Cyber Risk Engineering – Der Ablauf

CHUBB®

Chubb Cyber Risk Engineering

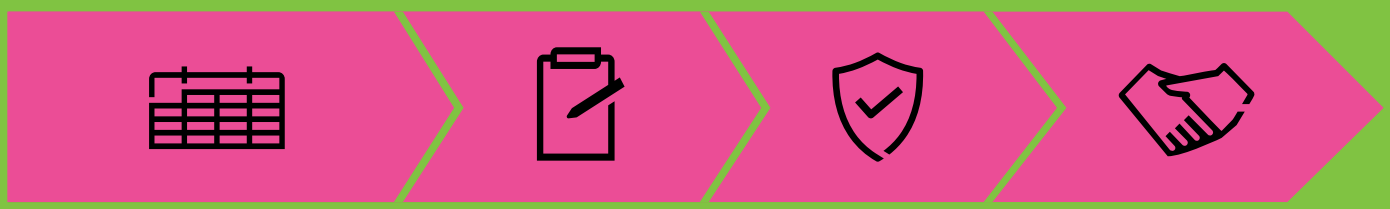
Der Ablauf

Cyber Risk Engineering ist ein hochgradig technischer und sich ständig weiter entwickelnder Service. Dies erfordert eine umfassende Fachexpertise, insbesondere da jedes Unternehmen unterschiedlichen Risiken ausgesetzt ist, die je nach Branche, den jeweiligen betrieblichen Abläufen und verwendeten Technologien variieren können. Unsere Risikoingenieure verfügen über die notwendige Erfahrung, um die individuellen Bedürfnisse und Anforderungen von Unternehmen jeder Branche bewerten zu können.

Wir unterstützen Kunden dabei, technische Schwachstellen in ihrem Unternehmen zu identifizieren, diese zu verstehen und somit künftigen Cybervorfällen vorzubeugen.

Unsere Vorgehensweise hierbei:

1	2	3	4
Vor dem Risikogespräch	Das Risiko-gespräch	Unsere Empfehlungen	Kunden-meeting



1 Vor dem Risikogespräch

Wir erläutern dem Kunden, welchen Zweck wir mit dem Risikodialog verfolgen, welche Punkte besprochen werden müssen, wer geeignete Gesprächspartner wären, welche Unterlagen wir möglichst vorab erhalten sollten und wie lange der Termin dauern wird.

2 Das Risikogespräch

Das von uns angedachte Gespräch dauert in der Regel zwei bis drei Stunden und umfasst dabei die folgenden Bereiche:

a. Tätigkeiten

Wir verschaffen uns einen Überblick über die Tätigkeiten und Geschäftsaktivitäten des Kunden, über seine Umsätze, Geschäftsfelder und die Regionen, in denen er agiert, sowie seine Prozesse und Geschäftsabläufe.

b. Räumlichkeiten

Wir nehmen keine vollständige Begehung der Unternehmensräumlichkeiten vor, im Fokus stehen aber die physischen Aspekte der Cyberdeckung: Notstromversorgung und Datenräume, Klimatisierung, Brandschutz, Redundanz und Verfügbarkeiten von Systemen sowie die Umgebungsüberwachung.

c. Netzwerk und Infrastruktur

Zu wissen, wo sich die Datenbestände befinden und welche Netzwerkverbindungen im Unternehmen bestehen, ist unerlässlich. Wir schauen gemeinsam auf die interne und externe Netzwerktopografie sowie die Datensegmentierung und vorhandene Verbindungen zu Dritt-anbietern.

Wir prüfen vorhandene Pläne zur Sicherstellung der Geschäftsfortführung, Disaster Recovery-Pläne für den Fall einer Betriebsunterbrechung sowie die angestrebten Zeiten bis zur Wiederherstellung (Recovery Time Objectives).

d. Bewertung der Datensensibilität

Wir verschaffen uns einen Überblick über die Art, Sensibilität und Anzahl von Daten, die im Unternehmen aufbewahrt und verarbeitet werden, sowie darüber, welche Informationen vertrauliche Daten des Unternehmens sind und wie diese gespeichert werden.

e. Richtlinien, Verfahrensweisen und Schutzmaßnahmen

Wir erstellen einen Bericht über die vorhandenen Richtlinien, Verfahrensweisen und Methoden des Risikomanagements, einschließlich der Risikomanagement-Struktur des Unternehmens, der Organisation des Sicherheitsteams, der angewendeten Standards und Vorgehensweisen sowie der Compliance- und Audit-Teams. Wir untersuchen das Personalmanagement, wie hierbei neue Mitarbeiter überprüft werden und was passiert, wenn Beschäftigte das Unternehmen verlassen müssen oder ihnen die Zugangsberechtigung entzogen wird.

f. Spezifische Sicherheitsverfahren

Wir nehmen eine eingehende Prüfung der Sicherheitsrichtlinien und -verfahrensweisen sowie der technischen Überwachungen vor: Firewalls, Verschlüsselungsverfahren, das Management mobiler Geräte sowie durchgeführte Penetrationstests.

g. Vorfälle erfassen

Damit Angriffe eingedämmt und minimiert werden können, ist es entscheidend zu verstehen, wie Kunden Vorfälle erkennen. Geprüft wird daher die Protokollierung, Überwachung und Untersuchung von Sicherheitsvorfällen.

h. Auf Vorfälle reagieren

Im Schadenfall richtig und schnellstmöglich zu reagieren, ist entscheidend. Wir beschäftigen uns daher mit den vorhandenen Notfall- und Krisenplänen und prüfen, welches Bewusstsein hinsichtlich der Meldepflicht von Sicherheitsvorfällen besteht.

i. Frühere Schäden und signifikante Sicherheitsgefährdungen

Zuletzt diskutieren wir in der Vergangenheit identifizierte Schwachstellen sowie zur Schadenminderung getroffene Maßnahmen und Reaktionen auf bereits eingetretene Vorfälle.

3 Unsere Empfehlungen

Nach Abschluss des Risikodialogs geben wir spezifische Empfehlungen, insbesondere zum identifizierten Restrisiko, potenziell zu erwartenden Schäden sowie detaillierte Informationen zur Risikooptimierung.

4 Kundenmeeting

Im Meeting mit dem Kunden erläutern wir unsere Erkenntnisse, bieten Vorschläge hinsichtlich Verbesserungsmöglichkeiten und arbeiten gemeinsam daran, das Risiko potenzieller Cybervorfälle zu begrenzen.

Kontakt

Chubb European Group SE
Direktion für Österreich
Kärntner Ring 5-7
1010 Wien

O +43 1 710 9355 0
F +43 1 710 9520
infoAT@chubb.com
chubb.com/at

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. Insured.℠

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: Mag. Michael Martinek, UID-Nr.: ATU 61835214.

AT0410 01/24