Interlunium

Quick scan digitale soevereiniteit

Test uw afhankelijkheid van Big Tech

Digitale soevereiniteit betekent dat uw organisatie de volledige regie voert over de eigen digitale werkomgeving, zonder digitale afhankelijkheid van proprietary software en/of commerciële kaders van Big Tech.

Wanneer de structuur van uw IT-omgeving in handen is van externe partijen, ontstaan er risico's voor de autonomie, continuïteit en privacy van uw organisatie:

- Geblokkeerde toegang: De leverancier kan de toegang tot uw e-mail en bestanden eenzijdig afsluiten.
- Vendor lock-in: Overstappen is moeilijk of onmogelijk omdat uw data en processen vastzitten in proprietary software.
- Privacyschending: De software verzendt ongemerkt gebruiksgegevens en metadata naar de softwareleverancier zonder dat u deze processen volledig kunt uitschakelen.
- Juridische machteloosheid: Buitenlandse overheden kunnen toegang tot uw data opeisen via de softwareleverancier, buiten de Nederlandse rechter om.
- Gedwongen vervanging: De softwareleverancier bepaalt wanneer uw hardware verouderd is, ook als de hardware zelfs nog jaren goed mee kan.

Interlunium

Doe de Digitale Soevereiniteitscheck

Beantwoord de onderstaande vragen en ontdek direct hoe digitaal soeverein uw organisatie is.

1. Zakelijke e-mail

Welk systeem gebruikt uw organisatie voor het dagelijkse e-mailverkeer?

a) Microsoft Outlook / Exchange
b) Gmail (Google Workspace)
c) Een e-mailomgeving via een internetprovider of hostingpartij (bijv. KPN, Ziggo, TransIP)
d) Een eigen e-mailserver in eigen beheer
e) Anders

2. Cloudopslag

Waar worden de bestanden en documenten van uw organisatie hoofdzakelijk opgeslagen?

a) OneDrive of SharePoint (Microsoft)
b) Google Drive
c) Dropbox Business
d) Op een lokale server binnen het eigen kantoor of een Nederlands datacenter
e) Anders

3. Data-veiligheid en back-up

Hoe is de back-up van uw cloudbestanden (zoals in OneDrive of Google Drive) geregeld?

a) Dat regelt de cloudprovider (b.v. Microsoft of Google) automatisch voor ons.
b) We maken gebruik van een extra online back-updienst van een andere partij.
c) We maken periodiek een kopie naar een eigen server of harde schijf op kantoor.
d) Er is geen aparte back-up; de cloudsynchronisatie is onze back-up.
e) Weet ik niet.

Interlunium

4. Besturingssysteem

Op welk systeem draaien de meeste laptops en computers binnen uw organisatie?

a) Windows (Microsoft)
b) macOS (Apple)
c) ChromeOS (Google)
d) Linux (b.v. Ubuntu)
e) Een mix van bovenstaande

5. Kantoorsoftware

Welke software wordt gebruikt voor tekstverwerking, spreadsheets en presentaties?

a) Microsoft 365/Office (Word, Excel, PowerPoint)
b) Google Workspace (Docs, Sheets, Slides)
c) Een online suite van een andere leverancier
d) LibreOffice of OnlyOffice (lokaal geïnstalleerd)
e) Anders

6. Identiteitsbeheer

Hoe loggen medewerkers in op hun computer en de verschillende bedrijfsapps?

a) Met één centraal Microsoft-account (Entra ID / Azure AD)
b) Met een Google-account
c) Iedere medewerker heeft losse inloggegevens voor elke app
d) Met een eigen gebruikersnaam/wachtwoord beheerd door de eigen organisatie
e) Weet ik niet

Interlunium

Puntentoekenning

Vraag 1

Bij keuze A of B: **0 punten**

- Achtergrond: Uw mailverkeer loopt via servers van een Amerikaanse partij.
- Wat dit betekent: De provider heeft technisch de mogelijkheid om uw account te blokkeren zonder tussenkomst van een rechter. Omdat uw mail in hun specifieke formaat staat, is het archief mogelijk niet zomaar te verhuizen naar een andere partij. U loopt het risico om toegang te verliezen. De provider heeft technisch de macht om uw account eenzijdig te blokkeren zonder tussenkomst van een rechter. Daarnaast loopt u ook een exportrisico: Hoewel migratie via standaarden zoals IMAP technisch mogelijk is zolang uw account actief is, verliest u bij een blokkade direct de toegang tot deze exportmogelijkheid. Tenslotte maken sommige providers gebruik van eigen, gesloten formaten waardoor een volledige overstap naar een andere partij vaak complex is en uw archief technisch toch gevangen blijft in hun ecosysteem.
- De soevereine oplossing: Gebruik van open e-mailstandaarden (denk aan IMAP) op een server die onder uw eigen beheer en de Nederlandse wet valt.

