Beazleys Sicherheitsanforderungen für die Cyber Versicherung

Um Cyber-Versicherungsschutz von Beazley zu erhalten, müssen folgende Vorrasussetzungen erfüllt sein:

4 KRITISCHE SICHERHEITS-ANFORDERUNGEN*	Ergänzende Informationen zur Erläuterung der Anforderungen von Beazley:	Praktische Beispiele, wie Sie oder Ihr IT-Dienstleister diese Anforderung umsetzen könnten:	Weitere Informationen
 Sie sichern regelmäßig kritische Daten an einem "kalten" oder "Offline"-Speicherort, der von einem Problem mit Ihrer Live-Umgebung nicht betroffen wäre. Ihre Back-ups werden regelmäßig getestet, um sicherzustellen, dass diese wiederherstellbar sind.	Alle Unternehmen sollten regelmäßig Backups ihrer kritischen/wichtigen Daten erstellen und sicherstellen, dass diese Backups aktuell und wiederherstellbar sind. So können Sie sicherstellen, dass Ihr Unternehmen den Betrieb nach einem Cyberangriff, einer unbeabsichtigten Daten-Löschung, einer Hardware-Beschädigung oder einem Datendiebstahl weiterführen kann. Wenn Sie außerdem über schnell wiederherstellbare Backups Ihrer Daten verfügen, sinkt das Risiko, erfolgreich von Ransomware-Angreifern erpresst zu werden. Je häufiger Sie Ihre geschäftskritischen Dateien und Daten ändern, desto häufiger müssen Sie Backups erstellen. Wenn Sie jeden Tag viele Änderungen an kritischen Daten vornehmen, sollten Sie tägliche Backups in Betracht ziehen. Wenn Sie nur wenige kritische Daten haben und nur wenige Änderungen vornehmen, können monatliche Backups ausreichen.	Viele Plattformen haben eine eingebaute Backup-Funktion. Prüfen Sie, welche Möglichkeiten bereits vorhanden sind. Alternativ können Sie entweder die Backup-Lösung eines Drittanbieters nutzen (z. B. Cloud-Backup-Plattformen) oder Ihre eigenen Backups auf externen Laufwerken durchführen. Diese müssen sicher und getrennt von Ihrer Live-Umgebung aufbewahrt werden.	BSI warnt vor gezielten Ransomware-Angriffen auf Unternehmen Verweis: Ab 2. 
 Sie verwenden Multi-Faktor-Authentifizierung (MFA) für Cloud-basierte Dienste (z. B. für den Zugriff auf Cloud-basierte E-Mail-Konten) und für alle Fernzugriffe auf Ihr Netzwerk.	Eine Multi-Faktor-Authentifizierung ist empfehlenswert, da Passwörter allein nicht mehr genügend Sicherheit bieten, insbesondere für Dienste, die über die Cloud verfügbar sind (z. B. Microsoft 365, Google Workspace usw.). Das begründet sich darin, dass Benutzer z.B. Passwörter aussuchen, die leicht zu erraten oder anfällig für eine versehentliche Weitergabe über Social Engineering sind. MFA erschwert es Kriminellen, Daten und andere Informationen Ihrer Organisation zu entwenden.	MFA ist kein Ersatz für das Verwenden von Benutzernamen und Passwörtern, sondern eine zusätzliche Schutzebene bei der Anmeldung. Beim Zugriff auf Konten oder Apps durchlaufen Benutzer eine zusätzliche Identitätsüberprüfung, z. B. durch das Scannen eines Fingerabdrucks oder die Eingabe eines Codes, den sie per Telefon oder mobiler App erhalten. MFA ist in den meisten Cloud-/Internet-basierten Diensten integriert und sollte aktiviert sein. Alternativ gibt es Drittanbieter, die eine MFA mittels Verwendung von SMS-Codes, eindeutigen Codes und sogar Hardware-Tokens anbieten.	Zwei -Faktor-Authentisierung nach dem BSI 
 Sie unterbinden Fernzugriff auf Ihre Umgebung ohne ein virtuelles privates Netzwerk (VPN).	Angreifer durchforsten regelmäßig das gesamte Internet nach sichtbaren Fernzugriffsdiensten wie dem Remote Desktop Protocol (RDP) von Microsoft. Diese offenen RDP-Dienste werden ständig auf Schwachstellen untersucht. Daher bietet es mehr Schutz, Ihre Fernzugriffsdienste hinter einem VPN zu verbergen.	Wie bei MFA gibt es viele Drittanbieter, die VPN-Dienste anbieten. Auch Ihre eigene Netzwerkinfrastruktur (z.B. Router) hat diese Funktionalität möglicherweise bereits integriert, sodass sie nur noch aktiviert werden muss. Diese Anforderung ist für Cloud-basierte Dienste nicht relevant.	BSI zum Virtual-Private-Network (VPN) 

