



SECURITY ASSESSMENT

Gebaseerd op



2SOURCE4.COM



Versterk je digitale veiligheid. **HET BELANG VAN INZICHT**

In een markt die pijlsnel verandert sta je als operationeel verantwoordelijke van een organisatie voor unieke uitdagingen.

Cyberdreigingen worden steeds geavanceerder en de bescherming van jouw bedrijfsgegevens en -systemen is belangrijker dan ooit. Maar hoe weet je of jouw huidige beveiligingsmaatregelen voldoende zijn?

En hoe kun je effectief navigeren door de complexiteit van digitale veiligheid, terwijl je liever aandacht wilt geven aan groei en innovatie?

Het Security Assessment van 2source4 is jouw antwoord op deze vragen. Dit assessment is niet zomaar een veiligheidscheck; het geeft belangrijke inzichten in de huidige staat van de digitale beveiliging van jouw organisatie en een routekaart biedt naar een veiligere toekomst.

Ons Security Assessment is een belangrijk onderdeel van jouw beveiligingsstrategie en kan jouw organisatie transformeren.

Waarom het **SECURITY ASSESSMENT** belangrijk is voor jou?

Als operationeel verantwoordelijke is het essentieel dat je een helder inzicht hebt in de beveiligingsstatus van jouw organisatie. Het Security Assessment van 2source4 biedt waardevolle inzichten en oplossingen voor verschillende uitdagingen:

Geen inzage in je huidige beveiligingsstatus

Als je momenteel geen duidelijk beeld hebt van hoe goed jouw organisatie beschermd is tegen digitale dreigingen, biedt dit rapport een gedetailleerd overzicht en inzicht in de huidige veiligheidsmaatregelen.

Als je niet weet waar je moet beginnen

Voor het geval je niet zeker weet waar te beginnen met het verbeteren van jouw beveiliging, helpt ons rapport bij het opstellen van een effectieve roadmap. Dit stelt prioriteiten voor acties en verbeteringen op basis van jouw specifieke situatie.

Behoeft een second opinion

Het kan altijd nuttig zijn een externe, professionele blik te werpen op jouw bestaande cybersecurity. Ons rapport biedt een deskundige second opinion, waardoor je vanuit meerdere perspectieven weet hoe je ervoor staat en waar verbeterlagen mogelijk zijn, die mogelijk over het hoofd zijn gezien.



Essentiële aspecten van **DIGITALE BEVEILIGING**

Bij 2source4 gaan we veel verder dan alleen het analyseren van wat data. We dompelen ons helemaal onder in jouw bedrijfsomgeving en bieden een helder overzicht, waarbij we elk element zorgvuldig onderzoeken. We belichten niet alleen de risico's, maar geven ook inzicht in de complexiteit van jouw specifieke situatie en adviseren over wat je als eerste zou moeten aanpakken.

Onze aanpak richt zich op vier essentiële aspecten van digitale beveiliging:

Toegangsbeheer:

De sleutel tot het beschermen van jouw organisatie begint bij het beheren wie toegang heeft tot jouw systemen en data. Effectief toegangsbeheer zorgt ervoor dat alleen geautoriseerde personen toegang hebben tot gevoelige informatie, wat cruciaal is voor het handhaven van de veiligheid en integriteit van jouw bedrijfsgegevens.

Apparaatbeheer:

In een tijdperk waarin mobiele apparaten en werken op afstand steeds gangbaarder worden, is het beveiligen en beheren van alle apparaten die toegang hebben tot jouw netwerk essentieel. Dit omvat het up-to-date houden van apparaten en ervoor zorgen dat ze voldoen aan jouw beveiligingsbeleid, om zo kwetsbaarheden te minimaliseren.

Cyberbeveiliging en gevaar detectie:

Dit omvat alle maatregelen die genomen worden om jouw netwerken, systemen en data te beschermen tegen digitale aanvallen. Dit kan variëren van het voorkomen van malware en phishing-aanvallen tot het beschermen tegen datalekken en het detecteren van aanvallen, waarbij zowel technologie als menselijke factoren een rol spelen.

