genua Ein Unternehmen der Bundesdruckerei

genucenter

Central Management Station

Technische Informationen

Inhaltsverzeichnis

1 Central Management Station für Ihre Sicherheitssysteme von genua

Gegen immer raffiniertere Angriffe aus dem Internet können Sie Ihre IT schützen, indem Sie Ihre Datenkommunikation mit VPN-Appliances verschlüsseln und mit zusätzlichen Firewalls innerhalb Ihres Netzes streng abgeschirmte Zonen für besonders sensible Systeme einrichten.

In der Theorie ist dieser komplexe Aufbau hochsicher, in der Praxis wird er jedoch schnell zum Problem: Alle eingesetzten Lösungen müssen richtig konfiguriert und fortlaufend betreut werden – denn das schwächste Glied entscheidet über das Niveau Ihrer IT-Sicherheit. Doch wie können Sie bei der Vielzahl der Sicherheitssysteme den Überblick behalten, ohne extrem hohen Administrationsaufwand leisten zu müssen?

Komplexe IT-Security-Architekturen bekommen Sie mit genucenter sicher in den Griff. Mit der Management Station werden die Sicherheitslösungen von genua zentral administriert. Durch die Multi-User-Fähigkeit können mehrere Administratoren gleichzeitig am System arbeiten. Die Aufgaben der einzelnen Produkte werden über ein modernes, übersichtliches Web-Interface in einem Standardbrowser konfiguriert, Statusmeldungen angezeigt und Aktualisierungen vorgenommen. Funktionen wie Autovervollständigung, Validieren von Eingaben sowie Drag & Drop sorgen für eine hohe Bedienungsfreundlichkeit – auch wenn viele tausend Appliances verwaltet werden.

genucenter eignet sich für Organisationen, die verschiedene Lösungen von genua oder eine größere Anzahl des gleichen Produkts einsetzen. Die Appliances können in Gruppen verwaltet werden, um nach bestimmten Kriterien auf sie zuzugreifen und spezifische Konfigurationen vorzunehmen.

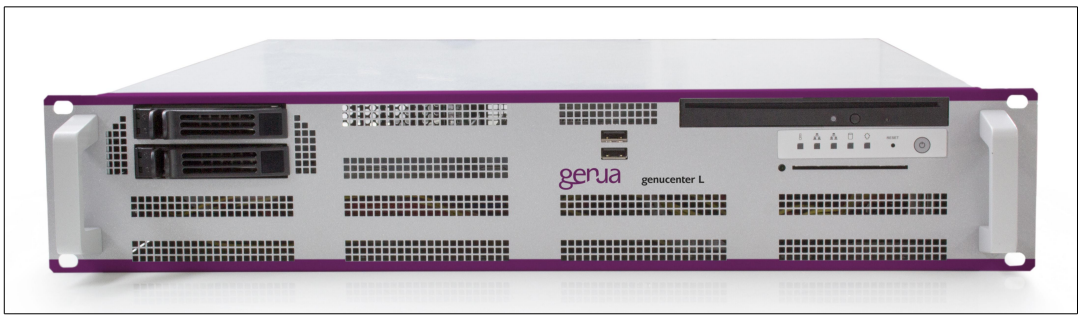

Abb. 1: Central Management Station genucenter

Der Einsatz der Central Management Station genucenter lohnt sich: Der Administrationsaufwand sinkt, das Sicherheitsniveau steigt. Und je komplexer das Netzwerk, desto größer die Vorteile. Aber auch die Administratoren kleiner Netzwerke werden durch das zentrale Management der Sicherheitssysteme bereits deutlich entlastet, da Routine-Aufgaben zentral und auf einmal erledigt werden können.

Folgende Produkte können mit genucenter verwaltet werden:

- Firewall & VPN-Appliance genuscreen
- VPN-Appliance genucrypt
- Personal Security Device genucard
- Fernwartungs-Appliance genubox
- Security Laptop cyber-top
- Security Laptop vs-top
- Datendiode cyber-diode
- Industrial Firewall genuwall
- Industrial Gateway GS.Gate

Auf den folgenden Seiten erhalten Sie einen kompakten Überblick über Funktionen und Einsatzmöglichkeiten der Central Management Station genucenter.

