H&S QM-Support UG
(haftungsbeschränkt) & Co. KG
Kurzes Geländ 6
D-86156 Augsburg

Telefon +49 (0)8 21/9 07 63 34
Telefax +49 (0)8 21/9 07 63 35
E-Mail: info@hs-qmsupport.de
Internet: www.hs-qmsupport.de

Musterfirma Anlagenbau KG

Musterweg 12, 10001 Berlin

Dieser Bericht wurde am 05.11.2018 mit einem Datenstand vom 06.09.2018 07:16-05.11.2018 01:20 erstellt. Er basiert auf Daten die zum Zeitpunkt der Erstellung öffentlich verfügbar waren bzw. zu einem früheren Zeitpunkt öffentlich verfügbar waren und historisiert wurden. Die erhobenen Daten wurden im Hinblick auf das Risiko eines erfolgreichen Cyberangriffs bewertet und ergaben ein beherrschbares Risiko.

Musterfirma Anlagenbau KG
Musterweg 12, 10001 Berlin

Basis für die Bewertung waren die folgenden eingegebenen Daten:

Basis Domains:	musterfirma.de
	musterfirma.com
Größe:	250-999 Mitarbeiter

Bewertung in der Übersicht

Die Ergebnisse eventuell angegebener Vergleichsunternehmen sind in blau eingezeichnet.

Cyber Security Score - Bewertung der Cyber-Sicherheitsrisiken eines Unternehmens auf Basis von ausserhalb des Unternehmens wahrnehmbaren technischen Gegebenheiten.

Die Bewertung setzt sich aus folgenden Kategorien zusammen:

Konkrete Gefährdungslage - Bewertung aller Indizien, die auf einen laufenden Angriff oder eine akute Angriffsmöglichkeit hindeuten

Reputation im Cyberraum - Bewertung der Reputation des Unternehmens im Internet

Mitarbeiterverhalten im Cyberspace - Bewertung aller Indizien, wie vorsichtig die Mitarbeiter des Unternehmens im Internet auftreten.

Organisations- & Prozessrisiken - Bewertung aller Indizien, die mit den Betriebs-, Wartungs- und Sicherheitsprozessen in Zusammenhang stehen

Länderrisiken - Bewertung der Risiken, die durch Präsenz in verschiedenen Jurisdiktionen und Kulturkreisen entstehen

Vertrauenswürdige Verschlüsselung - Bewertung der korrekten Konfiguration der SSL/TLS Verschlüsselungstechnologien

Angriffsfläche im Internet - Bewertung der offenen Ports, die für das gesamte Internet erreichbar sind

Details zu den einzelnen Ergebnissen finden Sie auf den folgenden Seiten.

Erläuterung der Bewertung

Für diesen Bericht wurden 37 IP Adressen, 75 Servernamen und 143 verschiedenen Applikationen / Ports untersucht. Insgesamt wurden 452 Prüfprogramme abgearbeitet. Dabei wurden insgesamt 1.208 Erkenntnisse (gute wie schlechte) generiert, davon 1.190 durch die Analyse der Server, IP-Adressen und Applikationen / Ports sowie 18 übergreifende.

Kategorie

Konkrete Gefährdungslage

Wenn keine Indizien vorliegen, ist die Bewertung hier optimal. Akute Hinweise wie die Verteilung von Malware oder ein TOR exit node im eigenen Netz senken das Rating auf D. Unsichere Hinweise wie ein offener Port, der gerne auch von Malware benutzt wird, senkt das Rating auf C. Angriffsmöglichkeiten, die zwar bestätigt vorhanden, aber derzeit von der organisierten Kriminalität noch nicht in der Fläche ausgenutzt werden, senken das Rating ebenfalls auf C. Dazu gehören die Angriffe CRIME, POODLE, Heartbleed, TLS CCS Injection, ROBOT (Return of Bleichenbacher Attack), die Verwendung alter SSL Versionen und Angriffe auf die Neuaushandlung von Schlüsseln im TLS Protokoll. Einstellungen, die das Abhören oder das nachträgliche Knacken von verschlüsselten Verbindungen erleichtern bzw. ermöglichen, senken das Rating auf B. Dazu gehören schwache Schlüssel, schwache Algorithmen (RC4, null) und fehlender Support für "Perfect Forward Secrecy".

	A	B	C	D	
352 Erkenntnisse	242x	42x	68x	0x	
Berechnungsmethodik: minimaler Wert					40%

Reputation im Cyberraum

In dieser Kategorie werden die Ergebnisse der Tests gegen hunderte von Black- oder Whitelists zusammengefasst. Sollte eine IP oder Domain auf einer Blacklist gelandet sein, wird dies mit 0%, ein Eintrag auf einer Whitelist mit 100% bewertet. Mit doppelter Gewichtung gehen die Ergebnisse von Reputationslisten ein, die ein abgestuftes Ergebnis zwischen 0 und 100% liefern. Auch die Ergebnisse von URL-Reputationstools (wie z.B. Google SafeBrowsing) gehen doppelt ins Ergebnis ein. Sollte eine Seite aktuell als infiziert gemeldet werden, wird das Rating deutlich abgesenkt. Diese Ergebnisse werden pro Server zusammengefasst und dann ein Durchschnitt gebildet.

	A	B	C	D	
269 Erkenntnisse	91x	1x	0x	177x	
Zusammengefasst pro IP: Durchschnitt	0x	10x	26x	1x	
Berechnungsmethodik: gewichteter Durchschnitt					39%

Mitarbeiterverhalten im Cyberspace

In dieser Kategorie wird bewertet, wie die Mitarbeiter des Unternehmens mit den Ihnen zugeteilten E-Mail Adressen umgehen. Geprüft wird die Nutzung von firmeneigenen E-Mailadressen auf sozialen Netzen und Chatseiten, Spieleseiten & Gamingplattformen, Musik- und Videoportalen, Datingseiten, Filesharing, P2P-Networking und Tauschbörsen. Ebenso wird die Verwendung in Hackerforen und auf Pornoseiten bewertet. Auf den Durchschnitt dieser Bewertung wird 1:1 zusätzlich eingerechnet, wie viele Passwörter in Leaks bekannt geworden sind. Alle Werte sind in Relation zur Unternehmensgröße berechnet.

	A	B	C	D	
8 Erkenntnisse	6x	2x	0x	0x	
Berechnungsmethodik: gewichteter Durchschnitt					80%

Organisations- & Prozessrisiken

Grobe Fehlkonfigurationen werden in dieser Kategorie mit einem D gewertet. Dazu gehören z.B. das Fehlen einer https-Webseite oder das Deaktivieren der (ohnehin optionalen) Verschlüsselung von E-Mail- oder Dateiübertragungen. Das Fehlen einer (kostenlosen) Mitgliedschaft in der Allianz für Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de) des Bundesamts für Sicherheit in der Informationstechnologie (BSI) wird mit C bewertet. Ebenso wird eine schlechte Anbindung an das Internet (DDoS Gefahr) und das Fehlen der HSTS Unterstützung auf der Webseite mit C bewertet. Dementsprechend wird das Vorhandensein der jeweiligen Punkte mit A bewertet. Auch die Verwendung eines EV Zertifikats geht in die Bewertung mit B (nicht-vorhanden) bzw. A (vorhanden) ein.

