htp GmbH • Mailänder Straße 2 • 30539 Hannover

Informationen zur sichere E-Mail Kommunikation bei htp

Inhalt

1 Ausgangslage

Die E-Mail ist in der heutigen Zeit neben dem Telefon und der klassischen Briefpost in der täglichen Kommunikation nicht mehr wegzudenken. Die schnelle und kostenlose Zustellung, die einfache Benutzung und die Erreichbarkeit von fast Jedermann auf der Welt haben für einen schnellen Einzug der E-Mail in unser Leben gesorgt.
Egal ob bei der rein privaten Kontaktaufnahme mit Freunden und Bekannten, ob im Berufsleben oder bei der Kommunikation mit Behörden, Ämtern oder beim Online-Shopping ist die E-Mail oftmals die erste Wahl.

Die Schattenseite des modernen Mediums E-Mail werden von Anwendern dabei oft ausgeblendet:

- E-Mails sind unverschlüsselt wie eine einfache Postkarte im Internet unterwegs. Rechnen Sie stets damit, dass Inhalte einer unverschlüsselten E-Mail von Dritten, wie Hackern oder Geheimdiensten, mitgelesen werden könnten.
- Die persönlichen Zugänge zu Ihrem Postfach sind für Cyber-Kriminelle ebenfalls ein interessantes Ziel. Mit Kenntnis Ihrer Zugangsdaten können Hacker beispielsweise Ihr Adressbuch auslesen und schadhafte Viren oder Spam-Mails mit Ihrem Absender an andere Personen versenden.
- Im geschäftlichen Umfeld sind oftmals zusätzlich Firmengeheimnisse und interne Informationen bedroht.

Mit den folgenden Sicherheitshinweisen möchten wir auf mögliche Risiken bei der E-Mail-Kommunikation und entsprechende Maßnahmen zur Vermeidung hinweisen.
Bitte nehmen Sie sich unsere Tipps zu Herzen und prüfen Sie Ihr Verhalten. Mit wenig Aufwand können Sie die Sicherheit Ihrer E-Mail-Kommunikation bereits erheblich verbessern.

Wir wünschen Ihnen weiterhin eine reibungslose Kommunikation mit Ihrer htp E-Mail-Adresse.

2 Starke Kennwörter für starken Zugangsschutz

Die E-Mail-Adresse oder der zugehörige Loginname als Teil der erforderlichen Anmeldedaten sind in der Regel für Hacker leicht zu erraten oder sogar bekannt. Der eigentliche Zugangsschutz zu Ihrem E-Mail Postfach ist Ihr persönliches Kennwort, welches nur Ihnen bekannt sein darf.

Damit das Kennwort nicht durch einfaches „ausprobieren“ von anderen erraten werden kann, sollte es möglichst kompliziert gewählt sein. Das Ausprobieren wird in der IT-Sprache als „BruteForce-Attacke“ bezeichnet. Dabei werden automatisiert durch trickreiche Programme Anmeldungsversuche mit wechselnden Kennwörtern vorgenommen, die entweder zufällig erzeugt werden oder aus einer Liste mit häufigen Kennwörtern kommen. Einfache Kennwörter können damit in begrenzter Zeit herausgefunden werden.

Bitte beachten Sie daher folgende Hinweise für die Erstellung eines starken und sicheren Kennwortes:

- Verwenden Sie keine Standardkennwörter oder einfache Wörter wie beispielsweise „start“, „start123“, „qwertz“, „kennwort“, „meinkennwort“, „passwort“
- Verwenden Sie ein Kennwort mit einer Länge von mindestens 10 Zeichen
- Verwenden Sie neben Kleinbuchstaben auch Großbuchstaben, Zahlen und Sonderzeichen
- Verwenden Sie wenn möglich keine Wörter sondern einen „Buchstabensalat“
- Das Kennwort sollte dennoch für Sie merkbar sein, damit Sie es sich nicht notieren oder ständig nachschlagen müssen

Sollte Ihnen jetzt ad hoc kein Kennwort einfallen, welches die genannten Hinweise erfüllt, versuchen Sie es einmal mit folgendem Trick:

1. Denken Sie sich einen Satz aus, den Sie sich gut merken können und der, wenn möglich schon eine Zahl enthält.
   Beispiel: Mein erstes Auto habe ich 1999 in Berlin gekauft.
2. Verwenden Sie für Ihr neues Kennwort nur die Anfangsbuchstaben und Zahlen des ausgedachten Satzes.
   Beispiel: MeAhi1999iBg
3. Tauschen Sie einige Buchstaben durch einprägsame Sonderzeichen aus.
   Beispiel: MeAh!1999!Bg

Haben Sie ein starkes, schwer zu erratendes E-Mail Kennwort?
Falls nicht sollten Sie es schnellstmöglich online im htp WebMailer (https://webmail.htp.net) unter dem Punkt „Einstellungen“ ändern.

3 Kennwortänderung

Auch jedes noch so gute Kennwort könnte von einem Unbefugten z.B. durch einen Blick auf Ihre Tastatur oder mittels einer Trojaner-Schadsoftware mitgelesen werden. Am Sichersten ist daher eine regelmäßige Änderung Ihres Kennworts, z.B. alle 6 Monate. Sollten Sie diesen Aufwand scheuen, so empfehlen wir Ihnen dringend eine Änderung, wenn Sie konkreten Anlass zur Sorge haben. Dieses könnte z.B. in folgenden Situationen der Fall sein:

- Ihr Virenscanner erkennt eine Schadsoftware auf einen Ihrer Rechner
- Sie haben ein offenes, unbekanntes WLAN genutzt und Ihre E-Mail über eine unverschlüsselten Verbindung abgerufen
- Ihre Freunde und Bekannte erhalten Spam-Mails mit Ihrem Absender

In jedem Fall sollten Sie das Kennwort bei einem neu eingerichteten E-Mail-Postfach ändern.

Haben Sie ein ungutes Gefühl oder einen Verdacht, Ihr Kennwort könnte gehackt sein?
Ändern Sie Ihr Kennwort schnellstmöglich online im htp WebMailer (https://webmail.htp.net) unter dem Punkt „Einstellungen“ ändern.

Haben Sie ein neues E-Mail-Postfach von htp erhalten?
Dann ändern Sie Ihr Kennwort sofort.

4 Zugangskennwort sicher aufbewahren

Das Kennwort für Ihr E-Mail-Postfach sollten Sie im Idealfall nicht aufschreiben sondern im Gedächtnis behalten. Doch für den Fall, dass das Kennwort aus dem Gedächtnis entfallen sollte, möchte man das Kennwort gerne zusätzlich in Schriftform ablegen.
Bewahren Sie ein Kennwortvermerk unbedingt unzugänglich für Dritte auf; z.B. in einer abschließbaren Schreibtischschublade und in einem verschlossenen Briefumschlag.
Für eine Speicherung auf Ihren PC empfehlen wir Ihnen den Einsatz einer Passwortmanagement-Software, wie z.B. „KeePass Passoword Safe“. Logins, Kennwörter und weitere Informationen werden so verschlüsselt gespeichert. Für den Zugriff zum „Passwort-Safe“ sollten Sie unbedingt ein starkes Kennwort verwenden.

Sollten Sie den Verdacht haben, das Unbefugte Zugang zu Ihrer Kennwortnotiz hatten, so sollten Sie schnellstmöglich ein neues Kennwort vergeben.

Haben Sie Ihr Kennwort notiert?
Bewahren Sie das Dokument mit dem Kennwort sicher verschlossen und in einem zugeklebten Briefumschlag auf. Verwenden Sie alternativ eine Passwortmanagement-Software.

5 Verschlüsselte Verbindung

Bei einer verschlüsselten Kommunikation werden die Daten abhörsicher zwischen Ihrem E-Mail-Programm und dem htp Mailserver übertragen. Hacker können auf dieser „Teilstrecke“ der E-Mail weder Einblick in die E-Mail erhalten noch die Anmeldedaten mit Ihrem Kennwort mitlesen.

