

# PCI-KONFORMITÄT **Checkliste**

Sind Sie nicht sicher, ob Ihre Fernsteuerungslösung den Sicherheitsanforderungen entspricht? Hier erfahren Sie, wie Netop Ihnen dabei hilft, selbst die strengsten Standards einzuhalten.

## PCI-SICHERHEITSANFORDERUNGEN

- Einsatz starker Kryptographie- und Sicherheitsprotokolle wie Secure Socket Layer (SSL) / Transport Layer Security (TLS) und Internet Protocol Security (IPSEC), um vertrauliche Karteninhaberdaten bei der Übertragung über offene, öffentliche Netze zu schützen. [ 4.1 ]
  
- Zuweisung einer eindeutigen ID an alle Anwender, bevor ihnen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gewährt wird. [ 8.1 ]
  
- Neben der Zuweisung einer eindeutigen ID sollte mindestens eine der folgenden Methoden zur Authentifizierung aller Anwender eingesetzt werden:
  - Passwort oder Passphrase
  - Zwei-Faktor-Authentifizierung (beispielsweise Tokens, Smartcards, biometrische Daten oder öffentliche Schlüssel) [ 8.2 ]
  
- Einbeziehung von Zwei-Faktor-Authentifizierung für den Fernzugriff (Zugriff auf Netzwerkebene mit Ursprung außerhalb des Netzwerks) auf das Netzwerk durch Mitarbeiter, Administratoren und Dritte. Einsatz von Technologien wie Fernauthentifizierung und Dial-In-Service (RADIUS), Terminal Access Controller Access Control System (TACACS) mit Tokens oder VPN (basierend auf SSL/TLS oder IPSEC) mit individuellen Zertifikaten. [ 8.3 ]
  
- Unlesbarkeit aller Passwörter während der Übertragung sowie Speicherung in allen Systemkomponenten anhand starker Verschlüsselung (im PCI DSS-Glossar für Begriffe, Abkürzungen und Akronyme definiert). [ 8.4 ]

## WIE NETOP REMOTE CONTROL IHNEN GERECHT WIRD

### Branchenführende Verschlüsselung

#### Verschlüsselung

Daten, die zwischen Netop Modulen unter Windows, Linux, Solaris und Mac OS X übertragen werden, können anhand des Advanced Encryption Standard (AES) mit Schlüssellängen von bis zu 256 Bit verschlüsselt werden. Dafür stehen 7 verschiedene Verschlüsselungsebenen zur Verfügung, unter anderem eine mit Netop 6.x/5.x kompatible Ebene für die Kommunikation mit älteren Netop Modulen.

#### Datenintegrität und Nachrichtenaufentifizierung

Gewährleistet durch Verwendung von Keyed-Hash Message Authentication Code (HMAC) auf Basis der sicheren Hash-Algorithmen SHA-1 (160 Bit) oder SHA-256 (256 Bit).

#### Schlüsselaustausch

Der Austausch von Schlüsseln für verschlüsselte Datenübertragung erfolgt anhand der Diffie-Hellman-Methode mit Schlüssellängen von bis zu 2048 Bit und bis zu 256-Bit-AES oder bis zu 512-Bit-SHA-HMAC-Authentifizierung.

### Zentralisierte 2- und 3-Faktor-Authentifizierung

#### Netop Authentifizierung über den Security Server

Der Netop Security Server prüft die Identität des Guest gegen den Datenbankdienst, in dem alle vordefinierten Benutzernamen und Passwörter für Guests gespeichert sind.

#### Windows Authentifizierung über den Security Server

Der Netop Security Server prüft die Identität des Guest, indem er den Authentifizierungsprozess über den Host an einen Windows Domain Controller weiterleitet.

#### Authentifizierung gegen den Verzeichnisdienst über den Security Server

Der Netop Security Server prüft die Identität des Guest über LDAP gegen einen Verzeichnisdienst.

#### RSA SecurID mit „Drei-Faktor-Authentifizierung“ über den Security Server

Der Netop Security Server kombiniert RSA SecurID „Zwei-Faktor-Authentifizierung“ mit einer Netop Authentifizierung per Benutzernamen und Passwort, die im Hintergrund durchgeführt wird.

