



Security Laptop cyber-top

Hochsicheres und mobiles Arbeiten in getrennten Netzen

Firmen müssen hochsensible Geschäftsdaten zuverlässig vor Verlust oder Spionage schützen. Deshalb werden für Bereiche, in denen die sogenannten Kronjuwelen bearbeitet werden, häufig eigene Sicherheitszonen eingerichtet: Beispielsweise bekommt der Vorstand ein eigenes Netz, die Fachleute für Acquisitions & Mergers, die Patentabteilung, der Forschungsbereich – dies variiert je nach Größe, Branche und Ausrichtung der Firmen. Zugreifen können hier nur die Vorstände bzw. Mitarbeiter der jeweiligen Abteilungen, von anderen Netzbereichen werden die Sicherheitszonen dagegen strikt separiert, um das Eindringen von Unbefugten und Malware zu verhindern. Mit dieser Netzwerk-Separation legen Sie eine wichtige Grundlage zum Schutz Ihrer vertraulichen Daten.

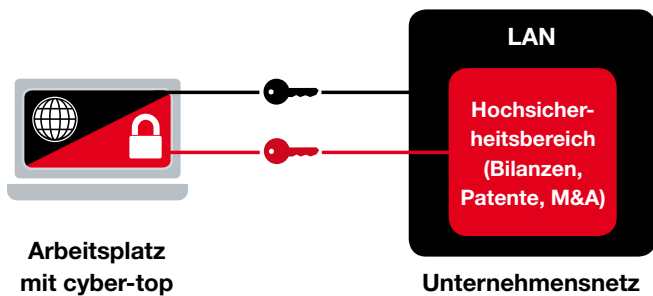
Hohe Sicherheit erfordert konsequente Separation

Um ein hohes Schutzniveau zu erreichen, müssen Sie die Netzwerk-Trennung konsequent bis zu den Workstations der Mitarbeiter weiterführen. Denn von hieraus wird auf Daten in Sicherheitszonen zugegriffen, gleichzeitig aber auch in anderen Netzbereichen mit E-Mail- und Office-Anwendungen gearbeitet oder via Browser im Internet gesurft. Diese Anwendungen bieten jedoch zahlreiche Angriffsflächen. Sollten Angreifer oder Malware darüber auf die Workstation gelangen, sind sie im nächsten Schritt in der Sicherheitszone. Mit dem Laptop cyber-top können Sie diese Sicherheitslücke schließen. Denn das Security Laptop hält mittels der Separationstechnologie L4 die unterschiedlichen Netzbereiche auf dem kompakten Laptop zuverlässig auseinander.



Kein Durchkommen für Angreifer und Malware

Das Separationssystem L4 erzeugt auf dem Security Laptop strikt isolierte Compartments: In einem laufen bspw. die Mail- und Office-Anwendungen, in einem weiteren werden die Vorstandsdaten bearbeitet – Sie können die Compartments individuell nach Ihrem Bedarf auf dem cyber-top einrichten. Da jedes Compartment mit einem eigenen Betriebssystem ausgestattet ist, bestehen keine Abhängigkeiten: Angreifer oder Malware finden somit keinen Weg von einer Arbeitsumgebung in eine andere, etwa aus dem Office- in den Vorstandsbereich. Diese konsequente Separation garantiert Ihnen hohe Sicherheit. Die komplette Festplatte des Security Laptops wird zudem zuverlässig verschlüsselt, und der Key auf einer Smartcard gespeichert. Selbst wenn das Laptop verloren gehen sollte, kommt somit niemand an Ihre Daten ran.



Überall ganz komfortabel arbeiten

Für Mitarbeiter ist das cyber-top trotz der starken Sicherheitsleistung komfortabel einzusetzen. Sie arbeiten unter Windows oder auch Linux mit den gewohnten Anwendungen. Und ein integriertes VPN-Gateway sowie eine Firewall, die als sicherheitskritische Systeme natürlich ebenfalls in einem isolierten Compartment laufen, schützen vor unbefugten Zugriffen und ermöglichen zudem den Aufbau verschlüsselter Verbindungen (Virtual Private Network) zur Datenübertragung bspw. via Internet. Unsere VPN-Lösungen arbeiten mit den stärksten Verschlüsselungsalgorithmen und sind mit heutiger Technologie nicht zu knacken. So können Ihre Mitarbeiter überall – im Büro, Home Office und unterwegs – sensible Daten abrufen und bearbeiten.

Das haben Sie vom cyber-top:

- Hohe Sicherheit durch Arbeiten in strikt getrennten Netzen
- Individuelle Einrichtung von getrennten Arbeitsumgebungen
- Sichere Anbindung mobiler Mitarbeiter
- Kompaktes Laptop mit gewohnten Anwendungen ist einfach zu bedienen
- VPN-Anbindung über Mobilfunk, WLAN und Ethernet
- VPN-Technologie Made in Germany
- Zuverlässige Festplatten-Verschlüsselung
- Unterstützung von IPv4 und IPv6
- Komfortable Administration über Management Station
- Kundenservice direkt vom Hersteller

Weitere Informationen unter:
www.genua.de/cyber-top

www.genua.de

Geringe Komplexität als Sicherheits-Feature

Die L4-Technologie des Security Laptops cyber-top schützt Ihre IT nicht nur durch konsequente Separation, ein weiteres wichtiges Sicherheits-Feature ist ihre geringe Komplexität. L4 ist als Microkernel-Betriebssystem ganz minimalistisch programmiert – lediglich einige tausend Zeilen Code. Hier kann, im Gegensatz zu anderen Betriebssystemen mit einigen Millionen Code-Zeilen, der gesamte Quellcode gründlich auf Fehler überprüft werden. Die hohe Qualität unserer Sicherheitslösung belegt auch die Zulassung des Laptops vs-top für die Geheimhaltungsstufe VS-NfD (Verschlusssache - Nur für den Dienstgebrauch) durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Denn das cyber-top basiert auf der gleichen Technologie wie das vs-top.

Zentrale Administration

Administriert wird das Security Laptop cyber-top über die Management Station genucenter. Darüber haben Sie die Laptops vieler Anwender von der Zentrale aus im Blick, können überall die gewünschte Konfiguration einstellen, jederzeit Änderungen vornehmen oder Up-dates aufspielen und somit Ihre Policy konsequent durchsetzen. So erreichen Sie unternehmensweit ein sehr hohes Sicherheitsniveau.

Über genua

Die genua GmbH ist ein deutscher Spezialist für IT-Sicherheit. Seit der Firmengründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken und bieten hochwertige Lösungen. Unser Leistungsspektrum umfasst die Absicherung sensibler Schnittstellen im Behörden- und Industriebereich bis hin zur Vernetzung hochkritischer Infrastrukturen, die zuverlässig verschlüsselte Datenkommunikation via Internet, Fernwartungs-Systeme sowie Remote Access-Lösungen für mobile Mitarbeiter und Home Offices. Unsere Lösungen werden in Deutschland entwickelt und produziert. Viele Firmen und Behörden setzen auf Lösungen von genua zum Schutz ihrer IT. genua ist ein Unternehmen der Bundesdruckerei-Gruppe.

SecurITy
 made
 in
 Germany

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