



Beveiliging Loon Online

Uitleg, maar we kunnen niet alles vertellen

We doen u graag uit de doeken hoe de beveiliging bij Loon Online is geregeld. We kunnen hierbij echter niet al te zeer ingaan op de details. Immers, wanneer wij precies gaan aangeven hoe onze beveiligings-infrastructuur is opgezet, maken wij ons systeem meer ontvankelijk voor een eventuele aanval van buitenaf.

Stap 1) Aanvrager betrouwbaar?

We beginnen met de rdp-file, die u op uw pc heeft staan om in te loggen op Loon Online. Deze is gebaseerd op de zogeheten Remote Desktop van Microsoft. Ook als u met een ander platform dan Windows inlogt, maakt u gebruik van deze technologie.

Zo gauw als u de verbinding maakt met Loon Online en er een verzoek komt om uw referenties (gebruikersnaam en uw wachtwoord) in te voeren, heeft onze firewall al gekeken of de aanvrager digitaal te vertrouwen is. Wij kijken daarbij onder meer naar de geografische ligging van het verzoek, en maken gebruik van geo-blocking: het uitsluiten van verzoeken uit bepaalde gebieden in de wereld.

Stap 2) Versleutelde verbinding

Onze digitale toegangspoort zal nu uw verzoek via een versleutelde verbinding afhandelen, mits u de juiste referenties heeft ingegeven. In de toekomst zullen we dit uitbreiden met een tweeweg authenticatie.

De referenties moeten voldoen aan de 'Password Complexity Requirements' van Microsoft.

Stap 3) Eigen afgeschermd deel Loon Online

Wanneer de verbinding met onze systemen is opgezet, komt u via dezelfde versleutelde verbinding op een Loon Online-server. Uw Loon Online-gedeelte is volledig afgeschermd van dat van de andere gebruikers.

Plus: eigen servers, penetratietests, back-ups, schaduwstelsel en ISO

We doen nog meer dan de bovenomschreven drie stappen om de beveiliging van Loon Online op een hoog niveau te houden.

- Loon Online draait op onze eigen servers. Private cloud, heet dat. We hebben maar liefst 36 eigen servers voor Loon Online in het datacentrum staan.
- Om te testen of de beveiliging van Loon Online correct werkt, houden we regelmatig een

penetratietest op en binnen het systeem, uitgevoerd door verschillende externe partijen.

- Voor de veiligheid van ons systeem houden we dagelijks back-ups bij op disk en wekelijks op tape. NB Dit staat los van uw eigen verantwoordelijkheid om zélf regelmatig back-ups van uw Loon-data te maken. In concreto: bij het afsluiten van Loon (Online) simpelweg aanvinken dat u een back-up wilt wegschrijven.
- En als laatste is het hele systeem ook als schaduwstelsysteem uitgevoerd op een andere locatie dan het hoofdsysteem. Dit alles ondergebracht in datacentra die voldoen aan de ISO27001-normen.

We vertrouwen erop u hiermee voldoende te hebben geïnformeerd over de beveiliging van Loon Online.

