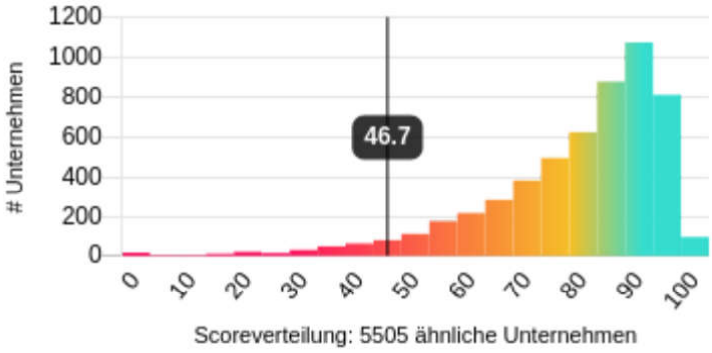
Managementübersicht | Ihre aktuelle IT-Sicherheitslage

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.

46.7	---	78.48
Security-Score*	Ø Mitbewerber**	Ø Gesamt***



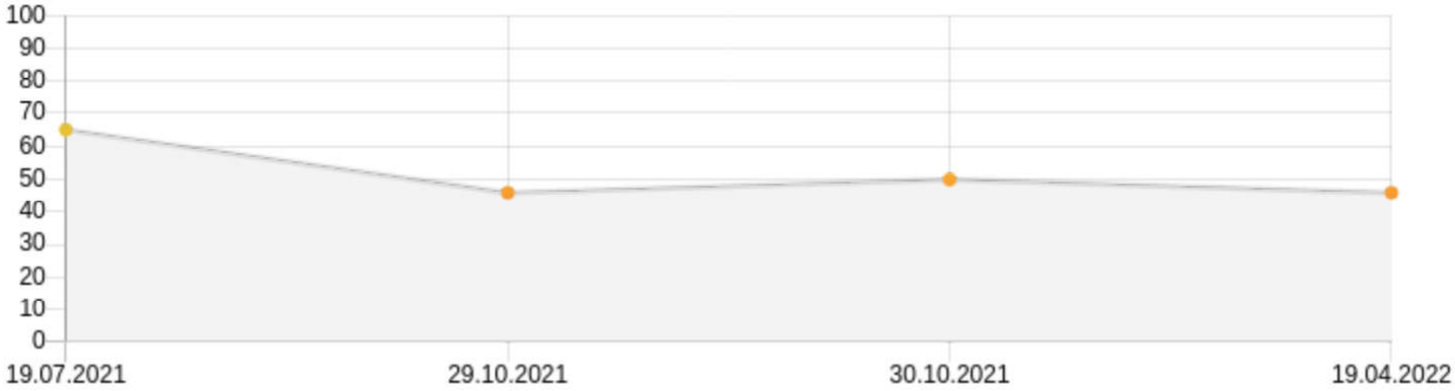
Mit einem Score von 46.7 liegt Ihr Ergebnis unter dem Durchschnitt. 94.7% der erfassten Unternehmen vglb. Größe (definiert nach der Serveranzahl) sind besser als Sie.

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 von bis zu 10 Unternehmen Ihrer Wahl
*** Durchschnittlicher Wert aller bewerteten Unternehmen

Funde 4041 high 117 | medium 1753 | low 2171	Erfasste Server 134	Geprüfte Domains 309

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.:

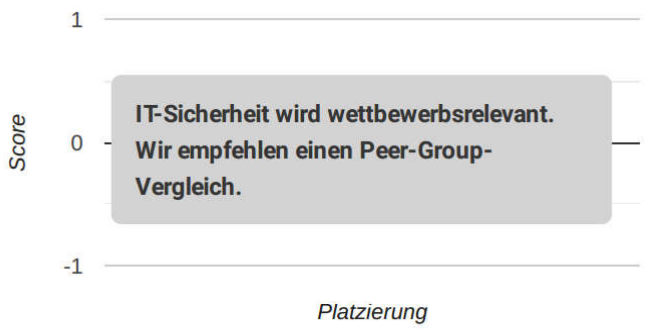
- NIST CIS (National Institute of Standards & Technology sowie das Center for Internet Security)
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- OWASP (Open Web Application Security Project) und viele mehr

