Brightfox

Salesforce Security Playbook

Hands-on tips om je Salesforce-omgeving te beschermen tegen cyberaanvallen, datalekken en misconfiguraties.

SECURITY TIPS

De Salesforce Security staat onder druk

Je Salesforce-omgeving voelt waarschijnlijk veilig. Alles werkt. Je MFA staat aan. Je team kan erbij. Alles voelt veilig, totdat iemand er écht naar kijkt.

De meeste moderne datalekken beginnen niet meer met een hack, maar met iets kleins: een gebruiker met te veel rechten, een app die toegang krijgt, een instelling die verkeerd staat.

Dat is precies hoe het misging bij Odido. Dit was geen complexe aanval, maar een simpele phishingtactiek waardoor toegang tot alle data makkelijk werd gegeven.

En dit gebeurt helaas vaker dan je denkt.

De vraag is dus niet: heb je jouw security al geregeld? Maar eerder:
↳ weet jij zeker dat alles goed staat?

In deze whitepaper helpen we je dat te checken. Met een praktische Salesforce Security Checklist en quick wins om je omgeving direct veiliger te maken.

Maar eerst: hoe werken moderne aanvallen?

Als we kijken naar de meest recente Salesforce-incidenten, dan volgen deze een vergelijkbare aanvalsketen.

Aanvallers maken gebruik van bestaande functionaliteit binnen het platform en proberen gebruikers te misleiden om zo toegang te verlenen. En als ze eenmaal binnen zijn, hebben ze vrij spel.

Typische aanvalsketen:

1. Social engineering (vaak vishing/phishing): Een medewerker wordt misleid en voert een actie uit.
2. Connected App wordt geautoriseerd: Onbewust krijgt een kwaadaardige app toegang tot Salesforce.
3. OAuth-token wordt aangemaakt: De aanvaller krijgt toegang zonder opnieuw in te loggen.
4. Aanvaller gebruikt API-toegang: Data wordt binnengehengeld via legitieme API-toegang.
5. Massale data-export: Grote hoeveelheden data worden geëxporteerd.
6. Afpersing of datalek volgt: De data wordt misbruikt of openbaar gemaakt.

Omdat deze acties vaak lijken op legitiem gebruik van het platform, worden ze niet altijd direct gedetecteerd. Daarom is het essentieel om niet alleen gebruikers te trainen, maar ook de configuratie van jouw Salesforce Security Framework structureel te controleren.

Om een Salesforce-omgeving effectief te beveiligen moeten organisaties kijken naar **vijf kerngebieden:**

1. Identity
Hoe gebruikers inloggen en worden geverifieerd.

2. Access
Welke data gebruikers mogen zien en wijzigen.

3. Integrations
Welke applicaties toegang hebben tot Salesforce.

4. Data protection
Hoe gevoelige data wordt opgeslagen en beschermd.

5. Monitoring
Hoe verdachte activiteiten worden gedetecteerd.

De checklist in deze guide is opgebouwd rondom de bovenstaande gebieden.

Met de vijf kerngebieden in het achterhoofd, hebben wij de onderstaande checklist ontwikkeld om admins te helpen hun Salesforce-omgeving systematisch te controleren.

Gebruik deze lijst als basis voor een periodieke security review of als startpunt voor een uitgebreidere audit.

Salesforce Security Checklist

Brightfox

Security Theme and Subject	Status	Date	Outcome	Cliënt owner	Comment
Session Security					
Time-out voor automatisch uitloggen van inactieve gebruikers					
IP-beperkingen voor inloggen in Salesforce (netwerktoegang)					
Beveiligde verbindingen (HTTPS)					
Tweefactorauthenticatie (2FA)					
Single Sign On (SSO)					
Password Policies					
Geldigheidsduur van wachtwoorden					
Wachtwoordhistorie afdwingen					
Minimale wachtwoordlengte					
Vereisten voor wachtwoordcomplexiteit					
Vereisten voor beveiligingsvragen					
Maximum aantal mislukte inlogpogingen					
Duur van accountvergrendeling					
Complexe/geheime antwoorden voor wachtwoordherstel					
Minimale geldigheidsduur van wachtwoord (minimaal 1 dag)					
Salesforce Security Basics					
Werkwijze rondom phishing en malware in relatie tot Salesforce besproken					
Doorverwijzingsinstellingen naar externe URL's					
Veldgeschiedenis bijhouden (Field History Tracking)					
Audit Trail (logboek van wijzigingen)					
Noodzaak van Salesforce Shield besproken					
Certificaat- en sleutelbeheer					
CSP vertrouwde sites					
Remote Site-instellingen					
Back-upstrategie besproken (wekelijkse export, tools zoals OwnBackup, Spanning)					
Data Accessibility					
Salesforce beveiligingsmodel besproken					
Delen van data binnen de organisatie besproken					
Overzicht datatoegang op basis van rollenhiërarchie					
Privacy by Design: AVG-programma binnen Salesforce					
AVG: inrichting Salesforce Individual-object en processen					
Emailing from Salesforce					
Organisatiebrede e-mailadressen					
Email-to-Case configuratie					
No-reply e-mailinstellingen					
SPF, DKIM, DMARC					
EWS (Exchange Web Services)					
Lightning Sync					
Outlook Add-in					
E-mailafleverbaarheid					
After implementation					
Security Health Check					
Opvolging van bevindingen uit de Health Check					

klik hier om het excel-bestand te downloaden

Ga je liever stapsgewijs door onze Salesforce Security Checklist? Dan hebben we op de volgende pagina's de checklist opgedeeld in verschillende onderwerpen en concrete stappen om af te vinken:

