Die Internet-Anbindung des virtuellen Datenschutzbüros – Open Source und innovative Internet-Konzepte in der Verwaltung

Roman Maczkowsky, Martin Rost, Marit Köhntopp[1]

Kurzfassung:
Der Anschluss an das Internet ist mit einer Reihe von Risiken verbunden. Dieser Text stellt ein innovatives Konzept für den Internet-Zugang vor, das die Anforderungen an eine sichere und datenschutzgerechte Anbindung erfüllt. Es basiert auf Virtual Network Computing, womit man auf entfernten Rechnern arbeiten kann. Zusätzlich werden einige Komponenten wie ein spezieller PGP-Server, ein Log-Server und ein Vorschlag für individuell zugeschnittene Zugriffsrechte zum Nachbilden einer Gewaltenteilung beschrieben. Das System wird im virtuellen Datenschutzbüro, einem Projekt von vielen Datenschutzinstitutionen, entwickelt und aufgebaut. Open Source ist in diesem Projekt ein Schlüsselprinzip sowohl für die Technikentwicklung als auch für das Veröffentlichen der Ergebnisse im Internet.

Stichwörter: Internet, Datenschutz, Datensicherheit, Open Source, Virtual Network Computing, Protokollierung, Virtuelles Datenschutzbüro, Verwaltung

Abstract:
Realizing Internet access means having to cope with many risks. In this text, an innovative concept, which fulfils the requirements for a both secure and privacy-suitable Internet access, is introduced. It bases on virtual network computing which enables the work on remote computers. In addition, some modules like a specific PGP server, a log server, and a proposal for fine-grained access rights in order to implement separation of powers are described. The system is being developed and used within the Virtual Privacy Office, a project of Privacy Protection Authorities. In this project, open source is a key approach for both building technology and publishing the results in the Internet.

Keywords: Internet, Privacy, Security, Open Source, Virtual Network Computing, Logging, Virtual Privacy Office, Civil Service

1. Das virtuelle Datenschutzbüro – ein Projekt von Datenschutzinstitutionen

Das virtuelle Datenschutzbüro betreibt im Internet eine **Plattform** zu allen Themen rund um den Datenschutz. Dazu hat sich eine ganze Reihe von Datenschutzinstitutionen aus aller Welt zusammengetan, um über das Internet zu kooperieren und den Nutzerinnen und Nutzern ihren Service anzubieten [3]. Im Vordergrund bei der technischen Realisierung steht, von Anfang an ein möglichst hohes Maß an Datenschutz und Datensicherheit zu integrieren und die Ergebnisse – wie bei dem Open-Source-Ansatz – allen Interessierten weiter zu geben [8].

[1] Roman Maczkowsky, Martin Rost, Marit Köhntopp,
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Kiel.

Eine der beteiligten Datenschutzdienststellen, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, hat die Dienstleistung übernommen, die grundlegenden Konzepte des virtuellen Datenschutzbüros zu entwickeln sowie die erforderliche Technik aufzubauen und zu betreiben, die dann allen Projektpartnern zur Verfügung gestellt wird. Im Folgenden wird das Konzept der Internet-Anbindung des virtuellen Datenschutzbüros beschrieben, das den Ansprüchen der Verwaltung und insbesondere denen der Datenschutzbeauftragten genügen muss.

2. Anforderungen an eine Anbindung an das Internet

Beim Anschluss an das Internet hat eine Verwaltung eine Menge an technischen und organisatorischen Maßnahmen zu treffen, damit das erforderliche Maß an Funktionalität, Datenschutz und Datensicherheit gewährleistet wird. Hinzu kommen in diesem Fall weitere Kriterien, die das Projekt Virtuelles Datenschutzbüro definiert, sowie einige praktische Rahmenbedingungen. Diese drei Kategorien von Anforderungen werden im Folgenden kurz skizziert.

2.1 Generelle Zielvorgaben aus Sicht des Datenschutzes

Im Rahmen des virtuellen Datenschutzbüros spielt die unmittelbare Verarbeitung personenbezogener Daten keine große Rolle. Trotzdem werden vergleichbare Anforderungen an Datenschutz und Datensicherheit angelegt, weil ein hoher Grad an Sicherheit erreicht werden soll, so dass die entwickelten Konzepte auch auf andere Verwaltungsbehörden übertragbar sein können. Eine erste Implementierung erfolgt bereits beim Aufbau des virtuellen Datenschutzbüros, indem die Internet-Anbindung für das Verwaltungsnetz des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, das das Projekt initiiert hat und von wo aus die zentralen Komponenten dafür zur Verfügung gestellt werden, in diesem Sinne realisiert wird.

Die Datenschutzanforderungen an eine Internet-Anbindung bestehen darin, dass **Vertraulichkeit, Integrität und Verfügbarkeit** der zu bearbeitenden (personenbezogenen) Daten im internen (Verwaltungs-)Netz nicht beeinträchtigt werden dürfen. Insbesondere darf kein unbefugter Zugriff aus dem Internet möglich sein: weder direkt über eine offene Verbindung noch indirekt über Manipulationen durch trojanische Pferde, die beispielsweise per E-Mail oder aktive Inhalte in das interne Netz gelangen könnten.

