Klaus Haller

Ethische Überlegungen zum Einsatz von Data-Loss-Prevention-Tools in Unternehmen

Snowden, CDs von Schweizer Banken oder die fast vergessene Bonusmeilen-Affäre – manche MitarbeiterInnen ignorieren arbeitsvertragliche und strafrechtliche Normen. Mögliche Gründe sind Frust, Geltungssucht oder der Reiz des schnellen Geldes. Manchmal passiert „nur" ein Fehler. Eine Mitarbeiterin verliert einen USB-Stick mit Forschungsergebnissen oder ein Mitarbeiter schickt eine Kundenliste an eine falsche E-Mail-Adresse. Ein solcher Datenabfluss *ist in hochkompetitiven, wissensintensiven Sektoren wie der Pharma- oder Automobilbranche besonders kritisch. Ähnliches gilt für Branchen mit sensiblen Kundendaten. Beispiele sind das Gesundheitswesen, Banken und Versicherungen. Auch der Sicherheitssektor ist gefährdet. Wie schützen sich also Unternehmen vor einem Datenabfluss?*

1 Data Loss Prevention Tools in Unternehmen

Wer einen schlechten Rat sucht, findet ihn in dem guten Artikel *The NSA and Snowden – How better security measures could have stopped the leak* in den *Communications of the ACM* [Tox14]. Der Artikel erklärt, wie klassische IT-Security-Methoden (Zugriffsrechte, Zwei-Faktor-Authentifizierung, Vier-Augen-Prinzip, Verschlüsselung etc.) verhindern, dass Administratoren Klartextdaten sehen. Natürlich sollten Administratoren den Inhalt von Datenbanken oder Dokumentensammlungen nicht im Klartext sehen, doch ist die Sicht viel zu eng. Auch viele „normale" Mitarbeiter sind ein Risiko, weil sie mit sensiblen Daten arbeiten. Wer die Profitabilität von Kundenbeziehungen analysiert und Margen bei Projekten prüft, kann allein mit diesen Daten einem Unternehmen ernsthaft schaden. Nicht der Zugriff auf Daten, sondern ein Datenabfluss ist das Problem. Klassische Security-Maßnahmen scheitern bei solchen Themen. Ihr Schwerpunkt liegt beim Datenzugriff, nicht beim Datenabfluss. IT-Security-Abteilungen erfahren viel zu oft erst aus der Presse von einem Datenverlust. Daher kombinieren immer mehr Unternehmen klassische IT-Security-Maßnahmen mit *Data Loss Prevention* (DLP). DLP-Tools erkennen, melden oder blockieren Datenabfluss. Dazu durchsuchen sie E-Mails, Dateien, Instant Messages und den Netzwerkverkehr nach kritischen Inhalten. Schlüsselwörter wie *al-Qaida* oder *streng vertraulich* können verdächtig sein, andere Unternehmen suchen nach Mustern von IBAN-Nummern oder *Social Security Numbers*. Je nach Konfiguration warnt ein DLP-Tool Mitarbeiter vor Fehlverhalten, es dokumentiert Verdachtsfälle, alarmiert Vorgesetzte, unterbindet E-Mails oder verschiebt kritische Dateien in sichere Verzeichnisse [Hal14]. Solche Tools werden oft von DLP-Teams betrieben, die aus dem Risiko-Management und weniger aus der IT-Security kommen.

Aus Sicht der Mitarbeiter schnüffeln das DLP-Team, die Personalabteilung und Vorgesetzte mittels DLP-Tools in „ihren" E-Mails, Instant Messages und Dateien herum. Ist ein solcher Einsatz von DLP-Tools angemessen? Was ist höher zu gewichten, der Wunsch des Arbeitgebers, Geschäftsgeheimnisse zu schützen, oder der Wunsch der Mitarbeiter, nicht überwacht zu werden? Gesetze geben juristische Antworten, die für Unternehmen verbindlich sind. Doch neben dem juristischen gibt es auch einen ethischen Aspekt. Dieser Artikel geht nicht auf den Aspekt der empirischen, deskriptiven Ethik ein (Was machen Unternehmen heute? Warum?). Er nähert sich dem Thema aus Sicht der normativen Ethik, die Prinzipien für „gutes Handeln" aufzeigen möchte [GW]. Dazu wendet er bekannte ethische Konzepte zur Überwachung erstmals auf DLP-Tools in Unternehmen an. Als Grundlage dient die Arbeit *Surveillance Ethics* von Kevin Macnish [Mac11], die eine Vielzahl an Quellen zu Ethik und Überwachung zusammenfasst.

Der Artikel ist dabei wie folgt aufgebaut: Zunächst grenzt Abschnitt 2 den Anwendungsfall genauer ein, bevor Abschnitt 3 die Folgen von Überwachung und DLP-Tools auf Unternehmen und Mitarbeiter erklärt. Abschnitt 4 geht der Frage nach, ob Mitarbeiter ein Anrecht auf Privatsphäre haben, wenn sie in der IT-Infrastruktur eines Unternehmens arbeiten. Schließlich entwickelt Abschnitt 5 konkrete Kriterien für den ethischen Einsatz von DLP-Tools in Unternehmen. Abbildung 1 veranschaulicht diese Gliederung graphisch.

