## Datenverschlüsselung nach Überwachungsskandalen in aller Munde

Datenverschlüsselung nach Überwachungsskandalen in aller Munde<br /><br />Internet Security-Experte: Verschlüsselung ist nicht gleich Verschlüsselung<br />Spätestens seit den Enthüllungen von Whistleblower Edward Snowden über angezapfte Glasfaserkabel und gigantische Spähprogramme des amerikanischen und britischen Geheimdienstes stellt sich Unternehmen wie privaten Nutzern eine brennende Frage: Wie sicher kann Surfen im Internet eigentlich sein? Immer wieder ist nun von Verschlüsselung die Rede. Diverse Begrifflichkeiten machen die Runde, mit denen viele Internet-Nutzer nur wenig anfangen können. <br />'Um das Ausspionieren versendeter Daten zu verhindern, gibt es grundsätzlich zwei verschiedene kryptographische Verfahren', klärt Christian Heutger, Geschäftsführer beim Internet Security-Spezialisten PSW GROUP ( www.psw.net ), daher auf. Unterschieden wird dabei zwischen symmetrischer und asymmetrischer Verschlüsselung. Bei Ersterer werden die Daten mithilfe eines geheimen Schlüssels ver- beziehungsweise entschlüsselt. Der Schlüssel muss dabei dem Sender und Empfänger bekannt sein und dazu vorher persönlich ausgetauscht werden. <br />Ein Vorteil des symmetrischen Verfahrens: Die relativ geringe Rechenleistung, die es benötigt. Der gravierende Nachteil: Es stellt keine große Herausforderung dar, eine entsprechend gesicherte Nachricht zu entschlüsseln, wenn der Private-Key von Dritten entdeckt oder abgehört wird. 'Genau deshalb ist es ratsam auf die sogenannte Public-Key-Infrastruktur (PKI) und damit auf die asymmetrische Verschlüsselung zu setzen', betont der Experte. <br />Die asymmetrische Verschlüsselung basiert auf der Verwendung eines zusammengehörenden Schlüsselpaares, wobei ein Schlüssel jeweils zur Ver- und einer zur Entschlüsselung genutzt wird. Beim Public-Key-Verfahren wird nun einer der Schlüssel veröffentlicht und kann von jedem Sender dazu genutzt werden, eine Nachricht an den Empfänger zu verschlüsseln. Nur der Empfänger, der im Besitz des zweiten Schlüssels (Private-Key) ist, kann die Nachricht lesen.<br />'Die asymmetrische Verschlüsselung kann auch zur digitalen Authentifizierung von Einzelpersonen und Firmen genutzt werden. Dazu gibt eine Zertifizierungsstelle - eine so genannte Certificate Authority (CA) - digitale Zertifikate heraus und beglaubigt diese. Ein solches Zertifikat integriert den Public-Key oder Informationen über diesen', erläutert Christian Heutger ein weiteres Anwendungsbeispiel dieser Form der Verschlüsselung, die auch bei SSL zum Einsatz kommt.<br />Mit Perfect Forward Secrecy (PFS) steht mittlerweile zudem eine zukunftssichere Verschlüsselung bereit, die über die bisherigen Verfahren hinausgeht. PFS - eine SSL-Funktion - verhindert, dass bereits abgeschlossene aber verschlüsselt aufgezeichnete Kommunikation durch nachträgliches Bekanntwerden des geheimen Schlüssels kompromittiert wird. 'Mit Perfect Forward Secrecy lassen sich Spionage-Angriffe wirksamer denn je vereiteln', so der Sicherheitsexperte.<br />Weitere Informationen unter www.psw.net <br />Honorarfreie Pressebilder zum Download:<br /> www.pressedesk.de/shared/images/psw/crew-heutger1.jpg (Christian Heutger)<br /> www.pressedesk.de/shared/images/psw/logo-allgemein1.jpg <br /> http://www.pressedesk.de/shared/images/psw/sicherheit1 <br /> http://www.pressedesk.de/shared/images/psw/sicherheit2 <br /> http://www.pressedesk.de/shared/images/psw/sicherheit3 <br />Über die PSW GROUP<br />Die PSW GROUP mit Sitz in Fulda ist einer der deutschlandweit führenden Full Service-Provider für Internetlösungen mit einem besonderen Schwerpunkt auf Internet Security. Als solcher bietet das Unternehmen - sowohl für den Web-Einsatz als auch für die E-Mail-Kommunikation - Zertifikats-, Signatur-, Verschlüsselungs- und Authentifizierungslösungen an. Das umfassende Produktportfolio reicht speziell in diesem Bereich von SSL-Zertifikaten über Code-Signing-Zertifikate bis hin zu qualifizierten elektronische Signaturen.<br />Aber auch Sicherheitslösungen wie das PCI-Scanning, Secure CDN und DNSSEC sowie Gütesiegel und Kundenbewertungssysteme speziell für E-Commerce-Anbieter finden sich im Repertoire der PSW GROUP. Neben der großen Produkt-Vielfalt verfügt das im Jahr 2000 gegründete Unternehmen über eine fast 11-jährige Expertise in den Bereichen Internet-Sicherheit, IT-Recht sowie Hosting- und Domaindienstleistungen.<br />Zu den Kunden der PSW GROUP zählen Webhoster sowie Webdesign- und Marketing-Agenturen, die als Reseller auf die Sicherheitslösungen des Full Service-Providers zurückgreifen, aber auch Betreiber von E-Commerce-Angeboten sowie Online-Shops.<br /><br />PSW GROUP GmbH <br> Co. KG<br />Flemingstraße 20-22<br />D-36041 Fulda<br />PresseDesk<br />Tel.: 030 / 530 47 73 - 0<br />E-Mail: psw-group@pressedesk.de<br /><img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=541603" width="1" height="1">

### Pressekontakt

PSW GROUP GmbH & Co. KG

36041 Fulda

psw-group@pressedesk.de

### Firmenkontakt

PSW GROUP GmbH & Co. KG

36041 Fulda

psw-group@pressedesk.de

Die PSW GROUP ist Ihr Full-Service-Provider für Internetlösungen mit einem besonderen Schwerpunkt auf Internet Security. Als Dienstleister bieten wir Ihnen sowohl für den Webeinsatz als auch für die E-Mail-Kommunikation maßgeschneiderte Zertifikats-, Signatur-, Verschlüsselungs- und Authentifizierungslösungen an. Unser voll umfassendes Produktportfolio reicht dabei von SSL-Zertifikaten über Code Signing-Zertifikate bis hin zu S/MIME-Zertifikaten und De-Mail.Als Partner aller namhaften Zertifizierungsstellen haben wir für jeden Anwendungsfall stets die passende Lösung. Auch Lösungen für PCI- und Malware-Scan, Secure CDN, DNSSEC sowie für Secure E-Mail, E-Mail-Security und E-Mail-Archivierung befinden sich in unserem Portfolio. Unsere Internetdienstleistungen komplettieren wir durch PDFlib-, Parallels-, Live-Config- und CloudLinux-Lizenzen zur Automatisierung und Virtualisierung Ihrer Geschäftsprozesse.Neben der großen Produktvielfalt verfügen wir über langjährige Expertise in den Bereichen Internetsicherheit und IT-Recht. Mit unserem tiefgreifenden und zertifizierten Fachwissen als Parallels Certified Automation and Virtualization Engineers, Symantec Sales Expert Plus, Sophos Certified Architects, IRCA ISO 27001 ISMS Lead-, Datenschutz- und IT-Security-Auditoren stehen wir Ihnen auch bei den komplexesten Fragestellungen beratend zur Seite.