Netzwerk Elektronischer Geschäftsverkehr

Fachhochschule Gelsenkirchen

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheitstipp: Sichere Kommunikation über das Internet

Schon in der Antike verschlüsselten Monarchen geheime Botschaften, die nicht in die Hände Unbefugter geraten durften. Das Prinzip ist seit tausenden von Jahren das Gleiche: Die Zeichen eines Textes werden mit Hilfe eines geheimen Schlüssels in eine nicht interpretierbare Zeichenfolge übersetzt. Nur mithilfe des passenden Schlüssels oder Schlüsselpaars kann die Nachricht entschlüsselt werden – daraufhin kommt die Information wieder zum Vorschein. In Zeiten des Internets ist das Verschlüsseln von vertraulichen Daten wichtiger denn je. Dank moderner Hilfsprogramme war es für Datendiebe nie so einfach wie heute, unverschlüsselte E-Mails und Chats auszuspähen oder Telefongespräche mitzuhören. Gerade für Unternehmen stellt die unverschlüsselte Kommunikation über das Internet ein hohes Sicherheitsrisiko dar. Erfahren Sie in diesem IT-Sicherheitstipp, was Sie beachten sollten, um Ihre Sicherheit bei der Kommunikation über das Internet zu erhöhen.

Nutzen Sie beim Austausch sensibler Daten stets eine Verschlüsselung

Der Datenaustausch im Internet erfolgt größtenteils unverschlüsselt. Die meisten Unternehmen ordnen sicherheitsrelevante Maßnahmen wie Datenverschlüsselungen der Praktikabilität von Arbeitsabläufen unter. Laut der Studie *„Netz- und Informationssicherheit in Unternehmen 2011“*, die vom *„Netzwerk Elektronischer Geschäftsverkehr“ (NEG)* im Rahmen des Verbundprojekts *„Sichere Geschäftsprozesse in KMU und Handwerk“* durchgeführt wurde, legen nur rund 43 Prozent der 254 befragten Unternehmen den Fokus auf Sicherheit, wenn sie sich zwischen Sicherheit und Funktionalität entscheiden müssten [1]. Dabei sind viele Daten, die online übertragen werden, sehr sensibel. Ein Datendiebstahl oder gar Verlust kann in manchen Fällen den Ruin des Unternehmens bedeuten. Handelt es sich beispielsweise um Personaldaten, Finanzdaten, oder Betriebs- und Geschäftsgeheimnisse, wird eine verschlüsselte Kommunikation zwingend erforderlich, um Sicherheitsrisiken zu minimieren [2]. **Stellen Sie mit Ihrem Unternehmen Online-Dienste zur Verfügung, bei denen Kunden vertrauliche Daten austauschen, müssen Sie serverseitig entsprechende Sicherheitsstandards einhalten. Ein Beispiel hierfür ist das Betreiben eines eigenen Online-Shops. Hier empfiehlt es**

sich besonders bei der Kaufabwicklung eine verschlüsselte Verbindung via SSL/TLS anzubieten. Dabei prüft der Internetbrowser einerseits, ob er tatsächlich mit dem Server verbunden ist, der sich hinter einer Internetadresse verbirgt. Andererseits ermöglicht eine SSL/TLS-Verbindung die Kommunikation über einen verschlüsselten Kanal. **Sie erkennen eine solche Verschlüsselung daran, dass in der Adresszeile des Browsers hinter dem „http“ ein zusätzliches Zeichen „s“ erscheint („https“).** Die meisten Browser stellen die erfolgreiche verschlüsselte Kommunikation mit dem Server optisch dar, indem ein kleines Schloss in der Statuszeile des Browsers erscheint.

Schützen Sie sich im öffentlichen Netzwerk

Besondere Vorsicht ist bei der Nutzung von Online-Diensten geboten, wenn Sie sich innerhalb eines öffentlichen Netzwerkes befinden. Viele Unternehmen, Restaurants und Cafés stellen Besuchern und Gästen heutzutage eine freie WLAN-Nutzung zur Verfügung. So komfortabel ungeschützte öffentliche Netzwerke auch sein mögen, so viele Gefahrenquellen tun sich bei unbedachter Nutzung auf. Prinzipiell kann hier Ihr gesamter Datenverkehr im Internet von einem anderen Rechner im selben Netzwerk abgehört werden. Darunter fallen Browserverläufe, Chats, Aktivitäten in sozialen Netzwerken, E-Mails und Downloads. Selbst wenn Sie Online-Dienste über eine Verschlüsselung mittels SSL/TLS in Anspruch nehmen, verfällt der Schutz: Gewiefte Angreifer schleusen sich heimlich zwischen Nutzer und Zielserver und manipulieren so die verschlüsselte Kommunikation, beispielsweise mit dem Online-Banking-Server. Dies kann erkannt werden, wenn plötzlich der Browser beim Besuchen der scheinbar seriösen Webseite eine Zertifikatswarnung meldet. **Tauschen Sie daher in öffentlichen Netzwerken niemals sensible Daten aus. Seien Sie sich immer darüber bewusst, dass jede Eingabe, die Sie in einem öffentlichen und damit fremden Netzwerk machen, problemlos mitgehört werden kann.**

