CHINA 華牌 BRAND®

# CYBERSECURITY IN CHINA – MULTI-LEVEL PROTECTION SCHEME 2.0

## Fragen und Antworten



CHINABRAND IP CONSULTING GMBH

Grashofstrasse 3 ▪ 80995 München ▪ +49 89 32 12 12 800

info@chinabrand.de ▪ www.chinabrand.de

# Das wichtigste im Überblick

***Was ist das Multi Level Protection Scheme 2.0?***

Das MLPS ist ein System zur Stärkung der Daten- und Cybersicherheit. Es verpflichtet Unternehmen dazu, anhand der gesetzlichen Vorgaben eines mehrstufigen Schutzsystems sicherzustellen, dass keine Daten gestohlen oder gefälscht werden können und ihre IT-Systeme frei von Interferenzen, Schäden oder unbefugtem Zugang sind.

***Für welche Unternehmen gilt das MLPS?***

Das MLPS 2.0 gilt für alle Unternehmen aller Branchen, die in China niedergelassen sind, und ist nicht auf Internet- oder IT-Unternehmen beschränkt.

***Wer führt die Zertifizierung der IT-Systeme durch?***

Zertifikate werden einzeln für jedes IT-System nach der Einstufung in den notwendigen Sicherheitslevel von der lokalen Polizei, dem Public Security Bureau (PSB), erstellt.

***Wie ist ein IT-Systeme definiert?***

Ein IT System (Definition nicht identisch mit der Definition des BSI Grundschutz ist eine logische (sinnvolle) Einheit zur Verarbeitung bestimmter zusammenhängender Daten mit einem bestimmten Ziel. Es beinhaltet alle Hard- und Software die notwendig ist, um das Erheben von Daten, die Verarbeitung, Bereitstellung und Speicherung zu ermöglichen. Oft hängt das System mit einer relevanten Geschäftsfunktion zusammen, ein gutes Beispiel hierfür sind das Enterprise-Resource-Planning System, oder das Customer-Relationship-Management System. Häufig besteht das IT-System nicht nur aus verschiedenster Hardware, sondern auch aus mehreren Anwendungen/Software. Vor allem im Bereich der industriellen Überwachung und Kontrollsystemen ist es meist sinnvoll mehrere Anwendungen zu einem IT-System gegliedert werden, beispielsweise zu einem Produktions-Überwachungs- und Kontroll-System.

Die Gliederung in IT-Systeme ist von Unternehmen zu Unternehmen unterschiedlich und kann nur unter Abfragung bestimmter Informationen, wie Netzwerktopologie, Geschäftsfunktionen, verarbeitete Daten, usw. erfolgen.

***Wie dringlich ist die Durchführung des MLPS für die IT-Systeme in China?***

Wir empfehlen allen in China niedergelassenen und auch den im Chinageschäft tätigen Unternehmen, die Themen Cyber Security und Datenschutz kurzfristig anzugehen und die gesetzlich geforderten Schutzmaßnahmen gemäß des MLPS zügig umzusetzen. Die chinesische Regierung hat die Überwachung in Sachen Cybersicherheit und Datenschutz jetzt deutlich verstärkt und drängt alle Unternehmen, ihre Verpflichtungen zu erfüllen. Unsere Erfahrungen in aktuellen Projekten zeigen, dass die Behörden die Umsetzung sogar durch unangekündigte Penetrationstests überprüft.

***Wie laufen die Überprüfung und Zertifizierung der IT-Systeme in der Praxis ab?***

Der erste Schritt ist die Ermittlung der notwendigen Sicherheitsstufe. Das geschieht durch die Abfrage verschiedener Informationen, unter anderem zur Netzwerktopologie, zu der Nutzung der Systeme, zu den verarbeiteten Daten, zu den Mengen der Daten, usw. Anhand dieser Daten kann die notwendige Sicherheitsstufe festgelegt werden. Die Einstufung muss durch Experten aus der Branche bestätigt werden. Danach wird der von den Experten unterschriebene Einstufungsbericht zusammen mit weiteren notwendigen Dokumenten wie der „Application Form“, dem „Network and Information Security Commitment“ und der „MLPs Emergency Contact Registration Form“ bei der Behörde für öffentliche Sicherheit eingereicht. Diese prüft die Unterlagen und stellt die Urkunde zur Sicherheitsstufe der Systeme aus. Danach beginnt die eigentliche Arbeit: die Anpassung der Sicherheitsmaßnahmen der Systeme an die gesetzlichen Anforderungen.

