CHUBB®

Immer einen Schritt voraus: Informiert bleiben und schnell auf Schwachstellen reagieren

In der heutigen sich ständig weiterentwickelnden digitalen Landschaft sind Unternehmen aller Größenordnungen konstant der Gefahr von Cyber-Risiken ausgesetzt. Laut der Cybersecurity and Infrastructure Security Agency (CISA) werden 50% der bekannten und ausgenutzten Sicherheitslücken innerhalb von zwei Tagen nach ihrer Entdeckung ausgenutzt und 75% innerhalb von weniger als einem Monat. Ein aktives Schwachstellen-Management ist unerlässlich, um schnell zu handeln und Abhilfe schaffen zu können, bevor böswillige Aktivitäten in das Netzwerk eines Unternehmens eindringen und sich dort ausbreiten.

Die dynamische Schwachstellen-Erkennung von Chubb

Mit unserem Vulnerability Management Outreach Programm überwacht, scannt und identifiziert unser Cyber Intelligence Team routinemäßig Schwachstellen und neue kritische Bedrohungen, um unsere Versicherungsnehmer zu schützen. Cyber-Versicherungsnehmer, die sich für den Erhalt von Warnungen registrieren, werden informiert durch:

Outreach Programm - Es erfolgt eine proaktive Benachrichtigung an Cyber-Versicherungsnehmer, wenn in der Systemlandschaft bekannte kritische Schwachstellen entdeckt werden, die mit hoher Wahrscheinlichkeit ausgenutzt werden können.

- Eine erste Mitteilung erfolgt per E-Mail, in der die Gefährdung und die zur Behebung erforderlichen Maßnahmen detailliert beschrieben werden.
- Nachfassaktionen werden per E-Mail und Telefonanrufe durchgeführt.

Eilmeldungen - Diese werden per E-Mail an Cyber-Versicherungsnehmer versendet, wenn neue Schwachstellen mit hoher Ausnutzungswahrscheinlichkeit entdeckt werden, die sich auf die Systemlandschaft auswirken könnten.

- Eine E-Mail mit Informationen über die neue Bedrohung wird in der Regel innerhalb von 24 Stunden versandt

Zusätzliche Lösungen für das Schwachstellen-Management

Zusätzlich zu unserem Vulnerability Management Outreach Programm können sich alle Chubb Cyber-Versicherungsnehmer für den folgenden kostenlosen Cyber-Service registrieren:

- **Externe Schwachstellenüberwachung** - In Kooperation mit BitSight können Versicherungsnehmer das Cyber-Risiko ihres Unternehmens täglich über eine Plattform überwachen, die anhand von bestimmten Kennzahlen sowohl Stärken als auch potenzielle Schwachstellen hervorhebt und einen Einblick in die Sicherheit ihrer Organisation bietet.

Um sich für das Chubb Vulnerability Management Outreach Programm anzumelden und um weitere Informationen über Chubb Cyber-Services zu erhalten, besuchen Sie bitte die folgende Webseite: https://www.chubb.com/at-de/austria-cyber-services.html

Chubb Vulnerability Outreach Programm

Häufig gestellte Fragen zur Red Flag Alert

Häufig gestellte Fragen

Welches Ziel verfolgt das Chubb Vulnerability Outreach Programm?

- Ziel ist es, Organisationen über ihre Gefährdung durch hochriskante Schwachstellen und andere schwerwiegende Fehlkonfigurationen (offene Ports, Malware-Infektionen, etc.) zu informieren. Chubb hat diesen Ansatz gewählt, um Versicherungsnehmer zu warnen und ihnen bei der Erkennung und Behebung internetbezogener Probleme zu helfen, die unser Cyber Intelligence Team als hohes Risiko eingestuft hat. Denn jede von uns erkannte Schwachstelle kann und wird auch von Cyberangreifern erkannt werden. Zudem gelten die Schwachstellen, nach denen Chubb sucht, extern als extrem riskant.

Warum werde ich von Chubb auf Schwachstellen in meinem Umfeld hingewiesen?

