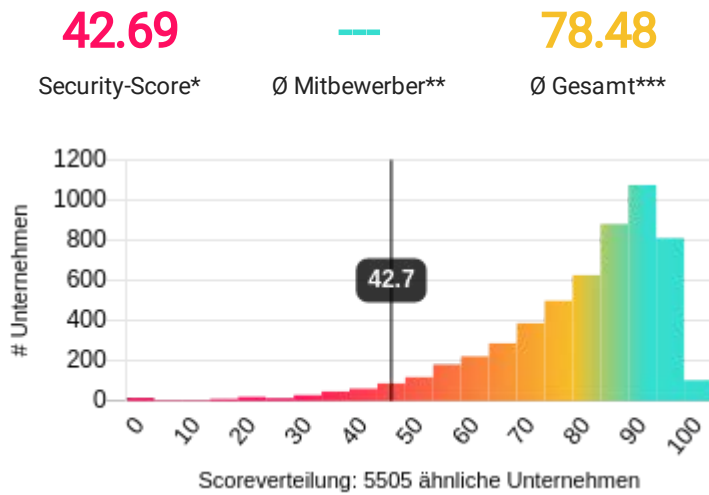


Managementübersicht | Ihre aktuelle IT-Sicherheitslage

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



Mit einem Score von 42.69 liegt Ihr Ergebnis unter dem Durchschnitt. 95.91% 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

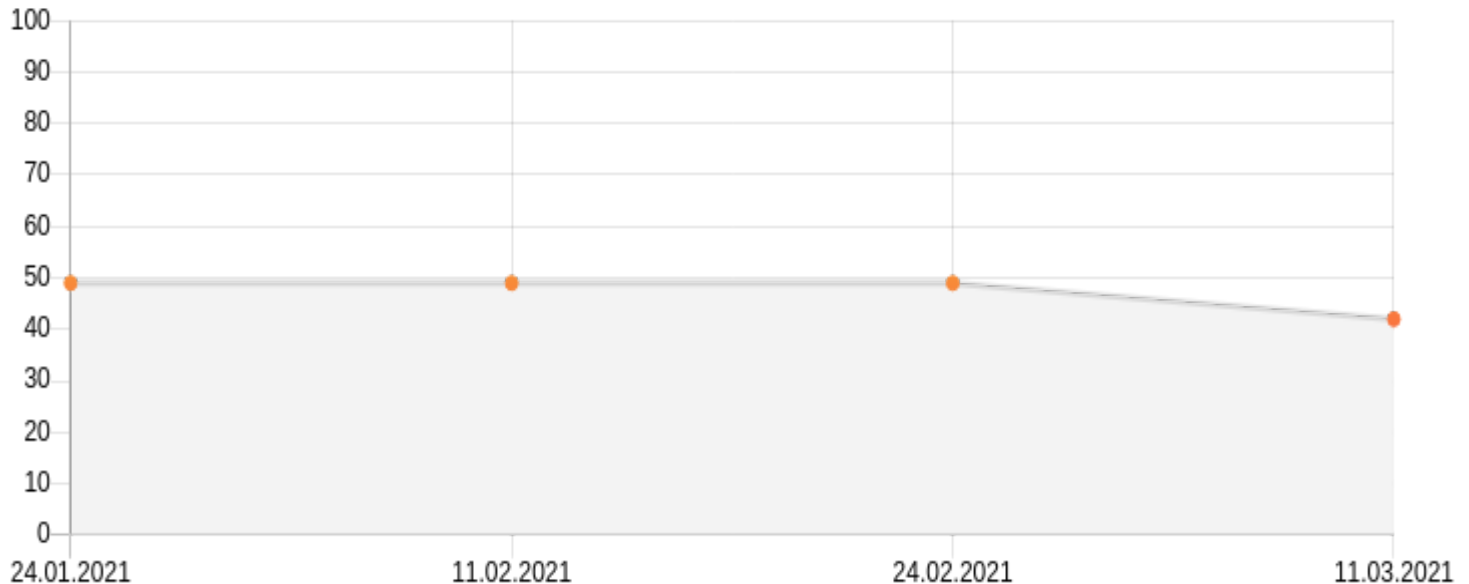
Funde 942

high 38 | medium 486 | low 418

Erfasste Server 14

Geprüfte Domains 75

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.:

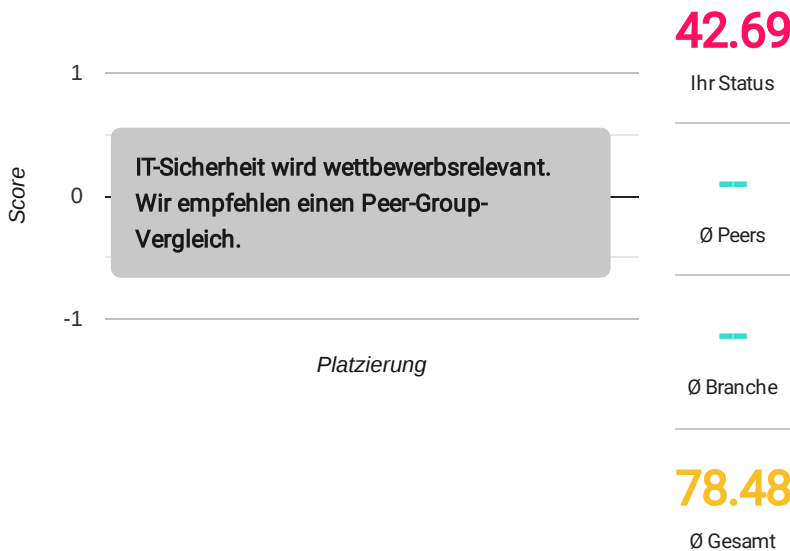
- NIST CIS (National Institute of Standards & Technology sowie das Center for Internet Security)
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- OWASP (Open Web Application Security Project) und viele mehr

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 verwenden, zu veröffentlichen 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

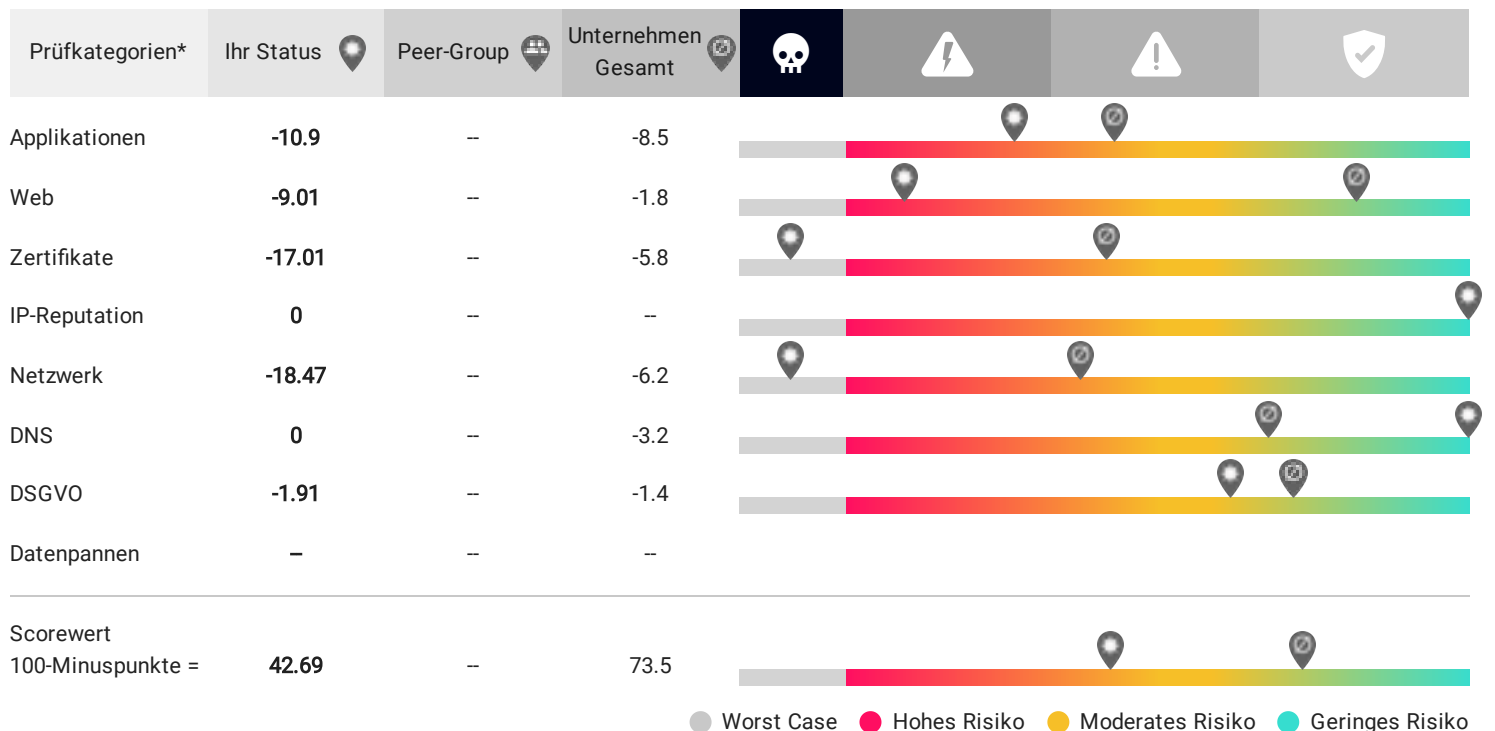
Ihre unternehmensweite IT-Sicherheitslage im Peer-Group-Vergleich



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.

