Verträge als Baustein der Lieferketten-Resilienz

Mit NIS2 rückt Cybersicherheit endgültig aus der rein technischen Ecke in die Unternehmenssteuerung. Für betroffene Einrichtungen sind insbesondere eine umfassendere Risikobetrachtung sowie die Resilienz zur möglichst kontinuierlichen Nutzung besonders wichtiger (inkl. kritischer) Dienstleistungen ("bw-Leistungen") für den Endkunden in den Vordergrund gestellt worden. Dies bedeutet auch eine umfassendere Betrachtung und Absicherung der Sicherheit der Lieferkette zu einbezogenen, unmittelbaren und mittelbaren Dienstleistern. Damit wird die Frage, welche Sicherheitsleistungen ein Lieferant oder Dienstleister schuldet, wie schnell er bei Schwachstellen oder Vorfällen reagiert und welche Nachweise er liefert, zu einer compliance-relevanten Vertragsfrage. Um hier einen konsistenten Sicherheitsprozess zu schaffen, ist die Ausprägung und Vereinbarung von "Security-SLA" hilfreich und sinnvoll, damit gesetzliche Anforderungen in konkrete, messbare und überprüfbare Vereinbarungen übersetzt werden.

Der Begriff Security-SLA meint dabei nicht nur eine Verfügbarkeitszusage. Er beschreibt eine verbindliche Vereinbarung über sicherheits- und resilienzrelevante Leistungen, Reaktionszeiten, Mitwirkungspflichten, Nachweise und Eskalationswege.

Warum Security-SLAs jetzt notwendig werden

NIS2 verlangt ein risikobasiertes Sicherheitsniveau. Dazu ist zu vergegenwärtigen, dass die Absicherung der Nutzung "bw-Leistungen" für den Endkunden, eben die gesamte Kette der beteiligten Supplier umfasst, d.h. alle Cloud- und Hosting-Anbieter, Softwarelieferanten, Wartungs- und Fernzugriffsdienstleister, Managed-Service-Provider, Logistikpartner oder sonstige Betreiber. Und als wichtige Ergänzung zum Fokus auf den Endkunden, sind eben sowohl **Vor- als auch Nach**lieferanten einzubeziehen. Wenn ein Glied dieser Kette ausfällt, kompromittiert wird oder zu spät informiert, kann die Inanspruchnahme durch den Endkunden gefährdet sein. Security-SLAs machen daher auch sichtbar, welche Beiträge jede Partei zur Absicherung der Endnutzerleistung leistet.

Security-SLAs müssen daher nicht isoliert pro Vertrag, sondern entlang kritischer Leistungs-, Angriffs- und Verteidigungsketten betrachtet werden. Je stärker ein Dienstleister an der Erbringung der eigenen "bw-Leistung" beteiligt ist, desto klarer müssen Sicherheitsanforderungen, Mitwirkungspflichten und Nachweisrechte ausfallen.

Auf Grund der Zielsetzung ist deutlich, dass ein Security-SLA von einem datenschutzrechtlichen Vertrag zur Auftragsdatenverarbeitung klar abgegrenzt ist. Letzteres regelt den Umgang mit personenbezogenen Daten, während das Security-SLA die operative Sicherheit, Resilienz und

Mitwirkung bei Cybervorfällen steuert. Beide Regelwerke müssen zusammenpassen, ersetzen einander aber nicht.

Was in ein Security-SLA gehört

Am Anfang steht die Übersicht über Systeme, Daten, Schnittstellen und Leistungen für die "bw-Leistung". Sinnvoll ist, dies anhand der Leistungskette einerseits (horizontale Kette) sowie an beteiligten Services und Funktionen der Supplier (vertikale Kette) darzustellen.
Daraufhin können dann Rollen und Verantwortlichkeiten identifiziert werden, mit denen ein Security-SLA entsprechend des Umfangs und Anteils eines jeden Beteiligten festgelegt wird.

Der Kern sind mess- und nachweisbare Details zu Sicherheits- und Resilienzanforderungen für den jeweiligen Anteil zu regeln. Basis hierzu muss eine Risikoanalyse zu möglichen Einflüssen und Auswirkungen im Gesamt-Kontext sein. Geeignete, mit Kennzahlen belegbare Inhalte sind etwa maximale Erstreaktionszeiten je Schweregrad, Fristen für Sicherheitsupdates, Zeitfenster für Schwachstellenbehebung, Verfügbarkeit sicherheitsrelevanter Dienste, Wiederanlaufziele, Protokollaufbewahrung, Meldewege sowie Regelungen zu Sicherheitsberichten, Audits und Nachweisen wie Zertifizierungen oder unabhängigen Prüfungen.

Besondere Aufmerksamkeit erfordert das Incident-Management. Das Security-SLA muss festlegen, ab wann ein Ereignis als sicherheitsrelevant gilt, welche Frühinformationen unverzüglich bereitzustellen sind und wie laufende Updates erfolgen. Durch den Security-SLA müssen die eigenen Pflichten durch den Dienstleister optimal unterstützt werden. Dazu gehören mindestens Zeitpunkt und Art des Vorfalls, betroffene Leistungen, erste Bewertung der Auswirkungen, getroffene Sofortmaßnahmen, bekannte Indikatoren, Ansprechpartner, erwartete nächste Schritte und eine Mitwirkung zum Abschlussbericht mit Ursachenanalyse und Verbesserungsmaßnahmen.
Der Dienstleister muss hierzu qualifizierte Ressourcen bereitstellen, Zugänge zu relevanten Informationen ermöglichen, Logs sichern, forensische Untersuchungen unterstützen und mit Behörden oder Ermittlungsstellen abgestimmt kooperieren. Für kritische Abhängigkeiten sollten ggf. Test- und Notfallübungen geregelt werden.

Schließlich ist je nach Kritikalität eine Ausweitung der Verpflichtungen auf Sub-Dienstleister zu definieren.

Pragmatische Umsetzung

Es empfiehlt sich eine risikobasierte Lieferantenklassifizierung: Standardlieferanten benötigen schlanke Mindestanforderungen, kritische Betriebs- oder IT-Dienstleister dagegen detaillierte Security-SLAs mit klaren Fristen, Berichtspflichten, Auditmöglichkeiten und Eskalationen. Hilfestellungen und Ausgangspunkt können etwas die neuen EVB-IT-Regelungen geben.
Bewährt hat sich ein modularer Ansatz: Ein allgemeiner Sicherheitsanhang definiert Mindeststandards für alle Lieferanten; besondere Anlagen regeln höhere Anforderungen für Cloud, Managed Services, Softwareentwicklung, Fernwartung oder Incident Response. Die Vereinbarungen sollten regelmäßig - längstens jedoch nach meldepflichtigen Ereignissen überprüft und ggf. angepasst werden. Als wichtiger Bestandteil der eigenen Pflichten ist eine Security-SLAs als laufendes Steuerungsinstrument zu verstehen.
Wer frühzeitig Security-SLAs in Dienstleistungsverträge verankert, stärkt nicht nur seine Compliance, sondern auch die praktische Widerstandsfähigkeit der eigenen kritischen Leistungen.

< Ein Beitrag von Security-System Engineering © >

Security-System Engineering; Security-System Buch