Joachim Wenzel

Seelsorge auch im Internet? - Aber sicher!

Inhalt

Beratung und Seelsorge per Internet bereits Realität

Am Internet als der zentralen Kommunikationsplattform der Gesellschaft im heutigen Informationszeitalter geht nichts mehr vorbei. So ist es nur natürlich, dass auch Beratung und Seelsorge in diesem medial vermittelten Bereich zur virtuellen Realität werden. Dabei muss es sich nicht einmal um ausdrückliche "Internetseelsorge" handeln. So wie Menschen in Not an der Haustür eines Pfarrhauses klingeln oder die Telefonnummer einer Seelsorgeeinrichtung wählen, so nutzen verzweifelte Menschen auch das Internet, um mit Seelsorgerinnen und Seelsorgern zu kommunizieren, ob dies ausdrücklich angeboten wird oder nicht. Allein über eine vorhandene Homepage (die eigentlich nur der Öffentlichkeitsarbeit dienen sollte) wurden Seelsorgeanfragen per E-Mail an TelefonSeelsorge-Stellen heran getragen, auch als diese das Medium E-Mail noch nicht als mögliche Form seelsorglicher Kommunikation angeboten hatten.
Die TelefonSeelsorge hat dabei das Internet als Kommunikationsplattform der nahen Zukunft für Beratung und Seelsorge ziemlich früh erkannt und als spezielles Angebot fachlich und technisch weiterentwickelt, so dass die ersten TelefonSeelsorge-Mitarbeiter/innen bereits als Pioniere der Internetberatung gelten.

Internet bewirkt Datenschutzprobleme neuer Qualität

Das Internet bietet fast unbegrenzte Möglichkeiten der Information und Kommunikation. In gleicher Weise steigern sich dabei aber auch die Problemstellungen hinsichtlich Datenschutz in einem bis dahin nicht gekannten Ausmaß. Dieser Entwicklung will sich die TeleonSeelsorge aktiv stellen:
In früheren Zeiten waren Computer von anderen Computern meist völlig getrennt. Eine Vernetzung wurde höchstens punktuell betrieben. Durch die globale Vernetzung des Internets sind jedoch Zugriffe von außen verhältnismäßig einfach möglich, wenn keine geeigneten Gegenmaßnahmen wie effektive Firewall- und Virenwall-Lösungen ergriffen werden. Dabei wird deutlich: Sicherheit ist auch im Internet machbar - allerdings nur, wenn ein Gesamtkonzept realisiert wird, das die unterschiedlichsten Sicherheitsdimensionen berücksichtigt. Ansonsten ist das Internet alles andere als anonym: Ausspionieren ungesicherter Inhalte und Kommunikationen ist an der Tagesordnung. Sobald personenbezogene Daten auf einem ungesicherten PC gespeichert sind, der (direkt oder indirekt per Netzwerk) an das Internet angeschlossen ist, sind Datenschutz und ggf. sogar Seelsorgegeheimnis in Gefahr:

Gefahren im Internet:
Die Gefahren durch die Internetvernetzung werden fälschlicherweise oft mit dem Telefonieren gleichgesetzt. Dies ist jedoch nicht angemessen. Um das Telefonieren abhören zu können, bedarf es aufwendiger technischer Mittel, die nicht ohne weiteres zu beschaffen sind. Im Internet haben hingegen oftmals sogar Jugendliche das nötige Know-How: Im Netz gibt es Seiten, die detailliert erklären, wie man per Internet auf Computer zugreifen kann, die nicht ausreichend gesichert werden. Zusätzlich gibt es sogar Software-Tools, die man kostenlos herunterladen kann, um auf ungesicherte PCs und Netzwerke zugreifen zu können: Weder Bereitstellung dieser Informationen und Software-Tools noch das Downloaden sind strafbar, was die Ausbreitung solchen Wissens und solcher Technik sehr leicht macht.

