Kurzgutachten

Zeitpunkt der Prüfung

01. Februar 2011-28. Februar 2011; Ergänzung im August 2012.

Adresse des Antragstellers

IC3S Information, Computer und Solartechnik AG
Bäckerbarg 6
22889 Tangstedt

Adresse der Sachverständigen

Rechtsanwältin Dr. Bettina Kähler
PrivCom Datenschutz GmbH
Behringstrasse 28a
22765 Hamburg

Dipl.-Ing. (FH) Silke Jacob
PrivCom Datenschutz GmbH
Behringstrasse 28a
22765 Hamburg

Kurzbezeichnung

Das IT-Produkt „mdex fixed.IP“ ermöglicht eine IP-basierte Kommunikation zwischen Mobilgeräten über Mobilfunknetze bzw. die Kommunikation von stationären Geräten mit einem Mobilgerät über ein Mobilfunknetz auf IP-Basis. Das ursprünglich zertifizierte Produkt „mdex fixed IP“ wird mittlerweile in einer erweiterten Version als „mdex fixed IP+“ vertrieben. Das Produkt „mdex fixed IP“ kann weiterhin als Teil einer sog. Complete Lösung erworben werden, jedoch nicht mehr in dem ursprünglich zertifizierten Rahmen. Inhaltlich sind die Produkte gleich, jedoch ist die Version „mdex fixed IP+“ um zwei Komponenten erweitert worden: web.direct und my-mdex.

Detaillierte Bezeichnung

Grundsätzlich ist die Erreichbarkeit von mobilen Endgeräten über die GPRS basierende Datenkommunikation im Mobilfunknetz und das Internet auf IP-Basis nicht möglich bzw. nicht vorgesehen. Ein Mobilgerät kann zwar z.B. eine Verbindung zu einer Leitstelle aufbauen, umgekehrt ist dies jedoch schwierig. Aufgrund von technischen Restriktionen der GPRS Mobilfunknetze ist es bislang grundsätzlich nicht möglich ein Mobilfunk-Modem vom Internet aus zu erreichen (z.B. für die Abfrage von Statusmeldungen oder für die Initiierung von Prozessen). Möglich ist prinzipiell immer nur, dass der Verbindungsaufbau über GPRS vom mobilen Endgerät aus initiiert wird, um die Kommunikation zu ermöglichen. In technischer und praktischer Hinsicht hat dies den Nachteil, dass sich viele Anwendungen in dieser Form nicht bzw. nur mit erheblichem Aufwand realisieren lassen.

Durch das IT-Produkt „mdex fixed.IP“ wird einem Mobilfunk-Modem (GPRS Router, GPRS Modem, PDA etc.) durch den einen verwendeten sog. IP-Server dauerhaft eine feste IP-Adresse zugeordnet. Damit ist es den Nutzern des Produktes möglich, das Modem und

daran angeschlossene Endgeräte sicher in einem privaten IP-Netzwerk über das Internet zu erreichen. Ferner ist eine Kommunikation der Mobilstationen untereinander in jede Richtung möglich.

Änderungen und Neuerungen des Produktes

Das Verfahren ist wie im Gutachten von 2008 beschrieben. Zweck des Verfahrens ist die Ermöglichung einer IP-basierten bidirektionalen Kommunikation von Geräten über Mobilfunknetze.

Die Erstzertifizierung 2008 bezog sich nur auf die Übertragung via GSM/GPRS. Eine Übertragung via UMTS bzw. LTE ist mit dem Verfahren auch möglich. Die Wahl des Übertragungsnetzes obliegt dem Anwender. Beim Einsatz in ländlichen Gebieten kann jedoch eine Übertragung von UMTS oder LTE nicht möglich sein, so dass dann zwangsläufig eine Übertragung via GSM/GRPS gewählt werden muss. Der Hersteller hat hierzu eine Risikoanalyse erstellt, deren Inhalt er im Gespräch mit dem Kunden diskutiert. Zudem ist das „Datenaufkommen“ bei der Nutzung des UMTS- bzw. LTE-Netzes durch permanentes Auf- und Abbauen von Verbindungen, ohne dass Daten fließen, sehr hoch und somit die Nutzung sehr teuer. Die Empfehlung des Herstellers zielt somit immer auf die Nutzung einer Verschlüsselung auf Applikationsebene ab (End-zu-End-Verschlüsselung), damit weder die Betreiber der Funknetze, noch der Hersteller einen Zugriff auf die übermittelten Daten bekommen.

Neu hinzugekommen sind die Komponenten web.direct und my-mdex. Web.direct ist standardmäßig abgeschaltet. Kunden, die diese Komponente nutzen wollen, erstellen sich im Zugangsportal ein Passwort und können web.direct dann aktivieren. Die Berechtigung des An- und Ausschaltens dieser Komponente liegt immer beim Kunden. Ic3s kann diese Berechtigung als Ganzes entziehen, nicht jedoch die Passwörter für den Zugang ändern.
My-mdex ist standardmäßig eingerichtet, die einzelnen Funktionen können jedoch von den Kunden abgeschaltet werden. Wenn sie deaktiviert sind, werden alle hinterlegten Daten automatisch gelöscht.

