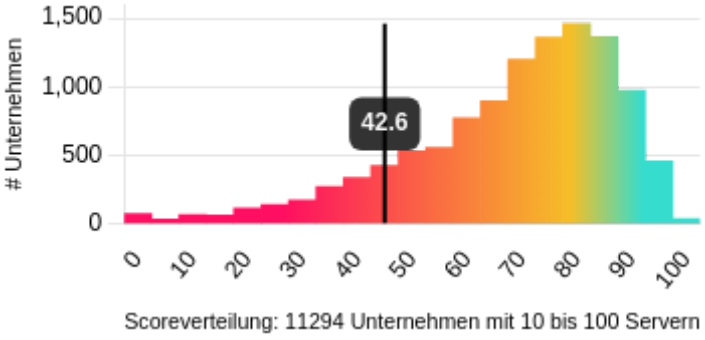
Managementübersicht | Ihre aktuelle IT-Sicherheitslage

Die Managementübersicht informiert Sie über die Sicherheitslage Ihrer unternehmensweiten IT-Systeme aus externer Sicht. Ein hoher Score-Wert steht für eine niedrigere Wahrscheinlichkeit eines Cybervorfalls.

42.56	64.68	68.15
Security-Score*	Ø Branche**	Ø Gesamt***



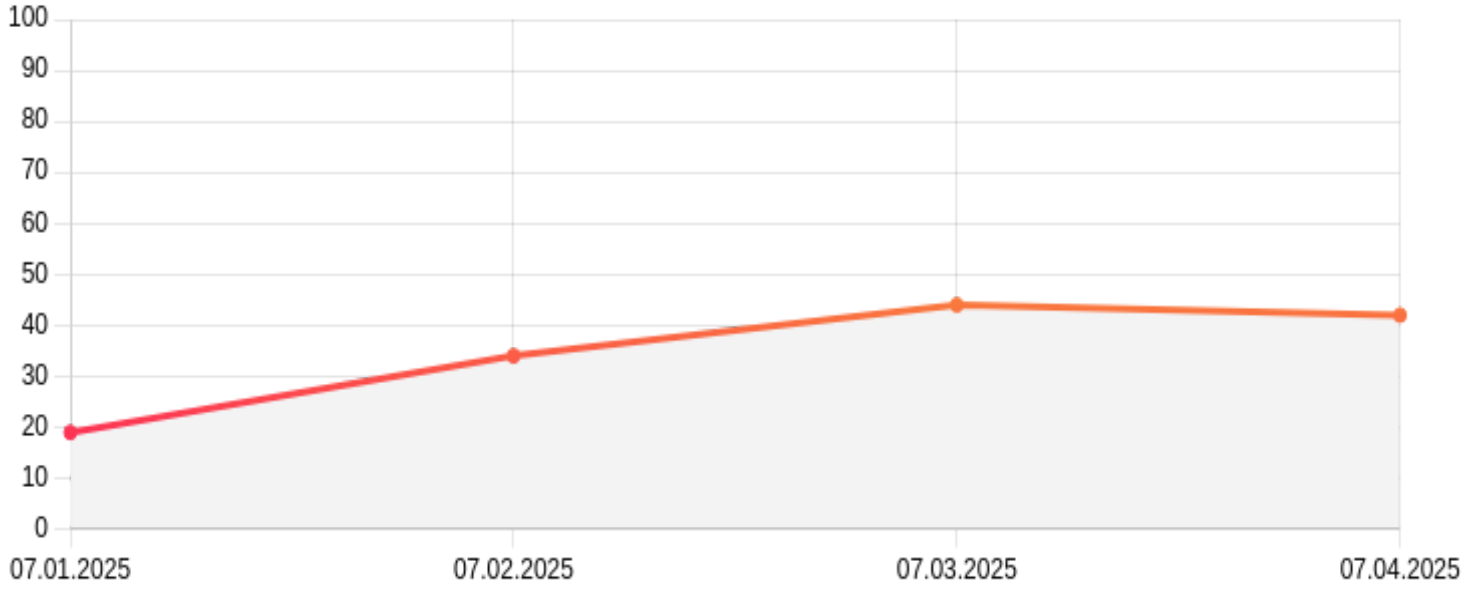
Mit einem Score von 42.56 liegt Ihr Ergebnis unter dem Durchschnitt. 88.49% der erfassten Unternehmen vglb. Größe (definiert nach der Serveranzahl) sind besser als Sie.

Der Score hat im besten Fall einen Wert von 100/grün, im schlechtesten Fall von 0/rot. Bei sicherheitsrelevanten Funden werden, je nach Kritikalität, Punkte abgezogen. Ein guter Wert liegt über dem Gesamt-Score.

* Ihre IT-Sicherheit im Vergleich zu Firmen vergleichbarer Größe
** Ihre IT-Sicherheit im Vergleich zu Unternehmen Ihrer Branche
*** Durchschnittlicher Wert aller bewerteten Unternehmen

Funde 886 high 21 | medium 398 | low 467	Erfasste Server 22	43 IP-Adressen	Geprüfte Domains 74

Der Score Verlauf zeigt die Entwicklung Ihres Sicherheitsrankings an, sodass Sie die Veränderungen leicht nachverfolgen können.



