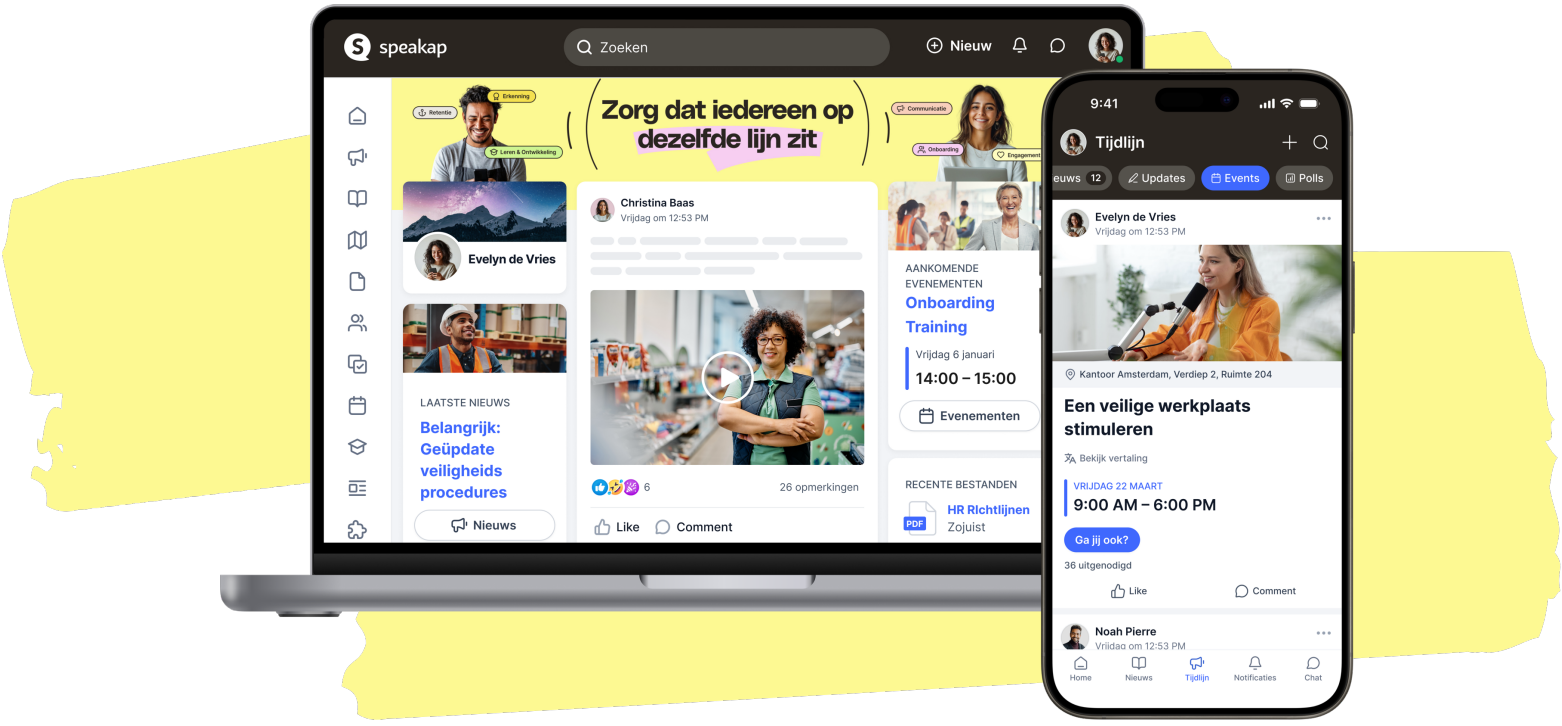
Speakap waarborgt dat gebruikers van het platform alleen toegang hebben tot data waar zij geautoriseerd voor zijn. Het veiligheidsmodel van de applicatie is gebaseerd op:

- **Gebruikers:** de leden van je organisatie, gemanaged door aangewezen beheerders binnen de organisatie. Alle leden van de organisatie (het 'netwerk') hebben een rol die hun rechten op netwerkniveau bepaalt.

- **Berichten:** privéberichten tussen twee personen waarbij alleen zender en ontvanger toegang toe hebben, of chatberichten gedeeld met een groep of een heel netwerk.

- **Tijdlijnen** waarop data wordt gedeeld in de vorm van berichten.

