

Sicherheit im virtuellen Versicherungsbüro



Andrea Klenk, Leiterin Security Solutions bei der media transfer GmbH, Darmstadt

Vermittler-Extranets und Online-Zugänge für Kunden gehören heute selbstverständlich zum Leistungsspektrum moderner Versicherungsinfrastrukturen. Die Kommunikation erfolgt dabei unschlagbar preiswert und flexibel über das Internet, und längst nicht mehr via Standleitungen oder Wählverbindungen wie früher einmal üblich. Das gleiche gilt für die Anbindung von Heimarbeitsplätzen und Außendienstmitarbeitern an das Firmennetz. Ohne zusätzliche Vorkehrungen werden aber bekanntermaßen alle gesendeten Daten im Internet im Klartext übermittelt. Will man einen bildlichen Vergleich mit traditionellen Übermittlungswegen machen, entspräche das einem Versenden vertraulicher Versicherungsunterlagen in Form von Postkarten, nicht per Einschreiben im verschlossenem Briefumschlag.

Das Sicherstellen der Vertraulichkeit und Unverfälschtheit der ausgetauschten Daten ebenso wie die zuverlässige gegenseitige Identifizierung der Kommunikationspartner ist also unumgängliche Pflicht bei der Realisierung von Online-Angeboten.

Nicht weniger wichtig ist der Schutz des internen Firmennetzwerks vor unerwünschten Eindringlingen, die Daten kopieren, löschen oder manipulieren könnten. Ebenso muss ein Blockieren oder Lahmlegen der angebotenen Online-Dienstleistung durch externe Angreifer verhindert werden.

Studien zum Thema E-Commerce kommen regelmäßig zu dem Schluss, dass bei Finanzdienstleistern und Versicherern für die IT-Sicherheit nach wie vor zu wenig getan wird. Mögliche Ursachen für die in den Studien festgestellten Defizite könnten fehlendes Bewusstsein für die Sicherheitsproblematik, mangelndes Know-how in den IT-Abteilungen oder auch Furcht vor immensen Investitionen sein. Dabei lässt sich ein angemessenes Sicherheitsniveau zu durchaus überschaubaren Kosten erzielen, wie im folgenden dargestellt wird.

Absicherung des Unternehmensnetzwerks

Der erste Schritt ist die wirksame Abschottung des internen Firmennetzes und die Bildung eines abgegrenzten Extranets. Auf das Extranet darf von außen in kontrollierter Weise entsprechend den angebotenen Online-Dienstleistungen zugegriffen werden. Die dafür erforderliche Hardware und Software (kaskadierte Mail- und

DNS Server, Firewall, Client-/Server basierter Virenschutz, NAT Router, Proxy Server) kann für weniger als 20.000 Euro beschafft werden. Der Implementierungsaufwand durch versierte Fachkräfte schlägt mit etwa zehn Personentagen zu Buche.

Vertrauliche Kommunikation

Online-Dienstleistungen sind in der Regel Web-Applikationen. Um ein „Mithören“ der ausgetauschten und in der Regel vertraulichen Daten zu verhindern, ist die Verschlüsselung der Kommunikation zwischen Webserver des Versicherers und Browser des Maklers oder Kunden also zwingend erforderlich. Alle heute gängigen Webserver- und Browserprodukte unterstützen das hierfür entwickelte Protokoll SSL (bzw. seinen Nachfolger TLS). Seit vor wenigen Jahren die Exportbeschränkungen für amerikanische Produkte aufgehoben wurden, existieren auf Seiten der Browser keine gesetzlichen Beschränkungen hinsichtlich der dabei einsetzbaren Verschlüsselungsalgorithmen und Schlüssellängen mehr. Sofern einigermaßen aktuelle Browserversionen eingesetzt werden, ist eine symmetrische Verschlüsselung per triple DES Algorithmus mit 168 bit Schlüssellänge möglich. Als Voraussetzung für die Anwendung von SSL bzw. TLS braucht der Webserver ein sog. SSL Serverzertifikat. Das Zertifikat bestätigt einerseits, dass es sich bei der vom Makler bzw. Kunden gewählten Internetadresse tatsächlich um die der Versicherung handelt, zum anderen ist es Basis für die Verschlüsselung der Kommunikation mit dem Browser.

