IHRE HERAUSFORDERUNG

Für den wirksamen Schutz eines Unternehmensnetzwerks sind die Planung und Vorbereitung Kernpunkte einer zukunftsfähigen Architektur und eines späteren sicheren Betriebs. Wir unterstützen Sie dabei, Ihre Anwendungen und Ihre Daten zu schützen und Schaden von Ihrer Infrastruktur abzuwenden sowie Risiken und Sicherheitslücken zu minimieren.

➲ Schutz des Unternehmensnetzwerkes muss stetig aktuell gehalten werden

Aufgrund unseres technisch-wirtschaftlichen Hintergrundwissens legen wir Wert auf „State of the Art“-Lösungen, ohne den wirtschaftlichen Fokus aus den Augen zu verlieren. Des Weiteren müssen Lösungen effizient betreibbar bleiben.

Technisch legen wir besonderes Augenmerk auf die Aspekte Vertraulichkeit, Integrität und Verfügbarkeit, welche die Kernelemente einer Sicherheitsarchitektur darstellen.

In die Betrachtungen beziehen wir prozessorientierte, organisatorische und technologische Fragestellungen ein, die unabdingbar zu einer Sicherheitsarchitektur gehören:

- Prozessorientiert, zur Implementierung reibungsarmer Abläufe
- Organisatorisch, zum Erreichen einer „Sicherheitskultur“ und Einbetten in die Unternehmensstrategie
- Technologisch, um Aspekte, wie z.B. Systemkomponenten, Inventar, Daten und Standards wie ISO und BSI Vorschriften einzubeziehen.

Im Ergebnis erarbeiten wir mit Ihnen gemeinsam wirksame und zukunftsgerichtete Schutzmechanismen für Ihre Unternehmensressourcen. Diese beinhalten beherrschbare Risiken und ermöglichen einen späteren sicheren Betrieb.

UNSERE LEISTUNGEN

Die Bedeutung des Sicherheitsniveaus von ITK Infrastrukturen in Industrie und öffentlicher Verwaltung steigt kontinuierlich. Stetig fortschreitende Anforderungen an die Digitalisierung in Unternehmen, vor allem aber das parallele Anwachsen von digitalen Risiken und akuten Bedrohungen, bedingen neue Maßstäbe an die Sicherheit, sowohl in der technischen Infrastruktur als auch bei den unternehmensinternen Prozessen.

➲ Passgenaue Lösung mit Fokus auf Ihre Unternehmensziele

Somit gehen Vorteile auf der einen Seite einher mit immer neuen Angriffs- und Bedrohungsszenarien, die zu hohen finanziellen Schäden, zu Verlust von Vertrauen sowie dem Verletzen von personenbezogenen Daten auf Kunden-/Partnerseite füh-

ren können. Zahlreiche Beispiele, wie z.B. aus Medien bekannte Fälle über Betroffene durch Ransomsoftware, aber auch neue Gesetze in Sachen IT-Sicherheit und Datenschutz untermauern den aktuellen Bedarf.

Unsere Aufgabe als ITK-Dienstleistungsunternehmen ist es, unsere Kunden, u.a. aus den Bereichen Mobilfunk, öffentliche Auftraggeber, Medien, Transport und Logistik bei den Herausforderungen bezüglich ihrer Netzwerk- und Sicherheitsinfrastruktur anforderungsorientiert zu unterstützen.

Hierfür bieten wir Ihnen folgende Leistungen an:

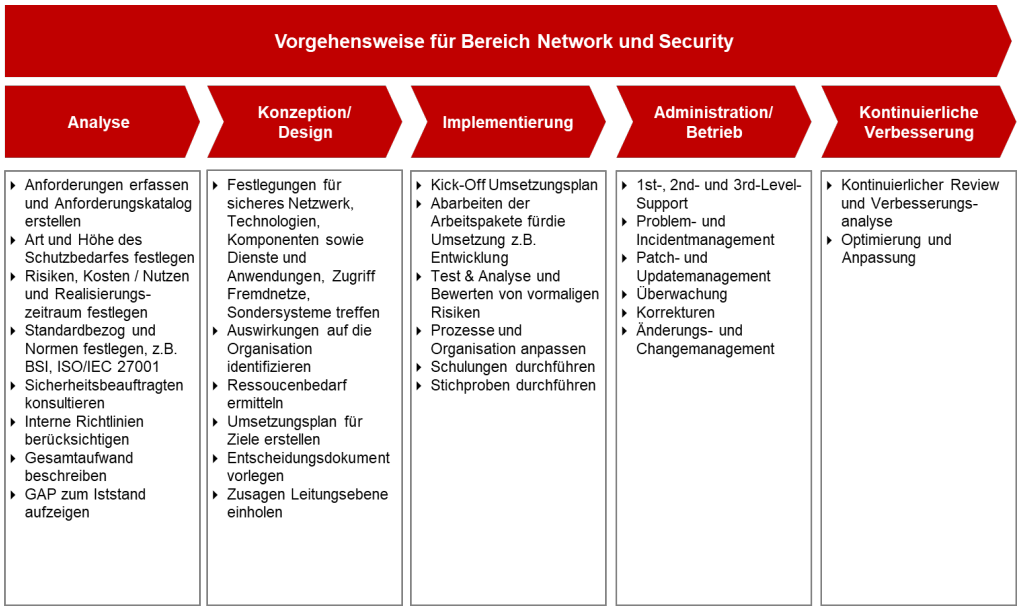
- Analyse des Ist Zustandes von LAN/WAN und IT-Architekturen (Ende-zu-Ende)
- Lösungsentwicklung, Design und Konzeption
- Umsetzungsplanung und Implementierung
- Bewertung und Einführung neuer Systeme und Komponenten
- Weiterentwicklung von technischen Konzepten
- Erstellung, Anpassung von Konfigurationsvorgaben
- Administration und Betriebsunterstützung
- Fortschreibung von Betriebshandbüchern

