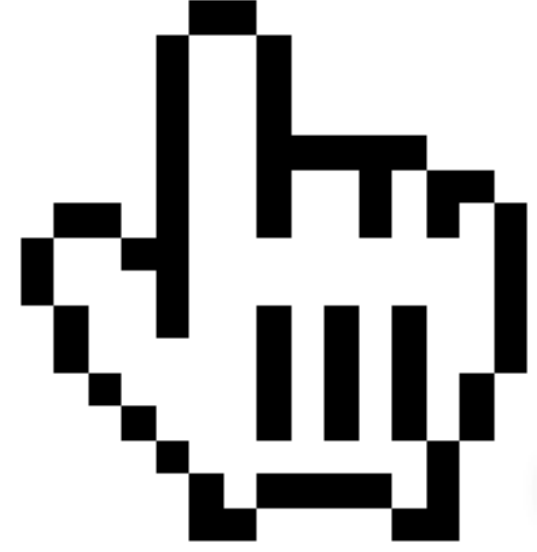


Kommunikation im Unternehmen

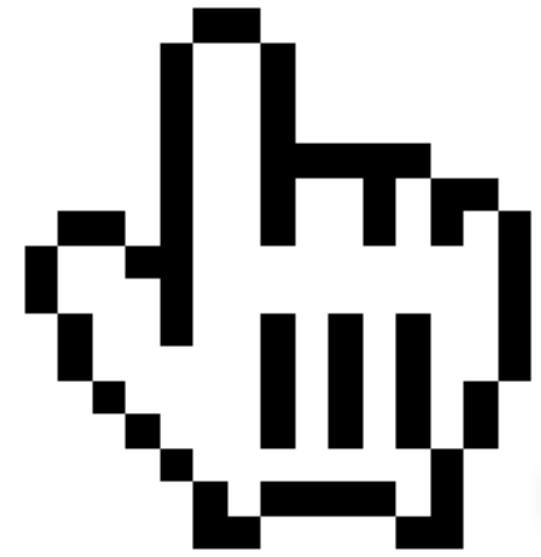






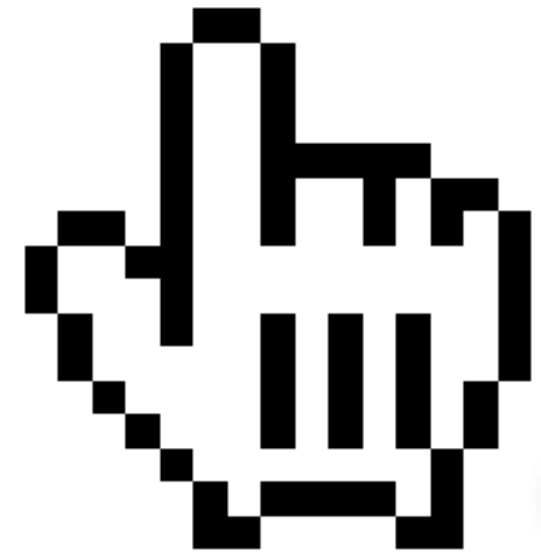
Vier Gruppen

Unternehmensleitung



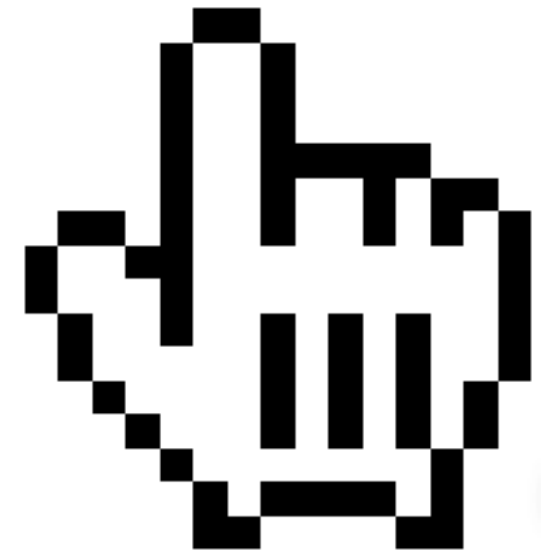
Unternehmensleitung

IT-Administration



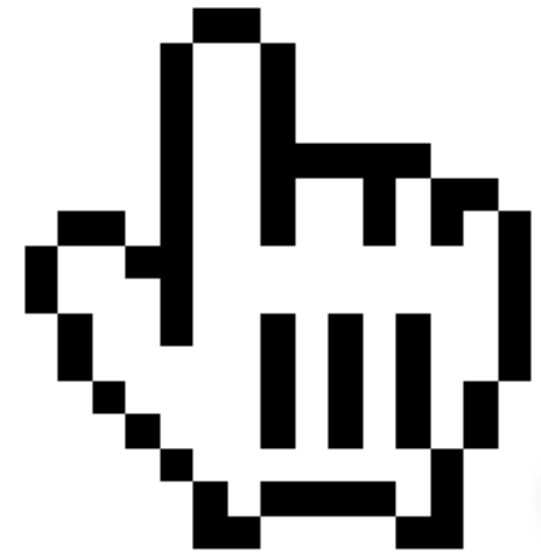
IT-Administration

Kunden



Kunden

BenutzerInnen



BenutzerInnen

Wer

Alle

Sicherheit ist ein Prozess

Alle



– Marc Coleman

Was passiert, wenn wir in die
Fortbildung unserer
MitarbeiterInnen investieren und sie
verlassen die Firma?

– Marc Coleman

**Was passiert wenn wir das nicht tun
und sie bleiben?**

– Marc Coleman

Alle

Gute Sicherheit ist benutzbar

Sicher



Sicher

Was bedeutet „sicher“?

Bedrohungsfrage?

Fehler in Software

Konkurrenz

Wirtschaftsspionage

Vorratsdatenspeicherung

Dezentrale Sicherungskopien

Zeit

Sicherer

Sicherer

Infrastruktur Lösungen

Altlasten loswerden

FAX

'43

1843

2014

~~FAX~~

Windows XP

~~Windows XP~~

Updates

Kommunikation

~~Klartext~~

~~Unverschlüsselt~~

Status Quo

Testen

Webserver

http://

https://

Webserver testen

<https://ssllabs.com/ssltest>

You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Domain name:

Do not show the results on the boards

Recently Seen

metronets.com	Err
slack.com	
owncloud.jonaskim.de	
wasserwacht-magdeburg.de	A-
pescaboutique.com	C
openmailbox.org	A
d2p-dev.novartis.com	Err
pop.openmailbox.org	A
client.investia.ca	F
smtp.openmailbox.org	A

Recent Best-Rated

londoners.ro	A+
openmailbox.org	A
pop.openmailbox.org	A
smtp.openmailbox.org	A
scottlinux.com	A-
sal.investpoint.automatedfin ...	A-
vlietlandziekenhuis.nl	B
votesmart.org	B
pescaboutique.com	C
office.com	C