Nachfolgend eine Auflistung zentraler Sicherheitsrisiken bei Internetvernetzung:

Risiko Internet-Zugang und Zugangs-Provider:
Der Internetzugang stellt den zentralen Unsicherheitsfaktor in der heutigen Zeit dar. Er macht den PC oder das Netz vor Ort angreifbar.
Risiko Hacker:
Selbst "Hobby-Surfer" finden im Internet nahezu alles, was nötig ist, um ungesicherte Computer ausspähen zu können und diese aus der Ferne zu steuern.
Risiko Internet-Speicherplatz-Provider:
Diese sind z.T. Ein-Personen-Firmen irgendwo auf der Welt. Sie haben meist unbeschränkten Zugriff auf alle Daten (z.B. E-Mails) ihrer Kunden und deren Kommunikationen.
Risiko nicht ausgebildeter MitarbeiterInnen:
Mangelndes Sicherheitsbewusstsein und mangelnde Kenntnisse bei den MitarbeiterInnen öffnen Sicherheitslücken.
Risiko PCs und Software:
Fehlerhafte Einstellungen am PC und nicht aktualisierte Software führen zu Sicherheitslücken und öffnen für Zugriffe von außen Tür und Tor.
Risiko unverschlüsselte Kommunikation im Internet:
Durch die technischen Gegebenheiten von Netzwerken werden Daten irgendwo zwischengespeichert; meist ohne dass ersichtlich ist, wo und wann und in welchem Ausmaß und wer die Daten lesen kann. Selbst das Versenden von Postkarten ist demgegenüber wesentlich sicherer.
Risiko halbherzige Sicherheitskonzepte:

Oft wird die Vordertür sicher verschlossen, während zahlreiche Hintertüren weit offen bleiben.
Risiko mangelhafte oder fehlende Sicherheitsrichtlinien:
In der Praxis existieren diese oft überhaupt nicht oder sind für Laien unverständlich formuliert. Um einen sicheren Umgang mit vertraulichen Daten zu gewährleisten, müssen die Risiken sowohl auf der technischen wie auf der personellen Ebene berücksichtigt und in ein Gesamtkonzept integriert werden.
Risiko EDV-Fachleute:
EDV-Fachleute werden häufig automatisch als fachkundig im komplexen Themenbereich Datensicherheit / Datenschutz angesehen. Häufig sind EDV-Fachleute jedoch nicht gleichzeitig Fachleute im Bereich Internetsicherheit.

Gesellschaftspolitisches Engagement der TelefonSeelsorge

Die TelefonSeelsoge will es nicht alleine der Technikentwicklung überlassen, die vielfach durch wirtschaftliche Interessen vorangetrieben wird, ob sich die Kommunikationsmedien zum Nutzen der Menschen entwickeln oder nicht. So wurden die Vertreter/innen der TelefonSeelsorge auch gesellschaftspolitisch aktiv und haben sich stets für eine datenschutzfreundliche Entwicklung in der Telekommunikation eingesetzt. Dabei ist der möglichst weitgehende Schutz der Privatsphäre der ratsuchenden Menschen immer das erklärte Ziel. Die alleinige Verantwortung für die Sicherheitsfragen den Nutzern der Kommunikationstechnologien zuzuschreiben macht dabei keinen Sinn, denn es handelt sich hier um eine immer komplexer werdende Technik, die von einem durchschnittlichen Internetnutzer nicht mehr zu überblicken ist. Selbst Fachleute können den gesamten Kompetenzbereich fachlich kaum abdecken und sind auf Kollegen benachbarter Spezialgebiete angewiesen.
Konkrete Erfolge kann die TelefonSeelsorge in ihrem jahrelangen Engagement verzeichnen: So wird die TelefonSeelsorge nun auch ausdrücklich in einem Bundesgesetz genannt. Durch das Telekommunikationsgesetz wird dabei sichergestellt, dass bei einem Anruf zu einer sozialen oder kirchlichen Einrichtung, die anonyme Beratung anbieten, die Nummer nicht im Einzelverbindungsnachweis (EVN) auftauchen darf. Nur so ist zu gewährleisten, dass ein Anruf bei der TelefonSeelsorge nicht in der monatlichen Auflistung des EVN erscheint. In einer Partnerschaft mit der Deutschen Telekom AG wird dies realisiert, indem die Anrufe durch das 0800er-Free-Call-System gebührenfrei zur TelefonSeelsorge möglich sind.
Mittlerweile ist die TelefonSeelsorge aber auch Vorreiterin in praktischen Fragen des Datenschutzes und der Datensicherheit im Bereich Internet geworden, was bereits von Datenschützern und Fachleuten aus dem Bereich IT-Sicherheit anerkannt wird. Die Beweggründe der TelefonSeelsorge zu sicherer und datenschutzverträglicher Beratung und Seelsorge sollen nachfolgend veranschaulicht werden. Dabei können die konkreten Hinweise und Links auch anderen kirchlichen Einrichtungen dazu dienen, selbst eine sichere und datenschutzverträgliche Infrastruktur für Kommunikation im Internet und gleichzeitig eine sichere interne Vernetzung per Intranet aufzubauen. Mit Hilfe einer solchen Infrastruktur ist es sogar möglich, anonym und vertraulich Seelsorge und Beratung per Internet anzubieten und auch in der sonstigen Alltagspraxis trotz Internetnutzung das Seelsorgegeheimnis und den Datenschutz effektiv zu wahren.

