TLS-Check Ergebnisse (Zusammenfassung), Tests vom 22. Februar 2016

Name des Tests	Ergebnis	Prozent
Webserver		
Alle gültigen Domains	16383	100 %
Alle erreichbaren Webseiten	15010	91,619 %
Webseiten die prinzipiell Verschlüsselung können	6760	41,262 %
Webseiten ohne Browser-Warnung (Host und Zertifikat verifiziert)	1339	8,173 %
Von den Webseiten, die prinzipiell Verschlüsselung können	6760	100 %
Beachten alle BSI-Empfehlungen zu Protokoll-Version/kryptografische Verfahren	0	0 %
Webseiten ohne Browser-Warnung (Domain und Zertifikat verifiziert)	1339	8,173 %
… haben ein zum Domainname passendes Zertifikat	1339	8,173 %
… mit validem Zertifikat einer von den Browsern akzeptierten Zertifizierungsstelle	6760	41,262 %
… mit validem Zertifikat, aber falschem Host	5421	33,089 %
… mit Unterstützung für extrem unsicheres Protokoll SSL 2.0	394	5,828 %
… mit Unterstützung für sehr unsicheres Protokoll SSL 3.0	1483	21,938 %
… mit Unterstützung für sehr unsichere Protokolle SSL 2.0 oder SSL 3.0	1519	22,47 %
… mit Unterstützung für veraltetes Protokoll TLS 1.0	5887	87,086 %
… mit Unterstützung für TLS 1.1	4187	61,938 %
… mit Unterstützung für TLS 1.2	4117	60,902 %
… unterstützen nur das aktuelle Protokoll TLS 1.2 von 2008	5	0,074 %
… halten die BSI-Vorgaben fürs Protokoll ein (TLS 1.2, evtl. TLS 1.1)	13	0,192 %
… unterstützen nur TLS 1.0 oder älter	1691	25,015 %
… bieten sehr schwache kryptografische Verfahren an (z.B. Export, NULL,)	418	6,183 %
… bieten schwache kryptografische Verfahren an (z.B. RC4, 56 Bit, ...)	5011	74,127 %
… bieten mittelschwache kryptografische Verfahren an	890	13,166 %
… bieten keine schwachen/mittelschwachen kryptografischen Verfahren an	1748	25,858 %
… bieten nur empfohlene kompatible kryptografische Verfahren an (Bettercrypto B)	259	3,831 %
… halten die BSI-Vorgaben für kryptografische Verfahren ein	0	0 %
… bieten mindestens eines der vom BSI vorgegebenen kryptographischen Verfahren an	3804	56,272 %
… bieten nur empfohlene sehr sichere kryptografische Verfahren an (Bettercrypto A)	0	0 %
… nutzen (auch) ECDSA Keys	13	0,192 %
… bieten auch Cipher-Suiten mit PFS an	5414	80,089 %
… bieten nur Cipher-Suiten mit PFS an	1102	16,302 %
… Leiten von verschlüsselter auf unverschlüsselte Verbindung um (schlecht)	1341	19,837 %

Name des Tests	Ergebnis	Prozent
… Leiten von unverschlüsselter auf verschlüsselte Verbindung um (gut)	830	12,278 %
… nutzen die Sicherheitsfunktion Strict Transport Security	421	6,228 %
… nutzen die Sicherheitsfunktion Public Key Pinning	11	0,163 %
Von den Webseiten, die ein gültiges Zertifikat haben …	1339	100 %
… mit Unterstützung für extrem unsicheres Protokoll SSL 2.0	30	2,24 %
… mit Unterstützung für sehr unsicheres Protokoll SSL 3.0	206	15,385 %
… mit Unterstützung für sehr unsichere Protokolle SSL 2.0 oder SSL 3.0	206	15,385 %
… mit Unterstützung für veraltetes Protokoll TLS 1.0	1279	95,519 %
… mit Unterstützung für TLS 1.1	975	72,816 %
… mit Unterstützung für TLS 1.2	954	71,247 %
… unterstützen nur das aktuelle Protokoll TLS 1.2 von 2008	2	0,149 %
… halten die BSI-Vorgaben fürs Protokoll ein (TLS 1.2, evtl. TLS 1.1)	4	0,299 %
… unterstützen nur TLS 1.0 oder älter	297	22,181 %
… bieten sehr schwache kryptografische Verfahren an (z.B. Export, NULL,)	39	2,913 %
… bieten schwache kryptografische Verfahren an (z.B. RC4, 56 Bit, ...)	1020	76,176 %
… bieten mittelschwache kryptografische Verfahren an	203	15,161 %
… bieten keine schwachen/mittelschwachen kryptografischen Verfahren an	318	23,749 %
… bieten nur empfohlene kompatible kryptografische Verfahren an (Bettercrypto B)	64	4,78 %
… halten die BSI-Vorgaben für kryptografische Verfahren ein	0	0 %
… bieten mindestens eines der vom BSI vorgegebenen kryptographischen Verfahren an	831	62,061 %
… bieten nur empfohlene sehr sichere kryptografische Verfahren an (Bettercrypto A)	0	0 %
… nutzen (auch) ECDSA Keys	13	0,971 %
… bieten auch Cipher-Suiten mit PFS an	1166	87,08 %
… bieten nur Cipher-Suiten mit PFS an	122	9,111 %
Webserver, die für die Heartbleed-Attacke anfällig sind	8	
Durchschnittlicher Score der Verschlüsselung unterstützenden Seiten	181,956	
Durchschnittlicher Score der Webseiten mit verifiziertem Zertifikat/Domain	207,151	
Gesamt-Score nach Einbeziehung aller Ergebnisse	68,16	
Mailserver (MX)		
Alle getesteten Mailserver	9363	100 %
Alle erreichbaren Mailserver	8829	94,297 %
Mailserver, die prinzipiell Verschlüsselung können	7397	79,002 %

Name des Tests	Ergebnis	Prozent
Von den Mailservern, die prinzipiell Verschlüsselung können	7397	100 %
… haben ein gültiges und zum Domainname passendes Zertifikat	2474	33,446 %
… mit Unterstützung für extrem unsicheres Protokoll SSL 2.0	1198	16,196 %
… mit Unterstützung für sehr unsicheres Protokoll SSL 3.0	3965	53,603 %
… mit Unterstützung für sehr unsichere Protokolle SSL 2.0 oder SSL 3.0	3978	53,779 %
… mit Unterstützung für veraltetes Protokoll TLS 1.0	7233	97,783 %
… mit Unterstützung für TLS 1.1	5188	70,137 %
… mit Unterstützung für TLS 1.2	5288	71,488 %
… unterstützen nur das aktuelle Protokoll TLS 1.2 von 2008	60	0,811 %
… halten die BSI-Vorgaben fürs Protokoll ein (TLS 1.2, evtl. TLS 1.1)	70	0,946 %
… unterstützen nur TLS 1.0 oder älter	1970	26,632 %
… bieten sehr schwache kryptografische Verfahren an (z.B. Export, NULL,)	2232	30,174 %
… bieten schwache kryptografische Verfahren an (z.B. RC4, 56 Bit, ...)	6022	81,411 %
… bieten mittelschwache kryptografische Verfahren an	3467	46,87 %
… bieten keine schwachen/mittelschwachen kryptografischen Verfahren an	1355	18,318 %
… bieten nur empfohlene kompatible kryptografische Verfahren an (Bettercrypto B)	76	1,027 %
… halten die BSI-Vorgaben für kryptografische Verfahren ein	0	0 %
… bieten mindestens eines der vom BSI vorgegebenen kryptographischen Verfahren an	4908	66,351 %
… bieten nur empfohlene sehr sichere kryptografische Verfahren an (Bettercrypto A)	0	0 %
… nutzen (auch) ECDSA Keys	3	0,041 %
… bieten auch Cipher-Suiten mit PFS an	7039	95,16 %
… bieten nur Cipher-Suiten mit PFS an	27	0,365 %
… könnten verschlüsselt mit„nur Bettercrypto B“-Server kommunizieren	7312	98,851 %
Mailserver, die für die Heartbleed-Attacke anfällig sind	14	
Durchschnittlicher Score der Verschlüsselung unterstützenden Mailserver	194,365	