

Informationen zum VPN-Zugang mit Einzelplatz-PC und für "kleine" Netze

Um den unproblematischen Zugang möglichst vieler Einrichtungen an das Intranet der EKHN voranzutreiben, waren noch einige Test, Veränderungen und Entwicklungen notwendig. Nachfolgend sind die Ergebnisse und Absprachen sowie Terminvorgaben systematisch aufgezeigt:

1. Einzelplatzlösung

Die Sicherheits-Programme auf der Intranet-CD sind auf allen Windows-Betriebssystemen lauffähig. Die Probleme, die aufgetreten sind, hatten vielfältige Ursachen, waren aber zumeist in den nach Deinstallation nicht automatisch gelöschten Eintragungen in der Systemregistrierungsdatenbank begründet. Dieses Problem kann mit dem Programm TuneUp (www.tuneup.de) behoben werden, welches 30 Tage kostenlos als Vollprodukt getestet werden kann.

Bei dem VPN-Client waren wir bisher an die Software von CheckPoint gebunden, da nur diese direkt mit der Firewall, die das Intranet schützt, kommunizieren kann. Mit dem Betriebssystem Windows XP waren Probleme in Verbindung mit der Personal-Firewall aufgetreten, die eine gleichzeitige Aktivität beider Programme nicht zuließ. Dieses Problem haben auch andere VPN-Clients und konnte noch nicht abschließend gelöst werden. Zur Zeit muss also noch bei einer Verbindung zum Intranet die Firewall deaktiviert werden.

Auf Grund der Konsolidierung unseres Netzwerkes und der Umstellung auf Linux bieten sich jetzt ganz neue Möglichkeiten. Mit der Firma NorCom, die auch die Netzwerkmstellung in der Kirchenverwaltung konzipiert und umgesetzt hat, wurden folgende Lösungen erarbeitet:

Betriebssystem	VPN-Client	Medium
Windows 95/98/ME	CheckPoint	auf Intranet CD
Windows 2000/XP	Windows-VPN-Client	wird bereitgestellt

Die Windows-VPN-Clients werden vorkonfiguriert in ein Installationsprogramm eingebunden, welches bis auf wenige vom Nutzer einzugebende Angaben, automatisch abläuft. Nach umfangreichen Vortests bei NorCom und in der Kirchenverwaltung, wird die Installation auch mit einigen Dekanatsbeauftragten getestet.

Mittelfristig wird die Anbindung ans Intranet mit dem Windows-VPN-Client favorisiert. Dies hat insbesondere seine Begründung in der vereinfachten Einbindung und Anbindung an Outlook, aber vor allem in der Wirtschaftlichkeit.

2. Lösung für "kleine" Netzwerke

In den Kirchengemeinden, den Dekanaten, Propsteien und anderen Einrichtungen sind die unterschiedlichsten Netzwerklösungen mit verschiedenartigen Topologien eingesetzt. Das Ziel unserer Überlegungen bezüglich der VPN-Anbindung und der Absicherung der "kleinen Netze" war es, eine wirtschaftliche Lösung herbeizuführen, die ein hohes Maß an Sicherheit bietet, leicht zu administrieren ist und unter Berücksichtigung den verschiedensten Netztopologien und der eingesetzten Hard- und Software gerecht wird. Dies ist uns in Verbindung mit der Firma NorCom, Frankfurt, gelungen.

Um auf die neue Infrastruktur der EKHN zugreifen zu können, ist ein abgesicherter Zugang erforderlich. Da die Daten über das unsichere Internet übertragen werden, müssen sie verschlüsselt und authentisiert werden. Hier-zu soll in den Außenstellen ein Server, das sogenannte dezentrale VPN-Gateway, installiert werden.

Durch die Umleitung des Internetverkehrs über die zentrale Firewall wird auch für die eingebundenen "kleinen Netze" eine deutliche Erhöhung des Sicherheitsstandards erreicht. Das heißt, vor das "kleine"

Netzwerk wird ein PC gestellt, der als VPN-Gateway fungiert. Das dezentrale Gateway kann entweder auf der von der Firma Nor-Com vorgeschlagenen Hardware umgesetzt oder auf einem von der Einrichtung gestellten Rechner implementiert werden.

Sollten Sie einen vorhandenen Personalcomputer stellen, beachten Sie bitte die folgenden Mindestanforderungen:

- PC ab Intel Pentium II Prozessor und 2 PCI-Slots
- CD-ROM und Floppy Laufwerk
- 128 MB Ram
- 1 x 10/100 Base-T Ethernet Netzwerkkarten
- Je nach Internetanbindung entweder zweite 10/100 Base-T Ethernet Netzwerkkarte oder ISDN-Karte (Linux-fähig)

Folgende Kosten fallen für die Umsetzung dieser sicheren Netzwerklösung an:

- a) Gateway (Hard- und Software) durch WL: 493,00
- b) Installation des Gateway, Anbindung an das Intranet, Kurzeinweisung pauschal: 900,00

Die Preise sind Bruttopreise und beinhalten bereits die Mehrwertsteuer.

