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

MUSTERFA AG

Teststraße 2b, 1000 Berlin

Dieser Bericht wurde am 07.08.2018 mit einem Datenstand vom 30.06.2018 23:44-05.08.2018 08:53 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 substantielle Risiken.

DIN EN ISO 9001 * AZAV * TAW Cert GmbH
Zertifikat Nr.
QM-030104
AZ-030104
Zertifiziert seit 2004

MUSTERFA

Teststraße 2b, 1000 Berlin

Basis für die Bewertung waren die folgenden eingegebenen Daten:

Basis Domains:	musterfa.com
Größe:	250-999 Mitarbeiter
Vergleich 1:	vgl.com Vergleich1 AG

Bewertung in der Übersicht

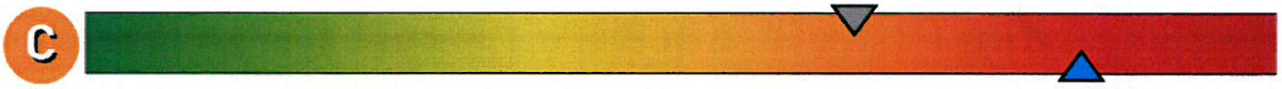
Die Ergebnisse eventuell angegebener Vergleichsunternehmen sind in blau eingezeichnet.

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:

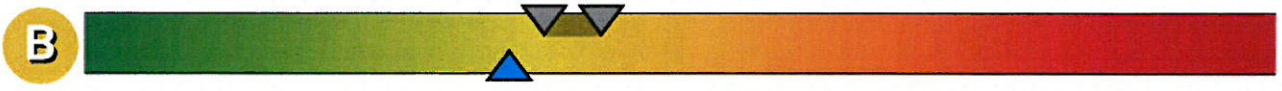
Konkrete Gefährdungslage - Bewertung aller Indizien die auf einen laufenden Angriff oder eine akute Angriffsmöglichkeit hindeuten

Reputation im Cyberraum - Bewertung der Reputation des Unternehmens im Internet

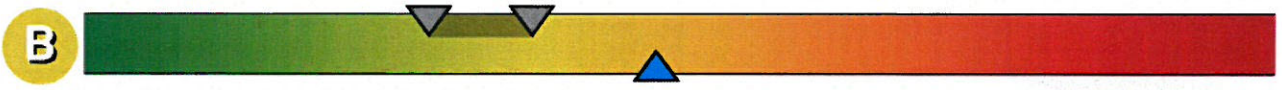


Mitarbeiterverhalten im Cyberspace - Bewertung aller Indizien, wie vorsichtig die Mitarbeiter des Unternehmens im Internet auftreten.

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

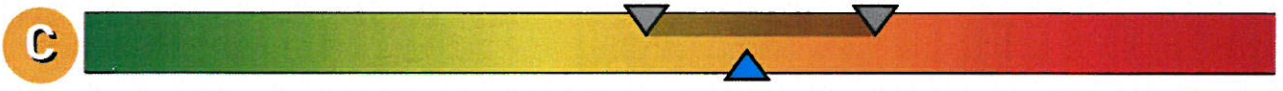


Länderrisiken - Bewertung der Risiken die durch Präsenz in verschiedenen Jurisdiktionen und Kulturkreisen entstehen



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 8 IP Adressen, 34 Servernamen und 106 verschiedenen Applikationen / Ports untersucht. Insgesamt wurden 211 Prüfprogramme abgearbeitet. Dabei wurden insgesamt 492 Erkenntnisse (gute wie schlechte) generiert, davon 474 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	
170 Erkenntnisse	108x	26x	36x	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. Dies Ergebnisse werden pro Server zusammengefasst und dann ein Durchschnitt gebildet.

	A	B	C	D	
93 Erkenntnisse	30x	0x	7x	56x	
Zusammengefasst pro IP: Durchschnitt	0x	1x	6x	1x	
Berechnungsmethodik: gewichteter Durchschnitt					35%

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	1x	0x	1x	
Berechnungsmethodik: gewichteter Durchschnitt					70%

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 Fehler 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	
80 Erkenntnisse	18x	34x	28x	0x	
Berechnungsmethodik: gewichteter Durchschnitt					59%

Länderrisiken

Über die Zuordnung von IP-Adressen zu Ländern wird ermittelt, wie stark die Internetpräsenzen 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	3x	3x	2x	0x	
Berechnungsmethodik: gewichteter Durchschnitt					67%

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 wir eine falsche Reihenfolge der Zertifikatskette oder ein fehlendes EV-Zertifikat werden mit B bewertet.

