Fernwartung und BDSG

So schauen Sie Ihren IT-Dienstleistern auf die Finger

IT-Systeme sind heute sowohl hardware- als auch softwaretechnisch derartig komplex, dass Anwender auf eine Unterstützung von Herstellern oder Spezialisten angewiesen sind. Da die Anfahrt häufig zu aufwendig ist, lösen Fachleute per Fernzugriff das Problem oder warten das System. Auch die Mitarbeiter des User-Helpdesk steuern zur Unterstützung der Nutzer vielfach per Remote-Verbindung deren Rechner fern. Dabei haben sie eventuell Zugriff auf sensible Daten. Vorsicht ist also angebracht, will man den Fernzugriff erlauben.

Der Zugriff der Spezialisten im Rahmen der Fernwartung erfolgt im Allgemeinen mit besonderen Zugriffsrechten, die mindestens dem des Administrators oder Superusers gleichgestellt sind. Oft gehen sie aber auch darüber hinaus.

Potenziell Zugriff auf alle Daten

Daher muss der Besitzer des ferngewarteten Rechners oder Systems davon ausgehen, dass im Rahmen der Fernwartung oder -unterstützung ein Zugriff auf alle Daten möglich ist.

Unter Umständen ist der Zugriff auf Daten durch den Dienstleister oder Hersteller auch notwendig, da die Fehlfunktion durch ein bestimmtes Datum ausgelöst wurde.

Das BDSG regelt auch die Fernwartung

Wird ein System gewartet, das personenbezogene Daten bearbeitet, können die Administratoren mit ihren besonderen Rechten meist auch auf die personenbezogenen Daten zugreifen.

Sind sie bei einem andern Unternehmen beschäftigt, können auf diese Art sogar Daten ungewollt übermittelt werden. Deshalb enthält das BDSG seit seiner Novelle im Jahre 2001 in § 10 eine besondere Vorschrift zum Thema „Fernwartung“:

Die Vorschriften zur Auftragsdatenverarbeitung sind demnach auch dann anzuwenden, wenn *„die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.“*

Es gelten dieselben Regeln wie bei der Auftragsdatenverarbeitung

Alle von der Auftragsdatenverarbeitung bekannten Regelungen sind auch bei der Fernwartung anzuwenden:

„Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.

Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.“

Eine wesentliche Konsequenz ist die Mitverantwortung für fehlende Schutzmaßnahmen. Der Auftraggeber muss diese nicht nur vorgeben, sondern auch überprüfen.

Notwendige Löcher in der Firewall

Bei der Fernwartung muss natürlich von außerhalb des Unternehmens auf interne Systeme zugegriffen werden. Die Firewall des Unternehmens, die genau dies im Normalbetrieb unterbinden soll, muss also geöffnet werden, damit der Fernzugriff möglich wird.

Es versteht sich von selbst, dass das Unternehmen die Firewall-Regeln mit größter Sorgfalt konzipieren muss. So verhindert es, unnötig große Löcher in die Firewall zu „bohren“.

Regeln für den Zugriff von außen

Es muss u.a. genau festlegen,

- von welchen Systemen beim Dienstleister (Quell-IP)
- über welche Netzwerk-Protokolle (Ziel-Ports)
- auf das zu wartende System (Ziel-IP) zugegriffen werden soll.

Seien Sie beim Thema Quell-IP nicht zu großzügig, nur weil beispielswei-

Unternehmen, die externe IT-Unterstützung in Anspruch nehmen, müssen klare Sicherheitskonzepte umsetzen.

se der Service-Techniker von seinem Notebook, egal wo er sich gerade aufhält, zugreifen will.

Den Zugriff zeitlich begrenzen

Da der Fernzugriff nicht permanent nötig ist, sondern nur nach Voranmeldung oder festgelegten Zeiten, können die erforderlichen Firewall-Regeln vorbereitet und dann deaktiviert werden. So ist sichergestellt, dass die Firewall keine unnötigen „Löcher“ hat.

Nur bei Bedarf aktiviert der Firewall-Administrator die Fernzugriffsregeln für die Wartung. Unmittelbar nach der Aktion deaktiviert er sie wieder.

Nur so kann er sicherstellen, dass die Firewall das Unternehmensnetz zu jedem Zeitpunkt maximal schützt.

Beobachten Sie die Zugriffe

Bei der Fernwartung ist die zentrale Frage, ob der Auftraggeber mitbekommt, was der Dienstleister während der Fernwartungssitzung genau tut.

Es gibt nur eine Möglichkeit, dieses Problem zu lösen: Der Dienstleister muss während der Fernwartungssitzung „beobachtet“ werden.

Protokollieren oder live zuschauen

Eine Möglichkeit ist, alle Aktionen während der Fernwartung in Log-Dateien detailliert zu protokollieren und im Nachinein auszuwerten.

Wer noch genauer hinschauen will und dies vielleicht sogar in Echtzeit tun möchte, muss die Arbeitssitzung live beobachten. Hierzu muss die laufende Sitzung auf den Monitor des Beobachters dupliziert werden.

Bei einer Remote-Desktop-Sitzung mit Fernsteuerung ist das im Allgemeinen recht einfach. Der Auftraggeber kann einfach den Bildschirm beobachten und so dem Dienstleister gleichsam auf die Finger schauen.

Schwarze Schafe wollen Verantwortung abgeben

Einige Anbieter von Fernwartung versuchen, das Bundesdatenschutzgesetz mit einer dubiosen Klausel in ihren allgemeinen Geschäftsbedingungen auszuhebeln: *„Der Auftraggeber stellt sicher, dass der Auftragnehmer im Rahmen der Fernwartung keinen Zugriff auf personenbezogene Daten hat.“*

Auf eine solche Klausel kann sich der Auftrageber nicht einlassen. Denn er kann nicht kontrollieren, ob die Regel auch eingehalten wird. Man müsste schon für die Dauer der Fernwartung alle personenbezogenen Daten aus dem System entfernen.

Hürden bei Verschlüsselung

Schwieriger ist die Kontrolle z.B. bei einer verschlüsselten SSH-Verbindung zu einem Unix- oder Linux-System. Hier lassen sich aber die Tastatureingaben und damit die eingegebenen Befehle mitprotokollieren. Der Auftraggeber kann dieses Protokoll dann später auswerten.

Am besten über einen unternehmenseigenen Server arbeiten lassen

Generell sollte die Fernwartung über einen unternehmenseigenen Login-Server abgewickelt werden. Auf diesem Sever lässt sich die Fernwartung genau beobachten. Gleichzeitig erschwert ein solches Gateway den unbeobachteten Abzug von personenbezogenen oder anderen vertraulichen Daten.

Gleiche Regeln gelten für einen externen Helpdesk

Es gehört in vielen Unternehmen zum Standard, dass die Helpdesk-Mitarbeiter per Fernzugriff auf den Desktop des Hilfesuchenden zugreifen, um ihn zu unterstützen.

Sobald der Helpdesk an eine Fremdfirma übertragen wurde, haben wir es mit der normalen datenschutzrechtlichen Problematik der Fernwartung zu tun. Dabei spielt es keine Rolle, ob diese Fremdfirma eine Konzerntochter ist oder nicht, da das BDSG keine Konzernprivilegierung kennt.

Achtung: Mitarbeiter dürfen nicht über den Helpdesk kontrolliert werden!

Es kommt aber ein weiterer Problemkreis dazu. Denn über den Fernzugriff auf den Desktop lassen sich die Beschäftigten auch überwachen.

Bei professionellen Systemen muss der Hilfesuchende aktiv den Zugriff freischalten. So weiß der Beschäftigte, dass gerade jemand seinen Bildschirm sieht, und er kann sich darauf einrichten. Er kann auch nachvollziehen, was der Helpdesk-Mitarbeiter tut und welche Daten er sieht.

Augen auf bei der Vertragsvergabe!

Datenschutzbeauftragte müssen Fernwartung und -hilfe unter Sicherheitsgesichtspunkten sorgfältig planen. Dabei gilt es, die korrekte Implementierung und die Schutzwirkung der Sicherheitsmaßnahmen zu überprüfen.

Der Auftraggeber muss die organisatorischen Rahmenbedingungen in Form eines Vertrags festlegen. Darin müssen die Vorschriften für die Auftragsdatenverarbeitung enthalten sein. Entsprechende Vorlagen finden Sie beispielsweise auf den Webseiten der Datenschutzbehörden.

Prüfen Sie die AGBs

Prüfen Sie die allgemeinen Geschäftsbedingungen der Dienstleister sorgfältig und akzeptieren Sie sie nicht automatisch!

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der Hochschule München.