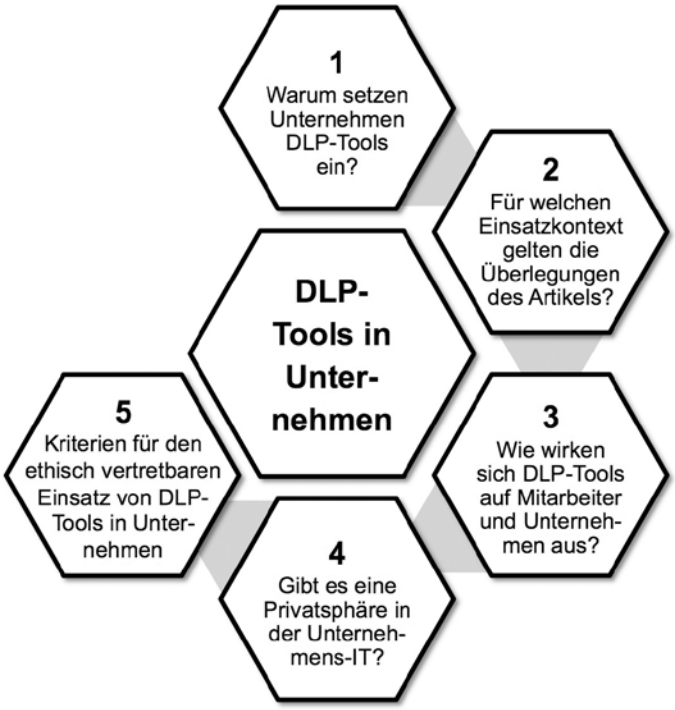

Abbildung 1: Themenüberblick

2 Berücksichtigter Einsatzkontext für DLP-Tools

Viele Technologien können missbraucht werden. Das gilt auch für DLP-Tools. Wer sie einsetzen möchte, muss zuerst ihre Missbrauchsrisiken und mögliche Gegenmaßnahmen analysieren. Dieser Artikel hilft dabei. Da DLP-Tools – wie fast jede Technologie – ethisch neutral sind, entscheidet der Einsatzkontext über „gut" oder „böse". Daher konkretisieren wir ihn mittels vier Annahmen:

1. Es geht um DLP-Tools in Unternehmen, nicht um staatliche Überwachung.

2. Das DLP-Tool soll Datenabfluss erkennen und unterbinden. Unternehmen messen nicht mittels DLP-Tools die Arbeitsleistung von Mitarbeitern und überwachen auch kein gewerkschaftliches Engagement.

3. Mitarbeiter werden nur innerhalb der Unternehmens-IT überwacht. Facebook, Xing etc. sind tabu, sofern kein Netzwerkverkehr über die Unternehmens-IT läuft.

4. Mitarbeiter können (teilweise) die Unternehmens-IT proaktiv vermeiden, auch während der Bürozeiten. Dazu verwenden sie private, mobile Geräte, die sich über das Mobilfunknetz mit dem Internet verbinden.

3 Überwachung durch DLP-Tools – Auswirkungen auf Mitarbeiter

Überwachung hat eine negative Konnotation, auch wenn sie teils im Interesse der Überwachten erfolgt. Macnish nennt als Beispiel Besitzer von Kreditkarten. Kreditkartenfirmen überwachen die Käufe ihrer Kunden. Weichen Einkäufe vom normalen Einkaufsverhalten ab, kann das ein Hinweis auf Kartenmissbrauch sein.

Doch nicht jede Überwachung erfolgt im Einvernehmen oder zum beiderseitigen Nutzen. Daher ist aus ethischer Sicht wichtig, wie sich Überwachung auf Menschen auswirkt. Macnish diskutiert unter anderem folgende Auswirkungen [Mac11]:

1. *Überwachung ersetzt Vertrauen* in Menschen und Mitarbeiter: Werden Menschen überwacht und drohen ihnen Sanktionen, verhalten sie sich meist korrekter als sonst. Wer Menschen überwacht, muss ihnen also weniger Vertrauen entgegenbringen.

2. Überwachung führt bei den Überwachten zu mehr *Stress*.

3. Überwachung kann übermäßige *Selbstzensur* bei der Kommunikation auslösen. Man ist vorsichtig und unterlässt Äußerungen oder Aktivitäten, um nicht gegen Regeln zu verstoßen oder aufzufallen (*chilling*).

4. Es gibt einen *Autonomieverlust* bezüglich der Selbstdarstellung. Dritte könnten durch die Überwachung Informationen erhalten, die man ihnen nicht geben würde.

