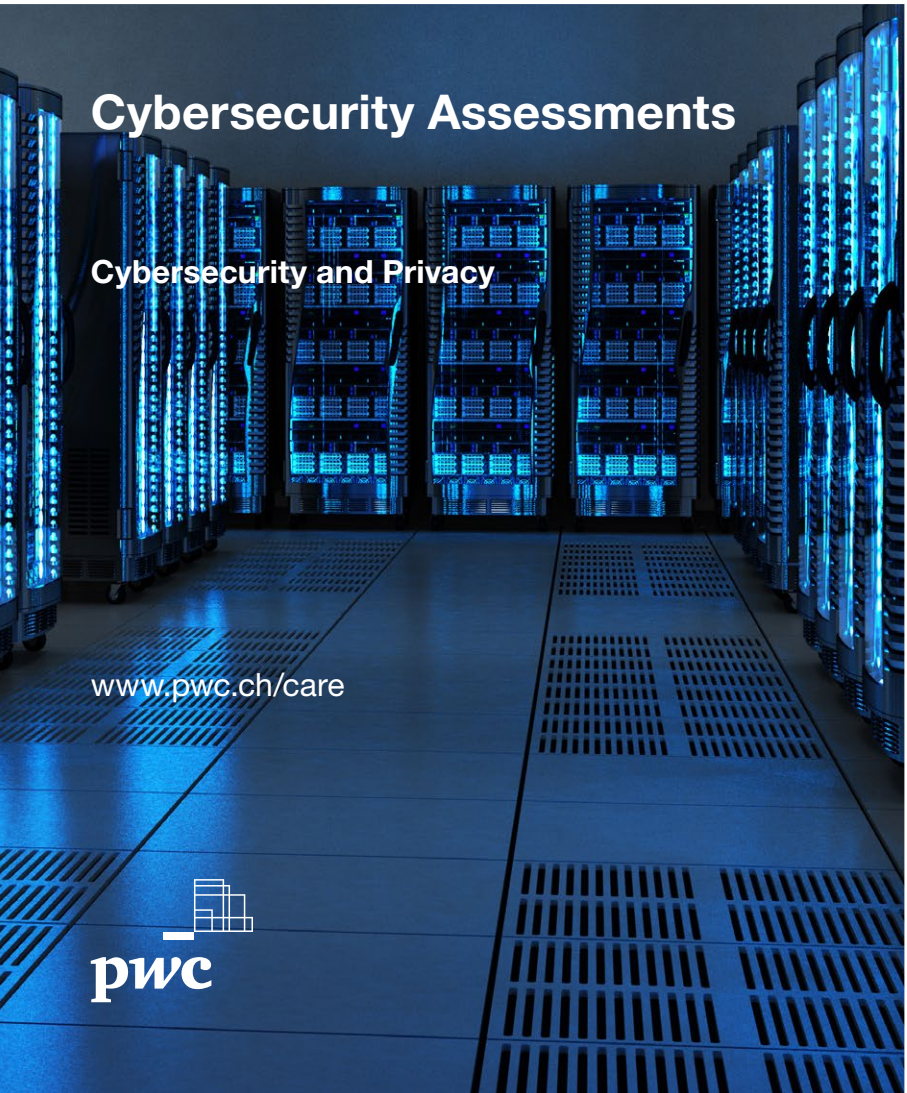
Cyber Attack and Readiness Evaluation



Cybersecurity Assessments

Cybersecurity and Privacy

www.pwc.ch/care

pwc

Cybersecurity bei PwC: Mit Fokus auf Risiken

Cybersecurity Attack and Readiness Evaluation (CARE)

CARE ist ein neuer Service von PwC, der Kunden bei der Bewertung ihres Sicherheitsdispositiv – ihrer Fähigkeit, mit den zentralen Bedrohungen der heutigen Cyberwelt umzugehen – auf einfache und verständliche Weise unterstützt.

Wie funktioniert CARE? In einem ersten Schritt führen wir mit Ihnen online einen Fragebogen durch, um Ihre Risikobereitschaft, sowie Ihre bereits umgesetzten Massnahmen zur Reduzierung der wesentlichen Cyberrisiken zu bewerten. Im Anschluss validieren wir die erhaltenen Antworten anhand einer technischen Bewertung Ihres Reifegrads.

