SECURITY ANALYSE

Gegen Hacker hilft nur eines:

Sie können Hackerangriffe nicht vermeiden! Aber Sie können dafür sorgen, dass sie keinen Schaden anrichten. Hacker verschaffen sich über normale Benutzer-Accounts, die nur in den seltensten Fällen ausreichend geschützt sind, Zugriff zu privilegierten Accounts und damit zu sensiblen Unternehmensdaten. Unsere Antwort darauf: ZAK – **Z**ielgenaue **A**nalyse**K**raft für BRAK – **B**estmögliche **R**eaktion **A**uf **K**atastrophen.

So unterstützt Sie ZAK BRAK

Wir finden die Active Directory-Schwachstellen in kurzer Zeit und schaffen einen Aktionsplan zur Bereinigung: ZAK BRAK umfasst sowohl die Analyse und Absicherung von Windows- sowie Linux-Servern und -Clients als auch die Erhöhung der Sicherheit im Betrieb. Unter die Betriebsbeschau fallen die Abläufe und die Arbeitsweise der Administratoren ebenso wie die Einführung noch notwendiger Lösungen. Mit ZAK BRAK wird so weit wie möglich verhindert, dass Schaden an den Maschinen entsteht, der ein Neuaufsetzen ohne die Möglichkeit einer Migration notwendig macht.

Darum ITdesign

Wir erkennen sehr schnell, welche Praktiken im Unternehmen gängig sind und können demzufolge punktgenaue Empfehlungen für eine sichere IT-Infrastruktur aussprechen. Meist sind unsere Kunden verblüfft, wie uns das gelingt. Wir betrachten nicht nur das Active Directory, sondern auch die lokalen User-Datenbanken – zum Beispiel vom Member Server. Wir prüfen Windows- und Linux-Systeme gleichermaßen, weil wir für beide Betriebssystemtypen Spezialisten im Haus haben. Sie erhalten eine personalisierte Analyse Ihrer Systeme und konkrete Handlungsempfehlungen, die zu großen Teilen auf Best Practice-Ansätzen und erst in zweiter Linie auf dem Einsatz von teuren Produkten beruhen. Auf Wunsch wird ein Wirksamkeitsversprechen für das strukturierte Vorgehen im Vertrag verankert.

Ihre Erfolgsfaktoren

- Aussagekräftige Analyseergebnisse von Praktikern
- Klare, gut umsetzbare Maßnahmen
- Microsoft- UND Linux-Betrachtung
- Maßnahmen von unseren Kunden selbst umsetzbar

ITdesign.
So klar muss die Lösung sein.

IT/DESIGN
software projects & consulting

Projektablauf

1. Datenaufnahme

- Aufnahme aller planungsrelevanten Informationen, wie aktuelle Konfiguration, eingesetzte HW- und SW-Produkte
- strategische Vorgaben der Unternehmensleitung
- funktionale und individuelle Anforderungen
- Aufnahme der bereits im Einsatz befindlichen oder lizensierten Security Produkte

2. IST-Analyse/Zieldefinition

- Betrachtung des bestehenden Microsoft Active Directorys und der Windows-Systeme im Hinblick auf neue Security- und administrative Aspekte
- Rechtevergabe der MS-Infrastruktur
- Applikationen und deren Authentifizierungsmöglichkeiten
- Auswertung bzw. Identifikation von sicherheitsspezifischen Schwachstellen
- Auswertung von schwachen Protokollen
- Auswertung der Account Security von Benutzerkonten

3. Handlungsempfehlungen

- Anhand der IST-Analyse und der Zieldefinition wird ein Dokument erarbeitet, welches kurz-, mittel- und langfristige-Maßnahmen für die Verbesserung der IT-Sicherheit darstellt.

4. Gemeinsame Ausarbeitung der Lösungsvarianten

- Wir erarbeiten gemeinsam mit Ihrem Projektteam Lösungswege, um die Handlungsempfehlungen bestmöglich umsetzen zu können.

Auf Wunsch unterstützen wir auch bei der Behebung der Security-Schwachstellen, damit Ihre IT-Infrastruktur, Ihre Daten und Mitarbeiter vor allen Risiken bestmöglich geschützt sind.