5. Die eigene *Kommunikation* mit Dritten wird *befangener*. Man weiß nicht, was Gesprächspartner von eigenen Schwächen und Fehlern durch die Überwachung wissen.

6. Weniger Privatsphäre *erschwert, Vertrauensverhältnisse* aufzubauen.

3.1 Überwachung mit DLP-Tools – erwünschte Auswirkungen für Unternehmen

Drei der sechs Auswirkungen sind Gründe, warum Unternehmen DLP-Tools einsetzen. Konkret sind das Vertrauensersatz, Selbstzensur und Autonomieverlust. Vertrauensersatz ist besonders in großen Unternehmen ein Thema. Je mehr Mitarbeiter sensible Daten sehen, desto größer ist das Risiko, dass eine Person fahrlässig oder kriminell handelt und dabei Daten abfließen. DLP-Tools reduzieren das Risiko, indem sie transparent machen, wie Mitarbeiter mit sensiblen Daten umgehen. Das sorgt für Selbstzensur und Autonomieverlust. Mitarbeiter werden bei sensiblen Daten vorsichtiger und verzichten auf riskante Aktionen. Das hilft den Unternehmen.

Der letzte Absatz klingt nach einem Plädoyer für totale Überwachung – ‚DLP-Tools sind gut, weil sie Unternehmensziele durchsetzen'. Das ist zu einseitig. Jede Demokratie lebt von freier Meinungsäußerung. Es ist eine Katastrophe, wenn staatliche Überwachung zu Selbstzensur und Autonomieverlust führt. In diesem Artikel geht es aber nicht um einen demokratischen Staat, der seine Bürger überwacht. Es geht um Unternehmen, die durch Überwachung Datenabfluss verhindern wollen. Selbstzensur und Autonomieverlust beziehen sich auf einen engen Bereich der täglichen Arbeit – auf den Umgang mit sensiblen Daten, insbesondere in der elektronischen Kommunikation. Deswegen sind DLP-Tools in Unternehmen für Mitarbeiter weniger bedrohlich als staatliche Überwachung, die Bürger rund um die Uhr beobachtet. Trotzdem haben DLP-Tools natürlich auch in Unternehmen unerwünschte Folgen.

3.2 Überwachung mit DLP-Tools – Nebenwirkungen

Einige der von Macnish genannten Auswirkungen von Überwachung sind im Falle von DLP-Tools in Unternehmen unerwünscht. DLP-Tools beeinflussen Mitarbeiter und ihre Arbeitsweise. Abläufe im Unternehmen können ineffizienter werden oder bei Mitarbeitern *Stress wegen Überwachung* [MW00] auslösen. Genauso kann Stress entstehen, weil Mitarbeiter wissen, dass sie unzulässig mit sensiblen Daten umgehen. Eigene Bequemlichkeit kann der Grund sein, unpassende Prozesse und Tools ebenso. Hier decken DLP-Tools auf, wenn *Soll* und *Ist* abweichen. Doch Stress für Mitarbeiter trifft letztlich auch die Unternehmen, wenn Arbeitszufriedenheit und Leistung sinken.

Eine andere negative Auswirkung von DLP-Tools ist, dass sie die Teambildung erschweren können. Viele Unternehmen haben Teams, deren Mitarbeiter weltweit verteilt arbeiten. Informelle E-Mails oder Instant Messages über Urlaub und Hobbies helfen den Teammitgliedern, Vertrauen aufzubauen und Kontakte zu pflegen. Merken Mitarbeiter, dass ihre Vorgesetzten mittels DLP-Tools E-Mails und Instant Messages heimlich mitlesen, wird die *Kommunikation befangener. Vertrauensverhältnisse* sind *schwieriger* aufzubauen. Die Teamleistung droht schlechter zu werden.

Zusammenfassend lässt sich sagen: DLP-Tools sind für viele Unternehmen sinnvoll. Allerdings müssen die Risiken für die Arbeitsleistung beachtet werden, die von Überwachungsstress oder schlechterer Zusammenarbeit ausgehen können. Decken DLP-Tools Schwachstellen beim Umgang mit sensiblen Daten auf, hängt viel von der Unternehmenskultur ab. Es kann eine positive Dynamik entstehen sich zu verbessern, aber auch ein Klima der Angst.

Doch zunächst stellt sich eine andere Frage: Dürfen Mitarbeiter eine Privatsphäre beanspruchen, wenn es um Dateien, Instant Messaging oder E-Mails innerhalb der Unternehmens-IT geht?

4 Privatsphäre, DLP-Tools und die Unternehmens-IT

MitarbeiterInnen haben auch in Unternehmen ein Recht auf Privatsphäre. Dieses Recht gilt nicht uneingeschränkt. Wer im Supermarkt an der Kasse arbeitet, kann sich nicht auf seine Privatsphäre berufen, wenn sein Bargeldbestand geprüft wird. Für DLP-Tools ist also zu klären, ob sie Bereiche überwachen, die eigentlich zur Privatsphäre der Mitarbeiter gehören.

