Cyber Advisory

Cyber Security Leistungs-Portfolio

September 2024

Übersicht der Leistungen der Advisory

CyQu+ ist ein PLUS aus Aon‘s **Risiko-Baukasten**,
der sich aus verschiedenen Modulen für kunden-spezifische Risikoanalysen zusammensetzen lässt.

Externe Analyse

- Non-invasive Bewertung des Unternehmens
- Umfasst Schwachstellen, E-Mail-Sicherheit, Netzwerksicherheit und offene Ports.
- Ermittlung der Security Hygiene
- Vorbereitung auf den Versicherer

Finanzielle Risiko Quantifizierung

- Darstellung von 2 Angriffsszenarien nach BSI
- Darstellung der möglichen Schäden in monetärer Sicht
- Szenario 1: Personendatenverlust durch Angriffe (DSGVO)
- Szenario 2: Verschlüsselung von kritischen Unternehmensdaten, Betriebsunterbrechung (Ransomware)

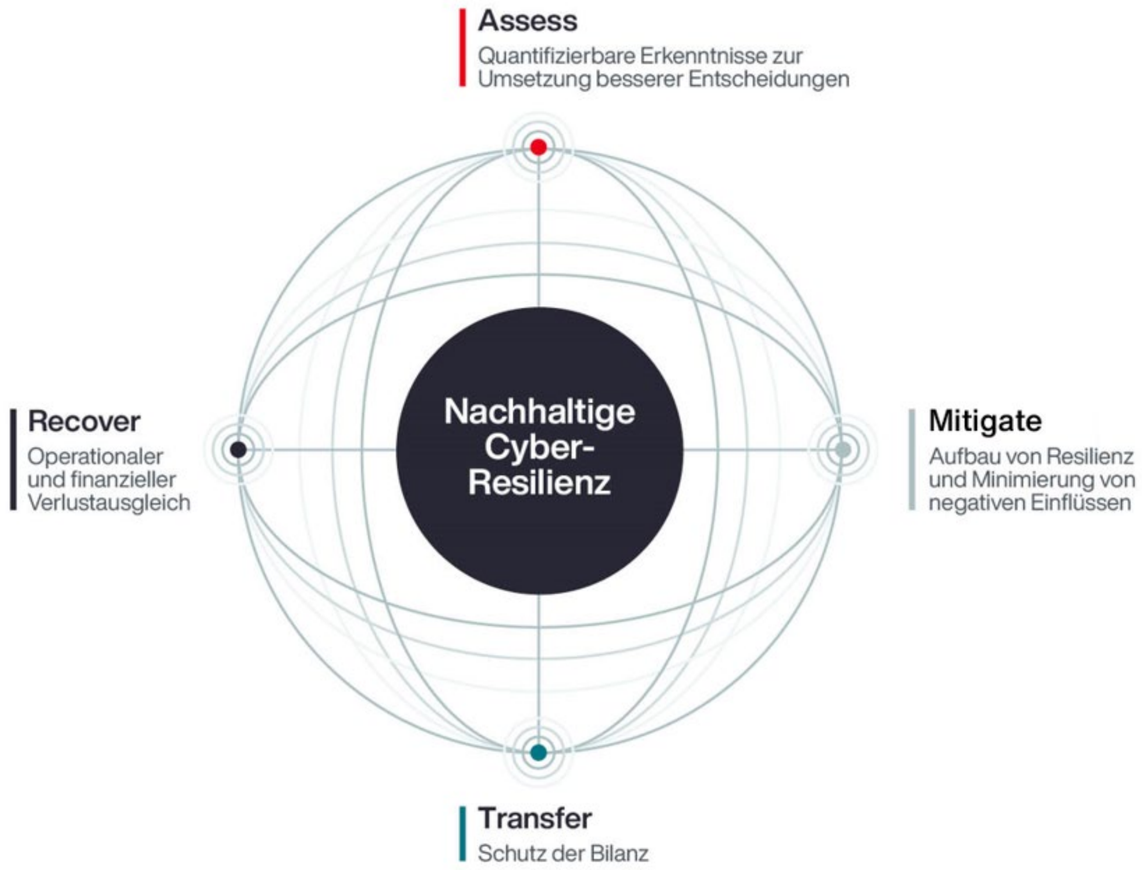
NIS-2 Compliance Check

- Ein Check der die wichtigsten Handlungsfelder für eine NIS-2 Compliance darstellt
- Handlungsfelder werden in die empfohlenen Maßnahmen im finalen Bericht mit aufgenommen

...u.v.m.