Das aufgebaute System muss **nachvollziehbar dokumentiert** sein. Insbesondere sollen eine Aufgabenbeschreibung, eine Verfahrensbeschreibung, ein Sicherheitskonzept, eine Risikoanalyse sowie Dokumentationen über Test und Freigabe vorliegen.[2]

[2] Für die öffentlichen Stellen des Landes Schleswig-Holstein ist dies sogar eine Pflicht, die sich aus dem Landesdatenschutzgesetz und der Datenschutzverordnung ergibt.

2.2 Besondere Kriterien für die Realisierung im virtuellen Datenschutzbüro

Im virtuellen Datenschutzbüro sollen **Musterlösungen** zum Einsatz kommen, die – sofern im praktischen Einsatz für gut befunden – dann auf andere Systeme übertragbar sind. Zu den im Projekt definierten Anforderungen gehören:

- Die technische Infrastruktur wird innerhalb der Datenschutzdienststelle, die die zentralen Komponenten für das Projekt betreibt, selbst konzipiert und aufgebaut, um ein hohes Maß an **technischer und organisatorischer Unabhängigkeit** zu erreichen. Die Konzepte werden mit den anderen beteiligten Datenschutzinstitutionen diskutiert und abgestimmt, so dass das Know-how aller Projektpartner einfließen kann.
- Die datenschutzrechtlichen Bestimmungen sollen, soweit möglich, unmittelbar in technischen Lösungen abgebildet werden. Zusätzlich sollen die Internet Service Provider, über die die Anbindung an das Internet erfolgt, zu einer vollständigen Einhaltung der **Datenschutzstandards** juristisch verpflichtet werden.
- Die Betreiber der zentralen Komponenten müssen tatsächlich über die **technische Kompetenz** verfügen, um beispielsweise die in den Log-Dateien der WWW-Server und insbesondere der Router bzw. Firewalls anfallenden Verkehrs- und Inhaltsdaten interpretieren und auch deren Schutzwürdigkeit beurteilen zu können. Diese praktische Erfahrung im Betrieb einer Internet-Anbindung ist eine gute Grundlage dafür, um neue Entwicklungen in der Kommunikationstechnik zeitnah verfolgen und so rechtzeitig auf ihre datenschutzrechtlich relevanten Aspekte hin überprüfen zu können.
- Wo immer es geht, sollen **Open-Source-Produkte** wegen der potenziell höheren Transparenz [1, 5, 7] und der Möglichkeit, Einschränkungen im Funktionsumfang vorzunehmen und damit passgenauer auf die Anforderungen zuzuschneidern, zum Einsatz kommen. Außerdem können damit die entwickelten Lösungen von allen anderen Interessierten leichter übernommen werden, ohne dass zusätzliche Lizenzgebühren anfielen.

Neben diesen allgemeinen Grundsätzen gibt es konkrete **Pflichtenheft**-Anforderungen, welche Internet-Dienste im virtuellen Datenschutzbüro angeboten werden sollen. Diese umfassen insbesondere Aufbau und Betrieb

- eines Web-Servers, dessen Inhalte erst unmittelbar mit dem Aufruf durch den Nutzer dynamisch aus einer Datenbank generiert werden, wobei diese Datenbank wiederum per Internet von Autoren mit verschiedenen Zugriffsberechtigungen gespeist werden kann (Content-Management-System);
- eines Mailinglist-Servers zur Verwaltung von Mailinglists mit verschiedenen Eigenschaften; dazu die Möglichkeit von Verschlüsselung und digitaler Signatur für E-Mails;
- eines Virtual Private Networks unter den Projektpartnern;

- der Möglichkeit zum Austausch per Webforen und Videokonferenzen über das Internet.

2.3 Praktische Rahmenbedingungen

Der Erstaufwand zur Realisierung neuer Konzepte ist in der Regel recht hoch, zumal zu Beginn manche scheinbar gute Idee in einer Sackgasse endet. Hat man jedoch erst einmal ein stabiles und tragfähiges Konzept, ist der Aufwand zur Umsetzung sehr viel geringer. Dies ist auch nötig, da kaum eine Verwaltung einschließlich der Datenschutzdienststellen mehrere Techniker in Vollzeit dafür abstellen kann, die Internet-Anbindung zu realisieren und einen sicheren Betrieb zu gewährleisten. Es gilt also, den **Aufwand** zur Entwicklung und zum Betrieb auf das wirklich erforderliche Maß zu **reduzieren** und auch Möglichkeiten eines verantwortbaren Outsourcings in Betracht zu ziehen.

3. Methodik im virtuellen Datenschutzbüro

Das virtuelle Datenschutzbüro arbeitet in der Tradition von **Open Source**. Dies bedeutet nicht nur, dass Open-Source-Produkte eingesetzt werden – z.B. Linux auf den Arbeitsrechnern und Servern des virtuellen Datenschutzbüros –, sondern dass die erarbeiteten Konzepte und Umsetzungen anderen Verwaltungen und der Internet-Community ganz allgemein zur Verfügung gestellt werden. Ebenso sollen offene Diskussionen und Beteiligungsmöglichkeiten von allen Interessierten zur Qualitätssteigerung der Konzepte und Prototypen beitragen. So ist ein Feedback nicht nur von den Projektpartnern, den Datenschutzinstitutionen, erwünscht, sondern von allen Interessierten aus der Internet-Community.

