Kurzfassung der Begutachtung zur Rezertifizierung der Firewall Dataport am Standort Altenholz

datenschutz nord GmbH, August 2006

1. Zeitpunkt der Prüfung

Die Begutachtung zur Rezertifizierung der Firewall erstreckte sich auf den Zeitraum von Dezember 2005 bis April 2006.

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 ist Herr Wolfgang Zachert.

3. Adressen des/der Sachverständigen

Sachverständige dieses Gutachtens ist die datenschutz nord GmbH, Barkhausenstr. 2, 27568 Bremerhaven. Ansprechpartner ist Herr Dr. Uwe Schläger; daneben haben Herr Günther Diederich und Frau Irene Karper an der Erstellung des Gutachtens mitgewirkt.

4. Kurzbezeichnung des IT-Produktes

Firewall Dataport Altenholz

5. Detaillierte Bezeichnung des IT-Produktes

Das Produkt „Firewall Dataport“ besteht aus mehreren Komponenten: Externen Paketfiltern, internen Paketfiltern sowie Proxies (Ersatzdienste) für Dienste auf Basis der Protokolle SMTP, HTTP, FTP, NNTP und Telnet (siehe Abbildung 1).

Für verschiedene Verfahren werden jeweils anwendungsspezifische Proxies eingesetzt. Die hierbei eingesetzte Technik ist identisch mit einem der folgenden Proxytypen:

- OPAL-SH (HTTP-basierter Proxy)
- OK.EWO (XML-basierter Proxy)
- SAP-ITS (Proxy auf der Basis SAP/HTTP).

Die anwendungsspezifischen Proxies werden für identische Systeme in gleicher Konfiguration eingesetzt. Die Proxies kommen im Netzwerk der Dataport nicht generell zum Einsatz, sondern ausschließlich im Zusammenhang mit speziellen Informationssystemen. Dementsprechend sind die Proxies Bestandteil der jeweiligen Informationssysteme. Diese Informationssysteme und damit auch ihre speziellen Proxies sind folglich nicht Gegenstand des Gutachtens. Zusätzlich werden zur Kontrolle von Zugriffen aus dem internen Netz auf Rechner außerhalb der Dataport SSH-Gateways oder im Rahmen des GBV (Gemeinsamer Bibliotheksverbund) weitere anwendungsspezifische Proxies eingesetzt. Diese werden im direkten Umfeld des Produktes betrieben und teilen sich Ressourcen mit der anwendungsunabhängigen Firewall. Dementsprechend werden diese Proxies im Rahmen der Einsatzumgebung berücksichtigt.

Die Produktkomponenten (Paketfilter und Proxies) schützen das Netz Dataports durch Einschränken der Verbindungen vom und zum Internet auf zulässige Dienste anhand von Kommunikationsbedingungen wie z.B. die Einschränkung auf bestimmte IP-Adressen für Zielrechner einer Verbindung, die Zugehörigkeit eines IP-Paketes zu einer bestehenden Verbindung oder dem protokollkonformen Aufbau eines IP-Paketes. Dabei werden Nutzungsdaten zu Abrechnungszwecken und zur Analyse von fehlerhaften oder unzulässigen Verbindungen in einer Gesamtprotokolldatei gespeichert. Aus der Gesamtprotokolldatei werden binnen 24 Stunden Teildatensätze zur Abrechnung durch die Rechnungsabteilung und zur Analyse nicht regulärer Zugriffe erstellt. Ebenfalls binnen 24 Stunden wird aus der Gesamtprotokolldatei eine anonymisierte Fassung für statistische Zwecke erstellt, indem das letzte Oktett der IP-Adresse gelöscht wird. Die Analyse und Erstellung von Statistiken erfolgt durch die Firewalladministration. Die Nutzungsdaten zu Abrechnungszwecken werden in einem, von der Firewall getrennten Verfahren, der Rechnungsstelle Dataports zur Verfügung gestellt. Jede Analyse der Protokolldaten, die nicht zu diesen genannten Zwecken erfolgt, sondern aufgrund spezieller Anforderungen (z.B. zu Zwecken der Strafverfolgung) erforderlich wird, erfolgt im Rahmen einer eigenständigen Auftragsdatenverarbeitung. Bei der Vertragsgestaltung wird der Datenschutzbeauftragte Dataports zur Beurteilung der datenschutzrechtlichen Grundlagen hinzugezogen. Die eigenständige Auftragsdatenverarbeitung ist nicht Bestandteil des Produktes und damit auch nicht Bestandteil des Gutachtens. Diese Einschränkungen und die protokollierten Informationen sind im Sicherheitskonzept der Firewall der Dataports festgelegt. Die technische Umsetzung des Sicherheitskonzeptes wird durch ein Betriebskonzept beschrieben. Da für alle Produktkomponenten im Sicherheitskonzept die gleichen technisch-organisatorischen Maßnahmen festgelegt wurden, werden diese in einem eigenen Abschnitt aufgeführt.

6. Tools, die zur Herstellung des IT-Produktes verwendet wurden

TIS Firewall Toolkit mit den Bestandteilen:

- nntp-gw V0.2 für NTTP
- tn-gw V2.1 für Telnet
- ftp-gw V1.3 für FTP

7. 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 Landesdatenschutzgesetz Schleswig-Holstein (LDSG-SH) sowie dem Teledienstegesetz (TDG), dem Mediendienste-Staatsvertrag (MDStV) und Teledienstedatenschutzgesetz (TDDSG).

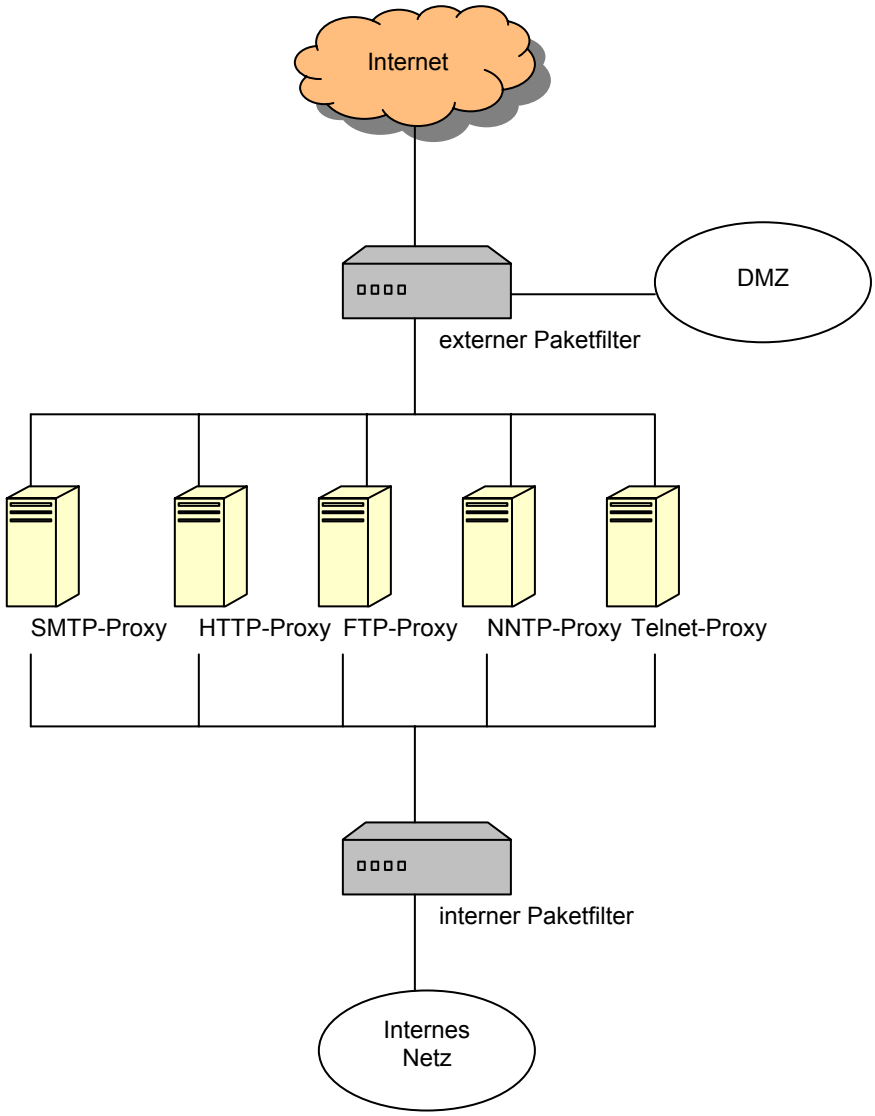

Abbildung 1: Firewalltopologie der Datenzentrale Schleswig-Holstein

8. Modellierung des Datenflusses

Das Produkt zielt auf die Analyse von IP-Paketen ab. Im Rahmen dieser Analyse werden zur Fehleranalyse und zu Abrechungszwecken Protokolle erstellt. Insgesamt lassen sich somit folgende Datenarten identifizieren:

Datenart A: IP-Pakete einschließlich der Inhaltsdaten

Datenart B: Protokolldaten

9. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Version 1.2

10. Zusammenfassung der Prüfungsergebnisse

Das Produkt „Firewall Dataport am Standort Altenholz“ schützt Ressourcen im Netzwerk Dataports 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, Telnet und NNTP.

Die Produktkomponenten werden auch zum Schutz anderer Verfahren eingesetzt. Ferner teilen sie sich einige Ressourcen mit anderen Anwendungen. Für einen sicheren Einsatz des Produktes ist dementsprechend auch eine sichere Einsatzumgebung wichtig. Hierzu gehören die Sicherheit der gemeinsam mit anderen Proxies und Diensten (z.B. der Proxytypen OPAL-SH, OK.EWO und SAP-ITS) genutzten Hardware (externer Router, Bastion-Host). Neben der Auswahl geeigneter Produkte (Postfix, FWTK) werden zur Zugriffssicherung sowohl technische (z.B. Software-Zertifikat, Ausweiskarten zur Zugangskontrolle) als auch organisatorische Maßnahmen (z.B. Sicherheitsdienst) eingesetzt.

Die Verarbeitung der IP-Pakete und die Protokollierung der Verbindungen erfolgt zur Gewährleistung des ordnungsgemäßen Betriebs der Firewall und zur volumenbezogenen Abrechnung mit dem Kunden und ist zulässig. Die Art und Weise des Betriebs – insbesondere die vorbildliche Sicherheit der Einsatzumgebung – sowie die Konfiguration des Produkts gewährleisten bei adäquater Transparenz in vollem Umfang eine auf notwendige Daten beschränkte Verarbeitung der IP-Pakete (Primärdaten) und Protokolldaten (Sekundärdaten).

Nr.	**Anforderungsprofil**	**Bewertung / Kommentar**
Datenart A: IP-Header		
A1	Aussagefähige Produktunterlagen	adäquat verständlich und aussagekräftig
A2	Zulässigkeit der Verarbeitung von IP-Paketen	zulässig
A3	Zugriffskontrolle auf die Produktkomponenten	in vollem Umfang gesichert
A4	Verfügbarkeit der Produktkomponenten	in vorbildlicher Weise
Datenart B: Protokolldaten		
B1	Aussagefähige Produktunterlagen	adäquat verständlich und aussagekräftig
B2	Zulässigkeit der Protokollierung	zulässig
B3	Vertraulichkeit der Protokolldaten	in vollem Umfang gegeben
B4	Integrität der Protokolldaten	in adäquater Weise gewährleistet
B5	Verfügbarkeit der Protokolldaten	in vorbildlicher Weise gegeben

11. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Die Produkttransparenz wird durch den Einsatz von Open Source Software gefördert. Ferner werden bereits bei der technischen Gestaltung des Produktes und der Einsatzumgebung 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. Der betriebliche Datenschutzbeauftragte wird auf konzeptioneller Ebene in Planung und Betrieb der Firewall miteinbezogen und überprüft stichprobenartig die Protokolldateien der Firewall. Das Produkt „Firewall Dataport am Standort Altenholz“ zeichnet sich datenschutzrechtlich dadurch aus, dass zum Produkt ein Benutzerhandbuch gehört, in dem für die gängigsten Anwendungen (z.B. Browser) die notwendigen Konfigurationen (z.B. Proxyeinstellungen) beschrieben sind. Dadurch wird eine sicherheitstechnisch geeignete Konfiguration der Anwendung erleichtert. Das Produkt zeichnet sich zudem insbesondere durch eine schnelle Anonymisierung und rechtzeitige Löschung der Protokolldaten aus.

Hiermit wird bestätigt, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht. Die ausführliche Analyse liegt bei.

Ort, Datum Unterschrift des Sachverständigen