

TA 2300-0006

Technische Richtlijn



Beveiligingsinstructies voor de internet - koppeling van Jenbacher-installaties



© INNIO Jenbacher GmbH & Co OG
Achenseestr. 1-3
A-6200 Jenbach, Austria
www.innio.com

1	Algemeen	1
2	Veiligheidsrisico's / gevaren.....	1
3	Oplossing middels de Jenbacher Firewall	2
4	Waarschuwing.....	2
5	Revisienummer	3

Dit document is bestemd voor:

klant, verkooppartners, servicepartners, IB-partners, (dochter-)filialen, locatie Jenbach

Copyrightverklaring van INNIO: VERTROUWELIJK

De informatie in dit document is beschermde informatie van INNIO Jenbacher GmbH & Co OG en zijn dochterondernemingen en is vertrouwelijk. De informatie is eigendom van INNIO en mag zonder voorafgaande schriftelijke toestemming niet gebruikt, aan derden doorgegeven of vermenigvuldigd worden. Hieronder valt ook, maar niet uitsluitend, het gebruik van de informatie voor de productie, fabricage, ontwikkeling of afleiding van reparaties, modificaties, reserveonderdelen, constructies of configuratiewijzigingen dan wel het indienen van aanvragen hiervoor bij overheidsinstanties. Als de volledige of gedeeltelijke vermenigvuldiging is toegestaan, dienen deze verklaring en de verdere verklaringen op alle pagina's van dit document helemaal of gedeeltelijk te worden vermeld.

AFGEDRUKTE OF ELEKTRONISCH VERSTUURDE KOPIEËN ZIJN ONGECONTROLEERD

1 Algemeen

Het INNIO Jenbacher GmbH & Co OG besturingssysteem DIA.NE® maakt met behulp van een netwerkkoppeling een koppeling met de klant mogelijk. Middels deze koppeling is het mogelijk met behulp van een webbrowser toegang te krijgen tot de DIA.NE® WIN-visualiseringsapplicatie en op deze wijze de installatie te bedienen.

Deze netwerkkoppeling is door INNIO Jenbacher GmbH & Co OG UITSLUITEND ontworpen ter aansluiting op een lokaal netwerk (LAN van de klant).

Gezien de huidige stand van de techniek en de het grote aantal internetaansluitingen zijn dergelijke netwerkkoppelingen in principe tevens geschikt voor toegang via internet. Een dergelijke toegang wordt door klanten meestal met behulp van router en port forwarding opgelost.

In deze Technische Instructie worden de gevaren van een dergelijke oplossing toegelicht en wordt een uit beveiligingsoogpunt zinvolle oplossing van een internetkoppeling van INNIO Jenbacher GmbH & Co OG-installaties geïllustreerd.

2 Veiligheidsrisico's / gevaren

Een oplossing via internet-router en port forwarding kent **grote beveiligingsrisico's!**

Daarbij valt o.a. te denken aan:

- Ongecodeerde transmissie van de gegevens via internet
 - het achterhalen van als leesbare tekst verzonden wachtwoorden door HACKERS!
 - de mogelijkheid van een 'man-in-the-middle'-aanval (het online wijzigen van de verzonden gegevens door HACKERS, zoals bijv. de instelling van gewenste waarden, parameters, ...).
- Indien de router in principe weliswaar correct is geconfigureerd (beperkt tot bepaalde poorten): mogelijk directe toegang tot de op de DIA.NE WIN-server geïnstalleerde Web-server
 - geen bescherming tegen webservergericht virus-, worm-, denial-of-service (DoS)- en exploit-aanvallen (bijv. Code Red)!

Beveiligingsinstructies voor de internet - koppeling van Jenbacher-installaties

- geringe bescherming tegen 'password cracking'-aanvallen door HACKERS (achterhalen van passwords)!
- Indien de router niet correct is geconfigureerd en/of de beveiligingsupdates niet of niet tijdig zijn uitgevoerd: directe toegang tot het besturingssysteem van de server
 - geen bescherming tegen aanvallen door virussen, wormen, trojan horses op het Windows-besturingssysteem (bijv. Blaster, Sasser, Spybot, Beagle, etc.)!
 - de passwordbeveiliging op alle niveau's kan door HACKERS worden uitgeschakeld!
- Geen toegangscontrole en – protokollering door het INNIO Jenbacher GmbH & Co OG Remote Access Portal
(2-layer authentication-procedure)

Dit kan resulteren in **directe bedreigingen voor de klant en de installatie**:

- toegang door derden op de installatie middels een achterhaald password of een 'man-in-the-middle'-aanval:
op deze wijze kunnen afhankelijk van het password-niveau, alle gewenste waarden, motorparameters, historische gegevens, worden gewijzigd of gewist.
- Overnemen van de controle van een server door derden:
 - uitschakelen van alle beveiligingsvoorzieningen van het bedieningssysteem en daardoor een onbeperkte toegang tot alle gewenste waarden, motorparameters en historische gegevens
 - gebruiken van de server voor andere criminele doeleinden (spam-mailer, DoS-aanvallen, etc.).
- Onherstelbaar beschadigen van de DIA.NE® WIN – server:
Het totaal uitvallen van de server door het wissen van alle gegevens op de harde schijf door toedoen van HACKERS of een virus.

