Technisches und rechtliches Rezertifizierungs-Gutachten

Einhaltung datenschutzrechtlicher
Anforderungen durch das
Produkt „mdex fixed IP“/ „mdex fixed IP+”

der
mdex AG
Bäckerbarg 6
22889 Tangstedt

für das Gütesiegel für IT-Produkte (ULD)

erstellt von:

Andreas Bethke
Dipl.-Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Papenbergallee 34
25548 Kellinghusen

E-Mail: bethke@datenschutzguetesiegel.sh

Dr. Bettina Kähler
Rechtsanwältin
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IT-Produkte (rechtlich)

Hallerstraße 70
20146 Hamburg

E-Mail: bettina.kaehler@privcom.de

Stand:
Mai 2018

Inhaltsverzeichnis

A. Einleitung

Mit dem vorliegenden Gutachten beabsichtigt die mdex AG ihr Produkt „mdex fixed.IP“ für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) rezertifizieren zu lassen.

Die Vorlage eines rechtlichen und technischen Gutachtens ist Voraussetzung für die Rezertifizierung des Produktes. Dieses Dokument dient als Gutachten zur Vorlage beim ULD im Zusammenhang mit der Rezertifizierung des Produktes.

Dem Gutachten wird der Anforderungskatalog in der Version 2.0 zu Grunde gelegt.

Die mdex AG möchte mit diesem Gutachten den Nachweis führen, dass das Produkt nach wie vor die datenschutzrechtlichen Anforderungen erfüllt.

Das Produkt ist mittels folgender Prüfmethoden evaluiert worden:

- Inaugenscheinnahme und Überprüfung der technischen und organisatorischen Maßnahmen in den Rechenzentren Norderstedt (RZ der Stadtwerke, in der eine Colocation angemietet ist) und das eigene RZ in Tangstedt
- Überprüfung der aktuellen Dokumentation und Komponenten
- Überprüfung des Sicherheitskonzeptes nach TKG und der Risikoanalyse, die für die BNetzA erstellt werden müssen.
- Überprüfung des Managementportals

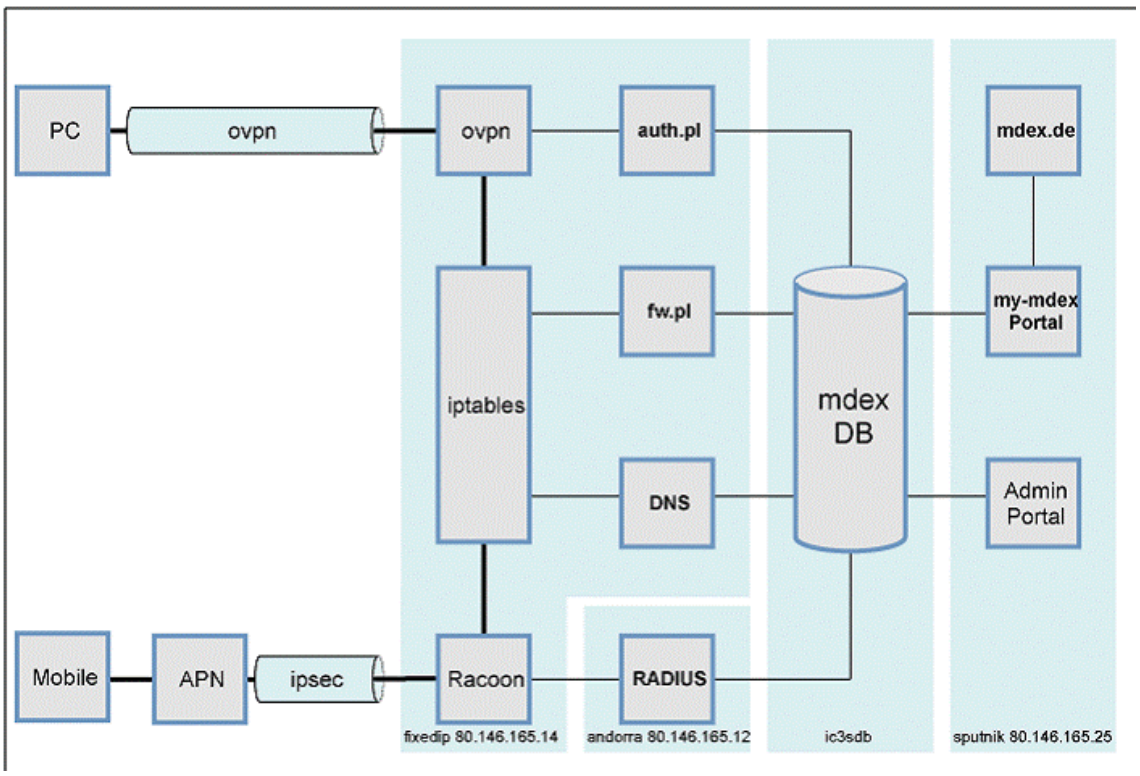
B. Zeitpunkt der Prüfung

Die Prüfung des Verfahrens fand von Mai 2017 bis April 2018 statt.