Nutzen Sie nach Möglichkeit eine VPN-Verschlüsselung zur drahtlosen Kommunikation

Mittlerweile bieten zahlreiche Unternehmen und Institutionen Ihren Beschäftigen an, auch innerhalb öffentlicher Netzwerke auf das eigene Unternehmensnetzwerk, mittels einer bereitgestellten sogenannten VPN-Verbindung (Virtual Private Network), verschlüsselt zuzugreifen. Somit können sensible Unternehmensinterna auch innerhalb eines öffentlichen Netzwerkes ausgetauscht werden. Sobald Sie die jeweilige VPN-Verbindung zu Ihrem Unternehmen hergestellt haben, sind Sie mit Ihrem Unternehmensnetzwerk so verbunden, als wären Sie tatsächlich vor Ort. Das öffentliche Netz stellt im übertragenen Sinne eine Brücke zu Ihrem Betriebsnetzwerk dar.

Für Angreifer innerhalb des öffentlichen Netzes sind jene Daten, die Sie mit Ihrem Unternehmensnetzwerk austauschen, nun nicht mehr direkt erreichbar. Die Datendiebe sehen dann nur, dass Sie innerhalb des öffentlichen Netzwerkes verschlüsselt kommunizieren – das Ausspähen unternehmensinterner Daten wird deutlich erschwert. **Die Kommunikation über das Unternehmensnetzwerk hinaus, z.B. privates Online-Banking, findet jedoch zumeist weiterhin unverschlüsselt im öffentlichen Netzwerk statt.**

Hinweise zum Aufbau und Erstellen Ihrer eigenen betrieblichen VPN-Verbindung erhalten Sie auf der Internetseite des *Bundesamtes für Sicherheit und Informationstechnik* [3].

Verschlüsseln Sie Ihre E-Mails

Welche E-Mails Sie verschlüsseln sollten und welche unverschlüsselt übertragen werden können, entscheiden sie am besten nach dem „Postkarten-Prinzip“: Stellen Sie sich vor, dass Sie keine digitale Nachricht, sondern eine Postkarte an Ihren Adressaten versenden wollen. **Alle Informationen, die Sie bedenkenlos auf die Postkarte schreiben würden, können Sie auch mittels unverschlüsselter E-Mail versenden. Das, was nicht so einfach von der Postkarte abgelesen werden sollte, verschicken Sie besser via verschlüsselter E-Mail.** Würden Sie sensible Kundendaten und betriebsinterne Informationen auf eine Postkarte schreiben? Sicherlich nicht.

Als Verschlüsselungsmechanismus für E-Mails eignet sich beispielsweise das *PGP*-Verfahren (*PGP steht kurz für Pretty Good Privacy*). Alle Teilnehmer dieser Methode besitzen zwei zusammengehörige Schlüssel: Einen öffentlichen, der für Jedermann zugänglich ist und einen privaten, den nur der jeweilige Besitzer kennt. Möchte ein Beschäftigter Ihres Unternehmens einem anderen ein vertrauliches Dokument zusenden, verschlüsselt er es mit dem öffentlichen Schlüssel des Adressaten. Der Empfänger des Dokuments kann das geschützte Dokument erst lesen, nachdem er es mit seinem privaten, passwortgeschützten Schlüssel entschlüsselt. Mit dem PGP-Verfahren ist es ebenfalls möglich E-Mails digital zu signieren, um die Identität des Absenders sicherzustellen. Dafür verschlüsselt der Absender der E-Mail das Dokument nicht nur mit dem öffentlichen Schlüssel des Empfängers, sondern unterzeichnet dieses auch mit seinem eigenen privaten Schlüssel. Der Empfänger entschlüsselt die E-Mail dann nicht nur mit seinem privaten Schlüssel, sondern prüft diese auch mit dem öffentlichen Schlüssel des Absenders. Er weiß nun, dass es sich um den richtigen Absender handeln muss und die Nachricht nicht manipuliert wurde, denn niemand anders ist in der Lage, die Nachricht mit dem privaten Schlüssel des Absenders zu signieren, als der Absender selbst. Weitere Hinweise hierzu finden Sie in dem IT-Sicherheitstipp *„Sicherer Dokumentaustausch via E-Mail“* [2].

