msi Michael Schulte Investmentberatung

msi-NEWS

Ausgabe 12/2016

Schwerpunktthema: E-Mail-Sicherheit mit GPG

Datensicherheit und GPG

Die E-Mail ist als Kommunikationsmedium Standard. Auch ich selber und meine Kunden kommunizieren gerne via E-Mail - selbst sensible und vertrauliche Daten erhalte ich oftmals per E-Mail. Das kann bei der Flut an elektronischem Mail-Verkehr, der sekündlich durch das Netz rauscht, auch nicht weiter schlimm sein - sollte man meinen. Trotzdem muss man ich darüber im Klaren sein, dass eine E-Mail in der analogen Welt einem Medium entspricht, mit dem nie wichtige Daten versenden werden sollten: Der Postkarte.

Liebe Kunden von msi,

zum Abschluss eines volatile Jahres, das mit einer schönen Jahres-End-Rallye endet, möchte ich die Gedanken mal auf ein ganz anderes Thema lenken: Die Sicherheit von E-Mails. Dieses Jahr gab es viel Wirbel, als Hacker Tausende von Telekom-Routern platt machten. Der US-amerikanische Wahlkampf soll durch russische Hacker beeinflusst worden sein, und für ThyssenKrupp stand das gesamte Jahr 2016 unter dem Damoklesschwert eines langfristig angelegten systematischen Hacker-Angriffs, der über Monate mit einer speziell eingerichteten Eingreiftruppe vorerst abgewehrt werden konnte.
Das Thema Datensicherheit wird immer wichtiger, von daher sollte es eine Selbstverständlichkeit sein, auch seine eigene Kommunikation zu schützen. Besonders, wenn sensible Daten wie Kontonummern, Gesundheitsdaten oder Depotauszüge versendet werden .
Ich selber biete allen meinen Kunden eine verschlüsselte E-Mail-Kommunikation an, doch eine Verschlüsselung funktioniert nur auf gegenseitiger Basis: Wenn nur eine Seite verschlüsselt, kann niemand etwas lesen - nicht mal der Empfänger, für den die Mail ja eigentlich bestimmt ist. Von daher mein Appell: Lesen Sie diese Hinweise und installieren Sie GPG!
Mit herzlichen Grüßen und meinen besten Wünschen für die Feiertage und das neue Jahr

Das Wesen von E-Mails
Wer in einer großen Firma oder einem Konzern arbeitet, der weiß, wie ernst das Thema Datenschutz dort genommen wird. In aller Regel gibt es in Konzernen eine strikte Trennung von Privat- und Firmen-Sphäre - sowohl was die Hardware (Computer, Notebooks, Festplatten, USB-Sticks) als auch die Software (Programme, E-Mails, Web-Inhalte) angeht.
Man muss akzeptieren, dass die E-Mail als Kommunikations-Medium nicht mehr wegzudenken ist - Fax und Post sind Auslaufmodelle, zu umständlich und zu langsam. Doch muss man sich ebenso darüber im Klaren sein, dass eine E-Mail vom Sicherheitsstandard einer Postkarte entspricht: Jeder kann sie lesen! Allein der unendlichen Flut von Mails ist es zu verdanken, dass die E-Mail letztlich doch relativ sicher ist - auch ein Postbote käme nicht auf die Idee, Tausende von Weihnachtskarten zu lesen, um zufällig auf irgendeine verwertbare Information zu stoßen. Dazu kommt, dass die überwiegende Zahl von E-Mails ohnehin aus Werbung, Spam oder Belanglosigkeiten besteht.

Kritisch wird es allerdings dann, wenn Hacker den riesigen Datenozean nach einzelnen Information gezielt abfischen - Big Data und fast unbegrenzte Rechnerkapazitäten machen es möglich. So hört man immer wieder von „Identitätsdiebstählen“ - also der gezielten Datensammlung zu einer bestimmten Person mit dem Ziel, in deren Namen Kredite aufzunehmen oder Bestellungen aufzugeben. Berichte von Personen oder auch Firmen, die auf diese Weise von Kriminellen

betrogen worden, tauchen mit schöner Regelmäßigkeit im Fernsehen in den bekannten Wirtschafts- und Verbrauchermagazinen auf.

Wenn jeder wüsste, wie einfach es ist, seine E-Mails vor fremdem Zugriff zu schützen, würde dies wohl nicht so häufig vorkommen.