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

Die in diesem Report enthaltenen Informationen sind strikt vertraulich zu behandeln und nicht ohne Zustimmung des bewerteten Unternehmens zu verwerten, zu verwenden oder an Dritte weiterzugeben. Die getroffenen Ratings und Analysen sind freie Meinungsäußerungen über zukünftige Sicherheitsrisiken. Es handelt sich nicht um Aussagen hinsichtlich der aktuellen und historischen Sicherheitslage von Unternehmen. Es handelt sich nicht um eine Zusicherung der Richtigkeit der Daten und der Schlussfolgerungen oder um den Versuch, die Sicherheitsmaßnahmen eines Unternehmens unabhängig zu bewerten oder dafür einzustehen. Für den Inhalt wird jegliche Haftung abgelehnt.

Sicherheitsvergleich | Cybersicherheit wird wettbewerbsrelevant

Ihre unternehmensweite IT-Sicherheitslage im Peer-Group-Vergleich



46.7
Ihr Status

--
Ø Peers

--
Ø Branche

78.48
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.

Für einen Peer-Group-Vergleich einfach Kontakt aufnehmen und uns 10 Mitbewerber Ihrer Wahl nennen.

Ihr IT-Risiko-Status im Peer-Group-Vergleich und 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.

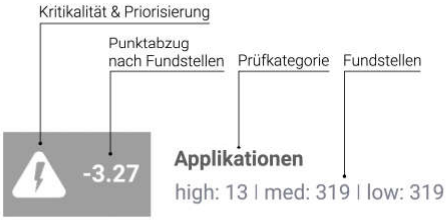
Prüfkategorien*	Ihr Status	Peer-Group	Unternehmen Gesamt
Applikationen	**-14.55**	--	-8.5
Web	**-19.63**	--	-1.8
Zertifikate	**-7.99**	--	-5.8
IP-Reputation	**0**	--	--
Netzwerk	**-6.18**	--	-6.2
DNS	**-3.61**	--	-3.2
DSGVO	**-1.33**	--	-1.4
Datenpannen	**--**	--	--
Scorewert 100-Minuspunkte =	**46.7**	--	73.5

Worst Case · Hohes Risiko · Moderates Risiko · Geringes Risiko

Die in diesem Report enthaltenen Informationen sind strikt vertraulich zu behandeln und nicht ohne Zustimmung des bewerteten Unternehmens zu verwerten, zu verwenden oder an Dritte weiterzugeben. Die getroffenen Ratings und Analysen sind freie Meinungsäußerungen über zukünftige Sicherheitsrisiken. Es handelt sich nicht um Aussagen hinsichtlich der aktuellen und historischen Sicherheitslage von Unternehmen. Es handelt sich nicht um eine Zusicherung der Richtigkeit der Daten und der Schlussfolgerungen oder um den Versuch, die Sicherheitsmaßnahmen eines Unternehmens unabhängig zu bewerten oder dafür einzustehen. Für den Inhalt wird jegliche Haftung abgelehnt.

Ihre aktuelle IT-Sicherheitslage | Die Prüfkategorien

Anhand der acht 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

-14.55	**Applikationen** high: 3 | med: 55 | low: 0	-6.18	**Netzwerk** high: 4 | med: 25 | low: 61
-19.63	**Web** high: 12 | med: 1499 | low: 1783	-3.61	**DNS** high: 7 | med: 25 | low: 57
-7.99	**Zertifikate** high: 73 | med: 133 | low: 206	-1.33	**DSGVO** high: 18 | med: 16 | low: 64
--	**IP-Reputation** high: 0 | med: 0 | low: 0	--	**Datenpannen** high: 0 | med: 43 | low: 0

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.

-14.55 **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.

-6.18 **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.**

Die in diesem Report enthaltenen Informationen sind strikt vertraulich zu behandeln und nicht ohne Zustimmung des bewerteten Unternehmens zu verwerten, zu verwenden oder an Dritte weiterzugeben. Die getroffenen Ratings und Analysen sind freie Meinungsäußerungen über zukünftige Sicherheitsrisiken. Es handelt sich nicht um Aussagen hinsichtlich der aktuellen und historischen Sicherheitslage von Unternehmen. Es handelt sich nicht um eine Zusicherung der Richtigkeit der Daten und der Schlussfolgerungen oder um den Versuch, die Sicherheitsmaßnahmen eines Unternehmens unabhängig zu bewerten oder dafür einzustehen. Für den Inhalt wird jegliche Haftung abgelehnt.

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.

Es wurden kritische Probleme in der Konfiguration der Webanwendungen gefunden. Aus unserer Sicht besteht dringender Handlungsbedarf, die entsprechenden Webanwendungen sollten abgesichert werden.

DNS | Ist Ihr Mailversand vor Identitätsraub geschützt?

Wie sicher sind Ihre Mitarbeiter vor Betrugsversuchen mit Pishing-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 Pishing-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.

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.

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.

Die in diesem Report enthaltenen Informationen sind strikt vertraulich zu behandeln und nicht ohne Zustimmung des bewerteten Unternehmens zu verwerten, zu verwenden oder an Dritte weiterzugeben. Die getroffenen Ratings und Analysen sind freie Meinungsäußerungen über zukünftige Sicherheitsrisiken. Es handelt sich nicht um Aussagen hinsichtlich der aktuellen und historischen Sicherheitslage von Unternehmen. Es handelt sich nicht um eine Zusicherung der Richtigkeit der Daten und der Schlussfolgerungen oder um den Versuch, die Sicherheitsmaßnahmen eines Unternehmens unabhängig zu bewerten oder dafür einzustehen. Für den Inhalt wird jegliche Haftung abgelehnt.

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.

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.

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.

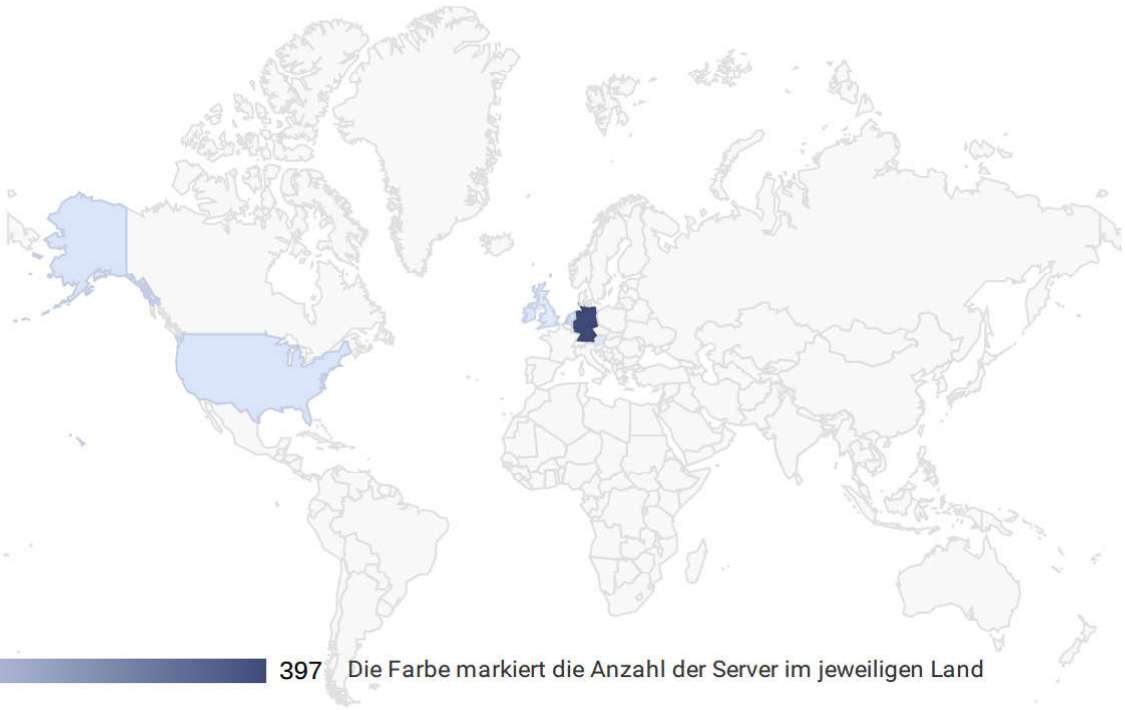
Cybervorfall Bei dem Business-Netzwerk LinkedIn wurden persönliche Daten von 500 Millionen LinkedIn-Nutzern abgeschöpft und stehen in einem Hacker-Forum zum Verkauf.

