Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

CISO Sprechstunde

02.05.2023

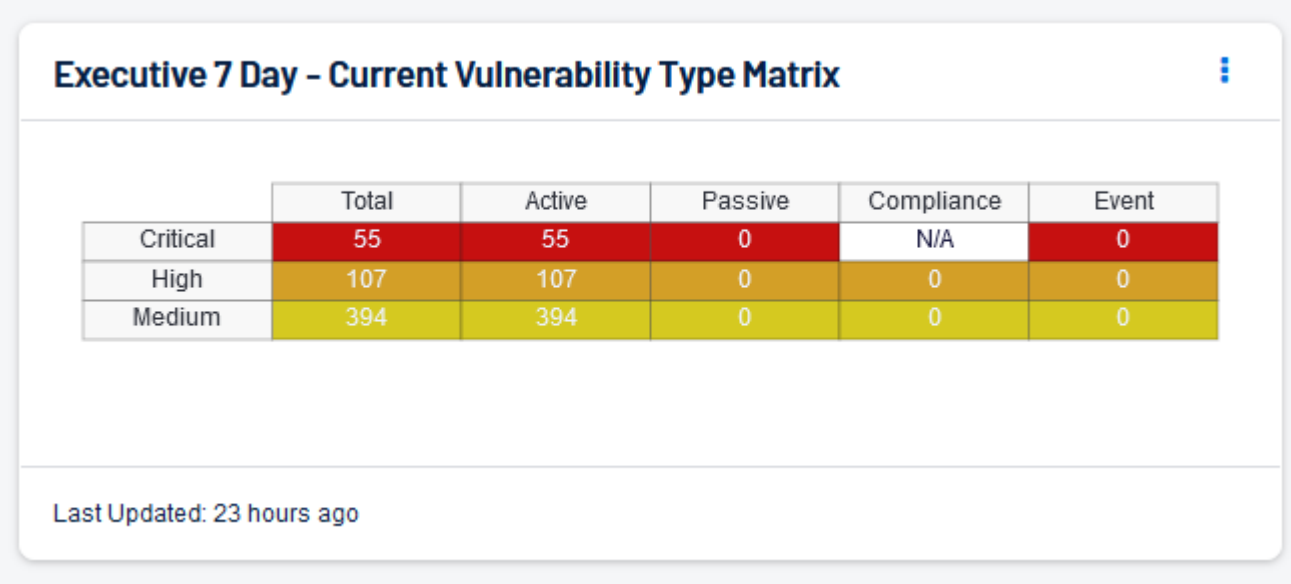
Agenda

Ihre Themen?

Schwachstellen und Internetsysteme

Netzanbindung

Dashboard



Executive 7 Day – Current Vulnerability Type Matrix

	Total	Active	Passive	Compliance	Event
Critical	55	55	0	N/A	0
High	107	107	0	0	0
Medium	394	394	0	0	0

Last Updated: 23 hours ago

Dashboard

Executive 7 Day - Current Asset Vulnerability Breakdown

10 Item(s) | 1 to 10 of 10 | Page 1 of 1

Asset	Medium	High	Critical
Systems that have been Scanned	394	107	55
SSL or TLS Servers	374	106	51
Assets FAU all IPv4	348	96	46
Linux Hosts	320	87	37
Windows Hosts	19	6	3
Exploited by Malware	25	39	3
Systems Discovered Passively	0	0	0
Voice or Mobile Client Devices	0	0	0
Device Type VPN	0	0	0

Last Updated: 23 hours ago

View Data >

Schwachstellen

Solution	Risk Reduction	Hosts Affected	Vulnerabilities
Upgrade to Apache version 2.4.56 or later.	36.03%	39	266
Upgrade to GitLab version 15.8.5, 15.9.4, 15.10.1 or later.	10.49%	6	423
Fix SSL Certificate Cannot Be Trusted	8.75%	483	626
Upgrade to Apache Tomcat version 8.5.86 or later.	7.37%	12	172
Fix TLS Version 1.1 Protocol Deprecated	3.73%	221	267
Fix TLS Version 1.0 Protocol Detection	3.61%	217	258
Fix SSL Self-Signed Certificate	2.64%	156	189
Fix HSTS Missing From HTTPS Server (RFC 6797)	2.36%	158	169
Fix Unix Operating System Unsupported Version Detection	1.86%	10	10
Fix SMB Signing not required	1.72%	123	123
Upgrade to OpenSSL version 1.0.2zh or later.	1.65%	3	21
Upgrade to nginx 1.22.1 or 1.23.2 or later.	0.99%	42	71
Fix PHP Unsupported Version Detection	0.93%	5	5
Upgrade CodeMeter Runtime to version 7.21a or later.	0.75%	4	4
Fix VMware ESX / ESXi Unsupported Version Detection	0.75%	4	4
Upgrade to PHP version 8.2.3 or later.	0.73%	6	11
Contact the Certificate Authority to have the SSL certificate reissued.	0.70%	12	15
Upgrade to the relevant fixed version referenced in Cisco bug ID CSCwc47201	0.62%	3	18