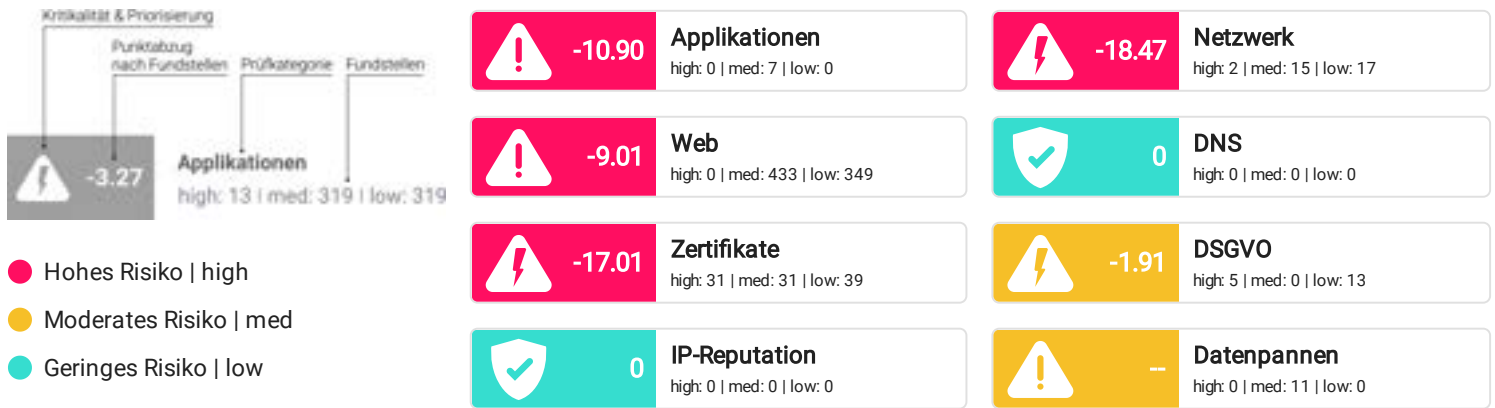
Ihr IT-Risiko-Status im Peer-Group-Vergleich und zum Durchschnitt aller geprüften Unternehmen Ihrer Branche. Sie sehen, in welcher Prüfkategorie Ihr Unternehmen in punkto Sicherheit vorne liegt und wo es Nachholbedarf gibt. Das Ranking basiert auf Fundstellen, die je nach Kritikalität zu Minuspunkten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



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.



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.

-10.90

Es fehlen Updates auf Ihren Systemen. Wir empfehlen, die eingesetzte Software diesbezüglich zu prüfen.

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.

-18.47

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 verwerfen, 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.



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

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.



Wir konnten an Ihrer DNS-Konfiguration keine Schwächen finden.

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 verwerfen, 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.

Cybevorfall 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.

Cybevorfall 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.

