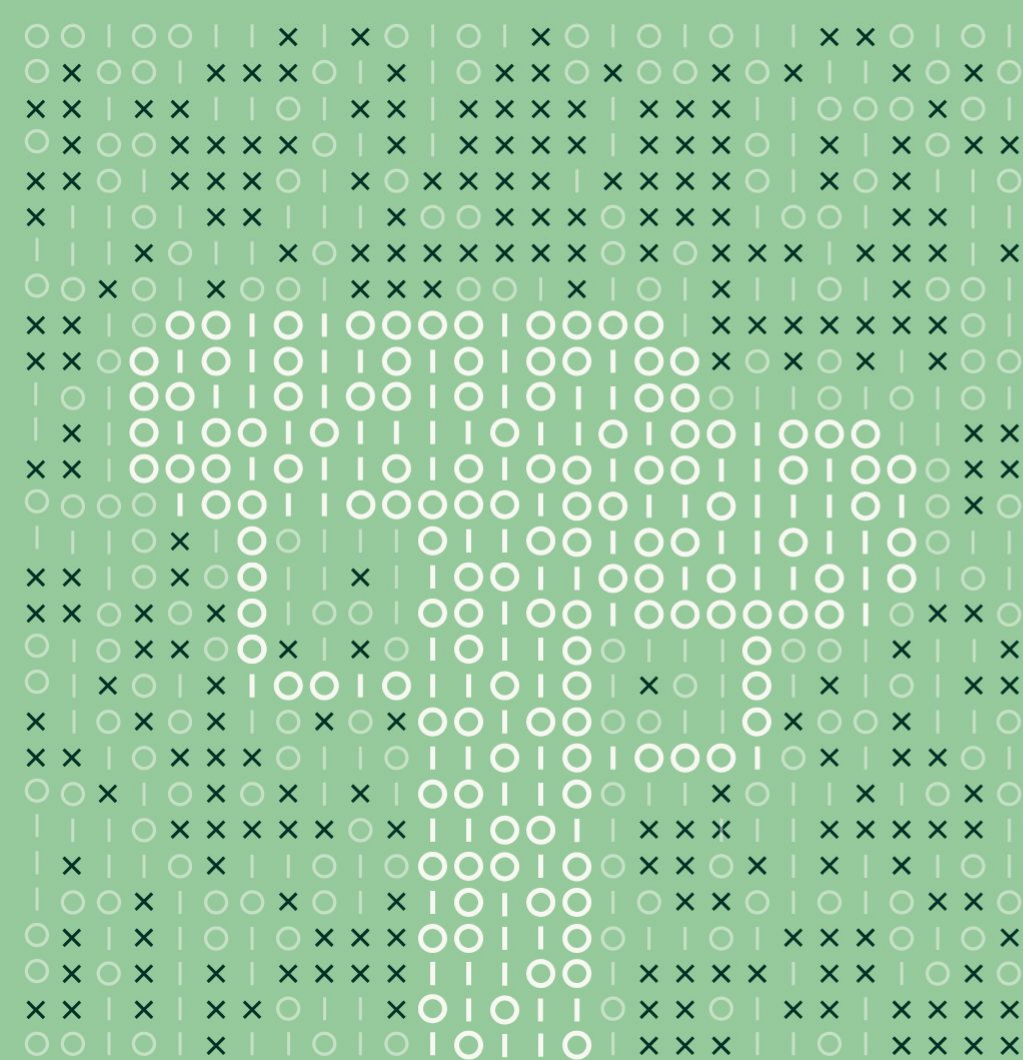




baobab



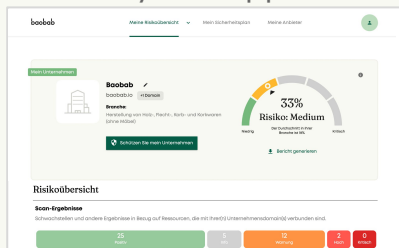
Baobab Insurance

Cyber-Assekuradeur mit integrierter
Cyber-Security und -Versicherung

Baobab – Cyber-Assekuradeur mit integrierter Cyber-Security und -Versicherung

Effektive Bedarfsweckung

Interaktive Bedarfsweckung durch Risikovisualisierung und Ad-Hoc Cyber Support



Baobab als Assekuradeur

Maklerfreundliches Underwriting mit Transparenz, Schnelligkeit & ganzheitlicher Risikobewertung

