Whitepaper

Sicherheitskonzept NotarnetzPlus

Bundesnotarkammer und NotarNet GmbH, Köln

Stand: 24.02.2023 Veröffentlicht

Inhalt

1 Einleitung / Übersicht

Das NotarnetzPlus-Produktportfolio ist ein abgerundetes Sicherheitskonzept, welches neben der Internetanbindung und Absicherung (Firewall) des Büronetzwerkes auch eine sichere Standortvernetzung zu weiteren Geschäftsstellen und Heimarbeitsplätzen, externe Zugriffe über Notarnetz-Mobilzugänge sowie VPN-Zugängen ermöglicht. Weiterhin gehört ein sicheres Domain- und E-Mail-Hosting zum Sicherheitskonzept, bei dem die E-Maildienste nur aus dem Notarnetz erreichbar sind.

2 Notarnetzbox – Zugangspunkt zum Notarnetz

Das **Notarnetz** ist ein geschlossene Wide Area Network („WAN“) für Notare und bestimmte angeschlossene Institutionen, welches die Bundesnotarkammer K.d.ö.R. (BNotK) im Rahmen eines Nutzungsverhältnisses ohne gesonderte Vergütung bereitstellt (Nutzungsbedingungen Notarnetz). Der Amtsträger ist verpflichtet, die jeweils aktuellen Bestimmungen der „Sicherheitsrichtlinien Notarnetz“ („Sicherheitsrichtlinien“) zu beachten; diese sind nachrangige Bestandteile dieser Nutzungsbedingungen. Das Notarnetz ist wiederum Grundlage für die **NotarnetzPlus-Produkte** der NotarNet GmbH, worüber das o. g. NotarnetzPlus-Produktportfolio als abgerundetes Sicherheitskonzept angeboten wird. Gegenstand des Nutzungsverhältnisses des Notarnetzes ist die Überlassung und Wartung für ein von der BNotK bereitgestelltes **Netzanschlussgerät** für das Büronetzwerk – die **Notarnetzbox**.

Die Notarnetzbox benötigt für die Verbindung zum Notarnetz eine Internetanbindung, die entweder über eine von der NotarNet GmbH bereitgestellten **NotarnetzPlus-Direktleitung** oder über einen **Fremd-Anschluss** hergestellt wird. Im ersten Fall baut die Notarnetzbox mit dem integrierten Modem eine Verbindung zum Notarnetz auf. Für den Fremd-Anschluss muss ein Internetrouter der Notarnetzbox vorgeschalten werden, welcher die Interneteinwahl übernimmt und somit der Notarnetzbox ein Netzwerk für den Verbindungsaufbau zum Notarnetz bereitstellt.

Die Notarnetzbox basiert in der Standard-Auslieferung auf ein **Cisco-Router 886 VA** Gerät mit einem maximalen Leitungsdurchsatz von 100 Mbit/s auf dem Internetanschluss. Für komplexere Notarnetz-Anschlüsse und -Vernetzungen setzt die NotarNet GmbH auf ein performanteres Router-Modell **Cisco-Router 926-4P** mit einem maximalen Leitungsdurchsatz von 400 Mbit/s auf dem Internetanschluss sowie Gigabit-LAN-Anschlüssen.

Entscheidungskriterien für das jeweilige Notarnetzbox-Modell sind folgende Punkte:

- **Bandbreite Internetanschluss** - unabhängig von NotarnetzPlus-Direktleitung oder Fremd-Anschluss soll die größtmögliche Bandbreite zur Verfügung stehen.
- **Anzahl von VPN-Zugängen und Bereitstellung verschiedener Betriebssystem-Versionen der VPN-Clients** (Microsoft Windows, Apple macOS, Linux)
- **Kombination mehrerer Notarnetzanschlüsse über Notarnetzboxen und VPN-Zugängen** – werden mehrere Notarnetzboxen durch Site-2-Site VPN miteinander vernetzt und kommen zusätzlich noch VPN-Zugänge hinzu, wird die zentrale Notarnetzbox im Büro stark beansprucht. Daher kann hier ein performanteres Notarnetzbox-Modell sinnvoll sein.