Innerhalb des Projektes sind zudem unterschiedliche Sichten dadurch vertreten, dass die Mitarbeiter aus verschiedenen Bereichen stammen. Dies ermöglicht ein fruchtbares **interdisziplinäres Arbeiten**. Aus Datenschutzsicht ist insbesondere von Bedeutung, dass die juristischen und die technischen Anforderungen und Möglichkeiten in den entwickelten Lösungen zusammengeführt werden.

Ein tiefgreifendes Ziel des virtuellen Datenschutzbüros besteht darin, das Niveau des technischen Datenschutzes insgesamt zu heben und den Stand der Technik fortzuschreiben. Nach Möglichkeit sollen **„Privacy-Enhancing Technologies“** [11] zum Einsatz kommen, die in diesem Rahmen auch einem Praxistest unterzogen werden. Die Erfahrungsberichte werden ebenso wie Eigenentwicklungen öffentlich für die Internet-Community gemacht.

In einigen IT-Labors von Datenschutzinstitutionen werden Internet-basierte Angriffe nachgestellt oder sogar selbst entwickelt, um sich mit der Wirkung vertraut zu machen und den Grad der Sicherheit von Konzepten zur Anbindung an das Internet abschätzen zu können. Solche **Tiger Teams** sind als Prüfer für die Konzepte und die Technik im virtuellen Datenschutzbüro eingeladen.

4. Ausgewählte Konzepte der Internet-Anbindung im virtuellen Datenschutzbüro

Die Anbindung der Web- und Mail-Server im virtuellen Datenschutzbüro erfolgt klassisch, d.h. über Router, Packetfilter und Application-Level-Gateway. Web- und Mail-Server stehen in einer Demilitarized Zone (DMZ). Zusätzlich kommen wegen der besonderen Anforderungen (siehe Abschnitt 2.2) neue Konzepte zum Einsatz, mit denen typische neuralgische Probleme behandelt werden. So ist ein heikler Punkt beispielsweise die Realisierung des Anschlusses eines internen Netzes, in dem sensible Daten bearbeitet werden, an das Internet. Dies kann mit Hilfe eines **VNC-Servers** (siehe Abschnitt 4.1) auf eine relativ sichere und sogar kostengünstige Art gelöst werden. Ein weiteres behandlungsbedürftiges Problem ist die **Protokollierung** von Daten. Dieser Themenkreis umfasst nicht nur den Aspekt, welche Daten man als Betreiber von Internet-Servern protokollieren kann, sondern auch, wie diese vor etwaiger Manipulation etwa durch Hacker oder vor Einsichtnahmen durch Unbefugte geschützt werden können. Der in diesem Text vorgeschlagene **spezielle PGP-Server** stellt eine geeignete Lösung für die Integration der PGP-Verschlüsselung in Nutzerumgebungen von Mailprogrammen dar. Zuletzt wird die selten realisierte **Gewaltenteilung** zwischen der technischen Administration und der Verwaltung einer Institution angesprochen, und es werden einige Vorschläge dazu unterbreitet.