Niederschwelligkeit und Sicherheit

Von Anfang an gehörte die Niederschwelligkeit des Zugangs zum zentralen Konzept der TelefonSeelsorge. Die Niederschwelligkeit der Telefonkommunikation konnte durch das Internet noch weiter herunter gesetzt werden. Für die TelefonSeelsorge wurde jedoch ziemlich schnell deutlich, dass Niederschweilligkeit nicht um jeden Preis geschehen darf:
Ratsuchende Menschen durch die seelsorgliche Beratungssituation der Gefahr auszusetzen, sehr einfach ausspioniert und vielleicht sogar durch die Preisgabe intimer Details erpresst werden zu können, wurde dabei nach Analyse der tatsächlichen Sicherheitsrisiken ausgeschlossen. Die TelefonSeelsorge wollte eher auf diese Form der Seelsorge und Beratung verzichten als gegen die eigenen Grundsätze zu verstoßen: nämlich gegen Vertraulichkeit, Verschwiegenheit und Anonymität. Schließlich würde die TelefonSeelsorge ihre Beratung und Seelsorge beispielsweise nicht innerhalb einer Fernsehsendung anbieten. Bei ungesicherter E-Mailberatung wäre es aber dauerhaft der Fall, dass die Kommunikation in der Öffentlichkeit des Internets stattfinden würde und das sogar noch unbemerkt.
Glücklicherweise zeigte sich bei der Realisierung der sicheren und datenschutzfreundlichen Kommunikationsplattform, dass Niederschwelligkeit nicht im Gegensatz zu Sicherheit stehen muss: In den Monaten vor und nach der Einführung des neuen Systems blieben die Maileingangszahlen konstant. Die recht kleine Hürde der Eingabe von Benutzernamen und Passwort führte also nicht dazu, dass sich weniger Menschen im Internet an die TelefonSeelsorge wandten. Gleichwohl sind aber auch andere Zugangshürden damit weggefallen. So kann in diesem neuen webbasierten System eine Mail nicht einfach verloren gehen

wie dies in Zeiten unzähliger Spam- und Virenmails bei der regulären E-Mail (smtp/POP3) immer häufiger der Fall ist.
Das Telefon war für die TelefonSeelsorge seit ihrer Gründung in Deutschland 1956 das zunächst einzig mögliche Mittel, um niederschwellige Hilfe anbieten zu können.
Inzwischen entstand durch das Internet mit seinen medialen Möglichkeiten ein noch niederschwelligeres Hilfsangebot: Es können sich nun auch Menschen an die TelefonSeelsorge wenden, die sich nicht in der Lage fühlen, über ihre Probleme zu sprechen und ihre Stimme preiszugeben, die aber in Schriftform nach Worten suchen.
Dabei kann die mediale Weiterentwicklung bedeuten, in neuer und noch niederschwelligerer Weise die ursprüngliche Zielsetzung zu realisieren, nämlich "hilflosen und verzweifelten Menschen durch die TelefonSeelsorge vertrauliche und unentgeltliche Hilfe" anzubieten.
TelefonSeelsorge im Internet versteht sich so als konsequente Weiterentwicklung des bereits vorhandenen und allgemein anerkannten Hilfsangebotes bei neuen technischen und medialen Möglichkeiten. Dies aber ausschließlich in angemessen sicheren virtuellen Kommunikationsräumen.

