Sewecom-Verfahren

secure web communication

Konzept für sichere Kommunikation im Internet

Aktuelle Version vom 15. Dezember 2005

Internetadresse: www.sewecom.de/sewecom-verfahren

Übersicht

Abbildung des Sewecom-Verfahrens

A) Organisation

A1) Gesamtkonzept erforderlich
A2) Leitungsebene der Organisation ist eingebunden
A3) Konkretes Sicherheitskonzept: Prozess definieren
A4) Sicherheitsbeauftragte
A5) Interne Sicherheitsrichtlinien und -standards werden definiert
A6) Schulung der Mitarbeiter/innen
A7) Mehrstufige Sicherheitsebenen / Stufenkonzept
A8) Beteiligte PCs, Software und Netzwerke
A9) Informations- und Kommunikationskonzept

B) Internet-Technik

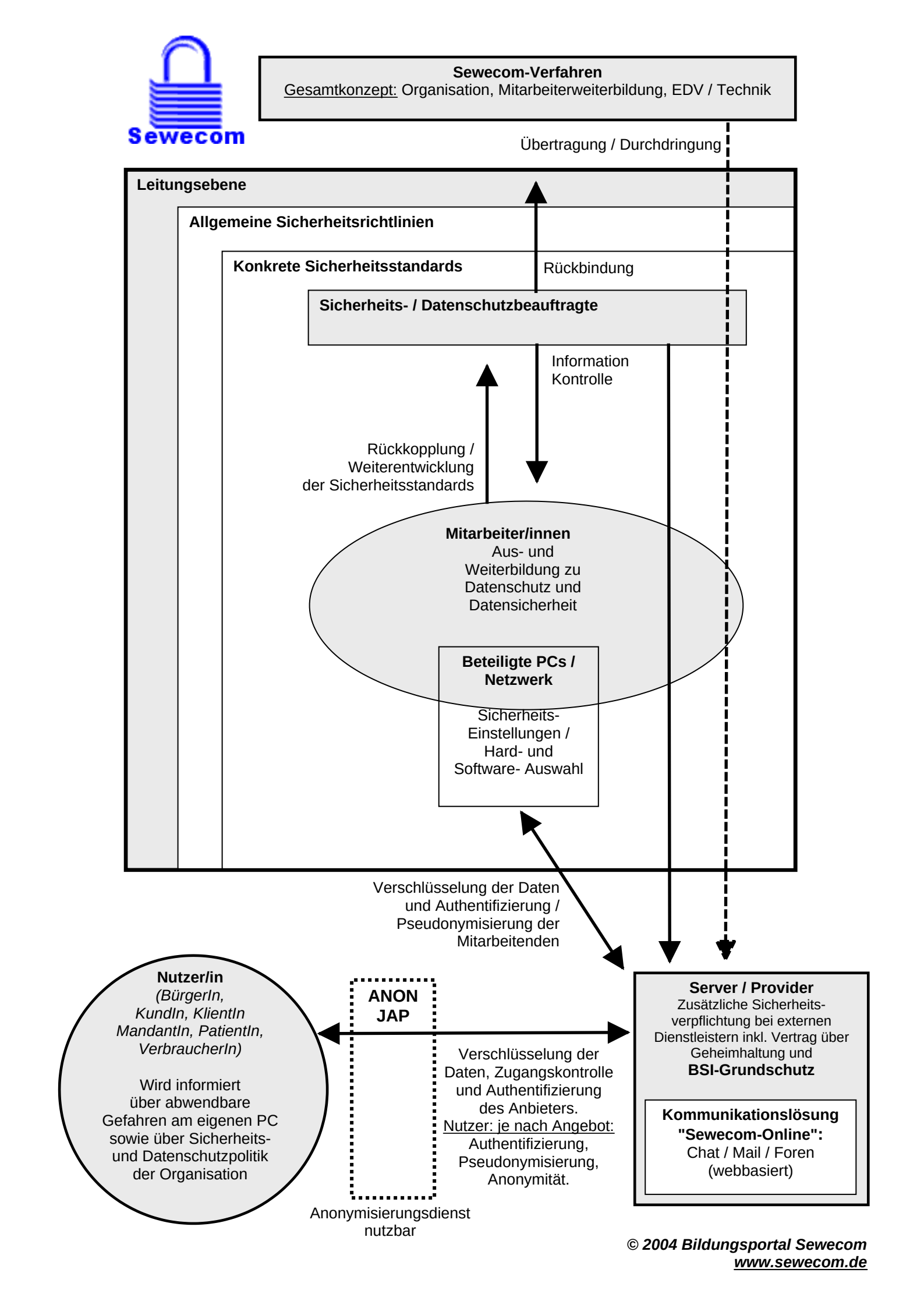
B1) Problem Outsourcing
B2) Technische Sicherheits-Infrastruktur
B3) Sichere Server-Infrastruktur
B4) VPN - virtual private network
B5) Administrative Zugänge zu Servern besonders gesichert
B6) Kommunikationslösung geschieht webbasiert
B7) SSL-Server-Zertifizierung nach Signaturgesetz
B8) Intranet besonders gesichert
B9) Systemüberwachung

