NCP Secure Communications

VPN Software erhält BSI-Zulassung

[12.07.2021] Die VPN-Software-Lösung NCP VS GovNet Connector hat die Zulassung des Bundesamts für Sicherheit in der Informationstechnik (BSI) erhalten. Dies betrifft die Übertragung von Daten der Geheimhaltungsstufen VS-NfD sowie RESTREINT UE/EU RESTRICTED und NATO RESTRICTED.

NCP hat jetzt die Version 2.0 des NCP VS GovNet Connector veröffentlicht. Wie der Software-Hersteller mitteilt, ist die Lösung für die Verarbeitung von Daten der Geheimhaltungsstufe „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD) sowie RESTREINT UE/EU RESTRICTED und NATO RESTRICTED vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen. Der NCP VS GovNet Connector 2.0 sei das Bindeglied zwischen dem VS-NfD-Daten verarbeitenden Arbeitsplatz und der zugehörigen Gegenstelle.
Laut NCP lässt sich die rein softwarebasierte Lösung VS GovNet Connector 2.0 mit Standardwerkzeugen auf die jeweiligen Arbeitsplätze verteilen. Die Software arbeite mit Verschlüsselungsalgorithmen und sei speziell auf den Einsatz in Ministerien, Behörden und geheimschutzbetreuten Unternehmen abgestimmt. Dabei diene sie der sicheren Bearbeitung und Übertragung von Daten mit der Einstufung unter anderem als VS-NfD. Ohne an eine spezielle Hardware gebunden zu sein, garantiere der Software Client eine einfache Handhabung. Roll-out, Inbetriebnahme, Software Update und Administration erfolgen über das NCP Secure Enterprise Management (SEM) als Single Point of Administration. Flexible Lizenzmodelle wie Pay-per-Use sollen jeden Kundenbedarf abdecken.
Das in der Version 2.0 neu integrierte Feature des Self Check (Integritätsdienst), so der Hersteller, steigert die Sicherheit des NCP VS GovNet Connector 2.0. Der VPN-Client führe beim Start und regelmäßig während des Betriebs Selbsttests der sicherheitsrelevanten Funktionen durch. Die Selbsttests beinhalten etwa die Überprüfung der Authentizität und Integrität der VPN-Software, die Prüfung der korrekten Ausführung von Krypto-Algorithmen sowie von Zufallszahlengeneratoren. Beim Fehlschlagen der Selbsttests nehme der VPN-Client einen sicheren Zustand ein und der Arbeitsplatzrechner dürfe nicht mehr kommunizieren.
Der NCP VS GovNet Connector 2.0 werde auf Endgeräten mit Standard Windows 10 Betriebssystem installiert. Nach erfolgreicher Authentisierung stehen dem Benutzer über LAN, WLAN oder Mobilfunk via VPN alle Anwendungen und Ressourcen aus dem zentralen Datennetz zur Verfügung.

Drei spezielle Features

Neben der Unterstützung von Zertifikaten beziehungsweise SmartCards in einer PKI (Public Key Infrastructure) biete der NCP VS GovNet Connector 2.0 eine biometrische Authentisierung vor der VPN-Auswahl. Diese erfolge beispielsweise über Fingerabdruck oder Gesichtserkennung. Die Authentisierung starte direkt nach dem Klick auf den Verbinden-Button in der Connector-GUI, wobei der Verbindungsaufbau erst einsetze, wenn die biometrische Authentisierung erfolgreich abgeschlossen sei. Besitze der Rechner keine Hardware zur biometrischen Authentisierung oder sei diese nicht aktiviert, könne sich der Anwender auch über sein Passwort authentisieren.
Die von NCP patentierte VPN Path Finder Technology ermögliche Remote Access auch hinter Firewalls beziehungsweise Proxies, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindere. Hierbei werde automatisch in einen modifizierten IPsec-Protokoll-Modus gewechselt, der den zur Verfügung stehenden HTTPS-Port für den VPN-Tunnel nutze. Alle in IPsec enthaltenen Sicherheitsmerkmale bleiben

zu 100 Prozent erhalten, sodass das VPN Path Finder Protokoll sicherheitstechnisch nicht neu bewertet werden müsse. Als großen Vorteil der VPN Path Finder Technology hebt NCP hervor, dass der Administrator seine Security Policy verlässlich behördenübergreifend umsetzen kann. Der Anwender nutze durchgängig alle Authentifizierungsmechanismen und Vorteile von IPsec.
Durch die Quality-of-Service-Funktion werde Bandbreite für konfigurierte Applikationen wie etwa VoIP reserviert. Die Priorisierung ausgewählter Datenquellen am Anwender-PC geschehe für den Datentransport im VPN-Tunnel in Senderichtung. Für den Anwender im Homeoffice ergebe sich daraus eine ungestörte VoIP-Kommunikation durch den VPN-Tunnel auch bei hohem Datenaufkommen.

(th)

Stichwörter: IT-Sicherheit, NCP engineering, BSI, NCP VS GovNet Connector, VPN