Web.direct:
Mit web.direct kann eine HTTP(S) Verbindung zu einer mobilen Webapplikation aufgebaut werden. Dazu wird jedem Zugang eine eindeutige URL zugewiesen. Der Verbindungsaufbau erfolgt über das mdex Gateway.
Das Gateway nimmt die Anfragen entgegen, authentifiziert und autorisiert die Anfrage, bevor sie in das geschützte VPN zu dem Zielgerät weiterleitet wird. Dabei wird zu der URL die entsprechende feste, private IP ermittelt und die HTTP Anfrage an diese IP gestellt.
Die Funktionalität steht nur zur Verfügung, wenn der Benutzer im Portal die Option für den gewünschten Zugang aktiviert hat.

My-mdex:
Über das my-mdex Portal können die Kunden ihre Zugänge administrieren und anpassen und sie können die Standortaufzeichnung aktivieren oder deaktivieren. Innerhalb von my-mdex werden RADIUS Daten aufgezeichnet, die eine Analyse der Zugänge ermöglichen (Datenvolumen, aufgebaute Sessions usw.). Die RADIUS Daten werden maximal 105 Tage gespeichert und dem Benutzer zur Verfügung gestellt. Die Standortdaten werden erst nach ausdrücklicher Aktivierung durch den Benutzer aufgezeichnet. Die Aktivierung kann widerrufen werden, dies führt zur sofortigen Löschung aller Standortdaten.

Datenschutzrechtliche Bewertung

Seit der Zertifizierung im Jahr 2008 sind erfolgreiche Angriffsszenarien auf das GSM/GRPS-Netz veröffentlicht worden. Das Risiko ist vom Hersteller in einer Risikoanalyse beschrieben worden. Die wirksamen Maßnahmen zur Reduzierung sind bereits vor Bekanntwerden der Angriffsmöglichkeiten vorbildlich angewendet worden. Die richtige Lösung kann nur sein, dass vertrauliche Daten bereits auf Applikationsebene, d. h. vor einer Übermittlung, verschlüsselt werden, so dass die Integrität und die Vertraulichkeit gewahrt bleiben. Diese Empfehlung wird auch ausgesprochen, wenn im Einsatzgebiet des Verfahrens kein sichereres Übertragungsnetz verfügbar ist. In diesen Fällen bietet der Hersteller einen VPN-Tunnel an, damit Angriffe auf das Netz oder Zugriffe durch den Netzbetreiber unterbunden werden. Hier besteht für den Nutzer das Restrisiko, dass der Hersteller selbst, bei der „Umschlüsselung“ (Übertragung) der Daten vom Mobilfunknetz auf das Internet Zugriff auf diese Daten hat.
Die Erweiterung des Produkts um die Komponenten web.direct und my-mdex erfolgte datenschutzkonform. Insbesondere sind beide Zugänge durch eine fünfminütige Sperrung nach fünf Fehlversuchen bei der Passworteingabe gegen massenhafte Log-In Versuche geschützt. Die Speicherung von Daten erfolgt nur aufgrund der ausdrücklichen Aktivität der Benutzer.
In rechtlicher Hinsicht hat es zwischenzeitlich eine Änderung der gesetzlichen Anforderungen gegeben, die für die vorliegende Rezertifizierung von Belang sind. Durch die Änderungen des § 11 BDSG, die mit Wirkung zum 01.09.2009 in Kraft getreten sind, ist das Verfahren hiervon betroffen. Die Gesetzesänderung sieht nun konkrete Inhalte für den schriftlichen Auftrag vor.

ic3s hat ihren Vertrag gemäß den Anforderungen ergänzt, so dass dieser den Anforderungen an eine Auftragsdatenverarbeitungsvereinbarung entspricht. Ein entsprechendes Muster des Vertrages wurde den Gutachtern zur Verfügung gestellt.

Die Daten werden im eigenen Rechenzentrum verarbeitet, für das ein entsprechendes Sicherheitskonzept vorliegt, das von der Bundesnetzagentur geprüft wurde, da der Anbieter Telekommunikationsdienstleister nach § 6 Abs. 4 TKG 2004 ist.

Das Verfahren „mdex fixed.IP“ der ic3s lässt sich nach wie vor als adäquat bewerten.

Zusammenfassung

Der Anbieter des Verfahrens hat auf die Veränderungen des Marktes (Einführung von neuen Übertragungsnetzen (LTE)), aber auch auf die Veränderung auf mögliche Angriffsszenarien reagiert und entsprechende Maßnahmen ergriffen. Die Qualität der Leistung ist durch eine permanente Qualitätskontrolle (sowohl intern, als auch durch die Kunden selbst) und entsprechende Maßnahmen, wie Schulungen und Weiterbildungen, aber auch technische Weiterentwicklungen gewährleistet.