Net2 - Empfehlungen zur Netzwerksicherheit

Übersicht

Damit Ihr Paxton Net2-System an Ihrem Standort so sicher wie möglich ist, empfiehlt Paxton, dass der Installateur (oder die IT-Abteilung) die besten IT-Sicherheitsmechanismen auf jeder der 7 Schichten des OSI-Modells (Network Open Systems Interconnection) implementiert.

Implementierung starker physischer Sicherheit

Einführung starker physischer Sicherheitsvorkehrungen auf dem Firmengelände, z. B. durch den Einsatz von Biometrie, Transponder-basierter Authentifizierung usw., so dass ein Außenstehender gestoppt werden kann, bevor er/sie in ein Gebäude mit einem Unternehmensnetzwerk eindringen kann.

Implementierung von Netzwerkzugangskontrollstandards wie IEEE 802.1X-Authentifizierung zur Sicherung von LAN und WLAN

Dieser Standard setzt Sicherheitsrichtlinien durch, indem er nur sicherheitsrichtlinienkonformen Geräten Zugang zu Netzwerkressourcen gewährt, wenn diese Geräte an einen physischen LAN-Port angeschlossen oder mit einer WLAN-SSID verbunden sind. Dieser Standard übernimmt nicht nur die Funktionen der Zugriffsauthentifizierung und -autorisierung, sondern kontrolliert sogar die Daten, auf die diese spezifischen Benutzer zugreifen, indem er die Benutzer, ihre Geräte und ihre Netzwerkrollen erkennt. IEE 802.1X wird von allen Windows-, Mac- und Linux-Rechnern nativ unterstützt.

Implementierung von Firewalls der nächsten Generation zum Schutz vor externen und internen Angriffen

Implementierung einer Firewall der nächsten Generation, die neben der herkömmlichen paketbasierten Zustandsorientierte Prüfung auch Prüfung der Anwendungsschicht, Verhinderung und Erkennung von Eindringlingen, Sicherung des Webverkehrs usw. durchführt.

Darüber hinaus sollten alle potenziell unsicheren internen Layer-2-VLANs auf die Firewall ausgedehnt und der Zugang von diesen VLANs zu anderen vertrauenswürdigen/sicheren VLANs durch konfigurierbare Sicherheitsrichtlinien geschützt werden.

Implementierung von VLANs (Virtual Local Area Networks) für Netzsicherheit und -trennung

VLANs ermöglichen es uns, Datenpakete aus verschiedenen Netzwerken (wie Abteilungsnetzwerke, kritische Servernetzwerke usw.) getrennt zu halten. Die Netzwerksegmentierung mit VLANs schafft eine Sammlung von isolierten Netzwerken innerhalb eines Unternehmensnetzwerks und reduziert die Angriffsflächen, denn selbst wenn ein Außenstehender Zugang zu einem kleinen logischen Netzwerk erhält, kann er/sie keine Geräte in anderen VLANs sehen oder direkt angreifen.

Implementieren Sie sichere Passwörter für die Net2 Server-Anwendungsauthentifizierung und die zugehörigen Datenbanken. Einzelheiten dazu finden Sie im Anwendungshinweis APN-1162.

Einen eigenen Rechner für Net2 Server haben

Der Net2 Server sollte auf einem eigenen Rechner laufen, auf dem außer den Netzwerküberwachungsprogrammen keine weitere Software installiert wird.

Der physische Net2-Server sollte nur für autorisiertes Personal zugänglich sein.