Dieser Service ist in erster Linie für kleinere und mittlere Unternehmen konzipiert, dank seiner Modularität kann er jedoch auf jede Grösse skaliert und spezifisch an jeden Tätigkeitsbereich angepasst werden. Wir verfügen über ausgewiesene Erfahrung in einer Vielzahl von Geschäftsfeldern, darunter öffentliche Verwaltungen, Banken sowie die Konsum- und Luxusgüterbranche.

Unser modularer Ansatz von CARE umfasst fünf zugeschnittene Services, welche aus den folgenden drei Dimensionen von Cybersecurity abgeleitet sind:

Prozesse sind das Rückgrat jedes Unternehmens.

Unser Service:
- Bewertung von Cyberrisiken

Cybersecurity ist ein zentraler Bestandteil von Technologie.

Unsere Services:
- Schwachstellen-Scanning
- Penetrationstests

Obwohl häufig als Schwachstelle der Cybersecurity dargestellt …

… können Mitarbeitende bei richtiger Schulung massgeblich zur Resilienz beitragen.

Unsere Services:
- Phishing-Sensibilisierungskampagne
- Cyber-Awareness-Workshop für Führungskräfte

Bewertung von Cyberrisiken

Serviceübersicht

Die Risiken kennen, bevor sie Schaden anrichten

Das Ziel einer Bewertung von Cyberrisiken ist es, potenzielle Probleme zu identifizieren, bevor sie auftreten. Auf diese Weise können Sie risikomindernde Massnahmen planen und diese nach Bedarf in Ihren Informationssystemen oder Projekten umsetzen.

In dieser Phase führen wir einen Online-Fragebogen zur Bewertung Ihrer Risiken und der Maturität Ihrer Sicherheitskontrollen durch. Unser Set an Kontrollen stützt sich auf den IKT-Minimalstandard des Bundesamts für wirtschaftliche Landesversorgung (BWL).

Leistung

Pragmatische Empfehlungen

- Ein Bericht mit einer vollständigen Liste der schwerwiegenden Cyberrisiken und einem Executive Summary zu Ihrem aktuellen Reifegrad
- Ein detaillierter Bericht gemäss definiertem Umfang in elektronischer Form, der für die diversen Organe Ihres Unternehmens erstellt und diesen präsentiert wird
- Ein Projektplan, der alle geplanten Aktivitäten aller Projektphasen nach der ersten Mobilisierungsphase abdeckt

Schwachstellen-Scanning

Serviceübersicht

Was sind die Schwachstellen?

Ein externes Schwachstellen-Scanning ist eine einfache, sofort einsatzbereite Lösung zur schnellen Identifizierung von Schwachstellen im Netzwerk Ihres Unternehmens, die potentiell von Hackern ausgenutzt werden können.

Leistung

Ihre IT-Abteilung erhält klare Aufgaben und eine Roadmap

Sie erhalten einen ausführlichen Bericht mit einer Liste aller Schwachstellen, die bei der Durchführung des Scanning-Prozesses entdeckt wurden. Im Bericht wird zudem aufgezeigt, welche Schritte zur Behebung der Schwachstellen erforderlich sind (Als Beispiel relevante, anzuwendende Patches).

Penetrationstests

Serviceübersicht

Eindringen!

Im Gegensatz zum Schwachstellen-Scanning, das Schwachstellen nur aufdeckt, zielen Penetrationstests darauf ab, die Existenz von Schwachstellen nachzuweisen, indem diese effektiv ausgenutzt werden. Penetrationstests decken die Schwere eines Problems auf und geben Aufschluss darüber, welche Art von Schaden entstehen könnte, wenn eine Schwachstelle durch Hacker ausgenutzt würde.

Leistung

Beobachtungen und Empfehlungen

Wir liefern einen handlungsorientierten Bericht mit Beobachtungen und Empfehlungen sowie „Quick Wins“. Darin werden die Methodik des durchgeführten Penetrationstests, die getroffenen Annahmen sowie die geschäftlichen Auswirkungen des „Hacks“ erläutert.

Phishing-Sensibilisierungskampagne

Serviceübersicht

Sensibilisierung für Mitarbeitende

Phishing ist die von Hackern am häufigsten angewandte Methode, um sich einen ersten Zugang zum Netzwerk eines Unternehmens zu verschaffen. Phishing weist eine hohe Erfolgsquote auf, da es das schwächste Glied der Sicherheitskette ins Visier nimmt: den Menschen. Unsere Sensibilisierungskampagne simuliert einen Phishing-Angriff, indem eine glaubwürdige E-Mail an eine definierte Personengruppe Ihres Unternehmens versandt wird, die diese zur Durchführung einer bestimmten Aktion auffordert (z.B. das Anklicken eines Links oder das Öffnen eines Anhangs), die das Endgerät gefährden oder die Empfänger zur Preisgabe von vertraulichen Informationen bringen könnte.

Leistung

Ein Bericht zur Reduzierung von „Phishing“-Risiken

Jede Handlung der getesteten Gruppe wird aufgezeichnet und in einem Bericht zusammengefasst. Darin wird die Reaktion Ihrer Mitarbeitenden beschrieben (z.B. die Anzahl der Personen, die auf den Link geklickt, den Anhang geöffnet und ihre Zugangsdaten angegeben haben), sodass Sie den Sensibilisierungsgrad der Mitarbeitenden effektiv messen und/oder die Wirksamkeit einer Schulung, die sie in diesem Bereich durchgeführt haben, ermitteln können.

Cyber-Awareness-Workshop für Führungskräfte

Serviceübersicht

Sensibilisierung für Führungskräfte

Angesichts der Tatsache, das sich Cyberrisiken rasant weiterentwickeln, müssen Unternehmensleiter und Führungskräfte regelmässig über die wichtigsten Technologien und Entwicklungen im Bereich Cyberrisiken informiert werden.

Unsere „Game of Threats™“-Simulation als interaktives Tool ermöglichen es Ihren Führungskräften oder Kollegen, einen nahezu echten Hackerangriff in der Rolle des Verteidigers oder Angreifers zu durchlaufen– gleichzeitig wird das Verständnis gefördert und mögliche Massnahmen erkannt.

Leistung

Bericht zur Simulation

Sie erhalten eine Präsentation, in der die zentralen, im Rahmen der Simulation gewonnenen Erkenntnisse (Ergebnis, Vorgehen, Teamarbeit und beobachtete Maturität) zusammengefasst und mit praktischen Massnahmen ergänzt werden.

Unser modularer Ansatz

Wir haben ein skalierbares und anpassungsfähiges Servicemodell entwickelt, um unser Angebot auf Ihre Bedürfnisse und Grösse auszurichten. Abhängig von der gewünschten Tiefe des Assessments, sowie Ihrer Erfahrung und Kenntnisse im Bereich Cybersecurity, stellen wir gemeinsam das passende Paket zur Erhebung von technischer Maturität und menschlichem Verhalten zusammen.

	Prozesse	Technologie	Mitarbeitende
Basic	Bewertung von Cyberrisiken > Online-Selbst-bewertung > Workshop mit unseren Cyber-security-Experten	Sicherheitsbewertung Web-Anwendung (Blackbox) > Bewertung einer kleinen spezialisierten Website/ E-Commerce-Anwendung	Phishing-Übung «Click & Download» > Bis zu 50 Mitarbeitende
Advanced	Bewertung von Cyberrisiken > Online-Selbst-bewertung > Mehrere Workshops mit unseren Experten für Cybersecurity, einschliesslich Workshops mit Ihren IT-/Security-Anbietern	Sicherheitsbewertung Web-Anwendung (Grey Box) > Bewertung einer mittelgrossen Anwendung, z.B. eines E-Banking-/Zah-lungsabwicklungssystems, oder eines mittelgrossen CRM-/ERP-Systems	Phishing-Übung «Click & Download» > Bis zu 100 Mitarbeitende
Extended	Bewertung von Cyberrisiken > Online-Selbst-bewertung > Workshop mit unseren Cyber security-Experten > Kontrolltests basierend auf dem NIST Cybersecurity Framework	Sicherheitsbewertung Web-Anwendung (White Box) > Grosse Website mit komplexen CRM-Systemen oder Web-Anwendungen auf der Basis von SAP/Oracle/Microsoft	Phishing-Übung «Click & Download» > Bis zu 250 Mitarbeitende Cyber-Awareness-Workshop für Führungskräfte > Game of Threats™

Ansprechperson

Kontaktieren Sie uns für eine erste Einschätzung Ihrer Bedürfnisse und um herauszufinden, wie wir Sie bei der Bewertung Ihrer Risiken, sowie im Hinblick auf eine verbesserte Abwehr, unterstützen können.

Urs Küderli
Partner
Cybersecurity and Privacy
+41 58 792 42 21
urs.kuederli@pwc.ch