DLP-Tools überprüfen Dateien und E-Mails auf sensible Unternehmensdaten. Aus Sicht der Privatsphäre ist das zentrale Problem, dass DLP-Tools wie Schleppnetze beim Fischfang arbeiten. Im Schleppnetz verfangen sich viele Fische, die man verkaufen kann. Daneben gibt es „Beifang", unverkäufliche Fische oder Müll. Man möchte ihn nicht, doch er ist unvermeidlich und kostet Zeit und Geld. Egal wie gut DLP-Tools arbeiten und wie integer das DLP-Team ist, auch bei DLP-Tools gibt es Beifang, die *False Positives*. DLP-Tools filtern aus E-Mails, Dateien, und Netzwerkverkehr mittels Regeln und Heuristiken Verdachtsfälle heraus (Abbildung 2). Verdachtsfälle sind Dateien oder E-Mails mit potenziell unerlaubten, sensiblen Daten. Stellt sich ein Verdachtsfall als harmlos heraus, ist er ein *False Positive*. Doch vorher hat ein Mitarbeiter des DLP-Teams die konkrete E-Mail möglicherweise gelesen. Ist die E-Mail aus Sicht des Unternehmens harmlos, enthält aber private Daten, ist die Privatsphäre eines Mitarbeiters verletzt. Doch warum haben Mitarbeiter überhaupt private Daten in der Unternehmens-IT? Ein Blick zurück in die 1960er Jahre gibt die Antwort.

In den Schwarzweißfilmen der 1960er Jahre gibt es Kaffeeklatsch im Pausenraum und in Büros mit vielen Aktenordnern. Die Aktenorder enthalten Briefe und Gesprächsprotokolle. Es ist normal, wenn Vorgesetzte Akten einsehen. Nicht akzeptabel sind heimliche Tonbandaufnahmen im Pausenraum. Das flüchtige, gesprochene Wort im Pausenraum und archivierte Briefe und Protokolle in Aktenordnern sind zwei getrennte Welten. Diese Zeiten sind heute vorbei. Verträge, Protokolle, Austausch von Ideen und Smalltalk, alles geht über die gleichen elektronischen Kanäle. Die Trennung – Akten sind für alle einsehbar, Gespräche sind privat – existiert nicht mehr. Verlieren nun Mitarbeiter ihr Recht auf Privatsphäre, weil in Unternehmen formale und informale Kommunikation über die gleichen Kanäle laufen? Das ist mehr als fraglich. Neben vermeidbarer privater Kommunika-

