Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im März 2013

Sehr geehrten Damen und Herren,

Unternehmen mit Firmenstandorten in aller Welt stehen vor der Problematik, Daten mit ihren Unternehmenteilen sicher über das Internet auszutauschen. Eine mögliche Lösung dieser Aufgabe ist die Verbindung mittels VPN[1].

Aus gegebenem Anlass möchten wir Ihnen einen aktuellen Fall zum Themenfeld verschlüsselte Datenübertragung per VPN näher bringen, der dem niedersächsischen Wirtschaftsschutz gemeldet wurde.

Wiederholt hat der Wirtschaftsschutz Niedersachsen zu den Risiken der Nutzung des Internets, speziell in China, sensibilisiert. In dem nachfolgenden Fall zeigt sich unter anderem die rechtliche Problematik in Ländern mit einer aktiven Internetzensur und deren Folgen bei Nichtbeachtung.

Für Rückfragen zu diesem Thema stehen wir jederzeit gerne zur Verfügung, wobei das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen unberührt bleibt.

Ihr Wirtschaftsschutz-Team

(1) VPN steht für "Virtual Private Network" oder "Virtuelles Privates Netz". Mit VPN lässt sich über ein offenes, ungeschütztes Netz (Internet, Funknetz) ein sicheres Teilnetz aufbauen, in dem die Kommunikation gegen Abhören und Zugriffe durch fremde Teilnehmer abgeschottet ist.

Niedersächsische Verfassungsschutzbehörde

Niedersächsisches Ministerium für Inneres und Sport
Referat 55 - Wirtschaftsschutz

Postfach 4420
30044 Hannover
Tel.: 0511 / 6709-247 oder -248
Email: wirtschaftsschutz@verfassungsschutz.niedersachsen.de

Falldarstellung

Ein mittelständisches Unternehmen mit einer eigenen Produktionsanlage in der VR China tauscht über eine VPN-Verbindung Daten zwischen dem Firmensitz in Deutschland und der Produktionsstätte in China aus.

Im Herbst 2012 treten Störungen bei der Übermittlung von Daten auf. Der VPN-Tunnel bricht ohne erkennbare Ursache zusammen und kann nicht wieder aufgebaut werden. Untersuchungen der firmeneigenen IT-Abteilung ergeben, dass der Port, der für die VPN-Tunnelung benutzt wird, von außen blockiert wird. Als erste Lösung werden andere Ports zum Aufbau der VPN-Verbindung genutzt. In der Folgezeit werden die neuen Ports in immer kürzerer Folge vom unbekannten Angreifer entdeckt und blockiert, so dass eine gesicherte Datenverbindung zwischen Deutschland und China dauerhaft nicht mehr möglich ist.

Im Frühjahr 2013 eskaliert die Situation. Der Firmenstandort in China wird komplett auf IP-Adressbasis blockiert. Ein Internetzugang ist seitdem nicht mehr möglich.

Dienstleister, die in China Internet-Services nutzen oder anbieten, berichteten zuerst über das Phänomen: Mehr und mehr Verbindungen wurden aus heiterem Himmel gekappt. Dazu gehören Virtual Private Networks (VPN), die vor allem Firmen die Anbindung von extern arbeitenden Angestellten ermöglichen und die unter anderem mit dem technischen Prinzip der Tunnelung eine sichere Verbindung zwischen zwei Punkten errichten.
Ein VPN-Anbieter für User innnerhalb und ausserhalb von China bestätigt, «dass mindestens vier für VPN gebräuchliche Protokolle in China geblockt werden».

Folgende Hintergründe sollten Sie kennen:

Die VR China gehört zu den Ländern, die eine Internetzensur durchführen. Anfang der 90er Jahre wurde im Rahmen des „Golden Shield Project“ zur Durchführung der Internetzensur in China die „Great Firewall of China“ als Gesamtsystem der Internetüberwachung eingeführt. Hier werden Techniken der IP-Adressblockaden, Filterung und Blockierung von Schlüsselworten benutzt. Das aktive Scannen nach VPN-Verbindungen und deren Blockade ist seit einiger Zeit offensichtlich ebenfalls Teil dieser Internetzensur.

Folgende Rechtslagen sollten Sie beachten:

In der Volksrepublik China darf nur eine staatlich genehmigte Verschlüsselungs-software genutzt werden. Der Gebrauch von Verschlüsselungstechniken oder Geräten, die Verschlüsselungstechniken verwenden, muss in der VR China bei der National Commission on Encryption Code Regulation (NCECR) angemeldet und genehmigt werden. Konkret enthält die Direktive Nr. 273 (Administration of Commercial Encryption Regulations – State Council Directive 273) folgende Kernaussagen:

1. Ohne Erlaubnis der chinesischen Regierung/Behörden ist der Betrieb von Verschlüsselungslösungen und Technologien untersagt.
2. Die Erlaubnis zur Einführung und zum Betrieb, ist über die chinesischen Behörden unter Angabe der notwendigen Produktinformationen einzuholen.
3. Beim Einsatz von Hardwareverschlüsselungsgeräten müssen chinesische Geräte genutzt werden.
4. Bei der Einfuhr in die Volksrepublik China muss auf die Einhaltung der zollrechtlichen Bestimmungen geachtet werden.

Wird gegen diese Maßgaben verstoßen, kann dies dazu führen, dass Computertechnik konfisziert wird. Vor diesem Hintergrund kann davon ausgegangen werden, dass nur Verfahren zugelassen sind, die von chinesischen Sicherheitsbehörden entschlüsselt werden können bzw. deren Schlüssel vom Verwender bei der NCECR hinterlegt wird.

Fazit:

In Ländern mit Internetzensur ist die Beachtung der landesspezifischen gesetzlichen Bestimmungen Voraussetzung für eine störungsfreie Datenübertragung ohne staatliche Repressionen. Die Sicherheit der Daten ist hier aber nicht in ausreichendem Maße gesichert. Grundsätzlich ist die Anbindung von Unternehmensstandorten im Ausland per VPN zur sicheren Datenübermittlung aber ein empfehlenswerter Ansatz.