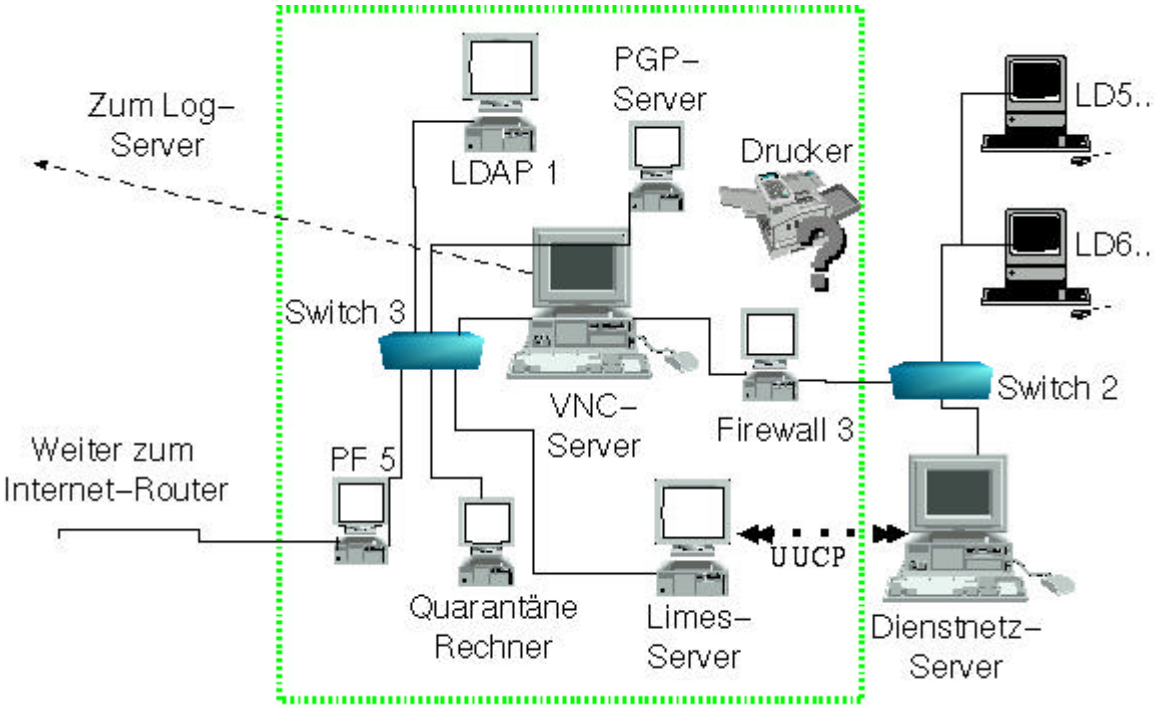

Abb. 1: Die wichtigsten Komponenten der Internet-Anbindung im virtuellen Datenschutzbüro

4.1 Anbindung des internen Netzes per Virtual Network Computing (VNC)

VNC steht für Virtual Network Computing [2]. Das Kernkonzept des VNC-Servers sieht vor, dass zwischen dem Client (konkret: dem VNC-Viewer[3] auf dem PC-Arbeitsplatz des Mitarbeiters) und dem VNC-Server ausschließlich Grafik-, Tastatur- und Mausinformationen übertragen werden. Dadurch ist es möglich, Netzanwendungen wie WWW, FTP und E-Mail dem internen (Verwaltungs-)Netz **vorzulagern**. Sämtliche Prozesse und Daten, die mit Internet-Diensten zu tun haben, befinden sich somit auf dem VNC-Server, auf dem sie auch zur Ausführung gebracht werden.

Der VNC-Server stellt das operative Zentrum der Anbindung der Dienststelle an das Internet dar. Programme werden – über eine Firewall hinweg, die die Verbindung zwischen dem VNC-Server und dem internen Netz herstellt – aus dem internen Netz heraus **ferngesteuert**. Auf diese Weise können somit prinzipiell keine Daten oder Programme direkt auf dem Arbeitsplatzrechner des Mitarbeiters eingesehen oder zur Ausführung gebracht werden. Die mögliche Schadenswirkung eines E-Mail-Angriffs mit aktiven Inhalten [4] beschränkt sich damit auf den Bereich des jeweils aktiven Nutzers auf dem VNC-Rechner.

4.1.1 Realisierung

Die Grundlage für die Realisierung der VNC-Server bildet eine Linux-Installation auf Basis von SuSE-Linux 7.0. Zum Einsatz kommen Programme aus dem KDE2-Paket[4] sowie Browser, Schreibprogramme und eigene Anpassungen. Der VNC-Bereich (siehe Abb. 1) umfasst neben den eigentlichen VNC-Servern eigene Server für die Nutzer-Verwaltung (LDAP-Server), für die Verschlüsselung mit PGP/GPG und einen Quarantäne-Rechner zum Test von (insbesondere per Diskette angelieferten) Dateien auf Viren und trojanische Pferde.

4.1.2 Sicherheit

Ziel ist eine weitestgehende Trennung von (relevanten) Nutzdaten und der Arbeitsumgebung, dem VNC-Server. Daher sind die Nutzer-Verzeichnisse und die Daten für ihre Authentisierung auf einem zentralen LDAP-Server ausgelagert.

Auf dem VNC-Server muss eine komplette Arbeitsumgebung zur Verfügung gestellt werden. Hier sind auch möglicherweise sicherheitsrelevante Programme enthalten, z.B. Browser und Mail-User-Agents (MUAs) mit Interpreter-Funktionalität oder andere Programme wie Entpacker, Editoren und andere Tools. Durch Begrenzung der installierten Programme, durch Festigung (sog. „hardening“[5]) der Betriebssystem-Installation und durch Einsatz von LIDS (Linux Intrusion Detection System) [9] werden

---

3 VNC-Viewer stehen für alle derzeit eingesetzten Standardbetriebssysteme zur Verfügung.

4 Insbesondere Kmail, bei dem die PGP/ GPG-Unterstützung integriert ist.

5 „Härten“ eines Betriebssystems bedeutet das Reduzieren der Programmteile und Module auf die wirklich notwendige Funktionalität.

regelbasiert feiner granulierte Rechte vergeben und auftretende Regelverstöße gemeldet. Auf dem LDAP-Server kommen die gleichen Maßnahmen zum Einsatz. Auf diese Weise sollen Angriffe und Manipulationen zuverlässig erkannt und verhindert werden.

4.1.3 Dimensionierung

Für die Anbindung der Client-Rechner wurde eine durchschnittliche Bandbreite von ca. 10 Mbit pro Client veranschlagt. Ein Switch sorgt für die Kanalisierung der Datenströme. Die Firewall(s) zwischen Client- und VNC-Rechnern müssen entsprechend dimensioniert werden. Die VNC-Server selber können flexibel kaskadiert werden. Für den Einsatzbereich von ca. 30 Clients sind zwei bis drei VNC-Server (je AMD-K7, 750 MHz, 640 MB RAM) vorgesehen. Die Anforderungen an die Ausstattung der Client-Rechner ist demgegenüber eher gering: Man kann mit einem 486er PC ab 100 MHz auskommen.

