execure

Netzwerk Sicherheitsarchitektur

Adaptives Zonendesign

Unsere Workshops richten sich an Firmen, deren Kerngeschäftsprozesse eine erhöhte Netzwerkabhängigkeit zu beschränkt vertrauenswürdigen Bereichen aufweisen. Des Weiteren orientieren sich diese Workshops an den spezifischen Bedürfnissen der Unternehmen, um ihre Assets angemessen zu schützen, sowie die Transparenz im Datenverkehr zu steigern.

Netzwerkzonen ermöglichen es den Unternehmen, eine granulare Zugriffskontrolle innerhalb der Datennetze anzuwenden, um so das Risiko möglicher Expositionen zu verringern bzw. zu begrenzen.

Die aus den Workshops resultierenden Konzepte basieren darauf, Systeme mit unterschiedlichen Vertrauensanforderungen voneinander zu trennen und entsprechend ihrem Schutzbedürfnis zu gestalten.

Moderne Security Gateways werden heute dazu verwendet, den Zugang und die Verbindungen zwischen den Netzwerkzonen zu kontrollieren. Mittels Authentifizierung, Autorisierung und Zugriffsvalidierung, wie auch durch Threat Prevention Features kann der Schutzlevel weiter erhöht werden.

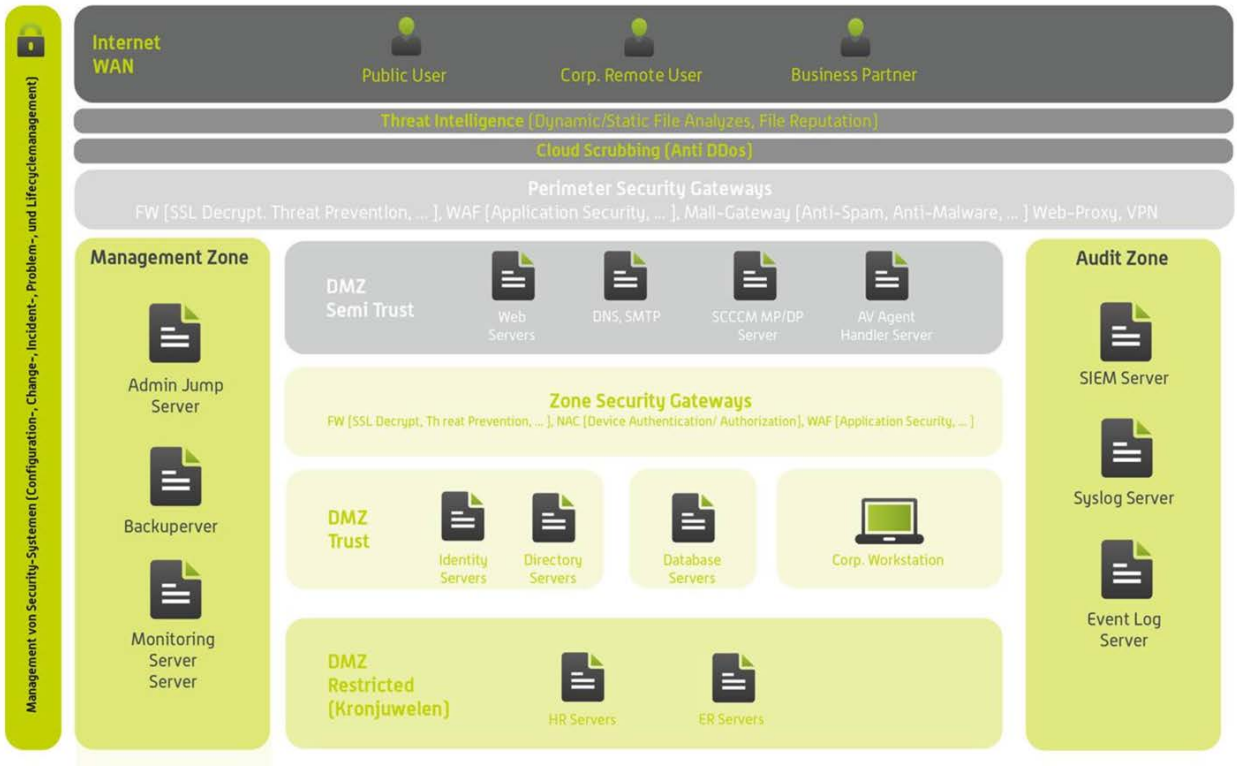

Abbildung 1. Beispiel einer logischen Netzwerk Sicherheitsarchitektur.

Vorgehen beim Entwickeln einer Netzwerk Sicherheitsarchitektur

Um eine effektive Netzwerk Sicherheitsarchitektur zu entwickeln, definiert die execure in einem ersten Schritt mit dem Kunden zusammen den Umfang. Dabei wird beispielsweise definiert, inwiefern bestehende Aussenlokationen sowie die Netzwerke der externen Dienstleister in das Konzept miteinbezogen werden. Anschliessend stellt die execure in Zusammenarbeit mit dem Kunden den Kontext her:

- Verstehen der kritischen Geschäftsprozesse, sowie deren Abhängigkeiten.
- Identifizieren der zugehörigen Assets.
- Ableiten des spezifischen Gefahrenumfelds sowie des Risiko Appetits.
- Identifizieren der IST Architektur, sowie der Funktionellen- und Nichtfunktionellen Anforderungen.
- Bestimmen der Vorgehensweise, um die Sicherheitsarchitektur zu entwickeln.

Ist der Kontext hergestellt, beginnt die eigentliche Entwicklung der Netzwerk Sicherheitsarchitektur.

- Erstellen der Sicherheitsarchitektur, wie auch das Identifizieren zusätzlicher Requirements-Provider.
- Abstimmen der entsprechenden Anforderungen und ebenso die Ergänzung der Netzwerk Sicherheitsarchitektur.
- Publizieren und Präsentieren der Netzwerk Sicherheitsarchitektur.

Ist die Sicherheitsarchitektur publiziert und akzeptiert, kann die execure den Kunden weiterhin unterstützen, je nach Ausprägung der Produkte. Demnach kann die execure bei der Planung und Umsetzung der Sicherheitsarchitektur behilflich sein oder aber den vollständigen operativen Betrieb inkl. Configuration-, Change- Incident-, Problem und Lifecyclemanagement von Security Systemen wahrnehmen. Für den operativen Betrieb werden an ITIL angelehnte Critical Success Factors (CSF) und Key Performance Indicators (KPI) zusammen mit dem Kunden definiert, um den Security Management Prozess möglichst produktiv zu gestalten.

Mögliche Outputs

Die execure erbringt in Abhängigkeit der Kundenbedürfnisse aufgrund ihrer langjährigen Erfahrung und hoch qualifizierten technischen Security Experten einen effektiven Mehrwert:

- Review der bestehenden Sicherheitsarchitektur.
- Vorschlag einer möglichen SOLL Architektur.
- Unterstützung bei der Implementierung.
- Betrieb von einzelnen Sicherheitssystemen.
- Betrieb der Sicherheitsinfrastruktur.

Möchten Sie mehr erfahren?

Gerne unterstützen wir Sie bei Ihrem nächsten Projekt und stellen Ihnen auf Anfrage Referenzen zur Verfügung.