Gegevensbeveiliging en compliance:

Het beschermen van gevoelige gegevens is meer dan alleen een technische uitdaging; het vereist ook naleving van relevante wet- en regelgeving zoals AVG en ISO-standaarden. Het gaat om het veiligstellen van jouw gegevens tegen ongeautoriseerde toegang en het zorgen voor de integriteit en privacy van de informatie die jouw organisatie verwerkt.



Wat zijn de **4 ESSENTIËLE PIJLERS VAN DIGITALE BEVEILIGING** die de Microsoft-suite biedt?

Microsoft 365 omvat een geïntegreerde set oplossingen die productiviteit en beveiliging naadloos combineren. Onze aanpak richt zich op de vier essentiële pijlers van digitale beveiliging. Dat vertalen we naar de vier essentiële pijlers die de Microsoft 365-suite biedt om organisaties te helpen hun data, apparaten en bronnen optimaal te beveiligen. Deze pijlers zijn:

01 Identity & Access Management

Toegangsbeheer en identiteitsmanagement zijn cruciaal voor de veiligheid van jouw organisatie. Identity & Access Management van Microsoft omvat een reeks processen en technologieën die zorgen dat alleen geautoriseerde gebruikers – dat kunnen werknemers zijn, maar ook partners of klanten – op de juiste manier toegang krijgen tot bedrijfsbronnen. Belangrijke functies zoals multi-factor-authenticatie, eenmalige aanmelding en identiteitsbeheer zorgen ervoor dat jouw bedrijfsomgeving veilig en beschermd blijft tegen ongeautoriseerde toegang.

Microsoft Entra

02 Device Management

In het kader van apparaatbeheer biedt Microsoft Intune uitgebreide oplossingen voor het monitoren, beheren en beveiligen van alle apparaten binnen jouw organisatie. Dit zorgt ervoor dat elk apparaat, van computers tot smartphones, tablets en andere apparaten, veilig, up-to-date en in overeenstemming is met jouw beveiligingsbeleid. Intune faciliteert een naadloze integratie van apparaatbeheer met jouw bedrijfsprocessen.

Microsoft Intune



03 Cyber Security

Voor cyberbeveiliging biedt Microsoft Defender een reeks van robuuste verdedigingsmechanismen om jouw netwerken, systemen en data te beschermen. Van het voorkomen van malware en phishing-aanvallen tot het beschermen tegen datalekken, Microsoft Defender integreert geavanceerde beveiligingstechnologieën en strategieën om jouw digitale omgeving te verdedigen.

Microsoft Defender

04 Compliance & Data Security

Binnen de context van Gegevensbeveiliging en Compliance biedt Microsoft Purview een allesomvattende oplossing. Het beschermt niet alleen jouw gegevens tegen ongeoorloofde toegang, maar zorgt er ook voor dat jouw organisatie voldoet aan wet- en regelgeving zoals AVG en ISO-standaarden. Purview waarborgt de integriteit en privacy van gevoelige informatie en zorgt ervoor dat jouw organisatie op een verantwoorde manier met data omgaat.

Microsoft Purview

CIS MICROSOFT 365 BENCHMARK, wat is het en waarom is het belangrijk?

De CIS Microsoft 365 Benchmark maakt deel uit van een uitgebreide set richtlijnen, ontwikkeld door het Center for Internet Security (CIS), die bedoeld zijn om jouw organisatie te ondersteunen bij het veilig configureren van systemen en software, specifiek binnen de Microsoft 365-omgeving.

Ontworpen door een wereldwijd netwerk van beveiligingsexperts, biedt de CIS Microsoft 365 Benchmark een verzameling van geconsolideerde best practices en gedetailleerde beveiligingsaanbevelingen.

Deze zijn speciaal samengesteld om jouw Microsoft 365-omgeving (voorheen Office 365) optimaal en veilig in te richten.

