IT CONSULTING & ENGINEERING

CYBER DEFENSE CENTER LÖSUNG PLANEN UND UMSETZEN

Daten sind in der modernen Arbeitswelt ein zentraler Wertfaktor und Treiber neuer Geschäftsmodelle. Die digitale Transformation erhöht dabei nicht nur die Datenmenge, sondern auch den Bedarf an deren Schutz.

Mit der grösser werdenden Bedeutung der Digitalsierung wächst auch die Bedrohung durch Cyberkriminalität. Mit der wachsenden Abhängigkeit von Daten und IT-Diensten rücken diese zunehmend ins Visier professioneller agierender Hackergruppen. Diese versuchen durch gezielte Angriffe oder durch Diebstahl und Verschlüsselung von Daten finanzielle Vorteile zu erlangen. Berichte des Bundesamtes für Cybersicherheit (BACS) sowie internationale Analysen wie der Data Breach Investigations Report zeigen eine stetige Zunahme sowohl der Häufigkeit als auch der Raffinesse dieser Angriffe.

Zum Schutz der Geschäftstätigkeit ist daher der Einsatz wirksamer Cybersecurity-Massnahmen unabdingbar. Eine zentrale Rolle kann dabei ein Cyber Defense Center (CDC) übernehmen. Ein solches Zentrum ermöglicht die kontinuierliche Überwachung der IT-Infrastruktur und reagiert flexibel auf sich ständig verändernde Angriffsmethoden. Angesichts der Tatsache, dass viele Angriffe mit einer zeitverzögerten Wirkung – etwa durch monatelang unerkannte Infektionen – einhergehen, ist es entscheidend, potenzielle Bedrohungen frühzeitig zu erkennen.

Basierend auf langjähriger Praxiserfahrung hat die In&Out AG ein Vorgehen zur Einführung von Cyber Defense Center Lösungen erstellt.

Schutzbedarf und Use Cases identifizieren

- Eingesetzten Applikationen und Systeme, inkl. den Umsysteme und externen Partnern identifizieren
- Bestehende Security Implementationen aufnehmen
- Definieren, welche Sicherheitsdienste des Cyber Defense Centers umgesetzt werden sollen und welche allenfalls später dazukommen
- Use Cases identifizieren und definieren, welche umgesetzt werden sollen, basierend auf dem grössten Risiko

Zielbild und Betriebsmodell definieren

- Ausarbeitung des zukünftigen Target Operating Models
- Definieren, ob die Cyber Defense Lösung selbst betrieben oder als Service bezogen werden soll
- Rollen, Verantwortlichkeiten und Schnittstellen zwischen internen und externen Beteiligten definieren

Implementierung der Cyber Defense Lösung

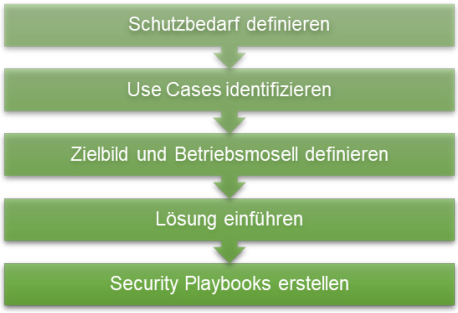
- Technische Umsetzung der Cyber Defense Lösung, inkl. Datenkollektor
- Integration der abzudeckenden Systeme und Sicherstellung, dass die notwendigen Informationen und Logs eingebunden werden
- Prozessumsetzung mit Einbindung aller Parteien und Prüfung der Prozesse
- Schrittweise Einführung der definierten Use Cases

Security Playbooks erstellen

- Definition der umzusetzenden Security basierend auf dem grössten Risiko
- Erstellen der Security Playbooks inkl. Einbindung aller Parteien
- Prüfung der Security Playbooks mittels Simulation oder Übung.

DAS VORGEHEN:

Der Leistungsumfang umfasst die Analyse des Schutzbedarfs, die Bestimmung des Betriebsmodells sowie die Begleitung bei der Einführung einer Cyber Defense Center Lösung.



IHR NUTZEN:

- Eine Cyber Defense Lösung, die exakt auf die Anforderungen Ihres Unternehmens zugeschnitten ist und die grössten Cyberrisiken abdeckt.
- Ein klar definiertes Betriebsmodell, das alle relevanten Abteilungen und Partner einbindet und die Bedürfnisse des Unternehmens berücksichtigt.
- Frühzeitige Erkennung und Verhinderung von Sicherheitsvorfällen und Schwachstellen.
- Definiertes Vorgehen im Falle eines Cyberangriffs sowie vordefinierte Massnahmen zur Eindämmung und Beseitigung des Angriffs

KONTAKTIEREN SIE UNS:

Wir freuen uns über Ihre Kontaktaufnahme zur fachlichen Vertiefung der Thematik!

Silvio Pelli
Senior IT Consultant
silvio.pelli@inout.ch