PATECCO
dynamic identity systems.

DIE 6 SÄULEN EINES PRAXISORIENTIERTEN INCIDENT-RESPONSE-(IR-)PLANS

Von PATECCO

VORBEREITUNG

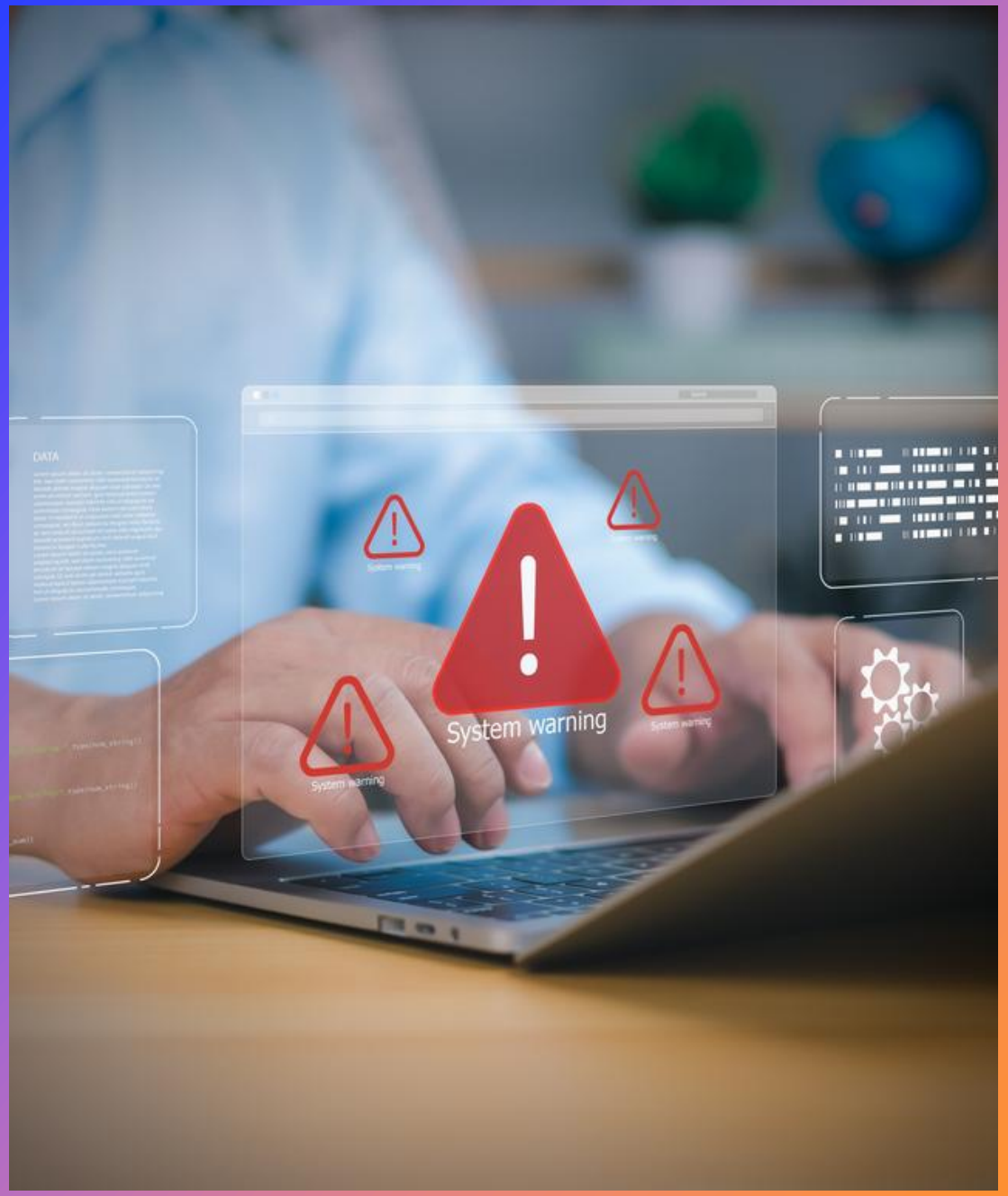
Bauen Sie die Grundlage auf, bevor ein Vorfall eintritt.

