.gv.at E-Mail Sicherheitsanalyse

EGIZ E-Government Innovationszentrum

The E-Government Innovation Center is a joint initiative of the Federal Chancellery and Graz University of Technology

TU Graz

BUNDESKANZLERAMT ÖSTERREICH

Arne Tauber, EGIZ

28. September 2016

Ermitteln der .gv.at Mail-Hosts

- Rund 1200 Subdomains in .gv.at Domain registriert
- Auslesen MX Records via DNS Lookup
- → Ergebnis: Knapp 550 eindeutige Mailserver
- Liste bildet Basis für folgende Analysen
  - Offene Ports (unterstützte Protokolle)
  - SSL/TLS Versionen
  - Digitale Zertifikate
  - Anfälligkeit auf bekannte Schwachstellen
  - Veraltete Software

Offene Ports

- Offene Ports ermitteln

Protokoll	Port	Verwendung
POP3	110	Transfer von Emails von einem Server auf einen lokalen Rechner.
POP3s	995	Verschlüsselte Variante von POP3. (SSL)
IMAP	143	Zugriff auf Email auf einem Server von mehreren lokalen Rechnern.
IMAPs	993	Verschlüsselte Variante von IMAP. (SSL)
SMTP	25	Unverschlüsseltes Senden von Emails.
SMTPs	465	Verschlüsseltes Senden von Emails. (SSL)
SMTPs	587	Verschlüsseltes Senden von Emails. (STARTTLS)

  - Auch http(s)-Ports für z.B. Web-Zugriff auf Mailbox (80,8080,8443,…)
  - Klassifikation anhand offener Ports in MTAs (nur SMTP Ports offen) und MDAs

SSL/TLS Versionen

- Verschlüsselte Kommunikation zwischen Teilnehmern
  - MTA – MTA, MUA – MDA, MTA – MDA
- Basiert auf Public Key Kryptographie
- Version wird während des Handshakes ausgehandelt
- Veröffentlichungstermine:
  - SSLv2 – 1994
  - SSLv3 – 1995
  - TLS 1.0 – 1999
  - TLS 1.1 – 2006
  - TLS 1.2 - 2008

Cipher-Suites

- Ciphersuite definiert folgende Parameter
  - Verfahren für Schlüsselaustausch zwischen Client und Server
  - Verfahren für Serverauthentifizierung
  - Verschlüsselung von Nutzdaten
  - Verfahren für die Sicherstellung der Datenintegrität
- Nur aktuellste SSL-Versionen unterstützen aktuellste Ciphersuites!
- Z.B: TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384

Beispiel	Erklärung
ECDH	Verfahren für den Schlüsselaustausch. Diffie Hellman basierend auf elliptischen Kurven
ECDSA	Verfahren für die Authentifizierung des Servers. Digital Signature Algorithmus basierend auf elliptischen Kurven
AES_256_GCM	Verschlüsselung von Nutzdaten. Hier AES (Keylänge 256bit) im GCM Verfahren
SHA384	Verfahren zur Sicherstellung der Datenintegrität; Hashalgorithmus SHA384

Digitale Zertifikate

- Serverzertifikat wird beim SSL Handshake an Client gesandt
- Dient zur
  - Identifizierung/Authentifizierung des Servers
  - Verschlüsselung der Kommunikation
- Test überprüft
  - Hashalgorithmus (Verwendung von aktuellen Algorithmen, wie SHA-256)
  - Schlüssellänge
  - Vergleich Domainname im Zertifikat mit Serverdomain
  - Gültigkeitszeitraum
  - Verwendung von selbstsignierten Zertifikaten (OK bei MTAs)

Bekannte Schwachstellen

- Heartbleed
  - Nutzt Bufferüberlauf aus durch nicht verifiziertes Längenfeld aus
  - Bestimmte OpenSSL Versionen sind betroffen
  - Ermöglicht Auslesen von Benutzerdaten und privaten Schlüsseln
- Poodle
  - Man-in-the-Middle Attacke
  - SSL V3.0 ist anfällig auf diese Attacke
- Freak
  - Downgrade-Attacke
  - Anfällig wenn RSA_EXPORT Keys unterstützt werden
    - Schlüssel mit 512bit werden verwendet → brechbar in wenigen Stunden