	A	B	C	D	
333 Erkenntnisse	146x	72x	61x	54x	
Zusammengefasst pro Host/Port: schlechtester Wert	0x	0x	0x	10x	
Berechnungsmethodik: gewichteter Durchschnitt					0%

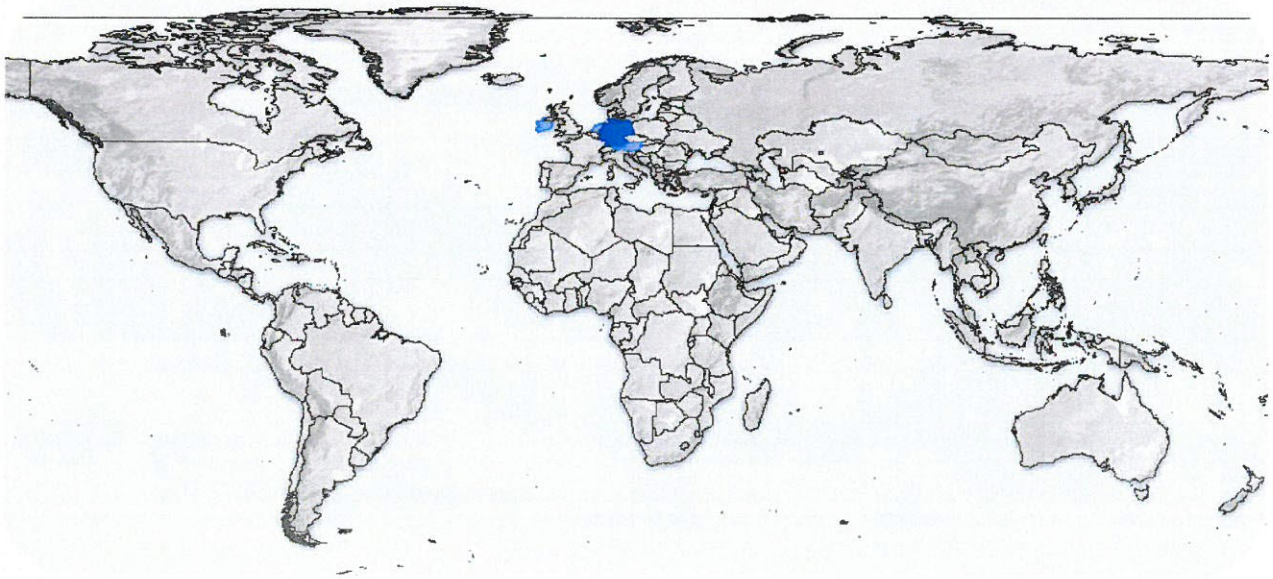
Angriffsfläche im Internet

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	
5 Erkenntnisse	0x	2x	3x	0x	
Zusammengefasst pro IP: schlechtester Wert	0x	1x	2x	0x	
Berechnungsmethodik: gewichteter Durchschnitt					43%

Internet-Fußabdruck

Wichtigste Länder: Deutschland
Weitere Länder: Österreich, Niederlande, Irland



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
Österreich	↓	A	B	B	B	B	A	C	A
Niederlande	↓	A	B	C	B	B	A	C	A
Irland	↓	A	B	B	B	B	A	C	B

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, sonder 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 privatwirtschaftliche 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 zur Herausgabe von Schlüsselmaterial bei der Einreise, bei Personenkontrollen oder durch andere staatliche Maßnahmen 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 effiktiv vorhandenen Grundrechte für Bürger im jeweiligen Land.