Es wurden E-Mail-Adressen Ihrer Mitarbeiter in einigen Datenleaks gefunden.*

*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.

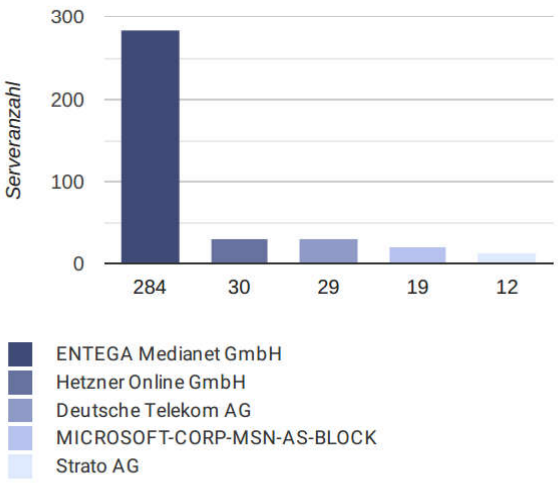
Die in diesem Report enthaltenen Informationen sind strikt vertraulich zu behandeln und nicht ohne Zustimmung des bewerteten Unternehmens zu verwerten, zu verwenden oder an Dritte weiterzugeben. Die getroffenen Ratings und Analysen sind freie Meinungsäußerungen über zukünftige Sicherheitsrisiken. Es handelt sich nicht um Aussagen hinsichtlich der aktuellen und historischen Sicherheitslage von Unternehmen. Es handelt sich nicht um eine Zusicherung der Richtigkeit der Daten und der Schlussfolgerungen oder um den Versuch, die Sicherheitsmaßnahmen eines Unternehmens unabhängig zu bewerten oder dafür einzustehen. Für den Inhalt wird jegliche Haftung abgelehnt.

Ihre unternehmensweiten Serverstandorte



1 397 Die Farbe markiert die Anzahl der Server im jeweiligen Land

Ihre Top-Serverbetreiber



Gartner

Bis 2022 werden Cybersecurity-Ratings bei der Beurteilung des Risikos von Geschäftsbeziehungen genauso wichtig werden wie Kreditratings.

Die in diesem Report enthaltenen Informationen sind strikt vertraulich zu behandeln und nicht ohne Zustimmung des bewerteten Unternehmens zu verwerten, zu verwenden oder an Dritte weiterzugeben. Die getroffenen Ratings und Analysen sind freie Meinungsäußerungen über zukünftige Sicherheitsrisiken. Es handelt sich nicht um Aussagen hinsichtlich der aktuellen und historischen Sicherheitslage von Unternehmen. Es handelt sich nicht um eine Zusicherung der Richtigkeit der Daten und der Schlussfolgerungen oder um den Versuch, die Sicherheitsmaßnahmen eines Unternehmens unabhängig zu bewerten oder dafür einzustehen. Für den Inhalt wird jegliche Haftung abgelehnt.

Analysierte Systeme

accas-group.com
www.accas-group.com
dialin.accas-group.com
webmail.accas-group.com
mailings.accas-group.com
autodiscover.accas-group.com
www.softecture.net
ftp.softecture.net
api.softecture.net
demoidp.softecture.net
www.acoris.de
acoris.de
h2341812.stratoserver.net
sac.mediamarket-world.de
wpdemo.softecture.net
saegmbh.com
aws.snsconnect.de
now.saegmbh.com
lyncdiscover.cairo.ag
sip.cairo.ag
mysite19dev.acoris.de
portal19.acoris.de