- ✓ Definieren Sie den Umfang der Incident Response (IR), die Rollen und Eskalationswege.
- ✓ Pflegen Sie aktuelle Kontaktlisten (intern + extern).
- ✓ Halten Sie sich an die gesetzlichen und versicherungstechnischen Anforderungen (DSGVO, NIS2).
- ✓ Überprüfen Sie, ob wichtige Backups und Überwachungstools funktionsfähig sind.

IDENTIFIZIERUNG

Erkennen und bestätigen Sie einen Vorfall schnell und präzise.

- ✓ Definieren Sie, was einen „Sicherheitsvorfall“ darstellt.
- ✓ Verwenden Sie SIEM, Endpoint Detection and Response und Überwachung, um Warnmeldungen zu erfassen.
- ✓ Schulen Sie Mitarbeitende darin, verdächtiges Verhalten zu erkennen und zu melden.
- ✓ Eskalieren Sie den Vorfall innerhalb von Minuten, nicht Stunden, an den IR-Leiter oder das SOC.



KONTROLLE

Verhindern Sie die Ausbreitung des Angriffs und begrenzen Sie den Schaden.

- ✓ Isolieren Sie betroffene Systeme oder Netzwerke sofort.
- ✓ Deaktivieren Sie kompromittierte Konten oder Anmeldedaten.
- ✓ Blockieren Sie bösartige IPs, Domains oder Ports.
- ✓ Bewahren Sie Protokolle und forensische Beweise auf, bevor Sie Systeme bereinigen.

ELIMINIERUNG

Beseitigen Sie die Bedrohung vollständig und schließen Sie ausgenutzte Schwachstellen.

- ✓ Identifizieren Sie die Ursache und den Angriffsvektor.
- ✓ Entfernen Sie Malware, unautorisierte Benutzer oder schädlichen Code.
- ✓ Beheben Sie Schwachstellen und stärken Sie Konfigurationen.
- ✓ Setzen Sie alle betroffenen Passwörter und Schlüssel zurück.
- ✓ Aktualisieren Sie Signaturen, Regeln und Erkennungssysteme.