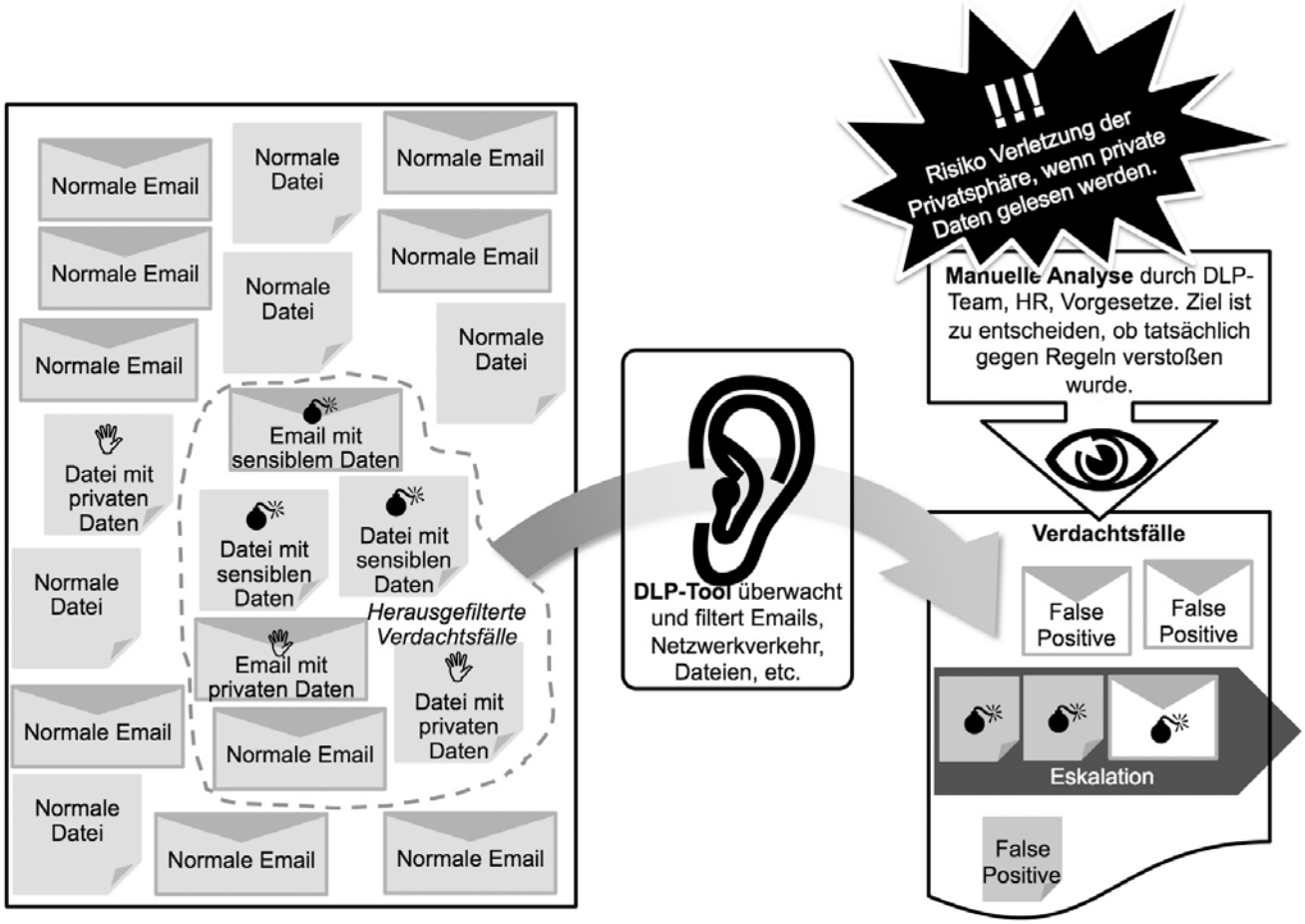

Abbildung 2: Funktionsweise von DLP-Tools und (Haupt-)Risiko der Privatsphären-Verletzung

tion gibt es nämlich *geduldete, geförderte und sogar notwendige private Kommunikation* im Unternehmensnetzwerk. Dazu vier Beispiele:

- *Informale Gespräche und Smalltalk*. Details aus privaten Aktivitäten oder Fotos werden mit Kollegen geteilt. Damit sind sie in der Unternehmens-IT. Teams bauen so leichter persönliche Beziehungen und Vertrauen auf. Das Unternehmen profitiert. Die Mitarbeiter riskieren aber, dass die Kommunikation peinliche Momente enthält. Filtert das DLP-Tool zufällig den peinlichen Moment als „Beifang", verbreitet er sich möglicherweise im Unternehmen. Chancen und Risiken für Mitarbeiter und Unternehmen wären so nicht fair verteilt.

- *Regelungen kleinerer persönlicher Angelegenheiten*, die nur zu Bürozeiten möglich sind und IT-Infrastruktur benötigen. Beispiele sind telefonische Rückfragen zu Online-Formularen oder zum Online-Banking, für die man auch die eigenen Daten sehen muss. Erledigen Mitarbeiter solche Anliegen schnell (!) am Arbeitsplatz anstelle Urlaub nehmen zu müssen, vermeidet das Störungen betrieblicher Abläufe aufgrund von Abwesenheiten.

- *Persönlich-geschäftliche Daten* wie E-Mails mit Bezug zu Personalthemen (Gehalt, Urlaub, Abwesenheiten wegen Krankheit). Die Kommunikation erfolgt zwingend innerhalb der Unternehmens-IT. Trotzdem muss das Unternehmen solche persönliche Daten der Mitarbeiter besonders schützen.

- Bei *bring your own device* (BYOD) arbeitet ein Mitarbeiter auf seinem eigenen Laptop. Mitarbeiter können erwarten, dass E-Mails bei Webmail-Anbietern und private Dateien nicht überwacht werden. Das DLP-Tool des Unternehmens darf private Laptops nicht beliebig durchsuchen.

Die Beispiele zeigen, dass Mitarbeiter aus ethischer Sicht eine Privatsphäre erwarten dürfen, auch in der Unternehmens-IT, selbst wenn das Unternehmen jede private Nutzung verbietet. Folgende Fragen helfen, die Situation und die Erwartungen zu klären:

1. Ist informale Kommunikation unter MitarbeiterInnen über elektronische Kanäle im Intranet erlaubt, geduldet oder erwünscht? Für welche Mitarbeiter gilt dies? Gilt es für E-Mails, Instant Messaging und auch für private Fotos und Videos?

2. Ist informale Kommunikation mit Kunden über elektronische Kanäle erwünscht? Für welche Mitarbeiter gilt dies? Gilt es für E-Mails, Instant Messaging und auch für private Fotos und Videos?

3. Müssen sensible Personalthemen oder andere Themen im privat-beruflichen Grenzbereich über das Intranet abgehandelt werden? Welche? Geht es um elektronische Kommunikation und/oder um Dateien? Wer ist betroffen?

4. Wie sieht die Abgrenzung bei BYOD zwischen privater und beruflicher Kommunikation beziehungsweise bei Dateien aus?

Das Management, die Rechts- und die Personalabteilung müssen bindende Antworten geben. Das DLP-Team hat eine rein beratende Funktion.