Marktführendes Bedingungsmerk mit Autonomie bis 100€ Mio Umsatz & 5 € Mio VS



Nachhaltige Risikominderung

Kostenloser Cyber Security Scan und Beratung für Kunden zur nachhaltigen Risikominderung

Führendes Cyber Security Partner-Netzwerk, die mit Rabatten bei Risikominderung unterstützen



Erfahrenes Team aus Versicherungs- und Cyberexperten



Vincenz Klemm
Geschäftsführer & Gründer

Gründer von Gabi, dem größten digitalen Sachversicherungs-makler der USA



Anton Foth
CTO & Gründer

Ex-CTO des Vollversicherers Coya und CTO zahlreicher BCG DV Ausgründungen



Andrew Saula
Leiter Cyber Security

Ex-Leiter des "Red Teams" & Technical Policy bei TUI, Leitung des offensiven Sicherheitsteams



John Braun
Leiter Vertrieb

Ex-Leiter der Broker Distribution von CyberDirekt und Willis Germany

Versicherungs- und Cyberexperten bauen die führende Cyber-Versicherung in Europa



Vincenz Klemm
Geschäftsführer &
Co-Gründer

Gründer von *Gabi*, dem größten digitalen Sachversicherungsmakler der USA



Anton Foth
Geschäftsführer (CTO),
Co-Gründer

Ex-CTO des Vollversicherers *Coya* und CTO zahlreicher *BCG DV* Ausgründungen



John Braun
Leiter Vertrieb

Ex-Leiter der Broker Distribution von *CyberDirekt* und *Willis Germany*



Benedikt Klingenheben
Leiter Cyber Underwriting

Ex-Cyber Underwriter und Practise Leader Mid-Market *Chubb*, davor *AIG*



Manuela Solescu
Leiterin Digitales Produkt

Ex-Produktleiterin *Wefox* (Aufbau Versicherungsportal) & Produktmanagerin bei *Revolut*



Andrew Saula
Leiter Cyber-Security

Ex-Leiter des "Red Teams" & Technical Policy bei *TUI*, Leitung des offensiven Sicherheitsteams



Jakob Merz
Strategie & Operations Lead

Ex-Berater bei der *Boston Consulting Group* mit Fokus auf Versicherungsbranche

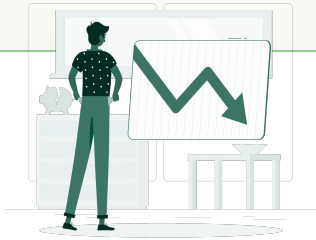
Bedarfsweckung und Risikovisualisierung im Kundenportal

Risikogerechte Absicherung mit Hilfe des Maklerportals

Bestandteile einer Cyber-Versicherung

FAQ

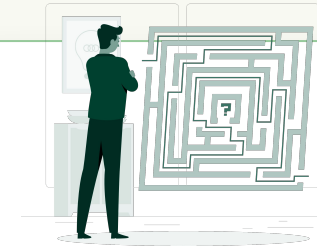
Cyberangriffe sind eine ernsthafte Bedrohung für KMUs, die weiter rapide zunehmen wird



Ransomware Angriffe haben sich in den letzten 2 Jahren verdoppelt ¹



Hacker automatisieren die Suche nach Schwachstellen in Unternehmen ²



KMU haben Schwierigkeiten, Lösungen für den Umgang mit Cyberrisiken zu finden ³

MunichRe erwartet, dass KMUs überproportional von Cyberangriffen betroffen sind und der Haupttreiber für die wachsende Nachfrage nach Cyber-Versicherungen sein werden. ⁴

1. Cyber Economics; 2. Bleuwire; 3. Welche Einstellungsänderungen sind erforderlich, damit KMU einen strategischen Ansatz für die Informationssicherheit wählen; 4. Munich Re