Das Recht auf Datenschutz als Teil der christlichen Wertordnung

Die TelefonSeelsorge legt auf die konsequente Realisierung des Datenschutzes großen Wert, weil nur so die Umsetzung ihrer zentralen Grundsätze "Vertraulichkeit, Verschwiegenheit und Anonymität" garantiert werden können.
Die TelefonSeelsorge ist dabei als ökumenische Einrichtung sowohl der katholischen als auch den evangelischen Datenschutzregelungen verpflichtet und will die Richtlinien der Katholischen Kirche, wie sie hier auf der Homepage beschrieben werden, auch in ihrer Praxis der Online-Beratung verwirklichen:
"Die Katholische Kirche hat bereits 1983 mit dem neuen Kirchenrecht, dem Codex Iuris Canonici (CIC) ein Fundamentalrecht auf Datenschutz geschaffen. Zu den anerkannten Rechten der Christgläubigen gehört seitdem auch der Schutz der Intimsphäre. Can. 220 CIC lautet: 'Niemandem ist es erlaubt, den guten Ruf, den jemand hat, rechtswidrig zu schädigen und das Recht irgendeiner Person auf Schutz der eigenen Intimsphäre zu verletzen.' Wie alle Bestimmungen des CIC hat dieser Grundsatz nicht nur juristische Bedeutung, sondern nimmt auch Anteil am Menschenbild der Kirche. Jeder soll die Möglichkeit haben, seinem Gewissen zu folgen und entsprechend zu handeln. Hierfür ist der Schutz der Intimsphäre wesentliche Voraussetzung. Für die Kirche ist das nicht neu. So hat das Beicht- und Seelsorgegeheimnis bereits eine lange Tradition. Im Zeitalter der Informations- und Kommunikationstechnik reicht das allein aber nicht mehr aus."
Das christliche Menschenbild hat schließlich auch in diesem Bereich Einzug in die Rechtsordnung der westlichen Welt genommen: Die Charta der Grundrechte der Europäischen Union (Nizza, 7.12.2000) nennt dieses Grundrecht ausdrücklich in Artikel 8: "Schutz personenbezogener Daten".
Im Grundgesetz der Bundesrepublik Deutschland ist dieses Recht nicht ausdrücklich genannt. Das Bundesverfassungsgericht hat jedoch in einem Urteil aus dem Jahr 1983 aus Artikel I Absatz I GG (Schutz der Menschenwürde) und aus Artikel 2 Absatz I GG (Freiheitsgrundrecht) allgemeinen ein 'Grundrecht auf informationelle Selbstbestimmung' abgeleitet. Dieses Grundrecht, kurz 'Recht auf Datenschutz' genannt, ist danach Grundbedingung für eine menschen- und bürgerrechtskonforme demokratische Informationsgesellschaft.
Unmittelbare Rechtsgrundlage für die TelefonSeelsorge sind das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) und die Anordnung über den kirchlichen Datenschutz (KDO) des Verbandes der Diözesen Deutschland.
Darüber hinaus setzt die TelefonSeelsorge aber auch auf eine Zusammenarbeit mit den Datenschutzbeauftragten von Bund- und Ländern, da sie auch gesellschaftspolitisch die Rahmenbedingungen für eine menschenfreundliche Kommunikationstechnik mitgestalten will.

Ethische Frage: Schutz der beteiligten Menschen

Datenschutz ist letztlich nur durch ethische Fragestellungen zu begründen. In der Praxis können Datenschutz- und Sicherheitskonzepte dabei aber auch die Vertrauenswürdigkeit eines Anbieters im Internet herausstellen. Im monetären Bereich sind umfassende Sicherheitskonzepte seit vielen Jahren bereits die Normalität: Eine Bank, die Kreditkartennummern im Internet ohne Verschlüsselung abfragt, ist kaum denkbar. Es würde als unverantwortlich gelten, wenn ein seriöses Unternehmen seine Kunden dazu verleiten würde solche sensiblen Daten ungeschützt zu übermitteln. Der Schutz von Privatpersonen, die persönlichste Dinge von sich preisgeben, wurde in der Vergangenheit vielfach noch nicht als entsprechend schützenswert erachtet.
Die TelefonSeelsorge sieht im Gegensatz dazu eine sichere und datenschutzkonforme Kommunikation im Internet im Einklang mit den oben genannten Grundrechten als notwendige Voraussetzung für ihre

