Allgemeine Geschäftsbedingungen für die Kommunikation per E-Mail

Die vorliegenden Allgemeinen Geschäftsbedingungen für die Kommunikation per E-Mail sind Bestandteil der zwischen dem/den Kontoinhaber(n), dem/den Kunden und den Vertragsparteien (nachfolgend zusammenfassend der "Kunde") und der Rothschild & Co Bank AG (nachfolgend "Bank") abgeschlossenen Vereinbarung für die Kommunikation per E-Mail.

Der Kunde und die Empfänger/Absender nehmen hiermit die nachstehenden Informationen und Allgemeinen Geschäftsbedingungen für die Kommunikation per E-Mail mit der Bank zur Kenntnis. Der Kunde ist sich bewusst, dass es im heutigen globalen Kommunikationsumfeld bestimmte Bedrohungen gibt und dass es wichtig ist, seine Daten im Zusammenhang mit Bankgeschäften sicher zu behandeln.

Risiken

Der Kunde und die Empfänger/Absender sind sich bewusst, dass per unverschlüsselter E-Mail verschickte Mitteilungen über ein offenes, für jedermann zugängliches Netzwerk, auch grenzüberschreitend übermittelt werden und diese daher grundsätzlich, wenn sie nicht verschlüsselt sind, für Dritte zugänglich sind. Dadurch können Dritten Kenntnis von einer bestehenden Kundenbeziehung zur Bank erhalten. Zudem verstehen der Kunde und die Empfänger/Absender, dass der sprachliche, wie auch der elektronische Inhalt von Mitteilungen per unverschlüsselter E-Mail durch Dritte verändert oder manipuliert werden könnte.

Wenn die Kommunikation zwischen der Bank und dem Empfänger/Absender verschlüsselt ist, ist der Inhalt der Kommunikation mit den angegebenen E-Mail-Adressen oder dem Domainnamen geschützt. Der Kunde und die Empfänger/Absender nehmen zur Kenntnis, dass aber nur der Inhalt geschützt ist, nicht aber die E-Mail-Adresse der Bank und die angegebenen E-Mail-Adressen oder Domain-Namen, da diese nicht anonym sind und somit sichtbar bleibt, dass eine Kommunikation mit der Bank geführt wird.

Der Kunde entbindet die Bank und die Empfänger/Absender dahingehend explizit vom Bankkundengeheimnis sowie von jeglichen Datenschutzbestimmungen.

Es besteht grundsätzlich stets die Gefahr, dass sich unberechtigte Personen während der Internet-Nutzung unerlaubten Zugriff zu den IT-Einrichtungen (z. B. dem Computer) des Kunden oder der Empfänger/Absender verschaffen. Der Kunde und die Empfänger/Absender sind sich bewusst und anerkennen, dass dieses Risiko erhöht sein kann, wenn nur bzw. auch ein Domain-Name angegeben wird. Jeder Nutzer ist daher selbst dafür verantwortlich, alle notwendigen technischen Vorkehrungen zu treffen, die mit der Nutzung des Internets verbundenen Risiken zu minimieren und sicherzustellen, dass sein EDV-System mit den aktuellen Methoden zur Abwehr von Malware (z. B. Viren, Würmer, Trojaner) sowie zum Schutz vor Hackern (z. B. durch eine Firewall) ausgestattet ist.

Der Kunde und die Empfänger/Absender nehmen zur Kenntnis, dass die Übertragung eines Auftrags, eine Mitteilung oder Kommunikation aufgrund von Übertragungsfehlern, technischen Mängeln, Ausfällen, Störungen, rechtswidrigem Eingriff, Netzüberlastung und mutwilliger Sperrung elektronischer Zugänge durch Dritte oder sonstiges Versagen seitens der Netzbetreiber verspätet, unterbrochen oder vollständig verhindert werden können. Darüber hinaus kann es auch aufgrund der Bearbeitungsdauer einer E-Mail in der Bank selbst zu Verzögerungen kommen.

Identitätsdiebstahl

Identitätsdiebstahl gehört zu den sich am schnellsten ausbreitenden Kriminalitätsformen in der Finanzbranche, von denen jedes Jahr Millionen von Menschen betroffen sind. Identitätsdiebstahl bezeichnet den Diebstahl der Identität/personenbezogenen Daten einer Person, wie Name, Geburtsdatum, Adresse, E-Mail usw., die von Betrügern zu ihrem finanziellen Vorteil genutzt werden. So können Betrüger beispielsweise Identitätsdaten verwenden, um Zahlungen und Geldüberweisungen auszuführen, oder sie können Kreditkarteninformationen nutzen, um Waren und Dienstleistungen auf Kosten der Person zu kaufen, deren Identität gestohlen wurde. Eine verbreitete Methode, mit der sich Betrüger Identitäten verschaffen, besteht darin, das E-Mail-Konto einer Person zu kompromittieren und sich Zugang zu deren E-Mail-Korrespondenz zu verschaffen, um so ihre Beziehungen zu ermitteln und sie möglicherweise missbräuchlich zu nutzen.