Die E-Mail als „Einschreiben“
Wie wäre es, wenn Sie zukünftig alle Ihre E-Mails wie ein Einschreiben versenden könnten? Ohne, dass Sie dafür extra zahlen müssten? Und - noch besser - ohne, dass Sie selber und der Empfänger es überhaupt merken?
Tatsächlich gibt es eine kostenlose Software, die - einmal installiert - im Hintergrund ihren Dienst tut und jede E-Mail zukünftig so gut verschlüsselt, dass es für Daten-Abfischer nahezu unmöglich wird, deren Inhalt zu rekonstruieren. Und da man es einer verschlüsselten E-Mail nicht ansieht, ob sie wichtige Inhalte oder eben nur die üblichen Urlaubsgrüße oder Belanglosigkeiten enthält, käme wohl kein Hacker auf die Idee, derartige Mails zu entschlüsseln.
Die Idee dieser „Einschreiben-Technik“ ist so simpel wie genial: Jeder Teilnehmer einer E-Mail-Kommunikation besitzt einen eigenen geheimen Decodier-Schlüssel, den nur er allein kennt. Außerdem hat er einen zweiten, öffentlichen Schlüssel, den er seinen Mit-Schreibern verrät. Mit diesem öffentlichen Schlüssel des Empfängers, den der Sender ja kennt, wird nun die Mail verschlüsselt. Der Witz: Nur mit dem privaten Schlüssel des Empfängers, den nur er allein kennt, kann diese Mail wieder entschlüsselt werden. Wenn zwei Personen also einmal die beiden öffentlichen Schlüssel getauscht haben, erfolgt in Zukunft die gesamte E-Mail-Kommunikation verschlüsselt. Wer von außen „zufällig“ mitliest, dem bietet sich in etwa folgendes Bild:

```
IfyPTNnbew4sO345dgrsDOFvRzWpmiPpU6P5M2BIROua
+hmw089wSAJQZotAsazlWqe3JG2ZPfA/sVoKwbUDMWewN/
S5/ycfvc3wcFjQJOx5X0DHksO+SmmcfX3SzEhy4Nes
+7VD2xHAGBn/BSZYUxZ1wuD6KGbLsfa7yrSSvhHa
+46sqrqinIFxsQlu82fuf5MjCU79cHAP5Uby9n+xbr-
DXXY1RzRegijeTW9/WsIV5MEqRvUF2aEWexD76kkKqLg/
5Q+u4w8R40QQKL2OY/lg3c2hna4scTQs/ete7SUji-
CBXMpt9DwaoLwLA8f7QOGCYGdZIBIyqZXLSS+9pj-
Czgui7V3ydgZAcM4StE8Gmje7vKlB178nmFiQ1jsjAP
```

So sieht eine verschlüsselte Mail aus, wenn man sie ohne Schlüssel liest. Man selber merkt nur an einem kleinen Schloß-Symbol im Mail-Programm, dass die Verschlüsselung aktiv ist.
Voraussetzung ist natürlich, dass beide Parteien ein entsprechendes GPG-Programm installiert haben.

So starten Sie mit GPG
Für PC- und Windows-Anwender gibt es die Pakete „GnuPG“ und „GPG4Win“zum Download hier:
www.gnupg.org
www.gpg4win.org

Wer einen Mac mit OS X besitzt, der findet GPG Suite (ein Paket mit den nötigen Einzelprogrammen) sowie eine detaillierte deutsche Schritt-für-Schritt-Anleitung im Support-Bereich hier:
https://gpgtools.org

GnuPG, GPG4Win und GPG beruhen auf der selben Technik und sind untereinander kompatibel - es kommt also nicht zu Problemen, wenn man Mails von Windows-Systemen zu Mac-Nutzern schickt. Und das Programm erkennt automatisch, ob der Empfänger bereits einen Schlüssel hinterlegt hat oder nicht und verschlüsselt die Nachricht nur dann, wenn der Empfänger ebenfalls GPG nutzt.

Wer sich intensiver mit GPG auseinandersetzen will, der kann bei Wikipedia recherchieren:
https://de.wikipedia.org/wiki/GNU_Privacy_Guard
erklärt die Funktionsweise der GPG-Verschlüsselung.

Wer sich nicht für die Theorie interessiert, sondern einfach nur wissen will, wie er das Programm schnell installieren kann, der sollte bei YouTube suchen. Dort sind jede Menge Filmchen hinterlegt, und wer „GPG Tutorial Windows“ oder „GPG Tutorial Mac“ eingibt, findet sofort eine Fülle hilfreicher Anleitungen. Hilfreiche Tipps sind auf der letzten Seite abgedruckt.

Bisher sind GPG-Verschlüsselungen (leider) nicht sehr weit verbreitet und bekannt. Ich selber bin in einem Kreis von Mac-Nutzern, die sich unter fachkundiger Anleitung regelmäßig zum Gedankenaustausch treffen, darauf aufmerksam geworden. Einer meiner Kunden, der im Bereich IT-Sicherheit unterwegs ist, hat mich dann ermutigt, es auch selber zu nutzen. Bisher kenne ich nicht einmal 20 Menschen, die ebenfalls GPG nutzen. Interessant aber, dass fast alle diese GPG-Nutzer aus dem beruflichen Umfeld der Software-Programmierung oder IT-Sicherheit kommen. Und die sollten wirklich wissen, was sinnvoll ist.

Daher lautet mein Tipp für Ihren besten guten Vorsatz für das kommende Jahr:

Installieren und nutzen Sie GPG!

Ausführliche Anleitung zur Installation von GPG (Mac):

https://gpgtools.tenderapp.com/kb/how-to/erste-schritte-gpgtools-einrichten-einen-schlssel-erstellen-deine-erste-verschlsselte-mail

Ich selber habe einen Mac und nutze GPGTools. Mit dieser Anleitung habe ich das Programm installiert.

