Schlussbericht

Jahresaudit 2019	
Kunde	Realisator AG
Datum	09.01.2020

REALISATOR

oneconsult®

Hauptsitz	Büro Bern	Büro Deutschland
Oneconsult AG Schützenstrasse 1 8800 Thalwil Schweiz Tel +41 43 377 22 22 Fax +41 43 377 22 77 www.oneconsult.com info@oneconsult.com	Oneconsult AG Bärenplatz 7 3011 Bern Schweiz Tel +41 31 327 15 15 Fax +41 31 327 15 25 www.oneconsult.com info@oneconsult.com	Oneconsult Deutschland GmbH Agnes-Pockels-Bogen 1 80992 München Deutschland Tel +49 89 248820 600 Fax +49 89 248820 677 www.oneconsult.com info@oneconsult.com

Inhaltsverzeichnis

Version	Datum	Beschreibung	Autor(in)
1.0	06.01.2020	Review	Claudio Anliker
0.9	24.12.2019	Reporting	Simon Gfeller

1 Einführung

Der vorliegende Bericht präsentiert die Resultate der technischen Sicherheitsüberprüfung, welche im Dezember 2019 durchgeführt wurde.

Oneconsult wurde mit folgenden Aufgaben betraut:

- Kick-off Meeting
- Security Scan DMZ
- Penetration Test ausgewählter Systeme in der DMZ
- Erstellung des vorliegenden Berichts

Der Bericht besteht aus einem Management Summary, Informationen zu den detektierten Risiken und Massnahmen (Kapitel 5) sowie weiteren technischen Details der Überprüfung (Kapitel 6).

2 Executive Summary

2.1 Overview

In this project, the security level of the DMZ (demilitarized zone), a part of the IT infrastructure of Realisator AG, was checked from an external and internal perspective by means of technical security tests. Automated vulnerability scans and manual penetration tests were used to search for network vulnerabilities on the systems. These tests are repeated annually.

2.2 Audit Objectives

The aim of the audit was to establish how vulnerable the DMZ infrastructure is from the outside as well as from the inside. The tests were conducted with regard to the scenarios of possible exfiltration of data as well as the possibility of malware infection within the DMZ.

2.3 Security Scan

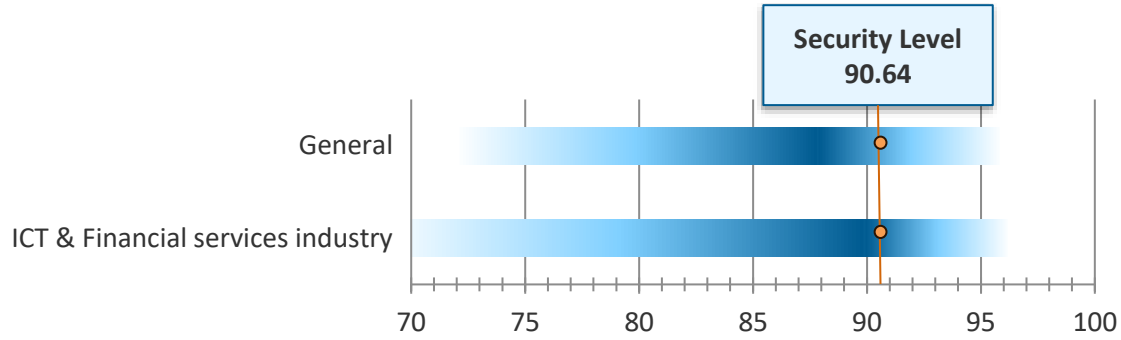
2.3.1 Detected Risks

The security scans were conducted between 06 and 09 December 2019. The following chart shows the distribution of the identified risks. More details about the risk categorization are listed in chapter 3.2.

Graph 1: Identified risks by category

2.3.2 Security Level and Benchmarking

The effective protection requirements depend on the test vector, surrounding systems, and assets that need to be protected. Based on the projects conducted by Oneconsult in the past years (over 850 OSSTMM- compliant projects), the following benchmark has been defined for the ICT and financial services industries. The calculation is illustrated in chapter 7.1.



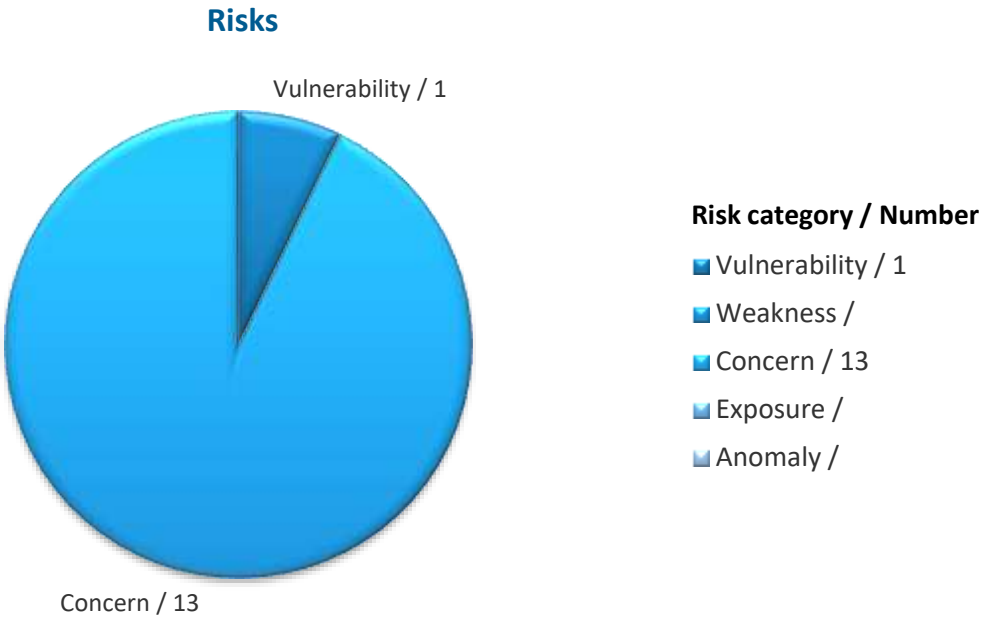
Graph 2: Security level and benchmarking

The security level above is considered to be rather high. However, a security scan is not comparable to a full penetration test. There may be additional risks, particularly in the case of web servers, which are often more vulnerable given their large attack surface. The security level may be further increased by implementing the recommended measures (see chapter 5.1).

2.4 Penetration Test

2.4.1 Identified Risks

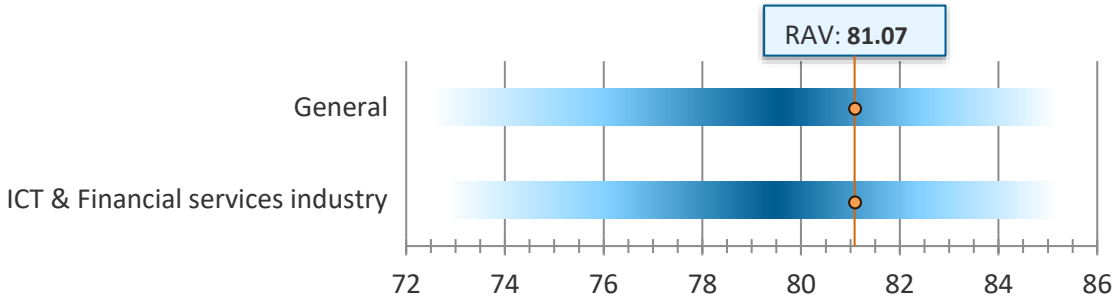
The tests took place between 09 and 10 December 2019. The following chart shows the distribution of the identified risks. More details about the risk categorization are listed in chapter 3.2.



Graph 3: Identified risks by category

2.4.2 Security Level and Benchmarking

The objective security level is reflected by the Risk Assessment Value (RAV). The formula is documented in chapter 7.2. The effective protection requirements depend on the test vector, the surrounding systems and the assets that need to be protected. Based on the projects conducted by Oneconsult in the past years (over 850 OSSTMM compliant-projects), the following benchmark for the ICT and financial services industry may be applied.



Graph 4: Risk Assessment Value benchmarking

Note: In practice, a RAV value of 100 is almost impossible. At this point an in-depth cost / benefit analysis (the ratio between the value of the analysed system and the investments in its security) should be performed to evaluate which improvements are worthwhile.

2.5 Conclusion

The security scan and the penetration test of the DMZ (Demilitarized Zone) have produced good results within the scope of the project. The systems are configured with professional competence and reflect the technical know-how of the people in charge. The achieved security level is above average. However, it should be considered that only a part of the systems within the DMZ were tested and that the test was unprivileged (without credentials), which means that for example the EasyTemp application and all its functions have not been tested.

The security scan contained a test of several DMZ systems from an external vector (Internet) and from the internal network. Only few risks were found during the security scan and most of them concern the configuration of the TLS servers and the TLS certificates in use. The TLS configuration could be further improved by disabling weak encryption algorithms.

Another issue is related to the mail ports (SMTP), which are mapped to all external IP addresses of Realisator and not only to the address of the mail server, which increases the attack surface. This should be mitigated by changing the appropriate settings on the firewall.

For four systems within the DMZ, a separate penetration test was conducted from an internal source address. To identify as many risks as possible, the firewalls were disabled for the tests. Consequently, more open ports and services could be found. Therefore, not all risk found during the tests could be exploited in the normal setup of the environment.

The penetration test has shown that a web application uses an old JavaScript library, which contains known vulnerabilities. It should be updated to the newest version. Other risks concern the configuration of the TLS server as already mentioned for the security scan.

Oneconsult recommends re-evaluating at least the mentioned risks as soon as possible. All risks and measures for the various test vectors are listed in chapter 5.

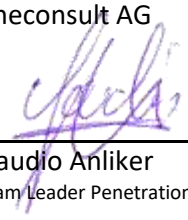
The cooperation between all involved people has been exemplary. At no point during the audit did Oneconsult think that information was concealed or presented in a better light.

Oneconsult would like to kindly thank all involved people for their cooperation and trust.

Oneconsult AG

Simon Gfeller
Senior Penetration Tester

Oneconsult AG



Claudio Anliker
Team Leader Penetration Testing

3 Lösungsansatz

3.1 Methode

Das Projekt wurde nach dem Open Source Security Testing Methodology Manual (OSSTMM) abgewickelt.

Das OSSTMM hat folgende primären Eigenschaften/Ziele:

1. Nachvollziehbarkeit und Transparenz der Tests und der Dokumentation
2. Vorgaben und Methoden zur Art und Durchführung von technischen Sicherheitsüberprüfungen
3. Neutrale Bewertung des Sicherheitsniveaus in Form eines Zahlenwerts (RAV)
4. Ethische Grundsätze

Die mit dem Projekt betrauten Consultants sind zertifizierte OSSTMM Professional Security Tester (OPST) und haben in den letzten Jahren bereits Dutzende Projekte nach OSSTMM abgewickelt.

3.2 Kategorisierung der Risiken

Als Sicherheitslücke wird eine Schwachstelle, ein Programmfehler oder ein Informationsleck bezeichnet, worüber eine unberechtigte Person bzw. ein unberechtigtes System/Programm (z.B. Malware) die Sicherheitsziele negativ beeinträchtigen könnte.

Damit die diagnostizierten Sicherheitslücken untereinander verglichen und deren Schadenspotential gewichtet werden kann, werden die detektierten Risiken nach OSSTMM in folgende Kategorien gegliedert:

Risikotyp	Beschreibung
Vulnerability (Verwundbarkeit)	Eine Schwachstelle im Sicherheitsmechanismus, worüber privilegierter Zugang zu einer Infrastruktur erlangt werden kann. Beispiel: Anfälligkeit auf «Buffer Overflow»-Attacke
Weakness (Schwachstelle)	Eine Schwachstelle in der Plattform, auf welcher der Sicherheitsmechanismus aufbaut. Beispiel: Tür-Alarm, der nicht ertönt, wenn die Türe länger geöffnet bleibt
Concern (Bedenken)	Keine direkte Bedrohung, entspricht jedoch nicht den Regeln der «best practices». Beispiel: nicht benötigter, aber aktiver Netzwerkdienst
Exposure (Informationsabfluss)	Preisgabe von Informationen über die Architektur. Beispiel: interne IP-Adressen im http Header
Anomaly (Anomalie)	Eine Unbekannte im System, welche der Tester mit den ihm zur Verfügung stehenden Informationen im vorgegebenen Zeitrahmen nicht identifizieren konnte. Beispiel: Nicht erwartete Antwort eines Routers

3.3 Prioritäten

Jede Massnahme wird zusätzlich mit einer Priorisierungsempfehlung nach folgendem Schema versehen:

Priorität	Beschreibung
1	Grosser Nutzen mit niedrigen Kosten oder geringem Aufwand oder sehr hohes Schädigungspotential.
2	Umsetzung empfohlen, aber Kosten/Nutzen-Verhältnis sollte beachtet werden.
3	Grosser Aufwand / hohe Kosten mit bedingtem Nutzen.

3.4 Projektorganisation

Das Projekt wurde wie folgt organisiert:

Rolle	Aufgabe	Verantwortlich
Projektleiter (Realisator)	→ Project Management → Schnittstelle zu Oneconsult → Koordination	Patrick Marty
Projektleiter	→ Schnittstelle zu Realisator → Ressourcenplanung → Koordination	Simon Gfeller
Analyse	→ Durchführung Tests → Analyse → Dokumentation	Simon Gfeller
Qualitätssicherung	→ Controlling → Review Dokumentation	Claudio Anliker

3.5 Generischer Prozess

Folgende Grafik illustriert den generischen Projektablauf:

Abbildung 5: Generischer Projektablauf

3.6 Aufgaben und Zeitablauf

Das Projekt wurde in folgende Module unterteilt:

Phase	Daten	Teilnehmer	Aufgaben
Kick-off Meeting	18.11.2019	Patrick Marty Simon Gfeller	→ Vorgehen und Zeitplanung → Evaluation von Methoden und Tools → Definition des Untersuchungsobjekts → Schnittstellen und Kontakte → Aufgaben zur Vorbereitung der Tests
Security Scan DMZ	06.12.2019 bis 09.12.2019	Simon Gfeller	→ Durchführung der Tests → Suche nach Sicherheitslücken → Grobe manuelle Verifikation → Feedback an Projektleiter → Research und Analysen
Penetration Test DMZ	09.12.2019 bis 10.12.2019	Simon Gfeller	→ Durchführung der Tests → Suche nach Sicherheitslücken → Manuelle Verifikation → Feedback an Projektleiter → Research und Analysen
Dokumentation	11.12.2019 bis 16.12.2019 06.01.2020	Simon Gfeller Claudio Anliker	→ Analyse der Testergebnisse → Erarbeitung von Massnahmen → Verfassen des Schlussberichts → Review des Schlussberichts

4 Scope

4.1 Security Scan DMZ

Folgende Systeme wurden untersucht:

Systeme	Datum	Source IP / Vektor	Whitelisting	Kommentar
www.realisator.ch (77.59.194.193)	06.12.2019	185.240.174.170 / Extern (Internet)	Portscanschutz wurde auf der Firewall für die Test-IP-Adresse deaktiviert	Die Scans wurden aus dem Internet durchgeführt.
test.easytemp.ch (77.59.194.194)				
test.easymission.ch (213.193.103.22)				
api.easytemp.ch (213.193.103.23)				
192.168.34.23 192.168.34.51 192.168.34.52 192.168.34.70 192.168.34.111 192.168.34.121 192.168.99.10	09.12.2019 – 10.12.2019	192.168.32.240 / Intern (Client Netzwerk)	-	Die Scans wurden aus dem internen Client Netzwerk durchgeführt. Die lokalen Firewalls (iptables) auf den Linux-Servern wurden temporär deaktiviert.

4.2 Penetration Test DMZ

Folgende Systeme wurden untersucht:

System	Datum	Source IP / Vektor	TCP	UDP*	ICMP	Whitelisting	Kommentar
192.168.34.23	09.12.2019 – 10.12.2019	192.168.32.240 / Intern (Client Netzwerk)	22 25 80 443 5555 7038	-	-		In einem ersten Schritt wurden die Server normal gescannt, in einem zweiten Schritt wurden die Client Firewalls (iptables) auf den Linux-Servern temporär deaktiviert. Die Ports, welche nur beim Scan mit den deaktivierten Firewalls geöffnet waren, sind rot markiert.
192.168.34.51	09.12.2019 – 10.12.2019	192.168.32.240 / Intern (Client Netzwerk)	22 25 80 443 3306 5555 30865	-	-		
192.168.34.52	09.12.2019 – 10.12.2019	192.168.32.240 / Intern (Client Netzwerk)	22 25 80 443 3306 5555 30865	-	-		
192.168.34.70	09.12.2019 – 10.12.2019	192.168.32.240 / Intern (Client Netzwerk)	21 22 25 80 443 5555 8080 9101	-	-		

Ausser über die aufgeführten TCP, UDP* und ICMP-Verbindungen konnte keine Interaktion mit den Systemen aufgenommen werden.

***** Beim UDP Protokoll wurden lediglich die 1‘000 am häufigsten verwendeten Ports gescannt. Aufgrund der Eigenschaften dieses Protokolls ist ein vollumfänglicher Scan ineffizient und unzuverlässig.

5 Risiken und Massnahmen

5.1 Security Scan DMZ

5.1.1 Externe Scans

Die folgenden Risiken wurden diagnostiziert und kategorisiert:

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.

test.easymission.ch (213.193.103.22)
api.easytemp.ch (213.193.103.23)
test.easytemp.ch (77.59.194.194)
25/tcp
587/tcp
465/tcp
 	
test.easymission.ch (213.193.103.22)
api.easytemp.ch (213.193.103.23)
www.realisator.ch (77.59.194.193)
test.easytemp.ch (77.59.194.194)
3400/tcp
	w1-13	**Sicherheitszertifikat auf falsche Domain ausgestellt**
		Das Sicherheitszertifikat des Systems wurde auf eine andere Domain ausgestellt und nicht auf den Host selbst. Somit kann die Authentizität des Servers nicht verifiziert werden.
		
		Dies ermöglicht Man-in-the-Middle-Attacken.
		
		Details aus den Zertifikaten:
		→ Port 25, 587, 465:
		`Subject (CN): *.realisator.ch`
		`SubjectAltName: *.realisator.ch, realisator.ch`
		→ Port 3400:
		`Subject (CN): red_server`
		`SubjectAltName: amon-amarth.realisator.ch`
		
		Bemerkung: Dieses Risiko besteht nur, weil die Ports 25, 465, 587 und 3400 auf alle öffentlichen IP-Adressen von Realisator gemappt werden. Wenn die betroffenen Services unter diesen Domains/IP-Adressen gar nicht verwendet werden, kann dieses Risiko vernachlässigt werden.
			Das Sicherheitszertifikat sollte auf die korrekte Domain ausgestellt werden.	Schutz vor Man-in-the-Middle-Angriffen	3

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.

test.easymission.ch (213.193.103.22)
api.easytemp.ch (213.193.103.23)
www.realisator.ch (77.59.194.193)
test.easytemp.ch (77.59.194.194)
3400/tcp
 	
test.easytemp.ch (77.59.194.194)
443/tcp
	c1-5	**RC4**
		Der TLS/SSL-Server unterstützt TLS 1.2-Chiffren, welche die Stromchiffre RC4 verwenden. Der Verschlüsselungsalgorithmus RC4 gilt als kryptographisch gebrochen.
		