Maschinensicherheit

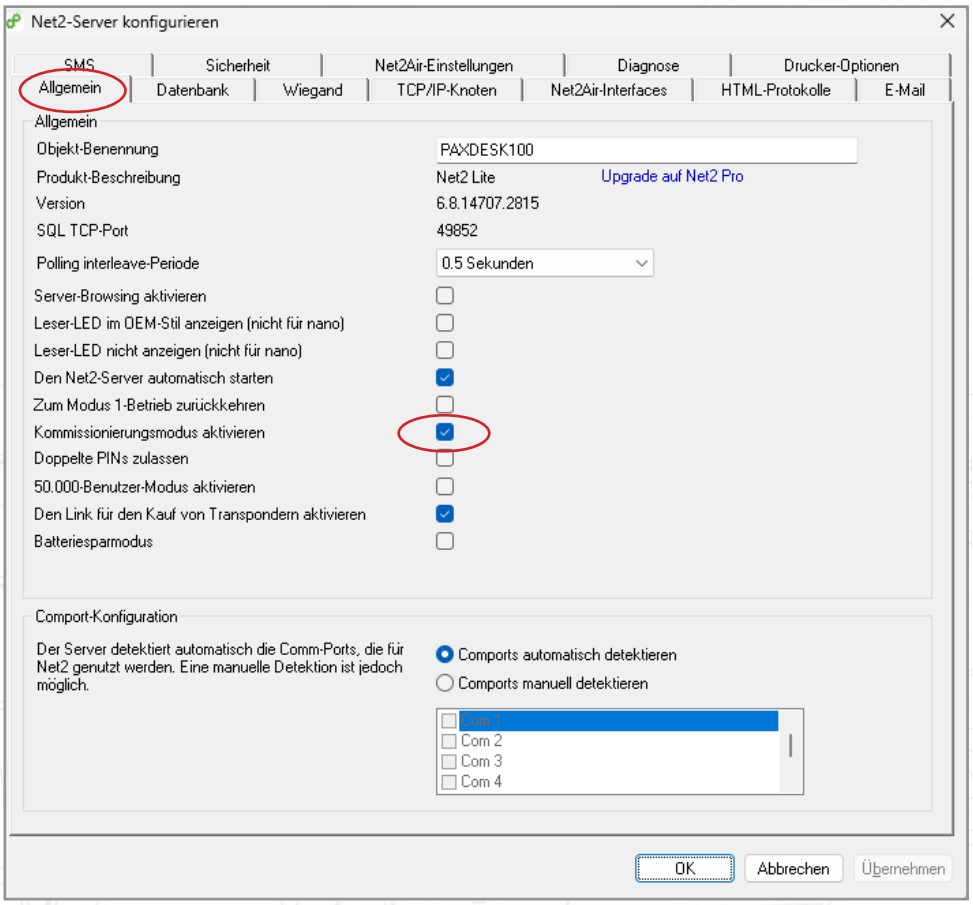
Halten Sie Server- und Client-Rechner mit den neuesten kritischen Betriebssystem-Updates auf dem neuesten Stand und sorgen Sie für einen Virenschutz auf den Client-Rechnern.

Net2-Clients sollten auf Rechnern ohne E-Mail-/Chat-Clients installiert werden, um die unbeabsichtigte Ausführung von bösartigem Code über Anhänge zu vermeiden.

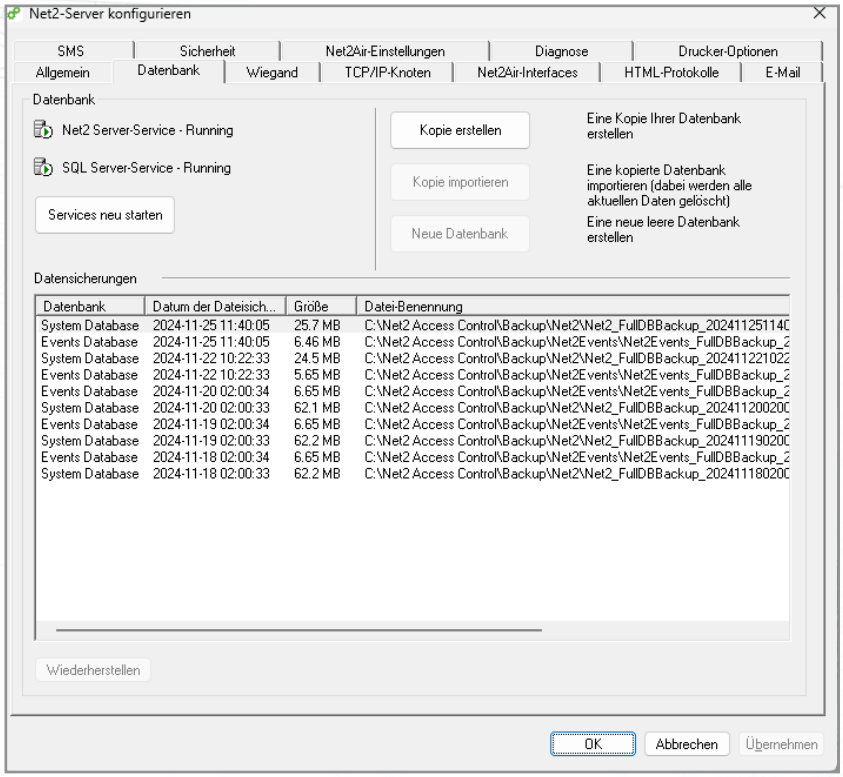
Kommissionierungsmodus

Sobald Sie Ihr System in Betrieb genommen haben, können Sie es sperren, indem Sie im Reiter **„Allgemein“** der Net2 Configuration Utility das Häkchen beim Kästchen **„Kommissionierungsmodus aktivieren“** entfernen.

Hinweis:
Bei deaktiviertem Kommissionierungsmodus ist es nicht mehr möglich, ACUs hinzuzufügen oder zu löschen. Außerdem werden sie an diesen Server gebunden.