	A	B	C	D	
210 Erkenntnisse	55x	92x	61x	2x	
Berechnungsmethodik: gewichteter Durchschnitt					61%

Länderrisiken

Über die Zuordnung von IP-Adressen zu Ländern wird ermittelt, wie stark die Internetpräsenz in den einzelnen Ländern ist. Auf Basis von Länderbewertungen der Corporate Trust wird gewichtet durch die Stärke der Internetpräsenz ein Rating durchgeführt. Die Kategorien IT-Diebstahl, staatliche Spionage, private Spionage, IT- & Kryptogesetzgebung und Betrug durch eigene Mitarbeiter werden einfach gewertet. Die Kategorien Korruption und Rechtsstaatlichkeit zählen je nur zur Hälfte. Dazu kommt der GDPR Status im jeweiligen Land. Über diese Werte wird der Durchschnitt gebildet.

	A	B	C	D	
8 Erkenntnisse	2x	2x	4x	0x	
Berechnungsmethodik: gewichteter Durchschnitt					55%

Erläuterung der Bewertung

Kategorie

Vertrauenswürdige Verschlüsselung

Für jede mögliche verschlüsselte Verbindung (TLS/SSL) wird ein Rating ermittelt. Als Referenz für ein A Rating gilt neben einer aktuellen Version der verwendeten Software die Technische Richtlinie TR-02102 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" des BSI. Wichtigster Punkt in der Ermittlung des Ratings ist die Schlüssellänge der verwendeten asymmetrischen und symmetrischen Schlüssel. Die Verwendung angreifbarer Software (veraltet oder mit bekannten Lücken), falscher Zertifikate (Zertifikat passt nicht zur Webseite) oder von schlechten Algorithmen (SHA1, RC4, null) senken das Rating auf D. Ein nicht vertrauenswürdiges Zertifikat (z.B. selbst-ausgestellt, alte Symantec CA) und die fehlende Unterstützung guter Kryptographie (z.B. PFS, TR-02102-2, Certificate Transparency) wird mit C bewertet. Wenn der Server in seinem Vorschlag eine unsichere Konfiguration vorschlägt wird dies mit einem B (an der Grenze zu C) gewertet. Ebenso werden kleinere Unschönheiten wie eine falsche Reihenfolge der Zertifikatskette oder ein fehlendes EV-Zertifikat mit B bewertet.

	A	B	C	D	
791 Erkenntnisse	396x	170x	128x	97x	
Zusammengefasst pro Host/Port: schlechtester Wert	1x	6x	2x	26x	
Berechnungsmethodik: gewichteter Durchschnitt					14%

Angriffsfläche im Internet

Jeder Dienst, der offen im Internet angeboten wird, ist per se auch ein Sicherheitsrisiko. Beschränkt sich die öffentlich sichtbare Angriffsfläche auf Webseiten und E-Maildienste und sind alle anderen Dienste nicht für das gesamte Internet sichtbar, liefert diese Kategorie ein A. Aufgrund des erhöhten Risikos wird bei global verfügbaren VPN und Dial In Ports, SSH-Zugängen, Telefonie- oder Videokonferenzsystemen das Rating auf B abgesenkt. Gibt es zusätzliche Mailserver (die keinen MX Eintrag haben) oder sind Webserver und Maildienste auf einem System integriert gilt das Gleiche. Werden Dienste für Dateiübertragung, Fernwartung per Bildschirmkontrolle, Datenbanken oder sonstige Applikationen global im Internet exponiert sinkt das Rating auf C. Ein D Rating wird durch offene Ports ausgelöst, bei denen es bereits früher Sicherheitsprobleme gab oder die auf Botnetze und sonstige Remote Access Malware hindeuten. Die Ratings werden pro Server zusammengefasst und dann ein Durchschnitt gebildet.

	A	B	C	D	
12 Erkenntnisse	0x	7x	5x	0x	
Zusammengefasst pro IP: schlechtester Wert	0x	4x	4x	0x	
Berechnungsmethodik: gewichteter Durchschnitt					48%

Mitarbeiterverhalten im Internet

Die Verwendung von Firmen E-Mailadressen im Internet birgt vielfältige gefahren. Insbesondere wenn Privates und Berufliches sich vermischen steigt die Gefahr eines ungewollten Informationsabflusses. Dazu kommt ein eventueller Reputationsschaden. Für die Domains in diesem Bericht wurden folgende problematische Verwendungen entdeckt:

	# verwendete Firmen E-Mailadressen
Soziale Netze & Chatplattformen	6
Video- & Musikportale	0
Filesharingdienste, P2P Netzwerke & Tauschbörsen	9
Spieleplattformen & Gamingforen	0
Hackerforen	0
Datingseiten	4
Erotik- und Pornoseiten	0

Anmerkung: Da die Recherche für diese Daten naturgemäß lückenhaft ist, existiert hier ein nicht unterhebliches Dunkelfeld.

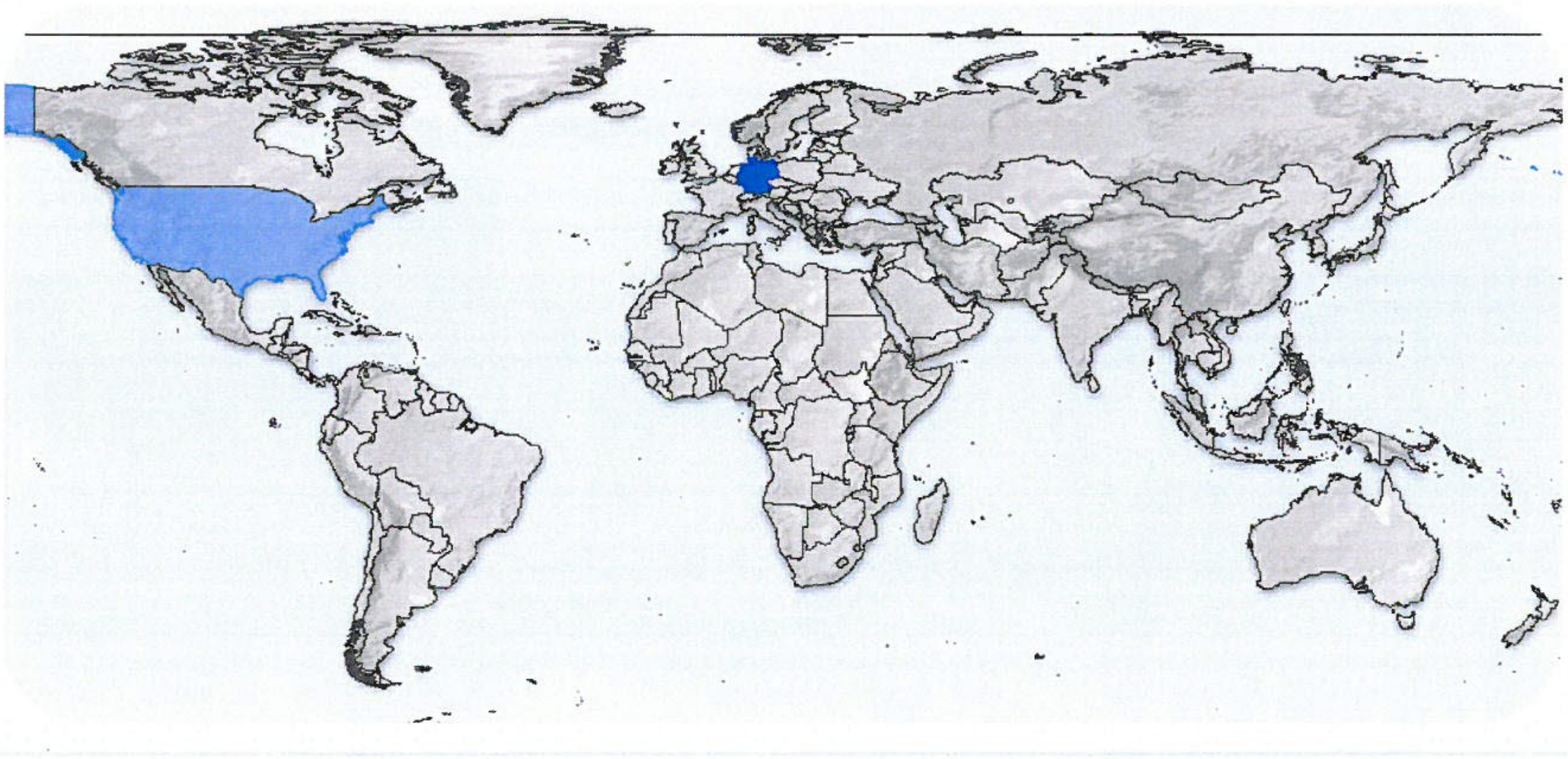
Einbrüche in Webseiten

Die H&S beobachtet teilweise legendiert, teilweise offen mehrere Quellen, auf denen die organisierte Kriminalität Daten austauscht. Insgesamt sind der H&S derzeit 7.070.661.236 E-Mail Adressen aus verschiedenen Einbrüchen in Webseiten und Datenbanken bekannt. Dabei sind etliche Dubletten (etwa 25-35%). Die Einbrüche werden in vier Kategorien mit folgenden Risiken eingeteilt:

	#	Identitäts-diebstahl	Informations-abfluss	Erpressung	Spear-Phishing	Social Engineering	Spam
Einbrüche mit guten Passwörtern im Klartext	30	↑	↑	↑	↑	↗	→
Einbrüche mit leicht entschlüsselbaren Passwörtern bzw. mit schlechten Passwörtern im Klartext	4	↗	→	→	↗	→	→
Einbrüche mit gut verschlüsselten Passwörtern oder sensiblen Daten wie Geburtsdatum, Religion oder sexuelle Ausrichtung	5			↗	↗	↗	→
Datensätze ohne Passwörter und sensible Informationen	47						→

Internet-Fußabdruck

Wichtigste Länder: Deutschland
Weitere Länder: USA



Einordnung der Länder

	Präsenz	DSGVO	IT-Diebstahl	staatliche Spionage	private Spionage	IT- & Krypto-gesetze	Korruption	Betrug	Rechts-staatlichkeit
Deutschland	↗	A	B	C	B	B	A	C	A
USA	↓	C	B	C	D	C	A	C	A

DSGVO: Artikel 44-49 der Europäischen Datenschutzrichtlinie regeln die Datenübermittlung ins Ausland. Länder mit A unterliegen dem DSGVO Regime, für Länder mit B gibt es einen Äquivalenzbeschluss der EU-Kommission. Für Länder mit C gibt es einen partiellen Äquivalensbeschluss, Länder mit D unterliegen den individuell zu regelnden Einzelfallbestimmungen.

IT-Diebstahl: Risiko dass IT-Geräte gestohlenen werden bzw. dass bei gestohlenen oder verlorenen IT-Geräten bzw. Datenträgern nicht der Materialwert im Vordergrund steht, sondern ein Weiterverkauf der Daten an Konkurrenten oder Drittverwerter oder eine Erpressung erfolgt.

Staatliche Spionage: Risiko Opfer einer staatlich finanzierten Informationsbeschaffungsmaßnahme oder einer geheimdienstlichen Wirtschaftsspionage zu werden. Dazu zählt auch die Überwachung von Internet, Mobilfunk und anderen Kommunikationstätigkeiten durch staatliche Stellen im jeweiligen Land.

Private Spionage: Risiko einer Industriespionage durch Konkurrenten, einer Ausspähung durch Detekteien und privatwirtschaftlicher Auskunftsdienste. Dazu zählt auch die Informationsweitergabe an private Stellen durch Vetternwirtschaft und Korruption.

IT- & Kryptogesetze: Risiko durch gesetzliche oder regulatorische Einschränkungen bestimmter IT-Technologien Probleme zu bekommen. Dazu gehört auch das Risiko bei der Einreise, bei Personenkontrollen oder durch andere staatliche Maßnahmen zur Herausgabe von Schlüsselmaterial gezwungen zu werden.

Korruption: Bewertung des Umfangs von Bestechung und Vorteilsnahme auf allen hierarchischen Ebenen in Politik, öffentlicher Verwaltung und Justiz im jeweiligen Land.

Betrug: Risiko Opfer von Betrug, Untreue und Unterschlagung durch eigenen Mitarbeiter in privatwirtschaftlichen Unternehmen im jeweiligen Land zu werden.

Rechtsstaatlichkeit: Bewertung der Unabhängigkeit der Gerichte und der effektiv vorhandenen Grundrechte für Bürger im jeweiligen Land.

Basierend auf Daten © Corporate Trust - Business Risk & Crisis Management GmbH.

Ergebnisübersicht der Computerprüfung

Die Analyse der Server, IP-Adressen und Applikationen / Ports erbrachte folgende 1.190 Erkenntnisse, aufgeschlüsselt nach Ergebnistypen:

Ergebnistyp	#Erkenntnisse	ø
Die IP Adresse ist auf einer Blacklist von bekannt schlechten Adressen	121	0%
Bewertung der Certificate Transparency Unterstützung	91	64%
Bewertung der TLS Versionsunterstützung	91	67%
Extended Validation Zertifikat	91	70%
Stärke der verwendeten symmetrischen Krypographie	91	70%
Vertrauensstatus des Zertifikats	91	91%
Stärke der verwendeten asymmetrischen Kryptographie	91	100%
Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2)	77	51%
Überprüft die Domain mit den meisten URL Reputation Tools (u.a. Google, Microsoft, etc.)	76	93%
HSTS Unterstützung	65	36%
Die Domain ist auf einer Blacklist von bekannt schlechten Domains	56	0%
Der Server ist anfällig für die POODLE Attacke	39	0%
Bewertung der Netzwerkeinbindung nach Anbindungen und beteiligten Firmen	37	95%
Der gebrochene RC4 Algorithmus kann verwendet werden	32	30%
Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2) wird vom Server akzeptiert	31	30%
Zertifikat und Hostnamen passen nicht zusammen	29	0%
Perfect Forward Secrecy wird vom Server nicht empfohlen	29	51%
Es gibt keinen Support für Perfect Forward Secrecy	8	30%
E-Mail (SMTP) Verschlüsselungsoption	8	87%
Die IP Adresse ist auf einer Whiteliste von bekannt guten Adressen	7	100%
Zugang zur verschlüsselten Fernwartung (SSH) für das gesamte Internet sichtbar	5	70%
Bewertung der Reputation der IP Adresse	5	88%
Verschlüsselungsoption bei der Dateiübertragung (FTP)	4	75%
Offener Port für die Dateiübertragung (FTP oder ähnliches) für das gesamte Internet sichtbar	3	27%
Mailserverports wurden auf Servern gefunden, die keinen MX Eintrag haben	2	55%
E-Mail (POP3) Verschlüsselungsoption	2	100%
E-Mail (IMAP) Verschlüsselungsoption	2	100%
Die Domain ist auf einer Whitelist von bekannt guten Domains	2	100%
Bewertung der Reputation der Domain	2	100%
Zugang zu einem Datenbanksystem für das gesamte Internet sichtbar	1	27%
Zusätzliche offene Ports für das gesamte Internet sichtbar	1	44%