Uralte SW-Stände bringen uns alle in Gefahr!

cpe:/o:debian:debian_linux:7.0
cpe:/o:linux:linux_kernel
cpe:/o:canonical:ubuntu_linux:12.04
cpe:/o:canonical:ubuntu_linux:12.04
cpe:/o:debian:debian_linux:7.0
cpe:/o:debian:debian_linux:7.0
cpe:/o:debian:debian_linux:8.0
cpe:/o:canonical:ubuntu_linux:12.04
cpe:/o:sun:sunos:9

SSL und TLS: Eine kurze Einführung

Sowohl SSL (Secure Socket Layer) als auch TLS (Transport Layer Security) sind kryptografische Protokolle, die Ihre Daten verschlüsseln, sodass diese sicher im Internet übertragen werden.

Bei SSL handelt es sich um den Vorgänger von TLS und entspricht nicht mehr dem aktuellen Stand der Technik.

SSL 1.0: Aufgrund von Sicherheitsproblemen nie öffentlich freigegeben.

SSL 2.0: Veröffentlicht 1995. Seit 2011 veraltet.

SSL 3.0: Veröffentlicht 1996. Seit 2015 veraltet.

TLS 1.0: 1999 als Upgrade auf SSL 3.0 veröffentlicht. Seit 2020 veraltet.

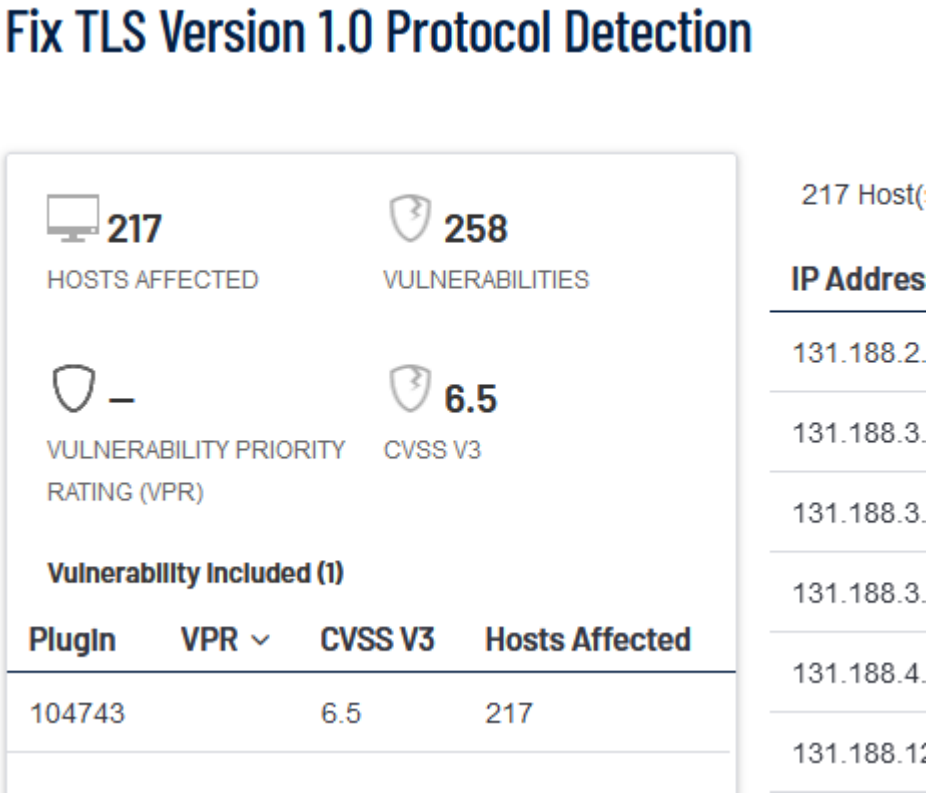
TLS 1.1: Veröffentlicht 2006. Seit 2020 veraltet.

TLS 1.2: Veröffentlicht 2008.

TLS 1.3: Veröffentlicht 2018.

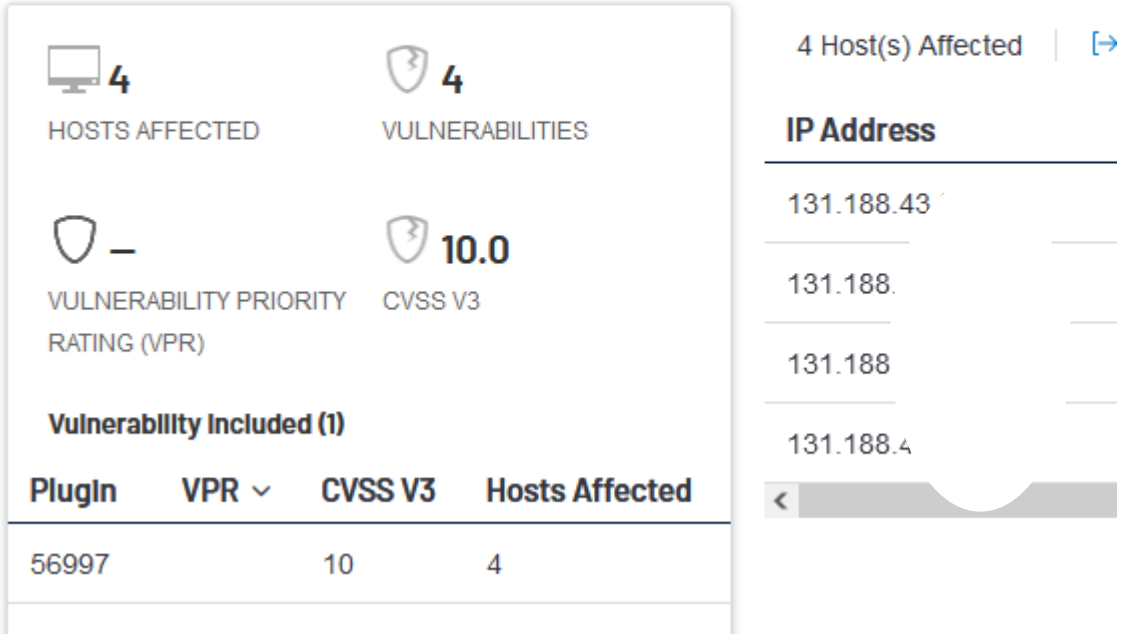
- Bitte nur TLS in der Version TLS 1.2 und/oder TLS 1.3 einsetzen.
- Andere TLS-Versionen bitte deaktiviert.

Uralte SW- und Protokollstände bringen uns alle in Gefahr!



Schwachstellen

Fix VMware ESX / ESXi Unsupported Version Detection



4 HOSTS AFFECTED

4 VULNERABILITIES

– VULNERABILITY PRIORITY RATING (VPR)

10.0 CVSS V3

Vulnerability Included (1)

Plugin	VPR	CVSS V3	Hosts Affected
56997		10	4

4 Host(s) Affected

IP Address
131.188.43
131.188.
131.188
131.188.4

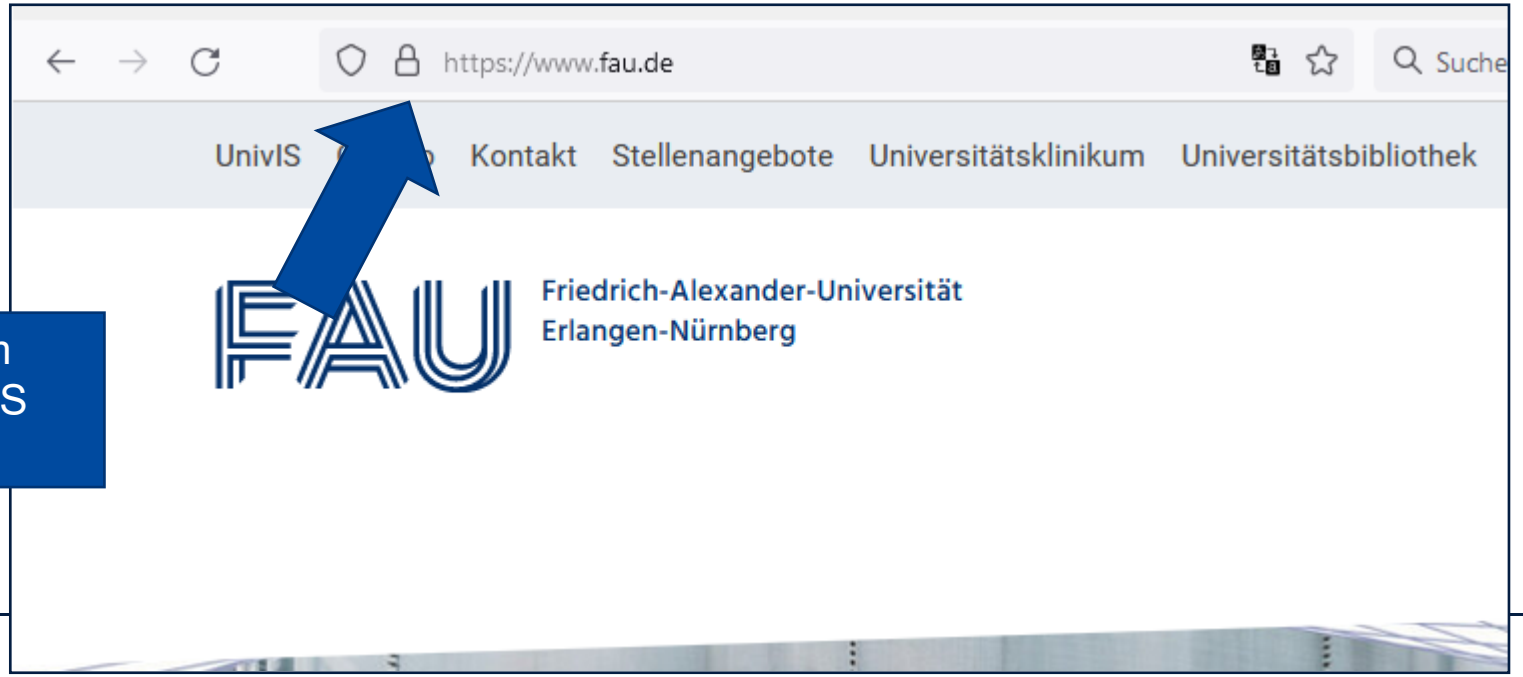
Bitte beachten:

- **Virtualisierungsplattformen** bitte immer im internen Netzwert oder in einer DMZ installieren!
- **Adminzugänge** ebenfalls nur intern einrichten oder extern mit 2. Faktor versehen!

Unterschied zwischen SSL und TLS

- Wenn Sie eine Verbindung zwischen einem Client (z.B. einem Browser wie Firefox) und einem Server (z.B. fau.de) via TLS oder SSL aufbauen, dann erkennen Sie an einem kleinen Schloss-Symbol, dass Sie eine verschlüsselte Verbindung zur Website aufgebaut haben.
- Dieser Prozess dazu wird auch als Handshake bezeichnet.
- Weitere Informationen zur Authentifizierung (wie z.B. der eindeutige Fingerabdruck oder die Identität des Webseitenbetreibers) befinden sich im Zertifikat.
- SSL und TLS sind Protokolle

d.h. die Verbindung zwischen dem Browser und fau.de wurde via TLS verschlüsselt.

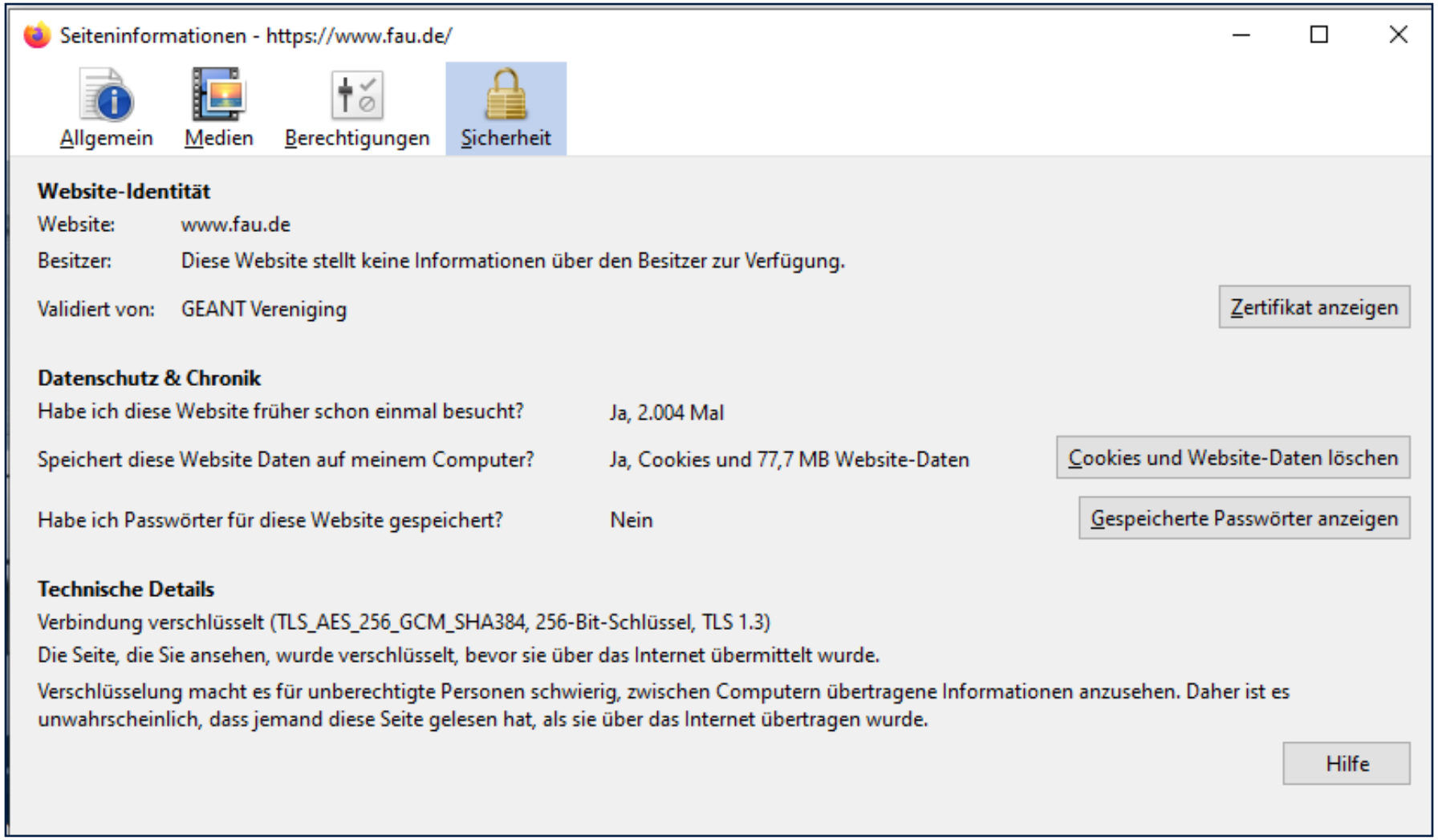


Unterschied zwischen SSL und TLS

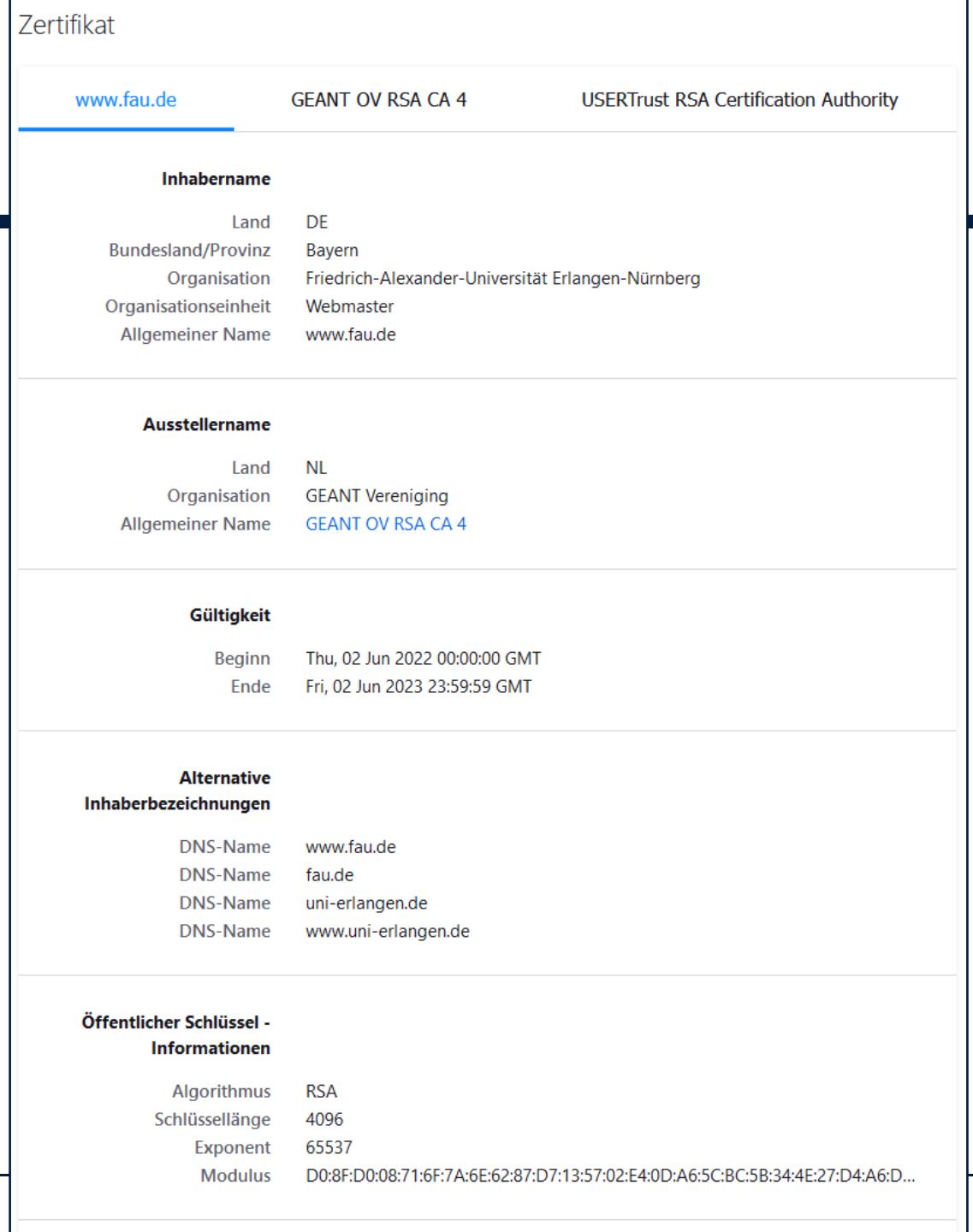
Ein Unterschied der Protokolle ist u.a. **die Art des Schlüsselaustausches.**

- TLS verwendet den *Digital Signature Standard* und den *Ephemeral Diffie-Hellmann Algorithmus* kombiniert mit RSA, was einen besseren Schutz gegen späteres Entschlüsseln bietet.
- SSL verwendet einen älteren Verschlüsselungsalgorithmus (*Message Authentication Code* (MAC), der bereits durch Angriffe entschlüsselt werden konnte.

Weitere Informationen



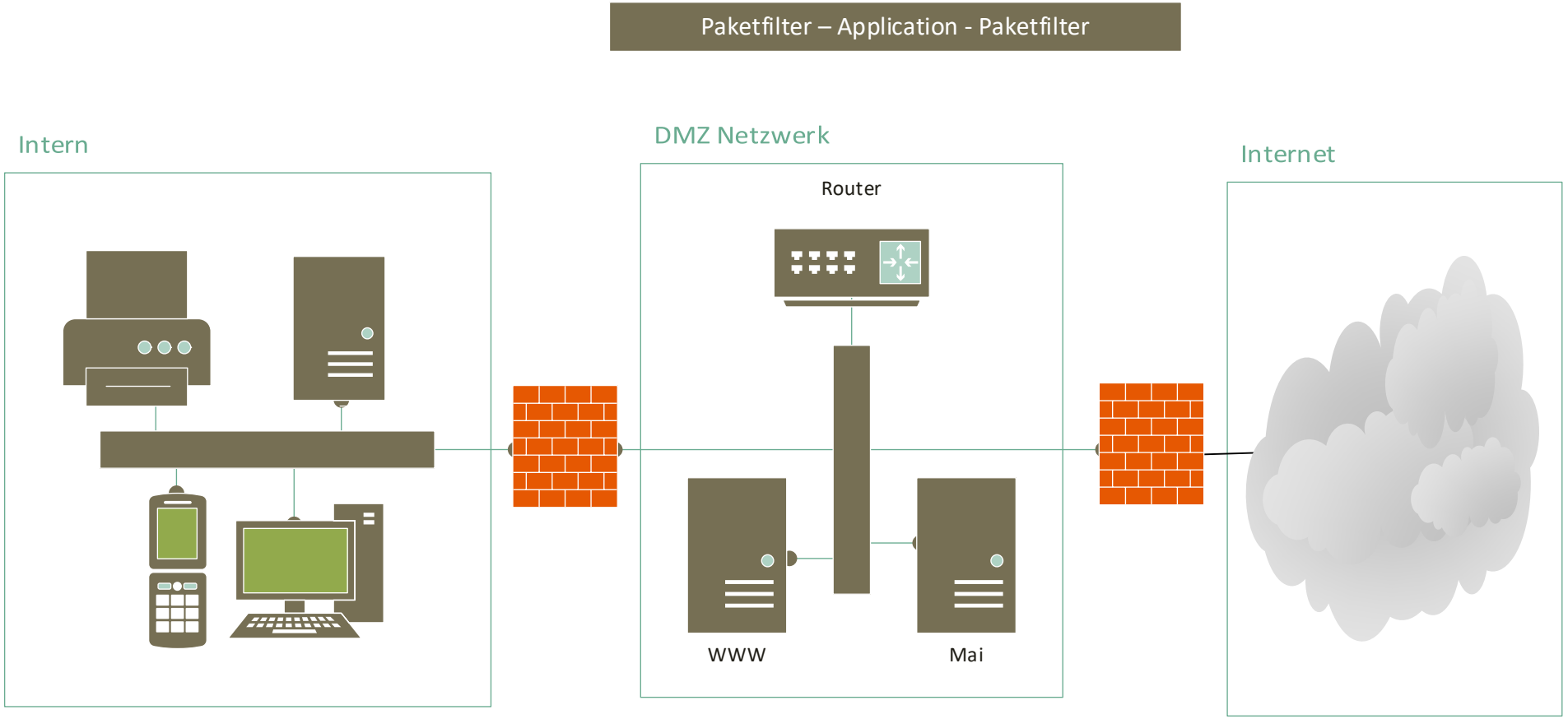
Zertifikat


Zertifikat
www.fau.de
GEANT OV RSA CA 4
USERTrust RSA Certification Authority
Inhabername
Land DE
Bundesland/Provinz Bayern
Organisation Friedrich-Alexander-Universität Erlangen-Nürnberg
Organisationseinheit Webmaster
Allgemeiner Name www.fau.de
Ausstellername
Land NL
Organisation GEANT Vereniging
Allgemeiner Name GEANT OV RSA CA 4
Gültigkeit
Beginn Thu, 02 Jun 2022 00:00:00 GMT
Ende Fri, 02 Jun 2023 23:59:59 GMT
Alternative Inhaberbezeichnungen
DNS-Name www.fau.de
DNS-Name fau.de
DNS-Name uni-erlangen.de
DNS-Name www.uni-erlangen.de
Öffentlicher Schlüssel - Informationen
Algorithmus RSA
Schlüssellänge 4096
Exponent 65537
Modulus D0:8F:D0:08:71:6F:7A:6E:62:87:D7:13:57:02:E4:0D:A6:5C:BC:5B:34:4E:27:D4:A6:D...

Anbindung von Internetsystemen

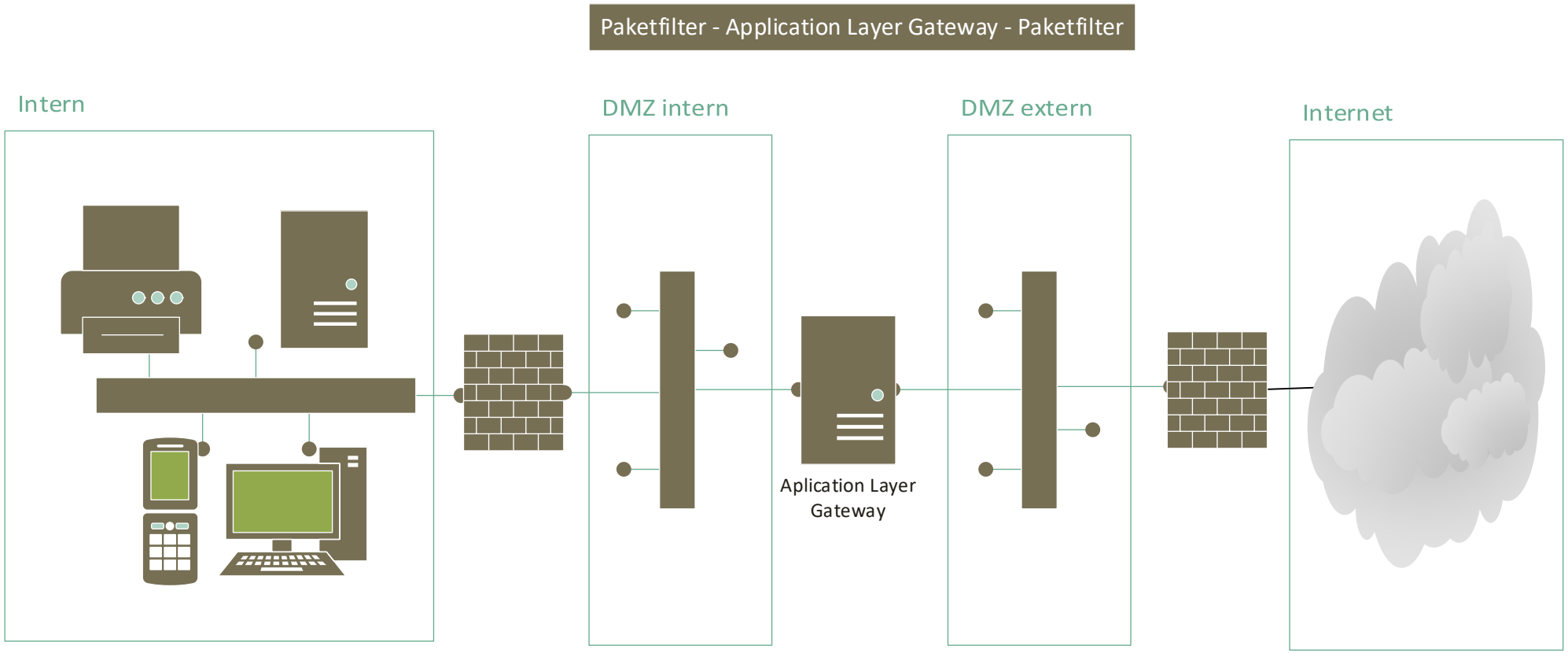
Anbindung Internetsysteme

Demilitarisierte Zone



Anbindung Internetsysteme

Demilitarisierte Zone



BSI Empfehlungen

Anbindung Internetsysteme

NET.1.1.A6 Endgeräte-Segmentierung im internen Netz (B)
Positionieren sie Endgeräte in einem Netzsegment, die einem ähnlichen Sicherheitsniveau entsprechen

NET.1.1.A7 Absicherung von schützenswerten Informationen (B)
Schützen Sie Ihre Informationen nach dem Stand der Technik durch sichere Protokolle, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird.
Können solche Protokolle nicht genutzt werden, verschlüsselt und authentisiert sie angemessen nach Stand der Technik

NET.1.1.A8 Grundlegende Absicherung des Internetzugangs (B)
Führen Sie den Internetverkehr über eine Firewall-Struktur. Schränken Sie die Kommunikationsbeziehungen durch eine Firewall-Struktur auf die benötigten Protokolle ein

NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen (B)

Legen Sie für jedes Netz fest, inwieweit es als vertrauenswürdig einzustufen ist. Netze, die nicht vertrauenswürdig sind, behandeln Sie wie das Internet behandelt und müssen entsprechend abgesichert werden.

NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet (B)

Die Firewall-Strukur MUSS für alle Dienste bzw. Anwendungen, die aus dem Internet erreichbar sind, um eine externe DMZ ergänzt werden.
Es SOLLTE ein Konzept zur DMZ-Segmentierung erstellt werden, das die Sicherheitsrichtlinie und die Anforderungsspezifikation nachvollziehbar umsetzt.
Abhängig vom Sicherheitsniveau der IT-Systeme MÜSSEN die DMZ-Segmente weitergehend unterteilt werden. Eine externe DMZ MUSS am äußeren Paketfilter angeschlossen werden.

NET.1.1.A11 Absicherung eingehender Kommunikation vom Internet in das interne Netz (B)
Ein IP-basierter Zugriff auf das interne Netz MUSS über einen sicheren Kommunikationskanal erfolgen. Der Zugriff MUSS auf vertrauenswürdige IT-Systeme und Benutzer beschränkt werden (siehe NET.3.3 VPN). Derartige VPN-Gateways SOLLTEN in einer externen DMZ platziert werden. Es SOLLTE beachtet werden, dass hinreichend gehärtete VPN-Gateways direkt aus dem Internet erreichbar sein können. Die über das VPN-Gateway authentisierten Zugriffe ins interne Netz MÜSSEN mindestens die interne Firewall durchlaufen.

IT-Systeme DÜRFEN NICHT via Internet oder externer DMZ auf das interne Netz zugreifen. Es SOLLTE beachtet werden, dass etwaige Ausnahmen zu dieser Anforderung in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

NET.1.1.A12 Absicherung ausgehender interner Kommunikation zum Internet (B)
Ausgehende Kommunikation aus dem internen Netz zum Internet MUSS an einem Sicherheits-Proxy entkoppelt werden. Die Entkoppelung MUSS außerhalb des internen Netzes erfolgen. Wird eine P-A-P-Struktur eingesetzt, SOLLTE die ausgehende Kommunikation immer durch die Sicherheits-Proxies der P-A-P-Struktur entkoppelt werden.