Es kann bei einer Zertifizierungsstelle, beispielsweise dem Trust Center der Deutschen Telekom (www.telesec.de), beantragt werden und kostet ca. 150 Euro pro Jahr.

Zuverlässige Authentifizierung der Kommunikationspartner

Noch gravierender als die zuverlässige Authentifizierung des Versicherers gegenüber den Benutzern ist umgekehrt die zweifelsfreie Identifikation der Benutzer, da ihnen Zugang zu sensiblen Informationen gewährt wird. Hierzu gibt es eine Reihe technischer Möglichkeiten, die sich hinsichtlich Sicherheitsniveau, Kosten und möglichem Mehrwert deutlich unterscheiden.

Login/Passwort Methode

Technologisch überholt, da mit diversen Nachteilen behaftet, ist die Zugangssicherung durch Login und Passwort. Passworte sind häufig vom Benutzer selbst definiert und entsprechend von unzureichender Güte, was Länge und Zeichensatz betrifft (von der Verwendung von Geburtsdaten, Namen von Verwandten etc. einmal ganz zu schweigen). Durch Einsatz von Passwort-Knackern, die systematisch Zeichenmengen probieren, lassen sich Passworte in kurzer Zeit knacken. Solche Attacken kann man natürlich mit der Sperrung des Zugangs nach einer Anzahl von Fehlversuchen abwehren, legt damit aber auch den Zugang für berechtigte Benutzer lahm.

Einmalpassworte

Schon sehr viel besser erscheint daher der Einsatz von Einmalpassworten. Der Makler oder Kunde erhält dazu ein kryptographisches Token (ein Stück Hardware), das das nächste gültige Passwort errechnet und anzeigt. Nach Eingabe dieses Passworts auf der Webseite erfragt der Webserver des Versicherers die Gültigkeit bei einem speziellen Server, der im Firmennetz oder extern betrieben wird. Ein Passwort ist jeweils nur einmal verwendbar, daher erreichen Angreifer mit den Passwort-Knackern nichts. Für eine solche Lösung müssen die Token angeschafft werden, wobei es einerseits batteriebetriebene Token gibt, die auf Knopfdruck arbeiten und nicht durch eine PIN zugriffsgeschützt sind, und andererseits Kartenleser und Chipkarte, die mit einer Zugangs-PIN arbeiten. Die Token sind ein wenig preiswerter als eine Chipkartenlösung, sollten aber aus

Sicherheitsgründen nicht verwendet werden. Schafft man einen hochwertigen Reader plus Chipkarte für Makler und Kunden an, sind dafür ca. 80 Euro pro Benutzer zu kalkulieren (bei großen Stückzahlen kann über Preisnachlässe verhandelt werden). Darüber hinaus muss der zentrale Passwortserver gekauft und betrieben oder die entsprechende Dienstleistung eines externen Anbieters eingekauft werden. Hier wird oft pro Prüfung abgerechnet. Eine solch kostenintensive Lösung kommt sicher nur dann in Frage, wenn man einen Mehrwert über den Zugangsschutz per Passwort hinaus (z.B. VPN, Zugriff auf Mail Accounts, remote Access, single logon etc.) erzielen könnte. Dieser ist im geschilderten Szenario des Extranets für Makler und Kunden jedoch nicht gegeben. Darüber hinaus sind – im Gegensatz zu der im folgenden vorgestellten Zertifikats-Technologie – die kryptographischen Verfahren nicht offengelegt und daher wie bei allen proprietären Verfahren Skepsis angebracht.

Elektronische Zertifikate

Das modernste und vielseitigste Verfahren, das den aktuellen Stand der Technik repräsentiert, ist der Einsatz von Zertifikaten. Ein Zertifikat entspricht einem elektronischen Maklerausweis oder einer elektronischen Kundenkarte. Mit Hilfe des Zertifikats ist eine zweifelsfreie und nicht durch Dritte manipulierbare Identifizierung des Maklers oder Kunden gegenüber dem Webserver des Versicherers möglich. Das technische Verfahren ist international standardisiert, die Algorithmen sind daher offengelegt und durch Jahrzehnte lange breit angelegte Forschung abgesichert.

Alle modernen Anwendungen, die mit Verschlüsselung und elektronischer Signatur arbeiten, sind zertifikatsbasiert (eMail, VPN, Browser/Server Kommunikation, Dateiverschlüsselung, etc.).

