Starke Lösungen für Ihre IT-Sicherheit

genua

genua: Ihr Partner für hochwertige IT Security Made in Germany

Je mehr vernetzt wird, desto wichtiger wird die IT-Sicherheit: Ihre IT-Systeme und Kommunikationswege müssen jederzeit reibungslos funktionieren, gleichzeitig sind Ihre Daten zuverlässig zu schützen. Dabei möchten wir Sie unterstützen. genua ist ein deutscher Spezialist für IT-Sicherheit. Die Firmengründer sind seit 1992 in der Unternehmensführung der genua gmbh tätig – so können wir unsere Ideen verfolgen und konsequent unseren Weg gehen. Das Ziel ist klar definiert: hochwertige Lösungen entwickeln, um bei unseren Kunden für zuverlässige IT-Sicherheit zu sorgen.

Alle unsere Lösungen werden in Deutschland entwickelt, produziert und sind auf hohe Sicherheitsanforderungen ausgerichtet. Dass wir diese Ansprüche erfüllen, belegen zahlreiche Zertifikate sowie Zulassungen für den Geheimschutzbereich. Zu unseren Lösungen bieten wir hochwertigen Service: Von der Implementierung über die fortlaufende Betreuung bis hin zur Umsetzung von Sonderwünschen – diesen Service bekommen Sie direkt vom Hersteller genua. Auf unsere Lösungen und Dienstleistungen vertrauen viele Firmen und Behörden, um ihre IT zu schützen.

Die drei Firmengründer: Dr. Michaela Harlander, Dr. Magnus Harlander, Bernhard Schneck (v.l.n.r.)

Netzwerk-Sicherheit

In Ihrem Netzwerk arbeiten Sie mit vielen sensiblen Daten: über Kunden und Produkte, Patente und Forschungsergebnisse, Projekte und Strategien oder auch Patienten und Therapien. Diese Informationen müssen Sie vor unbefugten Zugriffen oder Verlust zuverlässig schützen. Dazu können Sie Ihr Netzwerk aber nicht völlig abkapseln. Denn gerade die Vernetzung ermöglicht den schnellen Datenaustausch und somit effiziente Abläufe, die entscheidende Vorteile bringen: schnelle Entwicklung, intelligente Produktion, komfortable Administration und auch rasche Informationsverarbeitung bei Führungs- oder Sicherheitsaufgaben.

Um diese Vorteile zu nutzen – ohne Ihre IT-Sicherheit zu riskieren – müssen Sie die Übergänge von öffentlichen Netzwerken zu Ihrem LAN (Local Area Network) zuverlässig absichern. Ein größeres LAN sollte zudem in unterschiedliche interne Netzbereiche z. B. für die Verwaltung, Produktion und Forschung unterteilt und die Schnittstellen dazwischen sorgfältig kontrolliert werden. Dazu bieten wir Ihnen hochwertige Lösungen Made in Germany.

High Resistance Firewall genugate
für höchste Sicherheit an kritischen Schnittstellen durch umfassende Datenanalyse

Firewall & VPN-Appliance genuscreen
für starken Schutz an externen und internen Schnittstellen und zuverlässig verschlüsselte Datentransfers

Datendiode cyber-diode
zur hochsicheren Vernetzung von KRITIS und Maschinenanlagen

Datendiode vs-diode
für performante Einbahn-Datentransfers in Netzwerke im Geheimschutzbereich

Absicherung KRITIS und hochsensibler Schnittstellen

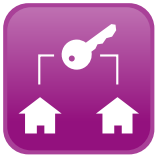
Bei einigen Netzwerk-Schnittstellen gelten besonders hohe Sicherheitsanforderungen: Z. B. wenn Sie bei Behörden oder Organisationen mit Sicherheitsaufgaben (BOS) Netze mit unterschiedlichen Geheimschutzstufen koppeln. Oder wenn Sie im Wirtschaftsbereich Systeme vernetzen, die kritische Infrastrukturen (KRITIS) oder andere Anlagen steuern, von deren fehlerfreier Funktion hohe Sachwerte oder gar Leben abhängen. Dazu gehören bspw. die Elektrizitätsversorgung, technische Einrichtungen auf Flughäfen und Bahnhöfen oder chemische Produktionsanlagen. An diesen sensiblen Schnittstellen muss ganz exakt kontrolliert werden, welche Verbindungen zugelassen werden – die Fehlertoleranz liegt hier bei null. Für diese anspruchsvollen Aufgaben bieten wir zuverlässige Lösungen Made in Germany, für den Einsatz bei BOS auch mit Zulassungen für den Geheimschutzbereich.

