Fernadministration von Firewalls – Der Feind in meinem Bett

Die Komplexität der IT-Struktur steigt von Jahr zu Jahr rasant an: während vor fast 70 Jahren Konrad Zuse mit ein paar Relais in einem programmgesteuerten Rechner seinen Kollegen die Arbeit erleichtern wollte, sind die heutigen Technologien so komplex, dass ein einzelner Administrator kaum den Überblick über in seinem Netzwerk eingesetzten Technologien behalten kann. Dankbar nimmt er die Angebote externer Firmen an, die ihn jederzeit unterstützen und sich per Fernwartung in das Firmennetzwerk einloggen.

Internet for Absolute Beginners

Alle wollen ins Internet, aber keiner macht sich Gedanken wie, Hauptsache:"…ich bin drin!!" Provider bieten Pakete mit Flatrates, locken mit Spielekonsolen bei Vertragsabschluss und als Kundenservice, einem Router, der sich fast von selbst einrichtet. Freundliche Mitarbeiter der Anbieter konfigurieren den Zugang zum Internet wie von Geisterhand und schon ist man drin. Welchen Risiken sich der Privatmann hier aussetzt, ist den wenigsten bewusst. Dankbar nutzt man die Einrichtung der kleinen Firewall, teilt mit fremden Menschen die Passwörter und somit den Zugang zu den privaten digitalen Daten.
Überträgt man diese Vorgehensweise in das reale Leben, so ist das so, als ob ein netter junger Mann den Hausschlüssel des Einfamilienhauses an sich nimmt und garantiert, dass er ihr Eigentum schützen wird. Während Sie sich in Sicherheit wiegen, nimmt der junge Mann schon mal die Wertsachen in Gewahrsam – dann können sie auch nicht gestohlen werden. Irgendwie logisch!?

Wenn der Router zweimal bootet

Was bei Privatanwendern schon gang und gäbe ist, ist in Firmen häufig nicht anders: Viele Provider übernehmen die Einstellungen am Router aus Sicherheitsgründen selbst und oft haben die Administratoren nicht einmal die Passwörter. Den Überblick, welche Ports geöffnet sind und welche nicht, haben die wenigsten. Die moderne IT wird immer komplexer und die meisten Firmen sind gezwungen, sich das Know-How zuzukaufen. Genau dieses fehlende Wissen ist es, das die IT-Verantwortlichen weder vor Strafe schützt, noch sie veranlasst, richtige Verträge mit dem externen Dienstleister abzuschließen. Findige IT-Anbieter versuchen sich mit Hilfe ihrer eigenen AGBs aus der Verantwortung zu stehlen und zu vertuschen, dass sie eigentlich dem Gesetz der Auftragsdatenverarbeitung unterliegen.

Von Rechten und Pflichten

Ganz gleich, wie man es dreht oder wendet, der Betreiber eines Netzes ist auch dafür verantwortlich und muss den Datenschutz und die Datensicherheit gewährleisten, auch wenn er keine Ahnung hat, wie seine Firewall konfiguriert ist. Aus diesem Grund empfiehlt es sich, die Aufträge an externe Dienstleister immer schriftlich zu formulieren, mündlich getroffene Vereinbarungen umgehend schriftlich niederzulegen und die Ausführung umgehend zu kontrollieren und Mängel unmittelbar Kund zu tun.
Der externe Dienstleister darf nicht ohne genauen Auftrag oder gar ohne das Wissen des Auftraggebers tätig werden. Auch dies muss unbedingt geregelt und kontrolliert werden.

Aber gerade die Kontrolle ist das Problem, weil der Auftraggeber das nötige Wissen meist nicht oder nur unzureichend hat. Ihm fehlt die Möglichkeit, den Dienstleister zu kontrollieren und er begibt sich völlig in die Hand eines Fremden. Dies ist fatal und entbindet den Netzbetreiber nicht vor der datenschutzrechtlichen Haftung. Deshalb müssen die Rechte des Dienstleisters auf ein Minimum beschränkt und deren administrative Tätigkeiten revisionssicher dokumentiert werden.

... ich weiß, was Sie gestern getan haben!

Wenn das ein Netzbetreiber von seinem Dienstleister sagen kann, ist er schon fast auf der sicheren Seite. Bevor ein externer Dienstleister beauftragt wird, müssen Rechte und Pflichten beider Parteien exakt festgelegt werden. Dazu gehören auch die genauen Zugriffsrechte, die der Dienstleister benötigt. Um Risiken für das Netzwerk zu minimieren, müssen geeignete technische Maßnahmen ergriffen werden und vor allem, der zuständige Administrator geschult werden. Um das Risiko klein zu halten, sollte das „Vier-Augen-Prinzip" gelten und mit geeigneten Authentifizierungsmethoden sichergestellt werden, dass nur spezielle Personen auf die sicherheitsrelevanten Geräte zugreifen. Dem Systembetreiber sollte jederzeit bekannt sein, mit welchen Mitteln auf welche Daten zugegriffen wurde und was damit gemacht wurde. Außerdem sollte der Zugriff nur aus dem Netzwerk heraus eingeleitet werden und nicht vom Dienstleister. Die ganze Aktion muss revisionssicher protokolliert werden.

Drum prüfe, wer sich ewig bindet!

Auf der Internet-Seite des hessischen Datenschutzbeauftragten finden sich Hinweise und Musterverträge, um diese Gefahren schriftlich zu bannen. In diesen Verträgen werden Kontrollmechanismen festgelegt, die den Zutritt, die Benutzer sowie den Zugriff regeln, genauso wie die Datenverarbeitung, die Verantwortlichkeit, die Dokumentation und die Kontrolle der Organisation festgeschrieben werden.
Nur mit detaillierten Verträgen kann ein Teil der Verantwortung auf den Auftragnehmer übertragen werden.

Diskutieren Sie mit im Forum: Wie wichtig ist Datenschutz in deutschen Unternehmen? Was bringt er wirklich?

Alexandra Klawonn, ADS-Consult,
IT-Sachverständige und externe Datenschutzbeauftragte DSB-TÜV 2010