- OT-Lite
- Business-/Cyber Impact Analyse (BIA/CIA)
- Deep & Dark Net Scan
- Regulations-Checks
- ...

Aon Cyber Solutions Ansatz



Cyber Loop

Der Cyber Loop visualisiert die vier zentralen Schritte auf dem Weg zu einer umfassenden Cyber Resilienz:

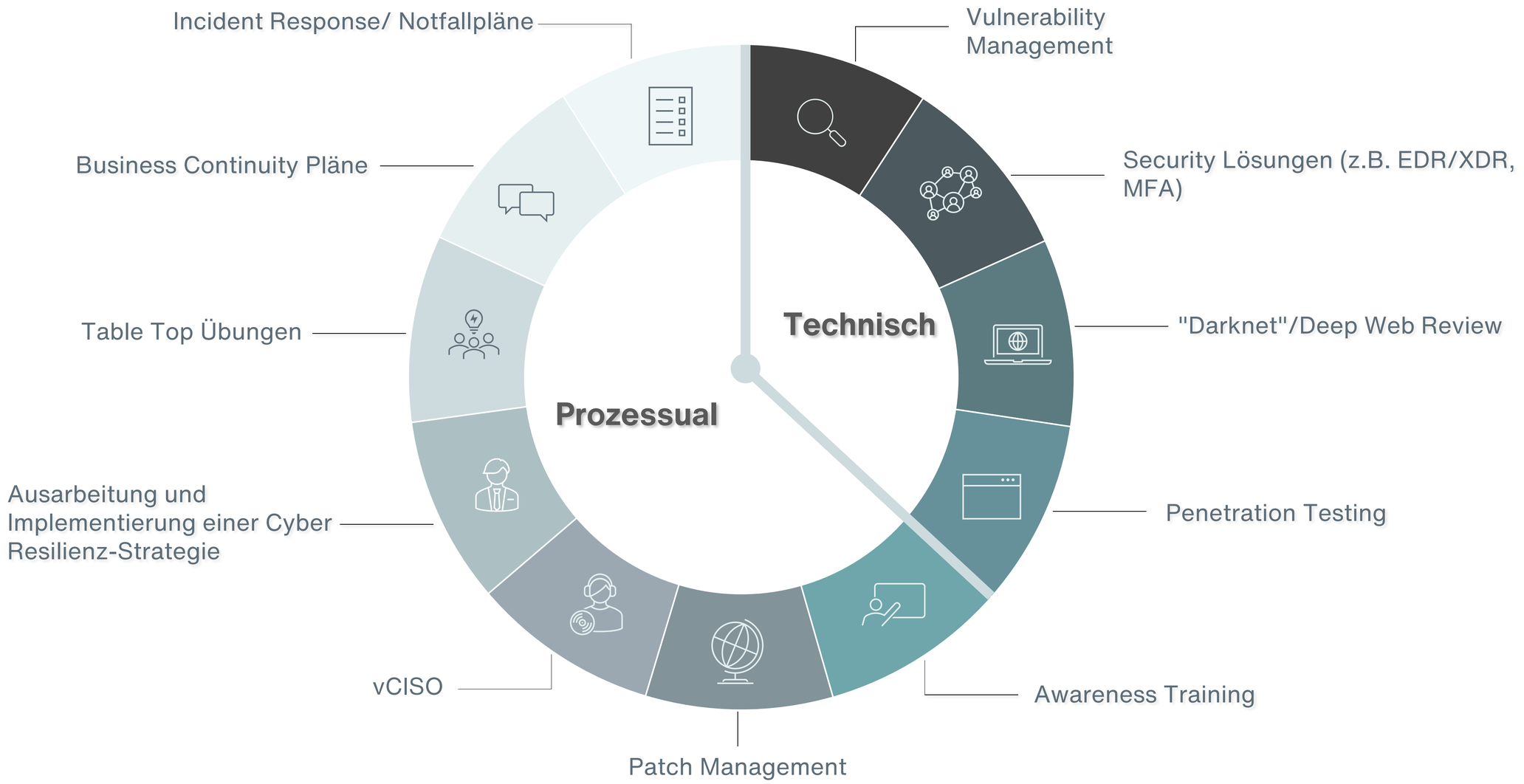
- **Assess:** Wir unterstützen Sie durch datengeschützten Analyseverfahren mit qualitativen und quantitativen Einschätzungen zur individuellen Cyberrisikosituation.
- **Mitigate:** Wir unterstützen Sie auf dem Weg in Richtung Cyber-Resilienz bei der Umsetzung von technischen und prozessualen Lösungen, um Cybervorfälle möglichst zu vermeiden.
- **Transfer:** Wir unterstützen Sie bei der Identifizierung Ihres Cyber-Exposures und Risikoprofils, um bessere Entscheidungen über die und den angemessenen Umfang des Risikotransfers zu treffen.
- **Recover:** Da eine schnelle und professionelle Reaktion die Folgen von Cyberangriffen signifikant reduzieren kann, stellen wir auch umfassende technische Kompetenzen für den Schadenfall zur Verfügung.

