BESCHERM UW DATA

Peter van der Linden
Directeur

“12 onbekende feiten die elke directeur moet weten over Data Backup, Security en Disaster Recovery.”

Ontdek wat veel ICT’ers Niet Weten of Niet Vertellen over het Back-uppen van uw Data en Herstellen ervan na een Ramp.

TROTS IT

“12 Onbekende Feiten En Insidersgeheimen Die Elke Ondernemer Moet Weten Over Het Maken Van Back-ups Van Hun Gegevens En Het Kiezen Van Een Externe Back-upservice”

Als uw data belangrijk is voor uw bedrijf en u het zich niet kunt veroorloven dat uw activiteiten dagen - of zelfs weken - stilliggen vanwege gegevensverlies of -beschadiging, moet u dit rapport lezen en handelen naar de gedeelde informatie. Dit rapport geeft een overzicht van de meest gemaakte, kostbare fouten die de meeste MKB-eigenaren maken met hun data back-up.

U Zal Het Volgende Ontdekken:

- Wat externe of managed back-ups zijn en waarom ELK bedrijf ze zou moeten hebben.
- 7 essentiële kenmerken die u absoluut van elke externe back-up leverancier moet eisen; vertrouw uw gegevens NIET toe aan iemand die niet aan deze criteria voldoet.
- Waar tape back-ups falen en u een vals gevoel van veiligheid geven.
- Beangstigende trends, casussen en vragen die elke bedrijfseigenaar zou moeten kennen en overwegen met betrekking tot gegevensbeveiliging.
- Het allerbelangrijkste waar u naar moet kijken bij een externe back-upservice leverancier.

TROTS IT

Van:
Peter van der Linden
Directeur Trots IT

Beste Collega-ondernemer,

Bent u ooit een uur werk aan uw computer kwijtgeraakt?

Stelt u zich dan eens voor dat u dagen of weken werk kwijtraakt - of dat u uw klantendatabase, financiële gegevens en alle werkbestanden verliest die uw bedrijf ooit heeft geproduceerd of samengesteld.

Stel u voor wat er zou gebeuren als uw netwerk dagenlang uitvalt en u geen toegang heeft tot e-mail of de informatie op uw pc. Hoe rampzalig zou dat zijn?

Of wat als een grote storm, overstroming of brand uw kantoor en al uw dossiers verwoest? Of als ransomware uw data gijzelt ... kunt u dan terugvallen op een noodherstelplan?

Hoe snel denkt u dat u zou kunnen herstellen, áls dat al kan?

Als u geen goede antwoorden hebt op bovenstaande vragen of geen ijzersterk herstelplan voor rampen heeft, speelt u letterlijk Russische roulette met uw bedrijf. Aangezien het aantal bedreigingen voortdurend toeneemt, is het niet de vraag *of* u een probleem krijgt, maar *wanneer*.

Maar Dat Kan Mij Nooit Overkomen!

(En Andere Leugens Die Ondernemers Zichzelf Graag Voorhouden Over Hun Bedrijf ...)

Na met meer dan 90 MKB'ers in de Randstad te hebben samengewerkt, zagen we dat 6 van de 10 bedrijven aanzienlijk risico lopen op een grote netwerk- of technologieramp die hen uiteindelijk tussen de € 9.000 en € 60.000 zal kosten aan reparatie- en herstelkosten.

Hier bovenop komt nog de schade doordat uw bedrijf niet kan opereren of beloften niet kan nakomen. Denk hierbij aan verloren productiviteit, omzetverlies en reputatieschade.

Hoewel het misschien moeilijk is om de daadwerkelijke financiële impact te bepalen die gegevensverlies op uw bedrijf zou hebben, kunt u niet ontkennen dat dit een groot negatief effect zou hebben.

” Maar Ik Maak Al Een Back-up Van Mijn Gegevens”, Zegt U…

Net als de meeste bedrijfseigenaren bent u slim genoeg geweest om een back-up op tape in te richten. Maar weet dit:

Het gemiddelde uitvalpercentage voor een tape back-up is 100% - ALLE tape back-ups falen op een bepaald moment.

Ongelofelijk, nietwaar? De meeste mensen realiseren zich niet dat ALLE tapes defect raken. Maar wat echt verontrustend is, is dat de meeste bedrijven het zich pas realiseren als het te laat is.