Identifizierte Computer

Folgende Computer wurden als sicherheitsrelevant identifiziert und sowohl selbst, als auch die zum Namen gehörigen E-Mail Server (MX-Records) untersucht:

- musterfirma.de[30]
- web01.musterfirma.de[27]
- web1.musterfirma.de[27]
- de01.musterfirma.de[27]
- lc01.musterfirma.de[27]
- superp.musterfirma.de[27]
- oili.musterfirma.de[27]
- com.musterfirma.de[27]
- ef1.musterfirma.de[27]
- bunt.musterfirma.de[27]
- promo.musterfirma.de[27]
- action1.musterfirma.de[27]
- m.musterfirma.de[27]
- mshop.musterfirma.de[27]
- action2.musterfirma.de[27]
- testweb1.musterfirma.de[27]
- static.musterfirma.de[27]
- test.musterfirma.de[27]
- newdny.musterfirma.de[27]
- xp.musterfirma.de[27]
- us.musterfirma.de[27]
- web.musterfirma.com[30]
- ti1.musterfirma.com[27]
- zek.musterfirma.com[27]
- zew.musterfirma.com[27]
- abw.musterfirma.com[27]
- fs1.musterfirma.com[27]
- mx1.musterfirma.com[27]
- nls.musterfirma.com[27]
- securemail.musterfirma.com[27]
- sho1-ka.musterfirma.com[27]
- shop-sg.musterfirma.com[27]
- videoweb.musterfirma.com[27]
- rdis4.musterfirma.com[27]
- autodiscover.musterfirma.com[27]
- meet.musterfirma.com[27]
- confer.musterfirma.com[27]
- bi.musterfirma.com[27]
- web.musterfirma.de[30]
- web02.musterfirma.de[27]
- sozialn.musterfirma.de[27]
- de02.musterfirma.de[27]
- go_todo.musterfirma.de[27]
- superp-plus.musterfirma.de[27]
- cms.musterfirma.de[27]
- zrn.musterfirma.de[27]
- ef2.musterfirma.de[27]
- vertr.musterfirma.de[27]
- it.musterfirma.de[27]
- action1plus.musterfirma.de[27]
- mobil.musterfirma.de[27]
- at.musterfirma.de[27]
- sho1.musterfirma.de[27]
- action3.musterfirma.de[27]
- banne.musterfirma.de[27]
- ueberuns.musterfirma.de[27]
- web.musterfirma.de[27]
- alphacent.musterfirma.de[27]
- musterfirma.com[30]
- newdny.musterfirma.com[27]
- mail.musterfirma.com[27]
- vertrieb.musterfirma.com[27]
- teststage2.musterfirma.com[27]
- info1.musterfirma.com[27]
- remote.musterfirma.com[27]
- media1.musterfirma.com[27]
- ma1.musterfirma.com[27]
- web34.musterfirma.com[27]
- shop-kr.musterfirma.com[27]
- sip.musterfirma.com[27]
- rdis1.musterfirma.com[27]
- web.musterfirma.com[27]
- lyncdiscover.musterfirma.com[27]
- dialin.musterfirma.com[27]
- av.musterfirma.com[27]

Identifizierte Computer

Zur Identifizierung der sicherheitsrelevanten Computer werden verschiedene Indizien bewertet und abgewogen. Dieser Computer wurde als sicherheitsrelevant eingestuft, weil

1. er in einem sehr kleinen Netzwerksegment liegt, in dem auch wichtige Server der Domain liegen
2. er in einem Netzwerksegment liegt, in dem die Domain im "whois"-Eintrag erwähnt wird
3. er in einem Netzwerksegment liegt, in dem die reverse Einträge der meisten Server auf die Domain zeigen
4. er im gleichen Netzwerk liegt, in dem auch wichtige Server der Domain liegen
5. er in einem Netzwerksegment liegt, in dem Firmenname oder -adresse im "whois"-Eintrag erwähnt werden
6. er einen Namen unterhalb der Domain hat
7. sich die Namen nur in der Länderkennzeichnung unterscheiden
8. der Name gleiche Namensbestandteile mit der Domain hat
9. die E-Mail Adresse des Domainverwalters identisch ist und dieser zur Domain gehört
10. die E-Mail Adresse des Domainverwalters identisch ist
11. die Domain des Domainverwalters identisch ist und dieser zur Domain gehört
12. die Domain des Domainverwalters identisch ist
13. er den gleichen Mailserver verwendet
14. sein Mailserver die gleiche IP-Adresse verwendet
15. die Namensauflösung auf die Domain verweist
16. er im gleichen Netzwerksegment liegt
17. er die gleiche umgekehrte Namensauflösung hat
18. der Name im gleichen Zertifikat auftaucht
19. der Aussteller des Zertifikats derselbe ist
20. auf der Webseite auf die Domain verlinkt wird
21. die Webseiten durch Umleitungen miteinander verbunden sind
22. auf der Domain auf diesen Computer verlinkt wird
23. der gleiche Nameserver verwendet wird
24. der gleiche Nameserver verwendet wird und dieser zur Domain gehört
25. der Aussteller des Zertifikats derselbe ist und dieser zur Domain gehört
26. er den gleichen Mailserver verwendet und dieser zur Domain gehört
27. der Name unterhalb einer Domain ist, die als zugehörig identifiziert wurde
28. die umgedrehte Namensauflösung auf die Domain zeigt
29. alle möglichen Namen aus der umgedrehte Namensauflösung auf die Domain zeigen
30. er manuell angegeben wurde
31. das Impressum mindestens eine gleiche VAT-ID enthält
32. das Impressum mindestens eine gleiche Telefonnummer enthält
33. das Impressum mindestens einen gleichen Gerichtsstand enthält

Dienstleisterübersicht

Serverbetrieb:

- abcd.de

Namensauflösung:

- abcd.com
- abcd.de

E-Mail Provider:

- abcd.de

Analysten-Details für 10.11.12.35 [US] (superp-plus.musterfirma.de)

Folgende offene Ports wurden bei der Untersuchung detektiert: 22:ssh, 80:http, 443:https(TLS)

- Die IP ist mit 3 verschiedenen Anbindungen im Internet. Firmen aus 2 Ländern (NL,US) sind beteiligt. Ergebnis: 79% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: superp-plus.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 128. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 3: 100% (Gewissheit:90% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: superp-plus.musterfirma.de Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Zugang zur verschlüsselten Fernwartung (SSH für das gesamte Internet sichtbar: Port 22: ssh. Ergebnis: 70% (Gewissheit:80%
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/ 10.11.12.35 Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei Suomispam Blacklist auf der Blackliste von bekannt schlechten Adressen (Erklärung: 20180729 www.kuumachat.com escalation google-spam-cloud-services. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei Suomispam Graylist auf der Blackliste von bekannt schlechten Adressen (Erklärung: 20180720 www.kuumachat.com. Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 11.10.10.78 [DE] (action2.musterfirma.de, action3.musterfirma.de)