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

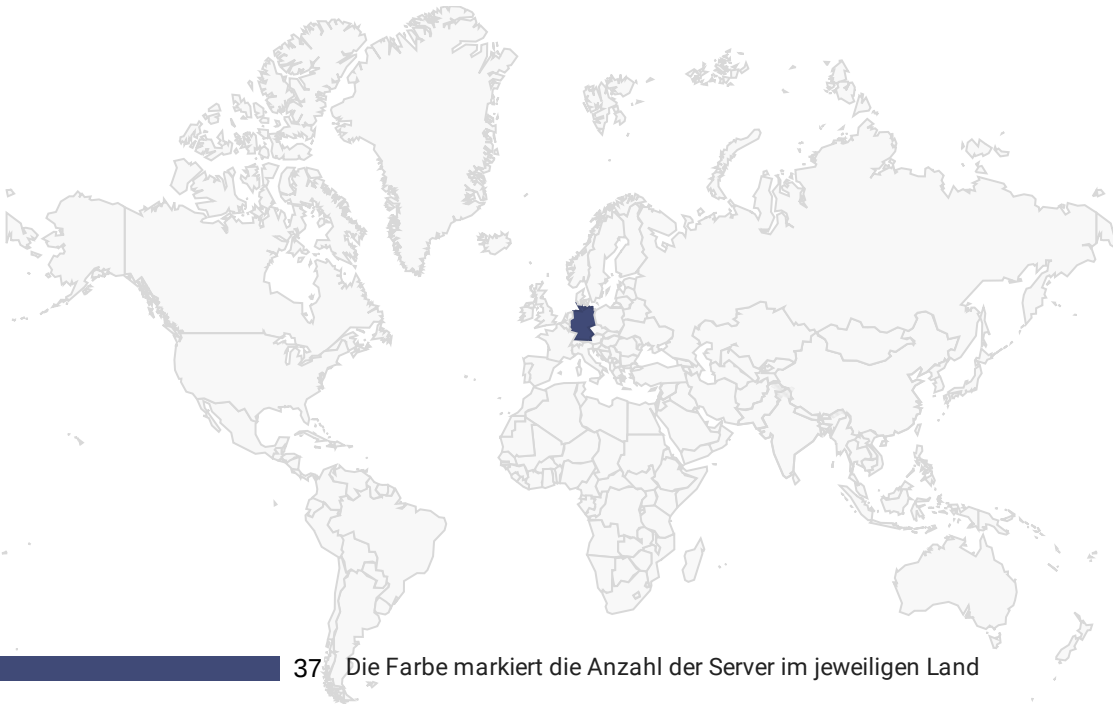


Es wurden E-Mail-Adressen Ihrer Mitarbeiter in einigen Datenleaks gefunden.*

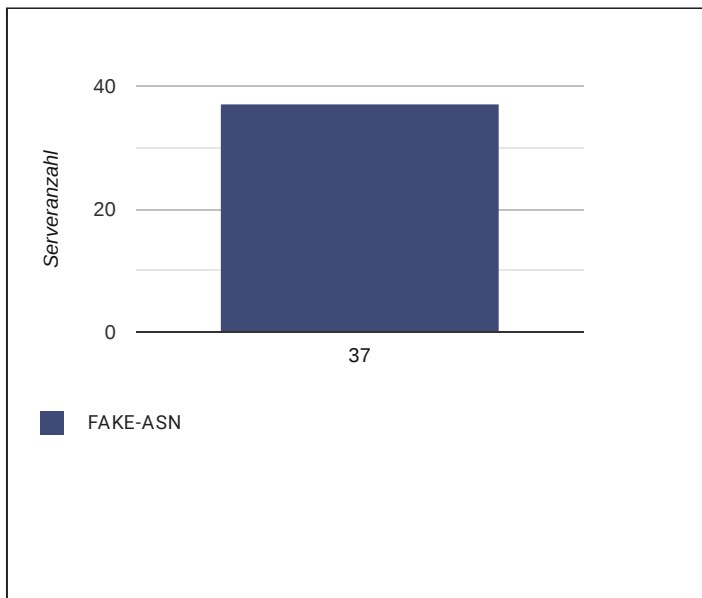
*Unsere Möglichkeiten sind aus Datenschutzgründen limitiert. Über die Web-App <https://haveibeenpwned.com/DomainSearch> finden Sie heraus, welche Accounts betroffen sind. Sorgen Sie dafür, dass Mitarbeiter gestohlene Passwörter ändern und niemals Passwörter doppelt verwenden.

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



Ihre Top-Serverbetreiber



NEU!

Für mehr Sicherheit in der Lieferkette

Testen Sie die Plattform zur vollautomatisierten IT- und DSGVO-Compliance-Prüfung von Geschäftspartnern, Dienstleister und Lieferanten.

Senden Sie eine Nachricht an sales@locaterisk.com oder rufen Sie uns an unter +4961516290246.

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

demo-company.com.demo-211619.com
 cms.demo-company.com
 fit.demo-company.com
 ris.demo-company.com
 ftp.demo-company.com
 turn.demo-company.com
 mail.demo-company.com
 mail02.demo-company.com
 archiv.demo-company.com
 meeting.demo-company.com
 extranet.demo-company.com
 buergerbus.demo-company.com
 kneipp-verein.demo-company.com
 www.kneipp-verein.demo-company.com
 demo-209878.com
 demo-508695.com
 demo-48066.com
 demo-188273.com
 demo-726061.com
 demo-377274.com
 demo-638648.com

demo-company.com
 www.demo-company.com
 bis.demo-company.com
 owa.demo-company.com
 srv.demo-company.com
 stun.demo-company.com
 azure.demo-company.com
 matrix.demo-company.com
 wahlen.demo-company.com
 service.demo-company.com
 intranet.demo-company.com
 app.element.demo-company.com
 www.feuerwehr.demo-company.com
 demo-26298.com
 demo-889675.com
 demo-560421.com
 demo-402413.com
 demo-738390.com
 demo-768443.com
 demo-970331.com
 demo-970910.com

sk.demo-company.com
 cms-demo-company.com.demo-211619.com
 vsp.demo-company.com
 tmp.demo-company.com
 ssl.demo-company.com
 core.demo-company.com
 cloud.demo-company.com
 mail03.demo-company.com
 sentry.demo-company.com
 bis2020.demo-company.com
 feuerwehr.demo-company.com
 autodiscover.demo-company.com
 archiv.feuerwehr.demo-company.com
 demo-149841.com
 demo-949139.com
 demo-569001.com
 demo-330631.com
 demo-607157.com
 demo-21507.com
 demo-3665.com
 demo-679308.com

und 41 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.