PRESSEINFORMATION

Produkt-Übersicht

Lösungen für zuverlässige IT-Sicherheit

genugate: High Resistance Firewall für sichere Schnittstellen

Die Firewall genugate ist ein mehrstufiges Komplettsystem: Zwei unterschiedliche Firewalls – ein Application Level Gateway und eine Paketfilter – laufen auf separater Hardware, sind jedoch in Reihe geschaltet. Daten aus dem Internet müssen beide Firewalls passieren, um in das LAN zu gelangen. Die zweistufige Prüfung und die Inhaltskontrolle durch das Application Level Gateway unterscheiden die genugate von vielen anderen Firewalls. Diese Lösung hat auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) überzeugt, das die genugate nach Common Criteria (CC) in der Stufe EAL 4+ zertifiziert hat. Beim zentralen Sicherheitsmerkmal des Selbstschutzes erfüllt die genugate darüber hinaus die Anforderungen der Stufe EAL 7 – als einzige Firewall der Welt. Dies belegt die hohe Qualität der Firewall genugate.

genuscreen: Firewall & VPN-Appliance mit Zulassung für VS-NfD

Die Firewall & VPN-Appliance genuscreen kann mehrere Aufgaben übernehmen: Als Stateful Packet Filter kontrolliert sie den Datenverkehr und lässt nur ausdrücklich erwünschte Verbindungen zu – alle anderen Anfragen werden konsequent abgeblockt. Darüber hinaus baut genuscreen verschlüsselte Virtual Private Networks (VPN) auf, über die sensible Daten geschützt via Internet übertragen werden können. Diese VPN-Funktion ist vom BSI zugelassen für den Transfer von Daten bis zur Geheimstufe VS-NfD. Die hohe Qualität der Firewall & VPN-Appliance genuscreen belegt zudem ein BSI-Zertifikat nach CC EAL 4+.

cogntitix Threat Defender: Echtzeit-Angriffserkennung mit KI-Technologie

Der cognitix Threat Defender sorgt innerhalb von Netzen für Sicherheit. Der Netzwerkverkehr wird in Echtzeit analysiert, Bedrohungen identifiziert und mit Abwehrmaßnahmen gezielt reagiert. Mit KI-Technologie, Data Analytics und Threat Intelligence erkennt die Sicherheitsplattform cognitix Threat Defender Angriffe in Realtime und ist somit signaturbasierten Systemen mit statischen Regeln überlegen.

genucard: Security Device für mobile Anwender

Das Security Device genucard wird via USB mit einem Laptop oder Desktop Computer im Home Office verbunden und schützt die gesamte Datenkommunikation zum Firmennetz. Dafür ist die genucard mit einer Firewall und einem VPN-Gateway ausgestattet. Die besonderen Merkmale der genucard: Sie läuft unabhängig vom Laptop auf eigener Hardware, und die VPN-Funktion ist vom BSI zugelassen für den verschlüsselten Transfer von Daten bis zur Geheimstufe VS-NfD. Mit dieser Lösung können Firmen und Behörden die Zugriffe von Mitarbeitern im Home Office in ihre Netzwerke absichern.

vs-top und cyber-top zur sicheren Anbindung mobiler Mitarbeiter

Zur sicheren Anbindung mobiler Mitarbeiter an Behörden- und Firmennetze bietet genua die Laptops vs-top und cyber-top. Diese sind mit einer Windows-Arbeitsumgebung, einer Firewall und einem VPN-Gateway ausgestattet, das Besondere liegt aber darunter: Als unterste Schicht läuft auf den Laptop das Separationssystem L4, das mehrere voneinander isolierte Compartments erzeugt. Die Windows-Umgebung und die Sicherheitssysteme sind hier in jeweils eigene Compartments eingeschlossen. Sollte jetzt Malware in den Windows-Bereich eingedrungen sein, findet sie keinen Weg zu den separierten Sicherheitssystemen. Diese bleiben voll funktionstüchtig und sorgen weiterhin für Sicherheit. Für das vs-top läuft das Zulassungsverfahren bis zur Geheimhaltungsstufe VS-NfD.

genubox: Appliance für sichere Fernwartungs-Lösungen

Die Sicherheits-Plattform genubox ermöglicht Herstellern die Fernwartung ihrer bei Kunden installierten Maschinenanlagen oder auch IT-Systeme. Dazu wird die genubox beim betreuten System vor Ort installiert. Mit einem VPN-Gateway erzeugt sie verschlüsselte Verbindungen zum Herstellerservice, über den der Wartungszugriff erfolgt. Dabei schirmt sie gleichzeitig mit einer Firewall das betreute System vom restlichen Kundennetz ab, damit der externe Zugriff ausschließlich auf den Wartungsbereich führt – und nicht in andere Bereiche.

Sicherheits-Gateways und Dioden für hochsensible Schnittstellen

Mit Sicherheits-Gateways und Datendioden ermöglicht genua die Koppelung von Netzwerken, die unterschiedliche Sicherheitsniveaus aufweisen, sowie die Vernetzung von hochkritischen Steuerungssystemen. Denn die Sicherheits-Gateways kontrollieren exakt den Informationsfluss, und die Dioden lassen Daten ausschließlich in eine Richtung passieren. So wird ausgeschlossen, dass eingestufte Informationen in ungeschützte Netze abfließen bzw. unbefugte Zugriffe auf vernetzte Steuerungssysteme erfolgen können.

Weitere Informationen:

genua GmbH
Alexandra Korolija
Domagkstraße 7
85551 Kirchheim bei München
tel +49 160 97953284
alexandra_korolija@genua.de
www.genua.de