Hierdoor kunnen geschiedenisboeken volgeschreven worden met verhalen over bedrijven die voor miljoenen aan gegevens verloren. In bijna alle gevallen hadden deze bedrijven wel een back-upsysteem ingericht, maar ontdekten ze dat het niet functioneerde op het moment dat ze het het hardst nodig hadden.

U moet een back-up van uw gegevens bewaren, maar een back-up op tape biedt u GEEN bescherming als ...

- Uw tapedrive niet meer goed werkt, waardoor deze onbetrouwbaar is en het onmogelijk wordt om uw data terug te lezen. BELANGRIJK: Het is niet uitzonderlijk dat een tapedrive defect raakt zonder waarschuwingssignalen te geven.
- Uw bedrijfspand (met alles erin) wordt verwoest door een brand, overstroming, of andere natuurramp.
- De fysieke tapes waarop u een back-up van uw gegevens maakt, beschadigd raken door hitte of verkeerd gebruik.
- Een virus de gegevens beschadigt terwijl ze op tape worden opgeslagen. Sommige van de agressievere virussen beschadigen niet alleen de bestanden, maar zorgen ook dat niemand meer toegang heeft tot de gegevens op de tapes.
- Iemand in uw kantoor de tape per ongeluk formatteert en zodoende alles erop wist, of een ontevreden werknemer alles opzettelijk wist.
- Bij een inbraak al uw apparatuur gestolen wordt.
- Een defect sprinklersysteem al uw elektronische apparatuur 'besprenkelt'.

Kort gezegd: u wilt er NIET achter komen dat uw back-up niet werkt wanneer u deze het hardst nodig heeft.

TROTS IT

Beangstigende Trends, Casussen en Vragen Die U In Overweging Moet Nemen:

- Tapedrives vallen gemiddeld in 100% van de gevallen uit; dat betekent dat ALLE tapedrives op enig moment defect raken en GEEN volledige bescherming aan uw gegevens bieden als een natuurramp, brand of terroristische aanslag uw kantoor en alles wat erin staat vernielt. Bedrijfseigenaren die werden getroffen door orkanen zoals Katrina leerden een harde les over het op afstand bewaren van back-ups.
- 93% van de bedrijven die hun data 10 dagen of langer moesten missen, vroegen binnen een jaar na de ramp faillissement aan en 50% vroeg onmiddellijk faillissement aan. *(Bron: National Archives & Records Administration in Washington.)*
- 20% van de MKB'ers krijgt eens in de 5 jaar te maken met een ramp waarbij cruciale gegevens verloren gaan. *(Bron: Richmond House Group)*
- Alleen al dit jaar verkreeg een hacker bij 40% van de MKB'ers, die hun eigen netwerk beheren en internet gebruiken voor meer dan alleen e-mail, toegang tot hun netwerk en meer dan 50% van hen weet niet eens dat ze zijn aangevallen. *(Bron: Gartner Group)*
- Ongeveer 70% van de mensen heeft ervaring met dataverlies (of zal dit nog gaan ervaren) door onbedoeld wissen van bestanden, defecte hardware, virussen, brand of een andere ramp *(bron: Carbonite, an online backup service)*
- De eerste reactie van werknemers die hun bestanden verliezen, is proberen de schade te beperken door willekeurig herstelsoftware te gebruiken of door hun computer opnieuw op te starten of de stekker uit het stopcontact te trekken - stappen die gegevensherstel onmogelijk kunnen maken. *(Bron: wereldwijd onderzoek uit 2005 door Ontrack Data Recovery uit Minneapolis)*

Online Back-ups: Wat Ze Zijn En Waarom ELK Bedrijf Erover Zou Moeten Beschikken

De ENIGE manier om uw data goed te beschermen en te kunnen garanderen dat u alles kunt herstellen na een ramp, is door continue een up-to-date kopie van uw gegevens te bewaren op een externe, zwaarbeveiligde locatie.

Externe back-ups, ook wel offsite back-ups, **online** back-ups of managed back-ups genoemd, is een service die een kopie van uw gegevens veilig op een andere locatie dan uw kantoor bewaart.

