

Zusammenarbeit mit Partnern

Anforderungen an ein Projektbüro

BMW Group



Anforderungen an ein Projektbüro bei externen Partnern (Besetzung des Projektbüros nur durch Partner-Mitarbeiter)

Grundsätze

- Die Geheimhaltung ist zwischen den Partnern im Vertrag geregelt und vereinbart.
- Alle Mitarbeiter sind persönlich zur Geheimhaltung zu verpflichten.
- Ausrichtung am Standard ISO/IEC 27001 bzw. 17799 (VDA-Empfehlung vom Mai 2005).

Bautechnische Infrastruktur

- Eigener Raum; Auf Sicht- und ggf. Mithörschutz ist zu achten.
- Die Hoheit des Projektraums liegt beim Partner (Hausrecht).
- Das Zutrittskontrollsystem wird vom Partner (mindestens Schlüssellösung) installiert.
- Der Partner-Gebäudebereich ist alarmgesichert (Alarmverfolgung).

Hinweis:

- Ein Projektbüro muss nicht BMW-projektspezifisch unterteilt werden – ein Büro für alle BMW-Projekte genügt.

Organisatorischer Schutz

- Die Verantwortlichkeiten sind zu regeln (Zutrittsschutz, allgemeines Informationsschutzverhalten).
- Die Zutrittsberechtigung wird durch Partner gepflegt und kontrolliert.
- Auf Partner-Hardware darf ein BMW-Mitarbeiter seine persönlichen BMW-Authentisierungsdaten nicht benutzen. Gleiches gilt auch für externe Mitarbeiter, die im Auftrag von BMW tätig sind, sofern sie Rechte innehaben, die über das Projekt hinausgehen.
- Vertrauliche Daten müssen zugriffsgeschützt auf den Festplatten abgelegt werden.
- Streng vertrauliche Daten müssen verschlüsselt abgelegt werden, sofern unautorisierter Zugriff möglich ist (wie z.B. auf der Festplatte eines LapTops).
- Der Einsatz von mobilen Speichermedien (auch Laptop) ist vom Projektleiter (FK) genehmigen zu lassen.
- FAX und Drucker müssen innerhalb des Büros stehen.

Anforderungen an ein Projektbüro bei externen Partnern (Besetzung des Projektbüros nur durch Partner-Mitarbeiter)

Netzwerk (LAN)

- Die physikalische oder logische Trennung vom Partner-LAN ist zwingend.
- Die offizielle IP-Adressen werden vom Partner zur Verfügung gestellt.
(Alternativ: BMW stellt IP-Adressen nach RFC1918 172.16.0.0/12, 192.168/16 zur Verfügung)
- Das NAT (Network Address Translation) der Partner IP-Adressen auf die IP-Ranges des Projektbüros ist nicht erlaubt!
- Die aktiven Netzwerkkomponenten stehen in einem abschließbaren EDV-Schrank - Zugang haben nur die Systemverantwortlichen.

Anbindung an andere Netze

- Zugriff vom Partnernetz in das Projektbüro ist generell verboten. Einzige Ausnahme ist die Remote Administration des IT-Equipments im Projektbüro.
- Der Netzwerkübergang zum Partnerbüro sind zu dokumentieren und auf Verlangen BMW vorzulegen.
- Rahmenbedingungen zur Remote Administration müssen erfüllt sein, siehe letzte Folie.

Netzwerk (Supplieranbindung; WAN)

- Den externen Partnern steht nur ein selektiver Zugriff zu den BMW-Applikationen im BMW-Corporate Network (CN) zur Verfügung.
- Liegt der WAN-Übergabepunkt außerhalb des Projektbüros, so muss gewährleistet sein, dass der Datenverkehr zwischen Projektbüro und WAN-Übergabepunkt abhörsicher ist.

Hinweis:

- Verschlüsselung kann nur auf Anwendungsebene durchgeführt werden und kann auf Netzebene derzeit mit Ausnahme des VPN Clients von BMW nicht bereitgestellt werden.

Anforderungen an ein Projektbüro bei externen Partnern (Besetzung des Projektbüros nur durch Partner-Mitarbeiter)

Software und Applikationen

- Auf den Rechnern darf nur die für den Projektumfang notwendige Software installiert sein. Ein BMW-Enterprise-Client (Musterclient für interne BMW Mitarbeiter) ist nicht erlaubt.
- Sofern auch Applikationen und Systeme des Partners genutzt werden, muss in diesen Applikationen und Systemen ein angemessener Schutz der BMW-relevanten Daten sichergestellt sein (u.a. Datensegmentierung mind. auf Ebene der beteiligten Partnerfirmen, sichere Authentisierung, Rechte und Rollen, gesicherte Datenhaltung und Übertragung).

Hardware

- Externen Partnern wird empfohlen, die Hardware nach dem BMW Blueprint Standard auszuwählen.

Systemadministration

- Die Infrastruktur (Rechner, Server, IT-Equipment/ Netzwerkkomponenten) des Partners wird vom Partner betreut.
- Es muss gewährleistet sein, dass aktuelle Virensignaturen und sichere OS-Release-Stände eingespielt sind.

Security-Audit

- Der Bedarf für einen Audit wird nach dem BMW Bewertungsschema analysiert.
- Das Audit wird durch akkreditierte Dienstleister durchgeführt.

Rahmenbedingungen zur Remote Administration des IT-Equipment in Projektbüros durch den Partner

Organisatorische Ebene

- Der Zugang zum administrierbaren IT-Equipment ist dediziert zu regeln.
- Der autorisierte Remote Administrator muss eine Geheimhaltungsverpflichtung unterschreiben.
- Es muss sichergestellt sein, dass nur die namentlich festgelegten Administratoren auf die IT-Systeme zugreifen können. Die Namen der Systemadministratoren müssen BMW auf Verlangen offen gelegt werden.

Systemebene

- Remote-Zugang zum Projektbüro ist nur temporär, überwacht und ausschließlich für Wartungs- und Administrationsarbeiten zulässig.
- Für die Remote-Administration ist starke Authentisierung erforderlich (Wissen + Besitz, z.B. UserId/Passwort + SecurID).
- Die Remote Administration muss mitprotokolliert werden und das Protokoll auf Verlangen BMW zur Verfügung gestellt werden.

Netzwerkebene

- Während der Administration darf die Administrationskonsole nur mit dem Netzwerk des Projektbüros verbunden sein.
- Eine abhörsichere Verbindung zwischen der Administrationskonsole und dem Projektbüro ist notwendig.