		Ein Angreifer könnte dies nutzen, um die übermittelten Daten zu entschlüsseln und auszulesen.
		
		Verwendete Chiffren mit RC4:
		`TLS_RSA_WITH_RC4_128_SHA`
		`TLS_RSA_WITH_RC4_128_MD5`
		`TLS_ECDHE_RSA_WITH_RC4_128_SHA`
			RC4 sollte als Verschlüsselungsalgorithmus nicht mehr verwendet werden. Daher sollten alle TLS 1.2-Chiffren mit RC4 deaktiviert werden.
			
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Schutz der Vertraulichkeit	1

test.easytemp.ch (77.59.194.194)
443/tcp
	c6	**Verschlüsselung mit 3DES**
		Der Server unterstützt TLS 1.2-Chiffren, welche den Verschlüsselungsalgorithmus 3DES benutzen.
		
		Dieser Algorithmus ist auf einen sogenannten "Meet-in-the-Middle"-Angriff anfällig, der die effektive Schlüssellänge von 168 bit auf 112 bit reduziert. Zudem arbeitet 3DES mit 64-bit Blöcken und ist deshalb auf einen sogenannten Geburtstagsparadoxonangriff anfällig, der es einem Angreifer erlaubt, Teile der Nachricht zu entschlüsseln.
		
		Weitere Informationen unter:
		→ https://www.openssl.org/blog/blog/2016/08/24/sweet32/
		→ https://sweet32.info/
		→ http://www.crypto-it.net/eng/attacks/meet-in-the-middle.html
		
		Folgende 3DES Chiffren werden verwendet:
		`TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA`
		`TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA`
		`TLS_RSA_WITH_3DES_EDE_CBC_SHA`
			Cipher Suites mit dem Verschlüsselungsalgorithmus 3DES sollten nicht mehr verwendet werden.
			
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Erhöhter Schutz der Vertraulichkeit	2

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.

test.easymission.ch (213.193.103.22)
api.easytemp.ch (213.193.103.23)
www.realisator.ch (77.59.194.193)
test.easytemp.ch (77.59.194.194)
443/tcp
3400/tcp
	c7-14	**Veraltete TLS-Version im Einsatz**
		Der Server unterstützt mindestens eine veraltete Version der Transport Layer Security (TLS). Diese Version setzt Verfahren zur Verschlüsselung ein, die nicht mehr den aktuellen Sicherheitsstandards entsprechen.
		
		Folgende veraltete Versionen werden unterstützt:
		`SSLv3 (nur Port 3400)`
		`TLS 1.0`
		`TLS 1.1`
		
		Ein Angreifer mit genügend Ressourcen kann unter Umständen die veraltete Verschlüsselung angreifen und dadurch die übermittelten Nachrichten auslesen.
		
		Weitere Informationen:
		→ https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls
		→ https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/
		→ https://blogs.windows.com/msedge-dev/2018/10/15/modernizing-tls-edge-ie11/
		→ https://security.googleblog.com/2018/10/modernizing-transport-security.html
		
		Anmerkung: Ab 2020 planen alle grösseren Browserhersteller auch die Unterstützung von TLS 1.0 und TLS 1.1 zu deaktivieren.
			Der Webserver sollte so konfiguriert werden, dass er nur Verbindungen über TLS 1.2 und TLS 1.3 zulässt.
			
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Schutz der Vertraulichkeit	2

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.
test.easymission.ch (213.193.103.22) **api.easytemp.ch (213.193.103.23)** **www.realisator.ch (77.59.194.193)** **test.easytemp.ch (77.59.194.194)** 433/tcp 3400/tcp	c15-22	**CBC-Chiffren in TLS 1.2 unterstützt** Der Server unterstützt SSL/TLS-Chiffren, die den Verschlüsselungsmodus "Cipher Block Chaining" (CBC-Modus) benutzen. Für die verwendete TLS-Version 1.2 sind derzeit keine Angriffe auf CBC-Ciphers bekannt, jedoch existiert ein theoretischer Angriff (Padding Oracle Attack) dazu. Dadurch kann es unter Umständen möglich sein, Teile von abgehörten Verbindungen zu entschlüsseln. Weitere Informationen zur Sicherheit von CBC-Chiffren: → https://docs.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode	Es sollten nur authentifizierte Verschlüsselungsmodi verwendet werden ("Authenticated Encryption with Associated Data", AEAD). Ein Beispiel wäre der "Galois/Counter Mode" (GCM). Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.	Verbesserter Schutz der Vertraulichkeit	3

test.easymission.ch (213.193.103.22)
api.easytemp.ch (213.193.103.23)
www.realisator.ch (77.59.194.193)
test.easytemp.ch (77.59.194.194)
443/tcp
	c23-26	**Wildcard-Zertifikat ist im Einsatz**
		Beim hinterlegten Zertifikat handelt es sich um ein Wildcard-Zertifikat.
		
		Wird dasselbe Wildcard-Zertifikat für Systeme mit unterschiedlichen Sicherheitsanforderungen verwendet, kann die Kompromittierung eines Systems mit geringem Schutzbedarf Angriffe auf ein System mit hohem Schutzbedarf begünstigen.
		
		Dies kann beispielsweise der Fall sein, wenn das Wildcard-Zertifikat auf Test- sowie Produktionssystemen verwendet wird.
		
		Verwendete Zertifikate:
		`*.easytemp.ch`
		`*.easymission.ch`
		`*.realisator.ch`
			Zertifikate sollten für eine spezifische Domäne oder Applikation ausgestellt werden. So können die Konsequenzen eines Angriffs eingedämmt werden.
			
			Beispiel:
			`api.easytemp.ch`
				Reduzierung der Angriffsfläche im Falle einer Zertifikatskompromittierung	3

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.
test.easymission.ch (213.193.103.22) **api.easytemp.ch (213.193.103.23)** **www.realisator.ch (77.59.194.193)** **test.easytemp.ch (77.59.194.194)** 25/tcp 465/tcp 587/tcp 3400/tcp	a1-16	**Diverse Ports auf allen externen IP-Adressen erreichbar** Dies Sophos UTM 9 Firewall ist so konfiguriert, dass jede öffentliche IP-Adresse auf dem WAN Interface auf den SMTP Ports (25, 465, 587) und dem RED (Remote Ethernet Device) Port 3400 hört. Dies scheint nicht notwendig zu sein, da der SMTP Server wie auch der Endpunkt für den RED-Tunnel nur auf den entsprechenden öffentlichen IP-Adressen erreichbar sein sollten.	Der SMTP-Server wie auch der Endpunkt für den RED-Tunnel sollten nur auf den dafür bestimmten öffentlichen IP-Adressen erreichbar sein. Da die Sophos UTM9 für transparente Proxys keine entsprechenden Möglichkeiten bietet, könnte eine mögliche Massnahme sein, den unnötigen Traffic per DNAT-Regeln in ein Black Hole zu leiten. **Bemerkung**: Durch das Schliessen dieser Ports auf den nicht benötigten IP-Adressen würden sich auch mehrere der anderen aufgelisteten Risiken erübrigen.	Reduzierung der Angriffsfläche	2

Anmerkung: Die obenstehende Tabelle steht auch in elektronischer Form als Arbeitsblatt zur Verfügung.