WIEDERHERSTELLUNG

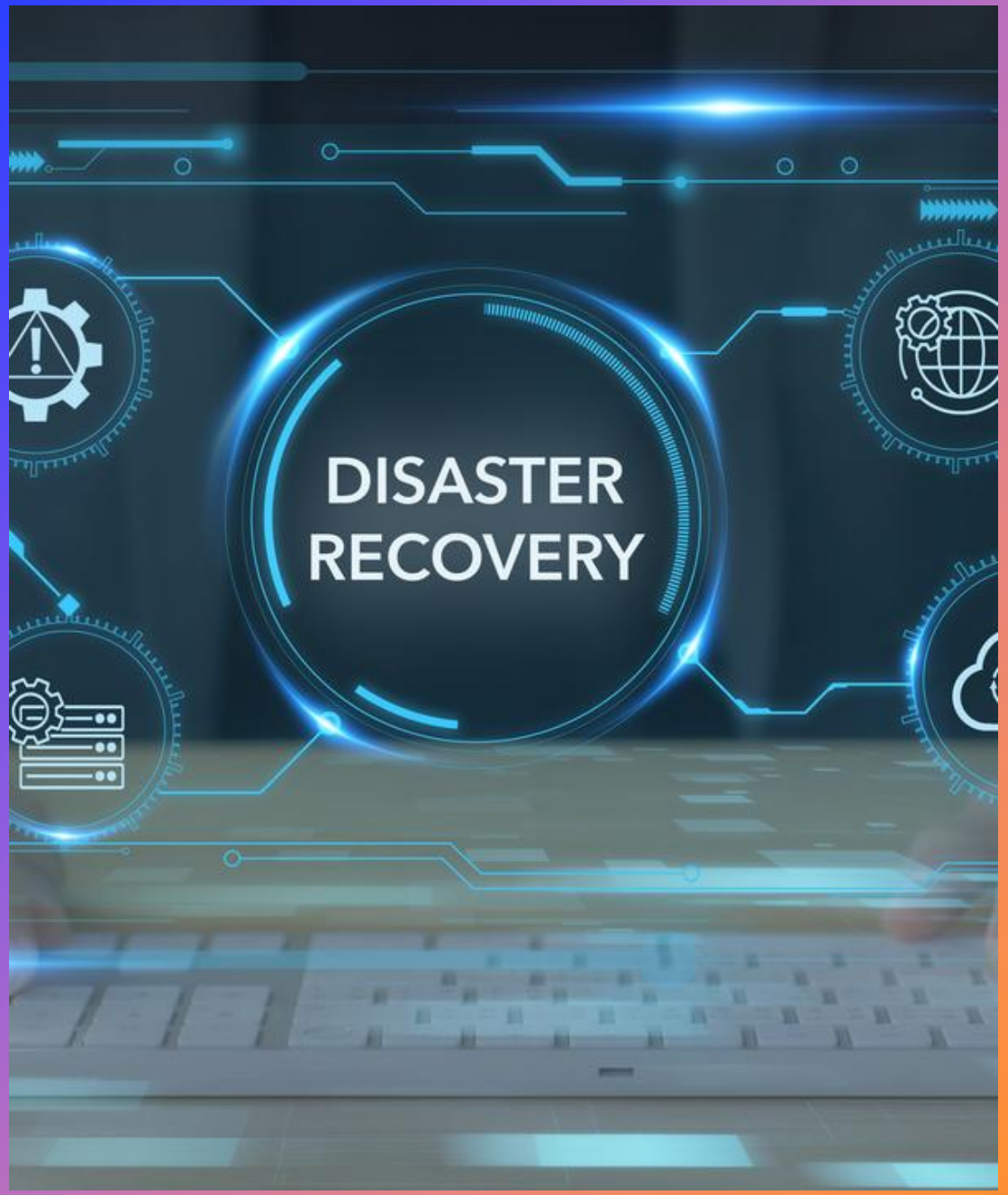
Den Geschäftsbetrieb sicher wiederherstellen und den Status überprüfen.

- ✓ Daten aus sauberen, verifizierten Backups wiederherstellen.
- ✓ Testen Sie die Systeme vor dem vollständigen Betrieb.
- ✓ Achten Sie genau auf eine erneute Infektion oder verdächtiges Verhalten.
- ✓ Kommunizieren Sie den Stakeholdern den Fortschritt der Wiederherstellung.

ERKENNTNISSE AUS VORFÄLLEN

Verwandeln Sie den Vorfall in eine langfristige organisatorische Stärke.

- ✓ Führen Sie innerhalb von 7 bis 10 Tagen eine Nachbesprechung durch.
- ✓ Identifizieren Sie, was funktioniert hat, was gescheitert ist und warum.
- ✓ Aktualisieren Sie den IR-Plan, Richtlinien und Schulungsmaterialien.
- ✓ Setzen Sie technische Verbesserungen basierend auf den Erkenntnissen um.
- ✓ Verfolgen Sie Kennzahlen: Reaktionszeit, Ausfallzeit, Kosten, Wiederherstellungsgeschwindigkeit.



Nehmen Sie Kontakt auf. Wir sind bereit, Sie zu unterstützen!

PATECCO GmbH
+49 (0) 23 23 - 9 87 97 96
www.patecco.com
info@patecco.com