3 Internetanbindung

Für den Betrieb der Notarnetzbox und damit des Notarnetz-Zugangs ist eine beliebige Internet-anbindung am Standort notwendig. Die Notarnetzbox kann sowohl an einer eigens vorgesehenen NotarnetzPlus-Direktleitung angeschlossen werden oder an einem Fremd-Anschluss. Für beide Varianten ist die Notarnetzbox bei Auslieferung entsprechend vorkonfiguriert, sodass auch ein Leitungswechsel vor Ort z. B. im Backup-Fall ohne weiteren Zugriff des Notarnetz-Rechenzentrums erfolgen kann.

3.1 NotarnetzPlus-Direktleitung

Für eine höhere und sicherere Verfügbarkeit der Internetanbindung im Büro kann eine **NotarnetzPlus-Direktleitung** zum direkten Anschluss der Notarnetzbox genutzt werden. Diese Direktleitung umfasst die Internetanbindung von der TAE-Anschlussdose (TAE Telekommunikations-Anschluss-Einheit) bei DSL-Leitungen oder von der Gf-TA-Dose (Glasfaser-Teilnehmeranschlussdose) bei FTTH/Glasfaser-Leitungen in den Büroräumen über die Infrastruktur des Leitungsträgers bis zum Zugangspunkt im Notarnetz-Rechenzentrum und dient als reine Datenleitung für die Anbindung an das Notarnetz. Der Leitungsträger ist hier die Telekom Deutschland GmbH, sodass im Büro für die Nutzung der NotarnetzPlus-Direktleitung eine entsprechende Verfügbarkeit der Leitungsinfrastruktur bestehen muss.

Die **Bereitstellung** der NotarnetzPlus-Direktleitung erfolgt durch einen Vorort-Einsatz eines Technikers vom Technischen Service der Telekom Deutschland GmbH im Auftrag der rockenstein AG (technischer Dienstleister der NotarNet GmbH). Der Techniker schaltet die Endleitung frei und setzt die erste TAE-Anschlussdose oder Gf-TA-Dose an die in der Bestellung angegebene Stelle (z. B. im Serverraum). Die Bereitstellung und Überlassung der NotarnetzPlus-Direktleitung setzt eine geeignete Teilnehmeranschlussleitung mit schaltbarer Endleitung zwischen Hausanschluss-Kasten (APL = Abschlusspunkt Linientechnik) und TAE-Anschlussdose bzw. Gf-TA-Dose voraus. Eventuelle Inhouse-Verkabelungen von der Netzabschluss-Dose zu einem anderen Büroraum sind nicht Bestandteil des Leistungsumfangs der NotarnetzPlus-Direktleitung.

Als **Leitungsarten für den Internetzugang** stehen je nach Anschlussverfügbarkeit die **FTTH**-Technik (Glasfaser „Fibre to the home“) mit Geschwindigkeiten bis zu 1.000 Mbit/s im Downstream, die **VDSL**-Technik (Very High Speed Digital Subscriber Line) mit Vectoring- und Supervectoring-Anschlüssen und Geschwindigkeiten bis zu 250 Mbit/s im Downstream sowie die **ADSL**-Technik (Asymmetric Digital Subscriber Line) mit Geschwindigkeiten bis zu 16 Mbit/s im Downstream zur Verfügung. Die **technische Verfügbarkeit** der NotarnetzPlus-Direktleitung beträgt **97,0 %** im Jahresdurchschnitt.

Der **Telefonanschluss** (SIP-Trunk) muss über eine separate DSL-Leitung des Telefonie-Providers betrieben werden. Die Telefonanlage wird an dem parallel zur NotarnetzPlus-Direktleitung bestehenden Telefonie-DSL-Anschluss angeschlossen. Der an diesem Anschluss befindliche Internetrouter stellt das Gateway ins Internet für die Telefonanlage dar.

Störungen der NotarnetzPlus-Direktleitung werden unverzüglich bearbeitet und im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten vom Leitungsträger beseitigt. Die Störungsannahme ist Werktags Mo – Fr von 9.00 bis 18.00 Uhr unter der gebührenfreien Support-Hotline 0800 3 550 222 sowie der E-Mail-Adresse support@rockenstein.de möglich.

Der **Anschluss** der NotarnetzPlus-Direktleitung an der Notarnetzbox erfolgt über das **integrierte Modem** und dem vorgesehenen Modem-Port. Das Büronetzwerk wird dahinter am LAN-Port der Notarnetzbox angeschlossen, wodurch die **Notarnetzbox das zentrale und einzige Gateway zum Internet** darstellt und damit den **Notarnetz-Perimeterschutz** gewährleistet.

