



SOC Austria
Wir erscannen Gefahren

IRS

Im Falle eines Cybersecurity Incidents ist es essentiell, die richtigen Handlungen zu treffen und auf erfahrenes Personal zurückzugreifen. Mit unserem **Incident Response Service** beraten wir Sie im Vorfeld und legen notwendige Rahmenbedingungen fest, um im Ernstfall sofort reagieren zu können und den aufgetretenen Vorfall zu analysieren, zu bewerten sowie die notwendigen Gegenmaßnahmen einzuleiten.

IT for
innovators.

Schnelle Hilfe im Worst Case

Erkennen, analysieren & abwehren

Eine schnelle Reaktion sowie genaue Analyse sind unverzichtbar, wenn ein Angriff auf Ihr Unternehmen rasch eingedämmt und der Schaden minimiert werden sollen. Unsere Experten beginnen nach einem Sicherheitsvorfall umgehend mit der Untersuchung:



Erkennen & identifizieren

In der ersten Phase wird festgestellt, ob ein Breach stattgefunden hat, worum es sich genau handelt und welche Systeme betroffen sind.



Bewertung

Als nächstes wird analysiert, welche Auswirkungen der Vorfall auf Ihr Kundennetzwerk hat.



Eindämmen & bereinigen

Anschließend werden alle nötigen Schritte getroffen, um die Schwachstelle nachhaltig zu schließen und Ihre Funktionalität wiederherzustellen.

Der Abschluss eines Incident Response Einsatzes bildet ein detaillierter **Incident Report**. In diesem Endbericht sind sämtliche relevante Informationen von Beginn bis Abschluss des Vorfalls enthalten. Unter anderem eine detaillierte Attack-Timeline, Analyseergebnisse sowie vorgeschlagene und umgesetzte Maßnahmen.

Gemeinsame Strategie

Mit ACP stehen Ihnen starke Ressourcen sowie langjährige Experten zur Seite. Bereits im Vorfeld eines Sicherheitsvorfalls legen wir gemeinsam Rahmenbedingungen für den Ernstfall fest. Hat ein Angriff stattgefunden, beleuchten wir nach Wiederherstellung Ihrer Funktionalität die veranlassten Schritte und planen noch umzusetzende Schutzmaßnahmen.

Sicherheit bekommen, erhalten und langfristig steigern

Sie möchten vorab auf Nummer Sicher gehen? Bei Bedarf steht Ihnen ein SOC Experte auch für die Durchführung von sicherheitstechnischen oder forensischen Analysen zur Verfügung.

Beispiele dafür sind:

- Prüfung von Phishing-Mails in Hinblick auf potenziellen Schaden und Möglichkeiten zur Nachschärfung der eigenen E-Mail-Security
- Malware-Forensik von PDF und Office-Dokumenten
- Untersuchung von Windows-Clients bzw. Servern auf potenziellen Malware-Befall bzw. Anzeichen von Cyberattacken
- Ersteinschätzung ob vermutete Security Incidents einer weitergehenden Behandlung bedürfen.

Unsere Expert*innen beraten Sie im Zuge der Analysen auch dahingehend, wie die untersuchten Vorfälle in Zukunft mit den richtigen Maßnahmen proaktiv reduziert werden können.

Ihr Nutzen

- > Kontinuierliches Monitoring Ihrer Security
- > Auswertung, Analyse und Validierung von Sicherheitsvorfällen durch SOC Experten
- > Rasche Eindämmung durch konkrete Handlungsempfehlungen
- > Schließung von Sicherheitslücken in Ihrem System
- > Kosten- und Aufwandsminimierung durch Managed Service Angebot



Preis auf
Anfrage
bei Ihrem
Ansprechpartner



Sie möchten mehr über unsere Security-Lösungen erfahren? Dann wenden Sie sich bitte an:

security@acp.at
www.acp.at/soc