Security „SecurIT“

Wir können nicht verhindern, dass Hacker kommen, aber, dass sie Schaden anrichten.

Normale Benutzer Accounts führen die Hacker zu privilegierten Accounts. Sie sind der Einstieg für Hacker in ein Unternehmen. Denn dann brauchen sie nur noch abwarten und mitlesen. Wer weiß schon, wie viele „Nicht-Mitarbeiter“ noch im System sind? SecurIT schließt diese Sicherheits-Lücke.

So unterstützt Sie SecurIT

SecurIT umfasst die Analyse und Absicherung von Windows Servern und Clients und Linux Servern sowie die Erhöhung der Sicherheit im Betrieb. Unter die Betriebsbeschau fallen sowohl die Abläufe und die Arbeitsweise der Administratoren, als auch die Einführung noch notwendigen Lösungen. Mit SecurIT 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 die Kunden verblüfft, wie uns das gelingt. Wir betrachten nicht nur das Active Directory, sondern auch die lokalen User Datenbanken von z.B. Member Servern. 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 Practices 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. SecurIT ist Teil des ITdesign Security Portfolios.

Ihre Erfolgsfaktoren

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

ITdesign.
So klar muss die Lösung sein.

Wettbewerb TOP SERVICE ÖSTERREICH

ITDESIGN
software projects & consulting