

Link: <https://www.computerwoche.de/a/datenverlust-kann-existenzen-bedrohen,1904382>

Interview mit Heiko Brenn, Group Technologies

## "Datenverlust kann Existenzen bedrohen"

Datum: 01.09.2009  
Autor(en): Thomas Pelkmann

**Datenklau im Unternehmen durch unzufriedene Mitarbeiter kann großen Schaden anrichten. Wir sprachen mit Heiko Brenn, Senior Consultant beim E-Mail Experten Group Technologies, wie man sich vor solchen Diebstählen wirksam schützen kann.**



Heiko Brenn, Group Technologies: "Datenklau kann Existenzen vernichten."

Computerwoche: Wie groß schätzen Sie die Gefahr ein, unternehmenskritische Daten durch Diebstahl zu verlieren?

**Heiko Brenn:** Insbesondere im Bereich der E-Mail-Kommunikation ist diese Gefahr sehr groß. Viele Unternehmen sichern oft nur den eingehenden E-Mail-Verkehr durch Viren- und Spamschutz.

Der Schutz der ausgehenden **E-Mail-Kommunikation**<sup>1</sup> wurde in der Vergangenheit dagegen meist nicht ausreichend berücksichtigt. Dabei passiert es - gerade aufgrund der Tatsache, dass die E-Mail als Medium für Geschäftsprozesse in das Zentrum der Unternehmenskommunikation gerückt ist - ohne umfassende Schutzmaßnahmen sehr leicht, dass bewusst oder unbewusst unternehmenskritische Daten verloren gehen.

Computerwoche: Wie hoch schätzen Sie die finanziellen Folgen solcher Datenverluste ein?

**Brenn:** Einer **Studie des Ponemon-Institutes**<sup>2</sup> zufolge bewegen sich die Kosten bei einem Datenverlust im Schnitt zwischen 267.000 und 6,75 Millionen Euro. Das ist aus meiner Sicht aber höchstens ein grober Richtwert. Denn bei der Beurteilung der Auswirkungen von Datenverlusten spielen viele unterschiedliche Faktoren eine Rolle. Für ein mittelständisches Unternehmen etwa kann der Verlust von patentrelevanten Konstruktionsinformationen Existenz bedrohende Auswirkungen haben. Der Verlust von Kundendaten dagegen kann vor allem rechtliche und Image schädigende Konsequenzen nach sich ziehen, die nur im Einzelfall zu bewerten sind.

Computerwoche: Was ist schlimmer: der Datenverlust oder der Imageschaden, wenn der Verlust von Daten bekannt würde?

**Brenn:** Grundsätzlich kann beides sehr negative Folgen für die betroffenen Unternehmen haben. Die Beurteilung hängt sowohl von der Art des Datenverlustes als auch von der jeweiligen Marktposition des Unternehmens und der Branche ab.

Bei Unternehmen, die in der breiten Öffentlichkeit stehen, Kreditinstitute oder Telekommunikationsanbieter beispielsweise, wird der Imageschaden sehr viel erheblicher sein als bei den "stillen Stars" des deutschen Mittelstandes.

Computerwoche: Wodurch und über welche Wege sind Unternehmensdaten vor allem bedroht?

**Brenn:** Zunächst einmal muss man sagen, dass sämtliche Daten, egal ob in elektronischer oder papiergebundener Form, Verlustgefahren ausgesetzt sind. Bei elektronischen Daten beginnt das beim Export von Daten aus Datenbanksystemen, betrifft das Speichern auf mobilen Datenträgern, wie **USB-Sticks**<sup>3</sup>, und reicht bis zum Versenden sensibler Daten per E-Mail.

## "Es kommt auf die Sorgfalt der Mitarbeiter an"

Computerwoche: Mit welcher Strategie schützen sich Unternehmen vor versehentlichem Datenverlust oder vor dem **Ausspähen von Daten**<sup>4</sup> schützen?

**Brenn:** An erster Stelle steht meiner Einschätzung nach die Sorgfalt der Mitarbeiter. Es ist wichtig, dass die ein Bewusstsein für die Relevanz von Daten und deren elektronischen Transport entwickeln. Gut ausgebildete und engagierte Mitarbeiter werden im eigenen Interesse sorgsam und vorsichtig mit wichtigen Daten umgehen.

Die Einstufung von Informationen in "unbedenklich", "sensibel", "kritisch", "geheim" ist dafür ein wichtiger erster Schritt. Darauf aufbauend, definiert man dann den Umgang und die Schutzmaßnahmen für diese Daten. Solche Guidelines sollten fester Bestandteil der allgemeinen Unternehmensrichtlinien sein. Selbstverständlich sind darüber hinaus technische Werkzeuge notwendig, um im Falle eines bewussten oder unbewussten Fehlverhaltens wichtige Informationen schützen zu können.