Falls die Einrichtungen mit "kleinen" Netzwerken also über einen PC mit vorgenannter Konfiguration verfügen, kann dieser als Gateway genutzt werden. Dann entfallen die Kosten hierfür und es fallen "nur" die Kosten für die Einrichtung und Anbindung in Höhe von 900,00 Brutto je Netzwerk an.

Ein Monitor zur Einrichtung des Gateway vor Ort sollte von der Einrichtung gestellt werden !!!

Die Kosten sind vom Halter des Netzwerkes, also von der Kirchengemeinde, der Diakoniestation, dem Dekanat usw., zu tragen.

Förderung

Die Kirchengemeinden und Dekanate können jeweils eine Förderung beantragen. Die Förderhöhe ist abhängig davon, ob das Gateway und die Installation (Zuschuß 1.100,-) oder die Installation auf einem vorhandenen Rechner vorgenommen wird (Zuschuß 800,-)

Achtung: Der Antragszeitraum ist bis zum 31.12.2003 beschränkt.

Antragsformular und Fragebogen

Den ausgefüllten Fragebogen und den Zuschußantrag senden Sie bitte an die Kirchenverwaltung

Umsetzung VPN-Lösung "kleine" Netze

- **NorCom / WL Netze und Systeme**
Die Firma NorCom erhält die Bestellung von der Kirchenverwaltung und den ausgefülltem Fragebogen und gibt die Bestellung der Hardware an WL weiter. Die Hardware wird von WL an NorCom geliefert.
Diese bereitet den PC vor und bindet diesen nach Terminabsprache entsprechend der Leistungsbeschreibung (siehe Anlage) in das Netzwerk ein. Ein bereits vorhandener PC für das Gateway wird von der Firma NorCom vor Ort für seine künftige Funktion vorbereitet.
Die Firma WL Netze und Systeme, als Lieferant der Gateway-PC, bietet neben einer guten Ausstattung des PC (Miditytower, Intel Celeron 1,8 GHZ, 128 MB-RAM, CD- und Floppy-Laufwerk, Netzwerkkarte, Festplatte 20 GB) auch eine 3 Jahre Vor-Ort-Garantie. Der Vertrag

kommt bei der Bestellung der Netzwerklösung bei der Firma NorCom direkt zwischen dem Besteller und der Firma WL zustande. Die Rechnung für die Hardware erhält der Besteller direkt von WL.

- **Terminierung der Installation und Implementierung**

In Absprache NorCom und Netzbetreiber wird ein Termin vereinbart, wann die Umsetzung erfolgen soll. Bei der Installation der Hard- und Software des Gateways sollte der zuständige Netzbetreiber zugegen sein.

Über die installierte Hard- und Software erhält der Netzbetreiber eine detaillierte Beschreibung, so dass sich ein autorisierter Dritter innerhalb kürzester Zeit ein Bild von der Konfiguration und dem Softwarestand machen kann.

Entscheidungshilfe für Netzbetreiber:

Die nachfolgende Matrix soll als Entscheidungshilfe für die Netzbetreiber dienen:

	Einplatz-VPN	Server Lösung der Firma Norcom
Einplatzversion	X	
PC's verkabelt, ohne Server	X1	X2
Netzwerk mit Server		X

X1 Sollte ein Einzel-PC mit dem VPN-Client ausgestattet werden, kann entweder nur dieser PC mit einem Intranet-Client ausgestattet werden, oder der PC auf dem der VPN-Client installiert wird, ist nicht an das Netz angeschlossen.

Vorteil:

- Keine Kosten

Nachteil:

- Nur immer ein PC kommt in das Internet/Intranet, nicht wie vorher evtl. noch möglich von allen Rechnern.

X2 Der angeschlossene PC übernimmt die Aufgabe des VPN-Clients

Vorteil:

- Alle User (bis 250) haben die Möglichkeit gleichzeitig im Internet/Intranet zu arbeiten
- Höhere Sicherheit und Geschwindigkeit
- Remote-/Fernwartung ist möglich
- Zentrale Updatemöglichkeit für das Gateway bezogen auf Betriebssystem und Applikationen
- automatischer Update der Gateway-Firewall
- Zentrale Installation und Aktivierung neuer Dienste (Proxy, Nat etc.) durch die Netzwerker der Kirchenverwaltung möglich

Nachteil:

- Höhere Kosten durch Gateway und Dienstleistung durch die Firma NorCom
- Bei ISDN oder DSL-Zeittarif kann die Verbindung nicht so komfortabel und einfach getrennt werden, wie bei einem Einzelplatzrechner.

Empfehlungen:

Für ein bestehendes Netzwerk empfehlen wir grundsätzlich die Gateway-Lösung, da nur diese zukunftssicher ist, die unabdingbar notwendige Netzsicherheit bietet, dem Netzbetreiber alle Möglichkeiten gibt, die Administration der Zugänge ans Intranet/Intranet im Netzwerk zu steuern und für zukünftige kirchliche Anwendungen (zum Beispiel NetKim im Jahre 2003) die vom Rechenzentrum geforderte Verbindungssicherheit bietet.

Eine DSL-Flatrate wird für "kleine" Netzwerke aus Kostengründen dringend empfohlen. Jede andere Lösung beinhaltet sehr große Kostenrisiken.