1. Authenticatie & Identity

Een goed beveiligde omgeving begint bij hoe gebruikers inloggen. De meeste aanvallen starten namelijk met een account dat wordt overgenomen of misbruikt. Zorg er daarom voor dat zaken zoals Multi-Factor Authentication (MFA), Single Sign-On (SSO) en sessie-instellingen goed zijn ingericht en regelmatig worden gecontroleerd.

Multi-Factor Authentication (MFA)

- [ ] MFA ingeschakeld voor alle gebruikers
- [ ] MFA-methode: Salesforce Authenticator, TOTP-app of hardware security key
- [ ] Elke gebruiker heeft minimaal twee verificatiemethoden geregistreerd
- [ ] MFA actief op alle inlogmethoden
- [ ] High Assurance session-level vereist voor gevoelige acti
- [ ] MFA-waivers gecontroleerd en beperkt

Single Sign-On (SSO)

- [ ] SSO via SAML of OpenID Connect ingesteld
- [ ] Directe Salesforce-logins uitgeschakeld waar mogelijk
- [ ] Identity Provider beveiligd met MFA en conditional acce
- [ ] SSO-certificaten regelmatig gecontroleerd

2. Toegangsbeheer: Gebruikers & Rollen

Een veelvoorkomende oorzaak van datalekken is dat gebruikers te veel toegang hebben tot data. Als een account wordt overgenomen, kan een aanvaller daardoor direct grote hoeveelheden informatie exporteren. Zorg er daarom voor dat gebruikers alleen toegang hebben tot wat ze echt nodig hebben.

Profielen

- [ ] Geen gebruik van System Administrator voor dagelijkse werkzaamheden
- [ ] Beperkt aantal admin-accounts
- [ ] Overbodige objectrechten verwijderd
- [ ] Export Reports alleen waar nodig
- [ ] API Enabled alleen waar noodzakelijk

Permission Sets

- [ ] Permission Sets gebruikt voor specifieke rechten
- [ ] Permission Set Groups logisch ingericht
- [ ] Regelmatige review van toegewezen permissies
- [ ] Geen ongebruikte permissies met hoge rechten

3. Object- & veldbeveiliging

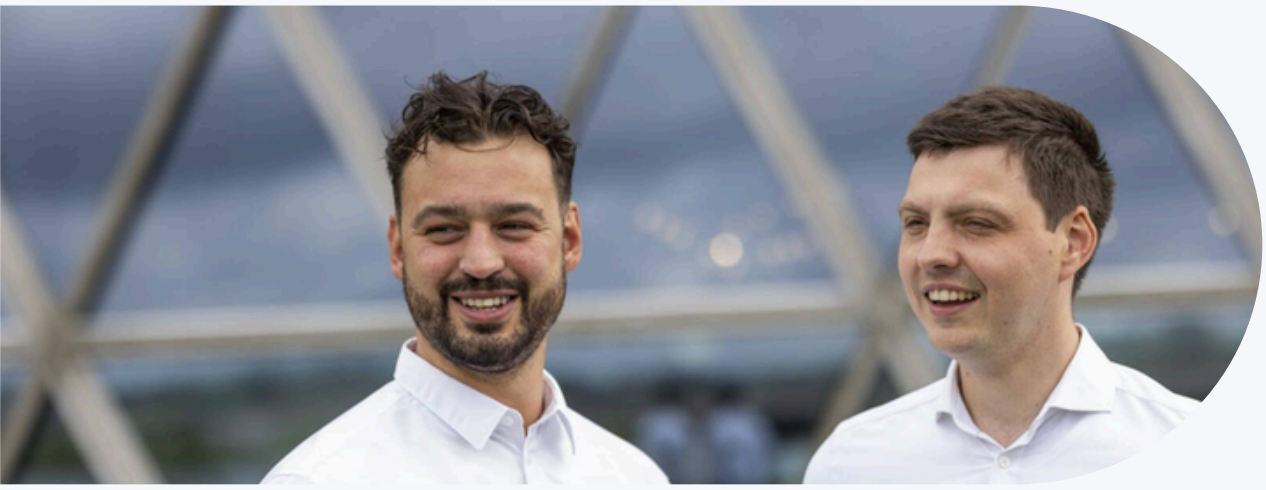
Data-toegang in Salesforce wordt grotendeels bepaald door het datamodel en de sharing-configuratie. Een verkeerde instelling kan ervoor zorgen dat gevoelige informatie zichtbaar is voor te veel users.