2 Mit genucenter Lösungen von genua verwalten

genucenter ermöglicht den Zugriff auf Ihre gesamte IT-Sicherheitsinfrastuktur von genua – an mehreren Standorten, Heimarbeitsplätzen und im mobilen Einsatz. Über das einheitliche GUI der Central Management Station werden alle Sicherheitslösungen konfiguriert, fortlaufend überwacht und administriert.

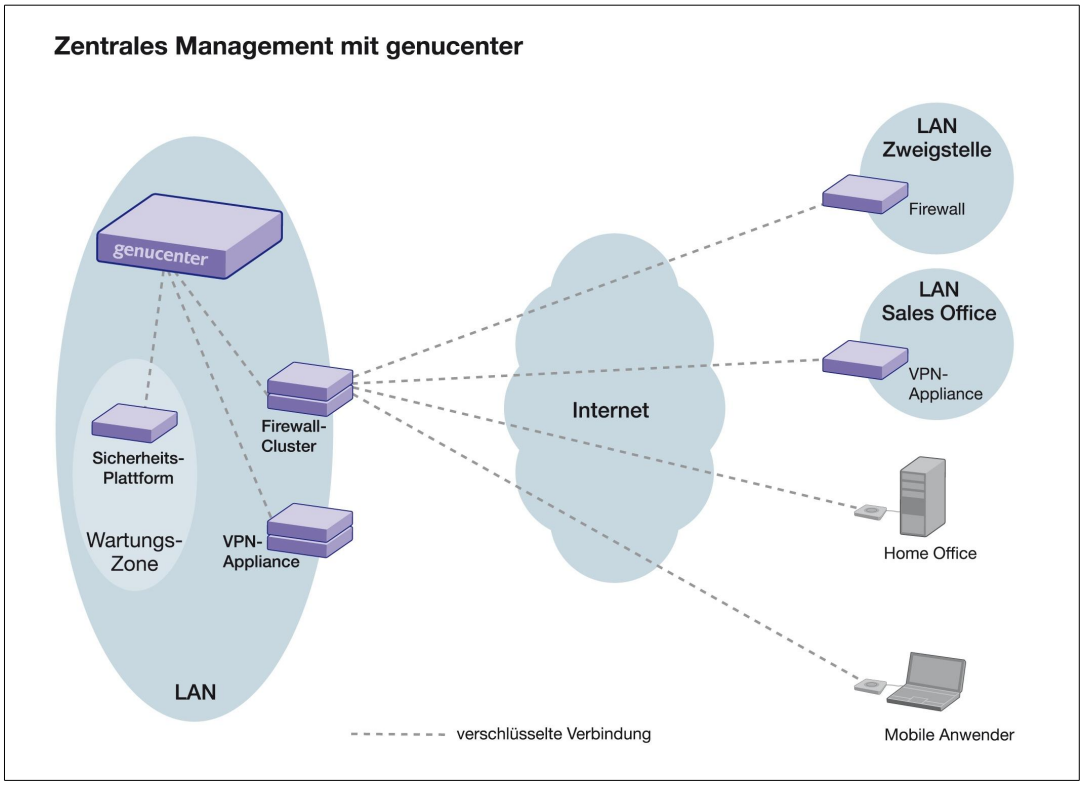

Abb. 2: Zentrales Management mit genucenter

Rollouts können schnell und zuverlässig durchgeführt werden. Änderungen und Updates lassen sich über komfortable Gruppierungs-Funktionen gleichzeitig auf beliebig viele Systeme per Bulk-Operation übertragen. So haben Sie den Status Ihrer IT-Sicherheit jederzeit im Blick und stellen sicher, dass alle Systeme auf dem neuesten Stand sind und einwandfrei funktionieren. Policies können auf diese Weise konsequent im gesamten Netzwerk durchgesetzt werden.

Mit genucenter können auch USB-Sticks geprägt werden, um damit Systeme zu initialisieren. Ein USB-Stick kann beispielsweise dann verwendet werden, wenn am Gerätestandort keine Internetverbindung vorhanden ist oder eine erste Konfiguration aufgespielt werden soll. Auch für schnelle Fallbacks sind USB-Sticks geeignet.

