NCP
SECURE COMMUNICATIONS

Schützen Sie Ihre kommunale Infrastruktur – mit VPN Made in Germany!

Cyberattacken auf die öffentliche Verwaltung und KRITIS-Einrichtungen sind längst keine Seltenheit mehr. Sowohl das BKA als auch das BSI warnen vor den stark gestiegenen Angriffszahlen auf kommunale Infrastrukturen. Wie NCP Sie beim Schutz sensibler Daten und wichtiger Bürger-Services zuverlässig unterstützt, lesen Sie im Folgenden.

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

IT-Sicherheit „Made in Germany"

Erhöhen Sie Ihr Sicherheitslevel und wirken Sie mit IT-Security „Made in Germany" der verschärften Bedrohungslage entgegen:

- Keine Backdoors
- VPN-Produkte nach höchsten Sicherheitsstandards
- Digitale Souveränität: Keine Datenspeicherung im Ausland
- Schneller, direkter Support vom Hersteller

Business Continuity

Auch in Krisenzeiten müssen Organisationen zu jeder Zeit produktiv und sicher arbeiten können. Die VPN-Lösungen von NCP ermöglichen dies auf vielfältige Weise:

- Inbetriebnahme für tausende Nutzer in kürzester Zeit
- Hohe Skalierbarkeit
- Kompatibel zu vorhandener Hard-/Software
- Bedarfsgerechte, flexible Lizenzmodelle

Security-Empfehlungen des BSI

- Absicherung des Netzwerks durch eine umfassende Firewall
- Überprüfung der Endgeräte auf Aktualität von Virenscanner, OS, etc.
- Aktualisierung verwendeter Software durch Sicherheits-Updates
- Mehrfache Absicherung durch Multifaktor-Authentifizierung
- Verwendung starker Passwörter

> *„Die Stärkung der Cyber-Resilienz von Bundesbehörden [....] duldet ebenso wie die Modernisierung der Cybersicherheitsarchitektur [...] keinen Aufschub."*
>
> ***Bundesministerium des Innern und für Heimat***

VPN-Bypass

Legen Sie mit wenigen Mausklicks fest, dass datenhungrige und nicht sicherheitsrelevante Dienste wie Videostreaming ihre Daten am VPN-Tunnel vorbei ins Internet schicken dürfen. Auf diese Weise entlasten Sie den Server und sorgen dafür, dass immer genügend VPN-Bandbreite für die sichere Datenübertragung zur Verfügung steht.

Quality of Service

Mithilfe der „Quality of Service"-Funktionalität kann der IT-Administrator bestimmten Anwendungen eine zugesicherte ausgehende Datenrate zuweisen. Auf diese Weise werden u. a. Verzögerungen oder Unterbrechungen bei Videoanrufen verhindert, wenn ein User im Homeoffice nur über eine langsame Upload-Geschwindigkeit verfügt.

Endpoint Policy Checks

Legen Sie individuelle Sicherheitsparameter fest, die bei jedem User und Endgerät vor dem Zugriff auf das Firmennetz automatisiert überprüft werden. Erfüllt ein Endgerät die Policy-Anforderungen nicht, wird die Verbindung zum Firmenserver so lange verwehrt, bis das Gerät die nötigen Software-Updates erhalten hat.

Multi-Faktor-Authentifizierung

Sichern Sie Ihre Nutzer-Zugänge mittels Multi-Faktor-Authentifizierung (MFA) doppelt vor Angriffen ab. Nutzen Sie entweder biometrische Faktoren wie Gesichts- und Fingerabdruckerkennung oder generieren Sie mithilfe unserer kostenlosen NCP Authenticator App zeitbasierte Einmalpasswörter für maximale Sicherheit.

+358%

Zunahme der Schäden durch Cyber-Angriffe (im Vergleich zu 2018/19)

22%

mehr Varianten an Schadprogrammen (im Vergleich zu 2020)

76%

der Deutschen haben Angst vor Eskalationen als Folge staatlicher Cyberangriffe

Quellenangaben:

Basistipps zur IT-Sicherheit (BSI)
Presseinformation: Drei Viertel der Deutschen haben Angst vor einem Cyberkrieg (bitkom, 2022)
Die Lage der IT-Sicherheit in Deutschland (BSI, 2021)
Programm-Papier „Deutschland gegen Krisen und Klimafolgen wappnen" (Bundesinnenministerium, 2022)
Studie „Wirtschaftsschutz 2021" (BSI, 2021)

Weitere Infos auf unserer Webseite!

Sie möchten sehen, wie sich die NCP-Lösung bei Ihnen einsetzen lässt?
Ihren Ansprechpartner erreichen Sie unter **vertrieb@ncp-e.com** oder unter **+49 911 9968 0**.

NCP engineering GmbH | Dombühler Straße 2
90449 Nürnberg | www.ncp-e.com