

IT-Sicherheitstipp: Bei Datenverlust richtig vorbereitet sein

Der Notfall Datenverlust tritt weitaus häufiger ein, als allgemein vermutet. Laut einer Studie des internationalen Softwarekonzerns *INFOWATCH* konnte im ersten Halbjahr 2010 weltweit ein Verlust von insgesamt 539 Millionen persönlichen Datensätzen festgestellt werden. Deutsche Unternehmen hatten in dieser Zeitspanne rund fünf Millionen Zwischenfälle gemeldet, die einen Datenverlust zur Folge hatten. Trotz dieser erschreckenden Zahlen besitzen nur wenige Unternehmen konkrete Regelungen, wie im Falle eines Datenverlusts größerer Schaden abgewendet werden kann. Bislang gibt es kaum Versicherungen, die bei betrieblichen Datenverlusten für den Schaden aufkommen, sofern sie nicht durch Brände oder Einbruchdiebstähle verursacht wurden. Daher ist es Aufgabe jedes Unternehmers, im Kontext der betrieblichen IT-Sicherheit auch für einen angemessenen Schutz vor Datenverlust zu sorgen. Laut einer aktuellen Studie des Bundesministeriums für Wirtschaft und Technologie in Zusammenarbeit mit dem Netzwerk Elektronischer Geschäftsverkehr (kurz: NEG) haben 21 Prozent der befragten Unternehmen schon einmal wesentliche Daten endgültig verloren [1]. In diesem IT-Sicherheitstipp werden Ihnen konkrete Handlungsempfehlungen gegeben, sodass Sie sich und Ihre Beschäftigten auf ein mögliches Notfallszenario Datenverlust richtig vorbereiten können.



► Sensibilisieren Sie Ihre Beschäftigten für das Thema IT-Sicherheit

Knapp die Hälfte aller von *INFOWATCH* registrierten Datenverluste geschahen unbeabsichtigt durch allzu lockeren Umgang mit vertraulichen Daten. Neben einem Basisschutz durch Sicherheitssoftware für die betriebliche IT-Umgebung ist es für Unternehmer ebenso wichtig, ein gemeinsames Sicherheitsbewusstsein innerhalb der Belegschaft herzustellen. Der IT-Sicherheitstipp „Mitarbeiter für das Thema IT-Sicherheit sensibilisieren“ [2] kann Ihnen eine Hilfe sein, Informationssicherheit fest in Ihre Unternehmenskultur zu integrieren.

Falls noch nicht geschehen, sollten Sie in Zusammenarbeit mit den Beschäftigten unterschiedliche Vertraulichkeitsstufen für alle relevanten Unternehmens- und Personaldaten festlegen. Diese dienen als Orientierungshilfe und sind mit konkreten Regeln zur Handhabung ver-

bunden. So sollten Daten mit bestimmtem Grad der Vertraulichkeit nur über festgelegte Kanäle, beispielsweise nur via Briefpost, kommuniziert werden dürfen. **Auch ist es ratsam, Zugriffsrechte und Speicherorte in eine Daten-Kategorisierung mit einzuschließen.** Statten Sie bewusst nur solche Rechner im Netzwerkverbund mit Administratorrechten aus, bei denen entsprechende Rechte für die tägliche Arbeit erforderlich sind. Welche Informationen generell als vertraulich anzusehen sind und wie Sie eine oben genannte Einteilung in Ihrem Unternehmen praktisch umsetzen können, erfahren Sie in dem IT-Sicherheitstipp „*Richtiger Umgang mit vertraulichen Daten*“ [2]. Beachten Sie auch die Praxistipps „*IT-Sicherheit - Faktor Mensch*“ [1].

► **Setzen Sie Produkte zum Schutz vor unerwünschtem Datenverlust ein**

Technische Unterstützung zur Organisation und Protokollierung des betrieblichen Datenverkehrs bieten so genannte „*Data-Loss-Prevention*“-Produkte, zu deutsch etwa „Produkte zum Schutz vor unerwünschtem Datenverlust“. **Diese können hilfreich bei der Festlegung der Vertraulichkeitsstufen sein und dadurch Zugriffsrechte steuern.** Falls gewünscht, kann durch eine Protokollfunktion festgehalten werden, welche Daten innerhalb des Betriebsnetzwerkes durch welchen Beschäftigten verändert, verschoben, gelöscht oder kopiert werden. Eine Vielzahl von Programmen bieten unterschiedlichen Funktionsumfang. Vor dem Kauf sollten Sie sich daher überlegen, welche Funktionalitäten Sie genau benötigen.

► **Benennen Sie einen IT-Sicherheitsbeauftragten**

Das *Bundesamt für Sicherheit in der Informationstechnik* (kurz: *BSI*) empfiehlt, dass jedes Unternehmen, welches E-Business nutzt, einen IT-Sicherheitsbeauftragten für die Informationssicherheit benennt. Im Notfall kann dieser dann in einem Krisen-Meeting zurate gezogen werden, um das weitere Vorgehen zu koordinieren. Hier kann er Aufgaben verteilen und eine beratende Funktion einnehmen. **Betriebliche Abläufe nach System-Abstürzen und Datenverlusten sollten in einem Notfallplan im Vorfeld dokumentiert sein.** Der ernannte Sicherheitsbeauftragte ist zuständig für die Umsetzung der Maßnahmen. Beispielsweise kann er anweisen, dass alle Internetverbindungen des Unternehmens gekappt und die Polizei kontaktiert wird, wenn der Verdacht auf Wirtschaftsspionage besteht (siehe hierzu: IT-Sicherheitstipp „*Notfallplan: Was tun, wenn es passiert ist?*“ [2]). Weitere Informationen zum IT-Sicherheitsbeauftragten erfahren Sie auch auf den Webseiten des *BSI* [3].