Bekannte Schwachstellen

- Logjam
  - Downgrade-Attacke mittel Man-in-the-Middle Angriff
  - Betroffen sind Ciphersuites die Diffie Hellman für den Schlüsselaustausch verwenden, nicht jedoch jene die auf elliptischen Kurven basieren
  - Problem: weit verbreitete Standard Primzahlen und EXPORT Suites
    - Meisten Server verwenden nur 2 verschiedene Primzahlen
    - Dank Vorberechung können Verschlüsselungen in unter 2 Minuten gebrochen werden

WeitereTests

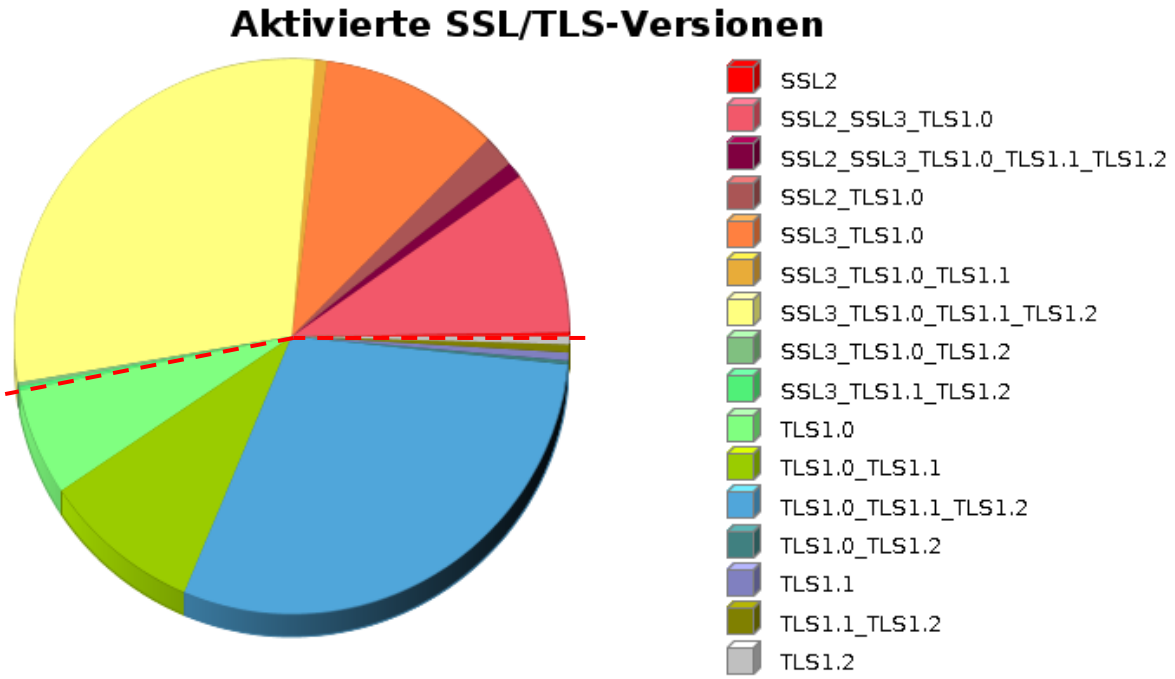
- Open Mail Relay
  - Über den Mailserver können beliebige Emails von beliebigen Absendern versandt werden
- Serversoftwareermittlung
  - Tool : nmap
  - Basiert auf Fingerprint des OS und Banner bei bestimmten Anfragen

Eckdaten

- 500 Mailserverdomains aus den MX Records ermittelt
  - 40% wurden anhand der offenen Ports als MDAs klassifiziert
  - 60% wurden als MTAs klassifiziert (nur SMTP Ports erreichbar)
- Zeitraum der Überprüfung: 1. bis 8. August 2016
  - Vorjahres-Überprüfung: 4. bis 12. Mai 2015
- Tools
  - nmap
  - testssl.sh
  - custom scripts
- Einzelergebnisse auf Nachfrage unter help@egiz.gv.at

TLS/SSL Versionen

- Knapp 400 Mailserver wurden getestet
- Problematisch:
  - SSLv2 : ca. 10%
  - SSLv3 : ca. 50%



Ciphersuites

- Top Ciphersuites
- Problematisch
  - SHA oder MD5
    - ersetzen mit SHA256
  - Anon, 3DES oder RC4
    - nicht mehr verwenden

