datenschutz cert

Kurzgutachten zur Re-Zertifizierung der Dataport Firewall Altenholz

im Auftrag von Dataport

datenschutz cert GmbH

Januar 2014

datenschutz cert

Inhaltsverzeichnis

Kurzgutachten zur Re-Zertifizierung der Dataport Firewall Altenholz

1. Gegenstand der Prüfung

Mit der im folgenden Kurzgutachten dokumentierten Auditierung strebt die Anstalt des öffentlichen Rechts Dataport (nachfolgend: Dataport) die Re-Zertifizierung des IT-Produkts „Dataport Firewall Altenholz“ mit Funktionsstand Oktober 2013 an. Das IT-Produkt wurde erstmals am 25.11.2003 erfolgreich gemäß der Datenschutzauditverordnung (DSAVO)[1] durch das vom Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) zertifiziert und seit dem regelmäßig re-zertifiziert, zuletzt im Jahre 2011.

Grundlage der Auditierung mit dem Ziel der Re-Zertifizierung ist der Anforderungskatalog des ULD in der Version 1.2.

Die Dataport hat am 22.05.213 eine Selbsterklärung [dataport_Selbsterkl] abgegeben, in der vermerkt wird, dass die Firewall am Standort Altenholz mit folgenden Änderungen betrieben wird:

--- Ersatz von „frox“ durch „ftp-proxy“.

Die Selbsterklärung wird diesem Gutachten als **Anlage 1** beigefügt. Eine aktuelle Dokumentation zum IT-Produkt hat der Hersteller den Auditoren in Form eines DokuWiki auf einem verschlüsselten USB-Stick bereitgestellt. Die Prüfung erfolgte anhand einer Dokumentenprüfung und der Durchführung von Plausibilitätstests.

Aufgrund der Tatsache, dass das IT-Produkt re-zertifiziert werden soll, wird im Folgenden zu den Fragen Stellung genommen,

--- inwieweit das geringfügig veränderte IT-Produkt weiterhin dem Stand der Technik entspricht,

--- inwieweit die Einsatzumgebung noch auf einem aktuellen Sicherheits-Stand ist,

--- inwieweit die an das IT-Produkt zu stellenden rechtlichen Anforderungen unverändert geblieben sind.

2. Zeitpunkt der Prüfung

Die Auditierung des IT-Produktes wurde im Zeitraum vom 15.04.2013 bis zum 29.10.2013 durchgeführt.

Am 10.01.2014 wurden im Rahmen des Zertifizierungsverfahrens die Anforderungen an eine Grafik zu den Löschfristen in diesem Bericht ergänzt.

3. Antragstellerin

Antragstellerin dieses Gutachtens ist die Anstalt des öffentlichen Rechts Dataport, Altenholzer Straße 10-14, 24161 Altenholz. Ansprechpartner ist Herr Frank Pliquett.

---

[1] Landesverordnung über ein Datenschutzaudit (Datenschutzauditverordnung - DSAVO) v. 18.11.2009, *GVOBl.* Schl.-H. *2008, S. 562ff. / GVOBl.* Schl.-H. *2009, S. 742ff.* Die Auditierung wurde auf Grundlage dieser Gesetzesfassung durchgeführt und im Oktober 2013 abgeschlossen. Die zum 01.01.2014 eingetretenen Änderungen der DSAVO wurden daher noch nicht berücksichtigt.

4. Sachverständige Prüfstelle

Sachverständige Prüfstelle ist die datenschutz cert GmbH, Konsul-Smidt-Str. 88a, 28217 Bremen. Ansprechpartner und Auditleiter sind Frau Dr. Irene Karper (Recht) und Herr Thorsten Kamp (Technik).