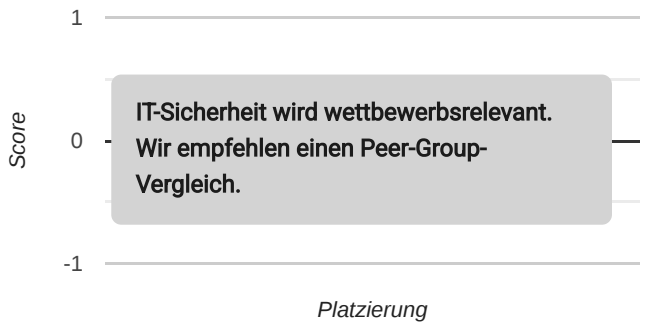
Die Bewertungen basieren auf branchenüblichen, öffentlich verfügbaren Standards, wie z.B.:

- NIST CIS (National Institute of Standards & Technology sowie das Center for Internet Security)
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- OWASP (Open Web Application Security Project) und viele mehr

Die Analysen berücksichtigen die Vorgaben der EU-DSGVO (Datenschutz-Grundverordnung).

Sicherheitsvergleich | Cybersicherheit wird wettbewerbsrelevant

Ihre unternehmensweite IT-Sicherheitslage im Peer-Group-Vergleich



42.56
Ihr Status

–
Ø Peers

64.68
Ø Branche

68.15
Ø Gesamt

Sie möchten wissen, wie Sie im Peer-Group-Benchmark abschneiden? Mit dem IT-Sicherheitsvergleich finden wir das für Sie heraus. In diesem Fall sehen Sie hier eine Grafik, die Ihre IT-Sicherheit im Vergleich von bis zu 10 weiteren Unternehmen aufzeigt.

Auf Anfrage und gegen Aufpreis, einfach Kontakt aufnehmen.

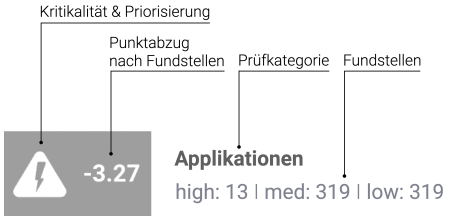
Ihr IT-Risiko-Status im Vergleich zum Durchschnitt aller geprüften Unternehmen Ihrer Branche. Sie sehen, in welcher Prüfkategorie Ihr Unternehmen in punkto Sicherheit vorne liegt und wo es Nachholbedarf gibt. Das Ranking basiert auf Fundstellen, die je nach Kritikalität zu Minuspunkten führen. Deren Summe vom Richtwert 100 abgezogen, ergibt den Score.

Prüfkategorien*	Ihr Status	Branche	Unternehmen Gesamt
Applikationen	**-19.44**	-15.41	-10.66
IP-Reputation	**0**	0	-0.05
Zertifikate	**-9.42**	-5.05	-6.54
Netzwerk	**-13.59**	-5.54	-6.12
DNS	**-10.16**	-2.68	-2.64
Web	**-4.13**	-6.05	-4.37
DSGVO	**-0.55**	-0.55	-1.71
Datenpannen	**0**	0	0
DDoS	**-0.15**	--	--
Scorewert 100-Minuspunkte =	**42.56**	64.68	68.15

Worst Case · Hohes Risiko · Moderates Risiko · Geringes Risiko

Ihre aktuelle IT-Sicherheitslage | Die Prüfkategorien

Anhand der neun Kategorien sehen Sie, was genau geprüft wurde und wo mit welcher Priorität gehandelt werden sollte. Je höher das Risiko ist, das von einem Befund ausgeht, umso mehr Minuspunkte gibt es.



- Hohes Risiko | high
- Moderates Risiko | med
- Geringes Risiko | low

-19.44	**Applikationen** high: 2 | med: 8 | low: 0	-13.59	**Netzwerk** high: 2 | med: 16 | low: 17
-4.13	**Web** high: 0 | med: 316 | low: 269	-10.16	**DNS** high: 1 | med: 35 | low: 71
-9.42	**Zertifikate** high: 14 | med: 23 | low: 23	-0.55	**DSGVO** high: 2 | med: 0 | low: 0
0	**IP-Reputation** high: 0 | med: 0 | low: 0	–	**Datenpannen** high: 0 | med: 11 | low: 0
-0.15	**DDoS** high: 0 | med: 0 | low: 87	-14.63	**Import interner Scans** high: 1 | med: 3 | low: 1

Applikationen | Ist Ihre Unternehmenssoftware auf einem aktuellen Sicherheitsniveau?

