CHINA 華牌 BRAND®

CYBERSECURITY IN CHINA - MULTI-LEVEL PROTECTION SCHEME 2.0

Questions and Answers

CHINABRAND IP CONSULTING GMBH

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

info@chinabrand.de ▪ www.chinabrand.de

The Most Important at a Glance

What is the Multi Level Protection Scheme 2.0?

The MLPS is a system for strengthening data and cyber security. It obliges companies to ensure that no data can be stolen or falsified and that their IT systems are free from interference, damage or unauthorized access, based on the legal requirements of a multi-level protection system.

To which companies does the MLPS apply?

The MLPS 2.0 applies to all companies in all industries established in China and is not limited to Internet or IT companies.

Who carries out the certification of the IT systems?

Certificates are issued individually for each IT system after classification into the necessary security level by the local police, the Public Security Bureau (PSB).

How is an IT system defined?

An IT system (definition not identical with the definition of the *BSI Grundschutz*) is a logical (meaningful) unit for processing certain related data with a specific goal. It includes all hardware and software necessary to enable the collection, processing, provision and storage of data. Often the system is related to a relevant business function, a good example being the Enterprise Resource Planning System, or the Customer Relationship Management System. Often the IT system consists not only of a wide variety of hardware, but also of several applications/software. Especially in the area of industrial monitoring and control systems, it usually makes sense to combine several applications into one IT system, for example a production monitoring and control system.

The classification into IT systems varies from company to company and can only be done by querying certain information, such as network topology, business functions, processed data, etc.

How urgent is the implementation of the MLPS for the IT systems in China?

We recommend that all companies established in China, as well as those engaged in business in China, address the issues of cyber security and data protection in the short term and swiftly implement the legally required protective measures under the MLPS. The Chinese government has now significantly increased cyber security and data protection monitoring and is urging all companies to meet their obligations. Our experience in current projects shows that the authorities are even verifying implementation through unannounced penetration tests.

How do the verification and certification of IT systems work in practice?

The first step is to determine the necessary security level. This is done by requesting various information, including the network topology, the use of the systems, the data processed, the quantities of data, etc. Based on this data, the necessary security level can be determined. The classification must be confirmed by experts from the industry. After that, the classification report signed by the experts along with other necessary documents such as the "Application Form", the "Network and Information Security Commitment" and the "MLPs Emergency Contact Registration Form" are submitted to the Public Security Authority. The latter checks the documents and issues the certificate for the security level of the systems. Then the real work begins: adapting the security measures of the systems to the legal requirements.

First, the requirements according to the determined security level are compared with the existing security measures and the systems are tested for vulnerabilities. Based on the results, a gap analysis is written, which in turn is used as a basis for developing recommendations for optimizing the security measures of the systems. Not all problems found have to be fixed. Problems that pose a high security risk must be fixed, problems that pose a medium security risk should be fixed to the best of our ability. Normally, it is sufficient if about 70-75% of the requirements are met, as long as all problems that pose a high risk are fixed. The elimination of the problems is the responsibility of the audited company, during this phase we act exclusively in an advisory capacity and support the company in assessing whether or not the desired technical solution meets the legal requirements.

After the security measures of the systems have been adapted accordingly, compliance with the requirements is confirmed by an external test centre.

Is it necessary to implement new hardware or software as part of an MLPS project?

As compliance with technical and organizational security requirements is checked during the MLPS project, it is likely that new hardware or software will need to be implemented. If it becomes apparent that new hardware or software needs to be installed, the final decision on which vendor to choose rests with the customer.
CHINABRAND assists in verifying that the selected components meet the requirements. The supplier of the components takes over the installation and configuration.

How long does an MLPS project usually take?

Since most MLPS projects are relatively complex and involve government agencies, the procedures often extend over several months. Companies should calculate a project timeframe of 6 to 12 months.

What costs can be expected for an MLPS project?

The costs depend on the number of IT systems to be checked, the necessary security level and the number of documents to be processed and translated. Depending on the level, up to 350 legal requirements have to be processed. The great effort involved leads to relatively high costs, which in current projects are in the high five-figure to low six-figure EUR range.

Does the verification have to be repeated and the certificate renewed?

As a rule, the certificate does not need to be renewed. Only in the case of relevant changes, for example the processing of significantly more or significantly more sensitive data than at the time when the certificate was created, is it necessary to reclassify and apply for a new certificate. Unlike the certificate, the verification of whether the security measures of the systems are compliant with the legal requirements must be carried out at least once a year from a necessary security level of 3 or at least once every half year from a security level of 4.

Further Information

You can find more information about our services here:

www.chinabrand.de

Contact and feedback

info@chinabrand.de

Blog | LinkedIn | XING

Grashofstraße 3, 80995 Munich

+49 89 321212800

www.chinabrand.de