4.1.4 Praxisbericht

In der Praxis zeigt sich, dass es fast keinen Unterschied macht, ob auf dem eigenen PC oder „remote“ auf dem VNC-Server gearbeitet wird. Allerdings bedeutet es eine Umgewöhnung, lokale und entfernte Daten nicht beliebig miteinander mischen zu können. Ein weiteres Problem stellt die Druckausgabe dar, die aufgrund der Trennung der beiden Netze nicht ohne weiteres am lokalen Drucker erfolgt. In Umgebungen mit (zentralen) Netzdruckern ist dies jedoch kein Problem.

4.2 Zentraler Log-Server

Sämtliche Log-Mitteilungen der einzelnen Rechner werden einem **speziellen Log-Server** zugeführt. Er dient dazu, die anfallenden Log-Dateien in Echtzeit aufzunehmen und sofort zu verarbeiten. Anschließend können sie auf dem Server ausgewertet werden. Um nachträgliche Manipulationen an den Log-Dateien insbesondere durch Angreifer über das Internet zu verhindern, sind sie **gegen Änderungen geschützt**. Zusätzliche Sicherheit bieten sind die verschlüsselte Übertragung signierter Log-Dateien sowie der Einsatz von Hilfsprogrammen zur Log-Auswertung (Intrusion Detection Systems (IDS) und Intrusion Response Systems (IRS)).

Die erreichbare Sicherheit gegenüber nachträglichen Manipulationen ist relativ hoch. Darüber hinaus werden die Zugriffe auch durch berechtigte Personen mit Hilfe von Kryptographie und Mehraugenprinzip eingeschränkt.

Eine datenschutzkonforme Auswertung der anfallenden Protokolle, die auch personenbezogene (Kommunikations-)Daten enthalten, muss eine Kombination aus technischen Analysetools, technischen Beschränkungen der Zugriffsrechte, klarer Trennung von technischen und inhaltlichen (Administrations-)Aufgaben (siehe Abschnitt 4.4) und einer vertraglichen Regelung sein. In jedem Fall ist für die Protokolldaten festzulegen, zu welchen Zwecken sie gespeichert und ausgewertet werden, wer auf sie zugreifen darf und wann sie nicht mehr erforderlich sind und gelöscht werden müssen. Für diese

Regelung innerhalb einer Dienststelle oder eines Betriebes muss der Personal- bzw. Betriebsrat einbezogen werden.

4.3 PGP-Server als „Big Smartcard“

Eine sichere Einbindung von Kryptosoftware wie PGP könnte konzeptionell am besten über eine Smartcard realisiert werden, die die jeweiligen (geheimen) Schlüssel enthält. Da eine solche **Smartcard**-Lösung nicht zur Verfügung stand, wird im virtuellen Datenschutzbüro zunächst eine Art Nachbau einer solchen Funktionseinheit in Form eines **speziellen PGP-Servers** eingesetzt. Der Server arbeitet nach außen über ein definiertes Protokoll mit OpenSSL (Secure Socket Layer) auf TCP/IP-Basis. Die Clients tauschen die PGP-Befehle und Daten mit dem Server über ein Skript aus.

Der PGP-Server hat die Aufgabe, das PGP- (genauer: GPG-)Verschlüsselungsprogramm [6] sowie die dazugehörigen öffentlichen und geheimen Schlüssel vorzuhalten und die kryptographischen Operationen auf diesem gesonderten Rechner ablaufen zu lassen. Die Handhabung verschlüsselter E-Mails soll für die Nutzer einfach und transparent sein; Abstriche an der Sicherheit dürfen nicht gemacht werden.

Verschlüsselte Dateien direkt in das interne Netz zu übertragen, ist unpraktikabel und stellt obendrein ein Sicherheitsrisiko dar, weil der Inhalt vor dem Entschlüsseln nicht auf Viren und trojanische Pferde geprüft werden kann. Auf der anderen Seite ist das Risiko unbefugter Zugriffe auf die geheimen Schlüssel vorhanden, wenn sie auf einer Festplatte gespeichert sind (z.B. Zugriff bei Diebstahl des Rechners). Ferner besteht das Risiko, dass auf dem VNC-Server andere Programme bzw. Benutzer Manipulationen vornehmen. Aus diesen Gründen ist eine physikalische Trennung der Verarbeitungslogik zwingend erforderlich. Als weitere Schutzmaßnahmen lässt sich das Dateisystem des PGP-Servers von außen nicht ansprechen, die Konsole ist gesperrt, und die PGP-Schlüssel befinden sich nur im Arbeitsspeicher (RAM).