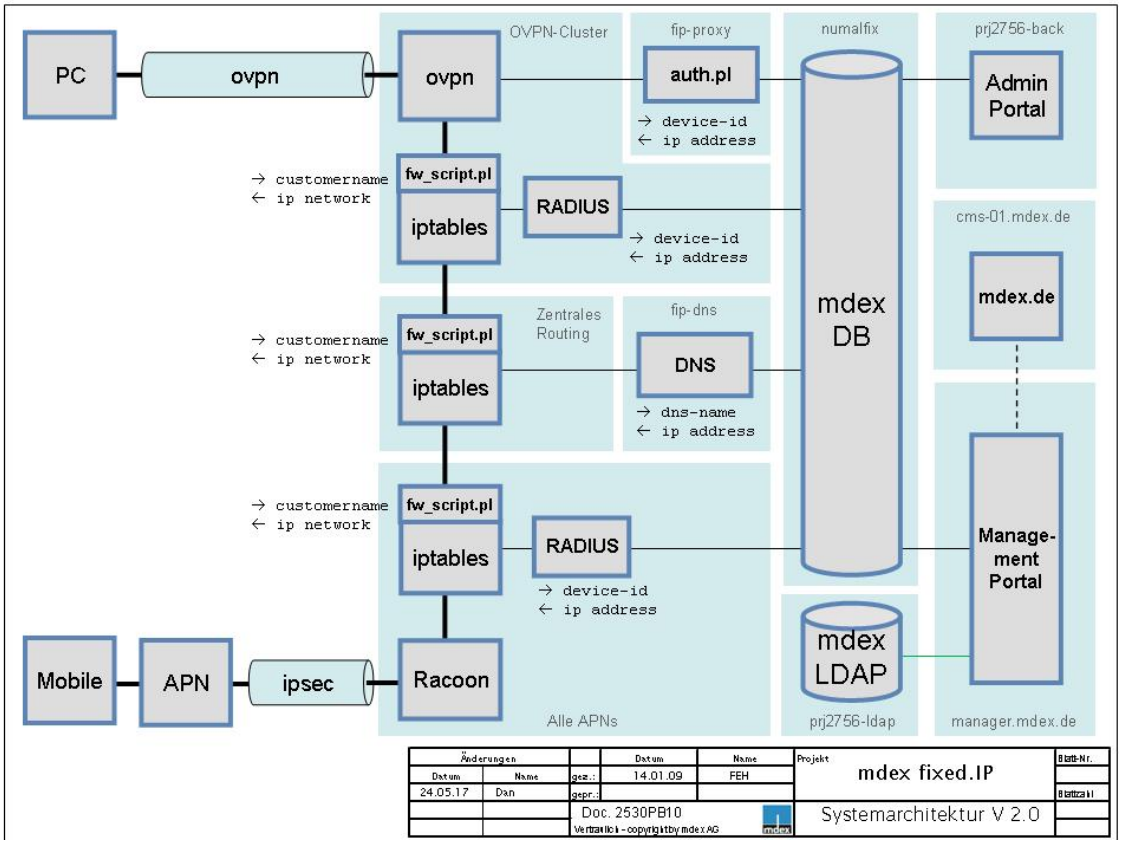
C. Änderungen und Neuerungen des Produktes

Das Verfahren „mdex fixed.IP“/ „mdex fixed.IP+“ ist weiterhin wie in den Gutachten von 2008, sowie den Rezertifizierungsgutachten von 2010, 2012 und 2015 beschrieben.

Die Übersicht der Komponenten sah im Ursprung wie folgt aus:



Gemäß aktuellem Stand sind die Komponenten nun wie folgt aufgebaut:



Die wesentliche Änderung besteht darin, dass die einzelnen Komponenten auf jeweils separate Systeme verteilt wurden und dass den Radius-Servern nun immer eine iptables-Firewall vorgeschaltet ist. Zudem ist das my-mdex-Portal nun in ein Managementportal umbenannt worden.