Meestal worden deze back-ups automatisch na kantoortijd via internet naar een zwaarbeveiligde faciliteit gemaakt. Het staat buiten kijf dat elk bedrijf een externe kopie van zijn gegevens moet hebben; er ZIJN echter grote verschillen tussen de diverse externe back-upservices en het is van cruciaal belang dat u een goede provider kiest. Anders zou u veel geld betalen om vervolgens te ontdekken dat het herstellen van uw gegevens - precies de reden waarom u externe back-ups opzette - geen makkelijke, snelle of simpele klus is.

7 Belangrijke Eisen
Waarover Uw Online Back-upservice Moet Beschikken

Het grootste gevaar dat ondernemers lopen met online back-upservices is gebrek aan kennis en niet weten waar ze op moeten letten.

Er zijn letterlijk honderden bedrijven die deze service leveren omdat ze het zien als een manier om makkelijk geld te verdienen. Maar niet alle leveranciers zijn hetzelfde en u wilt er absoluut zeker van zijn dat u een goede, betrouwbare partner kiest. Anders kunt u verrast worden door verborgen kosten en onverwachte beperkingen. Of komt u tot de vreselijke ontdekking dat uw data toch niet goed werd bewaard en u aan uw lot wordt overgelaten, wanneer u de back-up nodig heeft.

Als uw online back-up leverancier niet aan onderstaande 7 eisen voldoet, zou u gek zijn als u ze vertrouwt met uw gegevens:

1) **Militair niveau qua beveiliging, gegevensoverdracht en gegevensopslag**. Dit is vrij vanzelfsprekend; u wilt er zeker van zijn dat het bedrijf dat uw gegevens bewaart, ook daadwerkelijk veilig is. We hebben het tenslotte over uw financiële informatie, klantgegevens en andere gevoelige informatie over uw bedrijf. Vertrouw uw gegevens nooit toe aan iemand die niet over de volgende beveiligingsmaatregelen beschikt:

    a) Vraag uw leverancier of ze AVG, SOC2, ISO27001 en SSAE16 gecertificeerd zijn. Dit zijn overheidsvoorschriften die bepalen hoe organisaties met zeer gevoelige gegevens (zoals banken en artsenpraktijken) hun gegevens verwerken, opslaan en overdragen. Als u een medische of financiële instelling bent, bent u mogelijk wettelijk verplicht om alleen te werken met aanbieders die aan deze strenge eisen voldoen. Maar zelfs als u GEEN organisatie bent die onder een van deze voorschriften valt, wilt u toch een aanbieder kiezen die dat wel is, omdat het een goed teken is dat ze hoogwaardige beveiligingsmaatregelen hebben getroffen.

    b) Zorg ervoor dat de fysieke locatie waar de gegevens zijn opgeslagen, veilig is. Vraag uw leverancier naar hun ID-systeem, videobewaking en toegangscontrolesysteem. Kan alleen geautoriseerd personeel de locatie betreden?

    c) Wees er zeker van dat gegevensoverdracht is gecodeerd met SSL-protocollen om te voorkomen dat een hacker toegang krijgt tot de gegevens terwijl deze worden overgedragen.

2) **Meerdere datacenters, geografisch verspreid**. Iedereen die bekend is met gegevensbeveiliging, weet dat het inbouwen van redundantie de beste manier is om dataverlies te voorkomen. Het betekent dat uw gegevens op meer dan één locatie moet worden opgeslagen. Op die manier is er een back-up van uw back-up voor het geval een natuurramp of iets anders desastreus een van hun locaties vernietigt.

3) **Eis de mogelijkheid om de back-up van uw gegevens op externe harddisk of een andere gegevensdrager opgestuurd te krijgen**. Als uw hele netwerk is vernietigd, wilt u NIET dat downloaden via internet de enige optie is om de gegevens te herstellen. Dit kan namelijk dagen tot weken duren. Werk daarom alleen met leveranciers die uw gegevens via een koeriersdienst op een fysiek opslagapparaat aanleveren.

4) **Vraag om dezelfde reden aan uw leverancier of het mogelijk is om uw *initiële* back-up aan te leveren op een fysiek apparaat**. Nogmaals, het kan dagen tot weken duren om grote hoeveelheden data via internet over te brengen. Als u veel gegevens moet back-uppen, is het sneller en handiger om dit op een externe harddisk te verzenden.

5) **Zorg ervoor dat uw gegevens kunnen worden hersteld naar een andere computer dan de computer waarvan een back-up is gemaakt**. Verbazingwekkend genoeg kunnen sommige back-ups alleen worden hersteld op dezelfde computer als waar ze vandaan kwamen. Als de originele computer door brand is verwoest, of gestolen of onherstelbaar kapot is, heeft u nog geen back-up.