Seelsorgetätigkeit im Internet an. Wie beispielsweise das Beichtgeheimnis zum Schutze der Beichtenden gilt - unabhängig ob diese davon Kenntnis haben - so will die TelefonSeelsorge nach ihrem Sicherheitskonzept auch für einen vertraulichen Rahmen, der dem Seelsorgegeheimnis angemessen ist, vorab sorgen. Schweigepflicht und Seelsorgegeheimnis machten schließlich keinen Sinn, wenn unkalkulierbar viele unbekannte Menschen Zugriff auf die Seelsorgekontakte der TelefonSeelsorge hätten, wie dies im Internet ohne Sicherheitskonzept der Fall wäre.
Die TelefonSeelsorge ist bereits seit 1995 im Internet tätig, um Menschen mit Sorgen und Nöten möglichst niederschwellig zu erreichen. Sicherheits- und Datenschutzfragen waren damals in der Gesellschaft bezüglich Internet noch kaum im Blick. Dennoch wurde bei der eMailberatung frühzeitig eine optionale PGP-Verschlüsselung angeboten. Diese Technik wurde zuletzt (2002) jedoch von weniger als 1% der Ratsuchenden genutzt. Offensichtlich war der Verschlüsselungsvorgang zu kompliziert.
Die TelefonSeelsorge Deutschland hat deshalb seit dem 9.9.2002 bei ihrer Internetberatung ein umfassendes Sicherheitskonzept für den Schutz der Ratsuchenden realisiert. Die TelefonSeelsorge will dadurch auch den Menschen vertrauliche Kommunikation bieten, die eine Verschlüsselungstechnik per eMail nicht beherrschen oder in ihrer Notsituation nicht in der Lage sind, eine Verschlüsselungstechnik zu installieren. Die Verantwortung diesbezüglich allein den sogenannten "mündigen Nutzern" des Angebots zu überlassen wäre dabei fast zynisch, ist doch bekannt wie wenig die Menschen tatsächlich über diese komplexe Hintergrundtechnik wissen können.
Vielmehr sollen die Ratsuchenden der TelefonSeelsorge darauf vertrauen können, dass alles Mögliche für ihren Schutz unternommen wurde. Schließlich ist es für eine Organisation leichter machbar, vertrauliche und sichere Kommunikationswege zur Verfügung zu stellen als es Menschen möglich ist, die in einer akuten Notlage sind, sich mit speziellen Verschlüsselungstechniken auseinander zu setzen.
Die technischen Kenntnisse der durchschnittlichen Nutzer des Internets werden leider immer geringer. Die TelefonSeelsorge will es dabei also nicht dem Zufall überlassen, ob die Ratsuchenden geschützt sind oder nicht. Was Unbefugte mit den vertraulichen Informationen anfangen könnten ist schließlich nicht absehbar. Unzählige versierte Internetnutzer könnten die Ratsuchenden nicht nur erpressen, sie könnten sogar an Stelle und im Namen der TelefonSeelsorge selbst mit den Ratsuchenden kommunizieren ohne dass jemand eine Möglichkeit hätte dies zu bemerken.

Bewusstsein für Sicherheitsfragen wächst

Die "Pionierzeit des Internets" geht zu Ende. Wie bei anderen Techniken auch, wurde im Internet zunächst die Funktionalität weiter entwickelt. Auch beim Automobil beispielsweise wurde zunächst die Geschwindigkeit vorangetrieben. Erst später kamen Gurtpflicht und Airbag, um die Zahl der Verletzten und Toten zu minimieren.
In der Bevölkerung wächst derzeit das Bewusstsein zu Fragen der Sicherheit und der Anonymität erheblich. Ein solches Bewusstsein ist die Voraussetzung für vertrauliche Kommunikation im Internet, denn bedrohlich für Internetsicherheit und Datenschutz ist vor allem das Halbwissen, das vielfach über Internetkommunikation verbreitet wird:
Oft wird das Internet entweder als völlig unsicher beschrieben, wobei es angeblich keine wirkungsvolle Abhilfe gäbe oder es wird so getan, als sei die Kommunikation im Internet grundsätzlich nicht unsicherer als ein Telefonat oder eine Postkarte. Beide Positionen werden der Realität nicht annähernd gerecht und stellen somit unangemessenes oder sogar gefährliches Halbwissen dar.
Beachtet man keinerlei Sicherheitsmaßnahmen, so ist das Internet in der Tat sehr unsicher. Kennt man jedoch die zentralen Gefahren und weiß man bei gefährlichen Risiken Abhilfe zu schaffen, so kann das Internet im Gegensatz dazu sogar sehr sicher sein.

