Dataport
Dezember 2008

# Kurzfassung der Begutachtung zur Rezertifizierung der Firewall Dataport am Standort Altenholz

## 1. Zeitpunkt der Prüfung

Die Begutachtung zur Rezertifizierung der Firewall erstreckte sich auf den Zeitraum von September bis Dezember 2008.

## 2. Adresse des Antragstellers/der Antragstellerin

Antragstellerin dieses Gutachtens ist Dataport als Rechtsnachfolgerin der Datenzentrale Schleswig-Holstein. Der Unternehmenssitz bleibt unverändert in der Altenholzer Straße 10-14, 24161 Altenholz. Ansprechpartner sind Frau Haase und Herr Knutzen.

## 3. Adressen des/der Sachverständigen

Prüfstelle für dieses Gutachtens ist die datenschutz nord GmbH, Barkhausenstr. 2, 27568 Bremerhaven. Ansprechpartner sind Herr Dr. Uwe Schläger (Recht) und Herr Thorsten Kamp (Technik).

## 4. Kurzbezeichnung des IT-Produktes

Firewall Dataport Altenholz

## 5. Detaillierte Bezeichnung des IT-Produktes

Das Produkt „Firewall Dataport Altenholz“ besteht aus mehreren Komponenten: Externen Paketfiltern, internen Paketfiltern sowie 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-Verbindungs-vermittlung durch den Kunden zum Einsatz und wird durch in Anspruchnahme der Internet-Verbindungsvermittlung durch den Kunden und dessen Klientel indirekt genutzt.

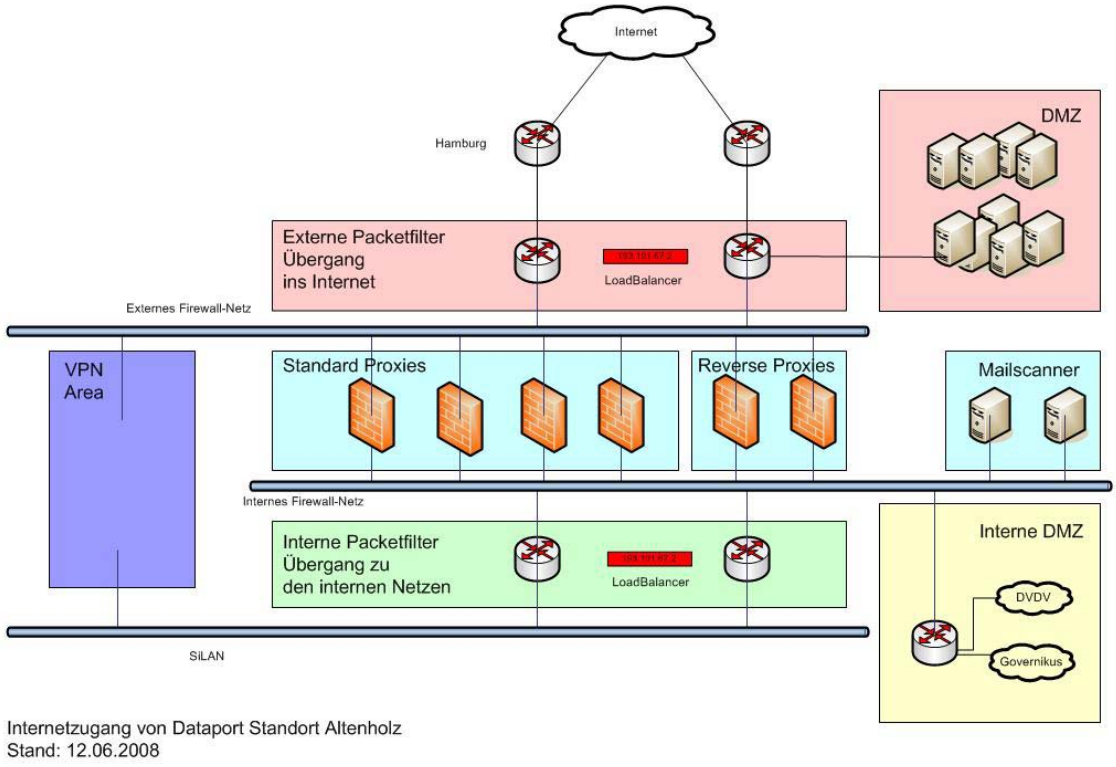


**Abbildung 1 Struktur der Firewall**

Die eingesetzten Proxies werden in Standard Proxies und Reverse Proxies unterschieden. Die Standard Proxies dienen der Absicherung des Zugriffs auf das Internet bzw. auf Systeme außerhalb des Dataport-Netzes. Die Reverse Proxies sichern den Zugriff von außerhalb auf Systeme im Netz von Dataport ab. Zu den eingesetzten Proxies gehören:

--- http-Proxy
--- FTP-Proxy
--- SMTP-Proxy
--- NNTP-Proxy
--- Aureg-Proxy[1]
--- Wahlschein-Proxy
--- OK-EFA Proxy
--- Autobahn Video Proxy
--- EGB-Proxy
--- GIS-Proxy

[1] Die folgenden, anwendungsspezifischen Proxies sind nicht Gegenstand der Begutachtung (s. Abschnitt 7)

--- Verkehrs-Proxy
--- Ziaf-Proxy
--- Probaug-Proxy
--- Wunschkennzeichen Proxy
--- WiskiWeb Proxy
--- OSCI-Proxy
--- Ausgewählte SSH-Verbindungen über einen generischen Proxy

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

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

Für den sicheren Betrieb des Produktes ist eine sichere Einsatzumgebung notwendig. Diese wurde im Rahmen einer Auditierung gemäß IT-Grundschutz nach ISO 27001 überprüft. Daher wird im Rahmen dieser Rezertifizierung eine sichere Einsatzumgebung, z.B. in Form von einer sicheren Infrastruktur, vorausgesetzt.

## 6. Zweck und Einsatzbereich

Die Komponenten der Firewall Dataport Altenholz können von den Kunden Dataports zum Schutz ihrer eigenen Ressourcen im Netzwerk Dataports gegen unberechtigte Zugriffe aus dem Internet in Anspruch genommen werden.

Der rechtliche Rahmen zur Auditierung des Produkts besteht aus der Datenschutzauditverordnung Schleswig-Holstein (DSAVO), dem Telemediengesetz (TMG) und dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG-SH) zusammen.

## 7. Zusammenfassung der Prüfergebnisse

Trotz einiger kleiner Erweiterungen des Produkts ist der Stand des Produkts gegenüber dem 2006 zertifizierten Zustand aus Sicht der Auditanforderungen unverändert. Dies liegt darin begründet, dass lediglich einzelne Systemkomponenten durch äquivalente, dem Stand der Technik angemessene Komponenten ersetzt worden sind.

Das Produkt „Firewall Dataport Altenholz“ schützt Ressourcen im Netzwerk von Dataport gegen unberechtigte Zugriffe aus dem Internet durch Einschränken der Verbindungen vom und zum Internet auf zulässige Dienste. Es besteht aus einem externen Paketfilter, einem internen Paketfilter sowie Proxies (Ersatzdienste) für Dienste auf Basis der Protokolle HTTP, SMTP, FTP und NNTP. Neben der Auswahl geeigneter Produkte (Postfix, frox) werden zur Zugriffssicherung sowohl technische (z.B. Software-Zertifikat, Ausweiskarten zur Zugangskontrolle) als auch organisatorische Maßnahmen (z.B. Sicherheitsdienst) eingesetzt.

Der rechtliche Rahmen zur Begutachtung besteht aus der Datenschutzauditverordnung Schleswig-Holstein (DSAVO), dem Telemediengesetz (TMG) und dem Landesdatenschutzgesetz Schleswig-Holstein (LDSGSH).

Bereichspezifische Regelungen finden keine Anwendung, da das Produkt ausschließlich anwendungsunabhängige Protokollinformationen verarbeitet. Die Verarbeitung der IP-Pakete und die Protokollierung der Verbindungen erfolgen zur Gewährleistung des ordnungsgemäßen Betriebs der Firewall und zur volumenbezogenen Abrechnung mit dem Kunden und sind zulässig. Die Art und Weise des Betriebs – insbesondere die vorbildliche Sicherheit der Einsatzumgebung – sowie die Konfiguration des Produkts gewährleisten in vollem Umfang eine auf notwendige Daten beschränkte Verarbeitung der IP-Pakete (Primärdaten) und Protokolldaten (Sekundärdaten) bei adäquater Transparenz.

## 7.1 Bewertung datenschutzfördernder Merkmale

Das Produkt „Firewall Dataport Altenholz“ zeichnet sich datenschutzrechtlich in folgender Weise aus:

--- Durch vorrangige Verwendung quelloffener Software wird ein hohes Maß an Produkttransparenz geschaffen.

--- Bereits bei der technischen Gestaltung des Produktes und der Einsatzumgebung werden sicherheitstechnische Aspekte mit einbezogen, dies zeigt sich am erhöhten Aufwand durch den Einsatz eines modifizierten FTP-Proxy zur Unterstützung des passiven Modus und die Nutzung von TCP-Wrapper zur besseren Verbindungskontrolle einiger Proxies.

--- Proprietäre Verfahren werden aus dem Internet in das interne Netz nicht getunnelt, sondern durch Eigenentwicklungen auf der Basis bewährter Produktteile geschützt.

--- Der betriebliche Datenschutzbeauftragte wird auf konzeptioneller Ebene in Planung und Betrieb der Firewall miteinbezogen und überprüft stichprobenartig die Protokolldateien der Firewall.