DATAMANAGEMENT
BEVEILIGING
BEREIKBAARHEID
BEHEERSBAARHEID
BESCHIKBAARHEID

Door vele jaren ervaring in het ontwerpen en implementeren van complexe datawarehouse, back-up en security oplossingen, kunnen wij wel stellen dat datamanagement onze specialisme is geworden. Door onze kennis zijn wij in staat om in te spelen op iedere situatie en behoefte van onze klanten.

Voor ons is het vanzelfsprekend dat we met de klant meedenken: eerst goed de ‘business’ van de klant begrijpen en daarna pas adviseren over een oplossing. Het is onze missie is om niet enkel een product te verkopen, maar door onze uitgebreide kennis zo onderscheidend te zijn dat elke klant uiterst tevreden is over onze high-end oplossingen.

Wij willen hoogstaande kwaliteit leveren. Deze eis stellen we niet alleen aan onze medewerkers, maar ook aan onze partners. We initiëren projecten en bedenken oplossingen om maximale resultaten te behalen. Onze oplossingen komen voort uit visie, inhoudelijke kennis, de juiste producten en een flinke dosis enthousiasme.

io4u
Our knowledge is your solution

Leeghwaterstraat 3-01
2811 DT Reeuwijk
085 9020 470 tel
www.io4u.nl

io4u
Our knowledge is your solution

Our knowledge is your SOLUTION

IO4U KNOWLEDGE

- DATA SECURITY
- (CLOUD) DATA MANAGEMENT
- BACK-UP & RECOVERY
- ARCHIVERING

Introductie

EEN KORTE INTRODUCTIE VAN IO4U

IO4U is een IT-organisatie die customer centric werkt. Wij leveren oplossingen en diensten op het gebied van gegevensbeveiliging en beheer. Het is onze ambitie om bij te dragen aan de bedrijfscontinuïteit van onze klanten door belangrijke data, informatie en IT-infrastructuren te beschermen met pragmatische oplossingen en diensten. IO4U biedt oplossingen en services om uw gegevens te beveiligen:

- Data Security Improvement
- Cloud Data Management
- Back-up & Recovery
- Archivering

Thuiswerken niet meer weg te denken

Nederland blijft doorwerken tijdens de coronacrisis, veelal in de vorm van thuiswerken. Ook als de normale leef- en werksituatie straks weer enigszins is teruggekeerd, is het thuiswerken hoogstwaarschijnlijk niet meer weg te denken uit onze economie. Met het thuiswerken neemt ook de kans op cybercriminaliteit drastisch toe voor bedrijven en instellingen.

Risico's en cybercriminaliteit

Cybercriminaliteit professionaliseert zich de afgelopen tijd in een rap tempo. Cybercriminaliteit is "big business", nu al zijn de verdiensten in cybercriminaliteit op jaarbasis hoger dan de tevens wereldwijd verspreidde drugshandel. Voor cybercriminelen is deze crisis de uitgelezen kans om gevoelige informatie of data buit te maken.

Aangezien de werksituatie voor werknemers anders is dan op het bedrijf is het van bedrijfsbelang dat men in een goed beveiligde thuiswerkomgeving werkt en dat men als werknemer goed op de hoogte is welke beveiligings-procedures zijn afgesproken.

Uit ervaring weten wij dat de beveiliging minder goed of in sommige situatie zelfs helemaal niet op orde is dan op het werk zelf. Het risico dat gevoelige of privacygevoelige gegevens op straat kunnen komen te liggen is daarom reëel. Tevens kunt de dupe worden van internetcriminelen (Ransomware) en daardoor (imago- en/of financiële) schade oplopen.

Security Quickscan Thuiswerken

Om dergelijke issues te voorkomen is het van belang om een goed beeld te hebben welke risico's er zijn inzake het thuiswerken. Met onze Security Quickscan Thuiswerken krijgt u binnen twee weken inzicht in het niveau van uw beveiligingsmaatregelen en mogelijke blinde vlekken inzake het telewerken.
Deze quickscan bestaat uit een inventarisatie van de aanwezige maatregelen, procedures en voorzieningen. Op basis van onze ervaring met vergelijkbare organisaties kunnen wij u ook een indruk geven of uw beveiliging marktconform is.

Onderzocht wordt onder meer:

- Hoe "aware" zijn uw medewerkers inzake het informatiebeveiligingsbeleid thuiswerken?
- Welke maatregelen heeft men genomen tegen "phishing"?
- Welke maatregelen heeft men genomen inzake het veilig en verantwoord video-conferecen / chatten?
- Hoe veilig zij de cloud-, opslag- of e-maildiensten die men ten behoeve van het thuiswerken gebruikt?
- Hoe gaat men thuis om met privacy gevoelige gegevens en met bijzondere persoonsgegevens?
- Welke opslagvoorzieningen gebruikt men inzake het veilig opslaan van gevoelige bedrijfsgegevens?Welke gedragscodes hanteert men als bedrijf inzake het thuiswerken?

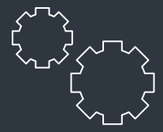
Rapportage

U ontvangt een duidelijk verslag waarin de belangrijkste aandachtspunten inzake het beveiligingsniveau thuiswerken staan beschreven: welke belanghebbenden lopen ten aanzien van de datastromen welke risico's? De risisco's worden duidelijk ten aanzien van de wel of niet volgen vanafgesproken bedrijfsprocedures en bedrijfskprocessen, toepasselijke wetgeving en gebruik- en instellingen van ICT apparatuur.

IO4U stelt de risisco's centraal van thuiswerken en de verantwoordelijkheid voor deze risisco's zijn afdelingsniveau overstijgend! IO4U is als geen ander in staat om voor de directie een overzicht tegeven van uw beveiligingsinformatieniveau van de thuiswerksitsuatie van uw medewerkers!

Kosten van deze quickscan zijn:

Tot 25 thuiswerkers	€ 1750,00
25 tot 50 thuiswerkers	€ 2500,00
Meer dan 50 thuiswerkers	prijs op aanvraag



Performance

IO4U biedt tevens de kennis en oplossingen om iedere omgeving te versnellen. Of het nu gaat om het versnellen van High performance databases of het versnellen van Virtuele desktops en servers.

Performance optimalisatie biedt u naast snelheidswinst ook kostenverlaging en een verhoging van gebruikerstevredenheid.

Datamanagement

Door een gedegen kennis te combineren met goede ervaring op het gebied van het gebruikte 'ijzer', zijn wij in staat complexe Storage en back-up omgevingen (inclusief de hierin gebruikte servers) te ontwerpen, op te zetten en te onderhouden.

Security

Ons diensten portfolio bevat de juiste elementen om stapsgewijs uw informatiebeveiliging te bevorderen. Met een integrale aanpak of een selectie van diensten is het mogelijk om inzage en verbetering te krijgen in de status van uw informatiebeveiliging.