

Ansprechpartner: Stephan Gelhausen
Leiter Informationszentrum der deutschen Versicherer

Postfach 08 04 31, 10004 Berlin
Tel.: 030-20 20-55 70, Fax: 030-20 20-65 70

E-Mail: s.gelhausen@ihre-versicherer.de
www.ihre-versicherer.de



Gefahr aus dem Netz: Versicherungsschutz für Unternehmen

Berlin/Regensburg, 30. August 2011. Gegenüber dem Vorjahr ist die Computerkriminalität in Bayern, auch Cybercrime genannt, um vier Prozent auf 8.510 Fälle angestiegen. Laut Daten des Bayerischen Landeskriminalamts hat insbesondere der Straftatbestand „Ausspähen/ Abfangen von Daten“ zugenommen (+ 24,8 Prozent). Der Freistaat liegt damit im Bundestrend. Auch die Polizeiliche Kriminalstatistik des Bundes verzeichnet 2010 mit mehr als 84.000 Fällen von Cybercrime einen neuen Rekordwert. Werden Unternehmen Opfer von Hackerangriffen, kann das weitreichende Folgen haben, wie erst kürzlich prominente Beispiele zeigten. Unbekannte veröffentlichten im Internet die Kundendaten großer Firmen, die neben E-Mail-Adressen und den zugehörigen Passwörtern auch Kreditkartendaten enthielten. Doch selbst kleine und mittelständische Unternehmen sind vor Online-Attacken nicht sicher. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zeigt, wie sich Unternehmen und Organisationen schützen können.

Das eigene Unternehmen richtig versichern

Ob E-Mail-Kommunikation, Unternehmenswebsite oder Online-Shop, ohne elektronische Datenübertragung und -speicherung kommt im digitalen Zeitalter kaum ein Unternehmen aus. Doch bei allen Möglichkeiten, die die globale Vernetzung bietet, birgt sie auch Gefahren. Laut Bundesministerium für Wirtschaft und Technologie kann Datendiebstahl ein mittelständisches Unternehmen im Einzelfall bis zu einer Million Euro kosten. Imageschäden und Vertrauensverlust bei Kunden können sogar die Existenz gefährden. Das Ministerium hat anlässlich der steigenden Gefahr aus dem Netz im März die Task Force „IT-Sicherheit in der Wirtschaft“ eingerichtet, in deren Fokus der Mittelstand steht.

Trotz guter Virenprogramme lassen sich Datendiebstähle oder gezielte Hacker-Angriffe nicht immer verhindern. Wenn darüber hinaus Dritte durch Selbst- oder Fremdverschulden betroffen

sind, kann das weitreichende Folgen haben. Fallen dadurch Kundendaten in die Hände Unbefugter oder werden Betriebsabläufe lahmgelegt, zahlt sich die richtige Versicherung, die für die Folgekosten aufkommt, schnell aus. „Unternehmer können ihr Online-Risiko reduzieren, indem sie ihre Betriebshaftpflicht um eine Zusatzversicherung für die Nutzer von Internet-Technologien erweitern. Diese schließt alle Schäden ein, die aus dem Austausch, der Übermittlung und der Bereitstellung elektronischer Daten im Internet, per E-Mail oder über Datenträger resultieren,“ sagt Stephan Gelhausen vom GDV.

Datenmanipulation mit Folgen

Weltweit kamen im vergangenen Jahr mehr als zwei Millionen neue Schadprogrammvarianten auf. „Dies birgt für Unternehmen zunehmend Probleme“, stellt Gelhausen fest. Von außen auf den Rechner geschleuste Computer-Viren oder Schadprogramme können Daten von Kunden löschen, unterdrücken, verändern oder unbrauchbar machen. Wenn es Hackern zum Beispiel gelingt, auf die Daten eines Steuerberatungsbüros zuzugreifen, Steuerelemente zu verändern oder Dateien komplett zu löschen, bedeutet es für die Mitarbeiter einen erhöhten Zeitaufwand, die Daten wiederherzustellen. Im schlimmsten Fall bemerken sie die Manipulation gar nicht und geben falsche Informationen an das Finanzamt weiter. Für den daraus resultierenden Schaden kommt die Zusatzversicherung auf.

Virenangriffe, die fehlerhafte Speicherung oder inkompatible Daten können auch dazu führen, dass eine Software nicht richtig installiert wird oder falsch läuft. Geht in der Folge eine technische Anlage kaputt oder verletzt sich gar ein Mitarbeiter, greift die Versicherung ebenfalls.

Server lahm gelegt, was nun?