Computerwoche: Was sollten Unternehmen zuerst machen, die sich dem Thema Datensicherheit nähern möchten?

**Brenn:** Wichtig ist: Das Unternehmen muss wissen, welche sensiblen Informationen in der internen und welche in der externen Kommunikation mit Kunden und Partnern gesendet und empfangen werden. Häufig genug ist dieses Wissen nicht vorhanden. Mit Hilfe eines **Assessments**<sup>5</sup> ist es möglich, einen Überblick über Menge und Inhalt der Kommunikation zu erhalten. Darauf aufbauend lassen sich dann organisatorische, technische und rechtliche Maßnahmen zur Verbeugung von Datenverlusten ableiten.

Computerwoche: Wie müssen sich die Mitarbeiter verhalten, um nicht aus Versehen zum Opfer zu werden?

**Brenn:** Es ist entscheidend, dass Mitarbeiter die Wichtigkeit einer Information für das Unternehmen und damit auch für den eigenen Arbeitsplatz richtig bewerten können. Ein oft unterschätzter Aspekt ist dabei das so genannte Social Engineering, wo es aufgrund persönlicher Vertrauensverhältnisse zu einem Datenverlust kommen kann. Wird ein vorher sensibilisierter Mitarbeiter von Dritten um die Herausgabe vertraulicher Informationen gebeten, weiß er, dass im Zweifelsfall eine Rückfrage bei Vorgesetzten oder beim Sicherheitsbeauftragten die richtige Konsequenz ist.

## "Die IT kann bei der Datensicherheit helfen"

Computerwoche: Wie kann die IT bei der Prävention helfen?

**Brenn:** IT-Lösungen zum Schutz von Daten bieten eine Fülle von Möglichkeiten. Nehmen wir den Bereich der E-Mail-Kommunikation: Hier sind Lösungen am Markt, die grundsätzlich verhindern, dass E-Mails an unerwünschte externe Empfänger - zum Beispiel an Mitbewerber - gesendet werden.

Andere Lösungen sorgen dafür, dass E-Mails nach sensiblen Dateianhängen beziehungsweise textlichen Inhalten in allen erdenklichen Dokumententypen untersucht werden und entscheiden dann über ein Regelwerk, wie mit der entsprechenden E-Mail verfahren werden soll.

Außerdem kann konkret festgelegt werden, welcher Mitarbeiter bestimmte Dokumententypen wie Konstruktionszeichnungen per E-Mail versenden darf.

Abhängig von der Antwort auf solche Fragen können dann Dateianhänge automatisiert entfernt, komplette E-Mails vor Versand gelöscht oder in Quarantäne gestellt werden.

Auch das Vier-Augen-Prinzip ist mit Hilfe von IT-Lösungen heute bereits realisierbar. Dabei erhält eine berechnete Stelle eine E-Mail mit solchen Inhalten zur Prüfung und kann dann nach Einsichtnahme die entsprechende E-Mail freigeben oder zurückweisen.

Befindet sich eine E-Mail nun berechtigterweise auf dem Weg ins Internet, so ist natürlich die Verschlüsselung der mit ihr übermittelten Daten von entscheidender Bedeutung. Dabei ist neben den klassischen Methoden mit **PGP**<sup>6</sup> und **S/MIME**<sup>7</sup> auch an die Empfänger zu denken, die nicht Willens oder in der Lage sind diese Methoden zu unterstützen. Hier kann dann eine Lösung wie unsere **iQ.Suite**<sup>8</sup> WebCrypt zum Einsatz kommen, die eine verschlüsselte E-Mail-Kommunikation ohne aktive Unterstützung der Empfänger umsetzt.

Computerwoche: Vielen Dank für das Gespräch.

## Links im Artikel:

<sup>1</sup> <https://www.computerwoche.de/software/crm/1901592/>

<sup>2</sup> [http://www.pcwelt.de/start/sicherheit/sonstiges/news/194345/datenverluste\\_kosten\\_24\\_millionen\\_euro\\_pro\\_vorfall/](http://www.pcwelt.de/start/sicherheit/sonstiges/news/194345/datenverluste_kosten_24_millionen_euro_pro_vorfall/)

<sup>3</sup> <http://de.wikipedia.org/wiki/USB-Massenspeicher>

<sup>4</sup> <https://www.computerwoche.de/security/1903766/>

<sup>5</sup> <https://www.computerwoche.de/management/it-strategie/1903108/>

<sup>6</sup> [http://de.wikipedia.org/wiki/Pretty\\_Good\\_Privacy](http://de.wikipedia.org/wiki/Pretty_Good_Privacy)

<sup>7</sup> <http://de.wikipedia.org/wiki/S/MIME>

<sup>8</sup> <http://www.group-technologies.com/de/produkte/overview.php>

---

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.