Seit kurzem steht ein neuer mdex OpenVPN-Server (openvpn20.mdex.de) für alle mdex OpenVPN-Zugänge zur Verfügung, der mindestens ein OpenVPN in der Version 2.3 erfordert.

Dabei wird eine verschlüsselte UDP-Verbindung von mdex empfohlen. Diese bietet als Cipher-Algorithmus entweder AES-256-GCM oder AES-256-CBC und als Authentifizierungsalgorithmus SHA256. Zusätzlich wird ein serverseitiges remote-cert-tls mindestens in der TLS-Version 1.2 eingesetzt.

Eine weitere Neuerung ist, dass mdex nach ISO 27001 zertifiziert ist.

Nach wie vor werden folgende Leistungen von mdex angeboten:

1. Basisleistung

   Bereitstellung einer festen, privaten IP-Adresse (RFC 1918), geeignet für die paketorientierte Datenübertragung über IPv4 (RFC 791), inklusive Zugriffsfunktion mdex web.direct. Bereitstellung eines Management Portals. Bereitstellung eines kundenindividuellen VPNs (geschlossene Benutzergruppe), mit denen die Kommunikation nur innerhalb des VPNs und über die web.direct-Funktionalität möglich ist. Zugriffsmöglichkeit auf weitere, am Router angeschlossene, Geräte über „IP-Portforwarding“.

2. Serviceleistungen

   Laufender 24/7/365-Betrieb und Kapazitätsanpassung der bereitgestellten Komponenten. Eine Verfügbarkeit des mdex-Dienstes: > 99 % p.a., sowie regelmäßige externe Security Audits.

3. mdex web.direct

Mit der Funktion mdex web.direct kann auf verschiedene Arten auf einen mdexfixed.IP+-Zugang
zugegriffen werden:

- Über das „my-mdex“ Management Portal: Durch einen Link aus dem „my-mdex“ Management Portal. Die Authentifizierung erfolgt hier durch die Anmeldung am „my-mdex“ Management Portal.
- Über den mdex Login-Link: Im „my-mdex“ Management Portal kann ein individuelles Passwort für jeden einzelnen mdex web.direct Login-Link gesetzt werden. Der Zugriff auf den mdexfixed.IP+ Zugang wird durch dieses Passwort geschützt. Der Login-Link kann auch ohne das „my-mdex“ Management Portal verwendet werden.
- Über den mdex Direkt-Link: Der Direkt-Link kann für jeden mdexfixed.IP+-Zugang individuell aktiviert/deaktiviert werden. In dem Direkt-Link ist ein „Hash-Wert“ enthalten, welcher mit Hilfe des Login-Link Passworts generiert wird und sich bei Änderung des Passworts ebenfalls ändert. Über den Direkt-Link kann ohne das „my-mdex“ Management Portal auf den mdexfixed.IP+-Zugang zugegriffen werden. Die Authentifizierung erfolgt über den „Hash-Wert“ in der URL. Der Zugriff ist über jeden beliebigen Port möglich. Als Übertragungsprotokoll steht ausschließlich HTTPS zur Verfügung

Für Übertragung von sensiblen Daten empfiehlt mdex nachdrücklich auf den Einsatz einer Ende-zu-Ende-Verschlüsselung.

D. Datenschutzrechtliche Bewertung

Zweck des Verfahrens ist die Ermöglichung einer IP-basierten bidirektionalen Kommunikation von Geräten über Mobilfunknetze.

Durch das aufgesetzte und zertifizierte Informationssicherheitsmanagment-System (nach DIN IEC ISO 27001) kann noch schneller und organisierter auf Lücken und Schwachstellen reagiert werden. So ist im Laufe der Begutachtung auf neue Angriffsvektoren auf das OpenVPN reagiert worden.

Die Umstrukturierung der Komponenten ist ebenfalls positiv zu bewerten, da sie zwar einen größeren Verwaltungsaufwand nach sich ziehen, aber durch eine mehrfache Anwendung von Firewall-Techniken die Sicherheit erhöhen.

Seit der letzten Rezertifizierung wurde der Anforderungskatalog des ULD Gütesiegels angepasst. Darum soll an dieser Stelle die neue tabellarische Darstellung erfolgen.