Für die verwalteten Systeme können auch Push- oder Pull-Mechanismen konfiguriert werden: So kann ein System Updates von genucenter abrufen, was wichtig bei mobilen Systemen oder Lösungen ist, die mit einer dynamischen IP angebunden sind. Alternativ überträgt genucenter Updates oder Konfigurationen auf die Systeme.

2.1 Erweiterbarkeit

Wenn Sie Ihre IT-Sicherheit mit neuen Appliances verstärken, werden diese ganz einfach in die Central Management Station integriert und gleich mit bewährten Konfigurationen ausgestattet. Beispielsweise muss eine zusätzliche Firewall & VPN-Appliance genuscreen nur in das bereits bestehende „Objekt“ VPN eingefügt werden. Alle notwendigen Einstellungen übernimmt genucenter selbständig und überträgt die entsprechende Konfigurationen automatisch auf alle Systeme des VPN-Verbunds. Hier zeigt sich ein wesentlicher Vorteil einer zentralen Management-Lösung: Zentrale Policies können konsequent auf alle verwalteten Appliances übertragen werden. Die Investition amortisiert sich schnell, da wachsende Infrastrukturen zeitsparend mit geringem Aufwand administrierbar sind.

2.2 Gruppierung von Appliances und Konfigurationseinstellungen

Bei der Verwaltung ist eine Gruppierung von Appliances und Konfigurationseinstellungen zu einer so genannten Domäne möglich. Dies verbessert die Übersichtlichkeit, wenn viele Maschinen zu verwalten sind:

In kleinen Setups mit wenigen Systemen und Administratoren kann eine Domäne ausreichen. In großen Setups mit vielen Standorten, Systemen und Administratoren werden Domänen üblicherweise genutzt, um beispielsweise geografische oder funktionell unterschiedliche Appliances voneinander zu trennen oder um den administrativen Zugriff darauf einzuschränken – Stichwort „Mandantenfähigkeit“.

So erlaubt die Abbildung in Form einer Baumstruktur mit mehreren Unterdomänen z. B. die Gruppierung von Systemen nach Standorten oder nach zuständigen Administratoren.

Für weitere Informationen lesen Sie unser Whitepaper „Central Management Station genucenter – Nutzung von Domänen zur strukturierten Verwaltung von Objekten und Systemen“.

2.3 Aufgabenzuweisung

genucenter ist mandantenfähig, so dass Sie Ihren Administratoren über ein Rollenkonzept bestimmte Aufgabenbereiche zuweisen können: Einer kümmert sich um die Firewalls in Deutschland, ein anderer um die internationalen VPN-Verbindungen usw. Auch für Vertriebspartner von genua und Dienstleister ist dieses Feature interessant: Sie legen alle Kunden, bei denen sie Support leisten, als Mandanten an – also jeden Kunden in eine eigene Domäne. So können über eine Central Management Station die Sicherheitssysteme verschiedener Kunden klar voneinander getrennt betreut werden.