Bij keuze C: **5 punten**

- Achtergrond: U bent juridisch beschermd door Nederlands recht, maar technisch blijft u afhankelijk van de beheerder van de server voor uw toegang.
- Wat dit betekent: De beheerder heeft toegang tot uw data en kan de toegang beperken. Daarnaast is het archief mogelijk niet eenvoudig te exporteren, waardoor u voor de continuïteit van uw historische correspondentie vastzit aan deze specifieke provider.
- De soevereine oplossing: Gebruik van open e-mailstandaarden op een server die onder uw eigen beheer en de Nederlandse wet valt.

Bij keuze E: **5 punten**

- Achtergrond: Een alternatieve leverancier biedt geen automatische garantie op digitale soevereiniteit.
- Wat betekent dit: Het kritieke punt is de mate van beheer: tenzij u gebruikmaakt van open-source software onder eigen beheer, blijft er een risico op afhankelijkheid bestaan. U moet zelf oordelen: heeft de leverancier de technische macht om u buiten te sluiten of uw data in te zien, of heeft u zelf de volledige controle over de broncode en de infrastructuur?
- De soevereine weg: Echte soevereiniteit is pas bereikt wanneer u niet langer afhankelijk bent van de welwillendheid of de voorwaarden van een externe partij, maar zelf de 'uit-knop' in handen heeft.

Bij keuze D: **10 punten**

- Goed bezig! U behoudt de regie. Door gebruik te maken van open standaarden bent u niet gebonden aan de grillen van één specifieke softwareleverancier. U kunt uw volledige archief verhuizen wanneer u dat wilt, zonder technische obstakels.

Interlunium

Vraag 2

Bij keuze A, B of C: **0 punten**

- Achtergrond: Uw data valt onder de Amerikaanse wetgeving (zoals de Cloud Act).
- Wat dit betekent: Buitenlandse overheden kunnen toegang tot uw bedrijfsdata opeisen zonder dat u daar toestemming voor geeft. Daarnaast heeft de leverancier technisch de macht om uw toegang eenzijdig te blokkeren en heeft deze in principe toegang tot uw data. Bij een eventuele overstap betaalt u vaak hoge kosten om uw data weer weg te halen ("egress fees").
- De soevereine oplossing: Dataopslag op Nederlandse bodem onder exclusief Nederlandse wetgeving, waarbij u de enige bent met de technische toegangssleutel en de volledige controle over de infrastructuur.

Bij keuze E: **5 punten**

- Achtergrond: Een alternatieve opslagmethode buiten de grote drie (Microsoft, Google, Dropbox) vraagt om een kritische beoordeling van de technische inrichting.
- Wat dit betekent: Onduidelijke regie: Tenzij u gebruikmaakt van een volledig eigen server of een platform waarbij de leverancier technisch niet kan meekijken (omdat alleen u de digitale sleutel bezit), blijft u kwetsbaar. U moet zelf oordelen: heeft de leverancier de macht om uw bestanden in te zien of de toegang te blokkeren? Als u niet de enige bent met de 'sleutel', heeft u de risico's op juridische machteloosheid of toegangsverlies nog niet volledig geëlimineerd.
- De soevereine oplossing: Echte soevereiniteit ontstaat pas wanneer u de data opslaat op een plek waar u niet alleen de eigenaar bent van de bestanden, maar ook de enige bent die de toegang tot die bestanden heeft en als enige kan beslissen wie nog meer toegang krijgt.

Bij keuze D: **10 punten**

- Goed bezig! Uw data valt onder Nederlands recht en u bepaalt zelf wie er technisch toegang krijgt. Hiermee voorkomt u dat buitenlandse overheden data opeisen én dat commerciële derden of beheerders ongevraagd kunnen meekijken in uw bedrijfsgevoelige informatie.

Vraag 3

Bij keuze A, B of D: **0 punten**

- Achtergrond: Synchronisatie is geen back-up.
- Wat dit betekent: Als een medewerker per ongeluk een map verwijdert of als een virus (ransomware) uw bestanden versleutelt, wordt die fout direct doorgegeven aan de cloud. De provider bewaart verwijderde bestanden vaak maar kort. Als uw account wordt geblokkeerd, kunt u bovendien ook niet meer bij uw 'back-up' omdat die op dezelfde plek staat.
- De soevereine oplossing: Een onafhankelijke, versleutelde back-up op een locatie waar jij de enige eigenaar van bent. Zo blijven je gegevens altijd beschikbaar, zelfs als de cloudprovider wegvalt of je account blokkeert.