- **Groepen** bestaande uit leden gemanaged door aangewezen beheerders. Alle leden van een groep hebben een rol binnen de groep, die hun rechten bepaalt. Groepen hebben hun eigen tijdlijnen en hun eigen content gedeeld in de groep (afhankelijk van het type groep) alleen toegankelijk voor leden van deze groep.



Webveiligheid

- Alle verbindingen naar en van de backend worden beveiligd met HTTPS met TLS 1.2 als minimum (TLS 1.3 heeft de voorkeur). Sterke cipher suites worden gebruikt, waaronder AES-256-GCM en ChaCha20-Poly1305 encryptie met ECDHE sleuteluitwisseling die perfect forward secrecy biedt.
- Het oudere en zwakkere SSL-protocol is uitgeschakeld.
- Gevoelige cookies zijn opgezet met secure en http-only flags.
- Alle input van gebruikers wordt gevalideerd voordat het verwerkt wordt. Speciale aandacht gaat uit naar het voorkomen van Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) en SQL injectie.

Malwarebescherming

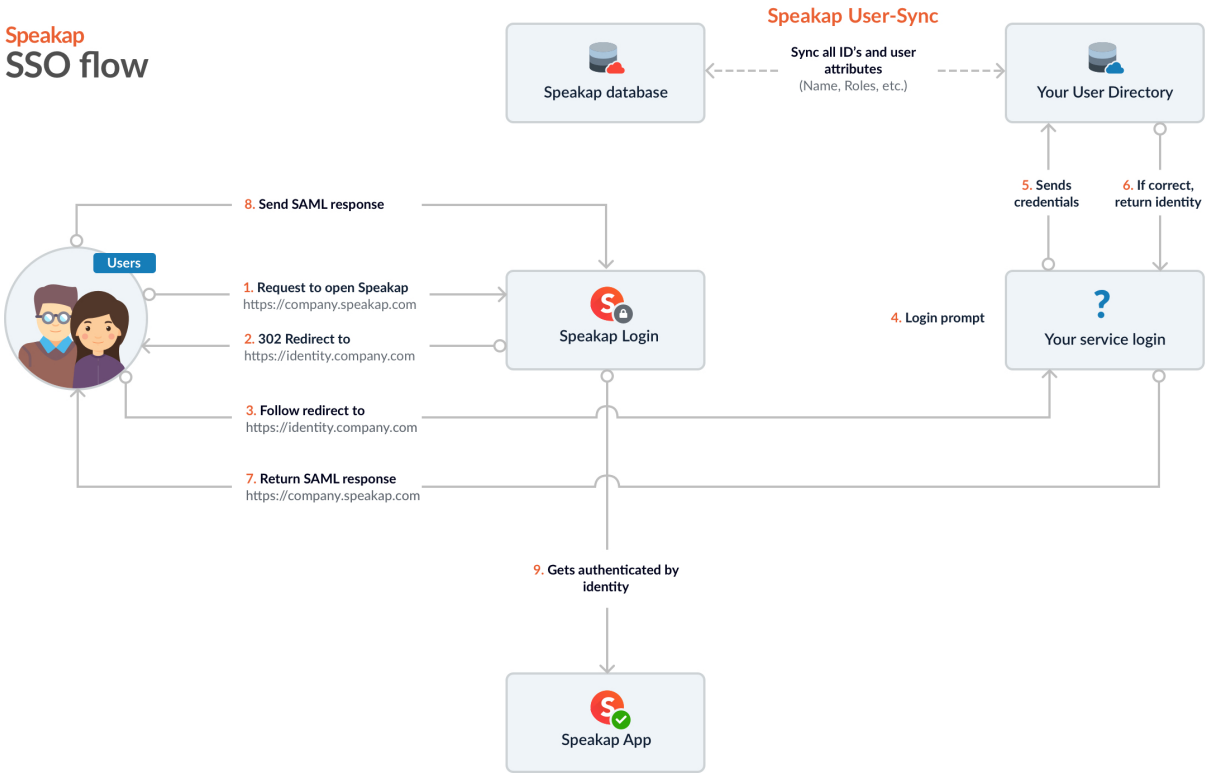
- Bestanden die door gebruikers worden geüpload, worden automatisch gescand op de aanwezigheid van malware tijdens het uploaden en geweigerd als daadwerkelijk malware wordt gevonden.
- Malwaredefinities worden regelmatig en automatisch geüpdatet.