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

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	0
Video- & Musikportale	1
Filesharingdienste, P2P Netzwerke & Tauschbörsen	42
Spieleplattformen & Gamingforen	0
Hackerforen	0
Datingseiten	0
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 über 6,5 Mio 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	17	↑	↑	↑	↑	↗	→
Einbrüche mit leicht entschlüsselbaren Passwörtern bzw. mit schlechten Passwörtern im Klartext	6	↗	→	→	↗	→	→
Einbrüche mit gut verschlüsselten Passwörtern oder sensiblen Daten wie Geburtsdatum, Religion oder sexuelle Ausrichtung	37			↗	↗	↗	→
Datensätze ohne Passwörter und sensible Informationen	7						→

Ergebnisübersicht der Computerprüfung

Die Analyse der Server, IP-Adressen und Applikationen / Ports erbrachte folgende 474 Erkenntnisse, ausgeschlüsselt nach Ergebnistypen:

Ergebnistyp	#Erkenntnisse	ø
Der Server ist anfällig für die POODLE Attacke	36	0%
Bewertung der Certificate Transparency Unterstützung	36	33%
Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2)	36	51%
Stärke der verwendeten symmetrischen Krypographie	36	58%
Extended Validation Zertifikat	36	71%
Stärke der verwendeten asymmetrischen Krypographie	36	100%
Bewertung der TLS Versionsunterstützung	36	100%
Vertrauensstatus des Zertifikats	36	100%
Die Domain ist auf einer Blacklist von bekannt schlechten Domains	29	0%
Die IP Adresse ist auf einer Blacklist von bekannt schlechten Adressen	27	0%
HSTS Unterstützung	27	30%
Der gebrochene RC4 Algorithmus kann verwendet werden	26	30%
Zertifikat und Hostnamen passen nicht zusammen	18	0%
Überprüft die Domain mit den meisten URL Reputation Tools (u.a. Google, Microsoft, etc.)	12	91%
Bewertung der Netzwerkeinbindung nach Anbindungen und beteiligten Firmen	8	100%
Die IP Adresse ist auf einer Whiteliste von bekannt guten Adressen	8	100%
E-Mail (SMTP) Verschlüsselungsoption nicht aktiviert	8	100%
Bewertung der Reputation der Domain	7	30%
Die Domain ist auf einer Whitelist von bekannt guten Domains	7	100%
Bewertung der Reputation der IP Adresse	3	100%
Zusätzliche offene Ports für das gesamte Internet sichtbar	2	44%
Zugang zu einem Datenbanksystem für das gesamte Internet sichtbar	1	27%
Es wird ein veraltetes Symantec Zertifikat verwendet	1	30%
Auf dem Mail Server sind www-Ports offen	1	60%
Zugang zur Netzwerkeinwahl für das gesamte Internet sichtbar	1	70%

Dienstleisterübersicht

Serverbetrieb:

- hoster.com

Namensauflösung:

- hoster-10.org
- hoster-45.co.uk
- hoster-28.com
- hoster-17.net
- hoster-14.org
- hoster-18.co.uk
- hoster-49.net
- hoster-06.org
- hoster-08.co.uk
- hoster-03.net
- hoster-08.com
- hoster-47.com
- hoster-40.net
- hoster-13.org
- hoster-27.co.uk
- hoster-59.org
- hoster-12.co.uk
- hoster-06.com
- hoster-20.net
- hoster-20.org
- hoster-39.co.uk
- hoster-43.com
- hoster-49.org
- hoster-46.co.uk
- hoster-32.com
- hoster-37.net
- hoster-52.org
- hoster-29.co.uk
- hoster-38.net
- hoster-11.com
- hoster-36.org
- hoster-38.co.uk
- hoster-48.com
- hoster-26.net
- hoster-38.org
- hoster-02.co.uk
- hoster-25.com
- hoster-10.net

E-Mail Provider:

- mailsec.com

Berichte

Mit Hilfe der H&S Technologie können sich Endkunden und Partner vollautomatisierte Berichte über die Sicherheitslage eines Unternehmens erstellen lassen. Solche Berichte können in mehreren Anwendungsszenarien nützlich sein:

- "Scoring": Die Finanz- und Versicherungswirtschaft kann die Informationen aus dem H&S Bericht verwenden um sich schnell und kostengünstig einen Überblick über das technische Außenbild eines Unternehmens zu verschaffen.
- "Large Scale Risk Management": H&S Berichte werden von unseren Kunden verwendet um sich schnell einen Überblick über die technischen Risiken Ihrer Partner, Lieferanten bzw. Kunden zu machen, da diese durch die zunehmende Vernetzung immer mehr an Bedeutung gewinnt.
- "Advanced Threat Analytics": Mit ihrem umfassenden Ansatz liefern die H&S Berichte einen schnellen Überblick über nahezu alle öffentlich verfügbaren Datenbanken - gefiltert auf die für ein bestimmtes Unternehmen relevanten Informationen. Ein Cyber Security Analyst kann diese "Open Source Intelligence" (OSINT) Informationen als zusätzliche Quelle für sein Lagebilde verwenden.
- Basis für weitere Dienstleistungen: etliche unserer Partner nutzen die Automatisierung der H&S Technologie um auf dieser Basis eigene, neue Dienstleistungs- und Beratungsprodukte zu erstellen.