Ausführliche Anleitung zur Installation von GnuPG und GPG4Win (Windows):

https://www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/anleitg.htm

Betreiber dieser Seite ist das Datenschutz-Zentrum für Schleswig-Holstein, eine Anstalt öffentlichen Rechts. Die Anleitung ist liebevoll aufgebaut, scheint mir aber eher für Nutzer älterer Windows-Varianten geeignet zu sein. Sie verweist auf die folgende Seite:

https://www.gpg4win.org/doc/de/gpg4win-compendium.html

Das ist die „offizielle“ Seite des GPG for Windows - Projektes, und die Anleitung ist leider auch schon 6 Jahre alt. Das ist die Kehrseite nicht-kommerzieller Projekte; sie werden nicht immer gepflegt. Betreiber der Seite ist Werner Koch, der Hauptentwickler der GPG-Software war und immer noch ist. Hier ist man also wirklich an der Quelle. Ein interessanter Artikel über Werner Koch findet sich hier:

http://www.taz.de/Verschluesselung-mit-GnuPG/!5020399/

Hier wird auch auf das außerordentlich hohe Sicherheitsniveau eingegangen, dass sich mit diesem einfachen Programm erreichen lässt. Seinerzeit - Anfang 2015 - hat sich selbst die NSA daran die Zähne ausgebissen - erfolglos.

Impressum

Michael Schulte, Lessingstr. 2, 22087 Hamburg
Email: info@vermoegen-besser-planen.de
Telefon: +49 40 4192938-8, Fax: +49 40 4192938-7

Zuständige Behörde für die Erteilung der Erlaubnis nach § 34 f, § 34 d und § 34 c Abs. 1 GewO sowie Zuständige Aufsichtsbehörde
Handelskammer Hamburg, Adolphsplatz 1, 20457 Hamburg
Telefon +49-(0)40-36138-138, Fax -401

Statusbezogene Pflichtinformationen gemäß § 42 b Abs. 2 S. 2 VVG sowie § 12 Abs. 1 der FinVermV in Verbindung mit § 34 f der GewO: unabhängiger Versicherungsmakler und registrierter Finanzanlagenvermittler mit Erlaubnis nach §§ 34 c, 34 d und 34 f Abs. 1 GewO durch Handelskammer Hamburg in der Bundesrepublik Deutschland. Mitglied bei und zuständige Aufsichtsbehörde für die Versicherungsvermittlung: Handelskammer Hamburg, Adolphsplatz 1, 20457 Hamburg, Telefon 0049-(0)40-36 13 8-138, Telefax 0049-(0)40-36 13 8-401, E-Mail service@hk24.de, Internet: www.hk24.de. Vermittlerregisternummer Versicherungen: D-QGQP-REMO9-62, Vermittlerregisternummer Finanzanlagen: DF- 131-5RLW-71. Das Vermittlerregister wird geführt bei: Deutscher Industrie-und Handelskammertag (DIHK) e.V., Breite Straße 29, 10178 Berlin, Tel: +49 (0) 180 500 585 0 (14 Cent/Min aus dem dt. Festnetz, höchstens 42 Cent/Min aus Mobilfunknetzen), Internet: www.vermittlerregister.info. Die Erlaubnis beinhaltet die Befugnis für Anlageberatung oder Vermittlung des Abschlusses von Verträgen über Anteilsscheine einer Kapitalanlagegesellschaft oder Investmentaktiengesellschaft oder von ausländischen Investmentanteilen, die im Geltungsbereich des Investmentgesetzes öffentlich vertrieben werden dürfen (§ 34f Abs. 1 Nr. 1 GewO) sowie Anteile an geschlossenen Fonds in Form einer Kommanditgesellschaft (§ 34f Abs. 1 Nr. 2 GewO). Es liegen keinerlei Beteiligungen an Versicherungsunternehmen mit mehr als 10 % Anteil an Stimmrechten oder Kapital vor. Die Anschriften der Schlichtungsstellen, die bei Streitigkeiten zwischen Vermittlern oder Beratern und Versicherungsnehmern angerufen werden können, lauten: Versicherungsombudsmann e.V., Postfach 08 06 32, 10006 Berlin, www.versicherungsombudsmann. de. Ombudsmann für die private Kranken-und Pflegeversicherung, Kronenstrasse 13, 10117 Berlin, www.pkv-ombudsmann.de. Weitere Adressen über Schlichtungsstellen und Möglichkeiten der außergerichtlichen Streitbeilegung erhalten Sie bei: Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin), Graurheindorfer-Straße 108, 53117 Bonn. Berufsrechtliche Regelungen: § 34 c, d und f GewO(Gewerbeordnung), § 12 Abs. 1 der Finanzanlagen-Vermittlungs-Verordnung (FinVermV), §§ 59-68 Versicherungsvertragsgesetz (VVG), Versicherungsvermittlerverordnung (VersVermV). Die berufsrechtlichen Regelungen können über die vom Bundesministerium der Justiz und der juris GmbH betriebenen Homepage www.gesetze-im-internet.de eingesehen und abgerufen werden.