

» Cyber-Notfall?

So handeln Sie jetzt.

Wenn Sie einen Vorfall vermuten, beginnen Sie mit diesen fünf Schritten. Nutzen Sie dafür ein nicht betroffenes Gerät oder einen Ausdruck.

Sind Menschen oder Anlagen in Gefahr? Befolgen Sie zuerst die vorgesehenen Sicherheitsabläufe. Schalten Sie Produktions- oder Sicherheitssysteme nicht pauschal ab.

Ihr vereinbarter IT-Notfallkontakt

Rufnummer / Vertretung

- 01 Sofort melden**
Rufen Sie Ihre IT oder den vereinbarten Dienstleister über einen sicheren Kontaktweg an. Sie müssen die Ursache dafür noch nicht kennen.
- 02 Arbeit stoppen**
Nutzen Sie das verdächtige Gerät oder Konto nicht weiter. Melden Sie sich dort nicht erneut an und bestätigen Sie keine unerwartete Anmeldeanfrage.
- 03 Nicht eigenmächtig neu starten**
Löschen, bereinigen oder setzen Sie nichts zurück. Ob das Gerät vom Netz getrennt oder abgeschaltet wird, regelt Ihr Notfallplan oder die verantwortliche IT.
- 04 Beobachtungen festhalten**
Halten Sie Zeitpunkt, Gerät oder Konto, sichtbare Meldungen und Ihre bisherigen Schritte fest. Öffnen Sie verdächtige Inhalte nicht erneut.
- 05 Koordiniert handeln**
Geschäftsleitung und IT stimmen Maßnahmen und Kommunikation ab. Legen Sie fest, wer Entscheidungen trifft und wer den Verlauf dokumentiert.

Werden gerade Daten verschlüsselt oder weitere Systeme angegriffen? Lassen Sie die IT sofort den Schaden begrenzen, während andere den Vorfall aufnehmen. Die IT isoliert betroffene Systeme und stimmt weitere Maßnahmen auf die Lage ab. Bei geplanter Analyse sichert sie flüchtige Beweise vor einer fachgerechten Abschaltung. [3, 7]

Technische Maßnahmen gehören in die Hände der zuständigen Fachkräfte oder richten sich nach Ihrem freigegebenen Notfallplan. Tragen Sie hier keine Kennwörter oder Wiederherstellungscodes ein.

Quellen: [1] BSI · IT-Notfallkarte, [3] BSI · Technik, [7] BSI · Erste Hilfe.