KMU können Cyber-Risiken nicht selber mindern oder auf auftretende Bedrohungen reagieren

46%

der deutschen KMUs
waren im letzten Jahr
von einem
Cyberangriff betroffen

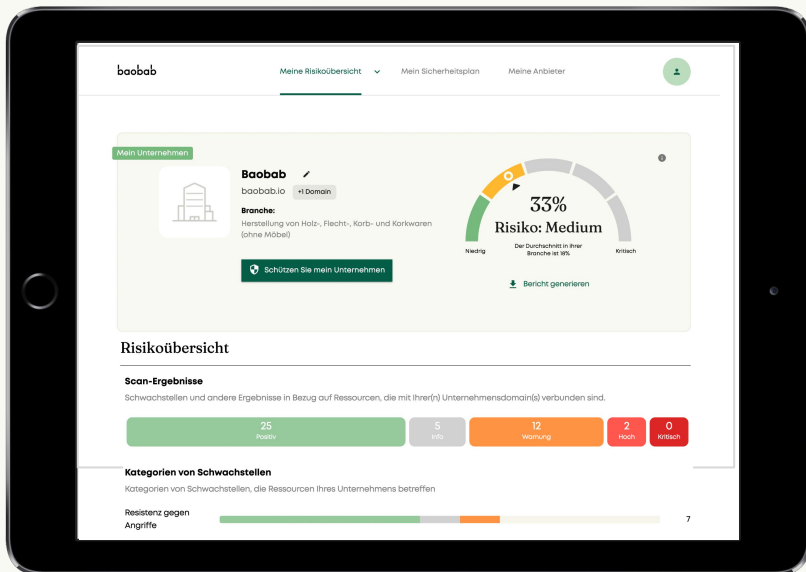
2 Jahre

durchschnittl. Alter der
Schwachstelle, die bei
Cyberangriffen genutzt
wird

<30%

der KMUs nutzen
Logging-/Warnsysteme
oder Cyber-Security
Schulungen

Baobab befähigt Makler erfolgreich Cyber-Policen zu platzieren



Risikobewusstsein

KMUs glauben fälschlicherweise, dass sie kein Ziel von Hackern sind, weil sie "klein" sind oder "eine gute IT-Sicherheit" haben



Lösungsorientierte Diskussion

KMUs verfügen selten über Fachwissen, um die Cyber-Security selbst zu verbessern



Cyber-Sicherheitsberatung

Begleitung auf dem Weg zur Versicherbarkeit

Analyse der Schwachstellen

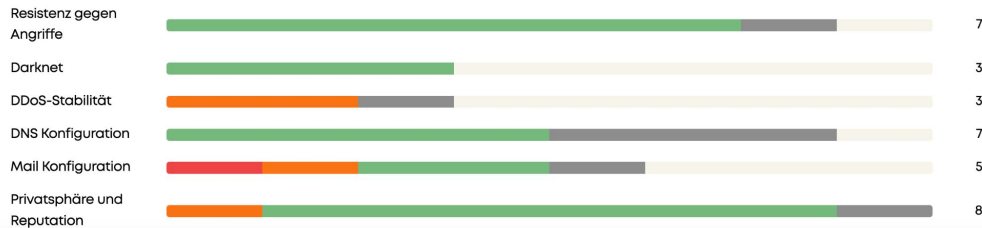
Scan-Ergebnisse

Schwachstellen und andere Ergebnisse in Bezug auf Ressourcen, die mit Ihrer(n) Unternehmensdomain(s) verbunden sind.



