

NOTFALLBLATT

Berichten über Cyber-Vorfälle: Wer weiß was?

Erste Recherchefragen, nachdem Sie von einem IT-Sicherheitsvorfall in Ihrem Berichtsgebiet erfahren haben. Die große Leitfrage kann lauten: Was funktioniert und was funktioniert nicht - und das nicht nur unter technischen Gesichtspunkten! Unsere Empfehlung: IT-Vorfälle eng begleiten und immer wieder nachfragen.

Recherchefragen an die betroffene Organisation

- Welche Systeme sind ausgefallen? Wie reagieren Sie darauf?
- Was heißt das für Ihre Organisation (Standorte, Produktionsausfall, Lieferketten, Beschäftigte)?
- War es ein Angriff oder ein Fehler (extern oder intern)?
- Gilt Ihre Organisation als kritische Infrastruktur (KRITIS)? Müssen/haben Sie den Vorfall an Behörden gemeldet (Landesdatenschutzbehörden, Bundesamt für Sicherheit in der Informationstechnik)?
- Haben Sie Anzeige erstattet?
- Sind personenbezogene Daten betroffen? (Artikel 33 & 34 Datenschutz-Grundverordnung)
- Was empfehlen Sie Ihren Kund:innen und Geschäftspartner:innen?
- Welchen Fragen gehen Sie derzeit nach?
- Bearbeiten Sie den Vorfall gemeinsam mit spezialisierten IT-Dienstleistern (Incident Response/Forensik)? Wie sehen Ihre nächsten Schritte aus?
- Gab es bereits ähnliche Vorfälle in Ihrer Organisation/Ihrem Unternehmen?

Recherchefragen zu den Auswirkungen des Vorfalls

an Mitarbeitende

- Wie arbeiten Sie derzeit? Sind Sie freigestellt, müssen Sie Urlaub nehmen?
- Welche Arbeit können Sie nicht erledigen, wofür brauchen sie Ausweich-Lösungen, wie kommunizieren Sie derzeit?
- Wie sind die Auswirkungen? (Abgleich zu Unternehmensangaben)
- Haben Sie Sorgen, dass Sie Ihr Gehalt nicht bekommen?
- Hat es bereits ähnliche Vorfälle im Vorfeld gegeben?

an Geschäftspartner:innen

- Haben Sie Maßnahmen zum Schutz Ihrer eigenen Systeme ergriffen?
- Wie lange können Sie diesen Zustand mitgehen, ohne sich nach neuen Partnerunternehmen umzusehen?

an Kund:innen oder Bürger:innen

- Was fehlt Ihnen? Wie gehen Sie damit um? Wann haben Sie davon erfahren?
- Welche behördlichen Dienstleistungen können Sie nicht in Anspruch nehmen (Antrag auf Personalausweis, Führerschein o.ä.)?
- Bekommen Sie gerade keine behördlichen Leistungen, auf die Sie Anspruch haben (Wohngeld, Asylleistungen, Grundsicherung o.ä.)? Was heißt das für Ihr Leben?

an IT-Sicherheitsexpert:innen, Datenschützer:innen, Polizei, et al.

- Was empfehlen Sie Kund:innen oder Bürger:innen der betroffenen Organisation, worauf sollten sie achten (Passwortwechsel, Kommunikationskanäle)?
- Gab es schon frühere vergleichbare Vorfälle? Ist es ein Einzelfall?
- Hat sich ein:e Täter:in bekannt?

Mehr zu Sprache, Bildsprache und weiterführenden Informationen in „Berichten über Cyber-Vorfälle – Handreichung für Journalist:innen“:

<https://www.dialog-cybersicherheit.de/media/>, Lizenz: [CC-BY-SA-Lizenz 4.0 International](#)