Die Methode, die PGP-Schlüssel auszulagern, ist in einer Dienststelle zum Zwecke der Ver- und Entschlüsselung dienstlich relevanter Daten unproblematisch. Eine Auslagerung eines **mitarbeiterbezogenen, geheimen Signierschlüssels** außerhalb des jeweiligen Mitarbeiterbereichs kommt jedoch nicht in Frage, da eine Nutzung durch Unberechtigte und damit ein unberechtigtes Auftreten unter der Identität eines anderen Mitarbeiters nicht ausgeschlossen werden kann: Möchte man also über die Verschlüsselung hinaus den Mitarbeitern individuelle digitale Signaturen ermöglichen, die ihnen zurechenbar sein sollen (z.B. für Willenserklärungen oder Mitzeichnungszwecke), müssen die Signierschlüssel im persönlichen Bereich des Mitarbeiters verbleiben.

4.4 Gewaltenteilung zwischen Technik und Verwaltung

Wichtig und oft übersehen: Die Systemadministratoren haben meist real zu viele Befugnisse, die ihnen vom Betriebssystem gegeben sind. Es ist mit den heutigen Systemen nicht einfach, die **organisatorische Trennung** von verantwortlichen Entscheidungsträgern und ausführenden Technikern unmittelbar umzusetzen. Spätestens ein Auslagern der Systemadministration wird damit zu einer gefährlichen Sicherheits-

lücke und ist datenschutzrechtlich in einigen Fällen sogar nicht erlaubt. Das Konzept im virtuellen Datenschutzbüro sieht daher vor, bereits konzeptionell diese Trennung vorzunehmen und technisch so zu gestalten, dass sich diverse Sicherheitsaspekte wie Mehraugenprinzip, Protokollierung, Sperrung und Freigabe von Ressourcen und Zugriffsrechtevergabe realisieren lassen.

Die wichtigsten Punkte zur Realisierung der Gewaltenteilung sind:

- die Definition der Aufgaben in Form einer möglichst genauen Beschreibung der Rechte, die den jeweiligen Parteien eingeräumt bzw. genommen werden sollen;
- der Ersatz des Superusers durch **spezifische Administrationsaccounts** mit eingeschränkten Rechten, insbesondere
- eigene Revisionsaccounts mit „Nur-Lese-Berechtigung“ für Kontrollzwecke, sowie
- die Vergabe von Rechten mit Hilfe von Access Control Lists (ACL).

Da unter Linux wie auch in den meisten gängigen Betriebssystemen standardmäßig solche Trennungen nicht vorgesehen sind, müssen diese zusätzlich eingebaut werden. Interessante Ansätze liefert hierbei z.B. RSBAC (Rule Set Based Access Control) [12] und LIDS (Linux Intrusion Detection System) [9].

5. Einordnung in Bezug auf andere Konzepte der Internet-Anbindung

Realisiert man den Internet-Zugriff über eine Umgebung, von der aus kein Zugriff auf die schützenswerten Daten möglich ist, erreicht man einen sehr hohen Grad an Sicherheit. Häufig lässt sich diese klare Trennung aber nicht erreichen, denn das Internet soll ja gerade bei der Bearbeitung der Aufgaben, die üblicherweise im internen Netz abgewickelt werden, behilflich sein, so dass Internet-Informationen in die interne Bearbeitung der Vorgänge einfließen sollen. Darüber hinaus muss man sich bereits dann, wenn es lediglich um eingehende oder ausgehende E-Mails geht, Gedanken über die erforderlichen Sicherheitsmaßnahmen machen: Zum einen stellen die E-Mails selbst womöglich sensible Daten dar, die zu schützen sind; zum anderen kann der E-Mail-Dienst als Vehikel für Angriffe[6] dienen.

Alle Konzepte, um sich vor Gefahren aus dem Internet zu schützen, bestehen in einer **(kontrollierten) Abschottung** der sensiblen Daten. Abgesehen von der vorgestellten VNC-Methode gibt es weitere Arten, solche **Schutzzonen** zu bilden:

- **vollständig physikalische Trennung:**
  Für den Zugriff auf externe Netze wird ein gesondertes Rechnersystem zur Verfügung gestellt.
- **Dual-Boot-System:**
  Beim Booten des Rechners kann sich der Nutzer entweder für die Internet-Zugriffsmöglichkeit oder für die Arbeit im internen Netz entscheiden.

[6] Mit Hilfe von Attachments, aber unter Umständen sogar ohne die Verwendung von E-Mail-Anhängen.

- **Einsatz von Firewalls:**
  Mit Hilfe von Firewalls soll die unerwünschte Kommunikation ausgefiltert werden. Je nach Art wird auf verschiedenen Ebenen gefiltert. Um sich vor ausführbaren Inhalten mit Schadensfunktionen zu schützen, gibt es zwei Möglichkeiten:

  - Filterung dieser Inhalte an der Firewall:
    Mit dieser Methode verhindert man von vornherein, dass bestimmte definierte Inhalte überhaupt in das interne Netz durchgelassen werden und damit dort ausgeführt werden können. Allerdings kann die Firewall nicht alle schädlichen Inhalte erkennen, insbesondere nicht bei der Übertragung verschlüsselter Daten. Deshalb ist nicht ausgeschlossen, dass sich schädliche Inhalte durch die Firewall hindurch schmuggeln lassen.
  - Deaktivierung dieser Inhalte durch Konfiguration und ggf. Zusatzprogramme auf den Nutzerrechnern:
    Die meisten Internet-Client-Programme sind so gestaltet, dass der Nutzer selbst darüber entscheiden kann, welche ausführbaren Inhalte er generell aktiviert bzw. deaktiviert oder im Einzelfall zur Ausführung bringt. Es bedeutet oft einen großen Aufwand, die Arbeitsplatzrechner so abzusichern, dass der Nutzer nicht absichtlich oder aus Versehen schädigende Inhalte zur Ausführung bringen kann. Häufig ist dies mit kaum tolerierbaren Einbußen an Funktionalität verbunden.