Recent Worst-Rated

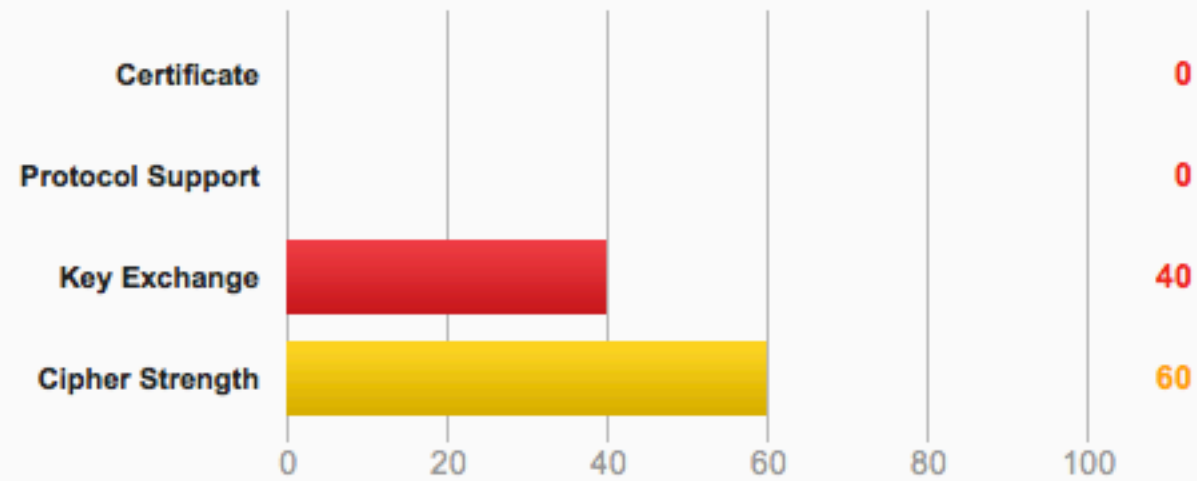
client.investia.ca	F
outlook.com	F
webmin.studiotwo.com	Trust
myhr.ahg.com.au	F
portal.lrgh.org	F
questful.com	F
poulp.net	Trust
mysql.triedtoswiminlava.net	Trust
my.sph.harvard.edu	F
api.2dehands.com	F

Summary

Overall Rating



If trust issues are ignored: F



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server's certificate is not trusted. Grade set to F.

This server supports SSL 2, which is obsolete and insecure. Grade set to F.

This server is vulnerable to MITM attacks because it supports [insecure renegotiation](#). Grade set to F.

This server does not mitigate the [CRIME attack](#). Grade capped to B.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

There is no support for secure renegotiation. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)



Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3	Yes
SSL 2 INSECURE	Yes



Cipher Suites (sorted by strength; the server has no preference)

SSL_CK_RC4_128_EXPORT40_WITH_MD5 (0x20080) INSECURE	40
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080) INSECURE	40
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) WEAK	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) WEAK	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) WEAK	40
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x14) DH 512 bits (p: 64, g: 1, Ys: 64) FS WEAK	40
SSL_CK_DES_64_CBC_WITH_MD5 (0x60040) INSECURE	56
TLS_RSA_WITH_DES_CBC_SHA (0x9) WEAK	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits (p: 128, g: 1, Ys: 128) FS WEAK	56
SSL_CK_RC4_128_WITH_MD5 (0x10080) INSECURE	128
SSL_CK_RC2_128_CBC_WITH_MD5 (0x30080) INSECURE	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
SSL_CK_DES_192_EDE3_CBC_WITH_MD5 (0x700c0) INSECURE	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) >

SSL Report:

Assessed on: Mon Feb 24 15:25:04 UTC 2014 | [Clear cache](#)

[Scan Another >>](#)

	Server	Domain(s)	Test time	Grade
1	Ready		Mon Feb 24 15:17:27 UTC 2014 Duration: 32.521 sec	F
2	Ready		Mon Feb 24 15:17:59 UTC 2014 Duration: 31.150 sec	F
3	Ready		Mon Feb 24 15:18:30 UTC 2014 Duration: 26.849 sec	F
4	Ready		Mon Feb 24 15:18:57 UTC 2014 Duration: 27.329 sec	F
5	Ready		Mon Feb 24 15:19:25 UTC 2014 Duration: 29.477 sec	F

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > wko.at

SSL Report: wko.at

Assessed on: Mon Feb 24 15:03:14 UTC 2014 | **HIDDEN** | [Clear cache](#)

[Scan Another >>](#)

	Server	Domain(s)	Test time	Grade
1	194.107.236.209 www.wko.at Ready	wko.at	Mon Feb 24 15:01:34 UTC 2014 Duration: 46.971 sec	B
2	194.107.236.210 Ready	www.wko.at	Mon Feb 24 15:02:21 UTC 2014 Duration: 52.849 sec	A-

Warning: Inconsistent server configuration

SSL Report v1.7.19

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [wko.at](#) > 194.107.236.210

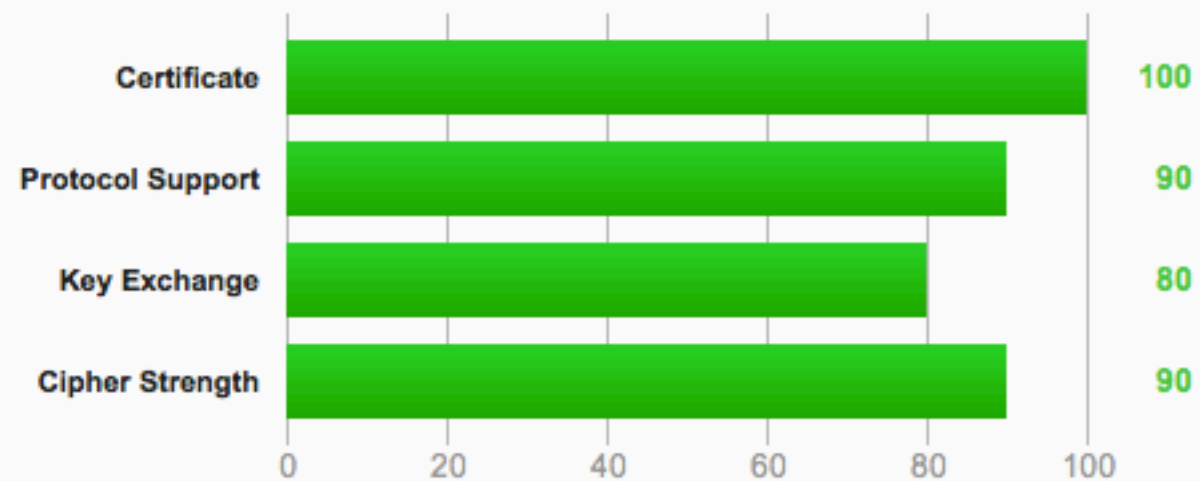
SSL Report: [wko.at](#) (194.107.236.210)

Assessed on: Mon Feb 24 15:03:14 UTC 2014 | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. [MORE INFO »](#)

Authentication

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > bettercrypto.org

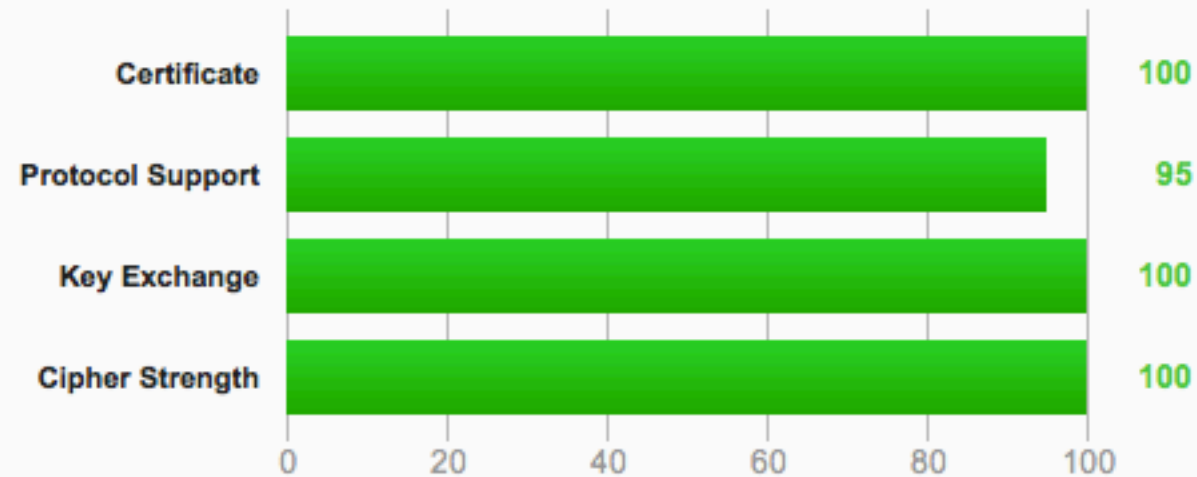
SSL Report: bettercrypto.org (78.41.116.68)

Assessed on: Mon Feb 24 15:13:26 UTC 2014 | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

Authentication

Email

<https://starttls.info/>

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the [blog](#).

Results for: **.gv.at**



Mail server	Result
mta3. .gv.at	STARTTLS not supported!
mta2. .gv.at	STARTTLS not supported!

Click the score for details.

[Check another!](#)

This site is a beta. | Read [about this](#). | Check the [stats](#).

Developed by [Einar Otto Stangvik](#).

Results for: .at



Mail server	Result
mail2. or.at	Error: The server rejected our check
mail1. .or.at	Grade: C (58.0%) ▼

Certificate

- The certificate is not valid for the server's hostname.
- There is a self-signed certificate in the trust chain. It may be a configuration problem.
- There are one or more fatal problems which causes the certificate not to be trusted.

There are validity issues for the certificate. Certificates are seldom verified for SMTP servers, so this doesn't mean that STARTTLS won't be used.

Generally speaking it's a bad practice not to have a valid certificate, and an even worse practice not to verify them. Any attempted encrypted communication is left all but wide open to Man-in-the-Middle attacks.

Protocol

- Supports TLSV1.

Key exchange

- Key size is 2048 bits; that's good.

Cipher

- Weakest accepted cipher: 40.
- Strongest accepted cipher: 56.

Click the score for details.

[Check another!](#)

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the [blog](#).

Results for: [ubermorgen.com](#)



Mail server

Result

ubermorgen.com

Grade: A (93.4%) ▼

Certificate

- No remarks.

Protocol

- Supports SSLV3.
- Supports TLSV1.
- Supports TLSV1.1.
- Supports TLSV1.2.

Key exchange

- Key size is 4096 bits; that's very good.

Cipher

- Weakest accepted cipher: 128.
- Strongest accepted cipher: 256.

Click the score for details.

[Check another!](#)



<https://starttls.info/stats>

Chat

<https://xmpp.net/>

[Score](#)[General](#)[DNS](#)[TLS](#)

IM Observatory client report for jabber.at

Test started 2014-02-24 15:25:47 UTC about an hour ago.

[Show server to server result](#) | [Permalink to this report](#)

Score

jabber.at:5222

Certificate score:



100

Key exchange score:



100

Protocol score:



90

Cipher score:



90

Grade:

A⁻

Warning: Server allows RC4 when using TLS 1.1 and/or TLS 1.2. Grade capped to A⁻.

General

jabber.at:5222

Version: ciphersuites 2.1.12



Handlungsbedarf



Technisches

Verschlüsselung als Standard

FTP

FTP

Unsicher seit 1971

Transportverschlüsselung

TLS 1.2

TLS 1.1

TLS 1.0

~~SSLv3~~

~~SSLv2~~

VPN

L2TP

IPSec

OpenVPN

PPTP

Festplatten Verschlüsselung

Passwörter

Zeichenvorrat ^{Länge}

Firewalls

Router

WiFi Access Points

Switches

IDS


Dokumentation


Emails

Postkarten

Verschlüsseln

GPG S/MIME

Sicherheit:  Signiert

Sicherheit:  Signiert



Verschlüsselt

security@beispiel.at
mit GPG Key

СЛУЖБА
ПРАВА



bettercrypto.org

Testseiten

https://ssllabs.com	Web
https://starttls.info	Mail
https://xmpp.net	Chat

Weitere Information

 <https://cryptoparty.at>

 <https://bettercrypto.org>

 <https://maclemmon.at>



Danke