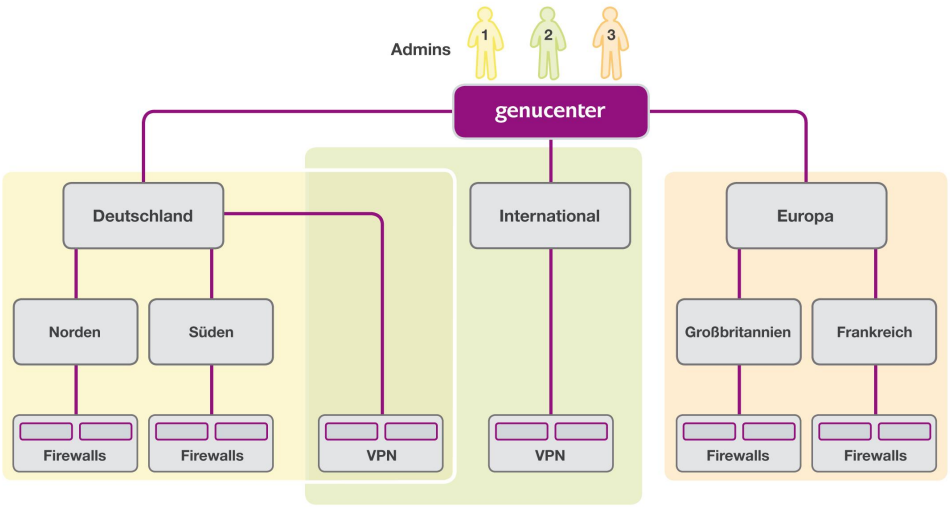

Abb. 3: Zuweisung von Zuständigkeiten an verschiedene Administratoren

2.4 Zentrale Durchsetzung komplexer Regelwerke

Komplexe Regelwerke lassen sich durch Objektreferenzierung weiterreichen: Erfolgen beispielsweise bei genuscreen Änderungen an einer Firewall-Regel, lassen sich diese über das Objekt, also eine wiederverwendbare Einstellung, auf alle Systeme innerhalb des Verbunds übertragen, die diese Regel verwenden.

So kann auch eine Rechtehierarchie über die Ebenen des Domänenbaums realisiert werden: Je höher die Rechteebene eines Administrators, desto mehr Appliances sind von seinen Einstellungen betroffen. Administratoren unterhalb dieser Rechteebene können dessen Einstellungen nicht beeinflussen. Sie können nur Regeln für Appliances unterhalb ihrer eigenen Rechteebene vorgeben, die nicht bereits auf einer höheren Ebene festgelegt wurden. Darüber hinaus lassen sich mit dem Revisionslog alle Änderungen lückenlos nachvollziehen.

2.5 Administration der Lösungen von genua

2.5.1 Firewall & VPN-Appliance genuscreen und VNP-Appliance genucrypt

genuscreen ist eine Kombination aus Firewall und VPN-Appliance, während es sich bei genucrypt um eine reine VPN-Appliance handelt.

genuscreen und genucrypt können über die Central Management Station genucenter sowohl installiert als auch administriert werden. Somit lassen sich VPN-Verbindungen einrichten und Geräte an unterschiedlichen Standorten zentral betreuen. Auch sehr große VPN-Netze können mit genucenter einfach aufgesetzt werden.

Zusätzlich bieten genucenter und genuscreen eine Lösung zur Initialisierung und Administration von Smartcards, auf denen sichere und nicht manipulierbare private Schlüssel und Sicherheitszertifikate gespeichert werden. So können mit genuscreen und dem Mobile Security Device genucard zuverlässig authentisierte VPN-Verbindungen erzeugt werden – Voraussetzung für den Einsatz auf der Geheimhaltungsstufe VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD). Das Smartcard-Management (Schlüssel erstellen und erneuern) erfolgt dabei über genucenter.

2.5.2 Personal Security Device genucard

Die genucard ist ein mobiles Sicherheitspaket mit Firewall, VPN-Gateway und Smartcard-Unterstützung für die VS-NfD-Datenkommunikation. Sie baut einerseits geschützte Verbindungen – Virtual Private Networks (VPN) – auf, mit denen das Internet sicher überbrückt wird. Andererseits schützt sie den Laptop durch die integrierte Firewall. Die Konfiguration, Administration und Überwachung mehrerer genucards erfolgt bequem mit der Central Management Station genucenter. Typische Aufgaben sind die Definition/Einschränkung von Verbindungen auf der genucard sowie die Einrichtung automatischer Updates.