5 Ethische Voraussetzungen für DLP-Tools in Unternehmen

Manche Autoren lehnen jede Überwachung von Mitarbeitern ab (siehe z. B. [Int03]). Das ist sehr einseitig. Natürlich können DLP-Tools die Privatsphäre von Mitarbeitern verletzen, doch genauso können sie sowohl Unternehmen als auch Mitarbeitern helfen. Will ein Mitarbeiter versehentlich sensible Daten per E-Mail an eine private Adresse schicken, kann ein DLP-Tool davor warnen. Das hilft dem Mitarbeiter und dem Unternehmen. DLP-Tools können existenzbedrohende Datenverluste verhindern. Davon profitieren das Unternehmen und alle Mitarbeiter, deren Arbeitsplätze nicht gefährdet werden. Daher nimmt der Artikel an, dass DLP-Tools ethisch angemessen sein *können*, aber Motiv und Ausgestaltung pro Einzelfall zu prüfen sind. Basierend auf [Mac11] formulieren wir fünf Prüfanforderungen: lauteres Motiv, Befugnis, Notwendigkeit, Angemessenheit und Organisation (siehe Abbildung 3). Ein Unternehmen muss stets alle fünf Anforderungen erfüllen, nicht nur einzelne.

Abbildung 3: Voraussetzungen für ethische Überwachung, zum Beispiel durch DLP-Tools in Unternehmen

5.1 Lauteres Motiv

Zentral für die ethische Beurteilung von Überwachung ist ihr Zweck (*purpose*) [Mac11]. Hat ein Unternehmen ein lauteres Motiv für die Überwachung? Das ist für DLP-Tools gegeben, wenn ein Unternehmen Datenabfluss erkennen und verhindern will. Ein unlauteres Motiv wäre, E-Mails von Mitarbeitern aus Neugierde zu lesen oder gewerkschaftliche Aktivitäten auszuspionieren.

5.2 Befugnis

Macnish spricht von einer Befugnis für das Überwachen (*authority*) [Mac11]. Das ist für staatliche Institutionen leicht zu erklären. Soll ein Nachrichtendienst Terroristen und die organisierte Kriminalität beobachten, sammelt er spezifische Daten über sie und nicht Daten über Falschparker, Raser oder Politiker. Das Konzept lässt sich auf DLP-Tools in Unternehmen übertragen. Ein DLP-Team betreibt das DLP-Tool und bearbei-

tet Verdachtsfälle. Dafür braucht es eine Befugnis als Auftrag. Ein DLP-Team kann sich nicht selbst ermächtigen. Falls die Unternehmensleitung nicht gerade einen „Blanko-Scheck" ausstellt, ist eine *kombinierte Befugnis* von Linienvorgesetzten und Dateneigentümern erforderlich.

Die *Linienvorgesetzten* müssen zustimmen, wenn ein DLP-Tool ihre Mitarbeiter überwachen soll. Die *Dateneigentümer* (*Data Owners*) entscheiden, welche Daten sensibel sind. Interne Sicherheitsrichtlinien (siehe zum Beispiel [Mtu11]) regeln solche Aufgaben. Welche Daten sensibel sind, hängt vom Kontext ab. Das können Kundenlisten, Forschungsergebnisse oder Angebote für Kunden sein. Klassifizieren Unternehmen konsequent, wie vertraulich ihre Dokumente und Daten sind – zum Beispiel „öffentlich", „intern", „vertraulich" – ist das eine Grundlage für DLP-Tools. Sie könnten so konfiguriert werden, dass sie als vertraulich klassifizierte Daten finden, aber möglichst nicht als öffentlich oder intern klassifizierte Daten.

5.3 Notwendigkeit

Notwendig ist eine Überwachungsmaßnahme, wenn das Schutzziel entweder nur mit ihrer Hilfe sinnvoll erreicht werden kann oder wenn alle Alternativen (noch) mehr Nachteile haben [Mac11].[1] Bei DLP-Tools ist zunächst zu klären, ob die Suchalgorithmen E-Mails und Dateien mit sensiblen Daten dieses Unternehmens aufspüren können. Außerdem sind Alternativen zu einem DLP-Tool zu prüfen. Kann man sensible Daten auf einem isolierten Rechner ohne Netzwerkanbindung ablegen? Kann man den Personenkreis mit Zugriff auf sensible Daten verkleinern? Vielleicht reicht es, einzelne Teams zu überwachen anstelle aller Mitarbeiter.

Zur Notwendigkeit gehört bei DLP-Tools auch die Frage, ob und wann der Mitarbeiter, seine Vorgesetzten, das DLP-Team, IT-Security oder die Personalabteilung informiert werden. Wer sieht Metadaten wie Dateinamen oder die Empfänger der E-Mails? Wer liest E-Mails oder Instant-Messaging-Protokolle oder schaut sich Dateien an? IT-Security muss nicht zwangsläufig den Inhalt verdächtiger E-Mails sehen, gerade wenn E-Mails automatisch blockiert werden und keinerlei Verdacht auf kriminelles Fehlverhalten vorliegt.

