



Bild: Getty Images

DATENKLAU Kundgebung für den mutmasslichen Verräter Bradley Manning. Er soll Wikileaks geheime Militärdokumente gegeben haben.

# Datensicherheit ist kaum zu garantieren

Gefahr für Unternehmensdaten droht nicht zuletzt von den eigenen Mitarbeitenden. Die Gratwanderung zwischen Freiheit und Sicherheit. **KILIAN ZANTOP**

Über Datenverlust oder Datendiebstahl wird heute in der Öffentlichkeit gesprochen: Credit Suisse, HSBC in Genf, LGT und LLB in Liechtenstein, comparis.ch, Bank Julius Bär und viele mehr. Vor einigen Monaten hat der 22-jährige Bradley Manning in den USA über 250 000 Datensätze gestohlen, der Wikileaks-Plattform zur Verfügung gestellt und damit den wahrscheinlich grössten Datendiebstahl in der amerikanischen Geschichte geschafft. Die Liste nimmt kein Ende und der härter werdende Konkurrenzkampf der Unternehmen steigert das Interesse an relevanten Daten des Mitbewerbers.

Die Gefahren für das oft wertvollste Gut einer Unternehmung wie Patente, Rezepturen, Baupläne, finanzielle Informationen, Übernahmeinformationen oder auch Kundendaten sind vielfältig. Es drohen Gefahren von ausserhalb wie innerhalb des Unternehmens, durch Sicherheitslücken in Systemen sowie beispielsweise von USB Ports, über die innerhalb weniger Sekunden tausende von Datensätzen auf einen Stick kopiert und aus dem Unternehmen getragen werden können.

Eine der möglichen Gefahrenquelle sind auch die eigenen Mitarbeiter: Finanzielle Schwierigkeiten, familiäre Probleme oder Krankheit sind Situationen, in denen die Hemmschwelle schnell sinkt und man offener wird gegenüber illegalen Aktivitäten wie mit geheimen Informationen einen Zusatzgroschen zu verdienen.

**Sensibilität hochhalten** | Doch wie wird die Datensicherheit im Unternehmen erhöht? Sogar Melani, die Melde- und Analysestelle Informationssicherung, hält sich gemäss eigenen Aussagen mit Warnungen über Sicherheitslücken zurück, da diese aufgrund der grossen Menge die Sensibilität ab stumpfen würden. Die Erfahrungen zeigen, dass nur wenige Benutzer Empfehlungen, um Sicherheitslücken zu beheben, umsetzen. Grund dafür seien die Komplexität oder die Einschränkungen, die damit einhergehen.

Datensicherheit respektive IT-Sicherheit generell ist mit Einschränkungen verbunden. Es müssen klare Regeln definiert und diese unter Androhung von Konsequenzen bei der Nichteinhaltung

## DER AUTOR

*Kilian Zantop ist Chief Technical Officer bei der Barclay Technologies (Schweiz) AG.  
kilian.zantop@barclaytechnologies.ch*

**Je komplexer  
Regelwerke sind,  
desto schneller  
schleichen  
sich Fehler ein  
und es entstehen  
Sicherheits-  
lücken.**

untermauert werden. Ein bekanntes Beispiel dazu ist die Einführung des Tragens eines Sicherheitsgurts in Fahrzeugen, das auch erst mit Bussen durchgesetzt wurde. Doch wer möchte seinen Mitarbeitern noch mehr Regeln auferlegen und Einschränkungen in den Arbeitsprozessen einführen?

**Schwierig umzusetzen** | Damit wächst der Bedarf nach Sicherheitslösungen, die nach wie vor viele Freiheiten für die Mitarbeiter oder Mitarbeitergruppen zulassen, keine zu straffen Regeln mit sich bringen und trotzdem sicher sind. Sie müssen sich individuell den Arbeitsprozessen anpassen und möglichst einfach zu bedienen sein sowie auch den meist geringen Budgets der IT-Abteilungen entsprechen.

Systeme, die den Arbeitsprozessen individuell angepasst werden, sind immer aufwendig und kostspielig. Ein bekanntes Beispiel ist die Einführung von SAP, die für ein Unternehmen einen hohen Bedarf an Zeit, Aufwand und Kosten bedeutet.

Auch im Bereich Datensicherheit gibt es solche Systeme: Data Loss Prevention Lösungen – kurz DLP genannt. Damit lassen sich fast alle gewünschten Prozesse individuell auf den Benutzer und seine Bedürfnisse anpassen.

Die Problematik der Implementierung solcher Systeme beginnt jedoch bereits vor der eigentlichen Installation: Es müssen sämtliche Daten, die meistens verteilt auf verschiedenen Systemen in verschiedenen Lokationen gespeichert sind, inventarisiert werden. Der ursprüngliche Ersteller einer jeden Datei muss ermittelt werden und bestimmen, wie kritisch der Inhalt der Datei ist. Nur mit Hilfe dieser Information lassen sich die Daten in entsprechende Gefahrenklassen einstufen, die für das Regelwerk einer DLP-Lösung benötigt werden.

Das bedeutet für viele Unternehmen ein kaum umsetzbarer Aufwand. Die Daten wurden meist über Jahre gesammelt und sind nicht bereinigt. Weil Speicherplatz heute fast nichts mehr kostet, ist es einfacher, ein paar Gigabytes wenn nicht gar Terabytes anzuschaffen als den Datensalat in Ordnung zu bringen.