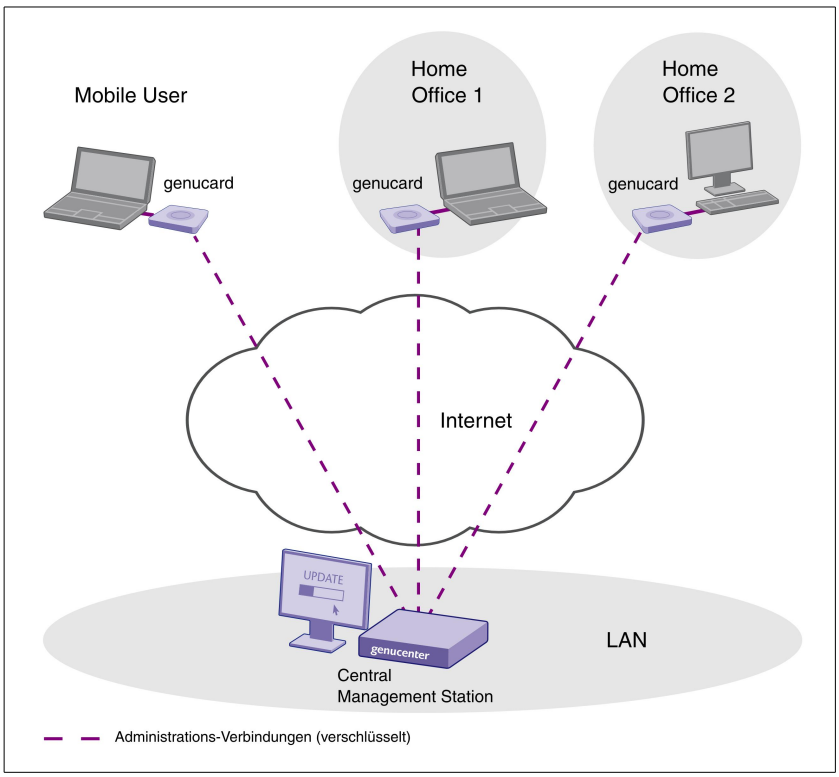

Abb. 4: Zentrale Administration von genucards im mobilen und Home Office-Einsatz

Das Personal Security Device genucard wird mit aufgespieltem Betriebssystem geliefert. Die genucard ist für eine zentrale Verwaltung ausgelegt, eine Administration durch den mobilen Benutzer ist nicht vorgesehen. Der Administrator legt die Karte auf der Central Management Station an und erstellt zumindest eine minimale Konfiguration, damit diese vom User verwendet werden kann. Für den Betrieb gilt grundsätzlich, dass eine genucard automatisch mit genucenter im lokalen Netzwerk Kontakt aufnimmt, sobald eine funktionierende Internetverbindung konfiguriert und diese vom mobilen Benutzer gestartet wurde. Nach der Kontaktaufnahme kann die Central Management Station Konfigurations-Updates der genucard durchführen. Einstellungen wie Firewall-Regeln können zentral vorgehalten werden und bleiben auf diese Weise auch bei Verlust oder Sperrung der Karte verfügbar.

2.5.3 Fernwartungs-Appliance genubox

genubox ermöglicht intelligente und sichere Remote Maintenance an jedem Ort, wie z. B. von Fertigungsrobotern und Druckmaschinen, Schiffsmotoren, Windrädern in abgelegenen Gebieten oder Ölförderanlagen auf See. Es besteht die Möglichkeit, den Wartungszugang zu Netzen zu autorisieren, zu authentifizieren, zu verschlüsseln und zu loggen.

genucenter erlaubt die zentrale Verwaltung der gesamten Produktfunktionalität. Damit lassen sich Steuerungs-, Überwachungs- und Fernwartungs-Anwendungen konfigurieren und Geräte an unterschiedlichen Standorten zentral betreuen. Ebenso ermöglicht genucenter die initiale Verteilung einer Fernwartungs-App für das beteiligte Personal zur einfachen Steuerung und Überwachung des Fernwartungsvorgangs.

Um unterschiedlichen Zuständigkeitsbereichen Rechnung zu tragen, bietet genucenter für die sichere Fernwartung mit dem Rendezvous-Konzept eine separate Bedienungsoberfläche. Damit kann ein Maschinenverantwortlicher lediglich den Fernwartungs-Zugriff durch einen Dienstleister steuern, weitergehende Einstellungen sind ihm nicht möglich. Die grundlegende Konfiguration der genubox bleibt dem Administrator vorbehalten, dem dazu das eigentliche Administrations-GUI zur Verfügung steht.

2.5.4 Security Laptops cyber-top und vs-top

Mit den Security Laptops cyber-top und vs-top können Mitarbeiter komfortabel in Hochsicherheitsnetzen arbeiten und gleichzeitig in anderen Bereichen Mail- oder Office-Anwendungen nutzen – ohne die bekannten Risiken. Dazu werden unterschiedliche Sicherheitsbereiche, sogenannte Compartments, mittels der Separationstechnologie L4 zuverlässig getrennt.

Mit genucenter lassen sich die Compartments, der verschlüsselte Netzwerkzugriff sowie die Firewall-Funktionen zentral administrieren.