Folgende offene Ports wurden bei der Untersuchung detektiert: 21:ftp(TLS), 22:ssh, 25:smtp(TLS), 80:http, 110:pop3(TLS), 143:imap(TLS), 443:https(TLS), 465:smtps(TLS), 587:submission(TLS), 993:imaps(TLS), 995:pop3s(TLS), 3306:mysql, 5432:postgresql(TLS)

- Die IP ist mit 5 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: action.musterfirma.dee). Ergebnis: 100% (Gewissheit:90% (Ports 443,25,21,587,143,995,993,110,465)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis:100% (Gewissheit:100% (Ports 443,25,21,587,143,995,993,110,5432,465)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 128. Ergebnis: 100% (Gewissheit:100% (Ports 443,25,21,587,143,995,993,110,5432,465)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Ports 443,25,587,5432,465)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 2. 79% (Gewissheit:90% (Port 443
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0. 100% (Gewissheit:100% (Ports 443,25,21,587,143,995,993,110,5432,465)
- HSTS Unterstützung (DNS Name: action3.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Ports 443,25,21,587,143,995,993,110,5432,465)
- E-Mail (SMTP Verschlüsselungsoption mit STARTTLS. Ergebnis: 100% (Gewissheit:100% (Port 25)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 3): 100% (Gewissheit:90%) (Ports 25,21,587,143,995,993,110,465)
- Zertifikat und Hostname passen nicht zusammen(DNS Name: action3.musterfirma.de). Ergebnis: 0% (Gewissheit:75%) (Ports 25,21,587,143,995,993,110,465)
- Verschlüsselungsoption bei der FTP-Dateiübertragung (STARTTLS. Ergebnis: 100% (Gewissheit:100% (Port 21)
- IMAP Verschlüsselungsoption mit STARTTLS. Ergebnis: 100% (Gewissheit:100% (Port 143)
- POP3 Verschlüsselungsoption mit STARTTLS. Ergebnis: 100% (Gewissheit:100%) (Port 110)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name:action3.musterfirma.de). Ergebnis: 30% (Gewissheit:90% (Port 5432)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0): 30% (Gewissheit:90%) (Port 5432)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: action2.musterfirma.de. Ergebnis: 100% (Gewissheit:90%) (Ports 443,25,21,587,143,995,993,110,465)
- HSTS Unterstützung (DNS Name: action2.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: action2.musterfirma.de Ergebnis: 0% (Gewissheit:75%) (Ports 25,21,587,143,995,993,110,5432,465)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: action2.musterfirma.de. Ergebnis: 30% (Gewissheit:90% (Port 5432
- Mailserverports wurden auf Servern gefunden, die keinen MX Eintrag haben. Ergebnis: 55% (Gewissheit:80%)
- Offene Port für die Dateiübertragung (FTP oder ähnliches für das gesamte Internet sichtbar: 21:ftp. Ergebnis: 27% (Gewissheit:80%)
- Zugang zur verschlüsselten Fernwartung (SSH für das gesamte Internet sichtbar: Port 22: ssh. Ergebnis: 70% (Gewissheit:80%)
- Zugang zu einem Datenbanksystem für das gesamte Internet sichtbar: 5432:postgresql. Ergebnis: 27% (Gewissheit:80%
- Die IP Adresse ist bei DNSWL.org IP Whitelist auf der Whiteliste von bekannt guten Adressen (Erklärung: autopromoted.invalid https://dnswl.org/s/?s=1004. Ergebnis: 100% (Gewissheit:100%
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Reputation der IP wird bei SenderScore Reputationlist mit 81% bewertet (Kommentar: Reputation: 81%. Gewissheit:100%
- Die Domain ist bei RFC-Clueless (RFC² whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%

Analysten-Details für 10.10.12.80 [DE] (bunt.musterfirma.de)

Folgende offene Ports wurden bei der Untersuchung detektiert: 21:ftp(TLS), 22:ssh, 80:http, 443:https (TLS)

- Die IP ist mit 3 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (EU,NL,US) sind beteiligt. Ergebnis: 86% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: musterfirma.dee). Ergebnis: 100% (Gewissheit:90% (Ports 443,21
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048 Ergebnis: 100% (Gewissheit:100% (Ports 443,21)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112 Ergebnis: 58% (Gewissheit:100% (Ports 443,21)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 2: 79% (Gewissheit:90% (Ports 443,21
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: bunt.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Ports 443,21
- Verschlüsselungsoption bei der FTP-Dateiübertragung (STARTTLS. Ergebnis: 100% (Gewissheit:100% (Port 21
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Port 21
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2) wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100%) (Port 21)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: bunt.musterfirma.de Ergebnis: 0% (Gewissheit:75%) (Port 21)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: SSL v3: 10% (Gewissheit:100% (Port 21
- Offene Port für die Dateiübertragung (FTP oder ähnliches für das gesamte Internet sichtbar: 21:ftp. Ergebnis: 27% (Gewissheit:80%
- Zugang zur verschlüsselten Fernwartung (SSH für das gesamte Internet sichtbar: Port 22: ssh. Ergebnis: 70% (Gewissheit:80%
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Domain ist bei RFC-Clueless (RFC² whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%

Analysten-Details für 11.10.9.130 [US] (superp.musterfirma.de)

Folgende offene Ports wurden bei der Untersuchung detektiert: 22:ssh, 80:http, 443:https (TLS)

- Die IP ist mit 2 verschiedenen Anbindungen im Internet. Firmen aus 1 Ländern (US) sind beteiligt. Ergebnis: 51% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name:superp.musterfirma.de). Ergebnis: 30% (Gewissheit:90%) (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048 Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112 Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: superp.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Zugang zur verschlüsselten Fernwartung (SSH für das gesamte Internet sichtbar: Port 22: ssh. Ergebnis: 70% (Gewissheit:80%
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei Spamhaus ZEN Combined Block List auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://www.spamhaus.org/query/ip/ 11.10.9.130. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/11.10.9.130. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei Spamhaus PBL Policy Block List auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://www.spamhaus.org/query/ip/ 11.10.9.130. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.8.8.193 [DE] (nls.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 80:http, 443:https(TLS)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,PL,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: nls.musterfirma.com). Ergebnis: 100% (Gewissheit:90% (Port 443
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 128. Ergebnis: 100% (Gewissheit:100% (Port 443
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 2: 79% (Gewissheit:90% (Port 443
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0: 100% (Gewissheit:100% (Port 443
- HSTS Unterstützung. Ergebnis: 100% (Gewissheit:100% (Port 443
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443
- Die IP Adresse ist bei DNSWL.org IP Whitelist auf der Whiteliste von bekannt guten Adressen (Erklärung: optivo.de https://dnswl.org/s/?s=9811. Ergebnis: 100% (Gewissheit:100%
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Domain ist bei RFC-Clueless (RFC²postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%

Analysten-Details für 13.13.12.193 [DE] (mail.srv2.de)

