
LESEPROBE

Datenschutznachrichten (DANA) 2/1999

Karin Schuler, Bonn

Vertragliche Regelung zu Fernwartungsverbindungen: Organisatorische und technische Maßnahmen festschreiben

Viele der heute eingesetzten EDV-Systeme können von ihren Betreibern nur noch bis zu einem gewissen Grad selbständig betrieben werden. Häufig ist kein oder nicht ausreichendes Fachwissen vorhanden, um Systeme vollständig in Eigenregie zu pflegen oder es fehlt durch immer heterogener werdende EDV-Landschaft schlichtweg die Kapazität. Auch üben manche Software-Hersteller finanziellen Druck auf die Kunden aus, indem sie Programm-Aktualisierungen und nötige Wartungsarbeiten zu günstigen Preisen über elektronische Wege durchführen, jedoch hohe Stundensätze und Reisekosten berechnen, sofern die Arbeiten vor Ort durchgeführt werden sollen.

Immer häufiger werden daher einzelne Rechner oder ganze Systemgruppen mit Fernwartungsverbindungen versehen. Heute handelt es sich häufig noch um ISDN-Wählverbindungen, wobei eine direkte Verbindung zwischen dem fernzuwartenden System und dem System des Händlers, Herstellers, Beraters oder Technikers hergestellt wird. Zunehmend ist aber zu beobachten, daß auch das Internet als Trägermedium für die Verbindung genutzt wird. Bei den Systemen, mit deren Hilfe die Fernwartung durchgeführt wird, kann es sich sowohl um stationäre Systeme handeln, die extra für diesen Zweck eingerichtet wurden, es werden ebenso aber auch Laptops (z.B. eines reisenden Beraters) eingesetzt. Die über eine Fernwartungsverbindung möglichen Arbeiten reichen von der im Notfall ausgeführten Fehlerbeseitigung bis zur vollständigen Administration ganzer Systeme.

Immer jedoch wird im Rahmen der Fernwartung eine Person tätig, die von außerhalb der Unternehmensgebäude über öffentliche Netze Zugang zu den betroffenen Systemen erhält. Da diese Systeme in aller Regel auch in die Unternehmensnetze eingebunden sind, bedeutet die Einrichtung einer Fernwartungsverbindung automatisch eine Öffnung des Unternehmensnetzwerkes, die es verantwortungsvoll abzusichern gilt. Denn es muß garantiert werden, daß personenbezogene und sonstige sensible Daten nicht unberechtigt eingesehen und verarbeitet werden können. Und diese Vorkehrungen müssen sowohl für die Systeme getroffen werden, die gar nicht in die Fernwartung einbezogen sind (aber über das Netz im Falle einer etablierten Verbindung auf einmal „sichtbar“ werden), als auch für die fernzuwartenden Systeme selbst.

Nicht zuletzt hängt es von der Art und Häufigkeit der aufzubauenden Fernwartungsverbindung ab, welche Schutzmaßnahmen im einzelnen ergriffen werden müssen. Schutzmaßnahmen müssen dem Bedürfnis nach Wahrung von Integrität, Vertraulichkeit und Verfügbarkeit der betroffenen Systeme und Daten Rechnung tragen. Gleichzeitig sollen sie, im Sinne des §9 BDSG dem Datenschutz dienen und sowohl auf den ferngewarteten Systemen wie auch auf verbundenen Systemen Datenschutzverstöße verhindern helfen.



Die Anforderungen an Fernwartungsverbindungen sind bereits vor langem aus dem Kreis der öffentlichen Datenschutzbeauftragten formuliert worden und inzwischen auch von anderen Gruppen und Autoren, teilweise leicht modifiziert, in Checklisten und Anforderungskataloge übernommen worden.

Bei dem Versuch, mit Hilfe dieser Anforderungslisten bei einem großen Konzernunternehmen einen Standard für die Gestaltung von Fernwartungsverbindungen zu etablieren, wurden aus datenschutzrechtlichen Erwägungen zusätzliche Unterscheidungen mit Auswirkung auf die Gestaltung von Anforderungen und Verträgen getroffen, und zwar:

- zwischen Fernwartung und Fernadministration und
- zwischen Verbindungen innerhalb Deutschlands und solchen ins Ausland

Als **Fernwartung** soll eine Verbindung gelten, wenn interne oder externe Beschäftigte über eine Außenverbindung auf ein System im eigenen Unternehmen(snetz) zugreifen und zwar zur Fehlerbehebung oder zu Wartungszwecken. Unter diese Definition fallen auch Beschäftigte, die beispielsweise in Ausübung einer 24-Std.-Bereitschaft von zu Hause aus arbeiten. Hierbei werden Fehlersituationen auf Systemen behoben, die dieser Personenkreis normalerweise (tagsüber) im Unternehmen betreut. Typisch für die Fernwartung ist die relativ geringe Häufigkeit derartiger Vorgänge. Die alltägliche Administrationsarbeit am betroffenen System wird von einem oder mehreren internen, vollberechtigten Administratoren durchgeführt, die die alleinige Verantwortung für den ordnungsgemäßen Betrieb des Systems tragen.

Dagegen zählt als **Fernadministration** eine Außenverbindung, mit deren Hilfe alle oder große Anteile der anfallenden Administrationsarbeiten am System durch interne oder externe Mitarbeiter durchgeführt werden. Diese Zugriffe erfolgen daher relativ häufig und regelmäßig. Die fernadministrierenden Personen sind entweder die für das System verantwortlichen internen Administratoren selbst (Heimarbeit) oder es handelt sich um externe Personen, die Verantwortung für die Administration und den ordnungsgemäßen Betrieb des Systems tragen. Ein solcher Fall tritt zum Beispiel ein, wenn zur Erbringung einer bestimmten Dienstleistung ein vorkonfiguriertes System in das Netz des Kunden eingebracht wird, ohne daß der Kunde selbst Zugang zum System erlangen kann, da die gesamte Administration weiterhin vom Dienstleister vorgenommen wird.

Da im Falle der Fernadministration, wie aus der Definition hervorgeht, nicht generell davon ausgegangen werden kann, daß es auf seiten des ferngewarteten Systems eine fachkundige Person gibt, die den Verlauf von Fernwartungssitzungen kompetent verfolgen kann, erscheint eine Forderung nach ständiger Kontrolle am Bildschirm nicht sinnvoll und aufgrund der Häufigkeit auch nicht realisierbar. Um die fehlende direkte Kontrolle auszugleichen, werden im Falle von Fernadministrationsverbindungen strengere Maßstäbe an die Protokollierung der Vorgänge und an die systematische Auswertung der Protokolle gelegt.



Die Anforderungen an den Betrieb von Fernwartungs- und Fernadministrationsverbindungen folgen dennoch im wesentlichen den oben zitierten Checklisten:

1. .Aufbau der Verbindung über zentralen, gesicherten Einwahlweg

Fernverbindungen sollen nur über einen dafür vorgesehenen, zentralen Authentifizierungs-Server aufgebaut werden. Sofern dies nicht möglich ist, soll mindestens ein call-back-Verfahren eingerichtet werden.

2. Verwendung von Einmal-Paßworten

Paßworte dürfen nur für eine Sitzung gültig sein, damit durch Abhören der Leitung gewonnene Paßwörter nicht zum unberechtigten Verbindungsaufbau benutzt werden können.

3. Persönliche Authentifizierung mindestens durch Paßwort, besser durch Chipkarte

Die für die Fernverbindung berechtigten Personen müssen namentlich bekannt gegeben werden. Sie erhalten persönliche Accounts. Sie müssen sich mindestens durch Paßwort identifizieren, um zu verhindern, daß Einbrecher in das System der Wartungsfirma eine Verbindung zu Unternehmensrechnern aufbauen können (Sprungbretteffekt). Die Paßworte müssen den Unternehmensstandards genügen und dürfen nicht weitergegeben werden (dies gilt auch für andere Authentifizierungssysteme wie z.B. Chipcards). Verstöße werden sanktioniert.

4. Verschlüsselte Verbindung

Daten dürfen während der Sitzung nicht im Klartext über die Leitung fließen.

5. Kein Zugriff auf sensible Daten

Ein Zugriff auf klassifizierte (vertraulich, streng vertraulich) und/oder personenbezogene Daten, die nicht ausdrücklich Gegenstand des vereinbarten Administrationsvorgangs sind, darf dem fernadministrierenden Unternehmen nicht möglich sein. Entsprechende Daten sind zu verschlüsseln oder auf sonstige Weise geeignet abzuschotten.

6. Berechtigungsvergabe

Den Personen, die die Fernadministration durchführen, sind nur diejenigen Berechtigungen zu erteilen, die sie zur Durchführung ihrer Aufgabe benötigen. Insbesondere ist zu vermeiden, sie mit SuperUser-Rechten auszustatten.

7. Fernwartungssitzung nur nach Erlaubnis und Wartung generell nur unter Kontrolle (nur für Fernwartung)

Für jede einzelne Fernwartungssitzung ist eine explizite (telefonische) Erlaubnis erforderlich. Sitzungen dürfen nicht unbeobachtet ablaufen, sondern müssen während der gesamten Dauer am Bildschirm verfolgt werden, d.h. alle vorgenommenen Schritte müssen am Bildschirm sichtbar sein. Benutzer/innen auf unserer Seite müssen die Verbindung sofort abbrechen, wenn Unklarheiten über den rechtmäßigen Verlauf der Fernwartungssitzung bestehen.

8. Protokollierung aller Vorgänge und Protokollauswertung

Jede Sitzung muß automatisch protokolliert werden. Die Protokollsprache (Syntax und Semantik) muß vollständig dokumentiert sein. Eine angemessene und zweckdienliche Auswertung (Filterung) muß möglich sein.

Das "Nachspielen" aufgezeichneter Protokolle (z.B. in Fehlerfällen) soll möglich sein.

(für Fernadministration):

Für die Auswertung der Protokolle ist eine Person (und ein Vertreter im Verhinderungsfall) namentlich zu benennen. Diese muß ausreichend geschult und qualifiziert sein, um das Vorgehen der Fernadministratoren anhand der Protokolle beurteilen zu können.

Es ist schriftlich verbindlich festzuhalten:

- auf welche Weise Protokolle archiviert werden,
- wo die primäre Ablage (Speicherung) stattfindet,
- wie die Protokolle archiviert werden (Medium, Ablageort,),
- die minimale Aufbewahrungsdauer (mindestens zwei Monate) und Löschfristen (spätestens nach einem Jahr), sofern nicht als Beweismittel für lfd. Verfahren nötig.
- wie technisch/organisatorisch sichergestellt wird, daß nur berechtigte Personen Zugriff auf archivierte Protokolle haben
- Häufigkeit und Art der Auswertung durch die beauftragte Person
- Form der Auswertungsergebnisse (Bericht) und Empfänger
- welche Reaktionen/Gegenmaßnahmen aufgrund entdeckter Unregelmäßigkeiten/Sicherheitsvorfälle ergriffen werden.



9. Virenvorsorge

Zum Abschluß jeder Fernadministrationssitzung muß eine vollständige Prüfung des/der betroffenen Datenträger veranlaßt werden.

10. Vertragliche Regelung der erlaubten Maßnahmen

Es wird ein separater Datenschutzvertrag für Fernwartung abgeschlossen.

Bei der vertraglichen Regelung mit Hilfe eines separaten Datenschutzvertrages wird ebenfalls zwischen Fernwartungs- und Fernadministrationsvorgängen unterschieden. Die unterschiedlichen Regelungen beziehen sich jedoch im wesentlichen auf die Festschreibung der in der Anforderungsliste enthaltenen Punkte (weniger direkte Kontrolle bei der Fernadministration, dafür stärkere Anforderungen an die Protokollierung).

Die zweite, bereits genannte Differenzierung zwischen Verbindungen innerhalb Deutschlands und solchen ins Ausland schlägt sich ebenfalls im Vertragstext nieder. Die Problematik des grenzüberschreitenden Datenverkehrs hat aus datenschutzrechtlicher Sicht im Falle von Fernwartungs-/oder Fernadministrationsverbindungen einen besonders zu bedenkenden Aspekt: Bei derartigen Verbindungen werden evtl. personenbezogene Daten ins Ausland übermittelt, wo sie dem Schutz des BDSG zunächst einmal entzogen sind. Übermittlungen ins Ausland können aber, neben anderen Voraussetzungen, nur zulässig sein, wenn die Rechte der Betroffenen gewahrt werden können und die Möglichkeit besteht, die Ordnungsgemäßheit der Datenverarbeitung bei der fernwartenden Stelle zu überprüfen. Aus diesem Grunde muß der Datenschutzvertrag zur Fernwartung von ausländischen Stellen aus besondere Schutzmaßnahmen festschreiben, um die Rechte des auftraggebenden Unternehmens und von Betroffenen (deren Daten möglicherweise ins Ausland übermittelt werden) zu erhalten.

Der Datenschutzvertrag zu Fernwartung ist beispielhaft im folgenden mit gekennzeichneten Unterschieden (Inland/Ausland) abgedruckt. Bei der Entwicklung der Standards zum Umgang mit den beschriebenen Verbindungen wurde schließlich entschieden, Fernadministrationsverbindungen, die aus dem Ausland aufgebaut werden, grundsätzlich nicht zuzulassen. Ohne eigene, voll verantwortliche Administratoren ein System aus dem Ausland warten und administrieren zu lassen erscheint als ein zu großes Risiko, insbesondere da die rechtlichen Möglichkeiten im Falle von Unregelmäßigkeiten stark beschränkt sind.



Datenschutzvertrag zur Fernwartung

Zwischen (Auftraggeber)

und (Auftragnehmer)

wird folgende Vereinbarung getroffen:

1 Gegenstand und Zweck des Vertrages

- 1.1. Der Auftragnehmer wird mit der Fernwartung der Systeme <SYSTEM1>, <SYSTEM2>,...beauftragt. Sämtliche Tätigkeiten im Rahmen der Fernwartung beschränken sich auf diese Systeme.
- 1.2. Die Fernwartung findet nur in den Fällen statt, in denen<genaue Beschreibung, z.B. durch den Administrator nicht behebbare Fehlersituationen, Software-Fehler,...> eintreten. Sie findet nur nach vorheriger Aufforderung durch den <System-Administrator> statt.
- 1.3. Die Fernwartung soll <Ziel definieren: Lauffähigkeit herstellen, Updates einspielen etc.>

2. Durchführung

- 2.1. Der Auftragnehmer stellt ausreichende Kapazitäten zur Verfügung um die unter 1. beschriebenen Leistungen jederzeit erbringen zu können.
- 2.2. Der Auftragnehmer ist nicht berechtigt, Subunternehmen mit der Erfüllung seiner Pflichten aus diesem Auftrag zu beauftragen.

3. Ablauf einer Fernwartung

- 3.1. Die Fernwartung wird vom Auftragnehmer ausschließlich von <Standort innerhalb Deutschlands>/<Standort außerhalb Deutschlands> durchgeführt.
- 3.2. Die Fernwartung wird auf seiten des Auftragnehmers nur von Personen durchgeführt, die dem <System-Administrator> bekannt sind und die eine persönliche Verpflichtungserklärung unterschrieben und an den Datenschutzbeauftragten übersandt haben. Diese Personen werden in Anhang 1 namentlich aufgeführt. Sie erhalten eine persönliche Zugangsberechtigung zur Durchführung der Fernwartung, die sie keinen weiteren Personen zugänglich machen dürfen (keine Paßwort- oder Chipkarten-Weitergabe)
- 3.3. Die im Anhang 2 vereinbarten Maßnahmen zu Datenschutz und Datensicherheit sind verbindlich einzuhalten.

4. Umgang mit Daten

- 4.1. Der Auftragnehmer hält sich bei der Erledigung seines Auftrags streng an die Weisungen und Vorgaben des Auftraggebers. Er führt keine Verarbeitungsmaßnahmen durch, die nicht zwischen den Parteien ausdrücklich vereinbart worden sind. Vereinbarte Verarbeitungsmaßnahmen dürfen ausschließlich zu den vereinbarten Zwecken durchgeführt werden. Der Auftragnehmer verpflichtet sich insbesondere, keine Einsicht in Daten zu nehmen, deren Kenntnis zur Erledigung seiner Aufgabe nicht erforderlich ist. Auch wird er keine Kopien von Daten anfertigen, es sei denn, daß er hierzu vom <System-Administrator> ausdrücklich aufgefordert worden ist.
- 4.2. Über alle Daten und deren Inhalt, die dem Auftragnehmer bei der Erledigung seines Auftrags zur Kenntnis gelangen, hat er strengstes Stillschweigen zu bewahren.
- 4.3. (für Inland)Datenschutzrechtlich soll das Verhältnis zwischen Auftraggeber und Auftragnehmer als Auftragsdatenverarbeitung gelten. Der Auftragnehmer verpflichtet sich, die sich daraus ergebenden Pflichten aus dem Bundesdatenschutzgesetz zu erfüllen.
- 1.3 (für Ausland)Soweit der Auftragnehmer bei der Verarbeitung im Ausland aufgrund zwingender ausländischer Gesetznormen nicht der deutschen Gesetzgebung unterliegen sollte, vereinbaren die Parteien zur Vermeidung von Rechtsnachteilen ausdrücklich die vertragliche Geltung der Normen des Bundesdatenschutzgesetzes.
- 4.4. Muß der Auftragnehmer Test- und Wartungsprogramme dauerhaft auf den fernzuwartenden Systemen ablegen, so darf dies nur unter einer speziell dafür angelegten Berechtigung erfolgen.
- 4.5. Der Auftragnehmer verpflichtet sich, den betrieblichen Datenschutzbeauftragten des Auftraggebers uneingeschränkt zu unterstützen, sofern für die Beantwortung von Auskunftersuchen Betroffener auch Informationen über Fernwartungsvorgänge benötigt werden.

5. Sonstige Festlegungen

- 5.1. Der Auftraggeber ist jederzeit zur Entsendung eines Beauftragten berechtigt, dem die Kontrolle der ordnungsgemäßen Durchführung dieses Vertrages obliegt. Der Auftragnehmer gewährt dem Beauftragten ungehinderten Zugriff und Zugang zu allen DV-Anlagen, Dateien und Unterlagen, die mit der Durchführung der hier vereinbarten Fernwartung in Verbindung stehen. Dem Beauftragten sind durch den Auftragnehmer alle Auskünfte zu erteilen, die dieser zur Erfüllung seiner Kontrollfunktion für erforderlich hält. Festgestellte Mängel werden vom Auftragnehmer unverzüglich beseitigt.
- 5.2. Verletzt der Auftragnehmer eine oder mehrere Bestimmungen dieses Vertrages, so gilt eine Vertragsstrafe von DM 50.000,-- für jeden Fall der Zuwiderhandlung als vereinbart. Der Auftraggeber hat dann das Recht zur fristlosen Kündigung des Vertrages.



Deutsche Vereinigung
für Datenschutz e.V.

-
- 5.3. Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Gerichtsstand ist –soweit gesetzlich zulässig– <Standort des Auftraggebers>.
- 5.4. Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein oder werden oder sollte dieser Vertrag eine Lücke aufweisen, so soll die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt werden. Anstelle der unwirksamen oder undurchführbaren Bestimmung oder zur Ausfüllung einer Lücke soll eine angemessene Regelung gelten, die im Rahmen des rechtlich Zulässigen und wirtschaftlich Vernünftigen dem am nächsten kommt, was die Vertragspartner gewollt haben oder gewollt hätten, wenn sie den Punkt bedacht hätten.
6. **Anhang 1** - Namen der akkreditierten Fernwartungstechniker
7. **Anhang 2** - Vereinbarte technische Maßnahmen

DANA
c/o Deutsche Vereinigung für Datenschutz e.V.
Bonner Talweg 33-35
53173 Bonn