Als ergänzende Methode lassen sich Informationen verschlüsselt speichern, und nicht mehr benötigte Daten können frühzeitig gelöscht werden, so dass sie damit auch kein Angriffsziel mehr darstellen.

Im Folgenden werden diese Methoden für eine abgesicherte Internet-Anbindung in Bezug auf ihr Schutzniveau, Aufwand und Kosten sowie die Möglichkeit von Schutzzonen übergreifenden Zugriffen für ein kombiniertes Arbeiten sowohl im internen Netz als auch im Internet eingestuft:

Methode	**Schutzniveau**	**Zugriffe zwischen Schutzzonen möglich?**	**Aufwand / Kosten**
Vollständig physikalische Trennung	sehr hoch	nein	sehr hoch: Vorhalten von gesonderter Hardware pro Arbeitsplatz oder unbequeme Lösung mit zentralisierten Einzelrechnern für Internet-Zugang
Dual-Boot-System	mittel bis hoch (in Abhängigkeit von Konfiguration, da kein Zugriff auf die anderen Festplattenbereiche und Netze bzw. Netzwerkkarten möglich sein darf); bei erfolgreichem Angriff kein weiterer Schutz	nein (falls doch: geringeres Schutzniveau)	geringe Kosten; unbequem, da bei Wechsel der Arbeitsumgebung jeweils ein Booten notwendig ist
Firewall mit Inhaltsfilter	mittel (Inhaltsfilterung nicht zuverlässig); bei erfolgreichem Angriff kein weiterer Schutz	ja	mittel: Personalaufwand für den Betrieb der Firewall inkl. Inhaltsfilterung
Firewall, Inhaltsfilter an Clients	mittel (Inhaltsfilterung nicht zuverlässig); bei erfolgreichem Angriff kein weiterer Schutz	ja	mittel: Personalaufwand für den Betrieb der Firewall inkl. Inhaltsfilterung
VNC-Server hinter einer Firewall	hoch; bei erfolgreichem Angriff auf eine Komponente sind weitere Schutzzonen zu überwinden	ja, denn es wird in zwei Netzen gleichzeitig gearbeitet	mittel: relativ geringe Kosten für die Hardware, kostenlose Software, Personalaufwand für den Betrieb der Firewall und des VNC-Servers

Bei dem VNC-Konzept ist eine komplette Ausführungsumgebung vorgelagert, die selbst bei erfolgreichem Angriff keine sensiblen Daten preisgeben kann: Das Konzept des Internet-Zugriffs über VNC-Server hat prinzipbedingt den Vorteil, dass alle Programme, die mit der Internet-Kommunikation in Zusammenhang stehen (z.B. Browser und Mail-Clients sowie aktive Inhalte [4, 13]) und momentan das größte Sicherheitsrisiko darstellen, *nicht* auf dem Rechner zur Ausführung kommen, von dem aus auch der Zugriff auf sensible (schützenswerte) Daten möglich ist. Bei der klassischen Anbindung hinter einer Firewall ist aber genau dies der Fall. Ein neu entdecktes oder ein noch nicht geschlossenes Sicherheitsloch in einer Firewall öffnet potenziellen Angreifern den gesuchten Zugang. Werden keine gravierenden Veränderungen durch die Angreifer vorgenommen, so wird das Eindringen oftmals nicht einmal bemerkt. Der

mögliche Schaden kann sehr hoch sein, wenn das interne Netz vollkommen unter Kontrolle von Angreifern steht.

Eine Firewall-Architektur, wie sie auch zum Schutz des VNC-Bereichs eingesetzt wird, kann durch den Einsatz verschiedener Hard- und Software-Systeme zur **Vermeidung von Monokulturen** gestärkt werden, sofern geschultes Personal für die Betreuung zur Verfügung steht.

Generell gilt, dass die Kosten für Hard- und Software im Vergleich zu den Kosten für **Personal**, das für den sicheren Betrieb der Internet-Anbindung zuständig ist, gering ausfallen. Um die erforderliche Sicherheit so gut wie nach dem Stand der Technik möglich garantieren zu können, ist eine **ständige Beschäftigung** mit dem Thema und den Systemen erforderlich. Alternativ kann man an ein Outsourcing von Teilen der Systeme denken, was bei sicherheitsrelevanten Komponenten jedoch problematisch ist. Ein **Outsourcing** der äußeren Firewall beim VNC-Konzept wäre dagegen relativ unkritisch, solange der wenig aufwändige Betrieb des VNC-Servers im eigenen Bereich verbleibt.