3.2 Fremd-Anschluss

Bei einem Fremd-Anschluss jeglicher Art wird die Internetverbindung zuerst vom Provider zur Verfügung gestellten Internetrouter aufgebaut. Die Notarnetzbox wird nachgelagert mit dem Internetrouter über die LAN-Ports verbunden und bezieht darüber per **DHCP eine LAN-IP-Konfiguration**. Danach baut die Notarnetzbox einen **L2TP-VPN**-Tunnel über **UDP-Port 1701** in das Notarnetz-Rechenzentrum auf. Der Internetrouter darf dabei das L2TP-Protokoll nicht blockieren oder stören. Unter Umständen muss in den Einstellungen des Internetrouters ein **Port-Forwarding für Port UDP 1701** zur IP-Adresse der Notarnetzbox eingerichtet werden, damit der L2TP-VPN konstant und stabil aufgebaut werden kann. Das Büronetzwerk wird dahinter am LAN-Port der Notarnetzbox angeschlossen, wodurch die **Notarnetzbox das zentrale und einzige Gateway zum Internet** darstellt und damit den **Notarnetz-Perimeterschutz** gewährleistet.

3.3 Port-Belegungen der Notarnetzbox

Die Notarnetzbox besitzt vorkonfigurierte Port-Belegungen für die jeweiligen Anschluss-Varianten, die sich je nach Geräte-/Router-Modell unterscheiden.

Der **Cisco-Router 886 VA** besitzt folgende Port-Belegungen:

- VDSL/ADSL (RJ11) ist das DSL-Modem und dient dem Anschluss an einer NotarnetzPlus-Direktleitung
- LAN-Port FE0 und FE1 (RJ45, Fast Ethernet) dienen zur Verbindung des internen Büronetzwerkes (LAN) mit der Notarnetzbox
- LAN-Port FE2 (RJ45, Fast Ethernet) dient dem Anschluss der Notarnetzbox an einem vorgeschalteten Internetrouter bei einem Fremd-Anschluss
- LAN-Port FE3 (RJ45, Fast Ethernet) wird nicht genutzt (dient einer Sonderkonfiguration des Notarnetz-Rechenzentrums)

Der **Cisco-Router 926-4P** besitzt folgende Port-Belegungen:

- Modem-Port (RJ11) ist das DSL-Modem und dient dem Anschluss an einer NotarnetzPlus-Direktleitung
- LAN-Port GE0, GE1 und GE2 (RJ45, Gigabit) dienen zur Verbindung des internen Büronetzwerkes (LAN) mit der Notarnetzbox
- LAN-Port GE3 (RJ45, Gigabit) wird nicht genutzt (dient einer Sonderkonfiguration des Notarnetz-Rechenzentrums)
- LAN-Port GE4 (RJ45, Gigabit) dient dem Anschluss der Notarnetzbox an ein Modem oder einem vorgeschalteten Internetrouter bei einem Fremd-Anschluss

4 Firewall und Netzwerksegmentierung

Mit dem Einsatz des NotarnetzPlus-Anschlusses und der **Notarnetzbox** als **zentrales Gateway im lokalen Netzwerk** besteht eine Absicherung gegenüber dem Internet. Diese Absicherung erfolgt durch einen **mehrschichtigen Perimeterschutz**, bestehend

- aus der Notarnetzbox vor Ort mit einer **Netzwerksegmentierung** des Büro-LAN gegenüber dem LAN/WAN des Internets und sonstigen Anwendungen (IoT, TK-Anlage, Gäste-WLAN etc.),
- im Notarnetz-Rechenzentrum befindlichen nachgelagerten Loadbalancern und Routern sowie einem Firewall-Cluster und
- einer ständigen (24/7) Ressourcen- und Performance-Daten-Überwachung durch das Rechenzentrum.

Sämtliche ein- und ausgehende Verbindungen des Büronetzwerkes ins Internet werden über diesen Perimeterschutz im Rechenzentrum geleitet und durch die Firewall gefiltert und überwacht. Dementsprechend ist der I**nternetanschluss des Büronetzwerkes nie direkt Angriffen aus dem Internet ausgesetzt**. Das **Rechenzentrum** stellt dabei **immer** den **zentralen Perimeterschutz** dar und wehrt Angriffe entsprechend ab. Die Verbindung von der lokalen Notarnetzbox zum Rechenzentrum ist dabei immer verschlüsselt, sodass hier kein Eingriff durch Dritte möglich ist.