Oder gibt es veraltete Anwendungen mit Sicherheitslücken? In dieser Kategorie prüfen wir die von Ihrem Unternehmen genutzte Software (z.B. Microsoft Exchange Server, TYPO3, Wordpress, Apache-Webserver, etc.) auf fehlende Updates und gleichen sie mit verschiedenen Quellen für veröffentlichte IT-Schwachstellen, wie dem CVE-Verzeichnis, ab.

Gefährdungspotenzial Nicht aktualisierte Software öffnet Angreifern Tür und Tor zur Ausnutzung von Schwachstellen.

Cybervorfall Durch eine Schwachstelle im Microsoft Betriebssystem legten Cyberkriminelle mit der Ransomware WannaCry über 230 Tsd. Computer in 150 Ländern lahm. Finanzieller Schaden: 4 Milliarden USD.

-19.44 **Es fehlen äußerst kritische Sicherheitsupdates auf Ihren Systemen. Wir empfehlen dringlichst, die ausstehenden Updates zu installieren. Zudem sollten Sie Ihre Patchmanagement-Prozesse überprüfen.**

Netzwerk | Sind sämtliche System-Zugänge angemessen gesichert?

Stehen in Ihrem Netzwerk Türen und Fenster unbeabsichtigt offen? In dieser Kategorie wird geprüft, ob es offene Zugänge zu kritischen Diensten und Systemen wie Datenbank- und Datei-Servern gibt. Ist dies der Fall, gibt es kräftig Punktabzug. Denn hier können sich Angreifer leicht Zugang verschaffen, Daten abgreifen und die Übernahme des kompletten Systems starten.

Gefährdungspotenzial Kritische Ports sind ein bevorzugtes Ziel von Angreifern, da sie ihnen Zugang zu weiteren Systemen und sensiblen Daten verschaffen.

Cybervorfall Beim Angriff auf eine französische Hotelkette wurden 1 Terabyte an Buchungsinformationen, Kreditkartendetails sowie Zugangsdaten von Kunden gestohlen.

-13.59 **Es wurden offene Ports mit kritischen Diensten gefunden, die nicht aus dem Internet erreichbar sein sollten. Aus unserer Sicht besteht dringender Handlungsbedarf. Die Erreichbarkeit sollte durch eine Firewall geregelt werden.**

Ihre aktuelle IT-Sicherheitslage | Die Prüfkategorien

Web | Sind Ihre Web-Plattformen sicher?

Ist Ihr Unternehmen ausreichend gegen Angriffe über die öffentlich erreichbaren URLs geschützt? In dieser Kategorie werden Ihre IP-Adressen und Webserver kontaktiert und auf die Verwendung des HTTP-Sicherheitsheaders sowie sicherheitsrelevante Konfigurationen durchsucht. Dabei werden auch IT-Entwicklungsverzeichnisse (GIT, SVN) erfasst, die unbeabsichtigten Zugriff auf sensible Daten ermöglichen.

Gefährdungspotenzial Cyberattacken auf Webserver können die Erreichbarkeit der Webseiten verhindern. Mögliche Folgen: Reputationsverlust und erhebliche Geschäftseinbußen.

Cybervorfall Bei einem SaaS-Unternehmen wurden Software und Kundendaten über den unbeabsichtigt auf der Webplattform veröffentlichten GIT-Ordner abgegriffen.

-4.13 Die Webanwendungen enthalten Konfigurationsprobleme, welche sicherheitskritisch werden können. Setzen Sie die entsprechenden Header in den Einstellungen des Webservers.

DNS | Ist Ihr Mailversand vor Identitätsraub geschützt?

Wie sicher sind Ihre Mitarbeiter vor Betrugsversuchen mit Phishing-E-Mails? Lassen sich im Namen Ihres Unternehmens massenweise Spam-E-Mails verschicken – beispielsweise um sensible Daten abzugreifen? In dieser Kategorie prüfen wir, ob Ihr Unternehmen ausreichend vor Mail-Fälschung (Identitätstäuschung) geschützt ist.

Gefährdungspotenzial Ungeschützter Mailversand ermöglicht Spam- und Phishing-Attacken im Namen Ihrer Domain(s). Angreifer können sich so Zugang zu weiteren Systemen verschaffen und diese mit Schadsoftware infizieren.

Cybervorfall Durch Missbrauch der E-Mail-Adressen von 3 Großkonzernen infizierte die Schadsoftware Emotet Ministerien, Institutionen und öffentliche Einrichtungen. Der Schaden: Alleine in DE mind. 14,5 Mio. Euro.

-10.16 Im DNS-Verzeichnis fehlen sicherheitskritische Einträge zum Schutz Ihres E-mail-Verkehrs und Ihrer Domains. Aus unserer Sicht besteht dringender Handlungsbedarf. Bitte setzen Sie die entsprechenden Einstellungen bei Ihrem Domainanbieter.

Zertifikate | Werden Ihre Daten ausreichend sicher ausgetauscht?

Ist der Datenfluss zwischen Ihren Mitarbeitern und Kunden oder Partnern vor dem Zugriff durch Dritte abgesichert? In dieser Kategorie wird die Verschlüsselungsqualität der Datenverbindungen bewertet. Dabei werden auch Gültigkeit und Version der Sicherheitszertifikate (SSLv3, TLS 1.0, ...) sowie deren korrekte Implementierung überprüft.