- Dies ist ein wichtiger Teil der Beziehung zwischen Chubb und seinen Versicherungsnehmern. Wir bieten unseren Versicherungsnehmern auf der ganzen Welt seit über hundert Jahren Risikoplanungsdienste, die unsere Versicherungsnehmer zu besseren Risikomanagern und Chubb zu einem besseren Versicherer macht. Cyberrisiken sind nicht anders. Wir konzentrieren uns deshalb auf Schwachstellen, die Verluste verursachen und/oder auf Hochrisiko-Cyberbedrohungslisten stehen, die wir im Umfeld unserer Versicherungsnehmer sehen, um die Risiken in Verbindung mit diesen Schwachstellen zu verringern.

Haben diese Hinweise Auswirkungen auf den Versicherungsschutz?

- Nein. Allerdings kann eine mangelnde Bereitschaft, Maßnahmen zu ergreifen, um diese Schwachstellen zu beheben, in Zukunft Auswirkungen auf Ihre Police haben. Wenn wir beispielsweise immer wieder Schwachstellen erkennen und keine Reaktion oder Maßnahme seitens des Versicherungsnehmers erfolgt, können wir in Erwägung ziehen, den Versicherungsschutz nicht zu erneuern.

Ist das ein Penetrationstest?

- Das ist kein Penetrationstest. Es gibt kein aktives Scannen oder Versuche, in Ihre Umgebung einzudringen. Dieses Verfahren nutzt externe passive Scanning-Plattformen mit einer Kombination aus Open Source Intelligence (OSINT) und passivem Scannen. Passives Scannen ist berührungsfrei und eine sichere Methode zur Identifizierung von Vermögenswerten mit Internetbezug und möglicher verbundener Schwachstellen oder Fehlkonfigurationen.

Häufig gestellte Fragen zu Warnhinweisen („Red Flags“)

Warum bekomme ich das?

- Sie erhalten diese Benachrichtigung, weil Sie beim Chubb Vulnerability Outreach Programm angemeldet sind, das unseren Versicherungsnehmern ergänzend zu ihrer Cyber-Police zur Verfügung steht. Sie bezieht sich entweder auf eine bekannte ausgenutzte Schwachstelle (KEV) oder auf ein anderes schwerwiegendes Cybersicherheitsproblem, das über berührungsfreie externe Scanning-Tools wie BitSight und Security Scorecard entdeckt wurde. Die Benachrichtigung enthält Informationen für das IT-Team des Versicherten, um den exponierten Vermögenswert zu identifizieren und zu schützen.

Was ist, wenn ich diese Benachrichtigungen nicht verstehe?

- Das Cyber Intelligence Team von Chubb ist gerne dazu bereit, diesen Prozess und Einzelheiten zur Benachrichtigung mit jedem Ihrer Mitarbeiter zu besprechen. Sie können sie auch zur Abklärung an Ihren internen Informationssicherheitsbeauftragten oder einen externen MSP weiterleiten, der Ihr Umfeld überwacht.

Ich weiß nicht, was das ist oder was ich tun soll. Können Sie mir helfen?

- Ja, Sie können beim Cyber Risk Advisory Team von Chubb einen Support-Anruf anfordern. Wenden Sie sich dazu an Cyber@chubb.com
- Bitte fügen Sie einen Kommentar hinzu, aus dem hervorgeht, dass Sie eine Schwachstellenbenachrichtigung erhalten haben und sie besprechen möchten.

Das ist nicht meine IP-Adresse. Sind Maßnahmen erforderlich?

- Bitte leiten Sie die Benachrichtigung an Cyber@Chubb.com weiter und verweisen Sie auf die falschen IP-Adressen. Wir werden dann unsere Unterlagen aktualisieren mit dem Hinweis, dass sie sich auf einen nicht versicherten Vermögenswert beziehen. Bei Interesse kann das Chubb Cyber Risk Advisory Team Ihrem IT-Team Anweisungen geben, um eine entsprechende Anfrage an Bitsight oder Security Scorecard zu richten, um künftige automatisierte Benachrichtigungen in Bezug auf diese falschen IPs zu verhindern.