Unsere Leistungen münden in den folgenden konkreten Ergebnissen für Ihr Unternehmen:

- Identifikation von Schwachstellen
- Aufzeigen von Schutzmaßnahmen
- Konzeption und Umsetzungen der Schutzmaßnahmen
- Kosten und Nutzenbetrachtung
- Verifikation und Test der Wirksamkeit der Maßnahmen
- Sichere Kommunikation von „innen“ und „außen“
- Einführung, Optimierung und Betrieb eines IT- Sicherheitsmanagementsystem
- Dokumentation der Lösung

UNSERE VORGEHNSWEISE

Das Thema Netzwerk- und Informationssicherheit ist ein kontinuierlicher Prozess, aufsetzend auf einer im Unternehmen bestehenden Sicherheitskultur. Unsere Erfahrungen und die Arbeitsweise aus verschiedenen Sektoren haben wir in der folgenden Grafik abgebildet:



Zunächst beginnen wir mit einer Anforderungsanalyse mit Schutzbedarfsfeststellung, in der die Art und Höhe des Schutzbedarfes festgelegt wird und ein Abgleich mit dem Ist-Stand der IT-Architektur erfolgt. Ggf. führen wir Penetrationstests durch, welche etwaige zusätzliche Schwachstellen aufdecken. Wir betrachten dazu Komponenten, Dienste und Anwendungen. Organisatorische, auf Prozessen beruhende Festlegungen fließen mit in die Betrachtungen ein.

Wir orientieren uns bei unserer Arbeit an den vorliegenden Erfahrungen aus vorangegangenen Projekten sowie an gängigen Festlegungen, Normen und Standards (wie z.B. DIN ISO/IEC 27001, Infrastrukturen mit hohen Sicherheitsanforderungen).

Wir berücksichtigen bei der Analyse Ihrer Gegebenheiten und möglichen Lösungsansätzen industrietypische Standards. Die Ergebnisse der Analyse bilden die Grundlage für das Konzept und die spätere Implementierung.

Die Konzeption beinhaltet entsprechende Maßnahmen, die dazu führen, Festlegungen für eine sichere Netzwerkarchitektur zu treffen. Wesentlich ist hier die Schaffung von Akzeptanz für die vorgeschlagenen Maßnahmen auf allen Ebenen.

In der Implementierung überprüfen wir, ob vormalige Risiken mit den getroffenen Maßnahmen gemildert bzw. ausgeschlossen wurden.

Die Umsetzung der getroffenen Sicherheitsmaßnahmen und die Schaffung der notwendigen Akzeptanz wird über Kommunikationsmaßnahmen, Schulungen und regelmäßige Feedback-Dialoge vorgenommen.

In der Administrations- und Betriebsphase werden die eingeführten Maßnahmen kontinuierlich auf ihre Wirkung hin überwacht und erforderlichenfalls Korrekturmaßnahmen eigeleitet. Dies erfolgt auf Basis eines kontinuierlichen Verbesserungsprozesses (KVP) mit dem Ziel, proaktive Maßnahmen gegen mögliche Angriffs- und Gefahrenpotenziale frühzeitig zu erkennen, in geordneter Weise auf mögliche Sicherheitsvorfälle zu reagieren und ggf. erforderliche Maßnahmen durchzuführen, z.B. durch Umplanungen. Das setzt voraus, dass im Betrieb klare Aufgabenzuordnungen vorhanden sind und entsprechende standardisierte Prozesse bestehen.

UNSERE REFERENZEN

➲ Wir kennen uns aus!

- Analyse der zu schützenden geschäftskritischen IT-Anwendungen und digitalen Informationen, Ermittlung der Schutzbedarfe und adäquate Segmentierung von anderen Unternehmensdatennetzen für eine Rundfunkanstalt
- Betrieb der IT Security Infrastruktur als Managed Service für eine Rundfunkanstalt
- Definition der Betriebsprozesse zur Messung und Steuerung der existierenden IT-Services und Schärfung und Umsetzung der dafür bereits geschaffenen Werkzeuge wie Prozessabläufe und Servicescheine für die Betriebsorganisation einer Rundfunkanstalt
- Konzeption und Einführung einer Lösung zur strategischen Identifizierung, Authentifizierung und Autorisierung aller ans Unternehmensnetzwerk angeschlossenen Endgeräte bei einer Rundfunkanstalt
- Schaffung einer neuen technischen Plattform zur Integration von zwei verschiedenen IT- und Netzwerksysteme für einen weltweit führenden Telekommunikationskonzern
- Erstellen von anwendungsspezifischer Lastenhefte für OT/IT Security Komponenten und durchführen des Anforderungsmanagements für technische Aspekte für ein EU Vergabeverfahren
- Testen von OT/IT-Security-Komponenten für Digitale Stellwerke eines Bahnunternehmen inkl. Dokumentation der Durchführung und der Ergebnisse zur Vorbereitung der Freigabe der Komponenten

Bildquelle: © denisismagilov/stock.adobe.com