

AIG Cyberschadenkontrollservices

Tier III: CyberEdge® Prämie ab 5.000 Euro

Selbst wenn ein Unternehmen alles dafür tut, um sich mithilfe der unternehmensinternen IT-Abteilung vor einem Cyberangriff zu schützen, kann dies in der heutigen, sich schnell verändernden Cyberumgebung nicht ausreichend sein. Im Rahmen des AIG Cyberresilienz-Programms stehen anspruchsberechtigten Versicherten mit einer jährlichen CyberEdge-Versicherungsprämie ab 5.000 Euro zahlreiche Tools und Dienstleistungen im Wert von bis zu 25.000 Euro zur Verfügung, um proaktiv einen Cybervorfall zu verhindern.

eLearning zum Thema

Cybersicherheit und Phishing-Simulationen für Mitarbeitende

Zeitnahe und messbare gesteuerte Schulungs- und Compliance-Dienstleistungen für bis zu 10.000 Mitarbeitende, verfügbar in mehr als 30 Sprachen und auf die Rollen der Mitarbeiter zugeschnitten, um die bewährten Verfahrensweisen der Kunden im Bereich Cybersicherheit zu stärken.

[Erfahren Sie mehr](#)

Blacklist-IP-Blockierung und Domainschutz

Unterstützt Unternehmen bei der Überwachung der Gefährdung ihrer Organisation durch kriminelle Aktivitäten mittels der Nutzung umfangreicher Bedrohungsdatenbanken, präzisiertem Geoblocking und der Automatisierung von Blacklists zur Risikoabsenkung.

[Erfahren Sie mehr](#)

Schwachstellen-Scan der Infrastruktur

Bis zu 250 ausgewählte IP-Adressen eines Kunden werden von Experten auf Schwachstellen überprüft, die von Cyberkriminellen ausgenutzt werden können. 90 Tage später wird ein weiterer Scan durchgeführt. [Erfahren Sie mehr](#)

Sicherheitsrisiko-Bewertungen

Kunden können mit leicht verständlichen Bewertungssystemen sehen, wie ihre Internet-Sicherheitslage und ihr Netzwerk aus der Perspektive eines „Außenstehenden“ bewertet werden.

[Erfahren Sie mehr](#)

Offenlegung von Zugangsdaten im Darknet

Ermittelt Cyberrisiken auf Domain-Ebene aus Unternehmensdaten, die im Darknet offengelegt sind, mit Berichten, die auf die spezifische Domain des Kunden zugeschnitten sind. [Erfahren Sie mehr](#)

Ransomware-Risikobewertung

Eine maßgeschneiderte Risikobewertung für Ransomware, basierend auf den neuesten Bedrohungserkenntnissen, kategorisiert und bewertet die wichtigsten Kontrollen des Kunden, die zur Verhinderung eines Ransomware-Ereignisses beitragen können.

[Erfahren Sie mehr](#)

Identitätsrisiko-Bewertung

Eine Identitätsrisikobewertung der Active-Directory-Infrastruktur des Kunden, um Risiken und Gefährdungen zu ermitteln, mit Beratung durch einen Techniker, der bei der Interpretation der Ergebnisse hilft und Fragen beantwortet.

[Erfahren Sie mehr](#)

CyberMatics®

Der patentierte Technologieservice von AIG hilft Kunden dabei, die Cyberrisiko-Position ihrer Organisation zu überprüfen, die Implementierung von Kontrollen zur Risikoabsenkung zu priorisieren und bessere Investitionsentscheidungen für ihr gesamtes Cybersicherheitsprogramm zu treffen – mit dem zusätzlichen Vorteil präziser abgestimmter Versicherungsbedingungen.

[Erfahren Sie mehr](#)

Maßgeschneiderter Vorfallreaktionsplan

Eine auf große Organisationen zugeschnittene Vorlage für einen geschäftlichen Vorfallreaktionsplan, um sicherzustellen, dass Kunden angemessen, schnell und effizient auf einen Cybervorfall reagieren können.