Authenticatie en wachtwoorden

- Speakap API-authenticatie is gebaseerd op OAuth 2.0. *Access tokens* hebben een lengte van 100 bytes, gegenereerd door OpenSSL's *pseudo-random byte-string generator* en hebben een geldigheid van 1 uur, waarna deze moeten worden ververst.
- Alle actieve *access tokens* worden ingetrokken als een gebruiker zijn of haar wachtwoord verandert.
- SAML 2.0 kan worden gebruikt voor *Single Sign On*.
- Apparaten kunnen op afstand worden uitgelogd.
- Wachtwoorden hebben een minimumlengte van 10 karakters, moeten ten minste één kleine letter, een hoofdletter en een speciaal karakter bevatten.

- Wachtwoorden worden opgeslagen als *salted hashes* gebruik makend van het BCrypt algoritme, wat betekent dat Speakap geen enkele informatie bezit over de daadwerkelijk gebruikte wachtwoorden.
- Om een wachtwoord te veranderen, moet de gebruiker altijd eerst het oude wachtwoord invullen.
- Als iemand zijn/haar wachtwoord niet meer weet, kan een gebruiker een wachtwoord-reset aanvragen. Een geheime link om het wachtwoord te resetten wordt naar het primaire e-mailadres van de gebruiker gestuurd.
- E-mailadressen moeten worden geverifieerd via een geheime *token* voordat het als primair e-mailadres kan worden ingesteld.
- Wachtwoorden worden nooit op het apparaat van de gebruiker of in de browser opgeslagen. In plaats daarvan, wordt een *OAuth-token* veilig opgeslagen.
- De *token* wordt wordt op mobiele apparaten verwijderd als de gebruiker uitlogt of de app verwijdert.

Speakap SSO flow



Encryptie

- Data wordt versleuteld in transit en at rest.
- Alle communicatie over openbare netwerken gebruikt HTTPS met TLS 1.2 als minimum (TLS 1.3 heeft de voorkeur). Sterke cipher suites worden gebruikt, waaronder AES-256-GCM en ChaCha20-Poly1305 encryptie met ECDHE sleuteluitwisseling die perfect forward secrecy biedt.
- Het oudere, zwakkere SSL-protocol is uitgeschakeld.
- Klantdata is encrypted at rest met behulp van het AES-256 algoritme.
- Wachtwoorden zijn gehasht opgeslagen, met gebruik van het veilige BCrypt-algoritme.

E-mailbeveiliging

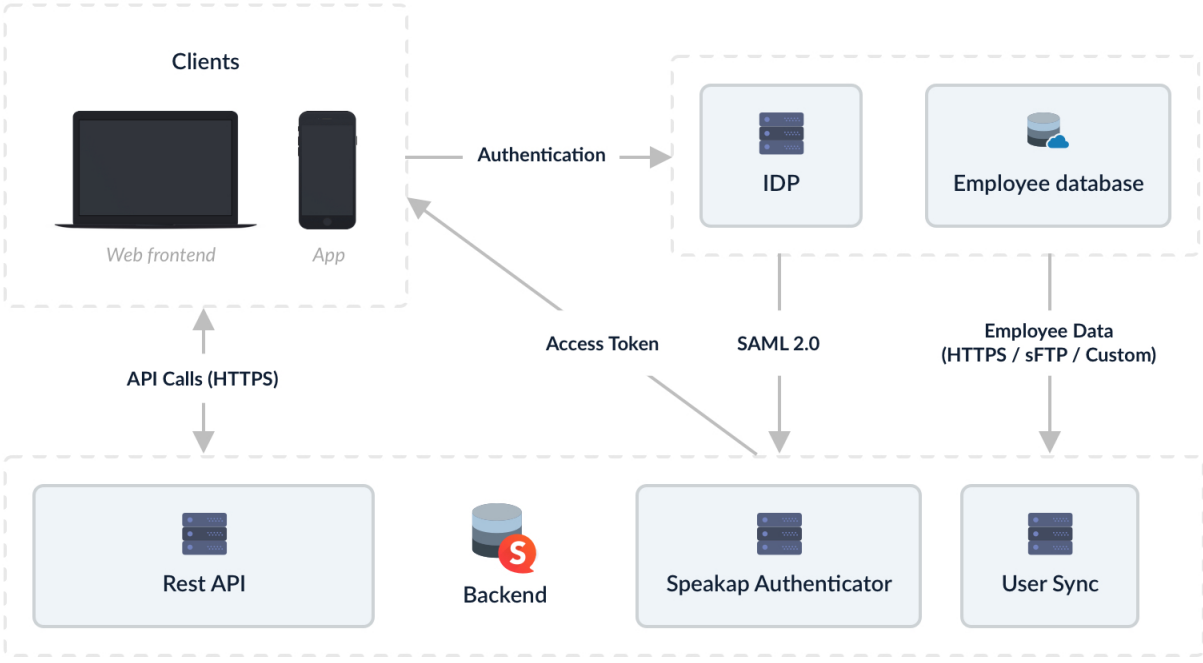
- Uitgaande transactionele e-mails worden verzorgd door AWS SES met uitgebreide authenticatiecontroles.
- DKIM-signing wordt toegepast op alle uitgaande e-mail.
- Afzendervervalsing wordt voorkomen met SPF.
- DMARC-beleid wordt afgedwongen met een "reject"-actie voor e-mails die authenticatiecontroles falen, wat uitgebreide bescherming biedt tegen e-mail spoofing en phishing-aanvallen.

Bescherming van servers en infrastructuur

- De productieomgeving is opgesplitst in meerdere veilige zones met firewall regels om het verkeer hiertussen te beveiligen.

- Toegang tot de productieomgeving vereist een VPN verbinding met een verplichte 2-factor authenticatie.
- Een beperkt aantal *senior system engineers* heeft toegang tot de servers in de productieomgeving.
- Het least-privilege principle wordt toegepast.
- Alle diensten zijn beschermd door firewalls.
- Op alle servers worden alle poorten en services automatisch geblokkeerd en alleen geopend als dit nodig is voor een service.
- Speakap-servers zijn voorzien van een centraal configuratiemanagementsysteem dat verzekert dat er een eenduidige, veilige configuratie is toegepast op alle servers. Versiebeheer wordt toegepast op alle configuratiegegevens.
- Kritieke veiligheidspatches worden geïnstalleerd binnen 24 uur nadat zij beschikbaar komen.
- Speakap-servers worden automatisch beschermd tegen DDoS aanvallen.

Speakap Architecture overview



Logging en monitoring

- Acties uitgevoerd door gebruikers in de applicatie worden opgeslagen in een centrale audit log.
- Server logs die relevant zijn voor de veiligheid worden centraal opgeslagen, geanalyseerd en leiden tot automatische alerts.
- 24/7 monitoring en automatische meldingen zorgen ervoor dat Speakap's system engineers snel kunnen handelen in het geval van storingen.

Disaster recovery, backup en redundancy

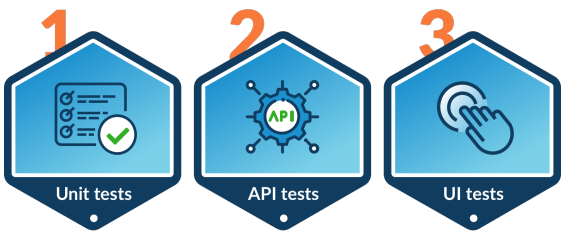
- Speakap garandeert 99,8% uptime, exclusief gepland onderhoud.
- Alle kritieke diensten zijn redundant opgezet om een hoge beschikbaarheid te garanderen, in de meeste gevallen met een volledige automatische failover.
- Alle klantdata wordt verschillende keren per dag gebackupt en een maand bewaard, zodat data kunnen worden hersteld indien sprake is van een noodgeval.
- Versleutelde back-ups worden opgeslagen over meerdere AWS availability zones binnen dezelfde regio (EU of VS), wat geografische scheiding en redundantie biedt terwijl compliance voor datalocatie wordt gehandhaafd.
- Speakap's disaster recovery plan helpt om diensten snel te herstellen in het geval van een calamiteit.

Datacentra

- De datacentra waar Speakap in wordt gehost zijn ISO 27001:2013 gecertificeerd.
- Speakap's primaire EU datacentrum wordt beheerd door Leaseweb, gevestigd in Nederland.
- Speakap's US datacentrum wordt beheerd door Amazon Web Services, Inc.
- Klantdata is opgeslagen in het EU datacentrum of in het US datacentrum. Er is geen overdracht van data tussen deze locaties en de klant bezit de volledige controle over de geografische locatie van de data.
- Fysieke toegang tot datacentra is louter mogelijk voor geautoriseerd datacentrum-personeel.