2.5.5 Datendiode cyber-diode

Mit der cyber diode können Industrieanlagen, Embedded oder Cyber Physical Systems zum Monitoring ohne Risiken vernetzt werden. Die cyber-diode kontrolliert die Netzanbindung und lässt ausschließlich Einbahn-Datentransfers zu – in Gegenrichtung wird dagegen

jeder Informationsfluss konsequent abgeblockt. Mit genucenter ist eine vollständige zentrale Verwaltung der cyber-diode möglich.

2.5.6 Industrial Firewall genuwall

Mit der Industrial Firewall genuwall lassen sich Produktionsnetze (LAN, WAN und VLAN) vor Angriffen schützen. Sie ermöglicht Sicherheitszonen für einzelne Maschinen, ganze Anlagen oder Produktionsbereiche. Die genuwall kontrolliert zuverlässig den gesamten Datenverkehr und lässt ausschließlich die gewünschten Verbindungen zu. Sie basiert auf der bewährten Firewall genuscreen, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem internationalen Standard Common Criteria (CC) in der anspruchsvollen Stufe EAL 4+ zertifiziert ist.

2.5.7 Industrial Gateway GS.Gate

Das GS.Gate lässt sich herstellerunabhängig an Produktionsanlagen anbinden und ermöglicht den Abruf, die Analyse sowie die sichere Weiterleitung von Maschinendaten. Bereits im Industrial Gateway werden aus der erfassten Datenmenge die für Industrie 4.0-Anwendungen relevanten Informationen herausgefiltert. Diese können über die integrierte Firewall hochsicher verschlüsselt via Internet an Analytics-Systemen oder zur Cloud weitergeleitet werden. Dabei schützt das Industrial Gateway die vernetzte Maschine zuverlässig vor Cyber-Angriffen. Eine Remote Access-Komponente ermöglicht darüber hinaus sichere Fernwartungszugriffe.

2.5.8 genua Advanced Secure Connect

Die hochsichere Fernwartungs-Lösung genua Advanced Secure Connect stellt den reibungslosen Betrieb Ihrer zentralen SAP-Anwendungen sicher und ermöglicht so höchste Effizienz bei Ihren Unternehmensprozessen. Damit ist sie ein wichtiger Baustein für den SAP Advanced Secure Support. Dieser greift bei Bedarf via Fernzugriff auf Ihr SAP-System zu, führt Service-Sitzungen durch oder analysiert und empfiehlt notwendige Schritte zur Problemvorbeugung und -behebung, bevor diese zu Ausfällen führen. Unsere Lösung genua Advanced Secure Connect, die wir gemeinsam mit SAP entwickelt haben, garantiert Ihnen bei diesem Zugriff auf das sensible SAP-System ein sehr hohes Schutzniveau.

3 Hardware-Varianten und Hochverfügbarkeit

3.1 Produkt-Varianten

genucenter ist in Hardware-Varianten und als virtuelle Lösung erhältlich. Jede Produkt-Variante ist durch ihre Leistungsfähigkeit darauf ausgelegt, eine bestimmte maximale Anzahl an Systemen zu verwalten. Neben den Kapazitätsunterschieden bieten die größeren Hardware-Systeme Redundanz und damit eine automatische Datensicherung. Bei Fragen zur Bedarfsplanung steht Ihnen der Vertrieb von genua zur Verfügung.

Alle Systeme werden auf Industrie-PC-Hardware in 19"-Technik realisiert. Die Geräte benötigen zwei Höheneinheiten. Zu beachten ist, dass die Systeme eine Tiefe von 650 mm aufweisen und somit nicht in jeden Netzwerk-Schrank passen.

Da genua die Ausstattung der Hardware-Varianten (z. B. den CPU-Typ) laufend der technischen Entwicklung anpasst, unterliegen diese Daten steten Veränderungen. Die aktuelle technische Ausstattung erfahren Sie von unseren Vertriebsmitarbeitern oder über ein spezielles Hardware-Datenblatt.

3.2 Hochverfügbarkeit

Die Central Management Station genucenter kann auch als Hot Standby-Lösung eingerichtet werden. So werden Ausfallrisiken vermieden und der Austausch einer Appliance ist ohne Verlust der Funktionalität möglich.