6) **Vraag dagelijkse statusrapporten van uw back-up**. Alle leveranciers zouden u dagelijks een e-mail moeten sturen om te laten zien dat back-up daadwerkelijk is uitgevoerd EN om storingen of problemen te melden. De professionelere aanbieders staan toe dat u naast uzelf meer dan één persoon (zoals een technicus of uw ICT-persoon) op de hoogte gesteld wilt hebben.

7) **Eis ondersteuning door een gekwalificeerde technicus**. Veel online back-upservices zijn 'zelfservice'. Hierdoor kunnen ze goedkoop aanbieden. MAAR als u uw back-up niet correct inricht, zal uw besparing in het niet vallen bij de verliezen die u lijdt. Vraag uw leverancier op zijn minst om u telefonisch te helpen om er zeker van te zijn dat u de installatie correct hebt uitgevoerd.

Het Allerbelangrijkste Waar U Op Moet Letten Bij Het Kiezen Van Een Online Back-up leverancier

Hoewel de bovenstaande punten belangrijk zijn, is een van de meest essentiële kenmerken - en een die vaak over het hoofd wordt gezien - het vinden van een leverancier die regelmatig herstel-tests uitvoert om uw back-up te controleren en ervoor te zorgen dat de gegevens kunnen worden hersteld.

U wilt met het testen van uw back-up niet wachten tot uw gegevens zijn gewist. Toch is dat precies wat de meeste mensen doen - en die moeten daar een hoge prijs voor betalen.

Als uw gegevens erg belangrijk zijn en u het zich niet kunt veroorloven om ze kwijt te raken, moet u ten minste maandelijks een herstel-test uitvoeren. Is het in uw situatie iets minder cruciaal, dan zijn driemaandelijkse herstel-tests voldoende.

Tal van oorzaken kunnen ervoor zorgen dat uw back-up beschadigd raakt. Door te testen, slaapt u een stuk beter, wetende dat u over een goede, solide kopie van uw gegevens beschikt en voorbereid bent op een onvoorziene ramp of noodsituatie.

Wilt U Zeker Weten Of Uw back-up Uw Gegevens Echt Veilig Houdt?

Onze Gratis Gegevensbeveiligingsanalyse Zal Het Laten Zien...

Als potentiële nieuwe klant wil ik u graag een 'leer ons kennen' -aanbod doen in de vorm van een gratis gegevensbeveiligingsanalyse. Normaal geef ik geen gratis diensten weg bij Trots IT, want als ik dat zou doen, zou ik failliet gaan. Maar aangezien uw bedrijf voldoet aan onze strenge selectiecriteria, leek mij dit een geweldige manier om onze diensten aan een paar nieuwe klanten voor te stellen.

Allereerst wil ik een 10 minuten durende telefonische analyse voorstellen, waarin wij uw unieke situatie en eventuele zorgen bespreken en natuurlijk al uw vragen over ons beantwoorden. Als u dat wilt, plannen we vervolgens een geschikt moment om onze unieke GRATIS 27-Punten IT-systeembeoordeling uit te voeren. Normaal vraag ik € 297 voor deze service, maar als potentiële klant wil ik deze gratis aan u geven om ons 'Managed IT Services'-programma met databack-up en -herstelservice aan uw bedrijf voor te stellen.

Tijdens deze analyse controleer ik op afstand uw systeem en...

- Check uw huidige back-upsysteem, inclusief de back-up- en herstelprocedures, taperotatie- en onderhoudsschema's, om te zien of er iets is dat de veiligheid van uw gegevens in gevaar brengt.

- Beoordeel procedures voor opslag en transport van gegevensdragers. Veel mensen realiseren zich niet dat de dragers door onjuiste zorg kunnen beschadigen (en daardoor hun gegevens verliezen).

- Controleer uw back-up om er zeker van te zijn dat een nauwkeurige back-up gemaakt wordt van alle bestanden en informatie die u NOOIT kwijt wilt raken.

- Presenteer een eenvoudig en makkelijk te begrijpen diagram waarin de samenstelling van uw gegevens gedetailleerd wordt weergegeven, inclusief de leeftijd en het type bestanden waarvan u een back-up maakt. Waarom zou u dat interesseren? Omdat veel bedrijven onbewust waardevolle back-upcapaciteit gebruiken voor de persoonlijke mp3-bestanden en video's van hun werknemers.

