Websicherheit bei HTTP

- HTTP-Verbindungen sind ohne weitere Maßnahmen nicht verschlüsselt. Die übertragenen Daten können von unbefugten Personen mitgelesen oder manipuliert werden.
- Es gibt bei HTTP keine Möglichkeit festzustellen, ob der Server, auf dem die Webseite liegt, vertrauenswürdig ist.
- HTTP-Verbindungen sind durch die Kennung **http://** in der Adressleiste zu erkennen. Weiters fehlt bei solchen Verbindungen das Schloss-Symbol in der Browser-Statusleiste.

Vertrauliche Daten, wie z.B. Kreditkarten-Informationen, dürfen auf keinen Fall über eine unverschlüsselte Verbindung (http://...) gesendet werden.

Werden vertrauliche Daten trotzdem über eine unverschlüsselte Verbindung gesendet, besteht die Gefahr, dass Angreifer die Daten lesen oder manipulieren.

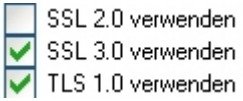
Websicherheit bei HTTPS

- HTTPS basiert auf anerkannten Sicherheitsprotokollen (SSL/TLS).
- HTTPS Verbindungen sind verschlüsselt.
- Bei HTTPS Verbindungen beweist der Server seine Authentizität mit Hilfe von Zertifikaten.
- Solche Verbindungen sind durch die Kennung **https://** in der Adressleiste und durch das Schloss-Symbol in der Browser-Statusleiste zu erkennen.

SSL (Secure Socket Layer) / TLS (Transport Layer Security)

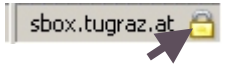
- HTTPS basiert auf SSL/TLS.
- SSL/TLS ermöglicht die Verschlüsselung von Webverbindungen und die eindeutige Identifizierung der Server auf denen die Webseiten zur Verfügung gestellt werden.
- Bei SSL sind die Versionen 2.0 und 3.0 im Einsatz. SSL 2.0 sollte aber nicht mehr verwendet werden, da es als unsicher gilt.

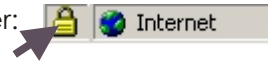
Deaktivieren Sie SSL 2.0!



Erkennen von sicheren Verbindungen

- Seiten, die mit HTTPS gesichert sind, werden durch das Schloss-Symbol in der Browser-Statusleiste erkennbar.

Mozilla/Firefox: 

Internet Explorer: 

- Bei Mozilla/Firefox werden durch Doppelklicken Details über die Verbindung angezeigt, insbesondere Verschlüsselung und Zertifikate.
- Bei Internet Explorer werden Details durch das Öffnen der Eigenschaften der Website (Menü Datei/Eigenschaften) angezeigt. Die Zertifikate erhalten Sie auch über Doppelklicken des Schloss-Symbols.

Serverzertifikate

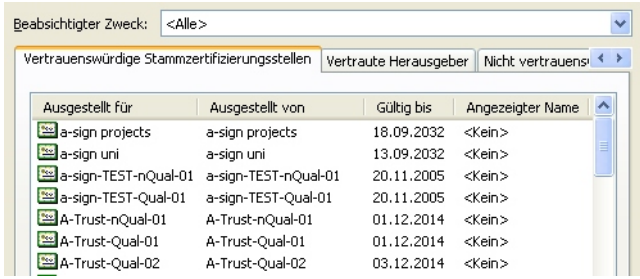
- Zertifikate geben über die Identität des Webservers Auskunft.
- Jeder Browser hat eine Liste von Zertifizierungsstellen, denen automatisch vertraut wird.
- Wird der Zertifizierungsstelle eines Serverzertifikats nicht automatisch vertraut, fragt der Browser den Benutzer, ob er das Zertifikat für die Verbindung akzeptiert.

Vorsicht im Umgang mit Vertrauen!

Stufen Sie nur jene Zertifikate als vertrauenswürdig ein, denen Sie auch wirklich vertrauen wollen.