Gefährdungspotenzial Die unsichere Übertragung sensibler Inhalte im Netz macht Datendiebstahl einfach und gefährdet Unternehmen samt Lieferketten.

Cybervorfall Jede Website, die Besucherdaten abfragt, ist verpflichtet ein gültiges SSL-Zertifikat zu führen. Bei fehlender SSL-Verschlüsselung drohen Verschlechterung des Google-Rankings und Abmahnung.

-9.42 Es wurden sicherheitskritische Konfigurationsprobleme in den verwendeten Zertifikaten gefunden. Prüfen Sie die verwendeten Zertifikate und aktualisieren Sie die Web- & Mailserver-Einstellungen hinsichtlich der verwendeten Konfigurationen und Versionen.

Ihre aktuelle IT-Sicherheitslage | Die Prüfkategorien

DSGVO | Gibt es Verstöße gegen die Datenschutzgrundverordnung?

Die Datenschutzgrundverordnung (DSGVO) stellt personenbezogene Daten unter besonderen Schutz. Diese werden immer dann verarbeitet, wenn Namen, (IP-) Adressen, Bankverbindungen, Gesundheitsdaten, Standortdaten uvm. von Website-Besuchern erfasst werden. In dieser Kategorie prüfen wir alle identifizierten Unternehmens-/Konzernwebseiten auf grundlegende DSGVO-Verstöße.

Gefährdungspotenzial Bei rechtswidrig gesetzten Cookie-Bannern und Marketing-, Tracking- oder Affiliate-Cookies drohen Abmahnungen und hohe Bußgelder.

Cybervorfall Gegen eine Fluggesellschaft wurde wegen der Verwendung eines nicht datenschutzkonformen Cookie-Banners ein Bußgeld von 30.000 Euro verhängt.

-0.55 Es wurden kritische DSGVO-Verstöße auf Ihren Webseiten entdeckt. Aus unserer Sicht besteht dringender Handlungsbedarf. Überprüfen Sie die Consentmaßnahmen hinsichtlich nicht geblockter Tracking-Cookies.

IP-Reputation | Sind die erfassten Server in Ihrer IT-Infrastruktur frei von Infektionen?

Gibt es bereits von Angreifern kompromittierte Systeme, die nun als Spam-Quelle dienen, unerwünschte Anfragen senden und bösartige Software verbreiten? Um das herauszufinden, durchsuchen wir Spam- und Schadsoftwarelisten nach IP-Adressen, die zu Ihrem Unternehmen gehören. Werden wir fündig, hat das Auswirkungen auf Ihre Reputation im Internet.

Gefährdungspotenzial Viele IoT-Geräte haben gravierende Sicherheitslücken und machen es Hackern leicht, das gesamte Netzwerk zu infizieren, Daten abzugreifen oder Schadprogramme zu platzieren.

Cybervorfall Einer Spielbank wurde das WLAN-Thermostat des hauseigenen Aquariums zum Verhängnis. Angreifer nutzten das Gerät als Hintertür, um ins Netzwerk vorzudringen und die interne Datenbank zu stehlen.

0 Es wurden keine Anzeichen für bösartige Aktivitäten gefunden.

Datenpannen | Ist Ihr Unternehmen bereits von Datendiebstahl betroffen?

Gibt es Datenpannen, durch die Unberechtigte Zugriff auf personalisierte Nutzerkonten oder Passwörter erlangten? Wir durchforsten Datenbanken im Netz nach Ihren Unternehmensdomains und zeigen die Funde inklusive der Leak-Quellen (z.B. LinkedIn, Adobe, Dropbox, uvm.) in der Analyse an.

Gefährdungspotenzial Von sozialen Netzwerken oder anderen Diensten gestohlene Nutzerdaten werden im Darknet veräußert bzw. zur Übernahme weiterer Accounts missbraucht, um Zugang zu internen Geschäftssystemen zu erlangen. Einfache und mehrfach verwendete Passwörter steigern das Risiko erheblich.

Cybervorfall Bei dem Business-Netzwerk LinkedIn wurden persönliche Daten von 500 Millionen LinkedIn-Nutzern abgeschöpft und stehen in einem Hacker-Forum zum Verkauf.

– Für Ihre Domain(s) gibt es keine Auffälligkeiten hinsichtlich Breaches, Leaks oder Blacklist-Einträgen.*

*Unsere Möglichkeiten sind aus Datenschutzgründen limitiert. Über die Web-App https://haveibeenpwned.com/DomainSearch finden Sie heraus, welche Accounts betroffen sind. Sorgen Sie dafür, dass Mitarbeiter gestohlene Passwörter ändern und niemals Passwörter doppelt verwenden.

Ihre aktuelle IT-Sicherheitslage | Die Prüfkategorien

DDoS | Könnten große Datenmengen, langsam ladende Daten oder fehlende Redundanz Ihre Website für DDoS-Angriffe anfällig machen?