5. Geringfügig veränderte Produktkomponente

Das Produkt „Dataport Firewall Altenholz“ besteht aus mehreren Komponenten: Externen Router/Paketfiltern, internen Router/Paketfiltern sowie Bastion Hosts als Proxies (Ersatzdienste). Diese Produktkomponenten können von den Kunden der Dataport zum Schutz ihrer eigenen Ressourcen im Netzwerk von Dataport gegen unberechtigte Zugriffe aus dem Internet in Anspruch genommen werden. Die Firewall kommt hierbei als untrennbarer aber unselbstständiger Bestandteil der Internet-Verbindungsvermittlung durch den Kunden zum Einsatz und wird durch Inanspruchnahme der Internet-Verbindungsvermittlung durch den Kunden und dessen Klientel indirekt genutzt.

Neben den generischen, protokoll-spezifischen Proxies (z.B. HTTP) werden auch spezielle Anwendungs-Proxies (z.B. EGB-Proxy) eingesetzt. Diese (Reverse-)Proxies sowie der Mailscanner sind Teil der jeweiligen Fachanwendung und daher, wie auch bei der Erst-Zertifizierung und den bisherigen Rezertifizierungen, nicht Gegenstand dieser Auditierung und Rezertifizierung.

Weiterhin gehören die internen und externen Paketfilter zum Produkt. Diese Regeln den Zugriff auf die Proxy-Systeme und fungieren als Loadbalancer.

Die Struktur der Dataport Firewall Altenholz wird auf der folgenden Seite im Überblick dargestellt.