High Resistance Firewall genugate
für höchste Sicherheit an kritischen Schnittstellen durch umfassende Datenanalyse

Firewall & VPN-Appliance genuscreen
für starken Schutz an externen und internen Schnittstellen und zuverlässig verschlüsselte Datentransfers

Datendiode cyber-diode
zur hochsicheren Vernetzung von KRITIS und Maschinenanlagen

Datendiode vs-diode
für performante Einbahn-Datentransfers in Netzwerke im Geheimschutzbereich



Sichere Standortanbindung

Sie möchten neue Standorte, nach einem Merger weitere Unternehmensteile oder wichtige Partner an Ihr Netz für Datenkommunikation anbinden? Der schnelle Austausch von Informationen via Internet ist komfortabel – muss aber zuverlässig abgesichert werden. Denn auch andere interessieren sich für Ihre Daten: Konkurrenten, Geheimdienste oder Kriminelle. Wenn Ihr Wissen in deren Hände gerät, kann dies gravierende Folgen haben. Mit unseren Lösungen können Unternehmen sowie Behörden und Organisationen mit Sicherheitsaufgaben die Datenkommunikation zwischen verteilten Standorten und mit Partnern zuverlässig schützen, falls erforderlich mit Zulassung bis zur Geheimstufe VS-NfD. Unsere Lösungen werden in Deutschland entwickelt und produziert und erfüllen höchste Sicherheitsanforderungen – hier kann keiner mitlesen.

Firewall & VPN-Appliance genuscreen
für starken Schutz an externen und internen Schnittstellen und zuverlässig verschlüsselte Datentransfers

Personal Security Device genucard
zur Anbindung von Home Offices und kleinen Standorten im Geheimschutzbereich

VPN-Appliance genucrypt
für stark verschlüsselte Datentransfers

Sichere Anbindung an die Cloud

Cloud Services sind komfortabel, sparen Aufwand bei der IT-Administration und Ressourcen. Verständlich, dass viele diese Vorteile nutzen möchten – ein weiteres entscheidendes Kriterium bei der Auslagerung sensibler Daten in die Cloud ist aber das Sicherheitsniveau: Up- und Downloads sollten hier ausschließlich über hochwertig verschlüsselte Verbindungen erfolgen. Auch in der Cloud selbst sollten Daten besser nur verschlüsselt abgelegt werden, um die Vertraulichkeit zu garantieren. Diese wichtigen Maßnahmen zur sicheren Cloud-Nutzung können Sie mit unseren Lösungen, die in Deutschland entwickelt und produziert werden, zuverlässig umsetzen.

High Resistance Firewall genugate
für höchste Sicherheit an kritischen Schnittstellen durch umfassende Datenanalyse

Firewall & VPN-Appliance genuscreen
für starken Schutz an externen und internen Schnittstellen und zuverlässig verschlüsselte Datentransfers

VPN-Appliance genucrypt
für stark verschlüsselte Datentransfers

Sichere Anbindung mobiler Anwender und von Home Offices

Mitarbeiter auf Reisen oder im Home Office möchten via Internet auf Ihr Netzwerk zugreifen, um ihre Arbeit zu erledigen: Daten abrufen und bearbeiten, interne Anwendungen online nutzen u. v. m. Von jedem Ort aus über alle heute möglichen Verbindungswege soll dies ganz komfortabel möglich sein. Dies sind die Anforderungen der Anwender, aber eine wichtige Frage muss noch geklärt werden: Wie wird beim Remote-Zugriff für zuverlässige IT-Sicherheit gesorgt? Denn hier sollen sensible Daten via Internet ausgetauscht und – aus der Sicherheitsperspektive noch gravierender – ein Zugang in Ihr LAN mit vielen vertraulichen Informationen zugelassen werden.

Bei diesen Zugriffen muss unbedingt ausgeschlossen werden, dass Dritte die Datentransfers mitlesen, manipulieren oder gar den Zugang zu Ihrem LAN missbrauchen können. Wir bieten komfortable Lösungen Made in Germany für Unternehmen, Behörden und Organisationen mit Sicherheitsaufgaben, falls erforderlich mit Zulassung bis zur Geheimstufe VS-NfD.