Veiligheid tijdens development

- Speakap's development-omgeving is gescheiden van de test- en productieomgeving.
- Productiedata wordt nooit gebruikt voor testdoeleinden.
- Productiedata wordt nooit verplaatst van de productieomgeving naar de testomgeving.
- Automatische test suites worden uitgevoerd bij iedere verandering in de Speakap code en veranderingen worden niet uitgerold tot alle tests succesvol zijn. In aanvulling daarop vinden handmatige tests en kwaliteitswaarborging plaats in een geïsoleerde testomgeving die niet toegankelijk is voor normale gebruikers.



- Alle veranderingen aan de Speakap code worden peer-reviewed door senior developers die uitgebreide kennis bezitten over de beveiliging van applicaties. De applicatie is ontwikkeld volgens best practices uit de branche en maatregelen zijn genomen om kwetsbaarheden te voorkomen zoals beschreven in de OWASP Top 10.

Veiligheids audits, penetratietesten en geautomatiseerde testen

- Minstens eens per jaar wordt een reeks penetratietesten uitgevoerd door een externe onafhankelijke partij.
- Dagelijkse automatische SSL-server-tests zorgen ervoor dat onze SSL-configuratie altijd voldoet aan branchestandaarden.
- De toegangscontrole tot de applicatie wordt onderworpen aan automatische tests die worden uitgevoerd bij iedere verandering en iedere release.
- Alle veranderingen aan de applicatie worden onderworpen aan een uitgebreide suite van API- en integratietests evenals unit tests en statische analyses.
- Klanten is toegestaan om op verzoek hun eigen penetratietests uit te voeren.

Organisatie en management

- Er worden regelmatig risicobeoordelingen en business impact analyses uitgevoerd.
- Het ISMS wordt jaarlijks zowel intern als extern geaudit zoals vereist volgens de ISO 27001:2013 standaard.
- Information Security Awareness trainingen verzekeren bewustzijn van veiligheidsrisico's en beheersmaatregelen bij het personeel.
- Personeel met toegang tot klantdata wordt gescreend voorafgaand aan hun indiensttreding.
- Developers moeten voorafgaand aan hun indiensttreding diepgaande kennis over veiligheidsonderwerpen aantonen.
- Om gevoelige data te beschermen, tekenen Speakap medewerkers een geheimhoudingsplicht bij hun indiensttreding.
- Clean desk en clear screen beleid waarborgen de vertrouwelijkheid.
- Medewerkers zijn verplicht om sterke wachtwoorden, volledige schijfversleuteling en automatische schermbeveiliging te gebruiken.
- Speakap's wachtwoordbeleid vereist dat medewerkers sterke, unieke wachtwoorden voor alle systemen gebruiken en dat zij waar mogelijk aanvullende maatregelen treffen, zoals 2-factor-authenticatie.
- Het informatie-classificatiebeleid samen met gedocumenteerde informatie en asset handling procedures waarborgen de vertrouwelijkheid, integriteit en beschikbaarheid van gevoelige informatie.
- Alle vormen van beleid hebben vastgelegde verantwoordelijken en worden regelmatig gereviewd.
- Access Management procedures waarborgen dat de toegang van medewerkers tot systemen wordt toegestaan en ingetrokken wanneer veranderingen zich voordoen, zoals onboarding, beëindiging van het dienstverband of veranderingen in rollen binnen de organisatie.

Respons op beveiligingsincidenten

- Speakap heeft een vastgelegde procedure voor information security incident response. Hierin staan de verantwoordelijkheden gedefinieerd en de bijpassende acties die in het geval van een veiligheidsincident dienen plaats te vinden.
- Speakap heeft een vastgelegde meldingsprocedure voor datalekken die ervoor zorgt dat de juiste mensen op de hoogte worden gesteld, zoals benoemd in de AVG artikelen 33 en 34.

Compliance

- Speakap heeft een Information Security Management System dat ISO 27001:2013 gecertificeerd is.
- Speakap handelt in lijn met de AVG wetgeving.
- Speakap heeft een succesvolle SOC 2 Type II-audit ondergaan door een onafhankelijke auditor met betrekking tot het ontwerp, implementatie en de operationele effectiviteit van de interne controlemaatregelen.
- Speakap is HIPAA-conform door te voldoen aan de eisen van de HIPAA-veiligheidscontroles.
- Er zijn verwerkersovereenkomsten met alle subverwerkers van informatie.
- Speakap heeft een aangewezen Functionaris Gegevensbescherming (FG).
- Speakap zal wethandhavingsverzoeken naar de klant doorzetten, tenzij bij wet verboden, zodat de klant kan besluiten om de gevraagde informatie aan te leveren of dit te weigeren.

www.speakap.nl