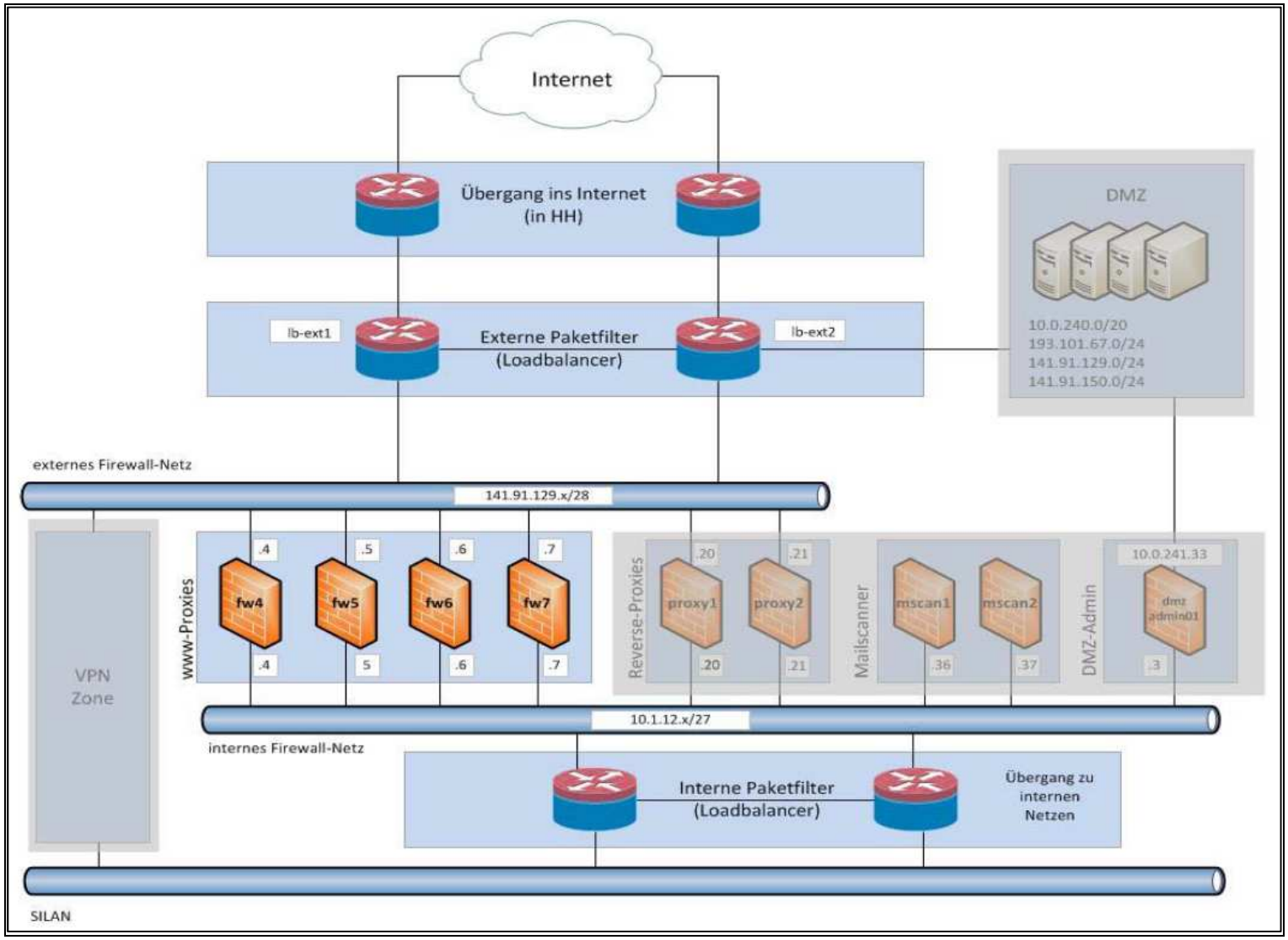


Abb. 1: Übersicht Struktur Dataport Firewall Altenholz

Der Aufbau des IT-Produktes hat sich gegenüber der letzten Rezertifizierung [GRZDF11] nur unwesentlich geändert. Insbesondere haben sich der Einsatzzweck und der Datenfluss innerhalb des Produktes sowie die Protokollierung und Verarbeitung der Protokolldaten nicht geändert. Die Dataport Firewall Altenholz wird auch noch immer am selben Rechenzentrumsstandort räumlich bereitgestellt.

Die relevanten Änderungen sind in Anlage 1 dargestellt und betreffen lediglich den Wechsel des ftp-Proxies von frox auf ftp-proxy.

Die IP-Adresse eines Kunden wird automatisch durch ein Script um ein Oktett gekürzt und dadurch verfremdet. Aus den squid-Logdateien werden alle aufrufenden IP-Adressen extrahiert und so der Traffic des Tages aufsummiert. Ein Skript löscht jede Nacht diese Summendaten, wenn die IP-Adresse in ein Netz fällt, das folgende Bedingungen erfüllt:

--- Das Netz gehört einem Kunden, der den Pauschaltarif „Land“ besitzt (und keine Einzelauflistung wünscht)

--- Das Netz gehört einem Kunden, der das ABS-Angebot nutzt (Citrix-Farm, Traffic pauschal, keine Einzelauflistung möglich)

--- Das Netz gehört einem Kunden, der mit der Kunden-ID „0“ geführt wird und keinen Surftarif besitzt (Dataport-Netze und Sonderregelungen).

Hingegen werden die verfremdete IP-Adresse und die dazugehörigen Trafficdaten für 10 Tage aufbewahrt und anschließend automatisch gelöscht, sofern diese Daten für den Tarif bzw. Vertrag abrechnungsrelevant sind. Hier wird die Abrechnung über die Volumengebühr bzw. zusätzlichen Freischaltungen für Clients u.Ä. am Monatsende an den jeweiligen Kunden geschickt. Diese etwas längere Aufbewahrung der IP-Adressdaten / Trafficdaten ist hier zu Abrechnungszwecken erforderlich.

6. Bewertung anhand der technischen Anforderungen

6.1 Wechsel des ftp-Proxies von frox auf ftp-proxy

Das Debian-Projekt teilt hierzu Folgendes mit: „*FTP-Proxy is a transparent, application-level proxy server for FTP connections, designed to protect FTP servers against attacks based on the FTP protocol. It is the first (and currently only) component of the SuSE Proxy Suite, a set of programs to enhance firewall security.*

FTP-Proxy is much less complex than any current FTP server, has been designed with great care and performs chroot(), setuid(), setgid() to avoid possible vulnerabilities, and is believed to be immune against current known attacks.“[2]

Das Programm ftp-proxy ist sowohl im aktuellen Ubuntu-Stable-Release wheezy, als auch in der Testversion jessie und dem unstable sid enthalten. Es wird daher aktuell und in Zukunft vom Debian-Security-Team gepflegt. Sicherheitslücken sind in den letzten Jahren nicht bekannt geworden. Die Debian-Distribution ist als sicher bekannt; die Gutachter haben daher keinen Zweifel an der Sicherheit des Programms ftp-proxy.