Könnten ineffiziente Datenstrukturen, langsame Ladezeiten oder fehlende Redundanz (wie DNS, Mailserver, CDN usw.) Ihre Website für DDoS-Angriffe anfälliger machen? In dieser Kategorie bewerten wir das potenzielle Risiko, dass Ihr Unternehmen durch diese Bedingungen DDoS-Angriffen ausgesetzt sein könnte, die Server durch übermäßige Anfragen lahmlegen können.

Gefährdungspotenzial

Große Datenmengen, langsame Ladezeiten und fehlende Redundanz können den Datenfluss Ihrer Website beeinträchtigen und sie attraktiver für DDoS-Angriffe machen, was zu finanziellen Verlusten und Schäden an Ihrem Markenimage führen kann.

Cybervorfall

Im Jahr 2016 fiel der DNS-Anbieter Dyn einem erheblichen DDoS-Angriff zum Opfer, der zahlreiche Internetplattformen, einschließlich Twitter, Reddit und The New York Times, durch ineffiziente Datenstrukturierung, langsame Ladezeiten und fehlende Redundanz für mehrere Stunden unzugänglich machte.

-0.15

Es wurden einige Schwachstellen in Bezug auf große Datenmengen, langsame Ladezeiten oder fehlende Redundanz auf Ihrer Website gefunden. Bitte überprüfen und optimieren Sie diese Bereiche.

Import interner Scans | Komplette Angriffsfläche in einem Bericht

Diese Kategorie fasst die Ergebnisse intern durchgeführter Schwachstellen-Scans in einem einheitlichen Score zusammen. So können Sie die intern wie extern ermittelte Angriffsfläche komfortabel in einem zentralen Dashboard verfolgen und priorisieren.

Gefährdungspotenzial

Nicht behobene Schwachstellen aus internen Scans eröffnen Angreifern eine direkte Einfallpforte für unbefugten Zugriff, Datenverlust oder Systemausfälle. Je länger kritische Findings ungepatcht bleiben, desto höher ist das Risiko, dass sie ausgenutzt werden - insbesondere, wenn bereits öffentlich verfügbare Exploits existieren oder Schwachstellen in extern erreichbaren Diensten liegen.

Sicherheitsverpflichtung

Kritische Schwachstellen binnen 72-Stunden schließen, Patches regelmäßig nachprüfen und alle Maßnahmen nachvollziehbar dokumentieren, um Compliance-Anforderungen wie ISO-27001 und NIS-2 einzuhalten.

-14.63

Es wurden kritische Schwachstellen gefunden, die sofortige Aufmerksamkeit erfordern. Patchen Sie Ihre Systeme und überprüfen Sie dringend die Netzwerksicherheitsrichtlinien.

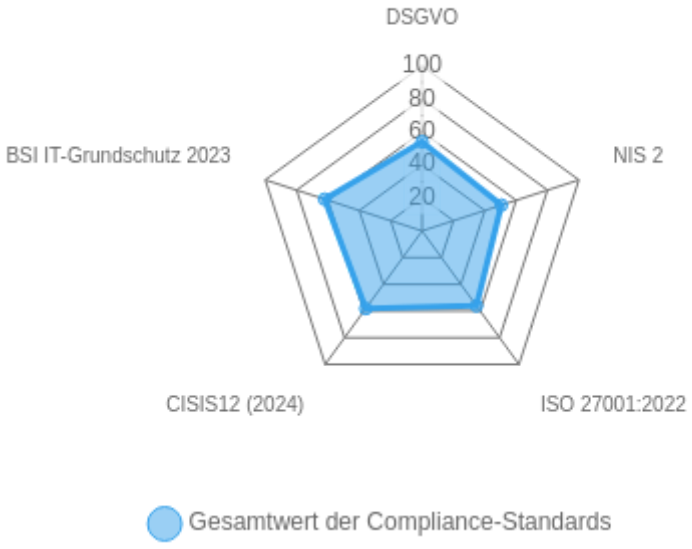
Ihr EASM Compliance-Status

Zeigt die technische Compliance der externen Angriffsfläche (ohne interne/organisatorische Faktoren).

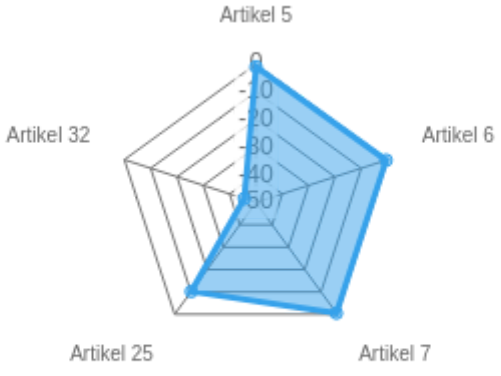
Das Compliance Mapping sorgt mit dem Abgleich der identifizierten Schwachstellen auf aktuelle regulatorische Anforderungen für Transparenz und deckt Abweichungen sowie Compliance-Risiken auf.