- ✓ **Beschränkung des Zugriffs auf Computing-Ressourcen und Karteninhaberdaten auf diejenigen Personen, die ihn tatsächlich benötigen.** [ 7.1 ]
  
- ✓ **Beschränkung der Zugriffsrechte auf autorisierte Anwender-IDs und auf die Berechtigungen, die zur Ausführung der jeweiligen Aufgaben nötig sind.** [ 7.1.1 ]
  
- ✓ **Die Zuweisung von Rechten basiert auf der Tätigkeit und Funktion der einzelnen Mitarbeiter.** [ 7.1.2 ]
  
- ✓ **Einführung eines Zugriffskontrollsystems für Systemkomponenten mit mehreren Benutzern, das den Zugriff auf Basis des konkreten Bedarfs der einzelnen Benutzer einschränkt und sämtliche Zugriffe verweigert, falls keine spezifische Genehmigung festgelegt ist.** [ 7.2 ]
  
- ✓ **Sicherstellen, dass für alle Systemkomponenten und Systemsoftware die aktuellen Sicherheits-Updates des Herstellers installiert werden. Installation kritischer Updates innerhalb eines Monats nach deren Veröffentlichung.** [ 6.1 ]
  
- ✓ **Implementierung automatisierter Audit-Trails für alle Systemkomponenten.** [ 10.2 ]
  
- ✓ **Sichere Audit-Trails, die nicht abgeändert werden können.** [ 10.5 ]
  
- ✓ **Schutz vor unbefugten Änderungen an Audit-Trails.** [ 10.6 ]

## Smartcard-Authentifizierung und -Tunneling

Durch Verwendung einer Smartcard und eines Lesegeräts am Windows Guest kann der Windows Host nun die Identität des Guest-Benutzers über den Security Server authentifizieren, welcher mit einem Windows Server kommuniziert, auf dem Microsoft CA installiert ist. Falls der Host-Computer eine lokale Anmeldung über Smartcard erfordert, werden die Zugangsdaten des Guest an den Host getunnelt.

## Netop Sicherheitsrolle

- Eine Sicherheitsrolle ist eine Reihe erlaubter Aktionen.
- Der Administrator kann neben den vordefinierten Sicherheitsrollen „Voller Zugriff“, „Nur Ansicht“ und „Verweigern“ auch individuelle Rollen erstellen.
- Jeder Sicherheitsrolle können eine oder mehrere Gruppen und beliebig viele Benutzerkonten zugewiesen werden.
- Die erlaubten Aktionen ergeben sich aus der Gesamtmenge sämtlicher Sicherheitsrollen, denen ein Benutzer zugewiesen ist.
- Zugriffsbestätigung ist erforderlich, wenn dies in mindestens einer Sicherheitsrolle festgelegt ist.

## Web-Updates

Netop Komponenten können für die Planung und Installation automatischer Updates konfiguriert werden. Dies garantiert, dass aktuelle Software-Updates über sichere und vertrauenswürdige Kanäle und unter Verwendung anbieterspezifischer Zertifikate mit digitaler Signatur zur Verfügung gestellt werden. Updates können direkt über von Netop gehostete Dienste vorgenommen oder anhand Ihrer eigenen internen Webserver verteilt und kontrolliert werden.

## Netop Protokollierung

Netop kann sämtliche Fernsitzungen vollständig aufzeichnen und ermöglicht so eine lückenlose Dokumentierung. Netop Security Server erstellt ein zentrales Protokoll mit über 100 Ereignistypen und speichert diese Informationen in einer ODBC-konformen Datenbank, um für maximale Sicherheit und Skalierbarkeit zu sorgen. Protokoll Daten können, zusammen mit der physikalischen Support-Sitzung, über einen unbegrenzten Zeitraum aufbewahrt werden, so dass Ihnen umfassende Audit- und Wiedergabemöglichkeiten zur Verfügung stehen.

Bildschirmaufzeichnungen werden in einem Format gespeichert, das mit Video-Editoren nicht bearbeitet werden kann.



RSA-ZERTIFIZIERT



[www.netop.com/sicherheit](http://www.netop.com/sicherheit)