Eine verschlüsselte Übertragung für den Versand und Empfang von E-Mails sollten Sie unbedingt mindestens dann verwenden, wenn Sie nicht über Ihren eigenen DSL Anschlusses mit Ihrem E-Mail-Programm auf Ihre E-Mails zugreifen oder E-Mails versenden. Insbesondere bei der Nutzung von öffentlichen, unverschlüsselten WLAN Zugängen sollten Sie auf eine verschlüsselte Verbindung achten.

Die htp Mailserver unterstützen die folgenden Protokolle für eine verschlüsselte Übertragung der Daten:

- POP3-STARTTLS (Port TCP-110)
- POP3 via SSL (Port TCP-995)
- IMAP4-STARTTLS (Port TCP-143)
- IMAP4-SSL (Port TCP-993)
- SMTP-AUTH-STARTTLS (Port TCP-25)
- SMTP-AUTH-SSL (Port TCP-465)

Die Aktivierung der verschlüsselten Verbindung nehmen Sie im Bereich Einstellungen Ihres E-Mail-Programmes vor. Auch E-Mail Programme von Tablet-Rechnern oder Smartphones unterstützen verschlüsselte Verbindungen.

Mit den Produkten htp Mail Pro und htp Mail Business können Sie Ihr Android oder Apple iOS Gerät mit Ihrem htp E-Mail-Postfach bequem synchronisieren. E-Mails, Termine und Kontakte werden somit online und sofort zwischen Ihrem htp E-Mail Postfach und Ihrem Endgerät abgeglichen. Diese Verbindung erfolgt ebenfalls verschlüsselt über das Active-Sync Protokoll (Port TCP-443).

Der Zugang zu Ihren E-Mails mit dem Webbrowser über den htp WebMailer erfolgt ausschließlich verschlüsselt über das https-Protokoll.

Bitte beachten Sie, dass mit einer verschlüsselten Verbindung ausschließlich die Daten zwischen Ihrem Rechner und dem htp Mailserver verschlüsselt werden. Die Übertragung Ihrer E-Mail kann dann im weiteren Verlauf durch das Internet unverschlüsselt erfolgen, so dass sie auf der Strecke zum Empfänger mitgelesen werden könnte.

Die htp Mailserver unterstützen ebenfalls eine verschlüsselte Kommunikation zu anderen Mailservern. Sollte der kommunizierende Mailserver ebenfalls eine verschlüsselte Übertragung unterstützen, so wird die E-Mail auch auf ihrem Weg durch das Internet verschlüsselt und somit anhörsicher übertragen.

Für einen sicheren Transport der E-Mail auf dem gesamten Weg durch das Internet benötigen Sie allerdings zwingend eine Ende-zu-Ende-Verschlüsselung.

Greifen Sie außerhalb Ihres DSL-Anschlusses auf Ihr htp E-Mail-Postfach zu?
Verwenden Sie unbedingt eine verschlüsselte Verbindung zwischen Ihrem E-Mail-Programm und dem htp Mailservern.

Die verschlüsselte Verbindung mit dem E-Mail-Programm bedeutet nicht, dass die E-Mail auch verschlüsselt durch das Internet übertragen wird!

6 Ende-zu-Ende Verschlüsselung

Bei einer Ende-zu-Ende Verschlüsselung werden die E-Mails vor dem Versenden vom Versender verschlüsselt und erst nach Empfang vom Empfänger wieder entschlüsselt. Damit erfolgt sowohl die Übertragung zwischen dem E-Mail-Programm und dem Mailservern als auch die Übertragung zwischen den Mailservern im Internet verschlüsselt.

Im E-Mail Umfeld kommen hierzu häufig die Verfahren OpenPGP oder S/MIME zum Einsatz. Beide Methoden basieren auf einer asymmetrischen Ver- und Entschlüsselung mit einem Schlüsselpaar: Der Empfänger der E-Mail besitzt hierzu einen privaten und einen öffentlichen Schlüssel. Der private Schlüssel ist geheim und verbleibt im Besitz des Empfängers. Er ist in der Regel zusätzlich mit einem persönlichen Kennwort („Passphrase“) geschützt, die vor der Benutzung des privaten Schlüssels eingegeben werden muss. Der öffentliche Schlüssel des Empfängers ist zur Verteilung an die Kommunikationspartner gedacht.
Die zu versendende E-Mail wird vom Versender mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und kann nur vom Empfänger mit dem zugehörigen privatem Schlüssel wieder entschlüsselt werden.
Für die Ver- und Entschlüsselung ist eine spezielle Software oder einen spezielles Addon für das E-Mail-Programm erforderlich.