Die Firewall im Notarnetz-Rechenzentrum umfasst u. a. folgende wichtigen **Schutzmechanismen**:

- **Prüfung und Überwachung Datenverkehr** –

  - Eingehende Verbindungen werden geprüft und überwacht. Dabei werden nur Verbindungen nach festgelegten Regeln zugelassen
    z. B. für den externen Zugriff auf eine lokal im Büronetzwerk befindliche Ressource wie einem E-Mailserver.
  - Ausgehende Verbindungen werden dagegen nahezu vollständig durchgelassen, da es sich normalerweise um von intern nach extern initiierte Verbindungen handelt wie z. B. der Zugriff auf eine Webseite von einem Arbeitsplatz-PC.

- **WebFilter** – Erkennung und Sperrung gefährlicher oder potentiell gefährlicher Verbindungen nach einem definierten Webfilter-Katalog, welcher einer ständigen Aktualisierung unterliegt.
- **Intrusion-Detection und -Prevention** (IDS/IPS) – Erkennung und Abwehr/Verhinderung von Angriffen, Missbrauchsversuche oder Sicherheitsverletzungen z. B. DoS-Attacken. Für die optimale Überwachungsfunktionalität werden stündlich Signatur-Updates durchgeführt.
- **SSL/SSH-Inspection** - SSL-Verbindungen zu bekannten SSL-Zielen von Command-and-Control-Server werden geblockt. Protokollierung von SSL-Anomalien (z. B. ausgelaufenen/ungültige Zertifikate) und Sperrung von Verbindungen bei folgenden Prüfergebnissen:
  - URLs mit ausgelaufenen SSL-Zertifikaten
  - URLs mit zurückgezogenen SSL-Zertifikaten
  - Zertifikate mit fehlerhafter Validierung

  SSL-Verbindungen werden beim SSL/SSH-Inspection nicht aufgebrochen.
- **ApplicationControl** – Erkennung bestimmter Anwendungen und anschließende Regelung oder Sperrung. Dieser Mechanismus greift nur für unverschlüsselte Verbindungen.
- **AntiVirus** – Virenprüfung bei Verbindungen über die Protokolle HTTP, SMTP, POP3, IMAP und FTP. Dieser Mechanismus greift nur für unverschlüsselte Verbindungen.

5 Standortvernetzung für Heimarbeitsplätze und Geschäftsstellen

Über den Einsatz weiterer **NotarnetzPlus-Anschlüsse** im Heimbüro und/oder in einer Geschäftsstelle können diese Standorte problemlos mit dem Büronetzwerk (ebenfalls NotarnetzPlus-Anschluss) über eine **Site-2-Site VPN** komplett vernetzt werden. Somit besteht:

- ein Vollzugriff vom jeweiligen Standort auf das Büronetzwerk,
- eine Verbindung zum Notarnetz bzw. Zugang zur IT-Plattform der Bundesnotarkammer und deren Anwendungen wie XNP, beN, ZTR etc.,
- die Absicherung des lokalen Standortnetzwerkes gegenüber dem Internet durch den Perimeterschutz des Notarnetz-Anschlusses und
- eine strikte Trennung vom privaten Netz und privaten Geräten bzw. sonstigen Geräten, Anwendungen (IoT) und Netzwerken.

Anwendungsbereiche: Sichere Vernetzung von weiteren Geschäftsstellen- und Heimarbeitsplätzen mit abgesichertem Notarnetz- und Internet-Zugriff.

6 Notarnetz-Mobilzugang

Mit dem **Notarnetz-Mobilzugang** wird ein **sicherer Zugriff von unterwegs** über ein Smartphone, Tablet oder Notebook auf das Büronetzwerk auf Basis einer Mobilfunkverbindung hergestellt. Dabei wird eine spezielle **Notarnetz-APN** (Access Point Name) mit einer **Benutzernamen-/Passwortkombination** in den Mobilfunk-Einstellungen des Endgerätes eingetragen. Dieser

Zugang ist gekoppelt an eine definierten SIM-Karte, sodass ein Zugriff nur mit SIM-Karte oder nur mit der Benutzernamen-/Passwortkombination nicht möglich ist.