[2] Online abrufbar unter http://packages.debian.org/de/wheezy/ftp-proxy (Stand: 10/2013).

6.2 Einsatzumgebung

Für den sicheren Betrieb des Produktes ist eine sichere Einsatzumgebung, z.B. in Form einer sicheren Infrastruktur, notwendig. Diese wurde im Rahmen einer anderweitigen Auditierung des Rechenzentrums von Dataport am Standort Altenholz auf der Basis des IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bereits festgestellt.[3]. Daher wird auch im Rahmen dieser Prüfung eine sichere Einsatzumgebung als gegeben vorausgesetzt.

7. Bewertung anhand der rechtlichen Anforderungen

Bei der Auditierung wurden folgende Rechtsnormen als Bewertungsmaßstab hinzugezogen:

--- Landesdatenschutzgesetz Schleswig-Holstein

--- Telemediengesetz

--- Telekommunikationsgesetz.

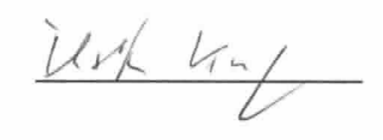
Die genannten Gesetze haben seit der letzten Re-Zertifizierung keine für das IT-Produkt relevanten Veränderungen erfahren.

Die oben genannten Änderungen wirken sich zudem nicht auf bereits zuvor getroffene rechtliche Ergebnisse aus. Insgesamt ergeben sich demnach keine Veränderungen im Hinblick auf die rechtlich einschlägigen Rahmenbedingungen und kein Bedarf an einer Änderung des seinerzeit zugrunde gelegten Anforderungsprofils.

8. Zusammenfassung der Auditergebnisse

Das IT-Produkt Dataport Firewall Altenholz erfüllt weiterhin die Anforderungen an den Datenschutz und die Datensicherheit in besonderer Weise, da die verwendeten technischen Lösungen innovativ die Umsetzung der gesetzlichen Vorgaben ermöglichen. Gegen eine Re-Zertifizierung bestehen keine Bedenken.

Bremen, den 13.01.2014



Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Thorsten Kamp
datenschutz cert GmbH

[3] Dieses und andere Zertifizierungen sind abrufbar unter http://www.dataport.de/ueber-uns/zahlenfakten/Seiten/auszeichnungen.aspx (Stand: 10/2013).

9. Dokumente

[GRZDF11] datenschutz cert GmbH, „Gutachten zur Rezertifizierung der Firewall der Dataport am Standort Altenholz“. März 2011

[dataport_Selbsterkl] Dataport, „Herstellererklärung Dataport Firewall Altenholz“, vom 22.05.2013

datenschutz cert

Anlage 1

Dataport · Altenholzer Straße 10 - 14 · 24161 Altenholz

datenschutz cert GmbH
Herrn Kamp
Konsul-Smid-Str. 88a
28217 Bremen

Altenholzer Straße 10 - 14
24161 Altenholz
Kontakt: Rolf Niedziella
Telefon: 0431 3295-6230
Telefax:
rolf.niedziella@dataport.de

Altenholz, 22. Mai 2013

Herstellererklärung Dataport Firewall Altenholz

Sehr geehrter Herr von Rahden,

hiermit bestätigen wir folgende wesentliche Veränderung an den Firewall-Systemen, die nach der letzten Rezertifizierung durchgeführt wurde:

- Ersatz von „frox" durch „ftp-proxy"

Wir bestätigen hiermit, dass diese Übersicht vollständig und korrekt ist.

Mit freundlichen Grüßen
Rolf Niedziella

Rolf Niedziella
TI35