Sichere E-Mail-Kommunikation mit SEH Computertechnik GmbH über GPG/PGP

Hintergrund und Ziel

Zum Schutz sensibler Informationen und zur sicheren Meldung von Sicherheitslücken können Sie verschlüsselte E-Mails an die SEH Computertechnik GmbH senden.
Dieser Artikel zeigt Ihnen, wie Sie mit PGP (Pretty Good Privacy) bzw. GPG (GNU Privacy Guard) verschlüsseln und sicher mit uns kommunizieren können.

Kontaktadresse für sicherheitsrelevante Hinweise: security@seh.de

Was ist GPG/PGP und warum nutzen wir es?

GPG und PGP sind bewährte Verfahren zur Verschlüsselung und Signatur von E-Mails. Sie basieren auf dem Prinzip der asymmetrischen Verschlüsselung:

- **Öffentlicher Schlüssel**: Wird von SEH bereitgestellt und dient zur Verschlüsselung Ihrer Nachricht.
- **Privater Schlüssel**: Bleibt ausschließlich bei SEH und wird zur Entschlüsselung verwendet.

Dieses Verfahren stellt sicher, dass ausschließlich autorisierte Empfänger bei SEH Ihre Nachricht lesen können. Darüber hinaus können Sie Ihre Nachricht digital signieren, um deren Authentizität nachzuweisen.

So kommunizieren Sie sicher mit SEH

- **Öffentlichen Schlüssel herunterladen**

  Laden Sie den öffentlichen Schlüssel der SEH Computertechnik GmbH von unserer Website herunter:
  https://www.seh-technology.com/de/service/sicherheit.html

- **Schlüssel importieren**

  Importieren Sie den öffentlichen Schlüssel in Ihre GPG/PGP-Anwendung.

- **Nachricht verfassen und verschlüsseln**

  Verfassen Sie Ihre Nachricht an security@seh.de und verschlüsseln Sie diese mit dem SEH-Schlüssel.

- **Nachricht senden**

  Senden Sie die verschlüsselte Nachricht per E-Mail an die oben genannte Adresse. Nur autorisierte Empfänger bei SEH können die Nachricht mithilfe des privaten Schlüssels entschlüsseln.

GPG/PGP installieren und verwenden

Um verschlüsselte E-Mails zu versenden, benötigen Sie eine kompatible GPG/PGP-Software:

- **Windows:** Gpg4win
- **macOS:** GPG Suite
- **Linux / andere Systeme:** GnuPG ist in den meisten Distributionen bereits enthalten.

1. **Eigene Schlüssel erzeugen**

   Erzeugen Sie ein eigenes Schlüsselpaar mit folgendem Befehl:

   ```
   gpg --full-generate-key
   ```

2. **Öffentlichen SEH-Schlüssel importieren**

   ```
   gpg --import SEH_Computertechnik_Product_Security-E4B0B3CD_public.asc
   ```

3. **Nachricht verschlüsseln und signieren**

   Verschlüsseln und signieren Sie Ihre Nachricht mit folgendem Befehl:

   ```
   gpg --encrypt --armor -r security@seh.de nachricht.txt
   ```

   Dies erzeugt eine ASCII-armierte Datei `nachricht.txt.asc`, die Sie als Anhang per E-Mail versenden können.

   > **Wichtig:** Bitte senden Sie bei der ersten Kontaktaufnahme auch Ihren **öffentlichen Schlüssel** mit, damit wir Ihnen ebenfalls verschlüsselt antworten können.