5.1.2 Interne Scans

Die folgenden Risiken wurden diagnostiziert und kategorisiert:

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.

192.168.34.111
192.168.34.121
443/tcp
	w14-15	**Das SSL-Zertifikat ist selbstsigniert**
		Das Sicherheitszertifikat der Webseite ist selbstsigniert. Die Vertrauenswürdigkeit des Zertifikats kann somit nicht ermittelt und die Authentizität des Servers folglich nicht verifiziert werden.
		
		Dies ermöglicht Man-in-the-Middle-Attacken.
		
		Details aus dem Zertifikat:
		
		192.168.34.11:
		`Subject: easymailout.dmz.local`
		`Issuer: easymailout.dmz.local`
		
		192.168.34.121:
		`Subject: smtp-out-20.dmz.local`
		`Issuer: smtp-out-20.dmz.local`
			Wenn möglich sollte das Zertifikat durch eine Certificate Authority (CA) signiert werden, welcher die zugreifende Software vertraut. Dies sind beispielsweise die im Webbrowser eingetragenen "Root CAs" oder eine eigene, firmeninterne CA.	Schutz vor Man-in-the-Middle-Angriffen	2

192.168.99.10 **192.168.34.70** 21/tcp	w16-17	**Daten werden über FTP unverschlüsselt gesendet** Benutzername, Passwort sowie Daten werden via FTP unverschlüsselt übertragen. Somit ist es für Dritte möglich, die Kommunikation zwischen Client und Server abzuhören.	Wenn möglich sollte nur entweder SFTP (SSH FTP) oder FTPS (FTP über SSL) verwendet werden, um die Vertraulichkeit der übertragenen Daten zu gewährleisten. Bei FTPS (FTP über SSL) sollte sichergestellt werden, dass sowohl der Steuerkanal (Username, Passwort) wie auch der Datenkanal verschlüsselt werden.	Schutz der Vertraulichkeit und Integrität	2

192.168.34.23
443/tcp
	c27	**RC4**
		Der TLS/SSL-Server unterstützt TLS 1.2-Chiffren, welche die Stromchiffre RC4 verwenden. Der Verschlüsselungsalgorithmus RC4 gilt als kryptographisch gebrochen.
		
		Ein Angreifer könnte dies nutzen, um die übermittelten Daten zu entschlüsseln und auszulesen.
		
		Verwendete Chiffren mit RC4:
		`TLS_RSA_WITH_RC4_128_SHA`
		`TLS_RSA_WITH_RC4_128_MD5`
		`TLS_ECDHE_RSA_WITH_RC4_128_SHA`
			RC4 sollte als Verschlüsselungsalgorithmus nicht mehr verwendet werden. Daher sollten alle TLS 1.2-Chiffren mit RC4 deaktiviert werden.
			
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Schutz der Vertraulichkeit	1

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.

192.168.34.23
443/tcp
	c28	**Verschlüsselung mit 3DES**
		Der Server unterstützt TLS 1.2-Chiffren, welche den Verschlüsselungsalgorithmus 3DES benutzen.
		
		Dieser Algorithmus ist auf einen sogenannten "Meet-in-the-Middle"-Angriff anfällig, der die effektive Schlüssellänge von 168 bit auf 112 bit reduziert. Zudem arbeitet 3DES mit 64-bit Blöcken und ist deshalb auf einen sogenannten Geburtstagsparadoxonangriff anfällig, der es einem Angreifer erlaubt, Teile der Nachricht zu entschlüsseln.
		
		Weitere Informationen unter:
		→ https://www.openssl.org/blog/blog/2016/08/24/sweet32/
		→ https://sweet32.info/
		→ http://www.crypto-it.net/eng/attacks/meet-in-the-middle.html
		
		Folgende 3DES Chiffren werden verwendet:
		`TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA`
		`TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA`
		`TLS_RSA_WITH_3DES_EDE_CBC_SHA`
			Cipher Suites mit dem Verschlüsselungsalgorithmus 3DES sollten nicht mehr verwendet werden.
			
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Erhöhter Schutz der Vertraulichkeit	2

192.168.34.70 8080/tcp	c29	**Der Webserver unterstützt die HTTP TRACE-Methode** Bei einer Cross-Site Scripting (XSS) Verwundbarkeit könnte ein Angreifer diese Methode missbrauchen, um Cookies auszulesen, welche mit dem HTTPOnly Flag geschützt sind (Cross-Site Tracing Angriff). Mehr Informationen: → http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf	Die TRACE-Methode ist nur für Debugging gedacht und sollte auf einem produktiven System deaktiviert werden.	Schutz vor Cross-Site Tracing (XST) Attacken	2

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.
192.168.34.70 9101/tcp	c30	**System unterstützt Telnet** Das System erlaubt Zugriff über das veraltete Protokoll «Telnet». Telnet überträgt sämtliche Daten unverschlüsselt. Ein Angreifer mit Zugriff auf die Kommunikation zwischen Client und Server kann beispielsweise Benutzernamen und Passwörter auslesen. Screenshot: 	Telnet sollte nicht mehr verwendet und durch einen verschlüsselten Dienst ersetzt werden (beispielsweise SSH).	Erhöhter Schutz der Vertraulichkeit und Integrität	2
192.168.34.111 **192.168.34.121** **192.168.99.10** **192.168.34.23** **192.168.34.51** **192.168.34.52** **192.168.34.70** 443/tcp	c31-37	**CBC-Chiffren in TLS 1.2 unterstützt** Der Server unterstützt SSL/TLS-Chiffren, die den Verschlüsselungsmodus "Cipher Block Chaining" (CBC-Modus) benutzen. Für die verwendete TLS-Version 1.2 sind derzeit keine Angriffe auf CBC-Ciphers bekannt, jedoch existiert ein theoretischer Angriff (Padding Oracle Attack) dazu. Dadurch kann es unter Umständen möglich sein, Teile von abgehörten Verbindungen zu entschlüsseln. Weitere Informationen zur Sicherheit von CBC-Chiffren: → https://docs.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode	Es sollten nur authentifizierte Verschlüsselungsmodi verwendet werden ("Authenticated Encryption with Associated Data", AEAD). Ein Beispiel wäre der "Galois/Counter Mode" (GCM). Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.	Verbesserter Schutz der Vertraulichkeit	3

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.

