

Rollenkarte für den Cybervorfall

Für Geschäftsleitung, IT und Fachbereiche: Zuständigkeiten klären, sicher kommunizieren und Entscheidungen dokumentieren. Vor der Nutzung Kontakte und Befugnisse ergänzen. Bei einem akuten Verdacht sofort den vereinbarten IT-Kontakt anrufen; nicht auf vollständige Unterlagen warten.

Unternehmen: _____ Verantwortlich: _____
Geprüft am: _____ Freigegeben durch: _____

Rolle und Aufgabe	Name und Vertretung	Kontakt und Ersatzweg
Vorfallsleitung Prioritäten, Aufträge und Lageupdates koordinieren	_____ _____	_____ _____
IT oder IT-Dienstleister Umfang prüfen, Eindämmung und Wiederherstellung steuern	_____ _____	_____ _____
Geschäftsleitung und Fachbereich Betriebsfolgen bewerten und Freigaben erteilen	_____ _____	_____ _____
Kommunikation Abgestimmte Meldungen intern und extern versenden	_____ _____	_____ _____
Datenschutz und Recht Meldepflichten und externe Einbindung fallbezogen prüfen	_____ _____	_____ _____

Kommunikation und Entscheidungsbefugnis

Freigegebener Ersatzkanal bei unsicherer E-Mail: _____
Wer darf Systeme isolieren oder abschalten: _____
Wer gibt Wiederanlauf und externe Meldungen frei: _____
Nächstes Lageupdate und verantwortliche Person: _____

Rollen dürfen in kleinen Teams kombiniert werden. Zuständigkeiten und Vertretungen bleiben ausdrücklich benannt. Sichere Erreichbarkeit auch außerhalb der üblichen Arbeitszeit klären. Betroffene Kommunikationskanäle nicht ungeprüft für die Abstimmung nutzen.

Interne Erstmeldung

Für die meldende Person und die Vorfallsleitung. Bekannte Beobachtungen eintragen, Vermutungen kennzeichnen und Unbekanntes offenlassen. Diese Vorlage ist eine interne Meldung; sie ersetzt keine vorgeschriebene externe Meldung.

Angabe	Eintrag
Vorgangsnummer und meldende Person Sicherer Rückkontakt	
Entdeckt am und um Zeitzone angeben	
Beobachtung und Quelle Was ist tatsächlich bekannt	
Betroffene Dienste und Betriebsfolgen Was funktioniert nicht mehr	
Bereits ausgeführte Maßnahmen Wer hat wann was getan	
Informierte Stellen und Übernahme Wer bearbeitet die Meldung	
Offene Fragen und nächstes Update Verantwortlich und Zeitpunkt	

Informationen sicher übergeben

Keine Passwörter, MFA-Codes oder unnötigen personenbezogenen Daten eintragen. Auf Belege nur über interne Referenzen und freigegebene Ablageorte verweisen. Originale und Protokolldaten durch zuständige Fachleute sichern lassen; Aufbewahrung und Zugriffsrechte abstimmen. Verdächtige Dateien nicht zur Prüfung öffnen oder unkontrolliert weiterleiten.

Vorfallprotokoll und Übergabe

Für die protokollierende Person. Jeden Eintrag mit Datum, Uhrzeit und Zeitzone versehen. Beobachtung, Entscheidung und Ergebnis unterscheiden. Weitere Protokollseiten bei Bedarf kopieren; Korrekturen als neue Einträge ergänzen.

Vorgangsnummer: _____ Protokollführung: _____

Zeit und Quelle	Beobachtung oder Entscheidung	Auftrag und Verantwortung	Ergebnis oder Belegreferenz
_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____

Übergabe und Wiederanlauf

Aktueller Umfang und verbleibende Risiken: _____
Offene Maßnahmen mit Verantwortung und Termin: _____
Übergeben von / an / Zeitpunkt: _____
Wiederanlauf freigegeben durch / Zeitpunkt / Voraussetzungen: _____
Funktionsprüfung, Beobachtungszeitraum und nächste Kontrolle: _____

Nachbereitung

Welche Verbesserung wird umgesetzt: _____
Verantwortlich / Termin / Wirksamkeit geprüft am: _____

Nutzung und fachlicher Bezug

Eigene Vorlagen der Paragamix GmbH. Kostenlos intern nutzen, anpassen und an Kunden weitergeben; ein Quellenlink ist willkommen. Vor Nutzung durch zuständige Personen prüfen. Organisatorische Arbeitshilfe, kein technisches Einsatzhandbuch. Ausgefüllte Unterlagen geschützt aufbewahren.

NIST SP 800 61 Rev 3 | Aktuelle Fassung und Werkzeuge