► **Betreiben Sie regelmäßig Datensicherungen gegen Datenverlust**

Datenverlust kann bedeuten, dass Informationen entweder unbeabsichtigt gelöscht werden, aufgrund von physikalischen Ursachen, wie technischen Defekten, verloren gehen, oder gezielten Angriffen Krimineller zum Opfer fallen, was Datendiebstahl bzw. -löschung bedeuten kann. Ne-

ben leichtfertigem Umgang mit Informationen in der internen und externen Unternehmenskommunikation (siehe hierzu: *NEG-Awareness-Video „Wie schütze ich mich vor Phishing und Social Engineering“* [2]), ist oft die unsachgemäße Datenspeicherung ein Risikoherd für unumkehrbare Verluste. **Datensicherungen sollten daher regelmäßig von dem IT-Verantwortlichen durchgeführt und überprüft werden.**

Speichern Sie unbedingt auch vor jedem Druckauftrag Ihre Daten nochmals ab. Nicht selten kommt es zu Systemabstürzen bei der Datenübertragung von PC zu Netzwerkdruckern.

Müssen zentrale Daten wie Dienstpläne häufig von vielen verschiedenen Personen geändert und jeweilige Änderungen nachvollzogen werden können, ist der Einsatz einer Versionsverwaltung ratsam. Diese erlaubt die automatische Versionierung und damit das Festhalten von Änderungen an Dokumenten. Jede Version einer Datei wird neben einem Zeitstempel mit einer Benutzerkennung in einem Archiv gespeichert und kann bei Bedarf schnell wiederhergestellt werden. Weitere Informationen zur Datensicherung erhalten Sie in der *Informationsbroschüre für Einsteiger „IT-Sicherheit: Themenfokus Datensicherung“* [1].

► Wählen Sie einen geeigneten Speicherort Ihrer Daten

Erhöhen Sie Ihren Schutz vor Datenverlust durch die Wahl des richtigen Speicherorts Ihrer Daten. Sofern möglich, speichern Sie Ihre Daten stets auf einem File-Server und nicht lokal auf Ihrer Festplatte ab, da bei File-Servern meistens eine automatische und regelmäßige Datensicherung eingerichtet ist und Sie bei Verlust auf diese zurückgreifen können. Die Datensicherungen des File-Servers sollten vom IT-Verantwortlichen regelmäßig auf Unversehrtheit überprüft werden. **Regelmäßige Datensicherungen sollten sich physikalisch nicht am selben Ort wie die Originaldaten befinden.** Andernfalls laufen Sie Gefahr, dass sowohl Ihre Originaldaten als auch Kopien bei einem Diebstahl oder Brand vernichtet werden. Neben der Speicherung auf zugriffsbeschränkten Ordnern innerhalb des Intranets, ist auch das Auslagern der Dateien in geschützte Online-Speicher, sogenannte Clouds, denkbar. **Beachten Sie stets, wer dann auf Ihre Daten zugreifen kann und entscheiden Sie sich gegen eine Auslagerung, sofern es sich um sensible Daten handelt.** Die Wahl des richtigen Anbieters und eine angemessene Dateiverschlüsselung tragen entscheidend zur Datensicherheit Ihrer ausgelagerten Informationen bei. Tipps hierzu finden Sie im IT-Sicherheitstipp *„Cloud-Dienste sicher nutzen“* [2].

► Grundvoraussetzung: Angemessener Basisschutz

Um das Unternehmensnetzwerk vor internen und externen Bedrohungen effektiv zu schützen, ist ein angemessener Basisschutz essentiell: Ein Virenschutzprogramm, das Schadsoftware aufspürt, blockiert und beseitigt; und eine Personal Firewall, die wie ein Türsteher den Netzwerkverkehr zwischen jedem Computer und dem Internet regelt. **Halten Sie diese sicherheitsrelevanten**

Programme und jede weitere installierte Software mit Sicherheitsupdates immer auf dem neuesten Stand, um neu entdeckte Sicherheitslücken sofort zu schließen und Datendieben weniger Angriffsfläche zu bieten. Schützen Sie alle Benutzerkonten und sensible Daten mit sicheren Passwörtern, die Sie regelmäßig ändern. Hinweise und Tipps zum angemessenen Basisschutz für Ihren PC erhalten Sie im IT-Sicherheitstipp „Basisschutz für Ihren PC“ [2].

Autoren

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen

[1] <http://www.kmu-sicherheit.de>

<http://www.ec-net.de>

[2] <http://ratgeber.it-sicherheit.de>

[3] <http://www.bsi.bund.de>

<https://www.internet-sicherheit.de>

<http://www.bsi-fuer-buerger.de>

<http://www.bitkom.de>

Bildquelle: © Rainer Grothues - Fotolia.com

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: <http://www.kmu-sicherheit.de>

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: <http://www.internet-sicherheit.de>