Nutzen Sie alternative Wege, um digitale Nachrichten sicher zu versenden

E-Mails sind längst nicht mehr die einzigen digitalen Nachrichten, die Sie versenden können. Mittlerweile gibt es einige Alternativen, die Sie unter sicherheitsrelevanten Gesichtspunkten vorziehen könnten. **Dazu gehört beispielsweise der *„E-POSTBRIEF“*. Mit diesem Verfahren stellt die *Deutsche Post* eine Möglichkeit zur Verfügung, wie Sie elektronische Nachrichten identitätsgeprüft versenden können.** Um diesen Service nutzen zu können, müssen Sie sich vorab registrieren und über das *POSTIDENT*-Verfahren legitimieren. Anschießend können Sie Briefe online versenden. Der Empfänger erhält Ihre Nachricht auf sicherem Wege elektronisch zu den Kosten eines Standardbriefes (Stand Dezember 2011), sofern er ebenfalls beim *E-POSTBRIEF*-Verfahren

angemeldet ist, oder ausgedruckt auf postalischem Wege. Hierbei fallen Kosten gestaffelt nach Gewicht an [4]. Durch das Verfahren sind auch elektronisch versandte Einschreiben möglich, bei denen der Empfänger einer Nachricht den Erhalt quittieren muss. Viele Behörden und Institutionen akzeptieren mittlerweile den E-POSTBRIEF auch für die Einreichung von Dokumenten, die sensible Daten enthalten. Hinweise und Nutzungsbedingungen des E-POSTBRIEF-Verfahrens erhalten Sie auf der Internetseite der Deutschen Post [4].

Ein weiteres sicheres Verfahren, um elektronische Nachrichten zu übertragen, ist das *De-Mail*-Verfahren, das vom deutschen Innenministerium koordiniert wird. Der Versand von digitalen Nachrichten und Dokumenten erfolgt über zertifizierte Provider auf verschiedenen Wegen. Je nach gewünschter Vertraulichkeitsstufe der Informationen, können verschiedene Verschlüsselungsverfahren bei der Übertragung der Nachricht zum Einsatz kommen. So geben beispielsweise elektronische Signaturen und Empfangsbestätigungen Auskunft über die richtigen Identitäten zwischen Sender und Empfänger. Hinweise zur Nutzung des *De-Mail*-Verfahrens erhalten Sie auf der offiziellen Seite der Bundesregierung [5].

Chatten und Telefonieren Sie nur verschlüsselt

Achten Sie auch beim Chatten und Telefonieren über das Internet darauf, dass Sie vertrauliche Daten nicht ungeschützt über das Internet kommunizieren. In vielen Unternehmen ist die Internettelefonie etwas alltägliches geworden, um mit Außendienstmitarbeitern und Geschäftskontakten in Verbindung zu treten. Selbst wenn Sie sich mit Ihrem Chatpartner im selben W-LAN aufhalten, sollten Sie Ihre Gesprächsdaten verschlüsselt übertragen, um nicht von Dritten abgehört werden zu können. Einige Chatprogramme wie *Skype* verschlüsseln Ihre Gespräche standardmäßig. Sofern Sie kostenlose Programme nutzen möchten, sollten Sie besonders auf die Nutzungsbedingungen und Schutzmaßnahmen des Herstellers achten. Überprüfen Sie, aus welcher Quelle das Programm stammt und entscheiden Sie sich ggf. für eine kostenpflichtige Alternative. Die Chatfunktionen sozialer Netze sind meist nicht ausreichend vor dem Zugriff Unbefugter geschützt. **Bedenken Sie also stets, welche Informationen Sie austauschen möchten und welche lieber via verschlüsselter E-Mail übersandt werden sollten.** Geben Sie Ihre Voice-over-IP-Telefonnummer nur mit Bedacht an ausgewählte Kontakte weiter. Deaktivieren Sie in jedem Fall die automatische Dateiannahme Ihres Chatprogramms und öffnen Sie keine unbekannten Dateianhänge.

Achten Sie auf einen ausreichenden Basisschutz

Grundvoraussetzung für einen angemessenen Basisschutz in Ihrer Internetkommunikation sind zwei Anwendungen: Ein Virenschutzprogramm, das Schadsoftware auf Ihrem PC aufspürt, blockiert und beseitigt und eine Personal Firewall, die wie ein Türsteher den Netzwerkverkehr zwischen Ihrem Computer und dem Internet regelt. **Halten Sie Virenschutzprogramm, Firewall und**

alle anderen installierten Programme mit Sicherheitsupdates immer auf dem neuesten Stand. So können Sie neu entdeckte Sicherheitslücken zeitnah schließen.

Autoren

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen

[1] http://www.kmu-sicherheit.de

http://www.ec-net.de

[2] https://ratgeber.it-sicherheit.de

[3] https://www.bsi.bund.de

[4] http://www.e-post.de

[5] http://de-mail.de

https://www.internet-sicherheit.de

http://www.bsi-fuer-buerger.de

http://www.sicher-im-netz.de

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.kmu-sicherheit.de

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de