- Leg in gewoon Nederlands uit waar uw risico's liggen. We weten dat iedereen een ander niveau van risicotolerantie heeft en we willen ervoor zorgen dat het risico wat u met uw gegevens neemt een bewuste keuze is en niet als gevolg van miscommunicatie, willekeur of gebrek aan kennis.

Afhankelijk van wat we ontdekken, geven we u een verklaring dat alles in orde is of tonen u potentieel rampzalige gebreken in uw back-up strategie. Indien u dit wenst, zullen we u

voorzien van een actieplan om uw gegevens goed te beveiligen met onze Disaster Recovery dienst.

Natuurlijk zal niet iedereen klant worden, maar ik weet dat een sommigen van u ons inhuren om het meest waardevolle bezit – uw bedrijfsgegevens - te beschermen en loyale klanten te worden net zoals Verhaar Omega en Lubbe Lisse.

Maar Ik Heb Geen Gratis Beveiligingsanalyse Nodig Want Mijn ICT-er Heeft Het Onder Controle…

Misschien heeft u niet het gevoel dat u een urgent probleem heeft wat onmiddellijk moet worden opgelost. Misschien denkt u dat uw gegevens volkomen veilig zijn. Veel van wat nu onze klanten zijn, dachten dat hun gegevens veilig waren totdat het nodig was om DATA TE HERSTELLEN.

Helaas is dat het moment waarop de meeste bedrijven hun oplossing voor back-up en -herstel “testen”. Wij helpen bedrijven zoals het uwe om pijnlijke en extreem dure datacatastrofes te VOORKOMEN.

Hier een voorbeeld:

> Een werknemer in een belangrijke commerciële functie bij onze klant zegde zijn baan op. Na enige tijd bleek dat deze persoon voor zijn vertrek ‘netjes’ zijn mailbox en bestanden had opgeruimd. Gewoon verwijderd dus. Maar goed, dat onze back-up **elk uur alles veiligstelt** en minstens 1 jaar bewaart.

hier is er nog een…

> Een mailtje van een onbekend iemand met een pdf-bestand erin. Uit nieuwsgierigheid werd er toch op geklikt en vervolgens waren alle bestanden onleesbaar gemaakt, gevolgd door het vriendelijke verzoek om wat Bitcoins ‘losgeld’ over te maken. Het overkwam onze klant. Een vervelend maar o zo veel voorkomend geval van ransomware. Gelukkig **binnen een uur** te herstellen met onze back-up.

en nog een…

> Donderdagochtend even voor half 4 begonnen werknemers van onze klant te klagen dat ze vanaf de server geen bestanden meer konden openen. Het blijkt dat het mainboard van de server defect is. Er kwam rook uit de kast. Snel de back-up van een half uur eerder opgestart als Business Continuity maatregel en **binnen 10 minuten kon iedereen weer werken**. Doordat om 3 uur nog een back-up gemaakt was, was dataverlies nihil. Met een back-up van de vorige avond had het werk van de hele dag opnieuw moeten worden gedaan en had men hier pas op maandag mee kunnen beginnen, toen een monteur de server was komen herstellen.

Waarom Zou U Uw Externe Back-ups Aan Ons Toevertrouwen?

Er zijn veel bedrijven die online back-upservices aanbieden, dus wat maakt ons zo speciaal? Waarom voor ons kiezen in plaats van de tientallen andere bedrijven die ogenschijnlijk dezelfde diensten aanbieden? Ik ben blij dat u het vraagt, want er zijn 6 BELANGRIJKE redenen om uw databeveiliging aan ons toe te vertrouwen:

1. Onze geavanceerde datacentra voldoen aan de strengste veiligheidseisen waaronder SOC1, SAE16 en SOC2, en zijn TIER 3 ingericht met een minimaal gegarandeerde beschikbaarheid van 99.982%. Uw data wordt standaard op 2 verschillende locaties bewaard. Dit betekent dat uw gegevens goed beveiligd zijn en beschermd tegen de ergste natuurrampen - brand, overstroming en diefstal.