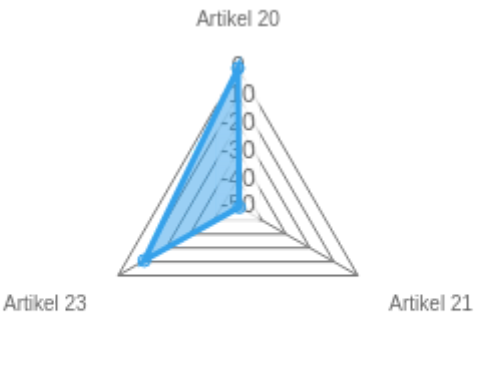
Das erste Radardiagramm zeigt das Abgleichergebnis in einer Übersicht zu allen Standards. Die max. erreichbare Punktzahl pro Standard beträgt 100. Identifizierte Schwachstellen werden als Minuspunkte an dem jeweiligen Standard von 100 abgezogen.

EASM Compliance-Mapping alle Standards

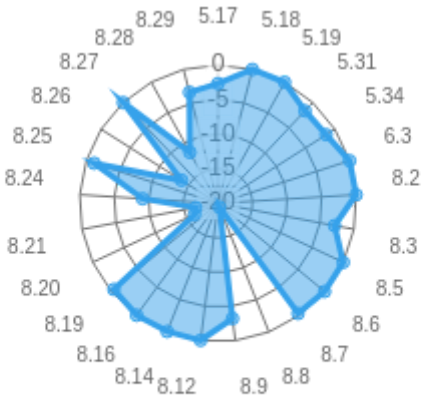


EASM Compliance-Mapping ausgewählte Standards

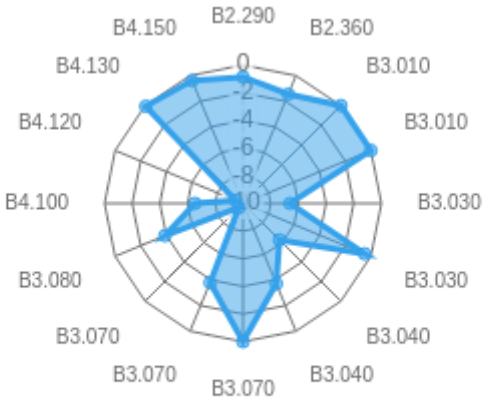




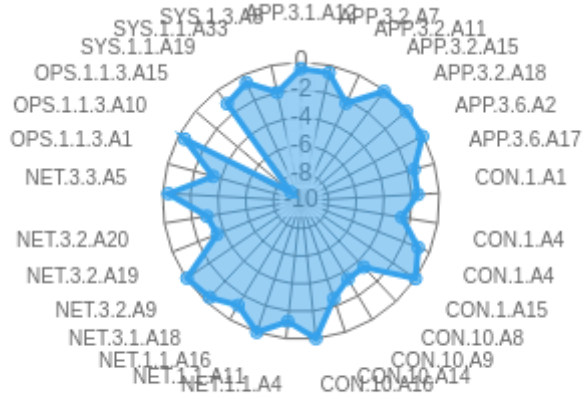
Ihr EASM Compliance-Status | Ergebnis für ausgewählte Standards