[Erfahren Sie mehr](#)

Informationsportal zur Cybersicherheit

Rund um die Uhr Online-Zugriff auf aktuelle Informationen zur Cybersicherheit, einschließlich Checklisten zu bewährten Verfahren, Schadenfalldaten und einem Rechner für Sicherheitsverletzungen.

[Erfahren Sie mehr](#)

CyberEdge Kommunikationsplattform (nur für UK)

Die von Cygnvs betriebene Plattform ermöglicht eine netzunabhängige Zusammenarbeit, um die Reaktion auf einen Vorfall und die Meldung eines Cyberschadens an AIG effizient zu managen. [Erfahren Sie mehr](#)

Schadenfallprozessorientierung von AIG

Eine persönliche Überprüfung der kritischen Reaktions- und Meldeschritte, die ein Kunde im Falle eines Cybervorfalles durchführen sollte.

[Erfahren Sie mehr](#)

Cyberschadenfall-Hotline

Sobald ein Anruf bei der rund um die Uhr erreichbaren Hotline eingeht, stimmt sich das CyberEdge-Schadenfallteam mit dem Kunden ab, um den Reaktionsplan umzusetzen, alle erforderlichen Dienstleister zu beauftragen, um unmittelbare Bedrohungen zu ermitteln und um mit den Wiederherstellungsarbeiten zu beginnen.

AIG Cyberschadenkontrolle-Onboarding

Ein 30-minütiges Einzelgespräch mit einem AIG Cyberrisiko-Berater, um mehr über die verfügbaren Dienstleistungen des Cyberresilienz-Programms zu erfahren.

AIG Cyber-Risk-Beratung

Einzelgespräch mit einem AIG Cyber Risk Advisor, um die Fragen der Kunden zu beantworten, wie z. B. ihre Risikolage, die Ergebnisse des Cyber-Reifeberichts oder die in ihrer CyberEdge-Police® enthaltenen Präventionsdienste. [Erfahren Sie mehr](#)

Cygnvs

Online-Plattform, die Out-of-Band-Kommunikation, Dokumentenablage und Speicherung wichtiger interner und externer Kontakte ermöglicht. Klicken Sie hier, um den [Termin für eine Demo](#) zu vereinbaren oder sich für die Plattform zu [registrieren](#).

Zusätzliche Vorteile, Tools und Dienstleistungen

Zusätzlich zu den in den anspruchsberechtigten Policen enthaltenen Dienstleistungen haben alle Cyberkunden von AIG Zugriff auf die folgenden Dienstleistungen zu Vorzugskonditionen, einige davon stehen in einer kostenlosen Demo-Version zur Verfügung. Diese Dienste wurden speziell auf der Grundlage unserer jahrzehntelangen Erfahrung ausgewählt sowie nach ihrer Fähigkeit, die Cybersicherheit einer Organisation zu verbessern.



Dienstleistungen bevorzugter Anbieter-Partner

Wir unterhalten Partnerschaften mit Cybersicherheit-Experten, um den Kunden zusätzliche Optionen anzubieten, mit denen sie ihre Schutzmaßnahmen ergänzen können. Diese Dienstleistungen stehen zur Verfügung:

BitSight Security Ratings, betrieben von BitSight Technologies, Kunden können damit ihr Netzwerk und das ihrer Drittanbieter messen und überwachen. [Erfahren Sie mehr](#)

Endpoint Detection and Response (EDR), betrieben von CrowdStrike's Falcon Insight, bietet kontinuierliche, umfassende Endpunkttransparenz und erkennt und priorisiert sicherheitsgefährdende Aktivitäten automatisch und intelligent, um zu gewährleisten, dass nichts übersehen wird und potenzielle Verstöße gestoppt werden. [Erfahren Sie mehr](#)