- Bei Bedarf können Zertifizierungsstellen entfernt bzw. hinzugefügt werden:

  Menü Internetoptionen/Inhalt bei Internet Explorer bzw. Menü Extras/Einstellungen/Erweitert bei Mozilla.



Verhalten bei Verbindungen mit unbekannten/abgelaufenen Zertifikaten

- Bei Servern mit Zertifikaten von unbekannten Zertifizierungsstellen oder bei abgelaufenen Zertifikaten fragt der Browser den Benutzer, ob das Zertifikat akzeptiert werden soll.
- Zertifikate dürfen auf keinen Fall blind akzeptiert werden! Vor allem bei Behörden, Telebanking oder wenn Sie über das Internet einkaufen, sollten sie vorher prüfen, welche Zertifikate verwendet werden. Nur die Existenz einer SSL- oder TLS-Verbindung sagt noch nichts über deren Vertrauenswürdigkeit.

Bei bekannten Seiten aus dem Telebanking/Behörden/Online-Shop-Bereich ist sehr große Vorsicht angebracht, wenn der Webserver ein unbekanntes Zertifikat hat.

Verhalten bei PHISHING

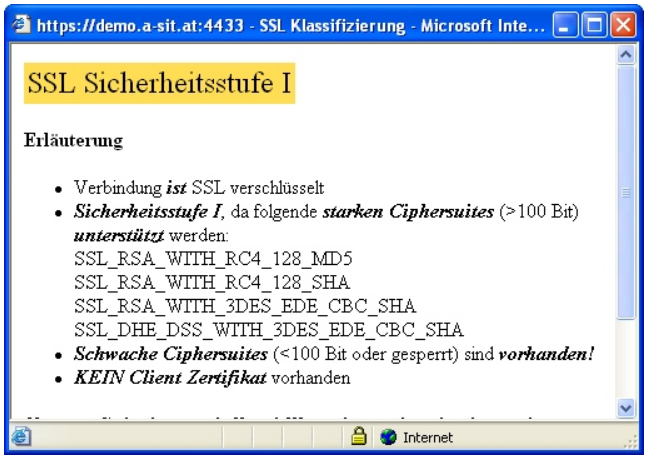
- Es wird zunehmend von Angriffen berichtet, bei denen Benutzer über E-Mail aufgefordert werden, auf täuschend echt wirkenden Webseiten von Kreditinstituten, Kreditkartenunternehmen, E-Commerce Seiten etc. Ihre Passworte einzugeben (so genanntes PHISHING).
- Kommen Sie derartigen Aufforderungen nie nach!

Geben Sie niemals Passworte oder TANs auf E-Mail- oder sonstige Aufforderung preis.

Kein seriöser Anbieter fordert per E-Mail Passworte an, auch nicht bei System-Problemen!

Tool zur Überprüfung von HTTPS-Servern und -Clients

- Sichere HTTPS-Verbindungen bedürfen entsprechend sicherer Verfahren und Schlüssellängen am Stand der Technik.
- Derzeit sind symmetrische Verfahren mit 100 Bit effektiver Schlüssellänge, bzw. Zertifikate mit 1024 Bit RSA oder DSA Schlüsseln oder 160 Bit ECC als sicher anzusehen.
- A-SIT bietet Ihnen ein Tool an, das Ihren Browser bzw. auch Webserver auf die unterstützten Verfahren überprüft:
  http://demo.a-sit.at/it_sicherheit/ssl_check



Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

Zentrum für sichere Informationstechnologie - Austria
A-SIT
Secure Information Technology Center - Austria

Sicherheit von Webservern

E-Government Flyer Nr.303

DIGITAL AUSTRIA

Sicherheit von Webservern
Schlüssellängen
Erkennbarkeit

- Sicherheit bei HTTP / HTTPS
- SSL/TLS
- Erkennen von sicheren Verbindungen
- Serverzertifikate
- PHISHING
- Schlüssellängen und Überprüfungstool