

## Service - Phishing Awareness Assessment

### In Partnerschaft mit Cofense

Chubb ist der Ansicht, dass Mitarbeiter ermächtigt werden sollten, Phishing-Abwehrmassnahmen ihres Unternehmens zu verbessern und Echtzeit-Informationen über Vorfälle zu sammeln, um potentielle Angriffe schnellstmöglich abwehren zu können.

Durch die Teilnahme an unserem Phishing Awareness Assessment-Programm hat jeder Chubb Cyber-Versicherungsnehmer Zugang zu den stark vergünstigten Dienstleistungen eines Beraters von Cofense Professional Services sowie zu einem Phishing-Schulungsprogramm, das darauf abzielt, die Anfälligkeit und das Risiko eines Unternehmens für Phishing-Angriffe zu ermitteln.



#### Das Programm

Innerhalb eines Zeitraums von vier Monaten führt Cofense mit „PhishMe“ zwei simulierte Echtzeit-Phishing-Szenarien für bis zu 500 verschiedene Email-Adressen durch. Ihr Unternehmen wird von einem Cofense-Berater unterstützt, der zusammen mit Ihnen folgende Schritte durchgeht:

- Festlegung des Ablaufs und Besprechung der Projektziele
- Erstellung einer Mitteilung, die an Ihre Mitarbeiter und Führungskräfte versendet wird und in der die Durchführung Ihrer Phishing-Szenarien angekündigt und deren Zweck erläutert wird.
- Motivierung zur Teilnahme und Wecken von Interesse bei Mitarbeitern.
- Information der Mitarbeiter, in welchen Bereichen ein mangelhaftes Compliance-Bewusstsein besteht.



#### Die Szenarien

Cofense erstellt und versendet zwei Phishing-E-mails, in denen der Empfänger aufgefordert wird, auf einen darin enthaltenen Link zu klicken.

1. Die erste E-Mail "**Anklicken**" fordert den Empfänger auf, auf den eingebetteten Link zu klicken. Der Link und die Darstellungsart werden kundenspezifisch angepasst. Unmittelbar nach dem Anklicken des Links gelangt der Empfänger zum ausgewählten Schulungsmaterial.
2. Die zweite E-Mail, die er erhält, ist ein "**Dateneingabe**"-Szenario, in dem der Versuch eines Angreifers simuliert wird, gültige Anmeldedaten für eine Netzwerkumgebung zu erlangen. Auch dieses Szenario basiert auf der E-Mail und dem kundenspezifisch anpassbaren Link des Klick-Tests, jedoch wird der Empfänger nun nach dem Anklicken des Links auf eine Landingpage weitergeleitet, auf der er dazu verleitet wird, sensible Daten preiszugeben.

Nach der Absolvierung eines Szenarios wird ein Bericht versendet, der umfassende Analysen enthält:

- Executive Summary der Kampagne
- die Ergebnisse und eine Response-Analyse, in der die Gesamtanfälligkeitsrate, die Melderate (falls zutreffend), und die Wiederholungsquote (nach dem zweiten Szenario) enthalten sind.

Auf Wunsch des Kunden kann auch über andere Datenpunkte Bericht erstattet werden:

- den Empfänger, die Fehlerrate
- für die Absolvierung der Schulung benötigte Zeit
- die vom jeweiligen Nutzer erzielten Ergebnisse

Der Cofense-Berater teilt Ihnen seine Erkenntnisse mit und spricht Empfehlungen für den weiteren Ablauf Ihres Programms aus.

### Weitere Informationen

Versicherte können sich unter [www.chubb.com/cyber-services](http://www.chubb.com/cyber-services) für das Phishing-Training und andere Dienstleistungen zur Schadensbegrenzung anmelden.

Chubb. Insured.™



Diese Informationen sind nur als allgemeine Erläuterungen zu betrachten. Sie stellen weder eine persönliche Beratung noch eine Empfehlung für Privatpersonen oder Unternehmen bezüglich eines Produktes oder einer Dienstleistung dar. Die spezifischen Versicherungsbedingungen entnehmen Sie bitte den Versicherungsunterlagen.