Organization-Wide Defaults

- [ ] OWD staat op Private voor gevoelige objecten
- [ ] OWD-instellingen expliciet gecontroleerd voor standaardobjecten
- [ ] Public Read/Write alleen waar noodzakelijk

Field-Level Security

- [ ] Gevoelige velden beperkt tot relevante profielen
- [ ] FLS ingesteld op zichtbaarheid én bewerkbaarheid
- [ ] Shield encryption gebruikt waar nodig



4. Connected Apps & OAuth

Connected Apps vormen een van de meest misbruikte toegangspunten in moderne Salesforce-aanvallen. Wanneer een gebruiker een applicatie autoriseert via OAuth kan deze applicatie toegang krijgen tot Salesforce-data zonder opnieuw MFA te vereisen.

Daarom is governance van Connected Apps essentieel.

- [ ] Inventarisatie van alle Connected Apps
- [ ] Onbekende of ongebruikte apps geblokkeerd
- [ ] 'Admin approved users only' ingesteld
- [ ] OAuth scopes beperkt tot minimum
- [ ] Token-vervaltermijnen ingesteld
- [ ] Consumer secrets regelmatig geroteerd

5. Monitoring & auditing

Last but not least: veel organisaties loggen wel security-events, maar analyseren deze logs niet actief. Monitoring is daarom cruciaal om aanvallen vroeg te detecteren.

Event Monitoring

- [ ] Login events gemonitord
- [ ] API events geanalyseerd
- [ ] Report exports gemonitord
- [ ] Connected App autorisaties gecontroleerd
- [ ] Alerts ingesteld bij verdachte activiteit

10 Quick wins om direct mee te starten

Weet je niet waar je moet beginnen? Start met deze quick wins. Dit zijn acties die je snel kunt uitvoeren en die direct een groot verschil maken in de veiligheid van je Salesforce-omgeving.

1. Health Check
Run de Salesforce Security Health check.

2. Audit connected apps
Verwijder onbekende apps en beperk toegang.

3. Check je OWD-settings
Zorg dat gevoelige data niet toegankelijker is dan nodig.

4. Beperk admin-rechten
Geef alleen adminrechten aan gebruikers die dit nodig hebben.

5. Stel Login IP ranges in
Beperk toegang tot vertrouwde netwerken of VPN.

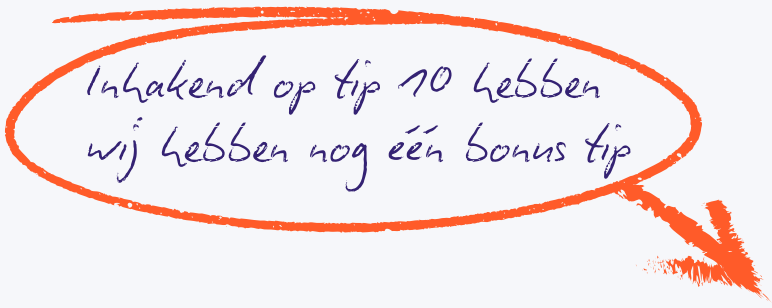
6. Controleer je FLS
Maak gevoelige velden alleen zichtbaar voor de juiste users.

7. Review actieve gebruikers
Verwijder en deactiveer accounts van oud collega's.

8. Check XC guest access
Voorkom dat onbekenden in in Experience Cloud komen.

9. Data protection
Let op verdachte logins, ongebruikelijke locaties/tijden.

10. Security Sessie
Zorg dat medewerkers phishing en social engineering herkennen.



Tip 11: Doe onze Salesforce Security Health Check

En ga van checklist naar act-list.

Wil je zeker weten dat jouw Salesforce-omgeving goed beveiligd is? Veel organisaties denken dat het wel goed zit. Totdat iemand er écht naar kijkt. Daarom helpen wij jou daar graag bij.

Bij Brightfox helpen we je om snel inzicht te krijgen in de risico's in jouw org met onze Salesforce Security Scan.

Tijdens deze Salesforce Security Scan →
Komen wij bij je langs op kantoor en lopen in 2 uur samen je complete Salesforce-omgeving door.

Tijdens deze check kijken onder andere naar:

- ✓ Toegang en gebruikersrechten
- ✓ Connected Apps en integraties
- ✓ Configuratie van je security settings
- ✓ Mogelijke datarisico's

Na de scan ontvang jij →

- ✓ Een duidelijk en praktisch rapport met:
- ✓ Concrete verbeterpunten
- ✓ Snelle quick wins die je direct kunt doorvoeren
- ✓ Langere termijn aanbevelingen

In andere woorden: In 2 uur tijd heb jij direct een handige act list om mee aan de slag te gaan.

Brightfox

Hoe veilig is jouw omgeving?

Wil je zeker weten dat alles goed staat?
Wij kijken graag met je mee en laten je precies zien waar je kunt verbeteren.

In één ochtend inzicht &
Diezelfde dag nog actie en resultaat.

Plan jouw Salesforce Security Scan.

Of neem vrijblijvend contact met ons team
om te sparren over jouw Salesforce org:
via: Brightfox.nl/contact