Gesamtpunktzahl der Abschnitte in ISO 27001:2022

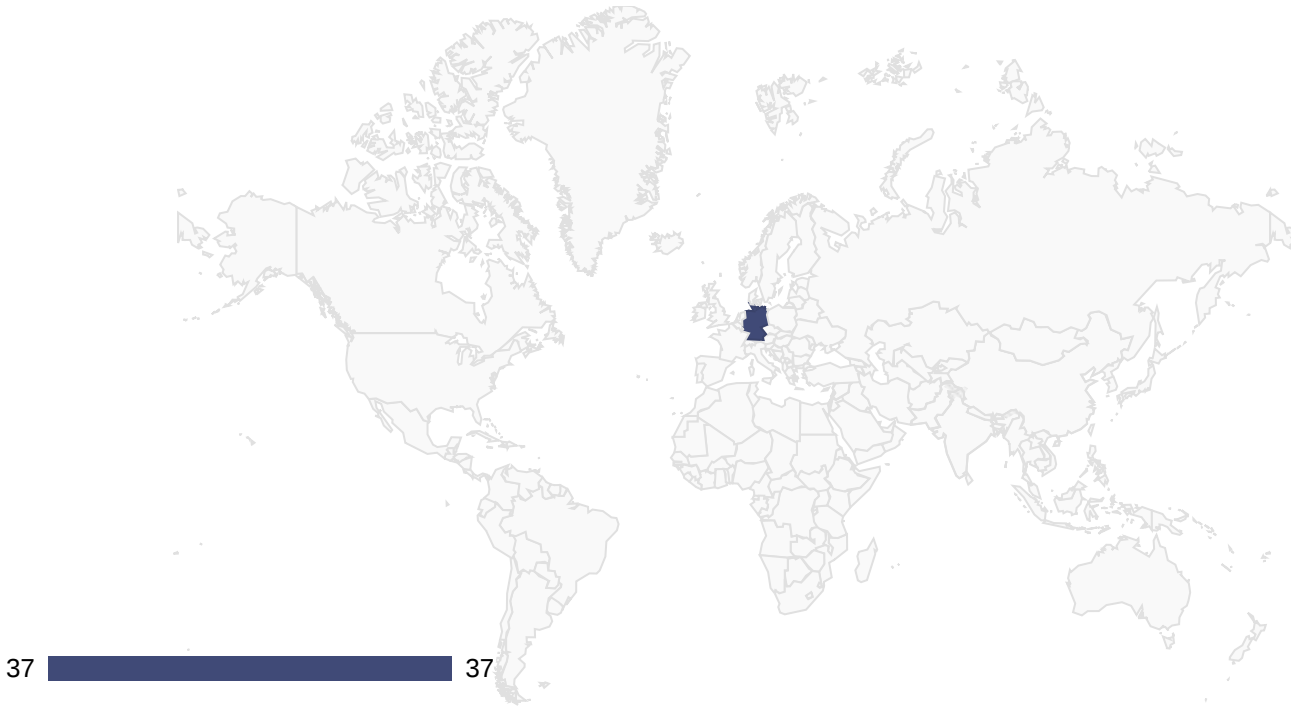


Gesamtpunktzahl der Abschnitte in CISIS12 (2024)

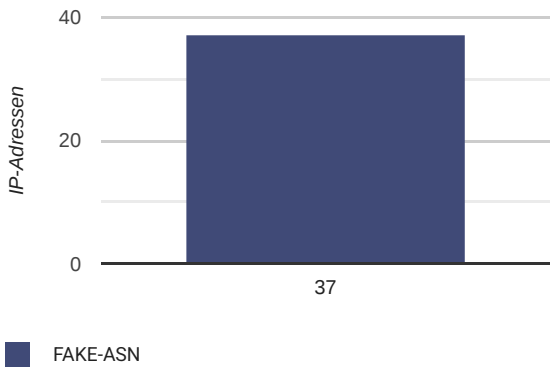


Gesamtpunktzahl der Abschnitte in BSI IT-Grundsch...