5.4 Angemessenheit

Angemessenheit verlangt eine Abwägung zu treffen. Rechtfertigen die Risiken, denen ein Unternehmen ausgesetzt ist, einen Eingriff in die Privatsphäre der Mitarbeiter? Es gibt drei Aspekte zu beurteilen:

1. Verhältnismäßigkeit
2. Diskriminierungsfreie, sachgerechte Auswahl, wer und was überwacht wird
3. Absolute Schranken der Überwachung

Verhältnismäßigkeit – proportionality und *discrimination* – fragt, ob die Stärke des Eingriffs in die Privatsphäre und die Anzahl der überwachten Personen angemessen sind [Mac11]. Ein DLP-Tool zum Schutz von Kundendaten ist nicht per se verhältnismäßig. Können alle Mitarbeiter auf eine CRM-Applikation zugreifen und Kundenlisten ausdrucken, ist fraglich, ob ein DLP-Tool alleine das Risiko eines Datenverlustes genug reduziert, um die Überwachung zu rechtfertigen. Haben weltweit nur fünf Personen Zugriff auf eine solche Kundenliste, ist der Fall anders zu beurteilen.

E-Mails und Dateien, die überwacht werden, müssen *diskriminierungsfrei und sachgerecht* ausgewählt werden. Soziale Vorurteile dürfen keinen Einfluss haben.[2] Eine Risikoanalyse muss entscheiden, welche Teams, Unternehmensteile und -standorte oder Management-Ebenen das DLP-Tool (nicht) überwacht.

Weiter sind *absolute Schranken der Überwachung* (*impermissible surveillance*) eine zentrale Forderung. Sie verhindern, dass die Überwachung schleichend ausgeweitet wird und inakzeptable Formen annimmt („function creep") [Mac11]. Absolute Schranken sind partielle Verbote von Überwachung. Ein solches kann beispielsweise für Daten der Personalabteilung gelten oder für Instant Messaging innerhalb des Unternehmens. Absolute Schranken vermeiden ethische Probleme, Rechtsverstöße und Spannungen zwischen Unternehmen und Mitarbeitern. Möchte das DLP-Team eine absolute Schranke aufweichen, muss die Befugnis (Abschnitt 5.2) angepasst werden.

5.5 Organisation

Setzen Unternehmen DLP-Tools ein, überwachen Mitarbeiter andere Mitarbeiter. Sie lesen private E-Mails und weisen Mitarbeiter auf Fehler hin. Bei Bedarf leiten sie disziplinarische Maßnahmen ein. Dafür brauchen sie psychologisches Geschick. Überwachung soll Risiken verkleinern, nicht die Firmenkultur zerstören. Macnish diskutiert dafür das Konzept der Distanz.

Distanz hat zwei gegensätzliche Pole. Einerseits sollen Mitarbeiter mit Überwachungsaufgaben keine einseitige, negative Sicht auf die anderen Mitarbeiter entwickeln. Die Gefahr ist besonders bei automatisierten Überwachungsmaßnahmen ohne Kontakt zwischen Überwachern und Überwachten groß. Andererseits hilft Distanz den Überwachten. Für sie bedeutet es weniger Stress, wenn sie nicht persönlich mit ihrem Fehlverhalten konfrontiert werden. Eine E-Mail mit Bitte um Antwort ist für sie angenehmer [Mac11]. Folglich sollte ein DLP-Team örtlich und organisatorisch von anderen Mitarbeitern getrennt sein.

Mit *situativem Verständnis* vermeidet ein DLP-Team eine zu negative Sicht auf andere Mitarbeiter. Situatives Verständnis verlangt, dass das DLP-Team versteht, wie die übrigen Mitarbeiter in ihrer täglichen Arbeit mit sensiblen Daten umgehen. Unternehmen erreichen dies durch die richtige Auswahl von Mitarbeitern. Nicht technische IT-Security-Spezialisten sind für ein DLP-Team gefragt, sondern Mitarbeiter mit Verständnis für betriebliche Abläufe, Risikomanagement und für sensible Daten. Gerade in größeren Unternehmen kann die Organisation eine Herausforderung sein. Die Unternehmen müssen entscheiden, ob sie ein zentrales DLP-Team für das ganze Unternehmen wollen oder kleinere Teams pro Standort, Land oder pro Geschäftseinheit.