Das ist nicht meine Domain.

- Bitte wenden Sie sich an Cyber@Chubb.com mit der Bestätigung der richtigen Domain. Chubb wird dafür sorgen, dass Ihre Police entsprechend aktualisiert wird. Anschließend stellen wir in unseren Aufzeichnungen klar, dass sich die Schwachstelle auf einen nicht versicherten Vermögenswert bezieht, und schließen den betreffenden Fall ab.

Alle Cyber-Dienste können sich ändern. Änderungen des Dienstangebots werden im lokalen Cyber-Services-Webformular angezeigt. Die Versicherungsnehmer sind dafür verantwortlich, die spezifischen Bedingungen und Konditionen jedes Cyber-Service-Anbieters zu überprüfen, um die Berechtigung zu gewährleisten und über eventuelle Änderungen auf dem Laufenden zu bleiben.

REDUZIERTE CYBER-DIENSTE VON DRITTANBIETERN:
Externe Schwachstellenüberwachung, Sicherer Passwort-Manager

Die oben genannten Cyber-Dienste werden von Drittanbietern angeboten und sind für Chubb-Versicherungsnehmer während des angegebenen Anfangszeitraums kostenlos, sofern der Versicherungsnehmer ein neuer Abonnent/Kunde der angebotenen Cyber-Dienste des ausgewählten Drittanbieters ist und die Bedingungen erfüllt. Nach Ablauf des angegebenen Anfangszeitraums können Versicherungsnehmer die Möglichkeit haben, ihre Cyber-Dienste zu einem ermäßigten Preis bei der Verlängerung fortzusetzen. Bitte beachten Sie, dass der spezifische Rabatt je nach Produkt und Service variieren kann. Rabatte für Produkte und Dienstleistungen von Cyber-Dienstleistern stehen nur Chubb-Versicherungsnehmern mit aktuellen Policen zur Verfügung und unterliegen den einschlägigen Versicherungsgesetzen. Die von Drittanbietern bereitgestellten Produkte und Dienstleistungen unterliegen den Vertragsbedingungen, die der Versicherungsnehmer mit dem Drittanbieter vereinbart. Chubb ist nicht in die Entscheidung des Versicherungsnehmers zum Erwerb von Dienstleistungen einbezogen und übernimmt keine Verantwortung für Produkte oder Dienstleistungen, die von Drittanbietern erbracht werden.

Diese Inhalte dienen ausschließlich der allgemeinen Information. Es handelt sich dabei nicht um eine persönliche Beratung oder Empfehlung für Privatpersonen oder Unternehmen hinsichtlich eines Produkts oder einer Leistung. Die exakten Deckungsbedingungen entnehmen Sie bitte den Versicherungsunterlagen.

Chubb European Group SE ist ein Unternehmen, das den aufsichtsrechtlichen Bestimmungen des französischen Versicherungsgesetzes unterliegt, eingetragen unter der Registrierungsnummer 450 327 374 RCS Nanterre, eingetragener Sitz: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Frankreich. Die Chubb European Group SE hat ein voll eingezahltes Aktienkapital von € 896.176.662,-- und unterliegt der Zulassung und Aufsicht der „Autorité de contrôle prudentiel et de résolution (ACPR) 4“, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09 sowie in Österreich zusätzlich den Regularien der Finanzmarktaufsicht (FMA) zur Ausübung der Geschäftstätigkeit, welche sich von den französischen Regularien unterscheiden können. Direktion für Österreich, Firmenbuchnummer FN 241268g Handelsgericht Wien, Hauptbevollmächtigter: Michael Martinek. UID-Nr.: ATU 61835214.

Wir verwenden personenbezogene Daten, die Sie uns direkt oder durch Ihren Makler zur Verfügung stellen, für die Ausstellung und Verwaltung Ihrer Versicherung, einschließlich der Bearbeitung im Zusammenhang damit anfallender Schadenfälle. Weitere Informationen finden Sie in unserer Rahmendatenschutzrichtlinie unter www.chubb.com/at-de/data-protection.html