Der Notarnetz-Mobilzugang kann mit bestehenden oder neuen **Mobilfunkverträgen** der Telekommunikationsgesellschaften **Telekom Deutschland GmbH und Vodafone GmbH** eingerichtet werden. Dabei müssen die Mobilfunkverträge „Mobile IP VPN“ bei der Telekom Deutschland GmbH bzw. „CorporateDataAccess“ (CDA) bei Vodafone unterstützen.

Nach Einrichtung des Notarnetz-Mobilzugangs auf dem Endgerät wird ein **Notarnetz-Zugang** hergestellt und **über Port-Weiterleitungsregeln Zugriffe auf das Büronetzwerk** gesteuert. Diese Weiterleitungsregeln müssen im Vorfeld auf der Notarnetzbox konfiguriert werden. Folgende vordefinierten Weiterleitungsregeln stehen zur Auswahl und werden beim Support in Auftrag gegeben:

- Zugriff auf Exchange-Server – ActiveSync Port 443 bzw. 8443 von extern (siehe Kapitel 7 VPN-Zugang Kapitel „Besonderheit ActiveSync“)
- Fernbedienung PC – Remotedesktop Port 3389
- Dateizugriff auf Server – SMB Port 445

Weitere individuelle Port-Weiterleitungsregeln sind möglich.

Anwendungsbereiche: Sicherer Zugriff von unterwegs auf E-Mails, Kontaktadressen und Termine oder mit dem Notebook von zu Hause und unterwegs auf das Büronetzwerk zugreifen.

7 VPN-Zugang

Mit dem VPN-Zugang wird der ungefilterte Zugang von extern über das Internet zu der Notarnetzbox des Büronetzwerkes ermöglicht. Für den Aufbau des VPN-Tunnels wir auf dem Endgerät die Client-Software **Cisco AnyConnect** installiert, die von der NotarNet GmbH bereitgestellt wird. Für Mobilgeräte kann die Client-Software über den App-Store heruntergeladen und installiert werden. Der Zugang ist durch eine Benutzername-/Passwortkombination abgesichert. Die Benutzerkennung wird in einem zentralen Kundencenter für VPN-Zugänge für jeden einzelnen Anwender eingerichtet. Somit ist eine **sichere Benutzer- und Berechtigungssteuerung** gewährleistet.

Da der VPN-Zugang nur durch die Benutzername-/Passwortkombination, und nicht wie bei NotarnetzPlus-Anschluss zusätzlich durch den Perimeterschutz abgesichert ist, empfehlen wir ein **hohes Maß an Sorgfalt** im Umgang mit den VPN-Zugangsdaten und der Absicherung der verwendeten Geräte und Zugänge gegen Schadcode und missbräuchlichen Zugriff.

Der Verbindungsaufbau erfolgt vom externen Endgerät über eine **SSL-Verbindung (SSL-VPN Port 443)** und terminiert auf der im Büro befindlichen Notarnetzbox. Die **Verifizierung** der Benutzername-/Passwortkombination erfolgt dabei auf einem **zentralen Radiusserver im Notarnetz-Rechenzentrum**.

Steht die VPN-Verbindung zur Notarnetzbox, erfolgt als erstes eine Update-Prüfung der Client-Software Cisco AnyConnect. Ist diese Prüfung abgeschlossen, steht die VPN-Verbindung und das Endgerät hat einen **Vollzugriff auf das Büronetzwerk**. Eine **Verbindung ins Notarnetz bzw. ins Internet wird über die VPN-Verbindung nicht bereitgestellt.** Letzteres kann allerdings im o. g. Kundencenter freigeschalten werden.

Besonderheit ActiveSync: Da für den SSL-VPN auf der Notarnetzbox Port 443 bereits reserviert ist, muss für einen externen ActiveSync-Zugriff (nur in Kombination mit Notarnetz-Mobilzugang) der **Port 8443** verwendet werden. Intern erfolgt die Weiterleitung auf den entsprechenden Mailserver wieder über Port 443.

Anwendungsbereiche: Externer Zugriff auf das Büronetzwerk für Remotedesktopanwendungen oder Dateizugriffe.