Aus der Diskussion lassen sich folgende Fragen für ethisch verantwortungsvolle Unternehmen ableiten:

- Warum soll ein DLP-Tool E-Mails, Dateien und Netzwerkverkehr überwachen? Ist das Motiv lauter? (Abschnitt 5.1)
- Wer mandatiert den Einsatz des DLP-Tools? Dateneigentümer und Linienvorgesetze müssen explizit oder implizit zustimmen. (Abschnitt 5.2)
- Ist die Überwachung mittels DLP-Tool risikominimierend oder gibt es Alternativen, die weniger in die Privatsphäre von Mitarbeitern eingreifen? (Abschnitt 5.3)
- Ist der Einsatz verhältnismäßig? Sind die Überwachungsziele diskriminierungsfrei gewählt? Sind absoluten Grenzen definiert? (Abschnitt 5.4)
- Ist die Organisation des Einsatzes von DLP-Tools derart, dass das DLP-Team situatives Einfühlungsvermögen für die Überwachten hat und gleichzeitig eine räumliche und organisatorische Trennung besteht? (Abschnitt 5.5)

6 Fazit

Verlieren Unternehmen sensible Daten, kann das ihre Existenz gefährden. DLP-Tools reduzieren solche Risiken. Dafür greifen sie in die Privatsphäre von MitarbeiterInnen ein. Das wirft die Frage nach der ethischen Zulässigkeit auf. Dieser Artikel bietet Unternehmen eine Liste von Fragen für eine Selbstbeurteilung. Mit ihrer Hilfe können sie existierende Lösungen evaluieren oder neue Lösungen ethisch akzeptabel konzipieren.

Die Überwachung von Mitarbeitern ist allerdings auch ein gesellschaftlich relevantes Thema. Entscheidungen zur Mitarbeiterüberwachung in Unternehmen dürfen nicht nur vom ethischen Gewissen einzelner Manager abhängen. Es geht um fundamentale Überwachungsverbote (absolute Schranken), die kein Unternehmen überschreiten darf. Weiter geht es um Verantwortlichkeit. Wer im Unternehmen muss garantieren, dass ein DLP-Tool nicht missbraucht wird? Die normativen Grundlagen gesellschaftlichen Zusammenlebens sind hier weiterzuentwickeln. Ansonsten behält Dieter Hildebrandt vielleicht doch Recht mit seinem Satz: „Politik ist nur der Spielraum, den die Wirtschaft ihr lässt."

Referenzen

[GW] Springer Gabler Verlag (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Ethik, http://wirtschaftslexikon.gabler.de/Archiv/2794/ethik-v9.html

[Hal14] Haller, K.: When Data Is a Risk: Data Loss Prevention Tools and Their Role within IT Departments, login (Usenix), Vol. 39, No. 1, February 2014

[Int03] Introna, L. D.: Workplace surveillance 'is' unethical and unfair. Surveillance & Society, 1(2), 210-216, 2002

[Lan06] Lango, J.: Last resort and Coercive Threats: Relating a Just War Principle to a Military Practice, Joint Services Conference on Professional Ethics, 2006

[Mac11] Macnish, K.: Surveillance Ethics, Internet Encyclopedia of Philosophy, http://www.iep.utm.edu, last update of the article: August 9, 2011

[Mtu11] Michigan Technological University, Information Technology Services and Security: Information Security Roles & Responsibilities, July 2nd, 2011, http://security.mtu.edu/policies-procedures/ISRolesResponsibilities.pdf , last retrieved July 26th, 2014

[MW00] Miller, S, Weckert, J.: Privacy, the Workplace and the Internet. Journal of Business Ethics, 28. Jg., Nr. 3, S. 255-265, 2000

[NA99] Norris, C., Armstrong, G.: CCTV and the social structuring of surveillance. Crime prevention studies, 10. Jg., Nr. 157-178, S. 1, 1999

[Tox14] Toxen, B.: The NSA and Snowden: Securing the All-Seeing Eye. Communications of the ACM, Vol. 57, No. 5, May 2014

Anmerkungen

1 *Mit eigenen Smartphones oder Tablets kann man sich nahezu überall per Mobilfunknetz mit dem Internet verbinden. Möchte man in Arbeitspausen private E-Mails oder soziale Netzwerke nutzen, gibt es keinen Grund, die Unternehmens-IT zu nutzen. In diesem Bereich können Mitarbeiter proaktiv ihre Privatsphäre schützen.*

2 *Macnish verwendet die Kriterien „feasibility standard" und „awfulness standard". Sie gehen auf Lango zurück, der sie im Zusammenhang mit „gerechtfertigten Kriegen" entwickelt hat [Lan06].*

3 *Macnish verweist auf die Gefahr, dass Vorurteile zu einer verstärkten Überwachung einer sozialen Gruppe führen können. Selbst wenn die Gruppe nicht krimineller ist als jede andere, hat man überproportional viele Vorkommnisse aus dieser Gruppe aufgrund der höheren Überwachungsdichte. Dadurch wird das – falsche – Vorurteil vermeintlich bestätigt. Er verweist auf eine Studie von Norris und Armstrong zur Videoüberwachung [NA99].*

Klaus Haller

Klaus Haller arbeitet im Consulting in den Bereichen IT-Risiko, Information-Security und Testorganisationen. Er verfügt über praktische Erfahrung in der Konzeption, Implementierung und Betrieb von Data-Loss-Prevention-Lösungen. Alle Äußerungen im Artikel geben seine Meinung als Privatperson wieder. Mehr zu ihm auf seiner Homepage *http://www.klaushaller.net.*