Generell ist die Berichtserstellung in vier vollautomatisierte Phasen untergliedert:

1. Aufklärungsphase: Herausfinden, welche Systeme, Netzwerke und Einzelcomputer unter der Kontrolle des Unternehmens stehen bzw. für die das Unternehmen verantwortlich ist.
2. Inspektionsphase: Intensive Untersuchung der Netzwerke, Computerkonfigurationen und Applikationen.
3. Bewertungsphase: Die Ergebnisse der Inspektionsphase werden bewertet und es wird ein Gesamtrating erstellt.
4. Berichtserstellung: Die Erkenntnisse werden in einem Bericht zusammengefasst.

Aufklärungsphase

Ziel dieser Phase ist es, herauszufinden, welche Systeme, Netzwerke und Einzelcomputer unter der Kontrolle des Unternehmens stehen bzw. für die das Unternehmen verantwortlich ist. Zuerst werden auf Basis der Unternehmensdaten die zugehörigen Netzwerke identifiziert. Dazu werden folgende Kriterien verwendet:

- die Größe des Netzwerksegments
- die Angaben zur Domain, zum Firmennamen oder der Firmenadresse im "whois"-Eintrag
- die reverse DNS Einträge der Server in diesem Segment

Bei der Erstellung des Reports kann gewählt werden, ob nur die vom Benutzer angegebenen Domains und deren Subdomains verwendet werden oder ob aktiv nach weiteren Domains gesucht wird. Im standardmäßig eingestellten zweiten Fall werden folgende Kriterien zur Suche von weiteren Domains verwendet:

- Nähe im Netzwerk zu anderen Servern
- Ähnlichkeit von Netzwerkregistrierungsinformationen
- Erwähnung von Firmenname oder -adresse in den Registrierungsinformationen
- Suche nach ähnlichen Domainnamen in der CyDIS Domaindatenbank (291.261.936 Einträge), z.B. gleiche Namensbestandteile, Unterschied nur in der Länderkennzeichnung
- Vergleich des eingetragenen Domainverwalters
- Verwendung gleicher Mail- oder Serverinfrastrukturen
- Gemeinsamkeiten in der Konfiguration der DNS-Server
- Namensauflösung bzw. umgekehrte Namensauflösung
- Verwendung gleicher Zertifikate oder gleicher Zertifikats-Aussteller-Adressen
- Verlinkungen auf den Webseiten

Sind dann alle mögliche zugehörigen Hauptdomains identifiziert, werden die zugehörigen Subdomains gesucht. Dies geschieht mit folgenden Hilfsmitteln:

- reverse DNS Datenbank (513.862.115 Einträge)
- historisierte DNS-Daten (2.141.989.201 aktuelle und 203.273.015 historische Einträge)
- Zertifikats-Datenbank (588.486.114 Einträge)
- Websuche
- Google Transparence Reports
- Wörterbuch / Brute-Force
- Shodan, Threat Crowd, VirusTotal
- DNSDB, HackerTarget, Netcraft
- Wayback Machine, PTRArchive
- Censys, PassiveTotal, Riddler

Am Ende der Suche kann der Benutzer die entdeckten Domains ggf. nochmals anpassen.

Inspektionsphase

Die Inspektionsphase beginnt mit einem intensiven Netzwerkscan der in der Aufklärungsphase entdeckten Netzwerke und Computersysteme. Die identifizierten Zugänge werden untersucht und für alle sicherheitsrelevanten Domains und IPs werden aktuell öffentlich verfügbare Daten erhoben. Für einige Datenkategorien liegen auch historische Werte von früher öffentlich verfügbaren Daten vor.
Aktuell werden folgende Prüfungen durchgeführt:

- Scan der offenen Ports der Zielsysteme und Bewertung der offenen Ports
- Ermittlung aller IT-Dienstleister
- Identifikation von Anomalien in der DNS Konfiguration mit der historisierten DNS-Datenbank (2.141.989.201 aktuelle und 203.273.015 historische Einträge)
- Qualität der eingesetzen Verschlüsselung u.a. mit der historisierten Zertifikatsdatenbank (588.486.114 Einträge)
- Reputation der Webseite mit >50 Reputationssystemen (->Details)
- Untersuchung der IP Adresse auf (frühere) TOR-Netzwerk Exitnodes
- Abfrage gegen historische Daten aus Threatdatenbanken (urlhaus, SURBL, Cisco)
- Mitgliedschaft in der Cyber-Allianz des BSI
- Check der IP in >250 White- oder Blacklists sowie der Domain in >60 White- oder Blacklists (->Details)
- Netzwerkanbindungen jedes Computers auf seine Einbindung in das Internet (BGP-AS-Peers)
- Check auf gestohlene Passwörter in 6.854.195.913 Datensätzen (->Details)
- Resistenz der Konfiguration gegen Domain Takeover

Aus diesen Prüfungen werden derzeit 68 parametrisierte Findings generiert (->Details).
Das Scoring wird regelmäßig erweitert. Folgende Prüfungen befinden sich aktuell im Beta Stadium:

- Up-to-date Check der eingesetzten Frameworks
- Analyse gegen die Corporate Trust Länderdatenbank
- Analyse der Cloudstrukturen und Bewertung gegen die Corporate Trust Sicherheitsbewertung der Cloudinfrastrukturen
- Suche im Darknet / TOR-Netzwerk
- Auswertung von Honeypot Daten

Bewertungssphase

Am Ende der Inspektionsphase sind bei Unternehmen mit kleinem "Fußabdruck" im Internet etwa 100 bei komplexeren, Internetbasierten Unternehmen schnell mehrere 10.000 Ergebnisse zusammengekommen. Diese Ergebnisse können positiv wie negativ sein. Der Scoring Algorithmus kombiniert diese Werte und ermittelt daraus folgende Kategorien:

- 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

Jedes dieser Ergebnisse wurde nicht nur mit einem festen Wert erhoben, sondern auch mit einer Angabe der "Gewissheit" - also einer Wahrscheinlichkeitsangabe für eine fehlerhaft Erkennung. Daraus ergibt sich für jede Kategorie ein Minimal- und ein Maximalwert. Je näher die beiden zusammen liegen, umso höher ist die Gewissheit. Die Gesamtbewertung findet dementsprechend in folgenden Stufen statt:

AAA	risikoarm, hohe Aussagekraft des Ratings
AA	risikoarm, mittlere Aussagekraft des Ratings
A	risikoarm, geringe Aussagekraft des Ratings
BBB	beherrschbare Risiken vorhanden, hohe Aussagekraft des Ratings
BB	beherrschbare Risiken vorhanden, mittlere Aussagekraft des Ratings
B	beherrschbare Risiken vorhanden, geringe Aussagekraft des Ratings
C	substantielles Risiko
D	kritisches Risiko

Berichtserstellung

Die Berichtserstellung ist modular und das Layout anpassbar. Derzeit existieren auf dem H&S System insgesamt 33 verschiedene Berichtsmodule, die die H&S und ihre Partner verwenden können. Je nach Komplexität der Untersuchung steht der Endbericht dem Auftraggeber normalerweise nach 4-48h zum Download zur Verfügung. Spätere Anpassungen und Kommentierungen sind (auch von Dritter Seite) möglich, werden aber im Bericht immer klar gekennzeichnet.

Identifizierte Computer

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

musterfa.com[4,7,8,10,12,13,14,17,18,19,21,23,25]	www.musterfa.com[4,7,8,10,12,13,14,17,18,19,21,23,25]
dev.musterfa.com[4,6,8,18,19,25]	www.dev.musterfa.com[4,6,8,18,19,25]
musterfa.biz[4,7,8,10,12]	www.musterfa.biz[4,7,8,10,12]
musterfa.ch[4,7,8,10,12,14]	www.musterfa.ch[4,7,8,10,12,14]
musterfa.co.uk[4,8,10,12,14,17,20,21]	www.musterfa.co.uk[4,8,10,12,14,17,20,21]
musterfa.de[4,7,8,10,12,14,17]	www.musterfa.de[4,7,8,10,12,14,17]
musterfa.eu[4,7,8,10,12,14]	www.musterfa.eu[4,7,8,10,12,14]
musterfa.info[4,7,8,10,12]	www.musterfa.info[4,7,8,10,12]
musterfa.net[4,7,8,10,12]	www.musterfa.net[4,7,8,10,12]
musterfa.org[4,7,8,10,12]	www.musterfa.org[4,7,8,10,12]
musterfa.sk[4,7,8,10,12,14]	www.musterfa.sk[4,7,8,10,12,14]
cr20.musterfa.com[4,6,8,18,19,20,25]	www.cr20.musterfa.com[4,6,8,18,19,20,25]
inside.musterfa.com[27]	www.inside.musterfa.com[27]