Cyber Advisory Offering im Bereich: Assess

Verfahren zur Identifizierung, Bewertung und Priorisierung von Cyber-Sicherheitsrisiken

Cyber Advisory Offering im Bereich: Mitigate

Resilienz aufbauen und Maßnahmen umsetzen



Cyber Advisory – zu diesen Themen stehen wir gerne zur Verfügung

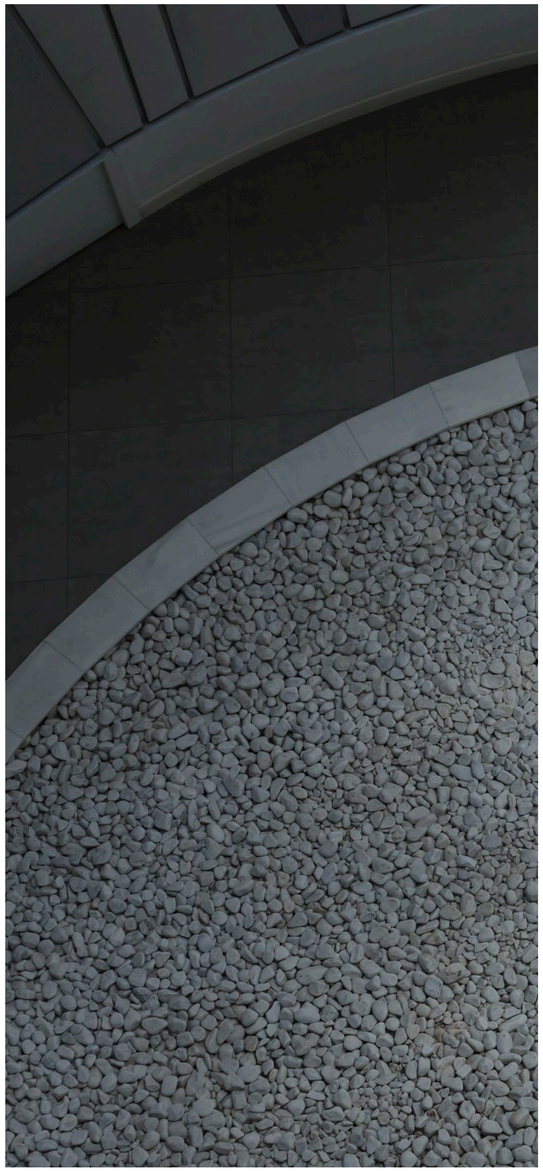
- CyQu +
- Operational Technology (OT) Assessment
- Lieferantenbewertung
- Supply Chain Bewertung
- Business Continuity Plan (BCP)
- Incident Response Retainer (IRR)
- Incident Response Plan (IRP)
- Incident Response - Readiness Assessment (IR-RA)
- Scan (non-invasiv)
- Multi Factor Authentication (MFA)
- Endpoint Detection EDR/XDR
- Threat Intelligence (TI+)
- Cyber Impact Analyze (CIA)
- vCISO
- Security Awareness Schulung für Geschäftsführung
- Security Awareness Schulungen für Mitarbeiter