Bij keuze E: **0 punten**

- Achtergrond: Onwetendheid over de back-upstrategie is een van de grootste risico's voor de bedrijfscontinuïteit.
- Wat dit betekent: Kritiek risico: Als u niet precies weet waar uw reservekopie staat en wie de toegang beheert, moet u er vanuit gaan dat u bij een calamiteit (zoals ransomware of een accountblokkade) geen toegang heeft tot uw historische data. Zonder een aantoonbare, onafhankelijke kopie in eigen beheer is uw data bij een incident feitelijk onherstelbaar.
- De soevereine oplossing: Inventariseer direct waar uw data wordt veiliggesteld. Echte soevereiniteit begint bij de zekerheid dat u de enige eigenaar bent van een actuele reservekopie die fysiek en logisch losstaat van uw cloudprovider.

Bij keuze C: **10 punten**

- Goed bezig! Een onafhankelijke, eigen kopie is de enige manier om continuïteit te garanderen. Uw dataherstel is niet afhankelijk van de beschikbaarheid of de voorwaarden van een extern platform of cloudprovider.

Vraag 4

Bij keuze A, B of C: **0 punten**

- Achtergrond: U werkt op een gesloten besturingssysteem waar u geen volledige controle over heeft.
- Wat dit betekent: Het systeem stuurt op de achtergrond continu gegevens (telemetrie) over uw locatie en uw gebruik naar de fabrikant. U kunt dit niet volledig uitzetten. Ook bepaalt de fabrikant wanneer uw hardware 'verouderd' is en vervangen moet worden.
- De soevereine oplossing: Een open-source besturingssysteem dat standaard geen gegevens verzendt en werkt op de hardware die u kiest.

Bij keuze E: **5 punten**

- Achtergrond: Een versnipperd landschap van verschillende besturingssystemen maakt het beheer van privacy en veiligheid complex.
- Wat dit betekent: Gedeeltelijke privacyschending: Voor alle apparaten die binnen uw mix op Windows, macOS of ChromeOS draaien, blijft de ongewenste verzending van gegevens (telemetrie) naar de fabrikant actief. U heeft slechts voor een deel van uw organisatie de regie op data en hardware-levensduur hersteld; de zwakste schakels bepalen uw totale risicoprofiel.
- De soevereine oplossing: Streef naar een uniform beleid op basis van open-source software. Alleen door over de gehele breedte de controle over de datastromen terug te pakken, voorkomt u dat informatie over uw bedrijfsvoering ongemerkt uw computers verlaten.

Bij keuze D: **10 punten**

- Goed bezig! Op een open-source systeem bepaalt u zelf welke gegevens wel of niet worden gedeeld. Er worden geen ongewenste gegevens naar een fabrikant verzonden en de software bepaalt niet langer hoelang uw hardware meegaat. U bent eigenaar van het systeem, in plaats van een gebruiker onder voorwaarden.

Interlunium

Vraag 5

Bij keuze A of B: **0 punten**

- Achtergrond: U bent voor uw dagelijkse werkzaamheden afhankelijk van een online abonnement.
- Wat dit betekent: U bent operationeel afhankelijk van een externe partij. Bij Google Workspace stopt uw werkproces direct zodra de internetverbinding of uw account wegvalt, aangezien de software volledig in de cloud draait. Bij Microsoft 365 kunt u tijdelijk offline doorwerken, maar blokkeert de bewerkingsfunctie zodra de periodieke licentiecontrole via internet faalt. In beide gevallen bent u geen eigenaar van uw werkmiddelen, maar slechts huurder. Ook heeft u geen controle over gedwongen software-updates of datastromen naar de fabrikant.
- De soevereine oplossing: Software die 100% lokaal werkt en gebruikmaakt van open standaarden, zodat documenten altijd leesbaar blijven, ook zonder abonnement.

Bij keuze C: **0 punten**

- Achtergrond: U heeft gekozen voor een alternatieve provider, maar het leveringsmodel blijft hetzelfde: software-as-a-service (SaaS).
- Wat dit betekent: Operationele afhankelijkheid: Hoewel u niet bij de grootste spelers zit, blijft u afhankelijk van de internetverbinding en de stabiliteit van deze specifieke aanbieder. Als zij hun voorwaarden wijzigen of de stekker eruit trekken, stopt uw werkproces onmiddellijk.
- De soevereine weg: Kies voor kantoorsoftware die volledig lokaal op uw hardware draait, zodat uw productiviteit nooit afhankelijk is van de status van een externe server.