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

TODOS für 172.172.78.86 (musterfa.biz)

- [ ] Prüfen warum der Server auf einer Blackliste gelandet ist.

TODOS für 172.173.145.18 (www.musterfa.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 80: http, 443(TLS), 444(TLS)

- [ ] Empfehlungen des BSI bzgl. Kryptographie (TR-02102-2) umsetzen. (Ports 443,444)
- [ ] Kryptolibrary gegen bekannte Angriffe härten bzw. patchen. (Ports 443,444)
- [ ] HSTS auf der Webseite aktivieren. (Ports 443,444)
- [ ] Server ggf. härten und Zusatzports schließen.
- [ ] Prüfen warum der Server auf einer Blackliste gelandet ist.

TODOS für 172.245.145.19 (musterfa.com, dev.musterfa.com, www.dev.musterfa.com, musterfa.co.uk, www.musterfa.co.uk, musterfa.de, www.musterfa.de, cr20.musterfa.com, www.cr20.musterfa.com, inside.musterfa.com, www.inside.musterfa.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 80: http, 443(TLS), 1723: pptp, 8000: http-alt, 8443: https-alt, 50000: ibm-db2

- ☐ Empfehlungen des BSI bzgl. Kryptographie (TR-02102-2) umsetzen. (Port 443)
- ☐ Vertrauensstatus des Zertifikats prüfen. (Port 443)
- ☐ Kryptolibrary gegen bekannte Angriffe härten bzw. patchen. (Port 443)
- ☐ HSTS auf der Webseite aktivieren. (Port 443)
- ☐ Server ggf. härten und Zusatzports schließen.
- ☐ Prüfen warum der Server auf einer Blackliste gelandet ist.

TODOS für 172.173.145.26 (ex.musterfa.com)

Folgende offene Ports wurden bei der Untersuchung detektiert: 25(TLS), 80: http, 443(TLS), 587(TLS)

- ☐ Empfehlungen des BSI bzgl. Kryptographie (TR-02102-2) umsetzen. (Ports 587,25,443)
- ☐ Zertifikatsanbieter prüfen und ggf. wechseln. (Port 587)
- ☐ Kryptolibrary gegen bekannte Angriffe härten bzw. patchen. (Ports 587,25,443)
- ☐ HSTS auf der Webseite aktivieren. (Port 443)
- ☐ Mailserver ggf. härten und Zusatzports schließen.
- ☐ Prüfen warum der Server auf einer Blackliste gelandet ist.

TODOS für 172.173.145.28 (www.musterfa.biz, musterfa.ch, www.musterfa.ch, musterfa.eu, www.musterfa.eu, musterfa.info, www.musterfa.info, musterfa.net, www.musterfa.net, musterfa.org, www.musterfa.org, musterfa.sk, www.musterfa.sk)

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

- ☐ Empfehlungen des BSI bzgl. Kryptographie (TR-02102-2) umsetzen. (Port 443)
- ☐ Vertrauensstatus des Zertifikats prüfen. (Port 443)
- ☐ Kryptolibrary gegen bekannte Angriffe härten bzw. patchen. (Port 443)
- ☐ HSTS auf der Webseite aktivieren. (Port 443)
- ☐ Prüfen warum der Server auf einer Blackliste gelandet ist.

TODOS für 172.94.120.74 (musterfa-eu0c.mail.protection.mailsec.com, musterfa-net0c.mail.protection.mailsec.com)

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

- ☐ Empfehlungen des BSI bzgl. Kryptographie (TR-02102-2) umsetzen. (Port 25)
- ☐ Kryptolibrary gegen bekannte Angriffe härten bzw. patchen. (Port 25)
- ☐ Prüfen warum der Server auf einer Blackliste gelandet ist.
- ☐ Prüfen warum die Reputation als Servers suboptimal bewertet wird.