Ihre unternehmensweiten Serverstandorte



Ihre Top-IP-Adressbereichsanbieter



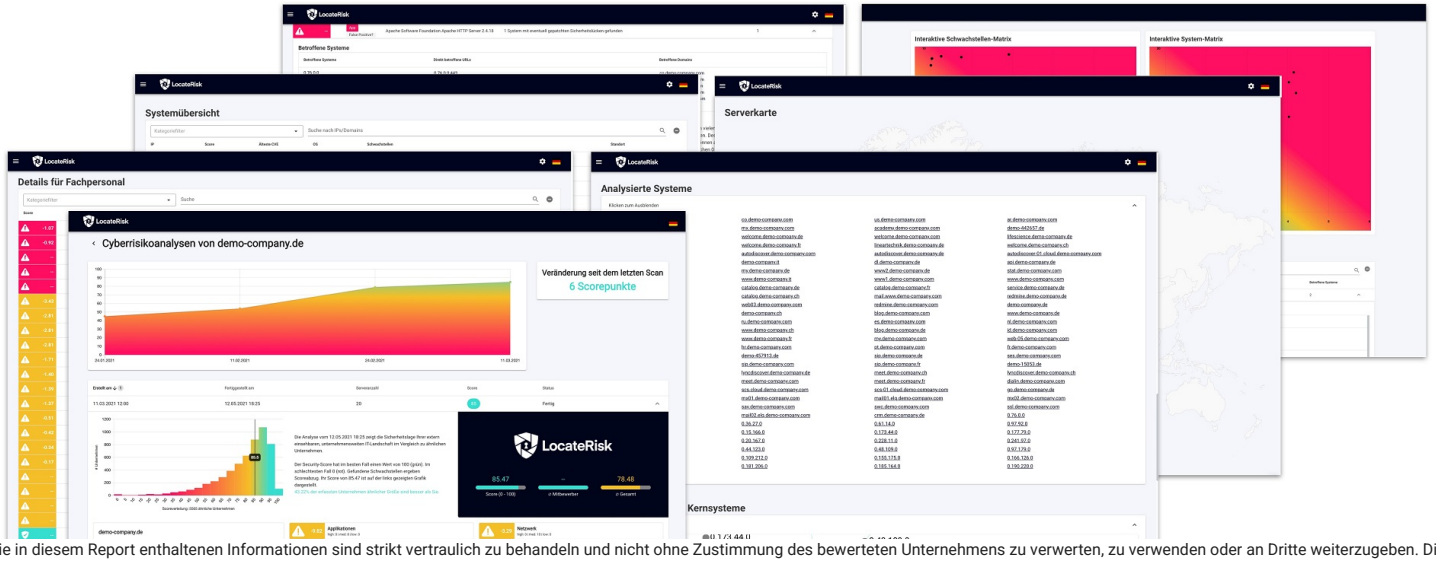
Analysierte Systeme

cms-demo-company.com.demo-211619.com
cms.demo-company.com
demo-26298.com
demo-company.com
demo-company.com.demo-211619.com
www.demo-company.com
demo-149841.com
fit.demo-company.com
demo-209878.com
meeting.demo-company.com
stun.demo-company.com
turn.demo-company.com
bis.demo-company.com
core.demo-company.com
mail02.demo-company.com
vsp.demo-company.com
app.element.demo-company.com
azure.demo-company.com
cloud.demo-company.com
extranet.demo-company.com
intranet.demo-company.com
mail03.demo-company.com
matrix.demo-company.com
owa.demo-company.com
ris.demo-company.com
service.demo-company.com
archiv.demo-company.com
archiv.feuerwehr.demo-company.com
bis2020.demo-company.com
buergerbus.demo-company.com
feuerwehr.demo-company.com
kneipp-verein.demo-company.com
sk.demo-company.com
tmp.demo-company.com
www.feuerwehr.demo-company.com
www.kneipp-verein.demo-company.com
demo-889675.com
ftp.demo-company.com
mail.demo-company.com
srv.demo-company.com
wahlen.demo-company.com
demo-949139.com
sentry.demo-company.com
ssl.demo-company.com
demo-508695.com
demo-560421.com
demo-569001.com
demo-330631.com
demo-402413.com
demo-48066.com
demo-188273.com
demo-738390.com
demo-607157.com
demo-726061.com
demo-768443.com
demo-21507.com
demo-377274.com
demo-970331.com
demo-3665.com
demo-638648.com
demo-970910.com
demo-679308.com
demo-472770.com
demo-927249.com
demo-517936.com
demo-350577.com

und 51 weitere Systeme

Sie wünschen tiefergehende Informationen?

Eine vollständige Übersicht über alle identifizierten Systeme und die entsprechenden Funde, inklusive Handlungsempfehlungen, ist in der interaktiven Schwachstellenliste enthalten. Wenn Sie mehr darüber erfahren möchten, wenden Sie sich gerne an uns.



Ihre aktuelle IT-Sicherheitslage | Die Top 10 Server

Score	Kritikalität	IP	Domains	Hoch	Mittel	Niedrig	Schwachstellen
-11.77	5	0.165.99.002	demo-638648.com	4	16	15	App, Web, SSL, Network, DSGVO, DNS
-8.92	5	192.168.1.13	example.com	1	0	0	Nessus
-7.91	4	0.182.223.0	demo-472770.com	3	28	25	App, Web, SSL, Network, DNS
-7.33	4	0.243.72.0	archiv.demo-company.com archiv.feuerwehr.demo-company.com bis2020.demo-company.com	3	127	110	App, Web, SSL, Network, DSGVO, DDOS
-5.92	4	0.192.73.0	demo-209878.com meeting.demo-company.com stun.demo-company.com	2	108	85	App, Web, SSL, Network, DNS, DDOS
-5.07	4	0.238.187.0	demo-949139.com sentry.demo-company.com ssl.demo-company.com	2	7	10	SSL, Network, DNS, DDOS
-3.85	3	192.168.1.14	login.example.com	0	1	0	Nessus
-3.52	4	0.165.99.010	demo-726061.com	1	17	17	App, Web, SSL, Network, DNS
-2.88	5	0.60.53.0	demo-3665.com	1	1	2	DNS
-2.72	4	0.60.100.0	bis.demo-company.com core.demo-company.com mail02.demo-company.com	2	47	62	App, Web, SSL, Network, DSGVO, DDOS

Ihre aktuelle IT-Sicherheitslage | Die Top 10 Schwachstellen

Score	Kritikalität	Schwachstelle	Beschreibung	Betroffene Systeme
-8.92	5	Unpatched Software	Outdated Software	1
-7.56	5	Anwendungen (Status unbekannt)	Erkannte Technologien ohne CVE-Zuordnung – Sicherheitsstatus unbekannt	6
-2.67	5	SPF-Konfiguration	SPF-Konfiguration	33
-3.70	4	Gültigkeitsdauer	Ablaufende oder abgelaufene Zertifikate	4
-3.41	4	Cyrus Mail Server 3.0.8	3 Systeme mit eventuell gepatchten Sicherheitslücken gefunden	3
-3.19	4	3389/tcp_ms-wbt-server	Der Remotezugriffsdienst RDP ist aus dem Internet erreichbar	1
-3.19	4	3306/tcp_mysql	Das Datenbanksystem MySQL ist aus dem Internet erreichbar	1
-1.68	4	Verschlüsselungsverfahren	Veraltete oder unsichere Verschlüsselungsverfahren	7
-1.47	4	Validierbarkeit	Nicht validierbare Zertifikate oder fehlerhafte Validierungspfade	9
-0.80	4	RC4	RC4 ciphers (angreifbar)	3