192.168.34.111
192.168.34.121
192.168.99.10
192.168.34.23
192.168.34.51
192.168.34.52
192.168.34.70
443/tcp
	c38-44	**Veraltete TLS-Version im Einsatz**
		Der Server unterstützt mindestens eine veraltete Version der Transport Layer Security (TLS). Diese Version setzt Verfahren zur Verschlüsselung ein, die nicht mehr den aktuellen Sicherheitsstandards entsprechen. Folgende veraltete Versionen werden unterstützt:
		`TLS 1.0`
		`TLS 1.1`
		Ein Angreifer mit genügend Ressourcen kann unter Umständen die veraltete Verschlüsselung angreifen und dadurch die übermittelten Nachrichten auslesen.
		Weitere Informationen:
		→ https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls
		→ https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/
		→ https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/
		→ https://security.googleblog.com/2018/10/modernizing-transport-security.html
		Anmerkung: Ab 2020 planen alle grösseren Browserhersteller auch die Unterstützung von TLS 1.0 und TLS 1.1 zu deaktivieren.
			Der Webserver sollte so konfiguriert werden, dass er nur Verbindungen über TLS 1.2 und TLS 1.3 zulässt.
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Schutz der Vertraulichkeit	3

Anmerkung: Die obenstehende Tabelle steht auch in elektronischer Form als Arbeitsblatt zur Verfügung.

5.2 Penetration Test DMZ

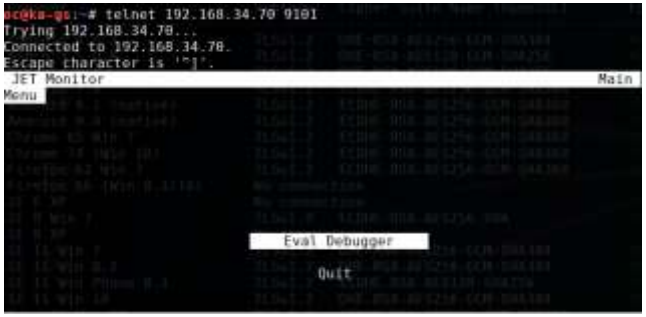
Die folgenden Risiken wurden diagnostiziert und kategorisiert:

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.
www.realisator.ch (192.168.34.51) 443/tcp	v1	**jQuery veraltet** Die Webapplikation verwendet die veraltete Version 1.12.4 der JavaScript-Bibliothek jQuery. Diese Version ist verwundbar für Cross-Site-Scripting (XSS). Wenn die betroffene Funktion von der Webapplikation verwendet wird, kann ein Angreifer beliebigen JavaScript-Code im Kontext des Benutzers ausführen. Befund: → https://www.realisator.ch/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp Weitere Informationen: → https://github.com/jquery/jquery/issues/2432 → http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ → https://nvd.nist.gov/vuln/detail/CVE-2015-9251 → http://research.insecurelabs.org/jquery/test/	jQuery sollte auf die neueste Version aktualisiert werden.	Schutz vor Cross-Site-Scripting-Angriffen	3
192.168.34.70 21/tcp	c45	**Daten werden über FTP unverschlüsselt gesendet** Benutzername, Passwort sowie Daten werden via FTP unverschlüsselt übertragen. Somit ist es für Dritte möglich, die Kommunikation zwischen Client und Server abzuhören.	Wenn möglich sollte nur entweder SFTP (SSH FTP) oder FTPS (FTP über SSL) verwendet werden, um die Vertraulichkeit der übertragenen Daten zu gewährleisten. Bei FTPS (FTP über SSL) sollte sichergestellt werden, dass sowohl der Steuerkanal (Username, Passwort) wie auch der Datenkanal verschlüsselt werden.	Schutz der Vertraulichkeit und Integrität	2

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.

192.168.34.23
443/tcp
	c46	**RC4**
		Der TLS/SSL-Server unterstützt TLS 1.2-Chiffren, welche die Stromchiffre RC4 verwenden. Der Verschlüsselungsalgorithmus RC4 gilt als kryptographisch gebrochen.
		
		Ein Angreifer könnte dies nutzen, um die übermittelten Daten zu entschlüsseln und auszulesen.
		
		Verwendete Chiffren mit RC4:
		`TLS_RSA_WITH_RC4_128_SHA`
		`TLS_RSA_WITH_RC4_128_MD5`
		`TLS_ECDHE_RSA_WITH_RC4_128_SHA`
			RC4 sollte als Verschlüsselungsalgorithmus nicht mehr verwendet werden. Daher sollten alle TLS 1.2-Chiffren mit RC4 deaktiviert werden.
			
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Schutz der Vertraulichkeit	1

192.168.34.23
443/tcp
	c47	**Verschlüsselung mit 3DES**
		Der Server unterstützt TLS 1.2-Chiffren, welche den Verschlüsselungsalgorithmus 3DES benutzen.
		
		Dieser Algorithmus ist auf einen sogenannten "Meet-in-the-Middle"-Angriff anfällig, der die effektive Schlüssellänge von 168 bit auf 112 bit reduziert. Zudem arbeitet 3DES mit 64-bit Blöcken und ist deshalb auf einen sogenannten Geburtstagsparadoxon-angriff anfällig, der es einem Angreifer erlaubt, Teile der Nachricht zu entschlüsseln.
		
		Weitere Informationen unter:
		→ https://www.openssl.org/blog/blog/2016/08/24/sweet32/
		→ https://sweet32.info/
		→ http://www.crypto-it.net/eng/attacks/meet-in-the-middle.html
		
		Folgende 3DES Chiffren werden verwendet:
		`TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA`
		`TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA`
		`TLS_RSA_WITH_3DES_EDE_CBC_SHA`
			Cipher Suites mit dem Verschlüsselungsalgorithmus 3DES sollten nicht mehr verwendet werden.
			
