

10 aandachtspunten om de continuïteit van uw ICT te waarborgen



Hieronder vindt u een aantal belangrijke aandachtspunten voor de continuïteit van uw automatisering. Soms heel voor de hand liggend, maar daarom niet minder belangrijk. We zien in de praktijk vaak dat het bij de uitvoering op de details fout gaat.

1. toegangsrechten

Kunnen alleen bevoegden bij vertrouwelijke data?

Controleer (met uw systeembeheerder) periodiek de toegangsrechten van uw gebruikers.

2. gebruikersrechten

Wat mag een gebruiker zelf op uw netwerk?

Een gebruiker die zelf software kan installeren is één van de grootste bedreigingen voor uw netwerk. De kans op besmetting met spyware, virussen, e.d. neemt hierdoor enorm toe.

Scherm uw netwerk zo af dat gebruikers zelf geen software kunnen installeren en wijzigen.

3. licenties

Heeft u een goed licentiebeleid?

Met een goed licentiebeleid voorkomt u onverwachte problemen vanwege illegaal licentiegebruik. Licenties geven u vaak ook recht op de juiste ondersteuning van de leverancier bij problemen.

Maak een overzicht van het softwaregebruik en de licentiecontracten. U weet dan wat u nodig heeft, welke licenties u heeft en wanneer de licenties en de support komen te vervallen. Het is belangrijk dat u dit overzicht up-to-date houdt.

4. back-ups

Let altijd op de volgende punten:

- Worden er dagelijks back-ups gemaakt?
- Is er van al uw data een back-up?
- Worden back-ups op een andere fysieke locatie bewaard?
- Wordt gecontroleerd of de back-ups geslaagd zijn?
- Worden de back-ups periodiek als test teruggezet? Pas dan is het echt zeker of een back-up bruikbaar is.

Maak een schema om al deze punten periodiek te controleren. Controleer of alle belangrijke data op laptops, lokale pc's en server(s) meegenomen wordt in de back-up procedure. Deze punten gelden ook als u een online back-up oplossing gebruikt.

5. beveiligingsbewustzijn

Zijn uw gebruikers bewust van beveiligingsrisico's?

Wachtwoorden mogen nooit aan anderen gegeven worden en ze mogen ook niet op of rond het bureau slingeren (bv. post-it op het beeldscherm).

Heeft u een wachtwoordbeleid?

Complexe wachtwoorden die regelmatig gewijzigd worden, zijn noodzakelijk om uw data te beschermen.

6. internetbeveiliging

Is uw netwerk beschermd tegen de risico's van internet?

Meestal is uw netwerk permanent met het internet verbonden. Internet is publiek toegankelijk, dit brengt bedreigingen met zich mee waartegen uw netwerk beschermd moet worden.

7. malware beveiliging

Is er bescherming tegen malware (virussen, spyware, etc)?

Zonder bescherming tegen malware loopt u een groter risico op verlies of beschadiging van gegevens. Tevens loopt u het risico dat externe onbevoegden zich toegang kunnen verschaffen tot uw data.

8. fysieke locatie servers

Zijn uw server(s) tegen diefstal beveiligd?

Voorals er iets met de server(s) gebeurt, zijn de problemen groot. Goede back-ups verminderen de schade, maar denk er ook aan dat uw data in de verkeerde handen kan komen.

Is de koeling van de server(s) goed geregeld?

Voorals in de zomer kan de temperatuur in een serverruimte zonder goede koeling flink oplopen. De kans op hardware defecten neemt hierdoor toe.

9. calamiteitenplan

Heeft u een calamiteiten plan?

Calamiteiten (brand, diefstal, hardware defecten e.d.) komen gelukkig niet vaak voor, maar als het gebeurt, kan met een goed plan veel ellende voorkomen worden.

10. structurele oplossingen

Zijn er problemen die regelmatig terugkeren?

Maar al te vaak worden problemen geaccepteerd of worden de symptomen bestreden. Op de lange termijn gaat dit ten koste van de continuïteit van uw automatisering.

Geef de gebruikers uitleg over de beveiliging en het gebruik van wachtwoorden om ze bewust te maken van de risico's.

Voer een wachtwoordbeleid in waarbij zwakke (bv. Pietje40) wachtwoorden niet zijn toegestaan. En zorg dat wachtwoorden (ook van de beheerder) periodiek veranderd worden.

Zorg dat u een goed beheerde firewall heeft en laat periodiek een security-check uitvoeren op uw externe verbinding.

Zorg voor een periodieke controle en een overzicht van de antivirus / anti-malware software. Vernieuw tijdig het update abonnement van deze software.

Zorg voor een adequate fysieke beveiliging van de server(s), een ruimte die alleen toegankelijk is voor bevoegden.

Regel voldoende koeling. Dit moet minimaal goede ventilatie van de serverruimte zijn, maar bij voorkeur een airconditioner die de temperatuur constant houdt.

Zorg dat het netwerk goed gedocumenteerd is, inclusief de beheerders wachtwoorden. Beschrijf wat er dient te gebeuren bij een calamiteit. Zorg er tevens voor dat bekend is hoe dit gedaan moet worden als uw beheerder niet beschikbaar is.

Achterhaal altijd de oorzaak en implementeer structurele oplossingen.