2. Wij garanderen onvoorwaardelijk de veiligheid en beschikbaarheid van uw gegevens. Als u data aan ons toevertrouwt, garanderen we dat deze 24/7 voor u beschikbaar zijn en anders geven we u uw geld terug!

   De meeste online back-up leveranciers promoten met geld-terug-garanties, maar als u de kleine lettertjes leest, gelden er tal van beperkingen. Wij doen niet moeilijk en bieden u een volledig jaar abonnementsgeld terug als we uw data niet beschikbaar kunnen stellen. Gelukkig kunnen wij u melden, dat een dergelijke situatie nog nooit bij onze klanten is voorgekomen.

3. We bieden gratis helpdeskondersteuning voor het herstellen van bestanden. Sommige leveranciers brengen extra kosten in rekening voor deze service of bieden deze helemaal niet aan.

4. We bieden gratis Disaster Recovery-service aan om uw gegevens te herstellen als ALLES tegelijk verloren is gegaan. Nogmaals, de meeste bedrijven rekenen hier extra voor of ze bieden het helemaal niet aan. Zonder extra kosten werken we rechtstreeks samen met uw ICT-manager of ICT-engineer om al uw gegevens te herstellen in het noodlottige geval van een catastrofaal incident.

5. Wij zijn een lokaal bedrijf met een echt kantoor. Dat lijkt misschien raar om te vermelden, maar wat u zich vast niet realiseert, is dat sommige online back-up leveranciers bestaan uit een paar jongens die vanuit hun slaapkamer werken zonder dat u ze, afgezien van per e-mail, daadwerkelijk kunt bereiken.

   Wij komen ter plaatse, schudden uw hand en bieden u een kop koffie aan als u bij ons langskomt. Zou u niet liever zakendoen met een lokaal bedrijf dat u persoonlijk kunt bezoeken in plaats van een onbekende onderneming in een andere regio - of een ander land?

6. We zullen dagelijks herstel-tests van uw servers uitvoeren om aan te tonen dat uw back-up werkt. Er is geen andere manier om het zeker te weten en de MEESTE online back-up leveranciers bieden deze service NIET aan.

U Hoeft Ons Niet Op Ons Woord Te Geloven.
Lees Hier Wat Onze Klanten Over Ons Zeggen…

…Afspraken nakomen was doorslaggevend…

Afspraken nakomen bleek niet voor elke IT-partner vanzelfsprekend, zo was onze ervaring. Bij Trots IT is het dat gelukkig wel. Voor ons de voornaamste reden, om voor onze automatisering naar hen over te stappen. Het grootste voordeel van Trots IT is, dat zij zich **ontfermen over alle automatisering** binnen ons bedrijf. In de praktijk draait het hart van Bouwbedrijf van Breda dus bij Trots IT. En dat is een geruststellend gedachte, want **onze ervaringen met deze IT-partner zijn gewoon goed**. Ik zou elke ondernemer dan ook aanraden Trots IT ook als IT-partner te kiezen.

Jeroen van Breda, Directeur, A.G.J.C. van Breda BV

…Altijd een bevredigend antwoord…

Toen onze vorige IT-relatie ophield te bestaan, moesten wij op zoek naar een nieuwe dienstverlener die ervaring had met onze sector en bijbehorende netwerk. Tijdens die zoektocht kwamen wij uit bij Trots IT. Het grote voordeel van samenwerken met Trots IT voor onze telefonie, infrastructuur en computers is de **uitgebreide kennis** van zaken die zij bezitten. Wij kunnen altijd met onze vragen en problemen op dat gebied bij ze terecht en krijgen **steevast een bevredigend en oplossingsgericht antwoord**. Dat is heel prettig! Met onze positieve ervaring zou ik Trots IT als IT-partner zeker aanraden aan andere bedrijven.

Marcel Helmus, Directeur, A. Helmus BV

…Nu wordt ons systeem altijd in de gaten gehouden…

In het verleden deden wij onze automatisering altijd zelf. Maar het gezegde is niet voor niets ‘schoenmaker, blijf bij je leest’. Dus besloten wij dit bij Trots IT neer te leggen. En inmiddels kunnen wij zeggen, dat wij heel blij zijn met het maatwerk dat ze leveren en het **persoonlijke contact** dat zij bieden. Met Trots IT is er altijd iemand, die ons systeem up-to-date houdt. Zij zijn een **zeer kundige en eerlijke IT-partner**. Een aanrader voor elke ondernemer, die een **betrokken IT-partner** zoekt.