8 WLAN und Gäste-WLAN

Auf die Nutzung eines WLAN für Bürotätigkeiten sollte verzichtet werden. Sofern die Nutzung erforderlich ist, stellen wir einen separaten **WLAN-Access-Point** mit WPA2-Enterprise und EAP-Protokoll für die sichere Einbindung von WLAN-fähigen Geräten wie Notebooks, Handys, Tablets etc. zur Verfügung. Dieser **WLAN-Access-Point wird mit dem lokalen Netzwerk der Notarnetzbox verbunden** und wird dort aufgestellt, wo die WLAN-Verbindung benötigt wird z. B. im Beurkundungsraum. Auch der Einsatz weiterer WLAN-Access-Points ist problemlos möglich.

Der **WLAN-Einrichtung am Endgerät** erfolgt mit dem **WP2-Enterprise-Sicherheitsstandard und dem EAP-Protokoll**, bei der eine Anmeldung am WLAN-Netz mit Benutzername und Passwort erfolgt anstatt eines WLAN-Schlüssels. Die Benutzerkennung wird in einem zentralen Kundencenter für WLAN-Zugänge für jeden einzelnen Anwender eingerichtet. Somit ist eine **sichere Benutzer- und Berechtigungssteuerung** gewährleistet.

Die **Verbindung** WLAN-fähiger Geräte erfolgt in Kombination **über den WLAN-Access-Point und einem zentralen Radiusserver im Notarnetz-Rechenzentrum**. Daher ist ein Verbindungsaufbau am WLAN-Netzwerk nur möglich, wenn für die Notarnetzbox eine aktive Verbindung zum Notarnetz besteht.

Ein **Gäste-WLAN** ist nicht über den WLAN-Access-Point vorgesehen. Falls ein Gäste-WLAN erforderlich ist, muss auf eine strikte Trennung zwischen diesem und dem Büronetzwerk geachtet werden. Das Gäste-WLAN sollte dazu an einem separaten Internetanschluss oder an dem der Notarnetzbox vorgelagerten Netzwerk/Internetrouter betrieben werden, um den Zugriff durch Dritte auf das vertrauliche Büronetzwerk zu schützen.

Anwendungsbereiche: Als Erweiterung der Büronetzwerk-Verfügbarkeit für WLAN-fähige Geräte wie Notebooks, Drucker, Smartphones, Tablets etc.

9 Domain- und E-Mail-Hosting

Das Domain- und E-Mail-Hosting hat neben der Absicherung des Büronetzes gegenüber dem Internet ebenfalls einen hohen Schutzbedarf, welcher mit dem Notarnetz gegeben ist.

9.1 Domain-Hosting

Die NotarNet GmbH ist über das DENIC/ICANN-Mitglied rockenstein AG Domain-Provider und kann **neue Domains registrieren** bzw. den **Umzug** von bereits bei einem anderen Provider registrierten Domains veranlassen. Weiterhin gehört der **DNS-Service** (Domain Name Server) zum Angebot.

9.2 E-Mail-Hosting

Mit diesem E-Mail-Hosting Angebot wird ein gehosteter **E-Mail- und Groupware-Service** auf Basis eines im Notarnetz-Rechenzentrum befindlichen **Zimbra-Servers** bereitgestellt. Damit können E-Mailpostfächer in zwei funktionalen Ausprägungen gebucht werden:

- **ProMail** – reines E-Mailpostfach zum Senden und Empfangen von E-Mails ohne weitere Mailserver-Funktionalitäten
- **ProTeam** – vollwertiges E-Mailpostfach mit allen Mailserver-Funktionalitäten und der Einbindung in Outlook per Zimbra Outlook Connector

Diese Postfächer verfügen über alle gängigen E-Mailprotokolle. ProTeam-Postfächer können auch mit einem Zimbra Outlook Connector (ZCO) in Microsoft Outlook eingebunden werden. Dieser bietet eine bidirektionale Echtzeit-Synchronisation von E-Mail-Nachrichten, Ordnern, Kalenderdaten, Adressbüchern und Aufgaben zwischen Outlook und Zimbra-Server. Der ZCO speichert dabei eine Kopie des Postfaches auf dem lokalen PC.