Kategorien von Schwachstellen

Kategorien von Schwachstellen, die Ressourcen Ihres Unternehmens betreffen



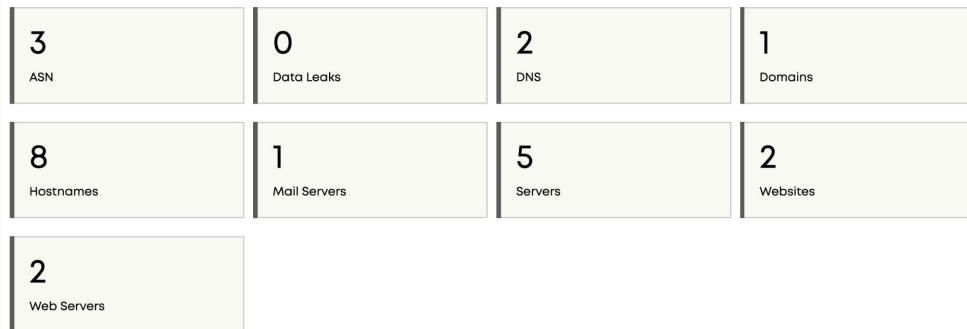
Risikobewusstsein

Mithilfe des Risiko-Scans kann das individuelle Risiko Ihrer Kunden visualisiert werden.

Aufzeigen der IT-Infrastruktur

Entdeckte Ressourcen

Die IT-Infrastruktur Ihres Unternehmens, die mit Ihrer Unternehmens-Domain verbunden und nach außen hin sichtbar ist.



Risikobewusstsein

Anhand der IT-Infrastruktur Ihrer Kunden, können Sie aufzeigen, was auch Hacker sehen können.

Cyber-Sicherheitsplan

Mein Cyber-Sicherheitsplan

Hier sind die wichtigsten Maßnahmen, die Sie auf Grundlage der ermittelten Schwachstellen ergreifen sollten.

[actionarius.de](#) [codeconcept.pl](#) [porsche.com](#)

Filter

Keine Filter angewendet

↓	BEZEICHNUNG	
⬆	🔒 Laut BSI IT-Grundschutz-Richtlinie soll die Anzahl der offenen Ports so gering wie möglich gehalten werden. Erkannte oder notwendige o...	⋮
⬆	🔒 Es wird empfohlen, die Konfiguration der TLS-Verschlüsselung auf dem Mailserver zu überprüfen.	⋮
⬆	🔒 Es sollten nur die sicheren Verschlüsselungstechnologien (TLS 1.2 und TLS 1.3) verwendet werden. Die alten Versionen müssen in der Konfig...	⋮
⬆	🔒 Es wird empfohlen, die Konfiguration der TLS-Verschlüsselung auf dem Webserver zu überprüfen.	⋮
⬆	🔒 Es sollten nur die sicheren Verschlüsselungstechnologien (TLS 1.2 und TLS 1.3) verwendet werden. Die alten Versionen müssen in der Konfig...	⋮
⊞	🔒 Das CMS sollte nur für berechtigte Personen sichtbar gemacht werden. Häufig dient der Zugang externen Agenturen, die die Webseiten...	⋮
⊞	🔒 Die komplette IT-Infrastruktur muss schnellstmöglich fachmännisch auf Malware, unerlaubte Zugriffe und andere Schäden überprüft we...	⋮
⊞	🔒 Es sollte darauf geachtet werden, dass Passwörter regelmäßig geändert werden und die Mitarbeiter dazu angehalten werden, die beruf...	⋮



Lösungsorientierte Diskussion

Best Practises ermöglichen Einblick in die Materie, ohne eigene Recherche oder eigenes Know How

Cyber-Sicherheitspartner-Netzwerk



Cyber-Sicherheitsberatung

Begleitung auf dem Weg zur
Versicherbarkeit

Cyber-Sicherheitspartner-Netzwerk



Asset Security

Action1 Lansweeper DEVICE42

Remote access management

REALVNC

Email security

DMARC by RED SIFT NINBOX by RED SIFT

Backups and Recovery

Simple Backups IDrive

1



Cyber-Sicherheitsberatung

Begleitung auf dem Weg zur
Versicherbarkeit

Bedarfsweckung und Risikovisualisierung im Kundenportal

Risikogerechte Absicherung mit Hilfe des Maklerportals

Bestandteile einer Cyber-Versicherung

FAQ

Versicherer können Cyber-Risiken oft nicht korrekt bewerten, da Verständnis für Cyber fehlt



Symptome

Engerer Cyber-Versicherungsmarkt
Prämien erhöhungen um
>300 % und Einschränkung
des Versicherungsschutzes

Ursachen

Keine Bewertung der Cyber-Risikoexposition
Die Versicherer bewerten
Cyber-Risiken eines Unternehmens
nicht auf Basis von Schwachstellen

Kein differenziertes Portfoliomgmt.
Auf hohe Schadenquoten wird
portfolioweit mit höheren Preisen &
geringerer Deckung reagiert

Cyber-Risiken müssen differenziert und individualisiert bepreist werden



Inputs, die in die Risikobewertung einfließen

A	Unternehmensdaten	Branche, Umsatz, Online-Anteil, Anzahl der Mitarbeiter
B	Risiko-Fragebogen	IT-Sicherheitsverfahren, Zahlungsrisiken, organisatorische Maßnahmen
C	Bewertung der Angriffsoberfläche	Scan, Erkennen von Sicherheitsverletzungen, Risikominderungsmaßnahmen

Bedarfsweckung und Risikovisualisierung im Kundenportal

Risikogerechte Absicherung mit Hilfe des Maklerportals

Bestandteile einer Cyber-Versicherung

FAQ

Incident Response

Betriebsunterbrechung

Daten- &
Systemwiederherstellung

Epressungsbedingte
Zahlungen

Koordination der Reaktion auf den Vorfall

- 24/7 Hotline mit IT-Experten
- Inanspruchnahme einer Computer-Forensik-Firma, die die Ursache bzw. das "Einfallstor" ermitteln kann
- Koordination von Maßnahmen, die u.a. im Rahmen der Datenschutzbestimmungen anfallen

Incident Response

Betriebsunterbrechung

Daten- &
Systemwiederherstellung

Epressungsbedingte
Zahlungen

Betriebsunterbrechungsschaden, der durch den Vorfall entsteht (max. 6 Monate nach dem Vorfall)

- Es ist wichtig zu verstehen, wie sich eine Betriebsunterbrechung bei dem jeweiligen Kunden auswirkt (z.B. Können Endkunden auf Substitute zurückgreifen? Wie schnell kann der Kunde zum Tagesgeschäft zurückkehren?)

Incident Response

Betriebsunterbrechung

Daten- &
Systemwiederherstellung

Epressungsbedingte
Zahlungen

- Wiederherstellung oder Rekonstruktion von **beschädigten, gefährdeten oder verlorenen Daten**
- Reparatur oder Wiederherstellung von **Software oder Anwendungen**

Incident Response

Betriebsunterbrechung

Daten- &
Systemwiederherstellung

Erpressungsbedingte
Zahlungen

Übernahme **notwendiger und angemessener Erpressungs-Zahlungen**

- Daten können nach Verschlüsselung nicht wieder hergestellt werden
- Verkauf der Daten soll verhindert werden
- Kosten für Zahlung sind günstiger als Betriebsunterbrechung
- Zahlung ist erfolgsversprechend

Drittschadenversicherung

Verbraucherentschädigungsfonds

PCI Vertragsstrafen

Medienrechtsverletzung

Versicherungsschutz bei **Inanspruchnahme durch Dritte** in Bezug auf Cyber-Vorfall

- Prüfung der Haftpflichtfrage
- Abwehr unberechtigter Ansprüche
- Freistellung von berechtigten Ansprüchen –
Ausschließlich echte Vermögensschäden inklusive immaterieller Ansprüche und Schmerzensgeld (emotional distress)

Drittschadenversicherung

Verbraucherentschädigungsfonds

PCI Vertragsstrafen

Medienrechtsverletzung

Verbraucherentschädigungsfonds = Rechtskonstrukte, die eher im Amerikanischen Rechtsraum geläufig sind

- Unternehmen können dazu verurteilt werden, dass sie in einen Entschädigungsfonds einzahlen müssen, aus dem Verbraucher entschädigt werden können
- In Europa ist dies bislang keine gängige Praxis

Drittschadenversicherung

Verbraucherentschädigungsfonds

PCI Vertragsstrafen

Medienrechtsverletzung

Vertragsstrafen wegen Verletzung des **Payment-Card-Industrie (PCI)- Datensicherheitsstandards**

- Wer PCI-Daten speichert, verspricht deren Sicherheit – mindestens im Kleingedruckten
- PCI-Daten sind vollständige Kreditkartendaten, die sich wie folgt zusammensetzen:
 - Name des Karteninhabers
 - Kartennummer
 - Prüfziffer