C) Darstellung nach Außen

C1) Aufklärung der Nutzer
C2) Erklärung zu Datenschutz und Datensicherheit / Privacypolicy

D) Varianten: Anonymität / Authentizität

D1) Organisation authentifiziert / Nutzer anonym
D2) Organisation authentifiziert / Nutzer authentifiziert
D3) Rechtsverbindliche Kommunikation: Verträge per Internet



Das Sewecom-Verfahren

A) Organisation

A1) Gesamtkonzept erforderlich

Bei einem Sicherheitskonzept nach dem Sewecom-Verfahren handelt es sich um ein umfassendes Gesamtkonzept, das alle beteiligten Personen und technischen Komponenten einer Organisation sowie die ggf. beteiligten externen Dienstleister umfasst. Als Organisation wird hier das Gesamtsystem (Konzern, Unternehmen, Dachverband, Einrichtung) verstanden, welches das Sicherheitskonzept entwickelt und realisiert. Nur wenn alle relevanten Bereiche in das Konzept integriert sind, kann dabei ein hohes Maß an Sicherheit gewährleistet werden. Nur dann entspricht das Sicherheitskonzept dem Sewecom-Ansatz. (Überblick: Sewecom-Abbildung)

A2) Leitungsebene der Organisation ist eingebunden

Sicherheit muss von der obersten Leitungsebene gewollt sein und vorangetrieben werden. Sicherheitsstandards, die nicht eingefordert werden können, erweisen sich schnell als unwirksam, weil sie in Vergessenheit geraten oder ohne Folgen untergraben werden können. Nur wenn sich die Leitungsebene ebenfalls die Sicherheitsthematik zu Eigen macht und diese bei Bedarf einfordert, ist eine Realisierung von wirksamen Sicherheitsstandards in der Organisation zu erreichen. Sicherheitsberatung von außen darf in diesem Sinne ausschließlich als Begleitung verstanden werden. Nur wenn die Verantwortung für Datenschutz und Datensicherheit in der Leitungsebene der Organisation verankert wird, kann ein für die Organisation angemessenes Sicherheitskonzept nachhaltig wirksam werden. Von außen können Beratung oder technische Komponenten eingekauft werden, die Verantwortung für den Sicherheitsbedarf sowie für die Entwicklung und Realisierung des jeweiligen konkreten Sicherheitskonzepts nach dem Sewecom-Verfahren verbleiben jedoch in der Organisation selbst.

A3) Konkretes Sicherheitskonzept: Prozess definieren

Datensicherheit darf nicht als etwas Statisches missverstanden werden, das einmal eingekauft werden kann und dann für immer da ist. Vielmehr ist Sicherheit in einer Organisation als Prozess zu verstehen, der sich der Veränderung der Umwelt anpassen muss. Im konkreten Sicherheitskonzept wird somit ein Prozess definiert, der alle Abläufe und beteiligten Personen mit ihren jeweiligen Aufgaben erfasst. Dabei werden unterschiedliche Kommunikationswege ermöglicht, die selbst bei möglichen Störungen eine zielgerichtete Alarmierung ermöglichen.