Dit type manipulaties kan resulteren in de onherstelbare beschadiging van de installatie en/of het in gevaar brengen van mensenlevens!

3 Oplossing middels de Jenbacher Firewall

Om de bovenstaand genoemde beveiligingsproblemen volledig op te lossen, heeft INNIO Jenbacher GmbH & Co OG een oplossing ontwikkeld.

Deze oplossing bestaat uit een ter plaatste geïnstalleerde Firewall, die een uiterst beveiligde, gecodeerde verbinding met de centrale Firewall bij INNIO Jenbacher GmbH & Co OG mogelijk maakt (Virtual Private Network, VPN). Deze verbinding en de daarbij gebruikte componenten worden rechtstreeks door INNIO Jenbacher GmbH & Co OG gecontroleerd en onderhouden. Hierdoor is het mogelijk zeer snel te reageren bij systeemgerelateerde beveiligingsproblemen (security-updates) en bij activiteiten door hackers.

Door de Firewall en de VPN-verbinding is de directe toegang via Internet tot de installatie niet meer mogelijk en is de gecontroleerde toegang via het INNIO Jenbacher GmbH & Co OG Remote Access Portal gegarandeerd.

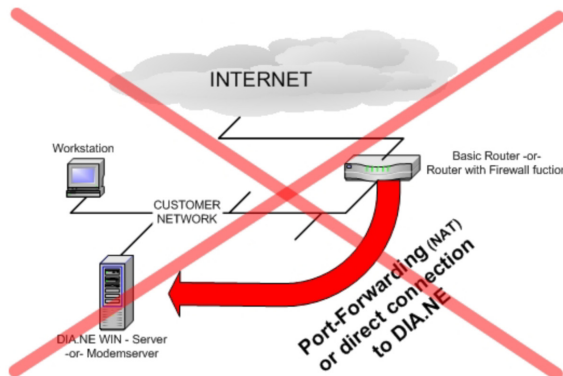
4 Waarschuwing

TEN STRENGSTE VERBODEN!

Onveilig

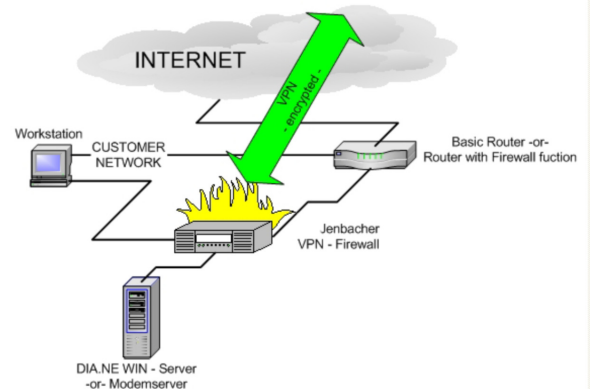
Veilig

Beveiligingsinstructies voor de internet - koppeling van Jenbacher-installaties



Router met Port Forwarding:

Rechtstreekse toegang tot DIA.NE® WIN met ongecodeerde login door DIA.NE®-password.



INNIO Jenbacher GmbH & Co OG Firewall-oplossing:

Toegang tot DIA.NE® WIN uitsluitend via INNIO Jenbacher GmbH & Co OG Remote Access Portal (1. gecodeerde authenticatie op het Portal, 2. gecodeerde login met DIA.NE®-password)

INNIO Jenbacher GmbH & Co OG is niet aansprakelijk voor defecten of schade ten gevolge van de toepassing van een router met Port Forwarding of een rechtstreekse verbinding met de DIA.NE® WIN-server. De garantieverplichting van INNIO Jenbacher GmbH & Co OG is niet van toepassing op dergelijke defecten of schade.

5 Revisienummer

Revisiehistorie

Index	Datum	Beschrijving / samenvatting wijzigingen	Deskundige Gecontroleerd door
2	30.04.2019	GE ersetzt durch INNIO / GE replaced by INNIO	Stojiljkovic T. Pichler R.
1	26.05.2010	Umstellung auf CMS / Change to Content Management System ersetzt / replaced Index: -	Schartner Pichler