Drittschadenversicherung

Verbraucherentschädigungsfonds

PCI Vertragsstrafen

Medienrechtsverletzung

Versicherungsschutz wegen **tatsächlichen oder behaupteten Medienrechtsverletzungen**

- Verunglimpfungen oder Rufschädigungen einer Person/ eines Unternehmens, Diffamierung, Verleumdung, Beleidigung, etc.
- Plagiate oder irreführende Werbung
- Verletzung des Urheberrechts, Domainnamens, der Aufmachung, des Titels oder des Slogans

Verbesserungskosten

Cyber-Kriminalität

Social-Engineering-Betrug

Cloud-Ausfall Betriebsunterbrechung

Verbesserungskosten sind die Kosten, die anfallen um den Kunden mit einem aktuellen System wieder arbeitsfähig zu machen

- Ein Beispiel: Der Kunde hat eine on-premise Lösung für seine Kundenverwaltung (Anwendungsserver: MS 2012 R2) und es kommt zur Beschädigung
- Es ergibt keinen Sinn den Server mit der Version von vor dem Angriff wiederherzustellen

Verbesserungskosten

Cyber-Kriminalität

Social-Engineering-Betrug

Cloud-Ausfall
Betriebsunterbrechung

Vermögensschäden infolge eines **Cyber-Diebstahls** oder **Telekommunikationsbetrug**

- Cyber-Diebstahl = Abfluss von Geld, Crypto oder Wertpapieren durch einen unbefugten Zugriff
- Telekommunikationsbetrug = unberechtigt in Anspruch genommene Sprach- und Datengebühren oder nicht genehmigte Bandbreite

Verbesserungskosten

Cyber-Kriminalität

Social-Engineering-Betrug

Cloud-Ausfall
Betriebsunterbrechung

Social-Engineering = Angriffe bei denen Täter menschliche Eigenschaften und Verhaltensweisen als Angriffsfläche nutzen

- Ein Beispiel: Fake President-Angriffe → Angreifer geben sich als Geschäftsführer aus, um Mitarbeiter zur Überweisung von Geldbeträgen zu bewegen
- Wird bei uns nur abgedeckt, wenn der Social Engineering Attacke ein unbefugter Zugriff vorausgeht

Verbesserungskosten

Cyber-Kriminalität

Social-Engineering-Betrug

Cloud-Ausfall
Betriebsunterbrechung

Betriebsunterbrechungsschäden aufgrund eines Cyber-Vorfalls in dem Teil des versicherten Computersystems, welcher der **Herrschaftsgewalt und Kontrolle eines dritten Dienstleisters** (z. B. externes Rechenzentrum, Cloud-Anbieter) **unterliegt**, den ein versichertes Unternehmen entgeltlich in Anspruch nimmt

Bedarfsweckung und Risikovisualisierung im Kundenportal

Risikogerechte Absicherung mit Hilfe des Maklerportals

Bestandteile einer Cyber-Versicherung

FAQ

Wöchentlicher, hochmoderner Scan erkennt neue Schwachstellen sofort nach Bekanntwerden