Bij keuze E: **5 punten**

- Achtergrond: Een afwijkende keuze voor kantoorsoftware vereist een check op de feitelijke controle die u heeft.
- Wat dit betekent: Onduidelijke regie: De belangrijkste vraag is: werkt deze software ook als de leverancier morgen stopt te bestaan? Als er een constante licentiecontrole of internetverbinding nodig is, zit u alsnog in een vendor lock-in. U moet zelf oordelen: bezit u de volledige vrijheid om de software te blijven gebruiken op uw eigen apparaten, zonder dat een externe partij een 'achterdeur' heeft om uw toegang af te sluiten?
- De soevereine weg: Echte digitale soevereiniteit betekent dat uw documenten en software altijd van u blijven, ongeacht contracten of verbindingen met de buitenwereld.

Bij keuze D: **10 punten**

- Goed bezig! U bent operationeel onafhankelijk. Uw documenten blijven toegankelijk en bewerkbaar, ongeacht internetverbinding of licentiestatus bij een externe partij. U werkt met open documentformaten die ook in de toekomst leesbaar blijven.

Interlunium

Vraag 6

Bij keuze A of B: **0 punten**

- Achtergrond: Uw digitale identiteit ligt in handen van een commerciële partij in de VS.
- Wat dit betekent: De leverancier heeft de 'uit-knop' van uw organisatie bedrijf in handen. Zij kunnen de toegang tot uw hele digitale werkomgeving in één klap afsluiten.
- De soevereine oplossing: Eigen beheer van de gebruikersaccounts, waarbij de organisatie zelf bepaalt wie wanneer toegang heeft, zonder afhankelijkheid van een extern platform.

Bij keuze C: **5 punten**

- Achtergrond: Het ontbreken van een centraal beheersysteem creëert een versnipperde digitale veiligheid.
- Wat dit betekent: Regieverlies: Hoewel u niet afhankelijk bent van één grote Big Tech-partij, heeft u als organisatie geen centrale 'noodrem'. Als een medewerker uit dienst gaat of een apparaat wordt gestolen, is het handmatig blokkeren van alle losse accounts foutgevoelig en traag. U heeft de regie over wie toegang heeft tot uw bedrijfskritische data gedelegeerd aan de individuele medewerker.
- De soevereine weg: Voer een centraal identiteitsbeheer in eigen regie. Hiermee combineert u het gemak van één inlog met de veiligheid dat u als organisatie op elk moment zelf de toegangssleutels kunt beheren, zonder afhankelijk te zijn van externe cloudprofielen.

Bij keuze E: **0 punten**

- Achtergrond: Onwetendheid over hoe de toegang tot uw systemen is beveiligd, is een fundamenteel beveiligingslek.
- Wat dit betekent: Kritiek risico: Als u niet weet wie de 'digitale sleutels' van uw organisatie beheert, kunt u ook niet garanderen dat deze toegang soeverein en veilig is. U loopt het risico dat een externe partij of een vergeten account de zwakke plek vormt waardoor onbevoegden toegang krijgen tot uw gehele netwerk.
- De soevereine weg: Breng onmiddellijk in kaart hoe de authenticatie binnen uw organisatie is ingericht. Digitale soevereiniteit begint bij het volledige inzicht in, en de controle over, de digitale identiteit van uw medewerkers.

Bij keuze D: **10 punten**

- Goed bezig! U bezit de toegangssleutels. Door uw eigen identiteitsbeheer te voeren, kan geen enkele externe partij uw medewerkers de toegang tot de werkomgeving ontzeggen. U heeft de volledige controle over wie wanneer bij uw systemen kan.

Interlunium

Score

Kritieke afhankelijkheid: 0 - 20 punten

- De continuïteit van uw organisatie ligt volledig in handen van externe partijen.

Gedeeltelijke autonomie: 25 - 45 punten

- U heeft stappen gezet, maar bent technisch nog kwetsbaar voor de 'uit-knop' van derden.

Digitaal soeverein: 50 - 60 punten

- U voert de regie en bezit de exclusieve controle over uw eigen digitale werkomgeving.

Wat nu?

Deze vragenlijst heeft als doel om snel inzicht te geven in hoe soeverein uw organisatie is.

Interlunium helpt organisaties digitale soevereiniteit te realiseren. We bieden inzicht in de digitale afhankelijkheden in uw organisatie en de risico's die dit met zich meebrengt voor de continuïteit, privacy, data, processen en de beheersbaarheid van kosten. Interlunium helpt u deze risico's te beheersen door het realiseren van volledige digitale soevereiniteit.

Met heldere analyses, praktische begeleiding en toekomstbestendige oplossingen ondersteunt Interlunium bedrijven in hun overstap naar digitale omgeving met meer autonomie, privacy en controle.

Wilt u de volgende stap zetten naar digitale soevereiniteit? Neem contact op met Interlunium en ontdek hoe uw organisatie de controle kan terugpakken.

Interlunium BV
Stationsplein 45 | Unit E7.154
3013 AK Rotterdam

W interlunium.nl
E yesreply@interlunium.nl
T 085 - 36 96 136