Legende

Rot: Problematisch

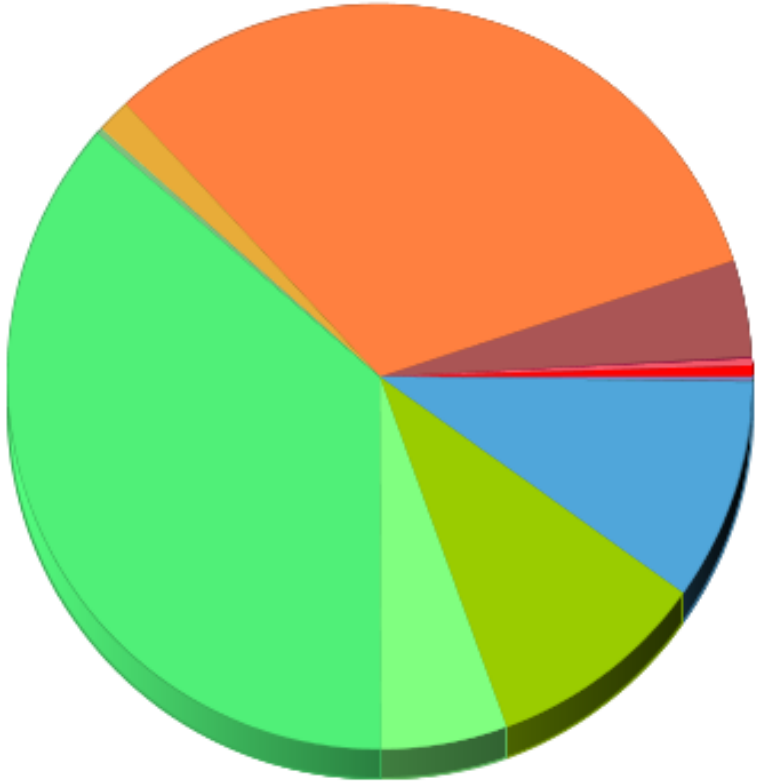
Blau: keine PF-Secrecy

Gelb: Logjam-Anfälligkeit

Grün: Sicherer Betrieb

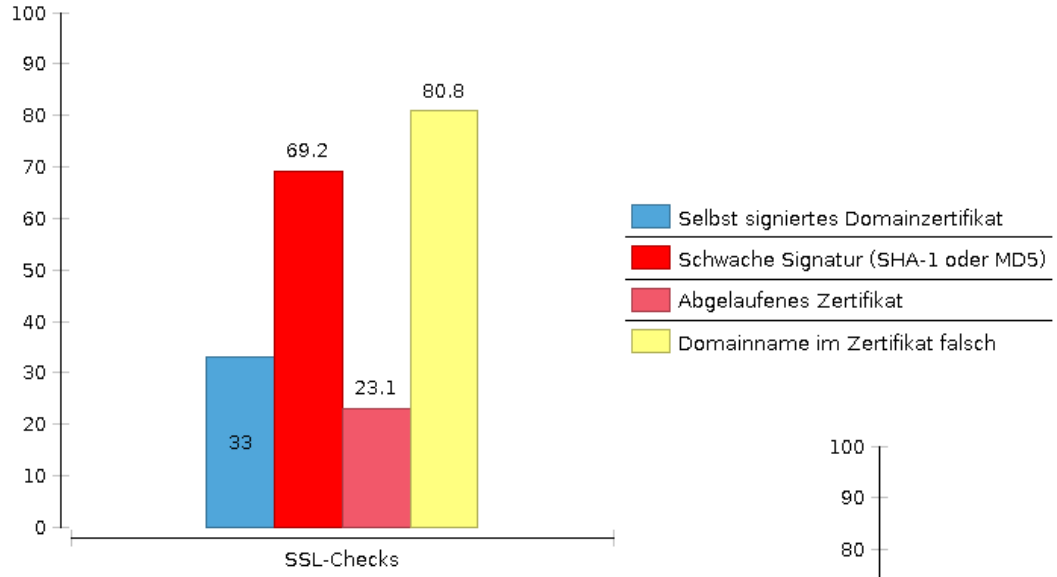
Ciphersuite	# Server [%]
TLS_RSA_WITH_AES_256_CBC_SHA	92,1
TLS_RSA_WITH_AES_128_CBC_SHA	89,6
SSL_RSA_WITH_3DES_EDE_CBC_SHA	88,2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	68,0
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	66,8
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	65,9
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	64,5
SSL_RSA_WITH_RC4_128_SHA	61,7
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	59,9
SSL_RSA_WITH_RC4_128_MD5	59,2
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	52,0
TLS_RSA_WITH_AES_256_CBC_SHA256	51,3
TLS_RSA_WITH_AES_128_CBC_SHA256	50,8
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	50,8
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	50,6
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	50,3
TLS_RSA_WITH_AES_256_GCM_SHA384	50,3
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	49,7
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	49,2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	49,0
TLS_RSA_WITH_AES_128_GCM_SHA256	49,0
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	48,7
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	43,6
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	42,2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	39,9

Digitale Zertifikate – Signaturalgorithmen

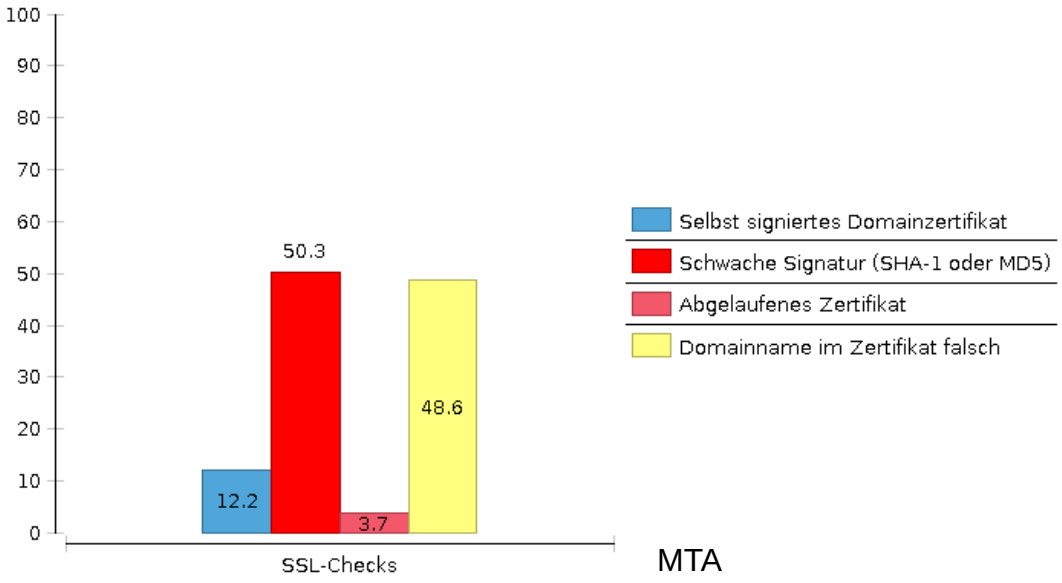


Keysize sollte mindestens 2048 Bit sein!

Digitale Zertifikate



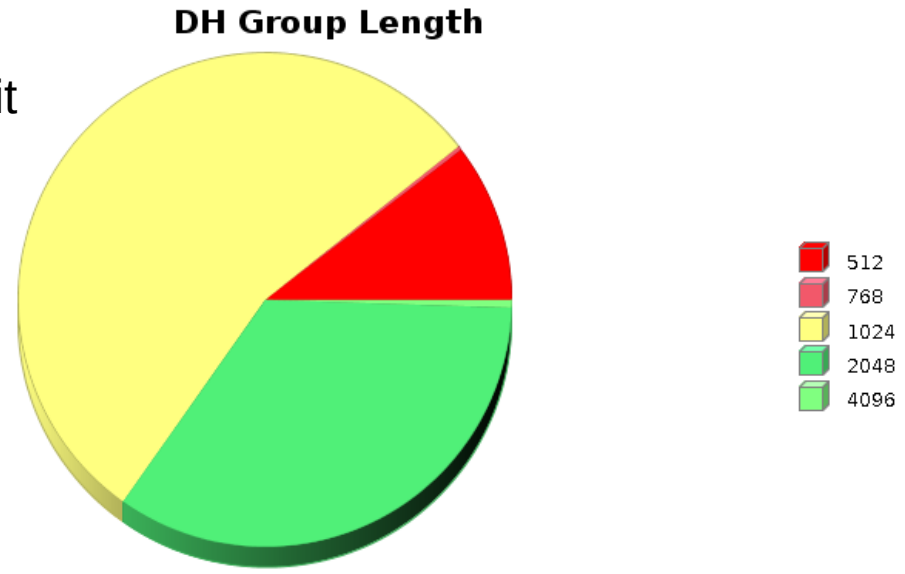
MDA



MTA

Schwachstellen / Attacken

- Freakattacke
  - EXPORT Ciphersuites aktiv
  - 45 der getesteten Server sind anfällig
- Logjam
  - DH Gruppengröße < 1024bit
  - Ca. 10% der Server sind anfällig für Logjam



Schwachstellen / Attacken (2)

- Heartbleed
  - Nur ein Server zeigte Auffälligkeit bei Tests, Attacke war jedoch nicht erfolgreich.
- Poodle
  - Prinzipiell sind alle Server die SSL V3 unterstützen gefährdet. Die automatisierten Tests waren bei 3 Servern erfolgreich.
- Openrelay (SPAM Versand)
  - Kein Server konnte als Openrelay verwendet werden
- Teilweise veraltete Software mit kritischen CVEs
- Entsprechende Stellen wurden verständigt.

Vergleich zu 2015

- Direkter Vergleich schwierig
  - Einige Domains wurden deaktiviert
  - Neue kamen hinzu
  - Von einigen Betreibern wurde kein erneuter Check gewünscht
- Trotzdem kurze Zusammenfassung:
  - SSL V3: Reduktion von 80% auf 50%
  - SSL V2: Halbierung auf rund 13%
  - Zertifikate Signaturalgorithmen SHA1 oder MD5
    - Bei MDAs 75% und bei MTAs 56% der Server

Vergleich zu 2015

- Schwachstellen
  - Heartbleed: Reduktion von 3 auf nur mehr einen Server
  - Poodle: Reduktion von 15 auf 3 Server
    - Prinzipiell sind jedoch alle Server die SSL V3 anbieten gefährdet
  - Freak: Reduktion von 74 auf 45 Server

Mailserver Empfehlungen

- Generelle Architektur
  - Trennung MTA und MDA innerhalb einer Domain
  - Nur MTA von außen erreichbar, restliche Ports geschlossen
    - Kommunikation mit anderen MTAs (SMTPs)
  - MDA nur von internen Mailclients erreichbar
  - Wenn möglich auf SSL/TLS setzen
  - Starke Authentifizierungsmechanismen für (Web-)Mail Clients
    - Z.B. SSL/TLS Clientauthentifizierung
    - Zugriffe nur von internem Netzwerk
    - VPN Zugänge verwenden

Empfehlungen

- Ciphersuites
  - SSLv2 und SSLv3 sollten deaktiviert werden
  - TLS 1.0 und 1.1 nur als Fallback verwenden
  - Idealerweise nur TLS 1.2
    - Bei DHE auf Gruppengröße achten
    - ECDHE für Perfect Forward Secrecy
    - SHA256, SHA384, …
- Softwareversionen
  - Updatemanagement
  - Zyklischer bzw. automatisierter CVE Datenbank Check

Empfehlungen (2)

- Zertifikate
  - Für MTAs
    - Zur Zeit selten Zertifikatsvalidierung zwischen MTAs
    - Selbstsignierte Zertifikate daher quasi Standard
    - Pushen von DNSSEC / DANE
  - Für MDAs
    - Zertifikate von vertrauenswürdigen CAs
      - Garantiert korrekte Validierung in Clientapplikationen bei Verwendung von TLS
  - Hashalgorithmus zumindest SHA256
  - RSA Schlüssellänge zumindest 2048 besser 4096 Bit

Empfehlungen (3)

- Tools
  - SSLLABS
    - https://www.ssllabs.com/ssltest/analyze.html
  - SSLTOOLS
    - https://ssl-tools.net/mailservers
  - BCRYPTO
    - https://bettercrypto.org

Vielen Dank für die Aufmerksamkeit

EGIZ E-Government Innovationszentrum

The E-Government Innovation Center is a joint initiative of the Federal Chancellery and Graz University of Technology

TU Graz

BUNDESKANZLERAMT ÖSTERREICH

Arne Tauber, EGIZ

28. September 2016