Folgende offene Ports wurden bei der Untersuchung detektiert: 25:smtp(TLS)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,PL,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- E-Mail (SMTP) Verschlüsselungsoption mit STARTTLS. Ergebnis: 100% (Gewissheit:100%) (Port 25)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: mail.srv2.de). Ergebnis: 100% (Gewissheit:90%) (Port 25)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6): 2048). Ergebnis: 100% (Gewissheit:100%) (Port 25)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 128). Ergebnis: 100% (Gewissheit:100%) (Port 25)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 3): 100% (Gewissheit:90%) (Port 25)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 25)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90%) (Port 25)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei Hostkarma no blacklist auf der Whiteliste von bekannt guten Adressen (Erklärung: whitelisted). Ergebnis: 100% (Gewissheit:100%)
- Die Reputation der Domain wird bei Hostkarma mit 100% bewertet (Kommentar: Reputation: 100%). Gewissheit:100%
- Die Domain ist bei RFC-Clueless (RFC²) whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 13.13.9.19 [DE] (media1.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 80:http, 443:https(TLS)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,PL,SE,US) sind beteiligt. Ergebnis: 100 (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name:media1.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 128. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 3): 100% (Gewissheit:90%) (Port 443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: media1.musterfirma.com. Ergebnis: 0% (Gewissheit:75%) (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei Hostkarma no blacklist auf der Whiteliste von bekannt guten Adressen (Erklärung: whitelisted. Ergebnis: 100% (Gewissheit:100%)
- Die Reputation der IP wird bei Hostkarma mit 100% bewertet (Kommentar: Reputation: 100%. Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 13.12.11.194 [DE] (mforwad.abcd.de)

Folgende offene Ports wurden bei der Untersuchung detektiert: 25:smtp

- Die IP ist mit 6 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- E-Mail (SMTP) Verschlüsselungsoption mit STARTTLS. Ergebnis: 0% (Gewissheit:100%) (Port 25)
- Die IP Adresse ist bei DNSWL.org IP Whitelist auf der Whiteliste von bekannt guten Adressen (Erklärung:abcd.de https://dnswl.org/5917. Ergebnis: 100% (Gewissheit:100%
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei Backscatterer.org auf der Blackliste von bekannt schlechten Adressen (Erklärung: Sorry13.12.11.194 is blacklisted at http://www.backscatterer.org/?ip= 13.12.11.194. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei nsZones.com DNSWL auf der Whiteliste von bekannt guten Adressen (Erklärung: Listed in White List - see http://db.nsZones.com/wl.ip?13.12.11.194. Ergebnis: 100% (Gewissheit:100%
- Die IP Adresse ist bei Hostkarma no blacklist auf der Whiteliste von bekannt guten Adressen (Erklärung: whitelisted. Ergebnis: 100% (Gewissheit:100%
- Die Reputation der IP wird bei Hostkarma mit 100% bewertet (Kommentar: Reputation: 100%. Gewissheit:100%
- Die Reputation der IP wird bei SenderScore Reputationlist mit 62% bewertet (Kommentar: Reputation: 62%). Gewissheit:100%
- Die Domain ist bei Hostkarma no blacklist auf der Whiteliste von bekannt guten Adressen (Erklärung: No Blacklist listedabcd.dee See http://wiki.junkemailfilter.com/index.php/Spam_DNS_Lists). Ergebnis: 100% (Gewissheit:100%)
- Die Reputation der Domain wird bei Hostkarma mit 100% bewertet (Kommentar: No Blacklist listed abcd.de See http://wiki.junkemailfilter.com/index.php/Spam_DNS_Lists. Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%

Analysten-Details für 13.12.12.194 [DE] [newdny.musterfirma.de, newdny.musterfirma.com, remote.musterfirma.com, ma1.musterfirma.com, autodiscover.musterfirma.com]

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https[TLS], 8443:https-alt[TLS]

- Die IP ist mit 7 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: mobile.musterfirma.com. Ergebnis: 100% (Gewissheit:90% (Port 443
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Ports 443,8443
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Ports 443,8443
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Ports 443,8443
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Ports 443,8443
- Perfect Forward Secrecy wird vom Server nicht empfohlen. Ergebnis: 51% (Gewissheit:100% (Ports 443,8443
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Ports 443,8443
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0. 30% (Gewissheit:90% (Ports 443,8443
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Ports 443,8443
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: SSL v2): 0% (Gewissheit:100%) (Ports 443,8443)
- HSTS Unterstützung (DNS Name: remote.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Ports 443,8443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90%) (Ports 443,8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: remote.musterfirma.com). Ergebnis: 30% (Gewissheit:90%) (Port 8443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: remote.musterfirma.com). Ergebnis: 0% (Gewissheit:75%) (Port 8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: newdny.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: newdny.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Ports 443,8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: newdny.musterfirma.com. Ergebnis: 30% (Gewissheit:90%) (Port 8443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: newdny.musterfirma.com). Ergebnis: 0% (Gewissheit:75%) (Port 8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: newdny.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: newdny.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Ports 443,8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: newdny.musterfirma.de). Ergebnis: 30% (Gewissheit:90%) (Port 8443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: newdny.musterfirma.de. Ergebnis: 0% (Gewissheit:75%) (Port 8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: autodiscover.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: autodiscover.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Ports 443,8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: autodiscover.musterfirma.com. Ergebnis: 30% (Gewissheit:90%) (Port 8443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: autodiscover.musterfirma.com Ergebnis: 0% (Gewissheit:75%) (Port 8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: ma1.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: ma1.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Ports 443,8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: ma1.musterfirma.com. Ergebnis: 30% (Gewissheit:90%) (Port 8443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: ma1.musterfirma.com). Ergebnis: 0% (Gewissheit:75%) (Port 8443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 13.12.12.195 [DE] (bi.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https(TLS)

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: bi.musterfirma.com). Ergebnis: 100% (Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Perfect Forward Secrecy wird vom Server nicht empfohlen. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: SSL v2): 0% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: bi.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU] Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 13.12.12.196 [DE] (ti1.musterfirma.com, abw.musterfirma.com, info1.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 80:http, 443:https(TLS), 8443:https-alt(TLS)

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100%(Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: info1.musterfirma.com). Ergebnis: 100% (Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Ports 443,8443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Ports 443,8443)
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Ports 443,8443)
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Ports 443,8443)
- Perfect Forward Secrecy wird vom Server nicht empfohlen. Ergebnis: 51% (Gewissheit:100% (Ports 443,8443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Ports 443,8443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0. 30% (Gewissheit:90% (Ports 443,8443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Ports 443,8443
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: SSL v2): 0% (Gewissheit:100%) (Ports 443,8443)
- HSTS Unterstützung (DNS Name: info1.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Ports 443,8443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90%) (Ports 443,8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: info1.musterfirma.com. Ergebnis: 30% (Gewissheit:90%) (Port 8443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: info1.musterfirma.com. Ergebnis: 0% (Gewissheit:75%) (Port 8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: abw.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: abw.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Ports 443,8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: abw.musterfirma.com. Ergebnis: 30% (Gewissheit:90%) (Port 8443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: abw.musterfirma.com. Ergebnis: 0% (Gewissheit:75%) (Port 8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name:ti1.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: ti1.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Ports 443,8443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 6, DNS-Name: ti1.musterfirma.com. Ergebnis: 30% (Gewissheit:90%) (Port 8443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: ti1.musterfirma.com). Ergebnis: 0% (Gewissheit:75%) (Port 8443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%

Analysten-Details für 10.19.0.134 [DE] (videoweb.musterfirma.com, lyncdiscover.musterfirma.com, meet.musterfirma.com, dialin.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https(TLS)

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100%
- (Gewissheit:95%) Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name:videoweb.musterfirma.com). Ergebnis: 100%(Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Perfect Forward Secrecy wird vom Server nicht empfohlen. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: SSL v2: 0% (Gewissheit:100% (Port 443)
- HSTS Unterstützung. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: dialin.musterfirma.com. Ergebnis: 100% (Gewissheit:90%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: meet.musterfirma.com. Ergebnis: 100% (Gewissheit:90%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: lyncdiscover.musterfirma.com. Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: lyncdiscover.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.0.134. Ergebnis: 0% (Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%
- Die Domain ist bei RFC-Clueless (RFC²postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%

Analysten-Details für 10.19.1.194 [DE] (fs1.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 21:ftp

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Verschlüsselungsoption bei der FTP-Dateiübertragung (STARTTLS). Ergebnis: 0% (Gewissheit:100%) (Port 21)
- Offene Port für die Dateiübertragung (FTP oder ähnliches) für das gesamte Internet sichtbar: 21:ftp. Ergebnis: 27% (Gewissheit:80%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.191.194). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.1.195 [DE] mail.musterfirma.com mx1.musterfirma.com, securemail.musterfirma.com

Folgende offene Ports wurden bei der Untersuchung detektiert: 25:smtp(TLS), 443:https(TLS)

- Die IP ist mit 7 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: mailmusterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Ports 443,25)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Ports 443,25)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Ports 443,25)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Ports 443,25)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Ports 443,25
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Ports 443,25
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Ports 443,25)
- HSTS Unterstützung (DNS Name: mail.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Ports 443,25
- E-Mail (SMTP) Verschlüsselungsoption mit STARTTLS. Ergebnis: 100% (Gewissheit:100%) (Port 25)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: mx1.musterfirma.comm). Ergebnis: 100% (Gewissheit:90%) (Ports 443,25)
- HSTS Unterstützung (DNS Name: mx1.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: securemail.musterfirma.com. Ergebnis: 100% (Gewissheit:90%) (Ports 443,25)
- HSTS Unterstützung (DNS Name: securemail.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Mailserverports wurden auf Servern gefunden, die keinen MX Eintrag haben. Ergebnis: 55% (Gewissheit:80%
- Die IP Adresse ist bei DNSWL.org IP Whitelist auf der Whiteliste von bekannt guten Adressen (Erklärung: autopromoted.invalid https://dnswl.org/s/?s=1004. Ergebnis: 100% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Reputation der IP wird bei SenderScore Reputationlist mit 100% bewertet (Kommentar: Reputation: 100%. Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.1.96 [DE] (zew.musterfirma.com, teststage2.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https(TLS), 8080:http-proxy

- Die IP ist mit 7 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,SE,US sind beteiligt. Ergebnis: 100% (Gewissheit:95%
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: teststage2.musterfirma.com. Ergebnis: 100% (Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Port 443
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.1): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: teststage2.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: miv1.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: miv1.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Zusätzliche offene Ports für das gesamte Internet sichtbar: 8080:http-proxy. Ergebnis: 44% (Gewissheit:80%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.1.96. Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.1.72 [DE] (zek.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https(TLS)

- Die IP ist mit 7 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: mis1musterfirma.comm). Ergebnis: 100% (Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 10000. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Es gibt keinen Support für Perfect Forward Secrecy. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: : 40% (Gewissheit:100% (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.1.72. Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.1.97 [DE] (vertrieb.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https(TLS)

- Die IP ist mit 7 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: vertrieb.musterfirma.com). Ergebnis: 100%) (Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100%) (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Perfect Forward Secrecy wird vom Server nicht empfohlen. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: SSL v2): 0% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: vertrieb.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.1.97. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.1.98 [DE] (rdis1.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https(TLS)

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100%
- (Gewissheit:95%) Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: wdes1musterfirma.comm). Ergebnis: 100%(Gewissheit:90%) (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Es gibt keinen Support für Perfect Forward Secrecy. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Perfect Forward Secrecy wird vom Server nicht empfohlen. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: rdis1.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.1.98. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.128.19 [DE] (web34.musterfirma.com, sho1-ka.musterfirma.com, sho1-kr.musterfirma.com, sho1-sg.musterfirma.com, rdis4.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https[TLS]

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis:100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: wdes2musterfirma.comm). Ergebnis: 100%(Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Es gibt keinen Support für Perfect Forward Secrecy. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Perfect Forward Secrecy wird vom Server nicht empfohlen. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: SSL v3): 10% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: rdis4.musterfirma.com. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: shop-sg.musterfirma.com. Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: sho1-sg.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: sho1-kr.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: sho1-kr.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: sho1-ka.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: sho1-ka.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name:web34.musterfirma.com. Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: web34.musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.128.19. Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%

Analysten-Details für 10.19.129.1 [DE] (sip.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https(TLS)

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100%
- (Gewissheit:95%) Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: sip.musterfirma.com). Ergebnis: 100%) (Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100%) (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der gebrochene RC4 Algorithmus kann verwendet werden. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Perfect Forward Secrecy wird vom Server nicht empfohlen. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: SSL v3: 10% (Gewissheit:100% (Port 443)
- HSTS Unterstützung. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net10.19.129.1. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.2 [DE] (confer.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https(TLS)

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: confer.musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 10000. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Es gibt keinen Support für Perfect Forward Secrecy. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Keiner der vom BSI empfohlenen Algorithmen (TR-02102-2 wird vom Server akzeptiert. Ergebnis: 30% (Gewissheit:100% (Port 443)
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 0: 30% (Gewissheit:90% (Port 443)
- Der Server ist anfällig für die POODLE Attacke. Ergebnis: 0% (Gewissheit:100% (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version:: 40% (Gewissheit:100% (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.129.2. Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.3 [DE] (av.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 443:https

- Die IP ist mit 8 verschiedenen Anbindungen im Internet. Firmen aus 4 Ländern (DE,NL,SE,US) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.129.3). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.4 [DE] (banne.musterfirma.de)

- Die IP ist mit 1 verschiedenen Anbindungen im Internet. Firmen aus 1 Ländern (DE) sind beteiligt. Ergebnis: 30% (Gewissheit:95%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.5 [DE] (de01.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.129.5). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.6 [DE] (de02.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/10.19.129.6). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.7 [DE] (ef1.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.57 [DE] (ef2.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%) Die
- IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.58 [DE] (web1.musterfirma.de)

Folgende offene Ports wurden bei der Untersuchung detektiert: 22:ssh, 80:http, 443:https(TLS)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: www1musterfirma.dee). Ergebnis: 100% (Gewissheit:90% (Port 443
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 128. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 2): 79% (Gewissheit:90%) (Port 443)
- Zertifikat und Hostnamen passen nicht zusammen (DNS Name: www1.musterfirma.de). Ergebnis: 0% (Gewissheit:75%) (Port 443)
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: www1.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90% (Port 443)
- Zugang zur verschlüsselten Fernwartung (SSH für das gesamte Internet sichtbar: Port 22: ssh. Ergebnis: 70% (Gewissheit:80%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.59 [DE] (test.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%) Die
- IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.60 [DE] (zrn.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%) Die
- IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.61 [DE] (static.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%) Die
- IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.62 [DE] (cms.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei SPFBL.net RBL auf der Blackliste von bekannt schlechten Adressen (Erklärung: https://matrix.spfbl.net/217.69.83.69). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.63 [DE] (web01.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%) Die
- IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Domain ist bei RFC-Clueless (RFC²) postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.64 [DE] (web02.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.65 [DE] (lic01.musterfirma.de)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]). Ergebnis: 0% (Gewissheit:100%)
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted). Ergebnis: 0% (Gewissheit:100%)
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%)

