Arzt im Dienst

Ärztlicher Notfalldienst

Telefon +423 230 30 30

18 bis 22 Uhr
Dres. Kranz/Hohenegger
9495 Triesen

Ab 22 Uhr tel. Beratung durch Spital bzw. Dienstarzt in Pikett.

Liechtensteinische Ärztekammer

Glaube

Gottesdienst im Kloster St. Elisabeth

SCHAAN Zum Sonntagsgottesdienst am 6. Juni um 11 Uhr sind alle herzlich zur Mitfeier ins Kloster St. Elisabeth nach Schaan eingeladen. Aufgrund der begrenzten Platzzahl ist eine Anmeldung erforderlich (Telefon: +423 239 64 57, vormittags; E-Mail: brotundrosen@kloster.li). (eps)

Gratulation

Viel Glück im Ehestand

Auf dem Zivilstandsamt in Vaduz vermählten sich am Mittwoch:

Thomas **Farrèr** (von und in Mauren) und Elisabeth **Egender** (aus Dornbirn in Mauren).

Wir gratulieren recht herzlich zur Vermählung und wünschen dem Brautpaar alles Gute und viel Glück auf dem gemeinsamen Lebensweg.

(Text: red; Foto: Tatjana Schnalzer)

Den Daten auf der Spur

Wie funktioniert Verschlüsselung?

RUBEN RHEINBERGER
TECHNIKER, DATENSCHUTZSTELLE

Mit den heutigen Kommunikationskanälen, wie beispielsweise Messenger, Social-Media-Plattformen oder E-Mail Diensten, stellen sich immer mehr Personen die Frage, wie die Vertraulichkeit ihrer Kommunikation gewährleistet werden kann. Spätestens seit den Enthüllungen von Edward Snowden vor etwa acht Jahren ist es ein offenes Geheimnis, dass vor allem staatliche Akteure elektronische Inhalte, die über das Internet versendet werden, systematisch sichten, auswerten und bei Bedarf speichern. Zudem zeigen die fast täglichen Meldungen von Datenlecks bei verschiedensten Unternehmen sowie gezielte Angriffe gegen diese als auch gegen Privatpersonen die Notwendigkeit, digitale Kommunikation entsprechend vor neugierigen Blicken zu schützen. Eine Möglichkeit hierbei bietet der Einsatz von modernen Verschlüsselungsverfahren.

Doch wie funktioniert moderne Verschlüsselung? Welche Verschlüsselungsverfahren gibt es? Welche Aspekte gilt es bei der Nutzung zu beachten beziehungsweise welche Schutzziele werden verfolgt? Ohne zu sehr auf technische Details einzugehen, sollen in diesem Artikel die Grundlagen und Verfahren anhand von Beispielen erläutert werden.

Grundsätzlich wird unter Verschlüsselung die Umwandlung eines Klartextes in einen Geheimtext verstanden. Wie der Begriff Schlüssel im Wort Verschlüsselung verrät, kann dieser Vorgang mit Hilfe des passenden Schlüssels wieder rückgängig gemacht werden. In diesem Fall wird von Entschlüsselung gesprochen. Die ersten dokumentierten Verschlüsselungsverfahren reichen bis ins Altertum zurück. Die sogenannte Caesar-Verschlüsselung beispielsweise war ein einfaches symmetrisches Verfahren, um die militärische Korrespondenz geheim zu halten. Dabei wird jeder Buchstabe im Klartext durch eine Rechtsverschiebung im Alphabet geändert, sodass dadurch ein Geheimtext entsteht. Diese Verschiebung basiert auf einem definierten Wert, zum Beispiel drei. Dieser Wert entspricht somit dem Schlüssel, der bekannt sein muss, um den Text verschlüsseln bzw. entschlüsseln zu können. So wird beispielsweise aus den Buchstaben A der Buchstabe D und aus G wird J. Der Geheimtext AD entspricht in diesem Beispiel dem Klartext DJ. Mit dem vorhin definierten Wert drei (Schlüssel) kann der Prozess nun mittels Linksverschiebung umgekehrt werden. In diesem einfachen Beispiel werden Leer- und Sonderzeichen nicht berücksichtigt.

Es ist offensichtlich, dass dieses einfache Verschlüsselungsverfahren aus heutiger Sicht als nicht sicher angesehen wird. Unter anderem ist die Anzahl an möglichen Schlüsseln (Schlüsselraum) viel zu klein, sodass bereits durch einfaches Ausprobieren von 25 unterschiedlichen Möglichkeiten auf den Klartext Rückschlüsse gezogen werden können. Wie eingangs erwähnt, handelt es sich dabei um ein symmetrisches Verfahren, d. h. es wird zum Ver- und Entschlüsseln derselbe Schlüssel verwendet. Daneben existieren asymmetrische Verfahren. Asymmetrisch deshalb, da unterschiedliche Schlüssel für das Ver- und Entschlüsseln zum Einsatz kommen, sprich ein Schlüsselpaar aus öffentlichem und privatem Schlüssel. Aus diesem Grund wird auch vom Public-Key-Verschlüsselungsverfahren gesprochen.