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Erhöhter Schutz der Vertraulichkeit	2

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.
192.168.34.70 9101/tcp	c48	**System unterstützt Telnet** Das System erlaubt Zugriff über das veraltete Protokoll «Telnet». Telnet überträgt sämtliche Daten unverschlüsselt. Ein Angreifer mit Zugriff auf die Kommunikation zwischen Client und Server kann beispielsweise Benutzernamen und Passwörter auslesen. Screenshot: 	Telnet sollte nicht mehr verwendet und durch einen verschlüsselten Dienst ersetzt werden (beispielsweise SSH).	Erhöhter Schutz der Vertraulichkeit und Integrität	2
192.168.34.23 **192.168.34.51** **192.168.34.52** **192.168.34.70** 443/tcp	c49-52	**CBC-Chiffren in TLS 1.2 unterstützt** Der Server unterstützt SSL/TLS-Chiffren, die den Verschlüsselungsmodus "Cipher Block Chaining" (CBC-Modus) benutzen. Für die verwendete TLS-Version 1.2 sind derzeit keine Angriffe auf CBC-Ciphers bekannt, jedoch existiert ein theoretischer Angriff (Padding Oracle Attack) dazu. Dadurch kann es unter Umständen möglich sein, Teile von abgehörten Verbindungen zu entschlüsseln. Weitere Informationen zur Sicherheit von CBC-Chiffren: → https://docs.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode	Es sollten nur authentifizierte Verschlüsselungsmodi verwendet werden ("Authenticated Encryption with Associated Data", AEAD). Ein Beispiel wäre der "Galois/Counter Mode" (GCM). Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.	Verbesserter Schutz der Vertraulichkeit	3

System	Ref.	Risiko	Empfehlung	Nutzen	Prio.
192.168.34.70 8080/tcp	c53	**Der Webserver unterstützt die HTTP TRACE-Methode** Bei einer Cross-Site Scripting (XSS) Verwundbarkeit könnte ein Angreifer diese Methode missbrauchen, um Cookies auszulesen, welche mit dem HTTPOnly Flag geschützt sind (Cross-Site Tracing Angriff). Mehr Informationen: → http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf	Die TRACE-Methode ist nur für Debugging gedacht und sollte auf einem produktiven System deaktiviert werden.	Schutz vor Cross-Site Tracing (XST) Attacken	3

192.168.34.23
192.168.34.51
192.168.34.52
192.168.34.70
443/tcp
	c54-57	**Veraltete TLS-Version im Einsatz**
		Der Server unterstützt mindestens eine veraltete Version der Transport Layer Security (TLS). Diese Version setzt Verfahren zur Verschlüsselung ein, die nicht mehr den aktuellen Sicherheitsstandards entsprechen. Folgende veraltete Versionen werden unterstützt:
		`TLS 1.0`
		`TLS 1.1`
		
		Ein Angreifer mit genügend Ressourcen kann unter Umständen die veraltete Verschlüsselung angreifen und dadurch die übermittelten Nachrichten auslesen.
		
		Weitere Informationen:
		→ https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls
		→ https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/
		→ https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/
		→ https://security.googleblog.com/2018/10/modernizing-transport-security.html
		
		Anmerkung: Ab 2020 planen alle grösseren Browserhersteller auch die Unterstützung von TLS 1.0 und TLS 1.1 zu deaktivieren.
			Der Webserver sollte so konfiguriert werden, dass er nur Verbindungen über TLS 1.2 und TLS 1.3 zulässt.
			
			Mehr Informationen zu empfohlenen Verschlüsselungsprotokollen sind in Kapitel 6.1 aufgeführt.
				Schutz der Vertraulichkeit	3

Anmerkung: Die obenstehende Tabelle steht auch in elektronischer Form als Arbeitsblatt zur Verfügung.

6 Test Details

6.1 TLS-Konfiguration

Für die sichere Verbindung über TLS, beispielsweise über HTTPS oder SMTP, gilt es bei der Konfiguration der verwendeten Chiffren neben der Sicherheit auch die Kompatibilität mit den zu erwartenden Clients zu beachten. Dabei ist das grösste Problem, dass Clients nicht nur unterschiedlichen Browser verwenden, sondern auch unterschiedlich aktuelle Betriebssysteme, die nicht dieselbe Version von TLS unterstützen. Die folgenden Empfehlungen legen einen Fokus auf Sicherheit.

6.1.1 SSL-/ TLS-Versionen

TLS 1.2 enthält als einzige TLS-Version noch Algorithmen und Modi ohne Sicherheitsrisiken oder -bedenken. Alle vorhergehenden Versionen sind deshalb idealerweise zu deaktivieren. Dies führt jedoch zu Verbindungsproblemen mit älteren Betriebssystemen, beziehungsweise deren verwendete Standardbrowser.

Folgende Programme unterstützen kein TLS 1.2:
- → Android OS Browser, Android vor Version 4.4.2
- → Internet Explorer vor Version 11
- → Java vor Version 1.7

Falls der Web Server keine Verbindungen von Clients mit den oben genannten Programmen akzeptiert, können somit alle anderen TLS-Versionen deaktiviert werden. Falls entsprechende Clients unterstützt werden sollen, dann müssen sowohl TLS 1.0 und TLS 1.1 aktiviert sein. SSLv3 und SSLv2 sollten unter keinen Umständen aktiviert werden, da diese erhebliche Sicherheitsschwachstellen aufweisen.

6.1.2 Chiffrenselektion

Idealerweise sollten nur authentisierte Verschlüsselungsmodi (Authenticated Encryption with Associated Data, AEAD) verwendet werden. Hierzu gehören Blockchiffren, welche im Galois/Counter Mode (GCM) oder CCM (Counter with CBC-MAC) Modus verwendet werden oder die Stromchiffre ChaCha20-Poly1305. Diese sind alle nur unter TLS 1.2 verfügbar.

In der Praxis werden oft die Blockchiffren im CBC-Modus verwendet. Diese gelten unter TLS 1.1 und TLS 1.2 zwar als sicher, jedoch wurden des Konzeptes wegen immer wieder Schwachstellen in diesem Verschlüsselungsmodus gefunden. Deshalb sollte der Gebrauch von Chiffren im CBC-Modus möglichst vermieden werden. Diese Empfehlung wird auch dadurch gestützt, dass CBC-Chiffren aus TLS 1.3 gänzlich ausgeschlossen wurden. Sollte der Server also TLS 1.3 unterstützen, werden für diese TLS-Version keine CBC-Chiffren angeboten.

Nicht verwendet werden sollten zudem alle Chiffren, welche die Stromchiffre RC4 oder die Blockchiffre 3DES verwenden, da beide als unsicher und gebrochen gelten[1].

6.1.3 Schlüsselaushandlung

Zu Beginn einer TLS-Verbindung wird jeweils zwischen dem Server und dem Client ein Schlüssel für die Session ausgehandelt. Idealerweise wird hier ein Algorithmus verwendet, welcher „Forward Secrecy“ verspricht. Dies bedeutet, dass auch wenn ein Langzeit-Schlüssel (z.B. der private RSA-Schlüssel) oder der Sitzungs-Schlüssel einer Verbindung kompromittiert wird, die Daten anderer Verbindungen nicht entschlüsselt werden können.

[1] Beispielangriffe:
Sweet32 auf 3DES: https://sweet32.info/
NOMORE auf RC4: http://www.rc4nomore.com/

Dabei sollte wenn möglich der Algorithmus „Ephemeral Diffie-Hellman“ mit elliptischen Kurven (ECDHE) verwendet werden, da dieser weniger Rechenleistung benötigt als der reguläre „Ephemeral Diffie-Hellman“ (DHE), bei dem auch zusätzlich darauf geachtet werden muss, dass ausreichend lange (mind. 2048 Bit) und zufällig gewählte Diffie-Hellmann-Gruppen benutzt werden. Dies kann nicht für alle Versionen aller Implementationen garantiert werden. In TLS 1.3 werden nur noch Varianten des DHE-Algorithmus unterstützt; somit wird auch hier das neue Protokoll automatisch die Sicherheit erhöhen.

6.1.4 Konfigurationsbeispiele

Zusammenfassend empfiehlt Oneconsult somit die folgenden Chiffren zu verwenden:

```
ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256
```

Dies sind alles Chiffren aus TLS 1.2 und werden somit von allen modernen Clients unterstützt. Die ChaCha20 Chiffren sind dabei vor allem für mobile Clients interessant, da diese oft keine Hardware-Unterstützung für AES besitzen. Diese Chiffren reichen aus, wenn ein Zertifikat mit einer ECDSA-Signatur versehen ist.

Wird ein Zertifikat mit RSA-Signatur verwendet, müssen für den Support von Internet Explorer 11 unter Windows 7 und 8.1 noch einige CBC-Chiffren hinzugefügt werden:

```
ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-
RSA-AES128-SHA256
```

Die CBC-Chiffren sind notwendig, da Microsoft GCM-Chiffren unter diesen beiden alten Betriebssystemen zurzeit (September 2018) nur in Zusammenhang mit einem DSA-Zertifikat unterstützt. Unter Windows 10 sind sowohl mit Microsoft Edge als auch mit Internet Explorer Verbindungen ohne diese Chiffren möglich.

Da TLS 1.1 und TLS 1.2 von den meisten Clients gleichzeitig unterstützt worden sind, muss für die Unterstützung von älteren Clients gleich eine grosse Anzahl schwächerer Chiffren erlaubt werden. Folgende Liste von Chiffren in Kombination mit einem RSA-Zertifikat unterstützt viele alte Clients:

```
ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-
AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-
AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-
DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS
```

Diese Auswahl unterstützt mehrere Chiffren, welche als unsicher gelten. Dies ist jedoch unumgänglich, wenn nicht mehr unterstützte Betriebssysteme wie beispielsweise Windows Vista mit IE9, Windows XP mit IE8 oder der Android Browser vor Version 5.0 unterstützt werden sollen. Wird die Reihenfolge eingehalten, werden jedoch moderne Clients den Datenverkehr zum Server mit einer sicheren Chiffre verschlüsseln.

Eine von Mozilla veröffentlichte Liste von Konfigurationen kann unter folgendem Link gefunden werden:

→ https://wiki.mozilla.org/Security/Server_Side_TLS

Mozilla hat zudem ein Tool veröffentlicht, um SSL-Konfigurationen für bekannte Webserver zu generieren:

→ https://mozilla.github.io/server-side-tls/ssl-config-generator/

6.1.5 Ausblick auf TLS 1.3

Mit TLS 1.3 wurde im August 2018 der neue TLS-Standard veröffentlicht. Dieser bringt im Vergleich zu vorhergehenden Versionen mehr Sicherheit und mehr Performance.
Durch eine Reduktion der zur Verfügung stehenden Chiffren und Schlüsselaustauschmechanismen auf die Menge der als sicher geltenden Algorithmen, können keine angreifbaren Verbindungen mehr aufgebaut werden. Zudem werden mehr Teile der anfänglichen Verbindungsaufbaunachrichten verschlüsselt.

Durch die Implementierung von Mechanismen für einen schnelleren Verbindungsaufbau wird die Zeit, bis der Benutzer den angeforderten Inhalt übermittelt bekommt, drastisch reduziert. So erhalten Clients einen erhöhten Schutz der übertragenen Daten und Server-Betreiber profitieren von einem erhöhten Durchsatz.
Schon zum Erscheinungstermin ist die Unterstützung für TLS 1.3 auf Clients besser als dies zum Erscheinungstermin von TSL 1.2 war. Sowohl Google Chrome als auch Mozilla Firefox unterstützen die neue Version von TLS schon und sowohl Microsoft als auch Apple werden in den nächsten Veröffentlichungen eine Implementation bereitstellen.
Somit sollte TLS 1.3 auf der Server-Seite sobald wie möglich unterstützt werden, so dass die Vorteile des neuen Standards genutzt werden können.

7 Anhang

7.1 Security Level Berechnung

Security Level Calculation

Hosts:	11
Ports:	70
Low:	60
Medium:	17
High:	0

Penalties	
Ports:	2.33
Low:	2.00
Medium:	5.67
High:	0.00
Total:	**10.00**
Penalties per Host:	0.91
Missing:	0.09

Security Level	**90.64%**

7.2 RAV-Berechnung - Penetration Test

Attack Surface Security Metrics

OSSTMM version 3.0

OPSEC	
Visibility	4
Access	28
Trust	0
Total (Porosity)	32

CONTROLS		
Class A		Missing
Authentication	8	24
Indemnification	5	27
Resilience	28	4
Subjugation	9	23
Continuity	0	32
Total Class A	50	110

Class B		Missing
Non-Repudiation	17	15
Confidentiality	8	24
Privacy	0	32
Integrity	8	24
Alarm	6	26
Total Class B	39	121

		True Missing
All Controls Total	89	231
Whole Coverage	27.81%	72.19%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	1	8.218750	8.218750
Weaknesses	0	4.437500	0.000000
Concerns	13	4.781250	62.156250
Exposures	0	1.159375	0.000000
Anomalies	0	0.437500	0.000000
Total # Limitations	14		70.3750

OPSEC	12.287028
True Controls	8.701778
Full Controls	8.701778
True Coverage A	31.25%
True Coverage B	24.38%
Total True Coverage	27.81%
Limitations	14.803103
Security Δ	-18.39
True Protection	81.61

Actual Security: 81.0732 ravs

7.3 Abbildungen