Michael Lubbe, Directeur, Lubbe Lisse

...Ze doen hun werk serieus goed...

Het grootste voordeel dat de samenwerking met Trots IT ons bracht is toch wel de **goede service** die zij verlenen. Ze **staan dichtbij je bedrijf** en bieden een snelle respons. Juist met **dat persoonlijke en die betrokkenheid** steekt Trots IT met kop en schouders uit boven de vorige IT-dienstverleners. Ze gaan serieus met jou als klant en je vraagstukken om en doen hun werk gewoon echt goed. Ik gun elke ondernemer zo'n IT-partner als Trots IT!

Niels Mulder, Eigenaar, Unex Inc

...Eén nummer om te bellen...

Voordat we met Trots IT werkten, was onze ervaring met IT-bedrijven niet heel goed; ze werkten op een reactieve manier. Bij Trots IT onderhouden ze onze IT middelen en **werken ze proactief.** Hun **deskundig personeel** monitort en waakt voortdurend over onze IT-omgeving om te voorkomen dat verstoringen escaleren. En als er een probleem optreedt, lossen ze het snel op. Wat een opluchting en groot gemak om één partij te hebben om te bellen als er een probleem is - één partij die niet anderen de schuld geeft als er iets misgaat! **We vertrouwen Trots IT volledig** als IT partner, ook wanneer het andere technologie gerelateerde services of oplossingen betreft. We zijn blij dat Trots IT waakt over ons bedrijf. Als u Trots IT niet belt om uw IT te bespreken, zult u er spijt van krijgen!

Victor van der Blom, Partner, ODIN-RVB bv

...Als het moet, staan ze in no-time op de stoep...

Ik moet er niet aan denken, dat ons bedrijf stilstaat door problemen met het computersystemen. Dat kunnen wij ons gewoonweg niet permitteren! Gelukkig beheert Trots IT ons complete systeem en wordt dit door hen **continue goed en streng bewaakt**. Ik word er echt niet vrolijk van, als mijn computer niet naar behoren functioneert. Maar ik weet dat Trots IT, als het nodig is in no-time op de stoep staat of van afstand inlogt, om het probleem **adequaat** op te lossen. Die persoonlijke aandacht is voor ons bedrijf erg belangrijk en echt **een hele zorg minder**. Bovendien gaat Trots IT met de tijd en de nieuwste IT-ontwikkelingen mee. Dat is ook wel iets, wat ik bij het vorige IT-bedrijf miste: dat **innovatieve vooruit- en meedenken**. Met Trots IT in zee gaan was voor ons dus een goede keuze. En dat zou het voor elke ondernemer zijn!

Mark Verhaar, Directeur, Verhaar Omega BV

U Bent Niet Verplicht Om Iets Te Doen Of Te Kopen Wanneer U “Ja” Zegt Tegen Een Gratis 27-Punten Gegevensbeveiligingsanalyse

We willen duidelijk zijn dat er van onze kant geen verwachting is, dat u iets doet of koopt wanneer u van ons aanbod gebruikmaakt.

Ik geef u zelfs mijn persoonlijke garantie dat u niet te maken krijgt met een opdringerige, arrogante verkoper, want ik waardeer zware verkoopdruk net zomin als u.

Ik kan dit aanbod echter niet voor altijd verlengen, omdat tijds- en personeelsbeperkingen het eenvoudigweg niet toestaan. Om uw gratis gegevensbeveiligingsanalyse voor uw bedrijf veilig te stellen, moet u snel reageren. De plekken ZIJN beperkt, dus kom vandaag nog in actie. Als u niet op tijd kunt reageren, zal ik dit aanbod helaas moeten intrekken en beschikbaar stellen voor iemand anders.

Bel mij direct op 088-2055888 om uw gratis analyse in te plannen.

Vriendelijke groet,

Peter van der Linden
Directeur Trots IT
peter@trotsit.nl
088-2055888

P.S. Mis het niet!!! Uw gratis 27-punten gegevensbeveiligingsanalyse (ter waarde van € 297) laat u zien of uw back-up echt alle gegevens die u niet kunt missen, kopieert en opslaat in een formaat dat kan worden hersteld. Onthoud dat u snel moet reageren om deze service te bemachtigen.

P.P.S. Om te reageren belt u mij direct op 088-2055888.