A4) Sicherheitsbeauftragte

Um diesen Prozess angemessen zu steuern, muss es Sicherheitsbeauftragte geben, welche in besonderer Weise dafür ausgebildet sind und für die gesamte Fragestellung in Zusammenarbeit mit der Leitung Verantwortung übernehmen.

A5) Interne Sicherheitsrichtlinien und -standards werden definiert

Verbindliche Sicherheitsrichtlinien der jeweiligen Organisation bilden die Basis für die Umsetzung eines Sicherheitskonzeptes. Darin werden die vertraglichen Rahmenbedingungen erläutert und es wird auf Konsequenzen und Sanktionen hingewiesen, die für die Mitarbeiter/innen bei Verstößen gegen diese Richtlinien eintreten können. Die Verpflichtung auf die geltenden Datenschutzbestimmungen wird hier beschrieben.
Die Sicherheitsstandards konkretisieren die Richtlinien und sind ebenso verbindlich. Sie müssen regelmäßig an die aktuellen Bedingungen angepasst werden. In ihnen wird festgelegt, welche Sicherheitseinstellungen an den beteiligten PCs vorzunehmen sind, welche Gefahren bei Soft- und Hardware abzuwenden sind und wie Angriffe effektiv abgewehrt werden können. In einem Alarmierungsplan wird dabei genau beschrieben, wer für was zuständig ist und wie mit möglichen Angriffen umzugehen ist.
Informationen zum Datenschutz: Virtuelles Datenschutzbüro

A6) Schulung der Mitarbeiter/innen

Alle Beteiligten werden entsprechend ihrer Zugangsrechte aus- und weitergebildet. Dies beinhaltet das Grundverständnis des Gesamtkonzepts sowie ausreichende Kenntnisse zu Datenschutz und Datensicherheit. Nur diejenigen Mitarbeiter/innen, welche die Gefahren kennen, sind in der Lage, diesen aktiv entgegenzuwirken. Aus- und Weiterbildung im Bereich Sicherheit stellt dabei einen zentralen Punkt für die Wirksamkeit eines Sicherheitskonzepts dar. Der Begriff "Social-Hacking" beschreibt in diesem Zusammenhang die Tatsache, dass es oft mit Tricks (z.B. gespieltes Telefonat) möglich ist Zugangsinformationen von Mitarbeitern zu erlangen, ohne dass diese sich überhaupt einer Gefahr bewusst sind.

A7) Mehrstufige Sicherheitsebenen / Stufenkonzept

Es werden unterschiedliche Sicherheitsebenen im Sicherheitskonzept miteinander kombiniert. Es kann immer sein, dass eine Sicherungsfunktion - aus welchen Gründen auch immer - vorübergehend ausfällt. Dadurch sollte aber nicht das Ganze zu schützende System tangiert werden. Diese Mehrstufigkeit gilt sowohl für die technischen Lösungen als auch für die beteiligten Mitarbeiter/innen. Die Stufung der Zugangswege und der Zugangsrechte wird in unserem Sewecom-Stufenkonzept verdeutlicht.

A8) Beteiligte PCs, Software und Netzwerke

Die beteiligten PCs und Netzwerk-Komponenten werden entsprechend den in den Sicherheitsstandards festgelegten Beschreibungen konfiguriert und ausgestattet. Bei einem Arbeits-PC, der dem Sewecom-Verfahren entspricht, dürfen dabei keine risikovollen Zugriffe von außen erlaubt werden. Insbesondere Software mit Serverfunktionalität darf nur installiert werden bzw. bleiben, wenn dies ausdrücklich erlaubt und für die Arbeit notwendig ist. Auch bei der Hardware dürfen lediglich unbedenkliche Komponenten verwendet werden. Gefahren, die zum Beispiel durch unverschlüsselte Funk-Komponenten (z.B. Maus, Tastatur) entstehen können, wird durch die konkreten und jeweils aktuellen Sicherheitsstandards ebenfalls entgegengewirkt.
Alle beteiligten PCs und Netzwerke gehen ausschließlich über einen gesicherten Zugang ins Internet. Dabei sind nur die notwendigen Internetdienste (http, https, ftp,...) freigeschaltet. Jeglicher Datentransfer - auch der Zugang zum Internet - wird durch Firewall- und Viruswall-Lösungen gesichert.