CyberArk DNA, betrieben von CyberArk, deckt privilegierte Konten, Anmeldeinformationen und Geheimnisse vor Ort und in der Cloud auf. CyberArk DNA kann den Kunden dabei helfen, die Konten mit dem höchsten Risiko, die vordringliche Maßnahmen erfordern, zu priorisieren. [Erfahren Sie mehr](#)

Enterprise Protection, betrieben von SpyCloud, ermöglicht es Unternehmen, Maßnahmen für gefährdete Authentifizierungsdaten von Mitarbeitern zu ergreifen, bevor Kriminelle sie für Cyberangriffe nutzen können.

[Erfahren Sie mehr](#)

Breach & Attack Simulation, betrieben von SafeBreach, ermöglicht den Kunden eine Bewertung der Wirksamkeit ihres Sicherheitsökosystems durch die Ausführung von Angriffsszenarien in Sicherheit, um festzustellen, wo die Schutzmaßnahmen erwartungsgemäß funktionieren und wo Schwachstellen für Angriffe bestehen. [Erfahren Sie mehr](#)

Unified Identity Protection Platform, betrieben von Silverfort, erzwingt einen adaptiven MFA-Schutz für den Zugriff der Nutzer auf alle lokalen und Cloud-Ressourcen und eine automatisierte Überwachung von Dienstkonten.

[Erfahren Sie mehr](#)

Starten Sie heute. Kontaktieren Sie das Cyberrisiko-Beratersteam von AIG unter cyberlosscontrol@aig.com.

Der Inhalt dieser Werbung dient ausschließlich Informationszwecken und kann nicht als Beratung oder Vertragsangebot betrachtet werden. Er kann nicht als Grundlage für die Inanspruchnahme von Versicherungsschutz oder die Haftung von AIG herangezogen werden. Ausschließlich die Versicherungsbedingungen enthalten eine verbindliche Beschreibung des Versicherungsschutzes. Alle Produkte und Dienstleistungen werden von lokalen Niederlassungen von AIG Europe S. A. abgeschlossen bzw. erbracht. Produkte oder Dienstleistungen sind möglicherweise nicht in allen Ländern und Gerichtsbarkeiten verfügbar. Der Versicherungsschutz unterliegt den Zeichnungsanforderungen und dem Wortlaut der Police.

AIG Europe S.A. ist ein Versicherungsunternehmen mit der luxemburgischen R.C.S.-Nummer B 218806. AIG Europe S.A. hat seinen Hauptsitz in 35D Avenue J.F. Kennedy, L-1855, Luxemburg und ist unter der Umsatzsteueridentifikationsnummer LU30100608 registriert, <http://www.aig.lu/>. AIG Europe S.A. ist vom luxemburgischen Finanzministerium zugelassen und wird vom Commissariat aux Assurances 11 rue Robert Stumper, L-2557 Luxembourg, GD de Luxembourg überwacht, Tel.: (+352) 22 69 11 - 1, caa@caa.lu, <http://www.caa.lu/>.

The policyholder is under no obligation to utilize any of the services that AIG makes available. AIG may modify (by adding, removing, or replacing a tool or service) or discontinue the availability of the services at any time. AIG may partner with third party vendors to provide any or all services. In some instances, AIG may have an ownership interest in certain third party vendors. AIG does not endorse, and assumes no liability arising out of, the services provided by any third party vendor. No warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any such service. It is at the sole and absolute discretion of the policyholder whether or not to utilize the available services, including any such services provided by any third party vendor. If the policyholder elects to utilize such services, the policyholder shall enter into a vendor relationship directly with the third party vendor. The policyholder may be entitled to a free demo and/or may be charged a fee by the third party vendor for such services. Any discount provided by the third party vendor may only be available while the policyholder has an in-force cyber policy with AIG. The policyholder shall be responsible for any such payments to the third party vendor and may be required to enter into a service agreement directly with the vendor.