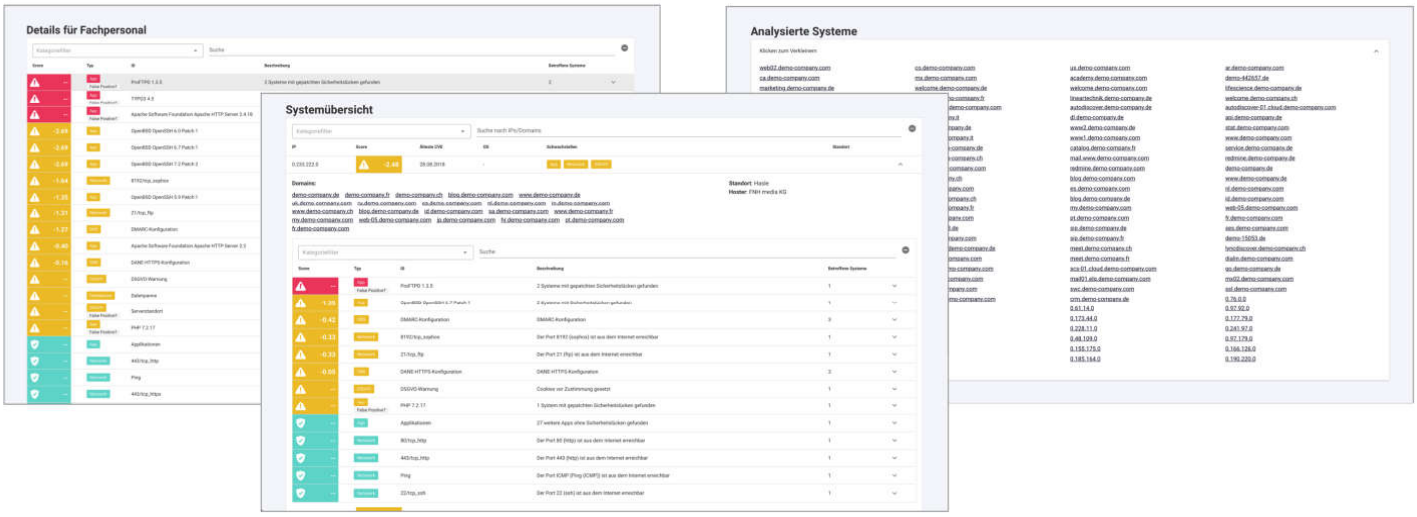
ndv.accas-group.com
mail.accas-group.com
cbooks.accas-group.com
prepaid.accas-group.com
securemail.accas-group.com
enterpriseregistration.accas-group.com
meet.softecture.net
web.softecture.net
sftp.softecture.net
softecture.net
web02.snsconnect.de
blog.snsconnect.de
www.accas-apps.com
office.softecture.net
business-24-114-26-1.pool2.vodafone-ip.de
dd7738.kasserver.com
p57f9b8c1a.dip0.t-ipconnect.de
www.fs.saegmbh.com
notes.saegmbh.com
sip.snsconnect.de
officeview.acoris.de
mysite19dev.acoris.de

sip.accas-group.com
login.accas-group.com
citrix.accas-group.com
chronos.accas-group.com
lyncdiscover.accas-group.com
data.softecture.net
softecture.de
sonar.softecture.net
mail.softecture.net
mail.softecture.de
data.snsconnect.de
prod.web.acoris.de
daisy13.accas-apps.com
ip-037-024-072.um08.pools.vodafone-ip.de
www.saegmbh.com
dokuwiki.snsconnect.de
fs.saegmbh.com
lyncdiscover.snsconnect.de
www.notes.saegmbh.com
webext.acoris.de
mailer.acoris.de
sysklddev.acoris.de

und 678 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.



Die in diesem Report enthaltenen Informationen sind strikt vertraulich zu behandeln und nicht ohne Zustimmung des bewerteten Unternehmens zu verwerten, zu verwenden oder an Dritte weiterzugeben. Die getroffenen Ratings und Analysen sind freie Meinungsäußerungen über zukünftige Sicherheitsrisiken. Es handelt sich nicht um Aussagen hinsichtlich der aktuellen und historischen Sicherheitslage von Unternehmen. Es handelt sich nicht um eine Zusicherung der Richtigkeit der Daten und der Schlussfolgerungen oder um den Versuch, die Sicherheitsmaßnahmen eines Unternehmens unabhängig zu bewerten oder dafür einzustehen. Für den Inhalt wird jegliche Haftung abgelehnt.