A9) Informations- und Kommunikationskonzept

Um Sicherheitsbewusstsein im Sinne von Datenschutz und Datensicherheit in einer Organisation zu verankern, bedarf es einer zielgerichteten Strategie. Je größer ein System ist, desto wichtiger ist es, hier ein angemessenes und nachhaltiges Konzept zu entwickeln. Dieses Informations- und Kommunikationskonzept stellt ein Teilkonzept eines gesamten Sicherheitskonzeptes dar. Insbesondere dort, wo die Fragen zu diesem Themenkomplex noch nicht im Bewusstsein der Mitarbeiterschaft sind, ist es wichtig, auch die möglichen Widerstände der Mitarbeiter/innen einzuplanen, um konstruktiv damit umgehen zu können. Die verschiedenen Ebenen müssen schon im Projektstadium rechtzeitig eingebunden und ein guter Informationsfluss muss sichergestellt werden. Dabei ist es hilfreich, unterschiedliche Kommunikationsformen und -wege bereit zu stellen.

B) Internet-Technik

B1) Problem Outsourcing

Immer häufiger wird die Informationstechnik bei einer Behörde, einem Unternehmen, einer Organisation oder von einem Angehörigen der freien Berufe nicht selbst im eigenen Hause realisiert, sondern von einem externen Dritten. Ein solches Outsourcing wirft rechtlich erhebliche Fragen im Hinblick auf Datenschutz aber ggf. auch hinsichtlich Strafrecht und Strafprozessrecht auf. Diese komplexe Thematik kann hier nicht näher erläutert werden. Diesbezüglich sei auf die nachfolgende Veröffentlichung verwiesen:

> *Ulrich Sieber, Teil 19. Strafrecht und Strafprozessrecht, Rn. 469 ff., in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs, Loseblatt, München: C.H. Beck 1998 ff.*

B2) Technische Sicherheits-Infrastruktur

Vor allem die EDV Infrastruktur (Server, VPN, Firewall, Viruswall) ist in der konkreten Ausgestaltung eine Frage der Finanzen, da es sich um dauerhafte Folgekosten (intern: Personal und Technik / extern: Dienstleistung) handelt. Dem Niveau an Sicherheit sind dabei keine Grenzen gesetzt. Gleiches gilt entsprechend für die Kosten. Ein angemessenes Maß an Sicherheit ist dabei allerdings nur zu erreichen, wenn Hard- / Software, Netze und alle technischen Komponenten nicht veraltet sind, Sicherheitslücken regelmäßig geschlossen werden und die verantwortlichen Mitarbeiter/innen kontinuierlich weitergebildet werden. Dabei ist auch die Verfügbarkeit zu gewährleisten. Brandschutz, Hochwasserschutzmaßnahmen und Einbruchssicherheit gehören zu den sicheren Rahmenbedingungen. Kann dies innerhalb der Organisation nicht gewährleistet werden, hilft unter Umständen ein externer Dienstleister, das Sicherheitsniveau zu erhöhen, wenn jener diese Punkte zuverlässig gewährleisten kann. Die technischen Komponenten sollten dabei den Richtlinien des BSI (Bundesamt für Sicherheit in der Informationstechnologie) entsprechen: www.bsi.de.

B3) Sichere Server-Infrastruktur

Die Daten werden ausschließlich auf einem Server gespeichert, der höchsten Sicherheitsanforderungen genügt. Die Verbindung zum Internet wird dabei durch Firewall- und Viruswall-Lösungen gesichert, die dem aktuellen Stand der Technik entsprechen.
Grundschutzhandbuch des BSI: Thema Firewall
BSI: Sicherheitsanforderungen an einzelne Firewall-Komponenten

B4) VPN - virtual private network

Falls die Technik nicht ausschließlich im eigenen Haus realisierbar ist, kann die Vernetzung über ein getunneltes VPN geschehen oder über Standleitungen bzw. Dial-In. Der Sewecom-Ansatz hat ein geschlossenes Netzwerk zum Ziel. Das Eindringen von Unbefugten muss also auch in diesem Falle effektiv abgewehrt werden. Notwendige Sicherheitsfaktoren sind im Falle eines VPN: Verschlüsselung, Authentifizierung und Zugangskontrolle, eingebettet in ein schlüssiges Vernetzungskonzept.
BSI mit einem VPN-Konzept: SINA Systemkonzept

B5) Administrative Zugänge zu Servern besonders gesichert

Die administrativen Zugänge sind also auf keinen Fall direkt über das Internet erreichbar, sondern (falls nicht im eigenen Haus möglich) über ein virtual private network (VPN), das den oben beschrieben Sicherheitsanforderungen entspricht.

B6) Kommunikationslösung geschieht webbasiert

Eine Kommunikationslösung über das Internet ist mit Kunden und Klienten per gängigen eMail-Protokollen nicht vertretbar. Der Verschlüsselungsvorgang ist zu kompliziert und wird in der Praxis von Kunden/Klienten kaum genutzt. Webbasierte Mail ist hier sinnvoll, weil sie nutzerfreundlich zu realisieren ist und den beschriebenen Gefahren entgegenwirken kann. Die Dimensionen von

Datensicherheit können dadurch verlässlich garantiert werden: Vertraulichkeit, Verbindlichkeit, Integrität, außerdem die Authentizität der Organisation. Bezüglich der Kunden / Klienten kann die Organisation selbst bestimmen, ob sie von den Nutzern Authentizität oder Anonymität erwartet. Sämtliche Kommunikationsverläufe verbleiben also auf dem Server der Organisation und können so gesichert und vor unbefugten Zugriffen geschützt werden.
Bei der Konkreten Software wird eine Lösung verwendet, die den Anforderungen des Datenschutzes entspricht: Open-Source-Software oder proprietäre Software (d.h. nicht Offene bzw. Freie Software), die von einem staatlich anerkannten Sachverständigen begutachtet wurde und ein staatlich anerkanntes Datenschutzsiegel erhalten hat.

B7) SSL-Server-Zertifizierung nach Signaturgesetz

Um den höchsten gesetzlichen Standards für Verschlüsselungstechnik zu genügen, wird ein nach deutschem Recht anerkannter Zertifizierer gewählt. Dieser muss von der zuständigen Regulierungsbehörde für Post und Telekommunikation (RegTP) (www.regtp.de) für die Ausstellung von Sicherheits-Zertifikaten akkreditiert sein. Mit einer Zertifizierung durch eine akkreditierte Zertifizierungsinstanz ist dann auch im Internet glaubwürdig nachzuvollziehen, dass es sich bei dem Internetangebot einer bestimmten Organisation auch wirklich um diese selbst handelt (Authentifizierung).
Liste der RegTP: Akkreditierte Zertifizierungsinstanzen (ZDA)

B8) Intranet besonders gesichert

Ein Intranet stellt im hier beschriebenen Sinne eine Plattform dar, über die Mitarbeiter/innen intern vernetzt sind und wo vertrauliche Daten gespeichert werden, die in besonderer Weise geschützt werden sollen. Ein Intranet nach dem Sewecom-Verfahren wird strengsten Anforderungen unterworfen. Auch hier ist die geregelte Zugangskontrolle mit Authentifizierung der zentrale Ansatzpunkt. Durch eine angemessene Firewall-Architektur wird ein direkter Zugriff aus dem Internet und von anderen Teilen des internen Netzes abgewehrt.

B9) Systemüberwachung

Computersysteme werden hinsichtlich ihrem Betriebsablauf durch so genanntes Monitoring überwacht. Nur so ist ein stabiler Betrieb auf Dauer zu gewährleisten, da Schwachstellen und Kapazitätsengpässe vorzeitig erkannt werden können. Zur Umsetzung des Monitorings gibt es je nach System unterschiedliche Hilfstools.
Darüber hinaus ist aber auch eine aktive Überwachung mit dem Ziel der Erkennung von Angriffen und von Missbrauch zu realisieren. "Intrusion Detection Systeme" (IDS) ist der Fachbegriff für diese Form der Überwachung.
BSI-Leitfaden zur Einführung von IDS

C) Darstellung nach Außen

C1) Aufklärung der Nutzer

Die Nutzer (Kunden/Klienten usw.) der Kommunikationsplattform werden auf mögliche Gefahren bezüglich PC und Internetzugang aufmerksam gemacht. Es werden zudem Hinweise und / oder Links bereitgestellt, die dazu beitragen können, den Zugang und die PCs ebenfalls angemessen sicher zu machen: PC-Sicherheits-Tipps
. Außerdem wird deutlich sichtbar auf einen Anonymisierungsdienst verwiesen, der die Datenspuren (IP-Adressen) in geeigneter Weise verwischen kann. Dies ist der Fall bei dem Anonymisierungsdienst ANON / JAP der Technischen Universität Dresden in Zusammenarbeit mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (Projekt AN.ON - Anonymität Online
).

C2) Erklärung zu Datenschutz und Datensicherheit / Privacypolicy

Die Nutzer werden an deutlich sichtbarer Stelle der Website über die Sicherheitspolitik der Organisation in Kenntnis gesetzt. Insbesondere auf die Frage der Speicherung und Löschung von personenbezogenen Daten wird hingewiesen. Der Umgang mit den IP-Adressen als Datenspuren muss ebenfalls beschrieben werden.

D) Varianten: Anonymität / Authentizität

D1) Organisation authentifiziert / Nutzer anonym

Durch das SSL-Zertifikat ist die Organisation, die das Online-Angebot bereitstellt authentifizierbar. Die Organisation verwendet lediglich die Daten, die auf diesem Weg durch den Nutzer übermittelt wurden. Vertraulichen personenbezogenen Daten werden darüber hinaus nicht mitgeteilt, da die Identität des Nutzers nicht überprüft ist.
Die anonymen Nutzer können nur über Daten kommunizieren, die sie selbst übermittelt haben oder die öffentlich zugänglich sind.

D2) Organisation authentifiziert / Nutzer authentifiziert

Nur unter diesen Bedingungen dürfen Daten aus dem Bestand der Organisation über diesen Kommunikationsweg übermittelt werden (Übermittlungsfunktion):
Durch das SSL-Zertifikat ist die Organisation, die das Online-Angebot bereitstellt, authentifizierbar. Die Organisation darf Informationen aus ihrem Datenbestand (z.B. aktueller Kontostand / Stand eines behördlichen Verfahrens) an den Nutzer nur übermitteln (Übermittlungsfunktion), wenn dies von dem jeweiligen Nutzer für seine Daten per rechtskräftiger Unterschrift genehmigt wurde. Dabei muss die Authentifizierung des Nutzers in geeigneter Weise stattfinden.
Die Nutzer gelangen zu ihrem persönlichen Account über ihren Benutzernamen und ihr Passwort. Sollten sie ihren Account vor der Authentifizierung angelegt haben (gemäß D1), müssen sie nach der Überprüfung für diese zusätzliche Funktionalität (Übermittlungsfunktion) freigeschaltet werden (z.B. durch Eingabe eines Aktivierungs-Codes).

D3) Rechtsverbindliche Kommunikation: Verträge per Internet

Für rechtsverbindliche Kommunikation bedarf es zusätzlicher Maßnahmen über ein SSL-Server-Zertifikat hinaus: Der Gesetzgeber in Deutschland hat dazu durch das Signaturgesetz umfassende Rahmenbedingungen geschaffen. So ist es unter bestimmten Voraussetzungen möglich auch über elektronische Kommunikationswege eine rechtsverbindliche "Unterschrift" zu leisten. Dabei gibt es die Möglichkeit so genannte Zeitstempel zu integrieren, welche einen bestimmten rechtsrelevanten Prozess zeitlich dokumentieren und auch im nachhinein nachvollziehbar machen (Beweiskraft).
Digitale Unterschrift und Zeitstempel bedürfen weiterer Maßnahmen: Elektronische Signatur

Grundlagen / Voraussetzung

Was die **Schaffung einer sicheren Infrastruktur** betrifft, so verweisen wir ausdrücklich auf das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI), das detailliert die notwendigen Rahmenbedingungen aufzeigt.
Webkurs des BSI_IT-Grundschutz
Leitfaden des BSI zu IT-Sicherheit
Fragen zum Datenschutz sollten im Virtuellen Datenschutzbüro vertieft werden, das als Projektpartner die Datenschutzbeauftragten von Bund, Ländern, Kirchen usw. hat. Es wird vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein realisiert.