Die Verfahren OpenPGP und S/MIME bieten auch Methoden zur Unterzeichnung bzw. Signierung von E-Mails. Dabei wird die E-Mail mit dem privaten Schlüssel des Versenders signiert und vom Empfänger mit dem öffentlichen Schlüssel des Versenders geprüft.
Mit einer Signierung kann sichergestellt werden, dass die E-Mail tatsächlich vom Versender stammt („Authentizität“) und dass die E-Mail nicht verändert wurde („Integrität“).

Sie möchten sicher gehen, dass eine E-Mail vom Versender bis zum Empfänger durchgängig für Dritte unzugänglich über das Internet übertragen wird?
Nutzen Sie etablierte Verschlüsselungsprogramme, wie z.B. OpenPGP.

Eine kostenfreie Software für OpenPGP und S/MIME erhalten Sie z.B. unter http://www.gnupg.org.

htp
Gut gewählt!

7 Wie sicher sind meine E-Mails bei htp?

Als Ihr Provider ist uns bewusst, wie sensibel mit Kundendaten, wie E-Mails und Zugangsdaten umgegangen werden muss.
Gesetzliche Regelungen, wie z.B. das Telekommunikationsgesetz (TKG) oder das Bundesdatenschutzgesetz (BDSG), geben Mindestanforderungen zum sicheren Umgang mit personenbezogenen Daten vor. htp betreibt darüber hinausgehend weitere Schutzmaßnahmen, um ein höchstes Maß an Sicherheit zu erzielen:

- Speicherung der Daten in hochsicheren htp DataCenter in der Region Hannover
- Strenge Zutrittsregelung und Zutrittsprüfungen
- Mehrfachspeicherung der Daten (Redundanz) und regelmäßige Datensicherung zum Schutz vor Datenverlusten
- Mehrstufige Sicherungssysteme (Firewalls) zur Absicherung vor Gefahren aus dem Internet
- Regelmäßige verpflichtende und freiwillige Sicherheitsüberprüfungen von externen Sicherheitsexperten zur Sicherstellung des Datenschutzniveaus
- Regelmäßige IT Sicherheitsschulungen der htp Mitarbeiter
- Verschlüsselter Zugang zum htp WebMail Service
- Verschlüsselter Zugang zum htp Mailserver mit Ihrem E-Mail-Programm
- Geforderte Mindestanforderungen an die Kennwortstärke
- Automatisch verschlüsselte Übertragung zwischen den Mailservern im Internet sofern der Mailserver des Kommunikationspartners eine Verschlüsselung unterstützt

Für weitere Fragen zum Thema Datenschutz und Datensicherheit stehen Ihnen unsere Mitarbeiter im ServiceCenter oder in einem htp Shop gerne zur Verfügung.

8 Information zu De-Mail

Das kostenpflichtige Cloud-Produkt „De-Mail“ basiert auf einer aktuellen initiative der Bundesregierung zur Einführung einer sicheren E-Mail-Kommunikation.
Eine „De-Mail“ soll in Zukunft den persönlich unterschriebenen Postbrief ersetzten. Ob dieses Ziel mit der aktuellen Version von De-Mail erreicht wird, ist derzeit noch strittig.
De-Mail hat im Vergleich zur einer echten Ende-zu-Ende Verschlüsselung aktuell noch gravierende Nachteile, wie z.B.:

- Keine Ende-zu-Ende Verschlüsselung durch die Anwender
- Provider hätten Zugriff auf die E-Mails
- Kostenpflichtig je E-Mail
- Derzeit noch geringe Durchdringung bei Ämtern und Behörden