Anforderung nach Katalog oder sonstigen Rechtsnormen	**Bewertung**	**Kommentare**
Komplex 1:		
1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit	vorbildlich	Sofern vom Kunden eine Ende-zu-Ende-Verschlüsselung eingesetzt wird.
1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)	vorbildlich	
1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)	adäquat	
1.4 Datenschutz-Schutzziel: Intervenierbarkeit	vorbildlich	
1.5 Anpassung des IT-Produkts	adäquat	
1.6 Privacy by Default	adäquat	
1.7 Sonstige Anforderungen	entfällt	
Komplex 2:		
2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten	adäquat	
2.1.2 Einwilligung des Betroffenen	entfällt	
2.1.3.1 Vorschriften über die Datenerhebung	entfällt	
2.1.3.2 Vorschriften über die Übermittlung	adäquat	
2.1.3.3 Löschung nach Wegfall des Erfordernisses	entfällt	
2.2.1 Zweckbindung und Zweckänderung	adäquat	
2.2.2 Erleichterung der Umsetzung des Trennungsgebotes	adäquat	
2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG)	vorbildlich	
2.3 Datenverarbeitung im Auftrag	adäquat	
2.4.1 gemeinsame Verfahren/Abrufverfahren	entfällt	-
2.4.2 Trennung der Verantwortlichkeiten	adäquat	-
2.4.3 Veröffentlichungen im Internet	entfällt	
2.4.4 Weitere besondere technische Verfahren	entfällt	
2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	adäquat	
Komplex 3:		
3.1.1. Physikalische Sicherung	Entfällt bzw. adäquat	Eine Speicherung der Daten von den Endgeräten ist nicht vorgesehen. Alle anderen Daten werden adäquat gesichert.

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
3.1.2 Authentisierung	adäquat	
3.1.3 Autorisierung	adäquat	
3.1.4 Protokollierung	entfällt	
3.1.5 Verschlüsselung und Signatur	adäquat	
3.1.6 Pseudonymisieren	entfällt	
3.1.7 Anonymisieren	entfällt	
3.2.1.1 Verfügbarkeit	vorbildlich	
3.2.1.2 Integrität	vorbildlich	
3.2.1.3 Vertraulichkeit	vorbildlich	
3.2.1.4 Nicht-Verkettbarkeit	vorbildlich	
3.2.1.5 Transparenz	adäquat	
3.2.1.6 Intervenierbarkeit	vorbildlich	
3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	entfällt	
3.2.1.8 Test und Freigabe	adäquat	
3.2.2 Erleichterung der Vorabkontrolle	adäquat	
3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses	adäquat	
3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	adäquat	
3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten	adäquat	
3.3.1 Verschlüsselung	vorbildlich	
3.3.2 Anonymisierung oder Pseudonymisierung	entfällt	
3.3.3.1 Mobile Datenverarbeitungssysteme	entfällt	
3.3.3.1 Video-Überwachung und –Aufzeichnung	entfällt	
3.3.3.1 Automatisierte Einzelentscheidungen	entfällt	
3.3.3.1 Veröffentlichungen im Internet	entfällt	
3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren	adäquat	
3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung	adäquat	
3.6 Sonstige Anforderungen	entfällt	
Komplex 4:		
4.1 Aufklärung und Benachrichtigung	adäquat	
4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten	adäquat	
4.3 Auskunft	adäquat	
4.4.1 Berichtigung	adäquat	
4.4.2 Vollständige Löschung	adäquat	
4.4.3 Sperrung	adäquat	
4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	adäquat	
4.3.5 Gegendarstellung	adäquat	
4.5 Sonstige Anforderungen	entfällt	

E. Zusammenfassung/Ergebnis

Der eingesetzten Technologie kann nach wie vor eine adäquate datenschutzrechtliche Umsetzung bescheinigt werden.

Der Anbieter des Verfahrens reagiert auf Veränderungen von Technologien für mögliche Angriffsszenarien und ergreift entsprechende Maßnahmen. Hierbei kommen regelmäßig sog. externe Penetrationstests zum Einsatz, die von spezialisierten Firmen

durchgeführt werden. Durch die Etablierung eines ISMS nach ISO 27001 ist der kontinuierliche Verbesserungsprozess gefestigt worden, der sowohl technische Maßnahmen und Weiterentwicklungen, als auch Schulungen und Weiterbildungen gewährleistet.

Das Produkt „mdex fixed.IP+“ der mdex AG lässt sich daher nach wie vor als adäquat bewerten.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den 14.05.2018

Andreas Bethke
Dipl.-Inf. (FH)

Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Hamburg, den 14.05.2018

Dr. Bettina Kähler
Rechtsanwältin

Beim Unabhängigen Landeszentrum für für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IT-Produkte (rechtlich)