arco
IT SECURITY SERVICES

Detection and Response

Bedrohungen für IT-Umgebungen treten häufig an Wochenenden und Feiertagen auf, wenn Angreifer davon ausgehen, dass die Systeme unbeaufsichtigt sind. Je früher Sicherheitsprobleme erkannt werden – desto schneller können Sie wieder zur Tagesordnung übergehen.

Wir von Arco IT möchten, dass Sie ruhig schlafen können, mit dem Wissen, dass Ihre Systeme 24x7 365 Tage im Jahr überwacht und Vorfälle sofort behoben werden. Um Ihr Unternehmen zu schützen, muss Ihre Sicherheitsüberwachung leistungsfähig sein um schnell reagieren können.

Wir haben uns mit dem internationalen Experten Obrela Security Industries zusammengetan, um ein leistungsfähiges Security Operations Center (SOC) bereitzustellen, dass sich nahtlos in Ihre bestehenden IT-Systeme integrieren lässt, um potenzielle Bedrohungsaktivitäten kontinuierlich zu überwachen und darauf zu reagieren.

WIE ES FUNKTIONIERT

Durch unseren strengen und gründlichen Prozess haben Sicherheitsbedrohungen keinen Platz, um sich zu verstecken.

1. ÜBERWACHEN

Wir integrieren Ihre Systeme (z. B. Endpunkte, Server, Active Directory, Firewalls, Netzwerke, Microsoft Office 365, Cloud-Ressourcen usw.) mit einer anpassbaren und bewährten Erkennungsplattform, die Ihr System rund um die Uhr mit einer auf künstlicher Intelligenz basierten Erkennungslogik überwacht.

2. ANALYSIEREN

Ein Team engagierter Sicherheitsanalysten kontextualisiert die Informationen und bewertet die Ereignisse.

3. REAGIEREN

Wenn ein Angriff entdeckt wird, sorgen wir dafür, dass das Problem auf jeden Fall behoben wird. Wir arbeiten unabhängig oder Hand in Hand mit Ihrer IT-Abteilung und Ihren Lieferanten, um die Bedrohung einzudämmen und Ihre Systeme so schnell wie möglich wiederherzustellen, wobei wir uns auf vorher vereinbarte Vorgehensweisen und jahrelange praktische Erfahrung stützen.

WAS SIE ERWARTEN KÖNNEN

Wir sorgen dafür, dass die Überwachung Ihrer Systeme und die Reaktion auf Bedrohungen mühelos und ohne Kopfschmerzen vonstattengeht. Nebst dem SOC erhalten Sie Unterstützung durch ein geschultes internationales Incident Response Team, das in der Analyse und Behebung von Problemen erfahren ist und Hand in Hand mit dem starken, lokalen Team in der Schweiz zusammenarbeitet. Sie arbeiten mit einem Partner zusammen, den Sie kennen und dem Sie vertrauen, somit geniessen Sie die Gewissheit, dass Ihre IT-Umgebung in sicheren Händen ist.

SIE PROFITIEREN VON

- Proaktivem, durchgängigen Schutz vor internen und externen Bedrohungen
- Live-Dashboards und regelmässigen Berichten über den Status Ihrer Systeme
- Plattformanpassungen für die Überwachung von Infrastrukturen oder kritischen Anwendungen
- Erschwinglicher Pay-as-you-go-Lösung, die schnell eingesetzt werden kann, um sich an veränderte organisatorische Anforderungen anzupassen
- Empfehlungen für kontinuierliche Verbesserungen der Sicherheitseinrichtung mit Industriestandards, wie dem MITRE ATT&CK-Framework, durch Analysen von Vorfällen und aktuellen Entwicklungen in der globalen Bedrohungslandschaft.

arco Albulastrasse 34, 8048 Zürich 044 244 02 20 info@arco-it.ch www.arco-it.ch