TODOS für 172.213.154.106 (musterfa-de0c.mail.protection.mailsec.com, musterfa-sk0c.mail.protection.mailsec.com)

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

- ☐ Empfehlungen des BSI bzgl. Kryptographie (TR-02102-2) umsetzen. (Port 25)
- ☐ Kryptolibrary gegen bekannte Angriffe härten bzw. patchen. (Port 25)
- ☐ Prüfen warum der Server auf einer Blackliste gelandet ist.
- ☐ Prüfen warum die Reputation als Servers suboptimal bewertet wird.

TODOS für 172.213.154.138 (musterfa-com0c.mail.protection.mailsec.com, musterfa-ch0c.mail.protection.mailsec.com, musterfa-co-uk0c.mail.protection.mailsec.com)

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

- ☐ Empfehlungen des BSI bzgl. Kryptographie (TR-02102-2) umsetzen. (Port 25)
- ☐ Kryptolibrary gegen bekannte Angriffe härten bzw. patchen. (Port 25)
- ☐ Prüfen warum der Server auf einer Blackliste gelandet ist.
- ☐ Prüfen warum die Reputation als Servers suboptimal bewertet wird.

Kritische Leaks

Für die Domains in diesem Bericht sind insgesamt 17 Accounts in der Kategorie "Rot" bekannt, bei denen die Passwörter im Klartext vorliegen.

0___.W___@musterfa.com
a___.m___@musterfa.com
a___.s___@musterfa.com
a___.c___@musterfa.com
a___.w___@musterfa.com
b___.d___@musterfa.com
d___.b___@musterfa.com
e___.b___@musterfa.com
h___.m___@musterfa.com
i___@musterfa.com
k___.h___@musterfa.com
m___.d___@musterfa.com
r___.k___@musterfa.com
s___.n___@musterfa.com
s___.m___@musterfa.com
s___.m___@musterfa.com
t___.m___@musterfa.com

Problematische Leaks

Für die Domains in diesem Bericht sind insgesamt 6 Accounts bekannt, bei denen die Passwörter in leicht entschlüsselbarer Form vorliegen oder für die einfache Klartextpasswörter (wie PINs oder sechsstellige Passwörter) bekannt sind.

K___.H___@musterfa.com
j___.k___@musterfa.de
m___.e___@musterfa.com
m___.g___@musterfa.com
o___.k___@musterfa.com
p___.w___@musterfa.com

Unschöne Leaks

Für die Domains in diesem Bericht sind insgesamt 37 Accounts bekannt, bei denen entweder gut verschlüsselte Passwörter (Angriffsdauer zur Entschlüsselung > 1 Monat) oder sensible Daten vorliegen.

a___.h___@musterfa.com
a___.k___@musterfa.com
a___.n___@musterfa.com
a___.w___@musterfa.com
b___.a___@musterfa.com
c___.g___@musterfa.com
c___.h___@musterfa.com
d___.r___@musterfa.com
f___.b___@musterfa.com
f___.l___@musterfa.com
g___.o___@musterfa.com
h___.b___@musterfa.com
h___.r___@musterfa.com
j___.t___@musterfa.com
j___.b___@musterfa.com
j___.s___@musterfa.com
j___.s___@musterfa.com
j___.b___@musterfa.com
k___.p___@musterfa.com
k___.f___@musterfa.com
k___.y___@musterfa.com
l___.e___@musterfa.com
m___.p___@musterfa.com
n___.z___@musterfa.com
o___.b___@musterfa.com
o___.s___@musterfa.com
o___.w___@musterfa.com
p___.n___@musterfa.com
r___.d___@musterfa.com
r___.b___@musterfa.com
s___.a___@musterfa.com
s___.k___@musterfa.com
t___.s___@musterfa.com
v___.s___@musterfa.com
w___.k___@musterfa.com
w___.g___@musterfa.com
w___.j___@musterfa.com

E-Mail only Leaks

Für die Domains in diesem Bericht gibt es insgesamt 7 Accounts bei denen nur E-Mailadresse bekannt geworden ist.

k___.h___@musterfa.com
l___.s___@musterfa.com
n___.s___@musterfa.com
p___.w___@musterfa.com
p___.w___@musterfa.de
r___.b___@musterfa.com
t___.h___@musterfa.com