Weitere Themen auf Anfrage

Ihr Kontakt bei Rückfragen

Dr.-Ing. Gunnar Siebert
Chief Security Advisor DACH

Role/position	Chief Security Advisor		
Contact	gunnar.siebert@aon.de	+ 49 176 1266 6406	Berlin



Über Aon

Über Cyber Advisory

Aon Cyber Advisory bietet ganzheitliches Cyber-Risikomanagement, unübertroffene Recherchefähigkeiten und proprietäre Technologien, um Kunden dabei zu unterstützen, Cyberrisiken aufzudecken und zu quantifizieren, kritische Vermögenswerte zu schützen und sich von Cyber-Vorfällen zu erholen.

Über Aon

Aon plc (NYSE:AON) ist der weltweit führende Anbieter von Risikomanagement-, Versicherungs- und Rückversicherungsmakler- sowie Personallösungen und Outsourcing-Dienstleistungen.

Die hierin enthaltenen Informationen und die geäußerten Aussagen sind allgemeiner Natur und sollen nicht dazu dienen, die Umstände einer bestimmten Person oder Einrichtung darzustellen. Obwohl wir uns bemühen, genaue und aktuelle Informationen bereitzustellen und Quellen zu nutzen, die wir für zuverlässig halten, kann es keine Garantie dafür geben, dass diese Informationen zum Zeitpunkt des Eingangs korrekt sind oder dass sie auch in Zukunft korrekt sein werden.

aon.com/cyber-solutions

Hinweis: Bei der Erstellung unseres Berichts haben wir ausschließlich die vom Empfänger an den CyQu-Fragebogen übermittelten Antworten berücksichtigt und uns darauf gestützt, ohne diese zu verifizieren. Wir haben die Richtigkeit, Vollständigkeit und Zuverlässigkeit dieser Antworten sowie die tatsächliche und aktuelle Situation des Cyber-Sicherheitskonzepts der Zielorganisation nicht überprüft. Die im CyQu Abschlussbericht enthaltenen Informationen basieren auf den uns zum Zeitpunkt unserer Prüfung gemeldeten Informationen und Bedingungen, die sich schnell und wesentlich ändern können. Obwohl diese Änderungen unsere Annahmen und Ergebnisse beeinflussen können, sind wir nicht verpflichtet, unsere Bewertungen, Annahmen oder Meinungen zu aktualisieren, zu überarbeiten oder zu bestätigen. Aon übernimmt keine Haftung gegenüber dem Empfänger oder einer anderen Partei, die sich aus der Verwendung dieser Informationen durch den Empfänger oder eine andere Partei ergibt.

Haftungsausschluss: Dieser Bericht enthält eine schriftliche Darstellung der von uns gesammelten und zusammengetragenen Informationen innerhalb eines begrenzten Zeitraums. Er enthält Informationen aus Quellen, die nicht validiert wurden und deren Richtigkeit oder Wahrhaftigkeit nicht garantiert werden kann. Der Bericht wird dem Empfänger wie gesehen mit besonderem Ausschluss jeglicher ausdrücklicher, oder stillschweigender, Garantien jedweder Art, einschließlich der Handelsüblichkeit, der Eignung für einen bestimmten Zweck, des Rechtsanspruchs und/oder der Nichtverletzung, zur Verfügung gestellt. Darüber hinaus geben wir keine Zusicherungen bezüglich der Angemessenheit unserer Arbeit für geschäftliche, finanzielle oder andere Zwecke, einschließlich des Zwecks, für den sie angefordert wurde. Wir geben keine Meinung zu geschäftlichen Entscheidungen im Zusammenhang mit dem Gegenstand unserer Leistungen ab. Die Angemessenheit der Arbeits- und Geschäftsentscheidungen liegt in der alleinigen Verantwortung des Empfängers. Wir haften nicht für Verluste oder Verletzungen, die durch die Vernachlässigung oder andere Handlungen oder Unterlassungen von uns und/oder unseren Vertretern bei der Beschaffung, Sammlung oder Übermittlung von Informationen verursacht werden. Darüber hinaus wird von uns keine Haftung für Verluste oder Schäden übernommen, die sich aus dem Vertrauen auf die in diesem Bericht enthaltenen Informationen ergeben.