Betrügerische E-Mails

Betrüger nutzen E-Mails oft als Mittel, um an personenbezogene Daten von Personen zu gelangen. Solche E-Mails können den Empfänger auffordern, seine personenbezogenen und finanziellen Daten zu aktualisieren oder zu überprüfen, einschliesslich Geburtsdatum, Anmeldeinformationen, Kontodaten, Kreditkartennummern usw. In der Regel geben diese E-Mails vor, von einer seriösen Organisation wie einer Bank oder einem Online-Händler zu stammen. Die E-Mail enthält einen Link, der Sie zu einer gefälschten Website führt, die identisch mit der echten Website der Organisation scheint oder sehr ähnlich aussieht. Der Betrüger kann dann personenbezogene Daten wie Passwörter abfangen, während Sie sie eingeben, oder Malware auf Ihren Computer herunterladen.

Wenn ein Kunde oder die Empfänger/Absender eine E-Mail mit bankenspezifischen Anfragen erhalten, bei der sie nicht sicher sind, ob die Quelle tatsächlich die Bank ist, sollten sie den Kundenberater telefonisch kontaktieren, um dies zu überprüfen. Wenn der Kunde und die Empfänger/Absender den Verdacht haben, dass ein E-Mail-Konto, von dem aus mit der Bank kommuniziert wurde, kompromittiert worden sein könnte, müssen der Kunde und die Empfänger/Absender die Bank unverzüglich informieren.

Schutz

Um das Risiko zu verringern, dass Ihr E-Mail-Konto kompromittiert wird oder Sie Opfer eines Identitätsdiebstahls werden, werden der Kunde und die Empfänger/Absender gebeten, die folgenden Sicherheitsempfehlungen zu beachten:

- Seien Sie im Internet immer besonders vorsichtig und überlegen Sie genau, an wen und wo Sie personenbezogene Daten weitergeben.
- Versenden Sie keine Passwörter per E-Mail und geben Sie sie nicht an andere weiter. Die Bank wird Sie nie nach einem Passwort fragen.
- Antworten Sie nicht auf unaufgeforderte oder unerwünschte E-Mails und geben Sie keine Angaben zu Bankkonten oder personenbezogenen Daten preis, wenn sie dazu aufgefordert werden und Sie nicht sicher sind, wer der Empfänger ist. Die Bank wird einen Kunden oder die Empfänger/Absender ausschliesslich über den jeweiligen Kundenbetreuer kontaktieren.
- Klicken Sie niemals auf Links in einer verdächtigen E-Mail. Das Anklicken eines solchen Links kann dazu führen, dass eine Schadsoftware wie z.B. ein Virus auf den Computer heruntergeladen wird, die es einem Betrüger ermöglicht, Zugang zu personenbezogenen Informationen zu erhalten.
- Verwenden Sie zum Schutz von E-Mail-Konten ein Passwort, das schwer zu erraten ist. Ein sicheres Passwort sollte aus mindestens acht Zeichen bestehen und Grossbuchstaben, Zahlen und Sonderzeichen wie / $ _ # - + usw. enthalten. Es wird ausserdem empfohlen, für verschiedene Anwendungen und Konten unterschiedliche Passwörter zu verwenden.
- Nutzen Sie Virenschutzsoftware auf Ihrem Computer und sorgen Sie dafür, dass sie stets mit neuen Versionen aktualisiert wird.
- Prüfen Sie regelmässig die Salden der Kontoauszüge und gleichen Sie sie ab, um sich von der Richtigkeit jeder Transaktion zu überzeugen. Überprüfen Sie auch immer die Kontoauszüge, um festzustellen, ob nicht autorisierte Überweisungen vorliegen.

Die sichere Kommunikationslösung der Bank

Die Bank bietet *Secure Email* an, eine sichere Umgebung für die E-Mail-Kommunikation mit der Bank. *Secure Email* bietet dem Kunden die folgenden Sicherheitsvorteile:

- Die E-Mail-Korrespondenz mit Rothschild wird von Ihren anderen persönlichen E-Mails getrennt, und für den Zugang zu den E-Mails ist ein zusätzlicher Benutzername/ein zusätzliches Passwort erforderlich. Daher würde ein Betrüger, der Ihr persönliches Konto kompromittiert hat, keine Kenntnis von Ihren E-Mails und den mit Rothschild ausgetauschten Informationen erlangen.
- Die E-Mails des Kunden oder eines Empfängers/Absenders werden ausschliesslich in den Systemen der Bank gespeichert; sie verlassen niemals die Räumlichkeiten der Bank.
- Die Systeme der Bank sind sicher und werden regelmässig von spezialisierten Cybersicherheitsunternehmen überprüft.
- Secure Email ist benutzerfreundlich und kann auf den meisten Geräten verwendet werden.