75%

der für Ransomware verwendeten Angriffsvektoren werden identifiziert

52%

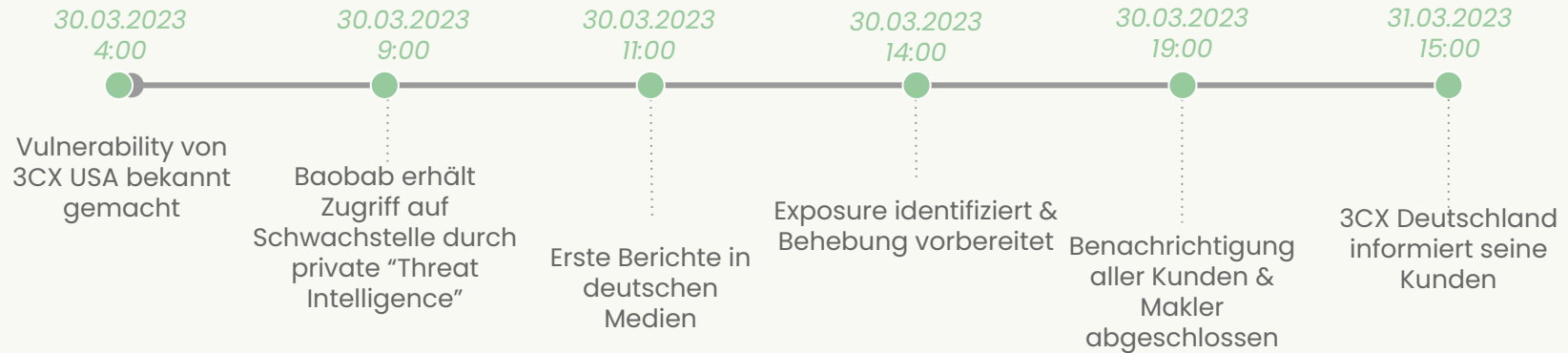
der US CISA Schwachstellen und Gefährdungen werden entdeckt

99%

falsch konfigurierter Datenbank-Ports sofort erkannt



Innerhalb von 5 Stunden identifiziert Baobab Exposure und Maßnahmen für Versicherte



Baobabs Risikopräferenzen nach Industrie

Präferiert

Architekten und Ingenieure	Landwirtschaft
Arzt-/Zahnarztpraxen	Lebensmittel
Bauwesen	Museen / Kunst / Unterhaltung
Berufsverbände	Persönliche Dienstleistungen
Call-Center	Reise- und Touristikbüros
Einzelhandel	Reparatur, Wartung
Fertigung/ Produktion	Restaurant / Bar / Cafés
Freiberufliche Dienstleistungen	Technische Berater
Gemeinnützige Organisation	Transportdienstleistungen
Großhandel	Musik-/Filmproduktion
Immobilienwirtschaft	Vermietungen (z.B. Autos)
Lagerung und Lagerhaltung	Vertriebsagenturen

Selektiv

Anwälte	Vermögensverwaltung, Banken, Versicherer, Crowd-Funding
Hotels, Camping und ähnliche	Investment- / Fondsmanager
Bergbau	Wirtschaftsprüfer
Bildungseinrichtungen	Elektrizitätsversorger
Factoring-Gesellschaften	Klimaanlagen
Gesundheit/Krankenhäuser	Wasserversorgung, Abwasserentsorgung
Immobiliendarlehenvermittler	Abfallwirtschaft & -beseitigung
Notare	E-Commerce Umsatz 30% - 60%
Öffentliche Körperschaften	Werbung
Öffentliche Versorger	Informationstechnologie
Luft- Schiff-, Raumfahrt, Bahn	
Pharmazeutika	
Steuerberater	

Verboten

E-commerce Umsatz > 60%
>20% Umsatz aus Tabakaktivität
Erwachsenenunterhaltung
THC/Opioid Herstellung/Vertrieb
Fossile Energieerzeugung/-transport
Kryptowährungen
Rundfunk
Online-Dating-Agenturen
Online-Wetten & -Glücksspiele
Rüstung, Waffen, Munition
Soziale Netzwerke
Online-Handelsplattformen
Zahlungsabwicklung, Kreditkarten, Inkasso
Cloud-Anbieter, Datenaggregator/-verarbeiter
Mobile und Saas Apps
>10% Umsatz in den USA

Sofern nicht explizit verboten

exkl. Medienhaftung

Kontaktieren Sie uns, bei offenen Fragen rund um die Anbindung

Mehr Cyber-Versicherungen verkaufen

durch Bedarfsweckung mittels individueller & interaktiver Risikobewertung

Cyber-Versicherung (fast) ohne Cyber-Wissen verkaufen

Baobabs Cyber-Experten unterstützen Sie von der Bedarfsgenerierung bis zur Umsetzung der Maßnahmen

Nachhaltige Reduzierung von Cyber-Risiken

für Ihre Kunden mit Baobab's KI- basiertem Cyber Pricing & Risikominderungs-Plan

[Kontakt aufnehmen](#)