SIGNAL IDUNA
füreinander da

Verhalten im Cyber-Vorfall

Ein Cyber-Vorfall ist jeder technische Angriff auf IT-Systeme sowie jede Verletzung der Informationssicherheit. Eine Informationssicherheitsverletzung ist eine Beeinträchtigung der Verfügbarkeit, Integrität und/oder Vertraulichkeit von elektronischen Daten oder informationsverarbeitenden Systemen. Durch Fehler und Alterung der Hard- und Software (insbesondere fehlende Durchführung von Aktualisierungen) kann ein Cyber-Vorfall generell begünstigt oder ausgelöst werden. Sichern Sie Ihre Daten daher immer und regelmäßig als Backup!

Was sollten Sie im Schadenfall als erstes tun – auch bei Verdacht?

Bitte melden Sie den Cyber-Vorfall jederzeit per Telefon unter der **Schadenhotline +49(0)231/135-3030** oder per Mail an **incident@perseus.de**.

Halten Sie hierzu bitte Ihre **Versicherungsnummer** sowie die **Kontaktdaten eines Ansprechpartners** (z. B. IT-Dienstleister oder IT-Beauftragten) bereit.

Welchen Vorfall oder Verdacht müssen Sie melden?

Zu einem Cyber-Angriff gehört beispielsweise der erfolgreiche oder versuchte

- ✓ Diebstahl von Zugangsdaten und/oder unerlaubter Zugriff auf IT-Systeme,
- ✓ Diebstahl von Daten allgemein,
- ✓ Befall durch Ransomware (Schadsoftware mit Forderung von Lösegeld), Viren oder Trojaner

sowie die erfolgreiche oder versuchte

- ✓ absichtliche Zerstörung von Daten,
- ✓ absichtliche Funktionsstörung der IT-Systeme

oder jegliche Veränderung der IT-Systeme (sowohl von Software als auch von Hardware) ohne Wissen und Einverständnis des Versicherungsnehmers/Repräsentanten.

Bitte beachten Sie:

Bei einem Fremd- bzw. Drittschaden sind die gesetzlichen Meldepflichten zu beachten, die u. a. in der europäischen Datenschutz-Grundverordnung (DSGVO) verankert sind. Besonders im Falle einer Verletzung des Schutzes von personenbezogenen Daten sind Sie verpflichtet, den Vorfall binnen 72 Stunden an die zuständige Aufsichtsbehörde zu melden (Art.33 DSGVO). Bitte beachten Sie, dass bei Verstoß der Meldepflicht hohe Bußgelder drohen. Bei Unsicherheit holen Sie gerne Rat bei einem Rechtsbeistand ein.

Wie verhalten Sie sich richtig?

- ✓ Rufen Sie sofort unsere Schadenhotline an,
- ✓ trennen Sie die Geräte nicht vom Stromnetz,
- ✓ starten Sie die Geräte nicht neu,
- ✓ nutzen Sie die Systeme nicht weiter,
- ✓ leisten Sie keine Zahlungen bei Erpressungsversuchen.

Hinweise zur Selbstbeteiligung:

Sofern eine Schadenbeseitigung im Rahmen der Soforthilfe nicht möglich ist, gelten die vereinbarten Selbstbeteiligungen. Diese können durch folgende Maßnahmen reduziert werden:

1.) Über die Dienstleister-Plattform werden Schulungen angeboten und die drei Wichtigsten zertifiziert. Wenn mindestens 70 Prozent der eingeladenen Mitarbeiter diese drei Schulungen absolviert haben, reduziert sich die Selbstbeteiligung um 50 Prozent.

2.) Sie können durch den Dienstleister einen kostenpflichtigen „Security-Baseline-Check“ (SBC) durchführen lassen. Bei diesem Check wird geprüft, ob grundlegende Cybersicherheits-Standards in Ihrem Unternehmen erfüllt sind. Sofern dies der Fall ist, erhalten Sie einen grünen SBC-Bericht, mit dem sich Ihre Selbstbeteiligung im Schadenfall um 50 Prozent reduziert. Der „SBC“ hat eine Gültigkeit von einem Jahr und sollte jährlich wiederholt werden.

Bei einer Erfüllung beider Maßnahmen entfällt die Selbstbeteiligung vollständig. Ausgenommen von der Reduzierungsmöglichkeit bleibt die zeitliche Selbstbeteiligung. Die jeweiligen, gültigen Nachweise (grüner SBC-Bericht und/oder Trainingszertifikate und/oder Bericht der Mitarbeiterverwaltung aus der Dienstleister-Plattform) sind im Schadenfall durch Sie zu erbringen.

5280901 Mrz24 (556211)