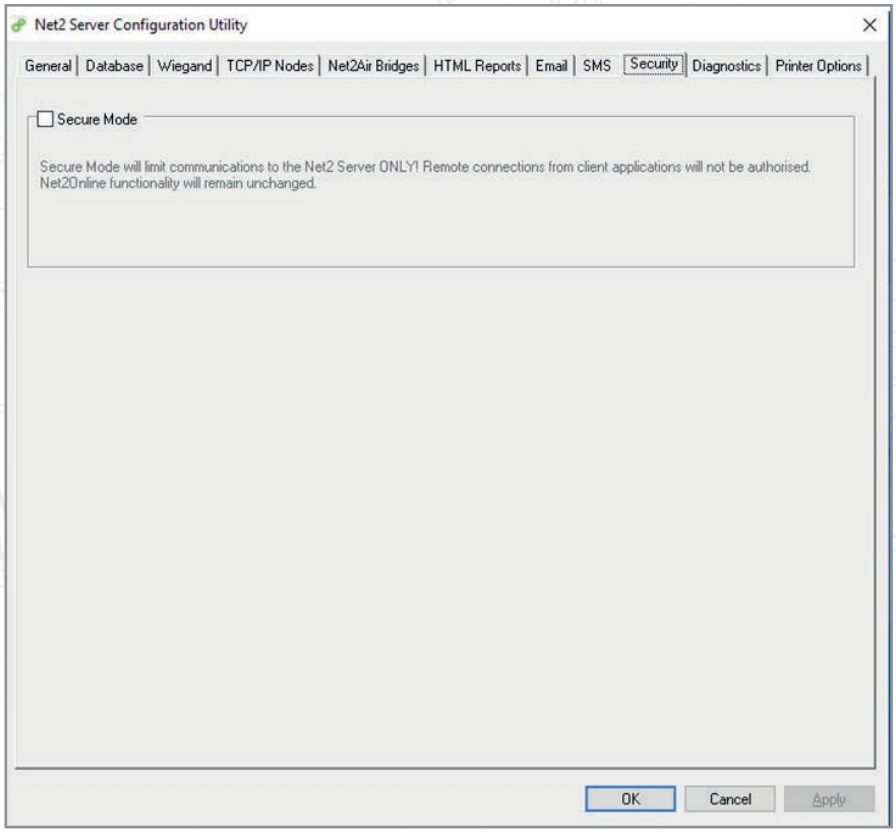


Bei deaktiviertem Kommissionierungsmodus werden die Optionen auf dem Reiter **„Datenbank“** in der Net2 Configuration Utility ebenfalls ausgegraut.



Net2 sicherer Modus

Für maximale Sicherheit sollten Sie die Server- und die Client-Software auf demselben Rechner ausführen und den TCP-SQL-Server-Port 1433 für eingehende Verbindungen blockieren. Dies kann durch Aktivierung des **„Sicheren Modus“** auf der Registerkarte „Net2-Sicherheit“ erreicht werden.



Alternativ können Sie für die volle Nutzung aller Client-Funktionen eine virtualisierte Anwendungssoftware wie VMware horizon verwenden, um eingeschränkte Net2-Client-Anwendungen zu verteilen, die mit einem Net2-Server in einem separaten LAN oder VLAN verbunden sind.

Um Transponder zu registrieren, verwenden Sie einfach einen vorhandenen Leser oder einen Leser, der mit einem drahtlosen Net2 Nano verbunden ist, falls eine Netzwerkverkabelung nicht möglich ist. Diese Lösung ermöglicht es auch, SDK- (Software Development Kit) und Videoanwendungen auf dem virtualisierten Desktop zu isolieren und einfach zu implementieren und im Rechenzentrum vollständig zu verwalten.

Was ist VMware Horizon? | VDI-Software | VMware | UK

Hinweis: VMware Horizon verfügt über USB-Passthrough, aber die Leistung hängt von der Netzwerkgeschwindigkeit ab und muss getestet werden. Dies könnte die Verwendung von Standard-Desktop-Lesern und Webcams ermöglichen.

Zusätzliche Sicherheitsvorkehrungen

1. Implementierung von MAC-Adressfilterung auf dem Switch

Implementieren Sie die MAC-Adressfilterung auf dem Entry-Port. Wenn ein unerkanntes Gerät eine Verbindung zu einem Port herstellt, wird der Port deaktiviert und eine Warnung gesendet.

2. Isolierung von VLAN

Kombinieren Sie alle Paxton-Geräte mit IP-Fähigkeit in ein eigenes VLAN. Isolieren Sie dieses VLAN vom Firmennetzwerk, um den Zugriff auf andere Bereiche als die Zugangskontrollgeräte zu beschränken.