CHUBB®

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

In der heutigen sich ständig weiterentwickelnden digitalen Landschaft sind Unternehmen aller Grössen konstant der Gefahr von Cyberrisiken ausgesetzt. Laut der Cybersecurity 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:innen zu schützen. Cyber-Versicherungsnehmer:innen, die sich für den Erhalt von Warnungen registrieren, werden informiert durch:

Outreach Programm - Es erfolgt eine proaktive Benachrichtigung, wenn in der Systemlandschaft bekannte kritische Schwachstellen entdeckt werden, die mit einer hohen 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:innen 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:innen für folgende kostenlose Cyber-Services registrieren:

- **Externe Schwachstellenüberwachung** - In Kooperation mit BitSight können Versicherungsnehmer:innen das Cyberrisiko 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: www.chubb.com/ch-de/switzerland-cyber-services.html

Chubb Vulnerability Outreach-Programm

Häufig gestellte Fragen zu 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 Bedrohungsinformationsteam 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 Program 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.

Tous les cyber-services sont susceptibles aux changements. Les modifications apportées à l'offre de prestations, sont indiquées sur le formulaire web local des cyber-services. Il est la responsabilité des preneurs d'assurance de vérifier leur éligibilité aux prestations, ainsi que les termes et conditions spécifiques des fournisseurs de cyber-services concernés et de se tenir informés sur tout changement.

SERVICES CYBER de TIERS à prix réduit :
Personal Cyber Risk Dashboard (surveillance des vulnérabilités) ;
Password Management Application (gestion des mots de passe)

Les preneurs d'assurance qui souscrivent à une cyber-assurance auprès de Chubb, ont la possibilité d'obtenir gratuitement les cyber-services susmentionnés auprès de fournisseurs tiers spécialisés, pendant une période limitée, pour autant qu'il n'existe pas encore de relation client avec le fournisseur tiers concerné lors de la conclusion du contrat et que les autres conditions soient accomplies. Par la suite, il y a l'option de continuer à acheter les cyber-services choisis à un prix réduit. Veuillez noter que la réduction spécifique varie en fonction du produit et du service et qu'elle ne peut être appliquée que si une cyber-assurance Chubb est en vigueur. Les produits et services proposés par des fournisseurs tiers sont exclusivement soumis aux conditions contractuelles, convenues entre les preneurs d'assurance et le fournisseur tiers. La décision d'acheter un produit ou un service auprès d'un fournisseur tiers relève de la seule responsabilité du preneur d'assurance. Chubb n'assume en outre aucune responsabilité pour les produits ou services proposés par les fournisseurs tiers concernés.

Les présents contenus ont pour seul objet une information générale. Il ne s'agit pas ici de conseils personnels ni d'une recommandation destinée à des personnes privées ou à des entreprises concernant un produit ou une prestation de service. Vous trouverez les conditions exactes de couverture dans les documents d'assurance.
Chubb Assurances (Suisse) SA / Chubb Versicherungen (Schweiz) AG / Chubb Insurance (Switzerland) Limited, Bärengasse 32, 8001 Zurich, T + 41 43 456 76 00, chubb.com/ch-fr

Nous utilisons les renseignements personnels que vous nous fournissez [ou, le cas échéant, à votre courtier d'assurance] à des fins de souscription, d'administration des polices, de gestion des sinistres et d'autres fins d'assurance, comme nous l'avons décrit plus loin dans notre politique de confidentialité principale, disponible ici: https://www.chubb.com/ch-fr/footer/privacy-policy.html