Security Laptop cyber-top
für mobiles Arbeiten in getrennten Netzen

Security Laptop vs-top
zur Anbindung mobiler Mitarbeiter im Geheimschutzbereich

Personal Security Device genucard
zur Anbindung von Home Offices und kleinen Standorten im Geheimschutzbereich

Verschlüsselte Kommunikation via VPN

Das Internet ist nahezu überall verfügbar und die Nutzung kostengünstig – damit ist es für die Datenkommunikation gut geeignet. Hohe Sicherheit ist dagegen kein Merkmal öffentlicher Netze: Beim weltumspannenden Datenverkehr lesen viele mit, und auch von Dritten angebotene vermeintlich sichere Services können Schwachstellen oder gar verborgene Hintertüren aufweisen. Dieses Risiko sollten Sie bei der Kommunikation zwischen verteilten Standorten oder der Anbindung mobiler Mitarbeiter nicht eingehen.

Ihre sensible Datenkommunikation via Internet sollten Sie ausschließlich über hochwertig verschlüsselte Verbindungen eines Virtual Private Network (VPN) führen, das von vertrauenswürdigen Sicherheitssystemen erzeugt wird. Unsere VPN-Lösungen werden in Deutschland hergestellt und arbeiten mit den stärksten Verschlüsselungsalgorithmen. Viele unserer Lösungen durchlaufen zudem regelmäßig Zertifizierungen und Zulassungen beim Bundesamt für Sicherheit in der Informationstechnik (BSI), um die hohe Qualität von unabhängiger Seite zu belegen. Unsere Lösungen haben keine Schwachstellen oder Backdoors – da können Sie ganz sicher sein.

Security Laptop cyber-top
für mobiles Arbeiten in getrennten Netzen

Security Laptop vs-top
zur Anbindung mobiler Mitarbeiter
im Geheimschutzbereich

Personal Security Device genucard
zur Anbindung von Home Offices und kleinen
Standorten im Geheimschutzbereich

Firewall & VPN-Appliance genuscreen
für starken Schutz an externen und internen
Schnittstellen und zuverlässig verschlüsselte
Datentransfers

VPN-Appliance genucrypt
für stark verschlüsselte Datentransfers

Verschlüsselte Kommunikation via VPN bis VS-NfD

Datenkommunikation via Internet ist komfortabel und kostengünstig. Diese Vorteile können Sie auch beim Austausch von amtlich eingestuften Informationen – Verschlusssachen (VS) – nutzen, hier müssen jedoch hohe Sicherheitsanforderungen beachtet werden: VS-Daten dürfen via Internet nur mittels VPN-Systemen (Virtual Private Network) verschlüsselt und transferiert werden, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) die Zulassung für die entsprechende Geheimhaltungsstufe erhalten haben.

Unsere VPN-Lösungen werden in Deutschland hergestellt, arbeiten mit den stärksten Verschlüsselungsalgorithmen und sind bis zur Geheimstufe VS-NfD (Nur für den Dienstgebrauch) zugelassen. Damit wird der größte Teil der VS-Daten abgedeckt, da nur wenige Informationen höher klassifiziert sind. Behörden, Organisationen mit Sicherheitsaufgaben und geheimschutzbetreute Unternehmen können über unsere VPN-Lösungen somit VS-NfD-Daten komfortabel via Internet austauschen. Mit unseren mobilen Lösungen können Sie zudem Laptop-Anwender auf Reisen oder Mitarbeiter im Home Office sicher an VS-NfD-eingestufte Netze anbinden.

Security Laptop vs-top
zur Anbindung mobiler Mitarbeiter im Geheimschutzbereich

Personal Security Device genucard
zur Anbindung von Home Offices und kleinen Standorten im Geheimschutzbereich

Firewall & VPN-Appliance genuscreen
für starken Schutz an externen und internen Schnittstellen und zuverlässig verschlüsselte Datentransfers

Absicherung Fernwartung von Maschinen und IT-Systemen

Die Fernwartung von Maschinenanlagen oder IT-Systemen via Internet ist für beide Seiten attraktiv: Hersteller oder Dienstleister können ihren Kunden schnelle Unterstützung garantieren und ihr Service-Angebot erweitern; Kunden können jederzeit professionellen Support erhalten, Wartungsaufwand und Ausfallzeiten minimieren und somit Kosten sparen. Damit aus dieser profitablen Geschäftsbeziehung keine hohen Folgekosten entstehen, müssen aber hohe Anforderungen an die IT-Sicherheit erfüllt werden. Denn für die Fernwartung von Maschinenanlagen oder IT-Systemen müssen die Kunden ihre Netzwerke für externe Zugriffe öffnen. Sollten über diesen Weg Malware oder unbefugte Dritte bspw. in den Produktionsbereich des Kunden eindringen und zu Ausfällen führen, würde dies erhebliche Kosten verursachen – und sich mit Sicherheit auch auf die Geschäftsbeziehung zum Hersteller bzw. Dienstleister auswirken.

Wir unterstützen Hersteller, Dienstleister und auch Kunden, die Fernwartungs-Services nutzen, beim Aufbau hochsicherer Lösungen. Wichtige Merkmale unserer Lösungen sind die einfache Integration in bestehende Netze, die komfortable Bedienung sowie revisionssichere Kontrollmöglichkeiten des Kunden über alle Fernwartungs-Zugriffe.

Fernwartungs-Appliance genubox
für hochsichere Remote Service-Zugriffe
auf Maschinenanlagen und IT-Systeme

Absicherung Automatisierung

Hochgradige Automatisierung ermöglicht intelligente Fabriken – das Schlagwort ist „Industrie 4.0“: Maschinen reden mit Maschinen, die zu bearbeitenden Produkte liefern Informationen via Barcodes oder RFID-Chips, auch alle weiteren Systeme entlang der Fertigungskette vom Lager über die Logistik bis hin zum Service sind miteinander vernetzt und organisieren selbständig optimale Abläufe. So werden hocheffiziente Produktionsprozesse erreicht, die individuelle Fertigungen ermöglichen – obwohl kein Mensch steuernd eingreift. Für die Industrieproduktion ist dies ein großer Fortschritt. Aus der Perspektive der IT-Sicherheit stellt sich aber die Frage: Wenn alle mit allen kommunizieren, wie können sensible Daten vor unbefugten Zugriffen oder Steuerungssysteme von Maschinen vor Malware und Manipulationen geschützt werden?

Mit unseren Lösungen können Sie die Datenkommunikation kontrollieren, beschränken oder gar Transfers ausschließlich in eine Richtung zulassen und somit Ihre automatisierte Produktion hochwertig absichern.

Datendiode cyber-diode
zur hochsicheren Vernetzung von KRITIS
und Maschinenanlagen

Fernwartungs-Appliance genubox
für hochsichere Remote Service-Zugriffe
auf Maschinenanlagen und IT-Systeme

Absicherung Industrial Monitoring

Wer Anlagen wie Gasturbinen, Industrieroboter oder Werkzeugmaschinen einsetzt, möchte möglichst einen störungsfreien 24/7-Betrieb erreichen. Denn jeder Ausfall verursacht schnell beträchtliche Kosten – den Image-Verlust durch verspätete Lieferungen und verärgerte Kunden noch gar nicht mitgerechnet. Für eine hohe Betriebszuverlässigkeit ist ein fortlaufendes Monitoring ein wesentlicher Baustein. Darüber haben Sie jederzeit alle Betriebsdaten der Anlage im Blick und können bereits bei den ersten Anzeichen einer Störung reagieren, bevor diese zu einem schwerwiegenden Problem oder gar Ausfall führt.

Hier ist aber zu beachten: Jede Anlage, die zum Monitoring vernetzt wird, ist über diese Verbindung prinzipiell auch angreifbar. Um durch das Monitoring keine Einfallstore für Malware und Hacker zu schaffen und somit neue Ausfallrisiken einzugehen, müssen die Anlagen-Anbindungen zuverlässig abgesichert werden. Dafür bieten wir Ihnen eine hochwertige Lösung.

Datendiode cyber-diode
zur hochsicheren Vernetzung von KRITIS und Maschinenanlagen

LB-0815-2-D

www.genua.de

genua gmbh, Domagkstraße 7, 85551 Kirchheim bei München
tel +49 89 991950-0, info@genua.de, www.genublog.de

Auszug aus unserer Kundenliste:

- Behörden und Organisationen mit Sicherheitsaufgaben
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bundesministerium für Arbeit und Soziales
- Bundeswehr
- Deutscher Bundestag
- EUROGATE
- Freudenberg Gruppe
- Hubert Burda Media
- HypoVereinsbank
- Informationsverbund Berlin-Bonn (IVBB)
- KASTO Maschinenbau
- Klinikum der Universität München
- Klüber Lubrication
- Landeshauptstadt München
- MAN
- MTU Aero Engines
- Statistisches Bundesamt
- THW
- WMF
- Würth-Gruppe