

Digitale Verschlusssachen: For your eyes only

Mit der passenden Architektur zeitgemäß und
VS-NfD-konform mobil arbeiten

Streng vertrauliche Kommunikation kann heutzutage auch für geheimhaltungsbetonte Unternehmen mobil erfolgen. Mit genua als Partner bauen Anwender individuell zugeschnittene Strukturen auf – gesetzeskonform und alltagstauglich.

Von Frank Jablonsky, freier Autor für genua GmbH

Da freut sich der Wettbewerb: Im vollbesetzten ICE-Abteil diskutiert der Entwicklungsleiter eines mittelständischen Unternehmens lautstark am Mobiltelefon über ein geplantes Aggregat, dessen Details zudem gut auf seinem Laptop einsehbar sind. Ein solches Verhalten kann nach hinten losgehen – etwa, wenn sensible Informationen in falsche Hände gelangen.

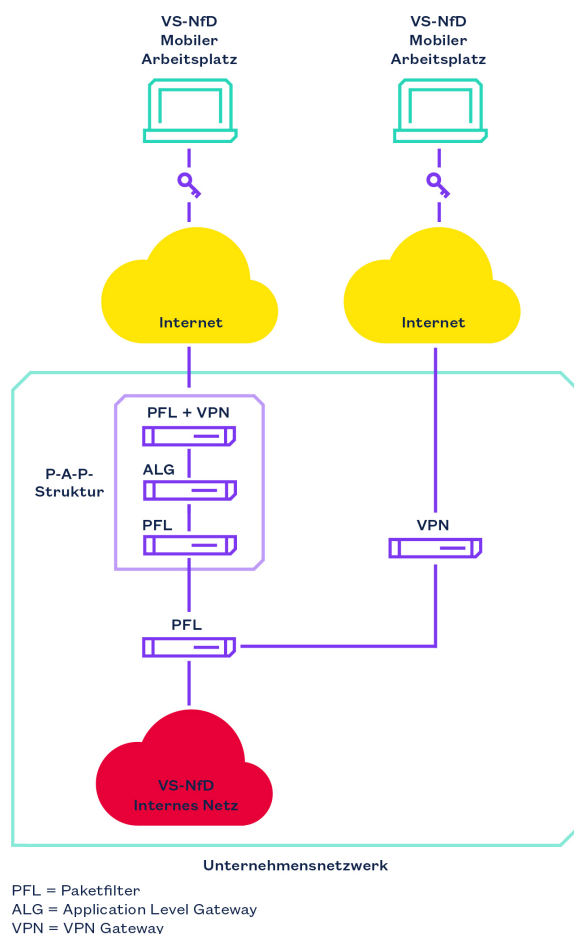
Besonders vorsichtig müssen Akteure agieren, die mit Informationen des Geheimhaltungsgrades „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD) umgehen. Mitarbeiter von Behörden, Rüstungsunternehmen, Ingenieurbüros oder Beratungsunternehmen sind es mittlerweile gewohnt, an unterschiedlichen Standorten, beim Kunden oder Partner zu arbeiten – oder auf dem Weg zwischen diesen Orten.

Zwar gibt es für den Fall, dass VS-NfD-Daten verarbeitet, gespeichert oder übertragen werden, klare gesetzliche Vorgaben für Technik, Betrieb und Organisation in Bezug auf die eingesetzte IT. Dennoch navigieren die betroffenen Unternehmen in der Praxis durch ein undurchsichtiges Spannungsfeld: Mobile Arbeitsweisen treffen auf gewachsene IT-Strukturen und komplexe regulatorische Rahmenbedingungen.

Der mobile Zugriff auf VS-NfD-Daten ist daher nicht selten eingeschränkt oder mit einem hohen Aufwand verbunden. Das betrifft sowohl die technische Umsetzung als auch die Integration in bestehende Prozesse. Damit Anwender nicht verleitet werden, unsichere Workarounds wie nicht zugelassene Datenträger zu nutzen, ist es wichtig, dass die mobilen Arbeitsplätze nicht nur regelkonform, sondern auch praxistauglich sind.

Einsatz BSI-zugelassener Lösungen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verlangt, dass VS-NfD-eingestufte Dokumente nur in einem entsprechend freigegebenen Netz bearbeitet und gespeichert werden dürfen. Sobald diese Enklave eine Verbindung zu einem Netz mit geringerem Sicherheitsniveau haben soll – etwa dem Firmen-LAN oder dem Internet –, muss dieser Übergang als P-A-P-Firewall-Struktur aufgebaut sein.



Diese mehrschichtige Sicherheitsarchitektur ähnelt einem Sandwich: Zwischen dem äußeren und dem inneren Paketfilter befindet sich ein Application Layer Gateway (ALG). Dabei analysieren die Paketfilter den Datenverkehr anhand netzwerk- und transportbezogener Merkmale wie Quelle, Ziel, Protokoll und Port (OSI-Schicht 3 und 4) und schützen dadurch das ALG vor direkter Exposition und unnötiger Belastung. Das ALG agiert dagegen als Proxy auf Anwendungsebene (OSI-Schicht 7), kontrolliert Protokolle, Inhalte und Verbindungsabläufe, terminiert bestehende Verbindungen und baut bei zulässiger Kommunikation eine neue Verbindung zum internen Netzwerk auf.

Mobile Arbeitsplätze, die auf Dokumente in einem VS-NfD-Netz zugreifen, müssen besonders abgesichert sein und strenge gesetzliche Vorgaben erfüllen. Dafür bietet die genua GmbH, ein Unternehmen der Bundesdruckerei-Gruppe, VS-NfD-konforme Lösungen wie die genusecure Suite an. Diese kombiniert den VPN-Client genuconnect mit einer Festplattenverschlüsselung und einer Smartcard-Middleware für eine sichere Multi-Faktor-Authentifizierung und digitale Signaturen. Mit diesem Bundle lassen sich Windows-11-Arbeitsplätze für mobiles Arbeiten, Homeoffice oder den Einsatz bei Partnern mit Lösungen „Made in Germany“ gesetzeskonform absichern.

VS-NfD-Minimallösung

Allerdings sind nicht alle Anwendungen über einen Kamm zu scheren. Je nach Aspekten wie Firmengröße, Budget, der erwarteten Nutzungshäufigkeit oder der verwendeten Verarbeitungsmethode der Dokumente können die Architekturen variieren. Möglicherweise reicht bereits eine Basislösung aus.

Das einfachste Setup kommt ohne P-A-P-Struktur im Heimatnetz aus. Es besteht aus einem abschließbaren Rack mit einem (File-)Server für VS-NfD-Dateien sowie einem zugelassenen VPN-Gateway. In dieser Minimalvariante besteht kein Übergang des VS-NfD-Netzes in ein unsicheres Netz (allgemeines LAN oder WAN). Der Zugriff auf den Server erfolgt ausschließlich über eine zugelassene verschlüsselte VPN-Verbindung, die am VPN-Gateway terminiert.

Erfolgt dieser Zugriff von einem mobilen Endgerät, benötigt dieses einen vom BSI zugelassenen VPN-Software-Client. Da VS-NfD-Daten lokal auf dem mobilen Endgerät gespeichert werden können, müssen diese auch im Ruhezustand geschützt werden. Daher ist zusätzlich eine BSI-zugelassene Festplattenverschlüsselung erforderlich. Da in dieser Variante kein Übergang in ein unsicheres Netz besteht, ist über diesen Rechner kein Zugriff auf Netzwerke außerhalb des VS-NfD-Netzes möglich – etwa für Recherchen im Internet.

Fokus auf Skalierbarkeit

Soll ein Übergang zwischen dem VS-NfD-Netz und einem nicht für VS-NfD freigegebenen Netz (zum Beispiel Firmen-LAN oder das Internet) bestehen, schreibt das BSI eine P-A-P-Struktur vor. Dadurch erhält ein mobiles Endgerät Zugriffe auf Netzwerke außerhalb des VS-NfD-Netzes. Dabei kann der äußere Paketfilter der P-A-P-Struktur als VPN-Gegenstelle agieren, sofern dieser über eine Zulassung als VPN-Gateway verfügt. Dadurch können mobile VS-NfD-Arbeitsplätze per VPN auf diesem terminieren.

In diesem Aufbau ist keine separate VPN-Komponente erforderlich und die bestehende P-A-P-Struktur kann für die mobile Anbindung mitgenutzt werden. Allerdings kann es auf dem äußeren Paketfilter bei höherer Last durch die zusätzliche Verarbeitung von VPN-Verbindungen zu Performance-Problemen kommen.

Zukunftssichere Lösung

Sollen mehrere Mitarbeiter mit Mobilgeräten Zugriff auf VS-NfD erhalten, ist der Einsatz eines zusätzlichen VPN-Gateways zwecks Lastverteilung sinnvoll. Diese VPN-Gegenstelle wird am Netzübergang in einer demilitarisierten Zone (DMZ) platziert und leitet den Datenverkehr zu einem internen Paketfilter im VS-NfD-Netz weiter. Durch die Kombination aus VS-NfD-konformer Netzarchitektur und VS-NfD-konformen Arbeitsplätzen (inklusive zugelassener Verschlüsselung) wird sichergestellt, dass die vertraulichen Dokumente die VS-NfD-Domäne nie verlassen.

Diese Beispiele zeigen, wie unterschiedlich die Herangehensweise an eine zeitgemäße und gleichzeitig sichere mobile Arbeitsweise im VS-NfD-Umfeld sein kann. Speziell beim Aufbau einer streng vertraulichen Kommunikation ist es sinnvoll, an den Anfang eine intensive Beratung zu stellen. Im individuellen Gespräch ist Raum für organisatorische und technische Vorgaben genauso wie für eine gemeinsame Planung der Segmentierung und Zugriffsmethode – basierend auf einer gründlichen Risikoanalyse.

Auf diese Weise entsteht – ausgehend von einem geeigneten Grundaufbau – eine VS-NfD-konforme IT-Infrastruktur, die flexibel mit dem Erfolg des Unternehmens skaliert. Sie bildet das Fundament für einen sicheren Umgang mit vertraulichen Dokumenten – auch in modernen, zunehmend mobilen Arbeitswelten. ■

Weitere Informationen unter genua.de/geheimschutz-mobil