Nur umfassendes Sicherheitskonzept wirkt Gefahren entgegen

Nur ein umfassendes Sicherheitskonzept kann all diesen Gefahren entgegenwirken. Dabei gilt es vor allem die zentralen nachfolgend genannten Dimensionen von Sicherheit und Datenschutz zu gewährleisten:

- Authentizität des Anbieters (Sicherstellung um welche Organisation es sich handelt)
- Anonymität des Nutzers (Anonymisierungsdienst zusätzlich nutzbar)
- Vertraulichkeit (Inhalte können unterwegs nicht gelesen werden)
- Integrität (Inhalte können unterwegs nicht verändert werden)
- Verbindlichkeit (Inhalte können nicht unbemerkt verloren gehen)
- Datensparsamkeit (Standardisierte Löschvorgänge werden eingeplant)

Für sensible Informationen und personenbezogene Daten würden zur Umsetzung dieser Anforderungen reine Softwarelösungen nicht ausreichen (bsp. Desktop-Firewall). Vielmehr muss ein Gesamtkonzept auf

verschiedenen Ebenen ansetzen, um in der Praxis die notwendige Wirkung zu erzielen: Ein solches Sicherheitskonzept muss mindestens folgende Bereiche umfassen: Organisation, Hardware, Software, Netze, Administration, datenschutzrechtliche Bewertung und Mitarbeiterschulung.

Empfehlung eines Landesbeauftragten für Datenschutz

Der Landesbeauftragte für Datenschutz Sachsen-Anhalt empfiehlt das Konzept, das die TelefonSeelsorge realisiert hat, ausdrücklich in seinem offiziellen VI. Tätigkeitsbericht. Dabei werden die zentralen Punkte des als "Sewecom-Standard" beschriebenen Sicherheitskonzepts zusammengefaßt:
"Grundaussage ist, dass Beratungseinrichtungen, gleich ob öffentliche oder private, die über das Internet mit Klienten, Bürgern und Kunden kommunizieren wollen, die Frage der Sicherheit nicht dem jeweiligen Nutzer überlassen, sondern von vornherein sichere Kommunikationswege zur Verfügung stellen sollten.
Unter anderem hat die TelefonSeelsorge Deutschland aufgrund der bekannten Sicherheitsrisiken bei der E-Mail-Beratung eine Alternative gesucht und eine webbasierte Beratung nach dem neuen Sicherheitsstandard realisiert. Auf das Versenden von E-Mails wird jetzt völlig verzichtet.
Der Ratsuchende meldet sich bei der TelefonSeelsorge mit einem beliebigen Nutzernamen und einem Kennwort an. Danach kann er sein Problem schildern und bekommt nach ca. 48 Stunden "Antwort" in der Form, dass er sich wiederum anmeldet und die Antwort des Beraters abrufen kann. Der gesamte Beratungskontakt verbleibt auf dem Server der TelefonSeelsorge, der u.a. durch eine Firewall und eine Viruswall gegen Zugriffe und Angriffe von außen gesichert ist.
Zum einen wird auf diese Weise die Anonymität gewahrt, da der Nutzer keine E-Mail-Adresse angeben muss, die personenbeziehbar ist und zum anderen wird die Übertragung der Daten im Internet automatisch durch eine SSL-Verschlüsselung gesichert.
Durch das SSL-Zertifikat, das vom Trust-Center der Deutschen Telekom AG (TeleSec) ausgestellt wurde, kann der Nutzer außerdem regelmäßig davon ausgehen, dass es sich bei dem Anbieter tatsächlich um die TelefonSeelsorge handelt.
Die Deutsche Telekom AG als privates Unternehmen unterliegt zugleich der Datenschutzkontrolle des Bundesbeauftragten für den Datenschutz. Damit ist sichergestellt, dass eine Kontrolle der einzuhaltenden datenschutzrechtlichen Bestimmungen erfolgt. Bei einem Zertifikatsanbieter außerhalb des Geltungsbereiches des Grundgesetzes wäre dies nicht so einfach.
Die beschriebene Lösung ist jedoch nicht nur für Einrichtungen zu empfehlen, die anonyme Beratung gewährleisten müssen oder wollen, sondern generell für öffentliche Stellen, die den Bürgerinnen und Bürgern eine sichere Kommunikationsmöglichkeit ohne vorherige Installation einer Verschlüsselungssoftware und aufwendige Schlüsselverwaltung zur Verfügung stellen wollen."

Kostenersparnis durch Synergie-Effekte

Eine einzelne TelefonSeelsorge-Stelle hätten ein solch komplexes Datenschutz- und Sicherheitskonzept nicht realisieren können. Dazu hätten weder die zeitlichen, fachlichen noch finanziellen Möglichkeiten einer einzelnen Stelle ausgereicht. Nur durch eine gemeinsame Strategie, ein gemeinsames Konzept, eine gemeinsame Infrastruktur und ein gemeinsames Projekt zur Umstellung auf die neue Kommunikationsplattform war es möglich, hier neue Wege zu gehen und damit ein hohes Sicherheits- und Datenschutzniveau zu ermöglichen.
Durch die Realisierung des gemeinsamen Gesamtkonzepts sind alle beteiligten PCs und Netzwerke der TelefonSeelsorge-Stellen durch zentrale und effektive Firewall- und Virenwall-Lösungen geschützt. Die Sicherheitstechnik wird dabei von speziell ausgebildeten Fachleuten administriert. Nur so ist zu gewährleisten, dass die Schutzmaßnahmen auf dem aktuellen Stand der Technik bleiben. Dies ist notwendig, weil sich die Angriffsformen immer häufiger und immer schneller verändern. Diese Infrastruktur ist nur bezahlbar, weil sie von vielen kirchlichen Stellen genutzt wird und somit für die einzelnen Einrichtungen finanzierbar bleibt.
Auch die Entwicklung der Server-Software wäre von einer einzelnen Stelle wohl kaum zu bezahlen gewesen. Bei der Server-Software wurde auf PHP und MySQL gesetzt, um auch hier eine zukunftssichere und bezahlbare Lösung im Open-Source-Umfeld schaffen zu können, die auch weiterentwickelt werden kann, ohne dass diese Investitionen jeweils von den einzelnen Institutionen getätigt werden müßten.
Für eine einzelne Einrichtung käme auch noch ein weiteres Problem hinzu: Es ist schwierig überhaupt eine Firma zu finden, die ein komplexes Sicherheitsprojekt überhaupt realisieren kann. Es gibt kaum Dienstleister, welche die gesamte Fragestellung fachlich abdecken. Leider erkennen und / oder benennen dabei auch zahlreiche EDV-Dienstleister ihre eigenen Grenzen hinsichtlich ihrer fachlichen Kompetenzen bezüglich Datensicherheit und Datenschutz im Internet nicht. Außerdem muss die Gesamtlösung ja auch mit den eigenen rechtlichen Datenschutzbestimmungen im Einklang sein. So wurde die zentrale Steuerung und

Koordinierung des Projekts zur Schaffung einer gemeinsamen Infrastruktur auch zu einer Entlastung für die Verantwortlichen der einzelnen Stellen.
Über die gemeinsame sichere Infrastruktur und Kommunikationsplattform können jetzt prinzipiell die unterschiedlichen Formen medialer Kommunikation webbasiert und datenbankgesteuert genutzt werden: Mail, Chat, Foren. Sogar die Anbindung an ein si cheres Intranet (inkl. Groupware-Lösung oder E-Learningmodul auf Open-Source-Basis) ist leicht möglich, da die Stellen dabei schon in einem gemeinsamen "virtual private network" (vpn) vernetzt sind.

