Unternehmen der Risikoklasse A Umsatzbereich 10 bis 50 Mio. EUR

Vorbemerkung

Im Folgenden werden die technisch-organisatorischen Anforderungen zur Cyber-Security aufgeführt, wie wir sie von unseren Kunden erwarten. Sie können je nach Risiko bzw. Schutzbedarf im Einzelfall in unterschiedlichem Maße Anwendung finden. Es gilt dabei der Grundsatz der Angemessenheit. In jedem Fall sind gesetzliche Anforderungen (z. B. aus dem Datenschutzgesetz oder dem IT-Sicherheitsgesetz) sowie behördliche Auflagen zu berücksichtigen. Verbindlich für den Versicherungsnehmer sind stets ausschließlich die Regelungen im Versicherungsschein und in den jeweiligen Versicherungsbedingungen (z. B. Auflagen und Vorbehalte).

Die Kriterien unterliegen einer ständigen Weiterentwicklung und Anpassung an die Risikosituation sowie dem Stand der Technik.

Die einzelnen Anforderungen können in einer Art **Präventionskette** eingeordnet werden:

Nr.	Was?	Stichworte (beispielhaft)
1	Schwachstellen von außen erkennen	Schwachstellen-/Port-Scan – Penetrations-Tests
2	Mensch / User	Awareness – Phishing-Simulationen – Email-Security - MDM
3	Software-Schwachstellen	Asset-Management - Patchmanagement - kritische Patche - EoL-Systeme
4	Lateral Movement	Segmentierung - Netzwerküberwachung
5	Berechtigungen	Berechtigungsmanagement - Privilegierte Accounts – Fernzugriffe - MFA
6	Detektion und Reaktion	AV/EDR - NAC - IDS/IPS - Logfiles - SIEM/SOC
7	Backups	Backupkonzept - Schutz vor Manipulation - Restore-Tests
8	Vorbereitet sein	Notfallplan - Desaster Recovery – Übungen - BCM
9	Ständige Verbesserung	ISMS - Risikomanagement - Due Dilligence

Für Unternehmen bis 10 Mio. EUR wird auf das Antragsformular und die Obliegenheiten in den Bedingungen ByteProtect 5.1 Kompakt verwiesen. Auf eine Darstellung wird hier daher verzichtet. Die Zuordnung zur jeweilige Risikoklasse erfolgt final nach Prüfung individuell durch den Underwriter.

Die Farben neben den Anforderungen bedeuten:
Grün = Empfehlung gelb = Versicherungsschutz mit Auflage rot = Voraussetzung für den Versicherungsschutz

Anforderungen an die Cyber-Security

Nr.	Kriterium	Stichwort	Anforderung
3	**Awareness**	Grundsatz	Das Unternehmen führt für seine Mitarbeiter, die Zugang zu IT und Internet haben, mindestens jährlich Maßnahmen zur Förderung eines sicheren Umgangs mit Internet, IT und Daten durch.
6	**Email-Security**	Grundsatz	Eingehende Emails werden hinsichtlich möglicher schädlicher Anhänge oder Internetlinks vor der Zustellung überprüft.
10	**Patchmanagement**	Asset-Management	Das Unternehmen verfügt über eine Übersicht aller eingesetzter Soft- und Hardware.
13	**Patchmanagement**	Updates	Das Unternehmen informiert sich regelmäßig über verfügbare Updates.
15	**Patchmanagement**	Kritische Schwachstellen	Kritische Schwachstellen in vom Unternehmen genutzter Software müssen zeitnah, spätestens aber 10 Werktage nach der Veröffentlichung einer für diese Schwachstelle relevanten Sicherheitsmaßnahme beseitigt werden. Hierbei sind als kritisch solche Schwachstellen anzusehen, die vom BSI Bundesamt für Sicherheit in der Informationstechnik (Warnstufe hoch oder sehr hoch) oder vom CVSS Common Vulnerability Scoring System als solche benannt bzw. eingestuft wurden (CVSS-Score von mindestens 9,0).
16	**Patchmanagement**	EoL-/EoS (Altsysteme)	Software, insbesondere Betriebssysteme und Anwendungsprogramme, bei denen der Hersteller den Support eingestellt hat und eine Aktualisierung nicht mehr erfolgen kann (end-of-life / end-of-support), sind spätestens nach 90 Tagen abzulösen oder die entsprechenden Systeme vom restlichen Netz mittels Firewall zu trennen und Zugriffe strikt zu reglementieren. Eine Erreichbarkeit vom Internet ist zu unterbinden.
17	**Berechtigungen**	Grundsatz	Der unbefugte Zugriff auf personenbezogene oder andere kritische Daten wird durch eingeschränkte Berechtigungen verhindert.
22	**Berechtigungen**	Nutzungstrennung	Administrative Accounts werden getrennt von regulären Nutzeraccounts und nur für Admin-Tätigkeiten genutzt.
34	**Fernzugriffe**	Grundsatz	Fernzugriffe sind technisch so abzusichern, dass ein nicht-autorisierter Zugriff verhindert wird (in der Regel zumindest eine VPN-Verbindung mit MFA).
37	**Fernzugriffe**	Mobiles Arbeiten	Zugriffe der Mitarbeiter von außen auf das interne Netzwerk z. B. im Rahmen des mobilen Arbeitens sind zumindest durch VPN mit MFA abgesichert. Dabei kann ein Gerätezertifikat nur dann als zweiter Faktor anerkannt werden, wenn das Gerät selbst als sicher gilt (also vollständig vom Unternehmen gemanagt ist).
39	**Netzwerksegmentierung**	Grundsatz	Das Netzwerk ist nach jeweiligem Schutzbedarf zu segmentieren.
43	**Detektion und Reaktion**	Grundsatz	Das Unternehmen verfügt über technische Schutzmaßnahmen gegen unbefugten Zugriff durch Firewalls und Virenscanner, die automatisch aktualisiert werden.
53	**Backup**	Häufigkeit	Das Unternehmen sichert seine betriebskritischen Systeme und Daten risikoadäquat in angemessenen Abständen (in der Regel werktäglich).
55	**Backup**	Sichere Speicherung	Sicherungsdatenträger werden so aufbewahrt, dass sie nicht vom selben Schadenereignis wie die Original-Dateien betroffen werden können (in der Regel "Offline-Sicherung"). Sofern eine Offline-Sicherung nicht erfolgt, muss zumindest eine Aufbewahrung außerhalb der Domain und vor Manipulation geschützt erfolgen.
58	**Notfallmanagement**	Grundsatz	Das Unternehmen verfügt über einen aktuellen Notfallplan für Sicherheitsvorfälle - insbesondere für das Szenario Cyber-Angriff / Ransomware. Hierin enthalten sind u.a. Sofortmaßnahmen, Verantwortlichkeiten, Kontaktdaten sowie ein Wiederanlaufplan.
59	**Notfallmanagement**	Verfügbarkeit	Der Notfallplan steht auch bei einem Ausfall der IT z. B. durch physische Ablage zur Verfügung.
62	**Betrugs-Prävention (sofern mitversichert)**	4-Augen-Prinzip	Bei Überweisungen von mehr als 10.000 EUR ist ein 4-Augen-Prinzip anzuwenden und zu dokumentieren.