Die zweite grosse Aufgabe ist die Ermittlung des Datenflusses: Welcher Anwender nutzt welche Daten über welche Wege? Nur wenn der Daten-

fluss klar definiert ist, können dem Benutzer die Profile zugeordnet werden, die ihm die Flexibilität in seinen Arbeitsprozessen auch nach der Implementierung einer DLP-Lösung ausreichend gewährleisten. Wie flexibel diese Profile sein dürfen, muss vorab in entsprechenden Unternehmensrichtlinien betreffend der Benutzung von Daten definiert werden.

In diesen Richtlinien muss aus Sicht des Unternehmens pro Daten-Gefahrenklasse festgelegt sein, welche Gefahrenklasse wie gehandhabt wird und bei welchen Gefahrenklassen für welche Mitarbeiter Ausnahmen erstellt werden dürfen. Beispiel: Daten der Gefahrenklasse 5 dürfen nur verschlüsselt per E-Mail versendet werden, da es sich um sehr kritische Informationen handelt. Eine Ausnahme stellen die Offerten dar, die ausschliesslich von den Verkaufsmitarbeitern unverschlüsselt versendet werden dürfen.

Nun sind einerseits die vorhandenen Daten inventarisiert und in Gefahrenklassen eingeteilt. Der Datenfluss ist bekannt und die Richtlinien desselbigen definiert. Somit können die Richtlinien mit den individuellen Wünschen der Mitarbeiter nach Flexibilität in Einklang gebracht werden. Anschliessend werden alle Informationen im Regelwerk einer DLP-Lösung abgebildet. Dieser Aufwand ist notwendig, damit individuelle Profile pro Benutzer oder Benutzergruppen abgebildet werden und der Mitarbeiter in seinen gewohnten Arbeitsprozessen nicht zu sehr eingeschränkt wird.

**Verwaltungsaufwand ist enorm hoch** | Nach der Implementierung einer DLP-Lösung beginnt die Arbeit erst. Jede neu erstellte Datei muss wiederum der entsprechenden Gefahrenklasse zugeordnet werden, damit das richtige Profil beim entsprechenden Benutzer greift. Man denke in diesem Zusammenhang an eine Pressemitteilung, die vor der Veröffentlichung streng geheim ist und nach der Veröffentlichung sozusagen für jeden Mitarbeiter zugänglich sein muss. Damit wird klar, dass der Administrationsaufwand einer solchen Lösung enorm hoch ist.

Zudem muss jeder Mitarbeiter entsprechend geschult werden. Die besten Regeln nützen nichts, wenn die Mitarbeitenden sie nicht kennen oder sie nicht korrekt umsetzen. Eine einmalige Schulung ist selten ausreichend, es ist vielmehr ein

kontinuierlicher Prozess, um das Bewusstsein aufrechtzuerhalten.

Lösungen sind immer nur so gut, wie sie implementiert und unterhalten werden. Zudem ist strittig, ob die heute vorhandenen Lösungen alle Bedürfnisse abdecken. Kritiker behaupten, dass die verfügbaren Technologien in einer Anfangsphase stecken und Schwierigkeiten haben, die feinen Anomalien zu entdecken, die von ausgeklügelten Spionage-Netzwerken angewendet werden. Das würde bedeuten, dass die Daten trotz der grossen Anstrengungen doch nicht vollständig abgesichert sind.

**Fehler sind Sicherheitslücken** | Solch komplizierte Regelwerke stellen zudem in sich selbst Gefahren dar: Je komplexer und unübersichtlicher, desto schneller schleichen sich Fehler ein und damit wiederum Sicherheitslücken für sensible Daten. Ausserdem können Datenabflüsse von berechtigten Benutzern auch nicht abgefangen werden. Hat nämlich ein Benutzer das Recht, Offerten unverschlüsselt per Mail zu versenden, ist er nach wie vor in der Lage, diese Informationen auch an einen

Mail-Empfänger zu versenden, für dessen Augen der Inhalt nicht bestimmt war.

Will man den Mitarbeiter in seinen gewohnten Arbeitsprozessen nicht einschränken, muss man diesen Aufwand auf sich nehmen – ob es sich lohnt oder nicht. Alternativ kann man grundsätzlich auf Datenschutzlösungen verzichten und das damit verbundene Risiko auf sich nehmen oder Lösungen wählen, welche die gewohnten Arbeitsprozesse einschränken.

Grundsätzlich auf eine Datenschutzlösung zu verzichten, kann schwerwiegende Folgen haben. Gelangen sensible Informationen beispielsweise zum Mitbewerber, bedeutet dies im schlimmsten Fall den Untergang eines Unternehmens. Die Frage ist somit, ob es wirklich notwendig ist, den Mitarbeitern so viele Freiheiten zuzugestehen. Denn auch die schlauesten Lösungen bieten keinen Schutz, wenn sie Ausnahmen zulassen. Ausnahmen bedeuten automatisch Hintertürchen, die einen verbotenen Weg unbeaufsichtigt lassen. Und wenn ein Mitarbeiter in einer Notsituation den Zusatzverdienst braucht, kann dieses Hintertürchen genutzt werden. <



## Tausende von Schweizer Finanzabteilungen zählen auf uns

Bruno Kuchler ist einer von mehr als zweihundert Mitarbeiterinnen und Mitarbeitern, die hinter Sage stehen. Dem Schweizer Softwareunternehmen, das sich auf die Entwicklung von betriebswirtschaftlichen Gesamtlösungen spezialisiert hat. Wir bieten jedem Schweizer KMU die passenden Softwareprogramme für eine professionelle Geschäftsadministration. Mehrere tausend Finanzverantwortliche in der ganzen Schweiz vertrauen dabei auf unsere Lösungen für ein modernes Finanzwesen.

KMU Business-Software.  
Damit Ideen Erfolg haben.  
[www.sageschweiz.ch](http://www.sageschweiz.ch)