Es ist möglich, eine oder mehrere Hot Standby-Maschinen als Backup einzusetzen. Im Fall mehrerer Backups können die Hot Standby-Maschinen georedundant stationiert werden. Ein Abgleich der Konfigurations- und Logging-Datenbank zwischen allen Backups erfolgt verschlüsselt im Sekundenbereich. Sollte der Master ausfallen, entscheidet der Administrator, welche Hot Standby-Maschine die Rolle des Masters übernimmt.

4 Zertifizierung und Zulassung

4.1 Zertifizierung

genua lässt wichtige Produkte nach internationalen Standards zertifizieren und regelmäßig re-zertifizieren, um die Qualität der implementierten Sicherheitsfunktionen nachzuweisen. Dadurch können die Produkte auch in Umgebungen mit höchsten Sicherheitsanforderungen eingesetzt werden.

Die Central Management Station genucenter ist in der Version 5.0 Z zur Konfiguration der Firewall & VPN-Appliance genuscreen Version 5.0 Z zertifiziert. Die Zertifizierung erfolgte nach Common Criteria (CC) Version 3.1 in der Stufe EAL 4+.

genucenter in der Version 7.0 Z durchläuft momentan ebenfalls das Verfahren zur Zertifizierung nach Common Criteria (CC) Version 3.1 in der Stufe EAL 4+.

4.2 Zulassung

Zulassungen können im Gegensatz zu Zertifizierungen nicht vom Hersteller beantragt werden. Zulassungsverfahren werden von staatlicher Seite angestoßen, wenn Behörden diese Produkte einsetzen möchten. Den Antrag stellt ein Bedarfsträger, die Zulassung wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bearbeitet und erteilt.

genucenter in der Version 7 wird für den VS-NfD-Einsatz von genuscreen in der Version 7.0 vorausgesetzt. Für weitere Informationen kontaktieren Sie bitte den Vertrieb von genua.

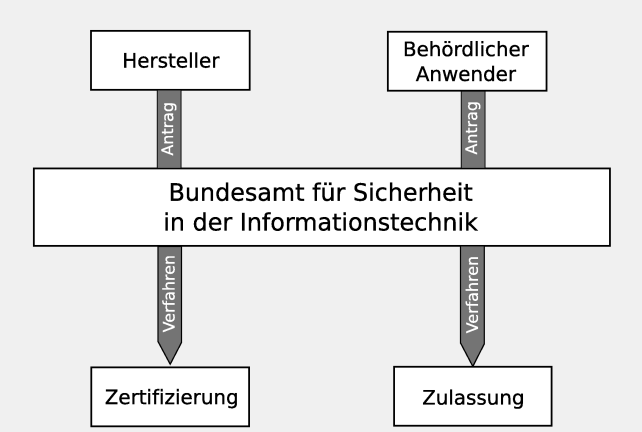

Abb. 5: Überblick Zertifizierung und Zulassung durch das BSI


5 Support

5.1 Einführung

Installations- und Konfigurations-Service: genua und spezialisierte Vertriebspartner unterstützen Sie auf Wunsch bei der Installation, Konfiguration und Inbetriebnahme der Central Management Station genucenter. Dabei werden die Administratoren ausführlich in die Benutzung und Pflege des Systems eingewiesen.

Anfangs-Support: Die Central Management Station genucenter ist so dokumentiert, dass die Inbetriebnahme und der laufende Betrieb keinerlei Schwierigkeiten bereiten sollten. Wenn Sie dennoch Fragen haben oder auf Schwierigkeiten stoßen, steht Ihnen unsere Hotline kostenlos 14 Tage lang zur Verfügung.

5.2 Schulungen

genucenter Training: Auf Anfrage bieten wir Administratoren und Technikern bedarfsgerechte Schulungen für Ihre Anwendung von genucenter. Sie lernen Aufbau und Funktionsweise der Central Management Station genucenter kennen sowie Konfigurationsmöglichkeiten und Überwachung des laufenden Betriebs – in Bezug auf die jeweils administrierten Sicherheitslösungen.

Dieses Schulungsangebot erfordert Absprache zu Inhalt und Termin. Unser Schulungsteam berät Sie gerne: E-Mail: schulung@genua.de, tel +49 89 991950-902.