Wenn Viren den elektronischen Datenaustausch behindern und den Zugang Dritter stören, bedeutet dies eine starke Einschränkung des Betriebsablaufs eines Unternehmens. DoS-Attacken (Denial of Service-Attacken) sind eine weitere, bei Hackern beliebte Methode, um Firmen Schaden zuzufügen. Dabei werden simultan Anfragen verschickt, um den Server zu überlasten, zu verlangsamen und schließlich arbeitsunfähig zu machen. Der Internetauftritt ist dann für Anfragen von Kunden oder Online-Bestellungen nicht mehr verfügbar. Je nachdem, wie lange die Behebung des Problems dauert, können die Umsatzverluste erheblich sein. Wer seine Betriebshaftpflicht um die entsprechende Zusatzversicherung ergänzt hat, kann auch daraus resultierende Schäden melden.

Persönlichkeits- und Namensrechte

Das Risiko, das Persönlichkeitsrecht eines anderen zu verletzen, wird durch das Internet wesentlich erhöht. Gibt ein Unternehmer aufgrund eines Systemfehlers von ihm gesammelte Kundeninformationen weiter, kann ein Unbefugter diese zum Beispiel für Werbezwecke nutzen.

Die betroffenen Personen können dann Ansprüche wegen Persönlichkeitsverletzungen geltend machen. Namens- oder Persönlichkeitsrechte Dritter können aber auch durch die Einrichtung eines Internetauftritts verletzt werden, etwa wenn ein Unternehmer unwissentlich eine Domain einrichtet, auf die andere Rechte erheben. Auch für diese sogenannten immateriellen Schäden kommt die Versicherung auf.

Damit der Schaden gar nicht erst entsteht

Gegen viele der Gefahren aus dem Internet können sich Betriebe weitestgehend schützen. Der Gesamtverband der Deutschen Versicherungswirtschaft empfiehlt die folgenden Regeln zu berücksichtigen, damit der Versicherungsschutz im Schadensfall tatsächlich greift.

1. Antiviren-Software und Firewall bieten Schutz vor Viren, Trojanern, Datendiebstählen und gezielten Angriffen. Regelmäßige Updates gewährleisten, dass der Computer auch gegen neue Schädlinge abgesichert ist.
2. Sicherheitsbackups auf einer externen Festplatte, auf CD bzw. DVD zahlen sich aus, wenn durch Angriffe von außen oder durch einen Systemfehler Daten gelöscht werden.
3. Passwörter sollten einmal monatlich geändert werden. Empfehlenswert ist eine mindestens zehnstellige Kombination aus Sonderzeichen und Zahlen.
4. Bei E-Mails mit fremdem Absender gilt es lieber zwei Mal hinzusehen. Phishing- und Scareware-Botschaften wirken durch ihre Aufmachung mit Logos oft seriös, entlarven sich jedoch durch Rechtschreibfehler und Freemail-Adressen. Phishing bezeichnet das Erbeuten von Nutzerdaten zum Missbrauch und Weiterverkauf, Scareware-Botschaften verunsichern den Nutzer und bringen ihn so dazu schädliche Software zu installieren oder teure Programme zu erwerben.
5. Ein allgemeines Sicherheitskonzept im Unternehmen ergänzt die technischen Vorkehrungen. Teil einer solchen „Security Policy“ sind zum Beispiel Regelungen zur Mitarbeiterschulung oder zum Umgang mit Warnhinweisen.

Für weitere Versicherungsinformationen wenden Sie sich bitte an:

Stephan Gelhausen

Gesamtverband der Deutschen Versicherungswirtschaft e.V.

Wilhelmstraße 43 / 43G

10117 Berlin

Tel.: 030 - 2020-5113

E-Mail: s.gelhausen@gdv.de

Über „Ihre deutschen Versicherer on Tour“:

Mit „Ihre deutschen Versicherer on Tour“ setzen die Mitgliedsunternehmen des Gesamtverbands der Deutschen Versicherungswirtschaft e.V. (GDV) ihre 2010 gestartete Imagekampagne fort. Im Rahmen einer Informationstour mit einem alten englischen Doppeldeckerbus durch ganz Deutschland sprechen Versicherungsexperten Woche für Woche mit Bürgern vor Ort über deren individuelle Bedürfnisse und informieren rund um Versicherungen. Dabei zeigen die Menschen in bundesweiten TV-Spots und regionalen Printanzeigen, was ihnen besonders wichtig und schützenswert ist und werden so zu den Darstellern der Kampagne. Die Werbefilme, alle Fakten zur Tour und Impressionen von den einzelnen Stationen sowie Informationen zu Versicherungsthemen finden Interessierte im Internet unter www.ihre-versicherer.de. Wer nicht zum Bus kommen kann, erreicht die Experten unter der gebührenfreien Telefonhotline 0800 - 33 99 399 oder unter info@klipp-und-klar.de.