Beim asymmetrischen Verfahren wird der öffentliche Schlüssel zum Verschlüsseln einer Nachricht verwendet. Nur noch der Besitzer des privaten Schlüssels kann daraufhin die Nachricht entschlüsseln. Dieses Prinzip zeigt zugleich den grossen Vorteil gegenüber dem symmetrischen Verfahren. Die Schlüsselverteilung muss nicht über einen sicheren Kommunikationskanal erfolgen, da der öffentliche Schlüssel, im Gegensatz zum privaten Schlüssel, nicht geheim gehalten werden muss. Beim symmetrischen Verfahren hingegen können unbefugte Dritte, die Kenntnis über den Schlüssel erhalten, jeden Geheimtext entschlüsseln, die mit diesem Schlüssel verschlüsselt worden sind. Ein Vorteil der symmetrischen Verschlüsselung ist die Geschwindigkeit bei der Ver- bzw. Entschlüsselung. Deshalb kommen symmetrische Verfahren oft bei der Verschlüsslung von Festplatten oder Speicherkarten zum Einsatz. Zudem ist in diesem Fall die Notwendigkeit in der Regel nicht gegeben, das Passwort mit mehreren Personen teilen zu müssen. Das Problem mit der sicheren Schlüsselverteilung entfällt somit.

Hybride Verfahren gängig

In der Praxis werden oft hybride Verfahren, das heisst eine Kombination der beiden Verfahren eingesetzt, um die Vorteile beider Verfahren nutzen zu können. Konkrete Anwendungsbeispiele sind unter anderem E-Mail Verschlüsselungen (PGP), Besuch von Internetseiten via https (SSL/TLS) oder auch diverse Messenger Dienste, die vermehrt eine durchgängige (Ende-zu-Ende) Verschlüsselung anbieten. Durchgängig bedeutet in diesem Fall, dass nur die Kommunikationspartner der jeweiligen Endpunkte die Nachricht lesen können. Für die Übertragung eingebundene Dritte, beispielsweise Telekommunikationsbetreiber, sind hingegen nicht in der Lage, die Nachricht zu lesen.

Doch wo liegen die Grenzen bzw. Gefahren beim Einsatz von Verschlüsselung? Neben der Herausforderung des Schlüsselmanagements sind in der Praxis oft veraltete Verschlüsselungs-Algorithmen oder zu kurze Schlüssellängen im Einsatz. Zum Zeitpunkt, als das Verfahren gewählt und die Schlüssel erstellt wurden, können sie durchaus sicher gewesen sein, doch mit der heutigen Rechenleistung können sie unter Umständen einfach gebrochen werden und bieten somit keinen ausreichenden Schutz mehr. Des Weiteren finden sich oft Unzulänglichkeiten bei der konkreten technischen Umsetzung von Verschlüsselungsverfahren. Ebenso muss klar sein, dass beim Empfang einer verschlüsselten Nachricht die Echtheit des Absenders (Authentizität) nicht automatisch gegeben ist. Um die Echtheit eines Kommunikationspartners zu überprüfen, kommen zusätzliche Massnahmen, wie beispielsweise digitale Signaturverfahren, zum Einsatz.

Fragen?

Im Rahmen dieser neuen Gastbeitragsreihe widmet sich die liechtensteinische Datenschutzstelle diversen Datenschutzthemen. **Brennt Ihnen eine Frage zum Datenschutz unter den Nägeln, dann schreiben Sie uns an redaktion@volksblatt.li.**

IMPRESSUM

Herausgeberin: Liechtensteiner Volksblatt AG, Im alten Riet 103, 9494 Schaan, Tel. +423 237 51 51, E-Mail verlag@volksblatt.li
Geschäftsleitung: Lucas Ebner
Chefredaktion: Lucas Ebner, Daniela Fritz, Hannes Matt
Redaktion: Sebastian Albrich, Daniel Banzer, Silvia Böhler, Holger Franke (Leitung Wirtschaft), Elmar Gangl (Leitung Kultur), Lucia Kind, Ursina Marti, David Sele, Michael Wanger; E-Mail redaktion@volksblatt.li; Robert Brüstle (Leitung Sport), Manuel Moser, Jan Stärker, Telefon +423 237 51 39; E-Mail sport@volksblatt.li
Leitung Online/Social Media: Sebastian Albrich
Redaktionskoordination: Susanne Falk, E-Mail sekretariat@volksblatt.li, Telefon +423 237 51 61
Fotografen: Michael Zanghellini (Leitung), Paul Trummer
Produktion/Layout: Klaus Tement (Leitung), Marco Boscardin, Franco Cardello
Finanzen/Personal: Michèle Ehlers
Marketing/Verkauf: Björn Bigger (Leitung), Nicole Ackermann, Cordula Riedi
Inseratenannahme/Empfang: Nihal Sahin, Telefon +423 237 51 51, Fax +423 237 51 66, E-Mail inserate@volksblatt.li
Abonnentendienst: Dominik Batliner, Telefon +423 237 51 27
Druck: Vorarlberger Medienhaus, Schwarzach

Bei Zustellschwierigkeiten wenden Sie sich unter der Telefonnummer +423 237 51 27 an unseren Abo-Dienst (Montag bis Freitag von 8 bis 10 Uhr).

Der Verlag übernimmt für die Inhalte der Anzeigen keine Verantwortung.

www.volksblatt.li

Leserfoto des Tages

Brunos Tierecke

Das heute veröffentlichte Foto stammt von Bruno Nigg aus Schaan, der in einem Viehstall auf einem Bauernhof den Auslöser betätigt hat. ‹‹Der Meisterpflästerer› baut sein Nest aus lehmartiger Erde, Stroh und Halmen, die mit Speichel zusammengeklebt werden. Die Gesellschaft des Viehs und des arbeitenden Bauern stören die Rauchschwalbe, die als klassischer Kulturfolger gilt und sehr nah am Menschen nistet, keineswegs – nicht einmal bei der Aufzucht der Jungen», schreibt Nigg. Vielen Dank für die Einsendung, weitere Fotos für diese Rubrik sind erwünscht und erreichen uns per E-Mail an redaktion@volksblatt.li.

(Text: red; Foto: Bruno Nigg)