BEWÄLTIGUNG

Den Einstiegspunkt (Patient-Zero; das erste kompromittierte System) eines Cyber-Angriffs festzustellen, ist aufwändig, aber gleichzeitig wertvoll. Außerdem sorgen nur eine vollständige Erhebung des Ausmaßes der Kompromittierung und die vollständige Beseitigung für einen sicheren Wiederanlauf der Geschäftsprozesse.

- Bewahren Sie Ruhe.
- Kontaktieren Sie sofort alle Ansprechpartner in Ihrem Unternehmen, die Sie zur Bewältigung brauchen.
- Befragen Sie ggf. betroffene Nutzer über Beobachtungen und Aktivitäten.
- Kontaktieren Sie einen IT-Dienstleister, der Ihnen bei der Bewältigung des Notfalls behilflich sein kann.
- Sammeln und sichern Sie System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen am besten, bevor Sie auf den Systemen eine Analyse starten. Diese Daten sind im Fall einer forensischen Auswertung essentiell (auch Strafanzeige).
- Dokumentieren Sie fortwährend alle mit dem IT-Notfall im Zusammenhang stehenden Sachverhalte.
- Prüfen Sie die Kontaktaufnahme zur Zentralen Ansprechstelle für Cybercrime (ZAC) beim Landeskriminalamt Ihres Bundeslandes und die Erstattung einer Anzeige.
- Vermuten Sie als Urheber des IT-Notfalls/Cyberangriffs einen fremden Nachrichtendienst, wenden Sie sich jederzeit vertrauensvoll an die Verfassungsschutzbehörde in Ihrem Bundesland oder an das Bundesamt für Verfassungsschutz.
- Prüfen Sie zusätzlich eine freiwillige Meldung des IT-Notfalls an die Meldestelle der Allianz für Cyber-Sicherheit (ACS).
- Beachten Sie Meldepflichten: Datenschutz, KRITIS, etc.

Weitere Informationen und Ansprechpartner:

Zentrale Ansprechstellen für Cybercrime der Polizeien der Länder und des Bundes

Ansprechpartner der Verfassungsschutzbehörden

Informationen der ACS zu IT-Sicherheitsvorfällen

NACHBEREITUNG

- Überwachen und monitoren Sie Ihr Netzwerk und Ihre IT-Systeme nach einem Cyber-Angriff besonders intensiv auf ungewöhnliche Aktivitäten, um sicherzustellen, dass Ihre Systeme wieder einwandfrei funktionieren und um einen möglichen Wiederholungsversuch rechtzeitig zu erkennen.
- Lessons Learned; prüfen Sie, ob es Regelungen, Maßnahmen oder Prozesse gibt, die optimiert und abgesichert werden müssen.
- Halten Sie Ihre Dokumentation zum Notfallmanagement stets auf dem aktuellen Stand.
- Schließen Sie durch den IT-Notfall aufgedeckte Schwachstellen und Sicherheitslücken.
- Entwickeln Sie Ihre IT-Sicherheitsarchitektur – Ihre Systeme, Netzwerke und Dokumente – kontinuierlich weiter.

Der IT-Grundschutz des BSI bietet ausführliche Informationen für die Gestaltung von Informationssicherheit und Notfallmanagement.

Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Cyber Security Sharing and Analytics e.V. (CSSA), Deutscher Industrie- und Handelskammertag e.V., eco – Verband der Internetwirtschaft e.V., G4C German Competence Centre against Cyber Crime e. V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit e.V., VOICE - Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik