Fernwartungsprogramme und Remote-Control-Systeme

Eberhard Kiesche / Matthias Wilke // AoB Bremen, dtb Kassel

HIER LESEN SIE:

- welche Chancen und Risiken mit dem Einsatz von Fernwartungs- und Remote-Control-Systemen verbunden sind
- warum Fernwartungs- und Remote-Control-Systeme spezieller Datenschutzregelungen bedürfen, insbesondere wenn sie von Externen betrieben werden
- welche Regelungen für Betriebs-/Dienstvereinbarungen und für Verträge zwischen Auftraggeber und Fernwartungs-Dienstleister nötig und sinnvoll sind

In Netzwerken zusammengeschlossene Rechner können mit Hilfe sogenannter Fernwartungssoftware entweder von externen Dienstleistern, von Systemherstellern oder durch eigene interne Systemverantwortliche eingerichtet, verändert, erweitert, verwaltet und gewartet werden. Auch können auf diesem Weg Fehlerursachen gesucht und beseitigt sowie vorhandene Soft- und Hardwareprodukte inventarisiert werden. Das klingt nach einer vorteilhaften Technik, dennoch ist Vorsicht geboten, denn diese Remote-Control-Systeme bergen Gefahren für die Persönlichkeitsrechte der betroffenen Arbeitnehmer in sich.

Es gibt viele Begriffe für das hier zu behandelnde Thema: Teleservice oder Telewartung, Fernwartung, Fernverwaltung, Remote-DV-Wartung oder auch schlicht Systembetreuung. Die gängigsten Begriffe aber sind Remote-Control- oder Remote-Management-Systeme (englisch: *remote* = entfernt, abgelegen; *control* = Beherrschung, Prüfung).

Dazu gehören Softwarepakete wie z.B. RemotelyAnywhere, DV-Inventar, PC Anywhere oder der System Management Server von Microsoft. Alle diese Programme wenden sich vorrangig an die Systemadministratoren, also an die für Einrichtung, Pflege und Wartung der Informations- und Kommunikationstechnik (IKT) Verantwortlichen, die von ihrem PC aus – teilweise über einen speziellen Verwaltungsrechner (Masterserver) – die angeschlossenen Arbeitsplatzrechner (die sogenannten Clients) warten und „administrieren".

Remote-Control-Systeme ersparen es dem Administrator, diese Tätigkeiten (etwa das „Aufspielen" neuer Softwareversionen oder das Beheben von Fehlfunktionen) direkt an jedem einzelnen PC eines Netzwerks vornehmen zu müssen. Und sie erlauben es vor allem, solche Tätigkeiten auch an Externe zu vergeben, seien es spezialisierte Dienstleister oder auch die Hersteller von IKT-Systemen selber. In jedem Fall muss sich der zuständige Wartungstechniker/Systembetreuer nur von seinem Rechner aus auf dem jeweils zu wartenden PC anmelden – ob dies über das interne Unternehmens-/Behördennetzwerk geschieht oder via Internet vom anderen Ende der Welt aus, das macht (technisch) keinen Unterschied aus.

Vielfältige Remote-Control-Funktionen

Welche Funktionen können nun mit Remote-Control-Systemen genau durchgeführt werden (siehe dazu auch C. Bieler: „Im Visier: Remote Control" in CF 11/04, Seite 23)?

Vieles ist möglich: Übertragen und Löschen von Dateien und Daten, Inventari-

sierung von Hard- und Software, Diagnostizieren von Hardwarefehlern und die zentrale Verteilung neuer Software oder neuer Softwareversionen (Updates). Ein mit einem Remote-Control-System ausgestatteter PC kann jederzeit die Verbindungen mit allen anderen Rechnern im Netz (den Clients) herstellen. Dabei kann der Administrator z.B. mithilfe bestimmter Tastenkombinationen spezielle Aufgaben (Tasks) aufrufen oder komplett die Kontrolle über einen Client übernehmen und dort beliebig auf Programme und Daten zugreifen.

Der Administrator kann aber auch, wie schon erwähnt, zugleich für eine ganze Gruppe von Clients Software oder zusätzliche Systemfunktionen installieren – und zwar unbemerkt. Mit der gleichen Technik ist es auch möglich, ein komplettes Netzwerk inklusive einem oder mehrerer ▶ Server von außen zu steuern und zu warten, ebenso wie es umgekehrt möglich ist, vom Unternehmens-/Behördennetzwerk aus auf angeschlossene Tele(heim)arbeitsplätze (siehe den Artikel ab Seite 15) zuzugreifen. Der Zugriff auf einen zu wartenden Rechner kann dabei entweder über ein geschlossenes Netzwerk, über Wähl-/Standleitungen oder auch mithilfe eines einfachen ▶ Browsers durch Nutzung von Internet/World-Wide-Web erfolgen.

Remote-Control-Systeme bringen also vielfältigen Nutzen mit sich. Sie machen es nicht nur möglich, die beschriebenen Wartungs-/Pflegearbeiten für ein möglicherweise weltweites Netzwerk zeitsparend von einem Adminstrator-Arbeitsplatz aus zu erledigen, sie erlauben es auch, auf Störungen bei der Hard- und Software schnell und „flächendeckend" zu reagieren und geeignete Maßnahmen zu ergreifen. Dies ist umso zeit- und ressourcensparender als Vor-Ort-Spezialisten oftmals nicht verfügbar sind (und wenn es sie gibt, können sie unter Umständen eingespart werden).

Risiken nicht unterschätzen

So weit, so gut. Nun stellt sich die Frage: Welche Risiken entstehen aufgrund des Einsatzes von Remote-Control-Systemen?

Grundsätzlich erhält jeder Wartungstechniker – ob intern oder extern – Einblick

REGELUNGSECKPUNKTE ZU FERNWARTUNG/REMOTE-CONTROL

Es bietet sich an, das Instrument einer Betriebs- oder Dienstvereinbarung für die Einführung, Anwendung, Erweiterung und Änderung von Fernwartungssystemen zu nutzen. Nur so können Risiken für die Beschäftigten ausgeschlossen werden. [1]

Folgende Eckpunkte sind für Betriebs-/Dienstvereinbarungen zu berücksichtigen:

- Beschreibung der eingesetzten Fernwartungssoftware,
- Erstellung eines Bestandsverzeichnis aller von der Fernwartung betroffenen IKT-Systeme als Anlage zur Betriebs-/Dienstvereinbarung,
- Vereinbarung der Einsatzzwecke,
- Festlegung des Umfangs, in dem personenbezogene Daten verarbeitet werden müssen,
- Festlegung von Löschfristen für alle anfallenden Daten,
- Verbot einer Verwendung zu Zwecken der Leistungs- und Verhaltenskontrolle, des Leistungsvergleichs oder der Leistungsbemessung,
- Anonymisierung aller Auswertungen über den Einsatz der Fernwartungssoftware (Beteiligung des Betriebs-/Personalrats),
- Mitbestimmungspflichtigkeit aller System-Änderungen und -Erweiterungen,
- Kontrollrecht für Belegschaftsvertretung (der Arbeitgeber/Auftraggeber stellt gegenüber dem Auftragnehmer vertraglich sicher, dass die Bestimmungen dieser Betriebs-/Dienstvereinbarung und des Datenschutzkonzepts eingehalten werden; eine Kopie des Vertrags als Anlage zur Betriebs-/Dienstvereinbarung),
- Aushändigung aller Protokolle an den Betriebs-/Personalrat,
- Regelung der Zugriffsberechtigungen und -gründe als Anlage zur Betriebs-/Dienstvereinbarung (bei interner Fernwartung sind die zugriffsberechtigten Personen festzulegen, mit Passwortschutz),
- Realisierung zusätzlicher Zugriffsbeschränkungen über Betriebssystem und Datenbank,
- Beweisverwertungsverbot (personelle Maßnahmen, die auf einer unzulässigen Verwendung der Fernwartungssoftware beruhen, sind unwirksam),
- rechtzeitige und umfassende Information aller von der Fernwartung betroffenen PC-Benutzer (über Anwendung und Folgen für ihren Arbeitsplatz sowie über die Vereinbarung selber),

Klauseln für ein Datenschutzkonzept und für eine Vertragsgestaltung „Fernwartung":

- Änderungen in der Konfiguration von Clients und Fernwartungszentrale sind nur bei Wahrung eines 4- oder 6-Augenprinzips (z.B. Hinzuziehung eines Beauftragten des Auftragnehmers und zusätzlich des Datenschutzbeauftragten sowie Betriebs-/Personalrates) möglich.
- Die Einstellungen der Fernwartung dürfen nicht automatisch verändert werden.
- Fernwartung erfolgt ausschließlich auf Anforderung des einzelnen Client-Benutzers.
- Der Verbindungsaufbau ist immer durch den Auftragnehmer vorzunehmen. Der Benutzer muss jedem Zugriff zustimmen. Auf Antrag kann in Einzelfällen auf das Zustimmungserfordernis verzichtet werden. In diesen Fällen ist ein gut sichtbarer Hinweis auf die Rechner anzubringen.
- Der Fernwartungsvorgang wird auf dem Bildschirm des Benutzers angezeigt.
- Für die Durchführung des Wartungsvorgangs ist eine Benutzerkennung zu vergeben und nach jedem Wartungsvorgang ist das Passwort zu verändern.

Fortsetzung auf Seite 8

- Spezielle Sicherheitseinstellungen und Profile für externes Wartungspersonal sind zu vereinbaren.
- Ein zeitlich ununterbrochener Zugriff auf andere Rechner durch die Fernwartungszentrale ist unzulässig.
- Zugriffe auf bestimmte Rechner (z.B. in der Personalabteilung) sind nicht zulässig.
- Bestimmte Dateien oder Verzeichnisse werden generell vom Zugriff ausgenommen. Das Wartungspersonal oder der interne Systemadministrator hat nur auf die Daten und Verzeichnisse Zugriff, die aktuell von der Wartung betroffen sind.
- Erforderliche personenbezogene Daten im Rahmen der Fernwartung sind nur für Fernwartungszwecke zu nutzen. Sie sind nach Abschluss der Wartungsaufgaben unverzüglich zu löschen.
- Der Benutzer kann jederzeit die Verbindung zur Kontrollstation abbrechen.
- Wenn personenbezogene Daten übertragen werden müssen, dann nur in verschlüsselter Form.
- Eine Weitergabe von personenbezogenen, bei der Wartung anfallenden oder offensichtlich werdenden Daten an Dritte ist verboten.
- Alle Fernwartungs-Zugriffe und Zugangsversuche sowie Tätigkeiten bei der Durchführung der Fernwartung werden protokolliert.2 Bei besonders kritischen Aktivitäten ist der gesamte Dialog zu protokollieren. Die Protokollierung erfolgt vor Ort unverschlüsselt. Die Protokolle werden nach einem Jahr gelöscht. Externe Zugriffe auf die Protokolldaten sind nicht zulässig. Die Auswertung der Protokolldaten erfolgt bei begründetem Missbrauchsverdacht unter Wahrung ders 6-Augen-Prinzips (z.B. Unternehmen, Datenschutzbeauftragter, Betriebs-/Personalrat).
- Auswertungen von Daten, die das Verhalten und die Leistung der Benutzer betreffen, sind nicht zulässig. Anonymisierte Daten dienen ausschließlich der Überprüfung der Funktionalität des Netzes.
- Bei der Inventarisierung der Rechner werden keine Dateiinhalte erhoben und auch nicht der Lizenzstatus von Softwareprodukten. Die Inventarisierung läuft täglich und automatisch ab.
- Übertragung von Daten sind nur mit Zustimmung des Betroffenen, im Einzelfall und verschlüsselt, zulässig.
- Die zu treffenden Sicherheitsmaßnahmen werden in einer Anlage zur Betriebs-/Dienstvereinbarung oder zum Vertrag beschrieben.
- Auf allen Clients sollte nach dem Wartungsvorgang ein Computer-Viren-Check durchgeführt werden.
- Die Systemverantwortlichen des Auftraggebers sind über den Ablauf der Fernwartung und der Sicherheitsvorkehrungen zu schulen.

Fußnoten

1 Vergl. Landesbeauftragter für den Datenschutz Baden-Württemberg: Merkblatt zur Fernsteuerungssoftware, www.baden-wuerttemberg.datenschutz.de → *Service* → *Hinweise und Merkblätter*; Landesbeauftragter für den Datenschutz Niedersachsen, Checkliste Ordnungsmäßige Wartung; www.lfd.niedersachsen.de/master/C27848_N13197_L20_D0_I560.html

2 Bundesamt für Sicherheit in der Informationstechnik (BSI): M.533 / Absicherung der per Modem durchgeführten Fernwartung, Stand 2006, www.bsi.bund.de/ghsb/deutsch/m/m05033.htm

in die jeweils aktuelle Bildschirmdarstellung des Benutzers und steuert notfalls den Dialog mit dem PC.

Er kann also Tastatur und Maus „übernehmen". So werden PC-Benutzer durch den Einsatz von Remote-Control-Systemen hinsichtlich ihrer Leistung und ihres Verhaltens transparent, auch weil Sicherheitsmechanismen – wie z.B. die Information an den PC-Benutzer, dass gerade eine Aufschaltung erfolgt – einfach umgangen werden können.

Oder es lässt sich bei einer Fernüberprüfung der auf einem PC installierten Software erkennen, ob sich nicht lizenzierte Software auf dem Rechner befindet oder ob Software vorhanden ist, die nicht vom Systemadministrator installiert wurde. Auch wird bei der Lizenzkontrolle deutlich, wer welche Software wie lange benutzt hat. Tastatureingaben können protokolliert und an einen anderen Rechner zur Auswertung geschickt werden. Und alle diese Daten können zu Zwecken der Leistungs- und Verhaltenskontrolle, der Leistungsbemessung und des Leistungsvergleichs genutzt werden.

Sensible Daten (wie z.B. Personaldaten oder Berufs-/Amtsgeheimnisse in Krankenhaus-Informations-Systemen – siehe dazu den Schwerpunkt in CuA 2/08) können während eines Wartungsvorgangs unberechtigterweise eingesehen werden. Zumindest bei Fällen, in denen eine Verschwiegenheitspflicht vorliegt, ist Remote-Control also datenschutzrechtlich bereits als bedenklich einzuschätzen und eine Aufschaltung grundsätzlich zu vermeiden.

Und bei einer reinen Hardwarewartung greift (externes) Wartungspersonal zwar nur auf rein technische Diagnosedateien zu, die in der Regel keine personenbezogenen Daten enthalten. In vielen anderen Fällen jedoch können mit Hilfe von Remote-Control bei der Fehlerdiagnose und -behebung auch personenbezogene Daten verarbeitet werden.

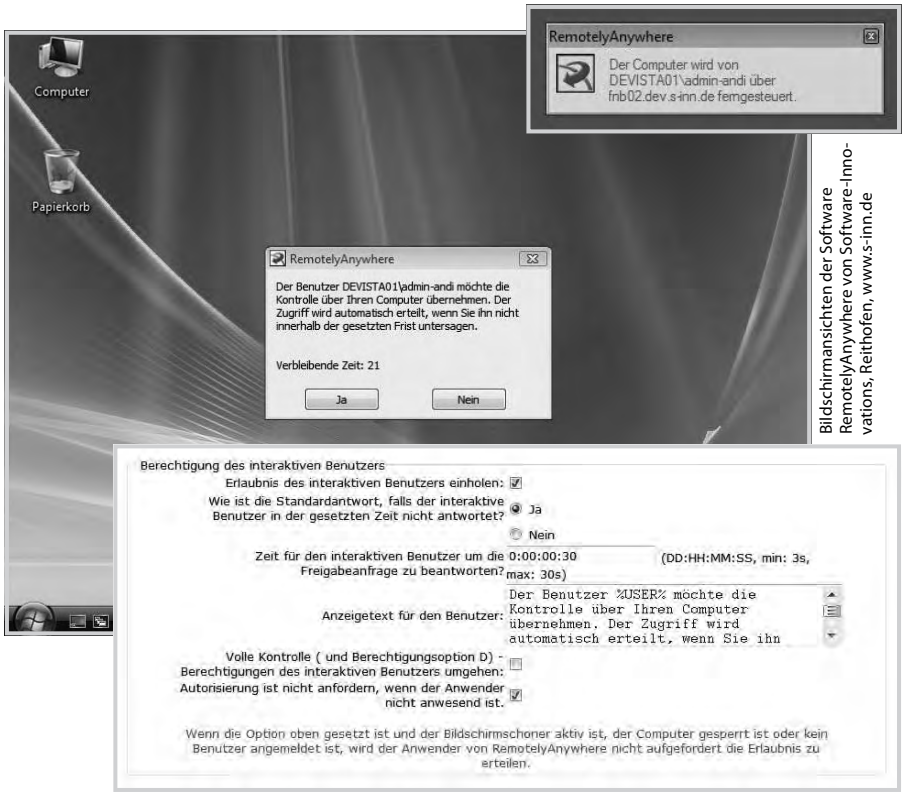
All dies ist natürlich dann besonders problematisch, wenn wir es mit einer echten Fernwartung, also einem steuernden, pflegenden, überwachenden Zugriff von außerhalb durch Dienstleister oder IKT-Hersteller zu tun haben.

Denn auch in diesen Fällen können Daten unbemerkt an die Fernwartungs-Kontrollstation übertragen werden. Dies ist umso problematischer, weil bei dieser Fernwartung vom Auftraggeber nur schlecht kontrolliert werden kann, welche Person die Wartungsarbeiten durchführt (und damit vielleicht auch unbeobachtete, unbefugte Eingriffe praktiziert). Grundsätzlich ist also eine Wartung vor Ort datenschutzrechtlich stets besser kontrollierbar. Auch behält das eigene Personal alle Eingriffsmöglichkeiten,

was bei einer Fernwartung meist nicht der Fall ist.

Datenschutz bei Auftragsdatenverarbeitung

Datenschutzrechtlich handelt es sich bei der Fernwartung durch Externe stets um Auftragsdatenverarbeitung nach § 11 Abs. 5 Bundesdatenschutzgesetz (BDSG).1 Dies ist immer dann der Fall, wenn im Zusammenhang mit der Prüfung und Wartung durch externe Stellen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.[2] Findet der Zugriff im Rahmen des Remote-Control hingegen durch interne Systemadministratoren statt, handelt es sich um einen Fall normaler (Personen-)Datenverarbeitung und muss im Falle des Falles dann vom Betriebs-/Personalrat in entsprechenden Vereinbarungen geregelt werden.



Bildschirmansichten der Software RemotelyAnywhere von Software-Innovations, Reithofen, www.s-inn.de

Im Interesse der sogenanten ► informationellen Selbstbestimmung muss jede vom einzelnen PC-Benutzer nicht zu bemerkende Kontaktaufnahme und Verbindung mit der Kontrollstation durch durch entsprechende Einstellung der Fernwartungssoftware verhindert werden. Hierzu gibt es durchaus Beispiele für eine betriebsrats- und datenschutzkonforme Konfiguration derartiger Software (siehe die Bildschirmansichten oben rechts).

Es können und müssen also technisch-organisatorische Vorkehrungen getroffen werden, die dem einzelnen PC-Benutzer jederzeit vollständige Klarheit über das aktuelle Fernwartungsgeschehen ermöglicht. Für jeden Wartungsvorgang ist ein passwortgestütztes Anmeldeverfahren zu nutzen. Die Verbindung ist immer nur für speziell autorisierte Personen zuzulassen. Und die mit der Durchführung von Wartungsaufgaben betrauten Personen sind von ihrem Arbeitgeber auf das Datengeheimnis zu verpflichten (mehr zur Auftragsdatenverarbeitung dann im folgenden Artikel ab Seite 11).

Technisch-organisatorische Maßnahmen

Vorkehrungen und Maßnahmen für die technisch-organisatorische Durchführung der Fernwartung müssen in einem Datenschutzkonzept schriftlich festgelegt werden (siehe den Kasten ab Seite 7). Diese Maßnahmen sind dann auch in die entsprechenden Verträge mit den IKT-Dienstleistern aufzunehmen, die auch die Umsetzung sicherzustellen haben.

Dazu ein Beispiel: Nur vom Dienstleister (Auftragnehmer) autorisierte Personen dürfen die vertraglich festgelegten Fernwartungsaufgaben durchführen. Der Abschluss etwa von Unter-Auftragsverhältnissen darf nur mit Zustimmung des Auftraggebers erfolgen. Sollte sich bei der technischen Durchführung der Fernwartung durch den Dienstleister etwas ändern, muss dieser eine rasche Abstimmung mit dem Auftraggeber herbeiführen.

Zugriffsschutz erforderlich

Von besonderer Bedeutung ist dabei ein klar geregelter Zugriffsschutz. Es sind nur solche Funktionen freizugeben, die für den individuellen Wartungsvorgang im Sinne einer Fehleridentifikation und -beseitigung unbedingt benötigt werden. Unbemerktes (englisch: silent = geräuschlos, still) Einspielen von Änderungen im Betriebssystem und in der Systemsoftware des Zielrechners darf aufgrund der weitreichenden Zugriffsberechtigungen der Wartungstechniker gar nicht zugelassen werden. Auch sollte der Wartungstechniker auf keinen Fall die vollen Administrator-Rechte erhalten.

Der Zugriff auf personenbezogenen Daten darf zudem nur ausnahmsweise und in dem für eine Fehleridentifikation und -beseitigung unbedingt erforderlichen Umfang ermöglicht werden. Sollte dies eine Fehlerbehebung unmöglich machen, muss die Zustimmung des Betroffenen eingeholt werden und ein für den Zugriff hinreichender Grund vorliegen. Bei Fernwartungsvorgängen sollte grundsätzlich ein fachkundiger IKT-Benutzer oder auch Systemadministrator des Auftragsgebers vor Ort beim Dienstleister die Fernwartung beobachten.[3]

Datenschutzanforderungen im Fernwartungsvertrag

Im Fall einer externen Fernwartung, sind – wie gesagt – detaillierte Anforderungen an die Datenverarbeitung in den Vertrag mit dem Dienstleister aufzunehmen. Der Auftraggeber muss dabei unter anderem den Auftrag exakt festlegen, die Kontrollrechte seines (!) betrieblichen Datenschutzbeauftragten und der Belegschaftsvertretung beim Dienstleister sicherstellen, die Aufgaben und Pflichten des jeweiligen Personals bei Wartungsvorgängen abgrenzen und dafür sorgen, dass der Verbindungsaufbau

FRISCH GELESEN

Betriebsratsarbeit im globalisierten Umfeld ist eine neue und alles andere als einfach zu bewältigende Aufgabe. Und sie ist ohne Einsatz aktueller Informations- und Kommunikationstechnik nicht zu bewältigen – ein CuA-Dauerthema, mit dem sich auch die Februarausgabe der Fachzeitschrift „Arbeitsrecht im Betrieb" (AiB) befasst. Eine Kehrseite der Medaille ist, dass die Belegschaftsvertretung nun oft mit Informationen „zugeschüttet" wird – eine wesentliche elegantere Methode als die früher übliche Informationsverweigerung, aber fast ebenso wirksam. Kurzum: Technik allein genügt nicht, die gesamte Organisation der Interessenvertretungsarbeit muss sich den neuen Gegebenheiten anpassen – und dazu gibt es in AiB 2/08 eine Menge praktischer und juristischer Hinweise.

Arbeitsunfälle sind beim Umgang mit Computern vielleicht nicht das drängendste Problem. Der Rückgang der Arbeitsunfallzahlen in den letzten Jahren mag also auch etwas mit der zunehmenden Computerisierung der Arbeit zu tun haben. Das heißt aber nicht, dass es nicht immer noch gravierende Mängel und Defizite im Arbeitsschutz gäbe. Das zeigt erneut das Schwerpunktthema der Fachzeitschrift „guteArbeit" in ihrer Februarausgabe.

Eine Kostenlawine im Gesundheitswesen (siehe CuA-Schwerpunkt 2/08) soll auf uns zurollen. Und um jedenfalls die individuellen Konsequenzen etwas abzumildern, kann man durchaus über einen Wechsel seiner Krankenkasse nachdenken. Ob die Versicherten darüber ausreichend informiert und die Kassen auf einen drohenden Mitgliederschwund vorbereitet sind, ist jetzt genauer untersucht worden. Einen Bericht dazu hat die Fachzeitschrift „Soziale Sicherheit" im Januar gebracht.

Bestellhinweis

Einzelexemplare der hier genannten Zeitschriften können bestellt werden bei: BDK Bücherdienst, PF 90 01 20, 51119 Köln, fon 02203 1002-453, bundverlag@b-d-k.de

immer vom einzelnen PC-Benutzer beim Auftraggeber gesteuert werden kann (ausführlich hierzu der Artikel ab Seite 11). Das externe Wartungspersonal muss auf das Datengeheimnis gemäß § 5 BDSG oder – im Fall etwa von Landesbehörden – der entsprechenden Paragrafen der Landesdatenschutzgesetze (z.B. § 5 im Niedersächsisches Datenschutzgesetz) verpflichtet werden.

Mitbestimmungsrechte des Betriebs-/Personalrats

Betriebs- und Personalräte haben auch im Fall von Remote-Control und Fernwartung Initiativ- und Mitbestimmungsrechte, denn auch diese Systeme sind selbstverständlich technische Kontrolleinrichtungen, die gemäß § 87 Abs. 1 Nr. 6 BetrVG und § 75 Abs. 3 Nr. 17 BPersVG mitbestimmungspflichtig sind. Eine Remote-Control- oder Fernwartungssoftware erhebt, speichert und verarbeitet personenbezogene Daten der Benutzer, die Rückschlüsse auf das Verhalten oder die Leistung der Beschäftigten ermöglichen. Sie sind damit für Leistungs- und Verhaltenskontrollen objektiv geeignet. Der Arbeitgeber hat also die Belegschaftsvertretung über die konkrete Ausgestaltung der Fernwartung und über die Funktionen der entsprechenden Software rechtzeitig und umfassend zu informieren (§ 80 Abs. 2 BetrVG und § 68 Abs. 2 BPersVG).

Zudem haben Betriebsräte ebenso wie Personalräte darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze eingehalten werden (§ 68 Abs. 1 Nr. 1 BPersVG und § 80 Abs. 1 Nr. 1 BetrVG). Hierzu gehören auch das Bundesdatenschutzgesetz oder die jeweiligen Landesdatenschutzgesetze mit ihren speziellen Vorschriften zur Fernwartung. Von daher ist in diesem Zusammenhang auch zu überwachen, ob die Vorgaben zum Datenschutz gemäß § 9 BDSG (oder Landesdatenschutzgesetze, z.B. § 7 im Niedersächsischen Datenschutzgesetz) verwirklicht werden.

Der Auftraggeber hat ein Datenschutzkonzept für die Fernwartung zu erstellen. Dieses ist mit dem Betriebs- oder Personalrat abzustimmen. Besonders ist darauf zu achten, dass der Auftragnehmer sich verpflichtet, vorhandene Betriebs- und Dienstvereinbarungen umzusetzen. Das Überwachungsrecht der Belegschaftsvertretungen schließt ein Zugangsrecht zu allen Räumen oder Betriebsteilen ein, in denen personenbezogene Daten verarbeitet werden (siehe B. Schierbaum: „Datenschutz bei Auftragsdatenverarbeitung, Wartung und Fernwartung" in CF 6/05, Seite 7).

Fazit

Fernwartungs- und Remote-Control-Systeme lassen sich für eine sichere Nutzung einrichten, wenn dazu noch begleitende organisatorische Regeln aufgestellt werden. Auch die Vorgaben des Datenschutzrechts zur Auftragsdatenverarbeitung helfen Betriebs- und Personalräten dabei, Leistungs- und Verhaltenskontrollen auszuschließen und den „Big Brother" vom Arbeitsplatz fernzuhalten …

Autoren

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen, eberhard.kiesche@t-online.de;
Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel, info@dtb-kassel.de

Lexikon

Browser ▶ (englisch: *browse* = blättern, durchsuchen) Software zum Aufsuchen und Betrachten von Inhalten im World-Wide-Web (WWW)

informationelle Selbstbestimmung ▶ durch Entscheidung des Bundesverfassungsgerichts (im „Volkszählungsurteil" von 1983) formuliertes Grundrecht jedes Menschen, über Verbleib und Nutzung der über ihn gespeicherten Daten prinzipiell selbst bestimmen zu können

Server ▶ (englisch: *server* = Zusteller) Bezeichnung für einen speziellen Rechner, der in Netzwerken für die angeschlossene Arbeitsplatzrechner bestimmte Aufgaben übernimmt (z.B. Netzwerkverwaltung, Datenspeicherung, E-Mail-Abwicklung)

Fußnoten

1 Däubler/Wedde/Klebe/Weichert, Bundesdatenschutzgesetz 2007, Kommentar, § 11 BDSG, Rand-Nr. 57
2 Däubler/Wedde/Klebe/Weichert, Bundesdatenschutzgesetz 2007, Kommentar, § 11 BDSG, Rand-Nr. 54
3 Hierbei handelt es sich um eine Datensicherheitsforderung des Bundesamts für Sicherheit in der Informationstechnik (BSI): „Die Fernwartung sollte lokal durch IT-Experten beobachtet werden. Auch wenn die Fernwartung eingesetzt wird, weil intern das Know-How oder die Kapazität nicht verfügbar ist, kann das Wartungspersonal nicht unbeaufsichtigt gelassen werden. Bei Unklarheiten sollte der lokale IT-Experte jederzeit nachfragen." (BSI M5.33 Absicherung der per Modem durchgeführten Fernwartung)