Analysten-Details für 10.19.129.66 [DE] (ueberuns.musterfirma.de, musterfirma.com, www.musterfirma.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 80:http, 443:https(TLS)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: www.musterfirma.com Ergebnis: 100% (Gewissheit:90% (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 2: 79% (Gewissheit:90% (Port 443
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: wwwmusterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: musterfirma.com). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: musterfirma.com). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%
- Die Domain ist bei RFC-Clueless (RFC²whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Domain ist bei RFC-Clueless (RFC²postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%

Analysten-Details für 10.19.129.67 [DE] (musterfirma.de www.musterfirma.de, socialn.musterfirma.de, go_todo.musterfirma.de, oili.musterfirma.de, com.musterfirma.de, vertr.musterfirma.de, promo.musterfirma.de, it.musterfirma.de, action1.musterfirma.de, action1plus.musterfirma.de, m.musterfirma.de, mobil.musterfirma.de, mshop.musterfirma.de, at.musterfirma.de, sho1.musterfirma.de, testweb1.musterfirma.de, xp.musterfirma.de, alphacent.musterfirma.de, us.musterfirma.de)

Folgende offene Ports wurden bei der Untersuchung detektiert: 80:http, 443:https(TLS)

- Die IP ist mit 4 verschiedenen Anbindungen im Internet. Firmen aus 3 Ländern (DE,PL,SE) sind beteiligt. Ergebnis: 100% (Gewissheit:95%)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: zukunftsprogramm musterfirma.dee). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- Stärke der verwendeten asymmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge (ECC=Länge im Quadrat/6: 2048. Ergebnis: 100% (Gewissheit:100% (Port 443)
- Stärke der verwendeten symmetrischen Kryptographie (Kleinste akzeptierte Schlüssellänge: 112. Ergebnis: 58% (Gewissheit:100% (Port 443)
- Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2. Ergebnis: 51% (Gewissheit:100% (Port 443
- Bewertung der Certificate Transparency Unterstützung (Anzahl SCTS: 3: 100% (Gewissheit:90% (Port 443
- Bewertung der TLS Versionsunterstützung (Kleinste akzeptierte SSL Version: TLS 1.0): 100% (Gewissheit:100%) (Port 443)
- HSTS Unterstützung (DNS Name: alphacent.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Extended Validation Zertifikat. Ergebnis: 70% (Gewissheit:90%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: us.musterfirma.de Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: us.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: xp.musterfirma.de. Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: xp.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: socialn.musterfirma.de Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: facebook.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: oili.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: oili.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: go_todo.musterfirma.de Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: go_todo.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: www.musterfirma.de. Ergebnis: 100%

(Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: www.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: com.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: com.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: mshop.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: mshop.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: testweb1.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: shoptest.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: shop.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: shop.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: nl.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: nl.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: mobil.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: mobil.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: action1plus.musterfirma.de Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: action1plus.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: action1.musterfirma.de. Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: action1.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: it.musterfirma.de. Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: it.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: promo.musterfirma.de Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: promo.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: vertr.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: vertr.musterfirma.de). Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Bewertung des Vertrauensstatus des Zertifikats (Anzahl Fehler bei der Validierung: 0, DNS-Name: m.musterfirma.de). Ergebnis: 100% (Gewissheit:90%) (Port 443)
- HSTS Unterstützung (DNS Name: m.musterfirma.de. Ergebnis: 30% (Gewissheit:100%) (Port 443)
- Die IP Adresse ist bei tuxad hartkore.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei rbl.rbldns.ru auf der Blackliste von bekannt schlechten Adressen (Erklärung: RBLDNS Server v1.1.0. Author VDV [Site: WWW.RBLDNS.RU]. Ergebnis: 0% (Gewissheit:100%
- Die IP Adresse ist bei tuxad dunk.dnsbl auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Ergebnisse von 67 URL Reputation Tools: 60x gut, 0x schlecht, 7x unbekannt. Ergebnis: 93% (Gewissheit:90%
- Die Domain ist bei RFC-Clueless (RFC² whois Blacklist for bad configured whois records auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%
- Die Domain ist bei RFC-Clueless (RFC² postmaster Blacklist for bad configured postmaster Mailbox auf der Blackliste von bekannt schlechten Adressen (Erklärung: blacklisted. Ergebnis: 0% (Gewissheit:100%

Kritische Leaks

Für die Domains in diesem Bericht sind insgesamt 30 Accounts in der Kategorie "Rot" bekannt, bei denen die Passwörter im Klartext vorliegen.

M___@mforwad.abcd.de	a___@musterfirma.com	a___@musterfirma.com	a___@musterfirma.com
a___@musterfirma.com	b___@musterfirma.com	c___@musterfirma.com	c___@musterfirma.com
c___@musterfirma.com	c___@musterfirma.com	g___@musterfirma.com	h___@musterfirma.com
h___@musterfirma.com	h___@musterfirma.com	i___@musterfirma.com	k___@musterfirma.com
m___@musterfirma.com	m___@musterfirma.com	m___@musterfirma.com	m___@musterfirma.com
t___@musterfirma.com	m___@musterfirma.com	r___@musterfirma.com	r___@musterfirma.com
u___@musterfirma.com	t___@musterfirma.com	t___@musterfirma.com	t___@musterfirma.com

m

Problematische Leaks

Für die Domains in diesem Bericht sind insgesamt 4 Accounts bekannt, bei denen die Passwörter in leicht entschlüsselbarer Form vorliegen oder für die einfache Klartextpasswörter (wie PINs oder sechsstellige Passwörter) bekannt sind.

a___@musterfirma.com	b___@musterfirma.com	m___@musterfirma.com	s___@musterfirma.com

Unschöne Leaks

Für die Domains in diesem Bericht sind insgesamt 5 Accounts bekannt, bei denen entweder gut verschlüsselte Passwörter (Angriffsdauer zur Entschlüsselung > 1 Monat) oder sensible Daten vorliegen.

c___@musterfirma.com	c___@musterfirma.com	i___@musterfirma.com	k___@musterfirma.com
p___@musterfirma.de			

E-Mail only Leaks

Für die Domains in diesem Bericht gibt es insgesamt 47 Accounts bei denen nur E-Mailadresse bekannt geworden ist.

K___@musterfirma.com	a___@musterfirma.com	a___@musterfirma.com	a___@musterfirma.com
a___@musterfirma.com	a___@musterfirma.com	b___@musterfirma.com	b___@musterfirma.com
c___@musterfirma.com	c___@musterfirma.com	d___@musterfirma.com	d___@musterfirma.com
d___@musterfirma.com	f___@musterfirma.com	g___@musterfirma.com	g___@musterfirma.com
h___@musterfirma.com	i___@musterfirma.de	j___@musterfirma.com	j___@musterfirma.com
j___@musterfirma.com	j___@musterfirma.com	k___@musterfirma.com	k___@musterfirma.com
k___@musterfirma.com	m___@musterfirma.com	m___@musterfirma.com	m___@musterfirma.de
m___@musterfirma.com	m___@musterfirma.com	m___@musterfirma.com	n___@musterfirma.com
p___@musterfirma.com	p___@musterfirma.com	p___@musterfirma.de	r___@musterfirma.com
r___@musterfirma.com	r___@musterfirma.com	s___@musterfirma.com	t___@musterfirma.com
t___@musterfirma.com	t___@musterfirma.com	t___@musterfirma.com	u___@musterfirma.com
u___@musterfirma.com	v___@musterfirma.com	w___@musterfirma.com	