Der **E-Mailserver steht im Notarnetz-Rechenzentrum** und ist somit gegenüber dem Internet geschützt. Sicherheits- und Funktions-Updates werden regelmäßig durchgeführt. Die Server

unterliegen einer ständigen System-Überwachung. Ein regelmäßiges **Backup** findet ebenfalls statt, sodass eine Wiederherstellung mit einem Datenstand von **maximal 57 Tage rückwirkend** möglich ist. Weiterhin ist ein zentraler **Antiviren- und Spam-Schutz** Bestandteil des E-Mail-Services.

Die **Postfächer** sind im Standard-Setup **nur aus dem Notarnetz erreichbar**, wodurch neben den üblichen Absicherungen noch eine **besondere Schutzwirkung** erreicht wird.

Die **Synchronisation** der Postfächer **von unterwegs über ein Smartphone** lässt sich optimal mit dem **Notarnetz-Mobilzugang** kombinieren.

Anwendungsbereiche: Einsatz einer gehosteten E-Mail- und Groupware-Lösung als Alternative zum eigenen Microsoft Exchange Server oder anderen Hosting-E-Mail Angeboten.

9.3 Anbindung lokaler E-Mailserver

Alternativ zum E-Mail-Hosting kann auch ein eigener E-Mail-Server im lokalen Büronetzwerk an den im Notarnetz-Rechenzentrum befindlichen SMTP-Relay-Server angebunden werden.

Dabei empfängt der **SMTP-Relay-Server** sämtliche **eingehenden E-Mails** einer oder mehrerer Mail-Domains und leitet diese mit entsprechendem **Antiviren- und Spam-Schutz** über die lokale Notarnetzbox auf die LAN-IP-Adresse des lokalen E-Mailservers weiter, der wiederum per Empfangsconnector die E-Mails entgegen nimmt. Hierbei sollte eine Einschränkung auf die IP-Adressbereiche und Ports erfolgen, von denen E-Mails angenommen werden dürfen. Das Routing wird entsprechend auf der Notarnetzbox konfiguriert.

Die **ausgehenden E-Mails** werden ebenfalls über den SMTP-Relay-Server verschickt, welcher eine Authentifizierung mit einem entsprechenden Account erfordert. Der Versand erfolgt durch den E-Mailserver über den Sendeconnector.

Durch die Anbindung des lokalen E-Mailservers im Notarnetz besteht noch ein **weiterer Schutz gegenüber dem Internet,** vor allem im Vergleich zum Betrieb des E-Mail-Servers an einem öffentlichen Internetanschluss.

Die **Synchronisation** der Postfächer **von unterwegs über ein Smartphone** lässt sich optimal mit dem **Notarnetz-Mobilzugang** kombinieren.

Anwendungsbereiche: Einsatz eines lokalen E-Mailservers (On Premise Lösung) im Büronetzwerk mit vorgelagertem SMTP-Relay-Server (Notarnetz) als Alternative zu einem gehosteten E-Mail Angebot.

10 Lokale Sicherheit

Zum Sicherheitskonzept NotarnetzPlus gehört auch die Gewährleistung der lokalen Sicherheit im Büronetzwerk durch entsprechende **technische und organisatorische Maßnahmen des Kunden**. Grundlage dafür sind die Nutzungsbedingungen sowie die Sicherheitsrichtlinien für die Teilnahme am Notarnetz. Dazu zählen unter anderem folgende **wichtigen Punkte**:

- Datensicherung und Offlinekopie an einem separaten Ort.
- Automatisierte Sicherheitsupdates
- Zugangsmittel (u.a. Notarnetzbox) und Konten absichern
- Antiviren- und Anti-SPAM und weitergehende Endpoint-Security
- Netzwerksegmentierung des lokalen Büronetzwerkes (Notarfachsystem von Netzwerk für sonstige Anwendungen)
- Notfallplan und Krisenstab

Weiterhin empfehlen wir die Berücksichtigung folgender wichtiger Informationen der Bundesnotarkammer (die Links sind nur über das Notarnetz erreichbar):

- **Handreichung IT-Sicherheit** - https://www.bnotk.de/intern/datenschutz/handreichung-it-sicherheit
- **Datenschutzrechtliche Verhaltensregeln** - https://www.bnotk.de/intern/datenschutz/datenschutzrechtliche-verhaltensregeln

11 Dokumenten-Historie

Datum	Autor	Beschreibung
30.11.2022	Christian Richter	Erster Entwurf
21.02.2022	Christian Richter	Ergänzung FTTH-Anschlüsse