Zuerst werden die Anforderungen gemäß des ermittelten Sicherheitslevels mit den vorhandenen Sicherheitsmaßnahmen abgeglichen und die Systeme auf Schwachstellen getestet. Anhand der Ergebnisse wird eine Gap Analysis verfasst auf Grundlage derer wiederrum Empfehlungen zur Optimierung der Sicherheitsmaßnahmen der Systeme erarbeitet werden. Nicht alle gefundenen Probleme müssen behoben werden. Probleme, die ein hohes Sicherheitsrisiko darstellen müssen behoben werden, Probleme, die ein mittleres Sicherheitsrisiko darstellen, sollten nach Kräften behoben werden. Im Normalfall reicht es, wenn ca. 70-75% der Anforderungen erfüllt sind, solange alle Probleme, die ein hohes Risiko darstellen, behoben sind. Die Behebung der Probleme obliegt dem geprüften Unternehmen, wir sind während dieser Phase ausschließlich beratend tätig und unterstützen das Unternehmen dabei zu beurteilen, ob die gewünschte technische Lösung die gesetzlichen Anforderungen erfüllt oder nicht.

Nachdem die Sicherheitsmaßnahmen der Systeme dem entsprechend angepasst wurden, wird durch ein externes Testzentrum die Compliance mit den Anforderungen bestätigt.

***Ist es notwendig im Rahmen eines MLPS-Projektes neue Hard- oder Software zu implementieren?***

Da während des MLPS-Projekts die Compliance mit technischen und organisatorischen Sicherheitsanforderungen geprüft wird, ist damit zu rechnen, dass neue Hard- oder Software implementiert werden muss. Wenn sich zeigt, dass neue Hard- oder Software installiert werden muss, liegt die letztendliche Entscheidung darüber, welcher Anbieter gewählt wird beim Kunden.
CHINABRAND unterstützt dabei zu überprüfen, ob die gewählten Komponenten den Anforderungen entsprechen. Der Lieferant der Komponenten übernimmt die Installation und Konfiguration.

***Wie lange dauert ein MLPS-Projekt in der Regel?***

Da die meisten MLPS-Projekte relativ komplex sind und staatliche Stellen involviert sind, erstrecken sich die Verfahren oft über mehrere Monate. Unternehmen sollten einen Projektzeitraum von 6 bis 12 Monaten kalkulieren.

***Mit welchen Kosten ist bei einem MLPS-Projekt zu rechnen?***

Die Kosten hängen von der Anzahl der zu überprüfenden IT-Systeme, dem notwendigen Sicherheitslevel und der Anzahl der zu bearbeitenden und zu übersetzenden Dokumente ab. Je nach Level müssen bis zu 350 gesetzliche Anforderungen bearbeitet werden. Der große Aufwand führt zu relativ hohen Kosten, die in aktuellen Projekten im hohen fünfstelligen bis niedrigen sechsstelligen EUR-Bereich liegen.

***Muss die Überprüfung wiederholt und das Zertifikat erneuert werden?***

Im Regelfall muss das Zertifikat nicht erneuert werden. Nur bei relevanten Änderungen, beispielsweise die Verarbeitung von wesentlich mehr oder wesentlich sensibleren Daten, als zu dem Zeitpunkt, als das Zertifikat erstellt wurde, ist es notwendig eine erneute Einstufung vorzunehmen und ein neues Zertifikat zu beantragen. Anders als das Zertifikat, muss die Überprüfung ob die Sicherheitsmaßnahmen der Systeme compliant mit den gesetzlichen Anforderungen sind, ab einem notwendigen Sicherheitslevel von 3 mindestens ein Mal jährlich oder ab einem Sicherheitslevel von 4 mindestens einmal alles halbe Jahr erfolgen.

# Weitere Informationen

Weitere Informationen über unsere Dienstleistungen finden Sie hier:

www.chinabrand.de

**Kontakt und Feedback**

info@chinabrand.de

Blog | LinkedIn | XING



Grashofstraße 3, 80995 München

+49 89 321212800

www.chinabrand.de