Cybersicherheit für unsere Lieferanten

Als Betreiberin des Berliner Stromverteilungsnetzes stellen wir eine kritische Infrastruktur für die Stadt und die Gesellschaft bereit. Daraus resultiert eine besondere Verantwortung, sowie erhöhte regulatorische und rechtliche Anforderungen.

Für die stetige Weiterentwicklung des Berliner Stromnetzes sind wir auf eine Vielzahl von Lieferanten und Partnern angewiesen. Ein größerer Sicherheitsvorfall, etwa durch einen Cyberangriff auf einen unserer Lieferanten, kann schwerwiegende Auswirkungen haben.

Deshalb ist Cybersicherheit ein zentraler Punkt in unseren Lieferantenbeziehungen.

Sicherheitsvorfälle erkennen und melden

Dafür müssen wir uns auf ein Netz an starken Partnern verlassen. Falls bei unseren Partnern ein Sicherheitsvorfall auftritt, dann muss der Vorfall kommuniziert werden.

Was sind meldepflichtige Sicherheitsereignisse?

Art	Beschreibung	Meldefrist	Beispiele
Nicht meldepflichtiges Ereignis	Störungen sind ungeplante Abweichungen vom üblichen Betriebszustand, die im Rahmen der normalen betrieblichen Abläufe bewältigt werden können.	Keine Meldefrist	• Krankheitsmeldungen • Spam Mails • Überschaubare betriebliche Störung
Meldepflichtige Ereignisse	Erkannter Vorfall, bei dem die Informationssicherheit des Lieferanten so beeinträchtigt wird, dass dadurch Risiken für Stromnetz Berlin entstehen können.	Unverzüglich, spätestens nach 24 Stunden	• Datenverlust oder -diebstahl • Kompromittierter Mail-Account • Malware-Infektion (z. B. durch Ransomware) • Störungen der Verfügbarkeit von IT-Systemen die für den Auftraggeber relevant sind.

Alle Ereignisse, die im Zusammenhang mit Stromnetz Berlin auftreten oder Auswirkungen auf die Leistungserbringungen des Auftraggebers haben, müssen gemeldet werden. Gerade in der frühen Erkennungsphase sind die Auswirkungen eines Ereignisses oft unklar.

Melden Sie daher bereits **im Verdachtsfall**, damit wir die Chance haben, frühzeitig zu reagieren und geeignete Maßnahmen zu ergreifen.

Ansprechpartner für Sicherheitsvorfälle

Hierzu werden auf beiden Vertragsseiten Ansprechpartner*innen als Kontaktpersonen für die Informationssicherheit festgelegt. Alle Lieferanten und Dienstleister müssen mindestens eine*n Ansprechpartner*in für Informationssicherheit benennen. Diese sind im Falle eines sicherheitsrelevanten Ereignisses sowie bei generellen Fragen zur Informationssicherheit der Erstkontakt. Diese Rolle darf auch mit anderen Rollen

(z. B. Serviceverantwortliche*r, Accountmanager*in) kombiniert werden. Der Wechsel eines/einer Ansprechpartner*in muss Stromnetz Berlin unverzüglich gemeldet werden.

Melden Sie Änderungen des Sicherheitskontakts an Stromnetz Berlin bitte über das entsprechende Kontaktformular. Nennen Sie dafür den Namen des/der neuen Ansprechpartner*in, die Telefonnummer und die E-Mail-Adresse.

Wie melde ich einen Sicherheitsvorfall?

Alle Arten von Sicherheitsvorfällen können an jedem Wochentag, rund um die Uhr (24/7), an das Security Operation Center (SOC) von Stromnetz Berlin gemeldet werden.

Security Operation Center (SOC) Stromnetz Berlin

E-Mail	soc@stromnetz.berlin.de
Notrufnummer	+49 30 49202 - 4444

Sicherheitsvorfälle müssen als schriftlicher Bericht an unser SOC gemeldet werden. Falls innerhalb der oben genannten Frist keine vollständigen Informationen zur Verfügung stehen, verpflichtet sich der Auftragnehmer eine Teilmeldung vorzunehmen und diese zu einem späteren Zeitpunkt (spätestens innerhalb von 72 Stunden) zu konkretisieren.

Folgende Informationen müssen in der Meldung enthalten sein:

Fragestellung	**Erwartete Inhalte**
Was ist passiert?	Art des Vorfalls und der betroffenen Leistung und Informationen in Bezug auf Stromnetz Berlin
Wie ist es passiert?	Ursache des Vorfalls (sofern Informationen vorliegen)
Was ist betroffen?	Betroffene Komponenten, Systeme, Informationen oder Anlagen, Voraussichtliche Folgen
Wer ist betroffen?	Betroffene Personengruppe, z. B. Kund*innen, Lieferanten, Mitarbeitende von Stromnetz Berlin
Wann ist der Vorfall aufgetreten?	Datum und Uhrzeit des Auftretens
Wer ist Ansprechperson zum Vorfall?	Kontaktperson für Rückfragen

Nach Eingang der Meldung wird unser SOC Kontakt mit Ihnen aufnehmen und gegebenenfalls weitere Rückfragen zur Aufklärung des Vorfalls stellen.

Security Best Pratices

Um die Sicherheit unseres Lieferantennetzwerkes zu gewährleisten, sind folgende Grundsätze zu beachten:

- **Sicherheitsvorfälle melden:** Melden Sie Cyberangriffe, verdächtige Aktivitäten oder Sicherheitsvorfälle unverzüglich an unsere zentrale Kontaktstelle, das SOC.
- **IT-Systeme schützen:** Sichern Sie Ihre Systeme und Netzwerke mit aktuellen Schutzmaßnahmen wie Firewalls, Virenschutz und Monitoring.
- **Zugriffe kontrollieren:** Nur befugte Personen dürfen Daten und Systeme nutzen. Zugriffsrechte richten nach dem Prinzip „so wenig wie möglich, so viel wie nötig“ und berücksichtigen die Aufgabentrennung.
- **Systeme aktuell halten:** Aktivieren Sie automatische Updates, wo möglich, und prüfen Sie Ihre Systeme regelmäßig auf bekannte Schwachstellen.
- **Daten verschlüsseln:** Schützen Sie vertrauliche Daten immer durch Verschlüsselung – sowohl bei der Speicherung als auch bei der Übertragung.
- **Beschäftigte sensibilisieren:** Sensibilisieren sie Ihre Mitarbeitenden für den sicheren Umgang mit vertraulichen Informationen.
- **Sichere Ablage nutzen:** Verwenden Sie sichere und überprüfte Speicherorte für Daten und aktivieren Sie bei sensiblen Daten die Mehr-Faktor-Authentifizierung.
- **Daten rechtzeitig löschen:** Speichern Sie (personenbezogene) Daten nur so lange, wie sie für den Zweck der Verarbeitung erforderlich sind.