6. Fazit und Ausblick

Die vorgestellte Lösung zur Internet-Anbindung realisiert durch die Methode der **Entkopplung** zwischen Internet und internem Netz mit Hilfe von Virtual Network Computing eine hohe Sicherheit unter Verwendung von Open-Source-Software. In Bezug auf den Schutz personenbezogener Daten nach dem Datenschutzgesetz kommt den genannten Maßnahmen eine besondere Bedeutung zu. Der unzureichende Schutz von Log-Daten gegen Veränderung sowie die Vergabe von „allmächtigen“ Superuser-Rechten an technische Systemadministratoren und verantwortliche Entscheidungsträger ohne weitere Differenzierung sind nicht mehr zeitgemäß und können datenschutzrechtlich bedenklich sein. Es bedarf des Umdenkens der Verantwortlichen, sich der Risiken bewusst zu werden, die datenschutzrechtlichen Implikationen frühzeitig mit einzubeziehen und ein umfassendes Datenschutzkonzept zu verfolgen.

Bereits jetzt liefert der **Open-Source**-Ansatz für den Bereich der Software für Datenschutz und Datensicherheit brauchbare Tools. Darüber hinaus sind Ergebnisse von Forschungsprojekten hilfreich, die Schutzmechanismen untersuchen und als Open Source implementieren. Hier sind weitere Fortschritte zu erwarten. Open Source bietet durch seine Transparenz und die Möglichkeit für alle Interessierten, die Software zu evaluieren, grundsätzlich gute Voraussetzungen für eine Qualitätssicherung, doch diese geschieht nicht notwendigerweise von allein im ausreichenden Maße. Aus diesem Grund ist eine Kombination mit Zertifizierungen durch Stellen wie dem Bundesamt für Sicherheit in der Informationstechnik wünschenswert. Darüber hinaus arbeiten Institutionen in verschiedenen Nationen auf der Basis von Open-Source-Software an der Entwicklung von Programmen für mehr IT-Sicherheit [10] und empfehlen ihren Einsatz gerade in sicherheitsrelevanten Bereichen [5].

Welche der diskutierten Lösungen am günstigsten sind, hängt von vielen Faktoren ab und ist für jeden Einzelfall individuell zu entscheiden. Die Arbeit endet allerdings nicht mit der Auswahl und dem Aufbau eines Systems, sondern fängt dann erst richtig an, denn für den Bereich des Datenschutzes und der Datensicherheit gilt:

„Security is a process, not a product." – Bruce Schneier[7]

Literatur

[1] Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder : Transparente Software – eine Voraussetzung für datenschutzfreundliche Technologien; Stand: 2000-11-02; http://www.bfd.bund.de/technik/aktech1.html.

[2] AT&T Laboratories Cambridge: Virtual Network Computing (VNC); 1999; http://www.uk.research.att.com/vnc/.

[3] Helmut Bäumler: Der neue Datenschutz, in: Helmut Bäumler (Hg.): „Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen; Tagungsband zur Sommerakademie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, August 1998 in Kiel; Luchterhand, Neuwied 1998; 1-10.

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ausführbare Inhalte – Sicherheitsrisiken und Lösungen; Bonn 1999; http://www.bsi.de/activein/aktiv.html.

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI): Empfehlungen zum Schutz vor verteilten Denial of Service-Angriffen im Internet; Version 1.1 vom 2000-06-20; Bonn; http://www.bsi.de/ddos.html.

[6] Gnu Privacy Guard; http://www.gnupg.org/.

[7] Kristian Köhntopp, Marit Köhntopp, Andreas Pfitzmann: Sicherheit durch Open Source? Chancen und Grenzen; in: Datenschutz und Datensicherheit (DuD) 24/9 (2000); Vieweg, Wiesbaden 2000; 508-513; http://www.koehntopp.de/marit/publikationen/opensource/KoeKP_00SicherheitOpenSource.pdf.

[8] Marit Köhntopp: Das virtuelle Datenschutzbüro; in: Helmut Bäumler (Hg.): E-Privacy; Tagungsband zur Sommerakademie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, 28. August 2000 in Kiel; Vieweg, Wiesbaden 2000; 291-304.

[9] LIDS (Linux Intrusion Detection System); http://www.lids.org/.

[10] National Security Agency: Security Enhanced Linux; http://www.nsa.gov/selinux/; Pressemitteilung vom 2001-01-02; Fort George G. Meade, Maryland; http://www.nsa.gov/releases/selinux_01022001.html.

[7] Siehe http://www.counterpane.com/.

[11] Henk van Rossum, Huib Gardeniers, John Borking u.a.: Privacy-Enhancing Technologies: The Path to Anonymity, Volume I u. II; Achtergrondstudies en Verkenningen 5a/5b; Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Canada; August 1995; http://www.ipc.on.ca/english/pubpres/sum_pap/papers/anon-e.htm.

[12] RSBAC (Rule Set Based Access Control); http://www.rsbac.org/.

[13] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Safer surfen – selbst sichern; Kiel 2000; Abschnitt zu aktiven Inhalten: http://datenschutz.inside.tm/safer/browser/actcntnt/index.htm.