PSW GROUP

„PUBLIC KEY“ ODER „PRIVATE KEY“

PRESSEMITTEILUNG

„PUBLIC KEY“ ODER „PRIVATE KEY“: UNTERSCHIEDE DER VERFAHREN ZUR DATEN-VERSCHLÜSSELUNG

Fulda, 29.02.2012 – Der Verschlüsselung von Daten bei der Kommunikation über das Internet kommt eine wachsende Bedeutung zu. Nicht nur Unternehmen, auch private Nutzer entwickeln ein Bewusstsein für das Schadenspotential von sensiblen, persönlichen Daten, die in die falschen Hände gelangen. Weniger bekannt ist jedoch, dass prinzipiell zwei unterschiedliche Verfahren – nämlich das Symmetrische und Asymmetrische – zur Datenverschlüsselung existieren. Der wesentliche Unterschied zwischen beiden: Bei der symmetrischen Verschlüsselung wird zum Ver- und Entschlüsseln ein und derselbe Schlüssel verwendet. Das macht das Verfahren vergleichsweise schnell, aber auch angreifbar. Denn es setzt voraus, dass der Schlüssel geheim gehalten wird (private key), was besonders bei dessen Übermittlung gefährlich werden kann.

Die asymmetrischen Verfahren gelten als sicherer, da zwei Schlüssel zum Einsatz kommen, die nicht auseinander ableitbar sind: Ein öffentlicher Schlüssel (public key) für die Verschlüsselung und ein privater Schlüssel für die Entschlüsselung. Der private Schlüssel bleibt stets beim Empfänger, etwa auf dem Server eines Online-Shops oder eines Website-Betreibers. Public Key-Verschlüsselungsverfahren erfordern ein funktionierendes Schlüsselmanagement, das die Generierung, Speicherung, Verteilung und Anwendung kryptographischer Schlüssel umfasst. Der Preis für die hohe Sicherheit des Verfahrens ist ein verlangsamter Arbeitsprozess.

Daher wurde dazu übergegangen, die Vorteile beider Verfahren im Rahmen einer hybriden Verschlüsselung zu kombinieren: Bei dieser erfolgt die Datenverschlüsselung per symmetrischen Verfahren. Für jede Datenübertragung wird ein eigener Schlüssel generiert, der per asymmetrische Verschlüsselung dann mit dem Datenpaket sicher an den Kommunikationspartner übermittelt wird. Die Geschwindigkeit des symmetrischen Verfahrens wurde so schließlich mit der Sicherheit des asymmetrischen vereint.

Mit der hybriden Verschlüsselung ist bereits jeder Internet-Nutzer in Berührung gekommen. Es kommt via SSL jedes Mal dann zum Einsatz, wenn zum Beispiel beim Besuch

einer Banken-Website oder eines Online-Shops ein Schloss-Symbol in der Adressleiste des Browsers erscheint. Klickt der Nutzer auf das Schloss werden ihm meistens noch weitere Informationen zur Stärke der Verschlüsselung angezeigt. Während 256 bit heute Standard bei der Verschlüsselungsstärke sind, weist die Schlüsselstärke in der Regel 2048 bit auf. Von rechtlicher Seite wichtig zu wissen: Für den Schutz von Nutzer-Daten ist der Betreiber der Website beziehungsweise des Online-Shops verantwortlich.

ÜBER DIE PSW GROUP

Die PSW GROUP mit Sitz in Fulda ist einer der deutschlandweit führenden Full Service-Provider für Internetlösungen mit einem besonderen Schwerpunkt auf Internet Security.

Neben Gütesiegeln und Kundenbewertungssystemen bietet die PSW GROUP sowohl für den Web-Einsatz als auch für die E-Mail-Kommunikation Verschlüsselungs-, Authentifizierungs-, Zertifikats- und Signaturlösungen an.

Das umfassende Produktportfolio reicht speziell in diesem Bereich von SSL- und Code-Signing-Zertifikaten über qualifizierte elektronische Signaturen bis hin zur Breitstellung von ganzen Zertifikatsinfrastrukturen. Aber auch das PCI-Scanning sowie Secure CDN finden sich im Repertoire der PSW GROUP.

Die PSW GROUP stellt ihren Kunden zudem professionelle Websites und Online-Shops zur Verfügung. Dabei können Kunden bei Bedarf auch auf außergewöhnliche Corporate Designs, maßgeschneiderte Marketingkonzepte und durchdachte Webapplikationen zurückgreifen, die von der zum Unternehmensverbund gehörenden Agentur PSW MEDIA entwickelt und umgesetzt werden.

Neben der großen Produkt-Vielfalt verfügt der Full Service- Provider über eine zehnjährige Expertise in den Bereichen Hosting- und Domaindienstleistungen, im Umfeld von IT-Sicherheit und IT-Recht.