Konzept der TelefonSeelsorge dient vielfach als Modell

Immer mehr Organisationen, Verbände und Unternehmen entwickeln derzeit Sicherheitskonzepte in Anlehnung an das Konzept der TelefonSeelsorge. Fachleute und Institutionen aus dem Bereich Datenschutz und Datensicherheit erachten dieses Konzept dabei als zukunftsweisend.
Darüber hinaus ist es möglich, dass mit der Software der TelefonSeelsorge ein "Open-Source-Projekt" gestartet wird. Dabei könnte diese Server-Software so weiterentwickelt werden, dass sie von den unterschiedlichsten Institutionen kostenlos übernommen und an den eigenen Bedarf optimal angepasst werden kann. Außerdem würde die Software zuvor von einer unabhängigen Datenschutz-Institution geprüft werden.
Dies würde bedeuten, dass die Software für eine sichere und datenschutzverträgliche Kommunikationsplattform auch von kirchlichen Einrichtungen kostenlos heruntergeladen werden könnte. So wäre eine Umsetzung des Sicherheitskonzepts der TelefonSeelsorge in den verschiedensten Bereichen preisgünstig realisierbar.
Mit dem hier benannten Konzept und den unten aufgeführten Links ist es vielleicht möglich, auch andere Einrichtungen zu einer vergleichbaren Vorgehensweise zu motivieren, wie dies bei der TelefonSeelsorge bereits der Fall ist:

Seelsorge auch im Internet? - Aber sicher!

Literatur

- VI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt vom 01.04.2001 - 31.03.2003 / Kapitel 12: Hinweise zum technischen und organisatorischen Datenschutz: 12.5 Sichere Kommunikation im Internet
- Eisenbach-Heck, Cordula / Weber, Traugott: Sechs Jahre "TelefonSeelsorge im Internet". Ein Bericht über die Entwicklung der E-Mail-Beratung. In: Etzersdorfer, Elmar / Fiedler, Georg / Witte, Michael (Hrsg.): Neue Medien und Suizidalität. Gefahren und Interventionsmöglichkeiten. Göttingen 2003. S. 73-86.
- FOCUS Nr. 52 vom 20.12.2003 (Print- und Onlineausgabe)
  Beratung: Erste Hilfe für die Seele. Die Telefonseelsorge hilft Ratsuchenden per E-Mail und im Chat. Zur Sicherheit verschlüsselt sie die digitale Korrespondenz, S. 102
  http://focus.msn.de/F/2003/52/Internet/seelsorge/seelsorge.htm
- Knatz, Birgit / Dodier, Bernard: Hilfe aus dem Netz. Theorie und Praxis der Beratung per E-Mail. Stuttgart 2003.
- Wenzel, Joachim: Telefonseelsorge. In: Bäumler, Helmut / Breinlinger, Astrid / Schrader, Hans-Hermann (Hrsg.): Datenschutz von A - Z. Neuwied / Kriftel 1999 (Grundwerk). 7. Lfg. Juni 2003: Gruppe: T 350. S. 1-4.
- Wenzel, Joachim: e-Mail-Management. Neues Mailkonzept für Behörden. In: Kommune21. eGovernment, Internet und Informationstechnik. Ausgabe 6/2003. S. 38.
- Wenzel, Joachim: Vertraulichkeit und Anonymität im Internet. Problematik von Datensicherheit und Datenschutz mit Lösungsansätzen. In: Etzersdorfer, Elmar / Fiedler, Georg / Witte, Michael (Hrsg.): Neue Medien und Suizidalität. Gefahren und Interventionsmöglichkeiten. Göttingen 2003. S. 56-70.

Links

Homepage der TelefonSeelsorge:
www.telefonseelsorge.de

Zusammenfassung des Sicherheitskonzepts der TelefonSeelsorge:
www.sewecom.de/telefonseelsorge/sicherheitskonzept

Der Sewecom-Standard für sichere Kommunikation im Internet als Grundlage des TS-Konzepts:
www.sewecom.de/sewecom-standard
www.sewecom.de/sewecom-abbildung.pdf (Visuelle Darstellung)

Sicherheits-Provider der TelefonSeelsorge (VPN-Vernetzung):
www.kondek.de

Themenportal "Sichere Internetkommunikation":
www.sewecom.de/sichere-internetkommunikation

Auszug aus dem VI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt:
www.datenschutz.sachsen-anhalt.de/tb/tb6/kap12-5.htm

Gefahren / Risiken im Internet konkret:
www.sewecom.de/datenschutz/risiken-im-netz
www.sewecom.de/datenschutz/szenarien

Hintergrundinformationen zu "Open-Source":
www.sewecom.de/open-source

Die umfassenden PC-Sicherheits-Tipps für alle Internetnutzer:
www.sewecom.de/pc