De CIS Microsoft 365 Benchmark behandelt diverse cruciale aspecten, waaronder:

- ✓ **Configuratie van Azure Active Directory**
- ✓ **Beveiligingsinstellingen van Microsoft Exchange Online**
- ✓ **Informatiebescherming en naleving**
- ✓ **Configuraties van Microsoft Teams, SharePoint en OneDrive**



Waarom is dit WAARDEVOL voor jouw organisatie?

Deze benchmark is een instrument om het risico op beveiligingsinbreuken te verminderen. Door de aanbevelingen op te volgen, zorg je ervoor dat jouw implementatie van Microsoft 365 voldoet aan erkende industriestandaarden en best practices. Dit helpt jouw organisatie niet alleen om veiliger te werken, maar zorgt ook voor een betrouwbare naleving van relevante regelgeving.

Het is echter belangrijk om te beseffen dat, hoewel de aanbevelingen van de CIS Microsoft 365 Benchmark hoog aangeschreven staan en betrouwbaar zijn, ze altijd geëvalueerd moeten worden binnen de specifieke context van jouw organisatie. Jouw unieke behoeften en vereisten bepalen hoe je deze richtlijnen het beste kunt toepassen.

Gegeven de complexiteit en de nuances van een veilige inrichting, kan de expertise en het scherpe oog van een professional het verschil maken in het optimaal benutten van deze richtlijnen voor jouw specifieke situatie.



Hoe komen we tot jouw unieke **SECURITY ASSESSMENT?**

01

Kick-Off met een kennismakingsgesprek en planning

Ons proces begint met een persoonlijk kennismakingsgesprek. Hierin bespreken we jouw specifieke behoeften en stellen we een gedetailleerde planning op voor de veiligheidsanalyse.

**02**

Toegang verkrijgen en starten van de analyse

Je geeft ons een veilige toegang tot jouw IT-omgeving, wat de basis vormt voor onze diepgaande analyse.

**03**

Bespreken van de huidige situatie en verheldering waar nodig

We gaan om tafel om onze eerste bevindingen en eventuele onduidelijkheden te bespreken.

**04**

Verwerken van informatie

Alle verzamelde gegevens gaan we zorgvuldig analyseren en verwerken, wat de basis vormt voor het opstellen van jouw Security Assessment.

05

Ingediend veiligheidsrapport

Na de analyse en verwerking van gegevens, voltooien we het veiligheidsrapport en dienen dit bij jou in voor beoordeling.

**06**

Gezamenlijke analyse van het beveiligingsrapport

In een tweede bijeenkomst nemen we samen het voltooide rapport door. Dit is een interactieve sessie waarin we alle aspecten van het rapport bespreken.

**07**

Vragen, antwoorden en optimalisatietips

Als afsluiting bieden we antwoorden op al jouw vragen en delen we praktische tips om jouw beveiliging zo optimaal mogelijk te maken.

Over **2SOURCE4**

Het team van 2source4 heeft maar één ultiem doel, en dat is een happy user. Dat bereik je niet door je te focussen op de beste techniek of de meest concurrerende prijs. Als wij in gesprek gaan met jou, focussen we op de wensen en behoeften van jou en je medewerkers. Wij denken mee hoe je het werk van je medewerker makkelijker en leuker kunt maken zodat ze beter kunnen bijdragen aan de doelstellingen van de organisatie. Samen werken we aan de beste oplossing. De techniek? Die kan je ook bij een ander halen. De oplossing? Daarin maken wij het verschil.

Wij denken mee hoe je het werk van je medewerker makkelijker en leuker kunt maken zodat ze beter kunnen bijdragen aan de doelstellingen van de organisatie. Samen werken we aan de beste oplossing. De techniek? Die kan je ook bij een ander halen. De oplossing? Daarin maken wij het verschil

Meer op:

www.2source4.com

Onze oplossing en aanpak

Bij 2source4 helpen we je graag bij het opzetten van een kostenefficiënte en veilige IT- omgeving. We bieden oplossingen die gebaseerd zijn op Microsoft-technologie en die jouw IT-organisatie een solide basis geven.

Bij 2source4 helpen we je graag!

contact@2source4.com**Bel nu! +31 33 299 0994**