5.3 Laufender Betrieb – Software Support

Update Service: Die Central Management Station genucenter wird ständig weiterentwickelt. Regelmäßig erscheinen neue Versionen, in denen aktuelle Entwicklungen aufgegriffen werden und der Funktionsumfang sinnvoll ergänzt wird. Je nach Bedarf erscheinen zusätzlich Zwischenversionen.

Unser Update Service sichert Ihnen die automatische Lieferung der neuesten Versionen und Zugriff auf unsere komplette Patch-Datenbank.

Hotline Service: Zusätzlich zu unserem Update Service bieten wir deutsch- und englischsprachigen Support via Telefon und E-Mail. Sie können unsere Hotline für alle Fragen zu Ihrer Lösung mit der Central Management Station genucenter nutzen. Der telefonische Hotline Support steht Ihnen auf Wunsch 24 Stunden an allen Tagen zur Verfügung.

Security System Management: Diese Leistung umfasst die ständige Überwachung und Wartung unserer Systeme, die bei Kunden für IT-Sicherheit sorgen, über stark verschlüsselte Internet-Verbindungen.

5.4 Laufender Betrieb – Hardware Support

Next Business Day Austausch-Service: Bei defekter Hardware erhalten Kunden innerhalb Deutschlands am nächsten Werktag ein baugleiches Gerät im Austausch für das defekte Gerät. Leistungsumfang und Voraussetzungen entnehmen Sie bitte den Allgemeinen Vertragsbedingungen der genua GmbH.

5.5 Support von Vertriebspartnern

Support-Leistungen von Vertriebspartern: Viele autorisierte Vertriebspartner von genua bieten zum Teil erweiterte Support-Optionen an, z. B. Vor-Ort-Austauschservice von Hardware innerhalb garantierter Maximalzeiten.

6 Kontakt und Vertrieb

Die Central Management Station genucenter ist über autorisierte Fachhändler und über genua erhältlich. Eine aktuelle Liste unserer Partner finden Sie unter:

https://www.genua.de/partner.html

Unser Vertrieb nennt Ihnen gerne einen Vertriebspartner in Ihrer Nähe.

GZ-WP-0619-10-D

So erreichen Sie uns:

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München
tel +49 89 991950-0, fax +49 89 991950-999, info@genua.de, www.genua.de


7 Glossar

Appliance	IT-System, das für einen bestimmten, eingegrenzten Verwendungszweck bestimmt ist. Es stellt eine für den jeweiligen Zweck optimierte Kombination von Hard- und Software dar.
BSI	Das Bundesamt für Sicherheit in der Informationstechnik ist der zentrale IT-Sicherheitsdienstleister des Bundes.
Cluster	Gruppe von Rechnern, die so eng zusammenarbeiten, dass sie nach außen wie ein einzelner Rechner auftreten. Cluster können gegenüber einzelnen Rechnern erhebliche Performance-Steigerungen erzielen und bieten ein hohes Maß an Ausfallsicherheit.
GUI	Graphical User Interface. Grafische Bedienungsoberfläche. Produkte von genua lassen sich komfortabel über ein GUI bedienen, das sich mit einem Standard-Webbrowser ausführen lässt.
Hot-Standby	Verhaltensweise redundanter Komponenten in einem IT-System zur Steigerung der Verfügbarkeit. Diese sorgt dafür, dass beim Ausfall einer Komponente automatisch Ersatzgeräte aktiviert werden. Daraus resultieren äußerst geringe Ausfallzeiten.
LAN	Local Area Network, nicht-öffentlicher Netzwerkbereich eines räumlich begrenzten Standorts.
Rendezvous-Konzept	Konzept, bei dem ein Unternehmen jeden Fernwartungszugriff auf seine Maschinen genau kontrollieren kann.
Smartcard	Hardwarekomponente, die Teil eines Systems zur Identifizierung und Authentisierung von Benutzern ist.
VPN	Virtual Private Network – Technik zur Verbindung externer Rechner mit einem lokalen Netzwerk, bei der das Internet als Transportmedium dient. Die Daten werden dabei verschlüsselt.
VS-NfD	Verschlusssache – nur für den Dienstgebrauch. Geheimhaltungsstufe für schutzbedürftige Informationen. Die Kenntnisnahme solcher Informationen durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein.