# Betriebsvereinbarungen und Arbeitsverträge

Sich als Forensiker mit Betriebsvereinbarungen und Arbeitsverträgen zu befassen scheint so ungewöhnlich, wie wenn der Pathologe Tipps für das gesunde Leben gibt. Doch auf den zweiten Blick sind beide Dinge gar nicht so abwegig, denn wer wüsste besser als der Pathologe, welche Krankheiten die häufigsten sind, die ihm auf seinen Seziertisch kommen. Genauso ist es bei den IT-Forensikern, die immer dann gerufen werden, wenn der „Patient IT" auf den Seziertisch muss. Dabei braucht es in vielen Fällen gar nicht so weit zu kommen, denn eine der häufigsten Ursachen für einen (Super)-GAU in der IT ist mangelndes Wissen. Mangelndes Wissen des Benutzers, des Administrators und nicht zuletzt der Geschäftsleitung.

Unsicherheiten im Umgang mit der EDV haben oft fatale Folgen. Wer kennt als Administrator nicht den Spruch: „Ich habe nichts gemacht! Nur OK gedrückt." (… am Kabel gezogen, … ausgeschaltet, … das Fenster weg geklickt, ….) Fast alle verhängnisvollen Katastrophen beginnen mit einem dieser Sätze. Dabei könnten viele EDV-Unfälle vermieden werden, wenn die Mitarbeiter, die Administratoren und auch die Geschäftsleitung Leitfäden an der Hand hätten, die ihnen im Unsicherheitsfall Hilfe bieten könnten. Dabei kann es sich „hochoffiziell" um Betriebsvereinbarungen und Arbeitsverträge handeln (empfehlenswert für größere Betriebe und größere KMUs) oder ein spezieller Bereich im Intranet, indem heimlich und schnell nachgeschlagen werden kann.
In diesem Beitrag werden nur Maßnahmen behandelt, die vom Personal, also den Menschen des Unternehmens getroffen werden können, um die EDV des Unternehmens zu schützen. Das schöne an diesen Maßnahmen ist, dass sie das Unternehmen kein Geld kosten, sondern lediglich etwas Hirnschmalz und Aufmerksamkeit der Mitarbeiter und Geschäftsführung.
Der wichtigste Punkt, der dem ganzen Maßnahmenkatalog vorausgeht, ist die Erkenntnis, dass die EDV und die Daten eines Unternehmens schützenswert sind. Auf sie muss genauso geachtet werden, wie auf die persönlichen Gegenstände am Arbeitsplatz, denn es ist sehr unwahrscheinlich, dass Sicherheitslücken in der EDV lange ungenutzt bleiben. Warum sollten Cyber-Verbrecher über den Zaun steigen und die Alarmanlage aushebeln, wenn Daten über das Internet abgezogen werden können oder ein paar Euro an einen unzufriedenen Mitarbeiter den elektronischen Zugriff auf Firmengeheimnisse ermöglichen.
Geregelt werden müssen 6 Teilbereiche. Dazu gehören die betriebliche Infrastruktur, die betriebliche Organisation, Verantwortungsbereiche des Personals, der Einsatz geeigneter Hard- und Software, Regeln zu betrieblichen Kommunikation und das Erstellen und Einhalten von Notfallplänen.

## Infrastruktur

Zur Absicherung der Infrastruktur gehören bauliche Maßnahmen, über die ein Betrieb meist sowieso verfügt. Dabei sollte geregelt sein, dass der Zutritt zu den zentralen EDV-Systemen vom produktiven Betrieb getrennt ist und eine Zugangskontrolle vorhanden ist und diese nicht durch offene Türen und Fenster umgangen wird. Brandschutzmaßnahmen und eine geeignet Kühlung sind ebenfalls von Nöten, sowie deren Einhaltung und Kontrolle.
Gerade in kleineren Betrieben sind die zentralen Server im Büro und für jeden zugänglich, der Serverraum ist unverschlossen, wird als Abstellraum oder vom Reinigungspersonal mitgenutzt, sogar die Nutzung als Teeküche soll schon

vorgekommen sein. Nicht nur das administrative Personal, sondern jeder Mitarbeiter sollte darauf achten, dass die wichtigen Server im Unternehmen gut geschützt stehen.
Auch die Verkabelung der Geräte sollte, nicht nur aus Haftungsgründen, vom Fachmann vorgenommen werden und gegen Stromschwankungen und Blitzschlag abgesichert sein. Des Weiteren sollte geregelt werden, wo die Datensicherung der Systeme aufbewahrt wird. Eine funktionstüchtige Vollsicherung sollte sich dabei immer außerhalb der Firma befinden, im Bankschließfach oder bei einem vertrauenswürdigen Mitarbeiter im häuslichen Safe.
Obwohl Maßnahmen im Bereich EDV-Infrastruktur gerne dem technischen Personal überlassen werden, sollten die Benutzer auch darin geschult werden, ein Augenmerk darauf zu haben. Denn jeder kennt die Geschichten, dass Benutzer im guten Glauben den Firmendrucker einem angeblichen Servicetechniker mitgegeben haben und so firmeninterne Daten auf der Druckerfestplatte den Weg nach Draußen fanden.

## Organisation

Die organisatorischen Vereinbarungen werden immer gerne zur Seite geschoben, weil es hier um „Verantwortung" und zusätzliche Arbeiten geht. In jedem Unternehmen – und sei es noch so klein – sollte es einen Verantwortlichen geben, dem die Sicherheit der EDV unterliegt. Diese Aufgabe wird nicht gern übernommen, weil man sich möglicherweise nicht sehr beliebt bei den Kollegen und Chefs macht, denn in diesen Aufgabenbereich fallen unter anderem Regelungen von Zugriffsberechtigungen, Nutzungsverbote nicht freigegebener Software, Regelung zum Passwortgebrauch und das Herausgeben einer PC-Richtlinie. Weitere unerlässlich, aber notwendige Aufgaben sind die Regelungen von Wartungs- und Reparaturarbeiten externer Dienstleister, das Begleiten von fremden Personen durch den Betrieb, die Betreuung und Beratung von Benutzern und das Einrichten deren Arbeitsplatzes. Und damit nicht genug, kommt auf diese Person auch noch eine Menge Verwaltungsarbeit zu: Dokumentation von Benutzerberechtigungen, von Änderungen an den Systemen und Berichte über den Einsatz externer Firmen. Die Rückgabe von Altgeräten muss geregelt werden, wie der Datenaustausch in der Firma auszusehen hat, sowie die Kontrolle des „aufgeräumten Arbeitsplatzes" und Richtlinien zum Fernzugriff der eigenen Mitarbeiter und Fremdfirmen. Gerade die letzte Tätigkeit führt oft zu Unmut in den Firmen, weil sich Mitarbeiter bespitzelt vorkommen. Hier kann mit Hilfe von Schulungen und Aufmerksam machen auf das Gefahrenpotential viel Brisanz aus dem Thema genommen werden.
Studien zeigen, dass gut informierte Mitarbeiter solche Angebote wie Schulungen häufiger in Anspruch nehmen und sicherer mit ihrer IT-Umgebung umgehen. Unwissenheit macht immer auch unsicher.
Ein Security-Consultant formulierte den Erfolge seiner Tätigkeit folgendermaßen: „Wenn ich in den Firmen von den Mitarbeitern nicht mehr gegrüßt werde, dann habe ich einen guten Job gemacht!" Ob feindselige Blicke immer der Gradmesser für IT-Sicherheit sein sollten, ist fraglich, aber im Prinzip geht es schon in die richtige Richtung. Allerdings kann man mit der Bewußtseinsschaffung für Gefahren im EDV-Bereich böse Blicke vermeiden und gleichzeitig zusätzliches „Personal" für den Datenschutz requirieren, denn wenn viele aufpassen, sehen zig Augen mehr als nur die zwei vom Administrator.

## Personal

Der Bereich Personal wird in Unternehmen häufig unterbewertet. Nur große Betriebe leisten sich eine Einführungsveranstaltung für ihre neuen Mitarbeiter. In diesen Bereich fallen nicht nur die Einführung in die Unternehmenskultur, sondern auch Hinweise, welche Gesetzte, Regelungen und Vorschriften beachtet werden müssen, wer, wen vertritt, sowie Schulungen für bestimmte Programme und Warnsignale: Wer muss gerufen werden, wenn am Drucker das rote Licht, der Server pfeift oder die Warnlampe am Eingang zum Serverraum blinkt.
Viel zu wenig beachtet wird die mentale Verfassung der Mitarbeiter. Nur selten gibt es Anlaufstellen für persönliche Probleme (Lohnpfändung, Scheidung, Krankheit), die dazu führen können, dass Mitarbeiter ihrem Betrieb nicht mehr so loyal gegenüber stehen. Je unzufriedener ein Mitarbeiter mit seinem Unternehmen ist, desto anfälliger wird er für „social engineering", das heißt, er gibt unbeabsichtigt in seiner Wut Informationen weiter oder ganz gezielt, um sich möglicherweise finanziell aufzubessern. Viele professionelle Organisationen und Geheimdienste wissen um diese Probleme und nutzen sie geschickt aus.
Ein anderer Punkt, der häufig vernachlässigt wird, ist die Schulung des Personals, also der Mitarbeiter und der Administratoren. Laufen die Geschäfte gut, dann ist keine Zeit für Schulung, laufen die Geschäfte schlecht, ist kein Geld da und das „Try-and-error"- Verfahren hält im Unternehmen Einzug.
Dabei wäre gerade jetzt die richtige Zeit, um Mitarbeiter zu schulen. Das Arbeitsamt bietet Maßnahmen für Mitarbeiter, die noch in Lohn und Brot stehen. WeGebAU ist für Mitarbeiter gemacht, die nicht die richtige Qualifikation für ihren Beruf haben (meist sind Administratoren Quereinsteiger), über 45 Jahre alt sind und die letzten 4 Jahre keine Leistungen vom Arbeitsamt bekommen haben. Trifft dies zu, übernimmt das Arbeitsamt die Kosten der Weiterbildung und der Chef muss die Administratoren nur noch von der Arbeitszeit freistellen, was in Zeiten von Kurzarbeit und Arbeitszeitverkürzung nicht besonders schwer sein dürfte.

## Hard- und Software

Im Bereich der Hard- und Softwareregelungen sollte nochmals auf den Gebrauch von Passwörtern hingewiesen werden, wie komplex sie sein sollten und wann sie getauscht werden müssen. Ebenso, dass der Bildschirmschoner mit einer Passwortsperre versieht, geheime Daten verschlüsselt werden und mobile Geräte nach den Unternehmensrichtlinien abgesichert werden. Im Rahmen dieses Punktes sollten auch Regelungen getroffen werden, welche Dateien potentiell als gefährlich gelten oder welche Dateien keinen Schaden anrichten können. Auch hier gilt, dass ein fundiertes Grundlagenwissen hilft Fehler zu vermeiden und Unternehmensdaten zu schützen.

## Kommunikation

Bei den Maßnahmen zur sicheren Kommunikation sind Regelungen zu treffen, die das Kommunikationsverhalten im Unternehmen absichern sollen. In diesen Bereich fällt der Umgang mit Handys (Herausnehmen des Akkus in geheimen Besprechungen, Abschalten der Bluetooth-Funktion), die Nutzung der Browser und das Surfverhalten (Einschränkung des privaten Surfens) und der Email-Kommunikation. Viel zuwenig Benutzer wissen, dass das Verbot der privaten Nutzung von Internet und Email nicht aus Boshaftigkeit der Unternehmensleitung herrührt, sondern das Ergebnis eines rechtlichen Konstruktes ist, häufig zu Streitfällen führt. Die private Nutzung von Internet und Email unterliegt dem Telekommunikationsgesetz. Wir diese gebilligt, ist es Administratoren nur noch

im Verdachtsfalle möglich, Protokolldateien einzusehen, weil er sonst gegen das Fernmeldegeheimnis verstößt. Eine schnelle und effiziente Fehlersuche ist in diesem Fall fast ausgeschlossen, wenn jedes Mal der Betriebsrat hinzugezogen werden muss.
Hierzu gehört auch eine Vereinbarung zum nachvertraglichen Wettbewerbsverbot, um das interne Wissen auch im Unternehmen zu halten.
Hierzu gehören auch Regelungen zum Ausscheiden von Mitarbeitern. Wie wird mit Firmeneigentum wie Handys, Notebooks und anderen digitalen Unterlagen verfahren? Besonders zu berücksichtigen sind Daten auf USB-Sticks und CDs, denn diese sind leicht zu übersehen und werden oft – nicht mal absichtlich – vergessen.

## Notfallpläne

Im Bereich der Notfallpläne sind hauptsächlich Regelungen für die administrative Fachabteilung zu treffen, aber auch nicht IT-Fachpersonal muss Kenntnis von Plänen im Katastrophenfall haben. Wer für welchen Notfall zuständig ist und was bei Feuer, Erdbeben, Hochwasser, etc. zu tun ist.

Die zu regelnden Punkte sind vielfältig und leicht kann der eine oder andere übersehen werden. Eine gute Basis sind die Vorschläge des BSI, die sehr detailliert sind. Nicht alle Punkte werden auf jedes Unternehmen zutreffen, können aber als durchaus als Gerüst verwendet werden. Je genauer interne Regelungen sind, desto weniger Datenverlust gibt es. Dabei muss aber immer eine Balance zwischen Gängelung der Mitarbeiter und Laissez-Faire gefunden werden, denn die besten Regelungen und Bestimmungen nützen nichts, wenn sie von den Mitarbeitern nicht akzeptiert werden und mutwillig untergraben werden.