Der offenkundige Mehrwert der Zertifikate liegt darin, dass damit auch die eMail-Kommunikation zwischen Versicherern, Maklern, Kunden und ganz allgemein auch mit allen anderen Kommunikationspartnern abgesichert werden kann.

An dieser Stelle entbrennt nun erfahrungsgemäß die Diskussion darum, ob man mit Softwarezertifikaten oder mit Zertifikaten auf Chipkarte arbeiten soll. Die Entscheidung darüber ist durch die beiden leider gegenläufigen Faktoren Sicherheitsniveau versus Kosten getrieben.

Softwarezertifikate kommen, wenn sie nur zum Zugriff auf einen einzigen Versicherungsserver dienen sollen, als echte Low-Cost Lösung daher. Wie beispielsweise im Vermittler-Extranet der Haftpflichtkasse Darmstadt durch die media transfer GmbH realisiert, können Zertifikate automatisiert erzeugt und verteilt werden. Der Realisierungsaufwand alleine dafür ist relativ gering. Wenn die Zertifikate exklusiv bei einem Versicherer genutzt werden, sind aufwändige Sperrmechanismen im Fall des Zertifikatsverlustes oder Ende der Vertragsbeziehungen nicht notwendig – Deaktivierung in der Datenbank genügt.

Für Makler oder Kunden entstehen keinerlei Kosten, einzige Voraussetzung ist ein Browser neuerer Version. Online-Zugänge für Kunden sind vermutlich nur in dieser Form finanzierbar. Auf der Benutzerseite treten neben diesem riesigen Vorteil dann aber auch die Nachteile der reinen Software-Lösung zutage. Sie ist weniger sicher als eine Chipkarten basierte, da der Benutzer durch entsprechende Konfiguration seines Browsers selbst dafür Sorge tragen muss, dass sein Zertifikat durch eine PIN vor jeder unberechtigten Verwendung geschützt ist. Eine Sensibilisierung der Anwender für Sicherheitsbelange ist also dringend erforderlich. Bei der Chipkarte ist die Eingabe einer PIN zwingend und kann vom Benutzer nicht umgangen werden. Überdies geschieht hier die Eingabe gesichert über einen PIN Pad.

Ebenso wäre es theoretisch möglich, durch ein Trojanisches Pferd die auf der Festplatte verschlüsselt gespeicherten Zertifikatsdaten zu stehlen. Der Einsatz von Chipkarten baut dem vor: Das Schlüsselmaterial verlässt die Karte niemals, kann also auch nicht von Angreifern ausgelesen und gestohlen werden. Selbst der rechtmäßige Inhaber kann sich aufgrund dieses starken Schutzes keine Sicherungskopie seiner Zertifikatsdaten anlegen. Wird das Zertifikat auch zur eMail-Verschlüsselung eingesetzt, kann dieser Umstand zum Pferdefuß werden, wenn die Karte verloren geht. Die Mails sind dann nicht mehr zu entschlüsseln.

Das Hauptargument gegen eine Chipkartenlösung sind jedoch in erster Linie die hohen Kosten sowie der nicht zu unterschätzende Aufwand für die Benutzer bei der Installation und Inbetriebnahme von Kartenlesern und zugehöriger Software. Unterstützung seitens des Diensteanbieters ist unumgänglich.

Die Erfahrung in vielen Projekten auch außerhalb des Versicherungsumfelds hat gezeigt, dass die Kosten-Nutzen-Abwägung häufig zum Einsatz von Softwarezertifikaten führt, deren Sicherheitsniveau als ausreichend eingeschätzt wird. Die Kosten für Hardware, Installation und Support bei einer Chipkartenlösung würden erst dann zu rechtfertigen sein, wenn zumindest Makler mit ein und demselben Zertifikat Zugriff auf die Extranets vieler Versicherer hätten. In diesem Fall wäre die zentrale Ausgabe der Zertifikate von einem unabhängigen Trust Center wie dem der Deutschen Telekom sinnvoll.

Kontakt:

Andrea Klenk
Leiterin Security Solutions
media transfer GmbH
Dolivostraße 11
64293 Darmstadt
Telefon: 06151 / 81 93-0
Telefax: 06151 / 81 93-43
Mail: contact@mtgnet.de