beazley

Sie bieten allen Personen, die Zugang zum Netzwerk Ihres Unternehmens oder zu vertraulichen/persönlichen Daten haben, regelmäßig (mindestens einmal jährlich) Schulungen zum Thema Cybersicherheit, einschließlich Anti-Phishing, an.	Ihre Mitarbeiter stehen an vorderster Front Ihres Unternehmens. Sie sind ständig der elektronischen Kommunikation mit Dritten ausgesetzt, was sie für Angriffe anfällig machen kann. Auch wenn technische Sicherheitsmaßnahmen wie E-Mail-Gateways und EDR-Software (Endpoint Detection and Response) bis zu einem gewissen Maße schützen, ist es wichtig, dass Sie und Ihre Mitarbeiter für die Risiken sensibilisiert sind. Schulungen helfen, Cyber-Risiken zu erkennen und zu reduzieren.	Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet kostenlose Cybersicherheitsschulungen für Mitarbeiter an, die auch ein Anti-Phishing-Modul enthalten. Es gibt auch Drittanbieter, die eine Reihe von Cybersicherheitsschulungen anbieten.	BSI-Sensibilisierung- und -Schulung zur Informationssicherheit BSI-Mitarbeiterschulung BSI zur Erkennung von Phishing-E-Mails und Websiten

*zwingende Voraussetzung für den Abschluß einer Cyber-Deckung

3 WICHTIGE SICHERHEITS ANFORDERUNGEN**	Ergänzende Informationen zur Erläuterung der Anforderungen von Beazley:	Praktische Beispiele, wie Sie oder Ihr IT-Dienstleister diese Anforderung umsetzen könnten:	Weitere Informationen
1. Sie implementieren kritische Patches und aktualisieren Systeme so bald wie möglich und verwenden keine nicht mehr unterstützte (EoS) oder end of life (EoL) Software.	Alle Software-Plattformen werden in Form von „Patches" aktualisiert. Einige davon fügen der Software neue Funktionen hinzu und/oder beheben Probleme wie Instabilität oder Bugs, die von Angreifern ausgenutzt werden können. Da ständig neue Schwachstellen entdeckt und behoben werden, ist die Installation von Patches der Softwarehersteller eine routinemäßige Sicherheitsaufgabe, die zum Kern der Cybersicherheitsvorkehrungen jedes Unternehmens gehören sollte.	Bei den meisten Betriebssystemen ist das Aktualisieren/Patching sehr einfach. Für andere Software überprüfen Sie bitte die Website des jeweiligen Anbieters oder andere Kanäle, um sicherzustellen, dass Sie bezüglich kritischer Patches und Releases auf dem neuesten Stand sind. Die Anbieter kündigen in der Regel an, wenn ihre Software nicht mehr unterstützt wird oder der Supportzeitraum endet. Es ist unbedingt erforderlich, dass Sie diese Mitteilungen zur Kenntnis nehmen, um Ihre Systeme zu aktualisieren.	Patch und Änderungsmanagement nach dem BSI Verweis: Ab 2.5
2. Sie scannen eingehende E-Mails auf bösartige Anhänge und/oder Links.	E-Mail ist nach wie vor die wichtigste Form der elektronischen Kommunikation. Wenig überraschend, dass sie auch ein Hauptziel für Angreifer ist, um Mitarbeiter als Einfallstor zu nutzen. E-Mail-Gateways schützen die Mitarbeiter vor E-Mail-Bedrohungen wie Spam, Viren und Phishing-Angriffen, indem sie potenziell schädliche Nachrichten von vorneherein abblocken.	Ein E-Mail-Gateway, das Spam-Mails direkt verschiebt oder blockiert, kann das Risiko weiter reduzieren. Die meisten E-Mail-Plattformen bieten eine grundlegende Filterung und das Verschieben in den Spam-Ordner an. Stellen Sie sicher, dass diese Funktionen aktiviert sind. Idealerweise wenden Sie sich für Lösungen auch an spezialisierte E-Mail-Gateway-Anbieter.	Spam: Zwielichtige E-Mails und Falschmeldungen
3. Sie schützen alle Ihre Geräte mit Anti-Virus, Anti-Malware- und/oder Endpoint-Protection-Software.	Anti-Virus, Anti-Malware und EDR sind Software-Typen deren Aufgabe es ist, bösartige Software auf Geräten zu erkennen, zu blockieren und/oder zu entfernen. Moderne EDR-Tools sind häufig auch in eine Protokollierungsplattform integriert. So haben Unternehmen die Möglichkeit, ihre gesamte Organisation zu monitoren und so Muster und Trends zu erkennen, die darauf hindeuten, dass sich ein Angreifer in ihrer Umgebung befindet. Diese Tools sind ein wesentlicher Bestandteil des Cybersicherheits-Repertoires jedes Unternehmens: Sie zielen darauf ab, proaktiv schädliche Software zu entfernen, was z.B. Firewalls nicht leisten können.	Der folgende Link des BSI bietet Ratschläge zur Auswahl, Konfiguration und Verwendung von Antivirus- und anderer Sicherheitssoftware auf Smartphones, Tablets, Laptops und Desktop-PCs.	Virenschutz und falsche Antivirensoftware Infektionsbeseitigung für PC's, Laptops und Co.

**nicht zwingend vor Abschluss einer Cyber-Deckung erforderlich, sind alle drei Punkte erfüllt, wird der Selbstbehalt für die Breach Response Services unter der Police gestrichen