# Zusammenarbeit mit Partnern

## Anforderungen an ein BMW Satellitenbüro

BMW Group

# Anforderungen an BMW Satellitenbüro

(Besetzung im Satellitenbüro durch BMW und externe 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.
- Sofern BMW die Hoheit über das Satellitenbüro hat, ist das BMW-Standard-Zutrittskontrollsystem (Ausweisleser) zwingend. Falls der Partner die Hoheit hat, muss er ein Zutrittskontrollsystem installieren, das vergleichbar mit dem BMW-Standard ist
- Büro muss alarmgesichert sein (Entweder durch direkte Alarmsicherung des Büros oder durch Alarmsicherung der Partnerlokation).

ISB = Informationsschutzbeauftragter PL = Projektleiter

# Anforderungen an BMW Satellitenbüro

(Besetzung im Satellitenbüro durch BMW und externe Mitarbeiter)

## Organisatorischer Schutz

- Die Verantwortlichkeiten sind zu regeln (Zutrittsschutz, allgemeines Informationsschutz-Verhalten).
- Die Hoheit für das Büro kann bei BMW oder beim Partner liegen.
- Sofern BMW im Satellitenbüro die Hoheit innehat, wird die Zutrittsberechtigung durch BMW Fachabteilung freigegeben, gepflegt u. kontrolliert. Sofern der Partner die Hoheit hat, muss BMW zumindest eine Kontrollmöglichkeit eingeräumt werden.
- Transparente Anbindung an das BMW CN ist nur für BMW-Mitarbeiter und nur mittels starker Authentisierung plus verschlüsselter Übertragung plus BMW Hard-/Software erlaubt.
- 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 Kooperationsprojekt hinausgehen.
- Das sichtbare Tragen des Firmenausweises ist obligatorisch.
- 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).
- FAX und Drucker müssen innerhalb des Büros stehen. Drucker dürfen vom BMW CN aus nicht ansprechbar sein, sofern kein weiterer Schutz aktiviert ist (Alternative: Printouts sind nur mittels Ausweisleser am Drucker möglich).

ISB = Informationsschutzbeauftragter PL = Projektleiter

# Anforderungen an BMW Satellitenbüro

(Besetzung im Satellitenbüro durch BMW und externe 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 Satellitenbüros ist nicht erlaubt!
- Die aktiven Netzwerkkomponenten stehen in einem abschließbaren EDV-Schrank im Satellitenbüro. Zugang haben nur die Systemverantwortlichen.

### Hinweis:

- Wird eine logische Trennung gewählt, muss eine Netzwerkabsicherung des Satellitenbüros gegenüber dem Partner-LAN vorhanden sein, z. B. durch eine Firewall.

## Netzwerk (WAN)

- Den BMW MA muss ein transparenter Zugriff auf das BMW- CN (ISDN, Festverbindung, VPN) ermöglicht werden.
- Den externen Partnern steht nur ein selektiver Zugriff zu den BMW-Applikationen im BMW-Corporate Network (CN) zur Verfügung.
- Sofern der WAN-Übergabepunkt nicht mindestens im Satellitenbüro (Alternativ: Im Secure-Office) liegt, muss der Datenverkehr verschlüsselt werden (siehe Hinweise).

### Hinweise:

- Ist der WAN-Übergabepunkt beim externen Partner, so muss gewährleistet werden, dass der Datenverkehr zum WAN Übergabepunkt NICHT abgehört werden kann.
- Heutiger Stand zur verschlüsselten Kommunikation: BMW VPN-Client nur für BMW MA (Verschlüsselung bis zum Endgerät). Entscheidung BMW VPN-Client für Externe ist offen. Lösung ist nur für Windowsplattform vorhanden. Für Workstations gibt es derzeit keine Lösung bei BMW, deswegen dürfen BMW Workstations nur im Secure-Office eingesetzt werden.

# Anforderungen an BMW Satellitenbüro

(Besetzung im Satellitenbüro durch BMW und externe Mitarbeiter )

## Software und Applikationen

- Der Zugriff auf das BMW CN bzw. auf BMW Applikationen darf nur mittels freigegebener Software (Blueprint) von BMW erfolgen.
- 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.
- Hinweis:
  BMW Rechner dürfen nur dann im Satellitenbüro stehen, wenn folgende Anforderungen erfüllt sind:
  - Schutz des Rechners durch Personal Firewall.
  - Zugriffsschutz für lokale, streng vertrauliche Daten durch Festplattenverschlüsselung.
  - Sichere Anbindung des Rechners zum BMW Netzwerk (z.B. mittels VPN und SecurID-Card).

## Systemadministration

- Die BMW IT-Infrastruktur (IT-Equipment/aktive Netzwerkkomponenten) wird von BMW bzw. Provider betreut.
- Die Partner IT-Infrastruktur (Rechner, Server, IT-Equipment/ Netzwerkkomponenten) wird vom Partner betreut.
- Es muss gewährleistet sein, dass aktuelle Virensignaturen und sichere OS-Release-Stände eingespielt sind.
- Wird eine Firewall zwischen dem Partnernetz und BMW-Satellitenbüro-LAN eingesetzt, so muss
  1. entweder die Konfiguration und Administration der Firewall durch BMW erfolgen
  2. oder es muss die Konfiguration und Administration vertraglich geregelt werden.

## Security-Audit

- Der Bedarf für einen Audit wird nach dem BMW Bewertungsschema analysiert.
- Falls BMW die Hoheit über die Räumlichkeiten hat, erfolgt die Durchführung durch BMW Fachbereiche.
- Falls die Partnerfirma die Hoheit hat und noch nicht zertifiziert ist, erfolgt die Durchführung durch akkreditierte Dienstleister.

# 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 Satellitenbüro ist nur temporär, überwacht und ausschließlich für Wartungs- und Adminstrationsarbeiten 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.

# Anhang

Definition der Benutzergruppen

- **BMW Mitarbeiter**
  - Zutritt zu allen vorgesehenen Büroflächen
  - Zugriff auf alle für seine Tätigkeit benötigten projektrelevanten Daten im Rahmen seines Arbeitsvertrags
  - Transparenter Zugriff auf BMW CN

- **Externer Mitarbeiter / Fremdkraft**
  - Zugriff auf alle für seine Tätigkeit benötigten projektrelevanten Daten

Hinweis:

In diesem Foliensatz enthaltene Aussagen zu externen Mitarbeitern / Fremdkräften setzen jeweils eine Mitarbeit im Kooperationsprojekt voraus.