datenschutz cert

Dataport
Mai 2011

Kurzfassung der Begutachtung zur Rezertifizierung der Firewall Dataport am Standort Altenholz

1. Zeitpunkt der Prüfung

Die Auditierung des IT- Produktes wurde im Zeitraum vom 11.02.2011 bis zum 31.03.2011 durchgeführt.

2. Adresse des Antragstellers/der Antragstellerin

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

3. Adressen des/der Sachverständigen

Sachverständige Prüfstelle ist die datenschutz cert GmbH, Konsul-Smidt-Str. 88a, 28217 Bremen. Ansprechpartner und Auditleiter sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik). Das Audit wurde mit der Hilfe von Herrn Thorsten Kamp von der Prüfstelle datenschutz nord GmbH durchgeführt.

4. Kurzbezeichnung des IT-Produktes

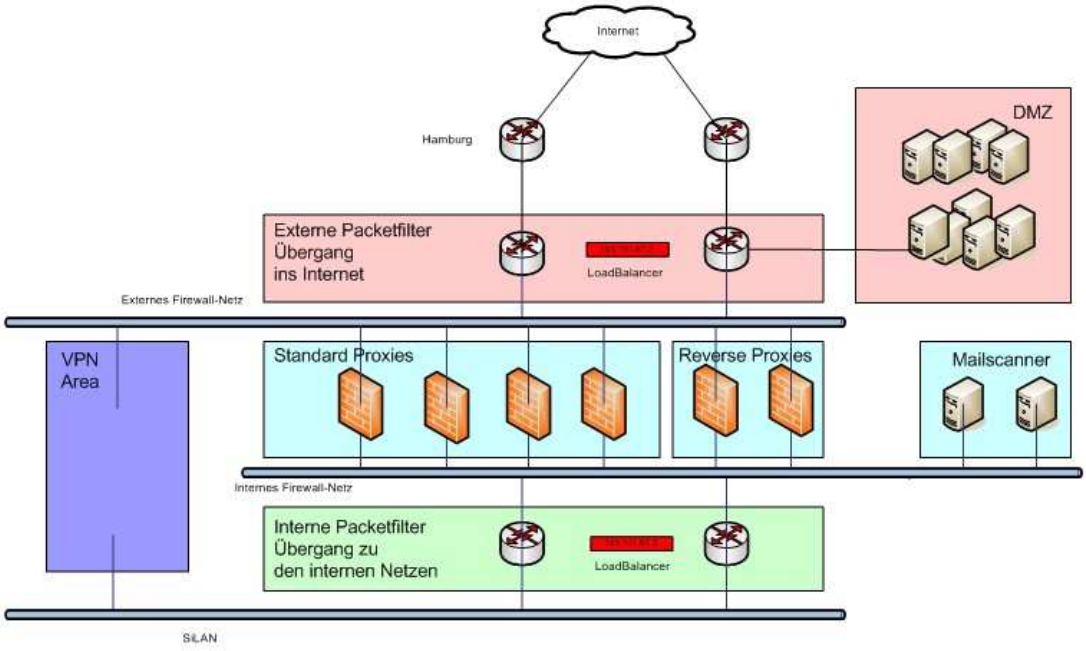
Firewall Dataport Altenholz

5. Geringfügig veränderte Produktkomponenten

Das Produkt „Firewall Dataport 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 in Anspruchnahme 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 sind Teil der jeweiligen Anwendung und daher, wie auch bei der Erst-Zertifizierung und der bisherigen Rezertifizierung, nicht Gegenstand dieser Rezertifizierung.

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



Internetzugang von Dataport Standort Altenholz
Stand: 12.06.2010

Abbildung 1 Struktur der Firewall

Der Aufbau des Produktes hat sich gegenüber der letzten Rezertifizierung [GRZDF08] nur unwesentlich geändert. Insbesondere haben sich der Einsatzzweck und der Datenfluss innerhalb des Produktes sowie die Protokollierung und Verarbeitung der Protokolldaten nicht geändert. Zu den relevanten Änderungen gehört,

--- der Umstieg von SuSE Linux auf Debian
--- die Einführung weiterer Überwachungstools (monit, tiger)
--- die Verwaltung der internen Loadbalancer mittels NetSPOC
--- der Einsatz von pound als Proxy
--- die Überführung der Governikus-DMZ in eine gewöhnliche DMZ

5.1 Bewertung der Änderungen

5.1.1 Umstieg von SuSE Linux auf Debian

Debian behandelt alle bekannt gewordenen Sicherheitslücken öffentlich, so dass Nutzer sich jederzeit über evtl. in den eingesetzten Produkten vorhandenen Schwachstellen informieren können. Dies führt dazu, dass bekannte Schwachstellen zeitnah behoben werden können. Damit wird auch die Sicherheit der Dataport Firewall verbessert.

5.1.2 Einführung weiterer Überwachungstools (monit, tiger)

monit ist ein Programm zum überwachen und managen von Prozessen und Dateien auf Unix-Systemen. Es kann zur Durchführung von automatischen Wartungs- und Reparaturaufgaben genutzt werden. Dataport nutzt monit um sicherzustellen, dass systemrelevante Prozesse laufen, bzw. dass diese Prozesse bei Bedarf neugestartet werden. Dies geschieht z.B. durch Connects und Test des Protokolls für Systemdienste oder die Überprüfung der zu bestimmten PID-Dateien gehörenden Prozesse. Weiterhin werden die Systemressourcen wie z.B. CPU-Nutzung und Speicherverbrauch überwacht und bei Überschreitung des definierten Schwellwertes wird eine Warnmeldung verschickt.

Durch die Überwachung bzw. den automatischen Neustart von Prozessen und die Überwachung der Systemressourcen kann die Verfügbarkeit der Firewall und der eingesetzten Proxies erhöht werden.

Tiger ist ein hostbasiertes Intrusion Detection System, welches das Dateisystem überwacht und die Ergebnisse als Statusemail verschickt. Während der Installation werden automatisch cronjobs angelegt, die täglich, wöchentlich und monatlich gestartet werden. Die per Email an den Administrator verschickten Ergebnisse müssen ausgewertet werden. Bei sicherheitsrelevanten Vorfällen (wie z.B. Änderungen an Binaries oder Konfigurationsdateien kritischer Dienste) werden die betreffenden Systeme kontrolliert und, sofern notwendig, entsprechende Maßnahmen eingeleitet.

Die Überwachung des Dateisystems erfolgte auch schon bei vorhergehenden Rezertifizierungen durch das Programm Aide. Damit ergänzt Tiger die Nutzung von Aide.

5.1.3 Verwaltung der internen Loadbalancer mittels NetSPOC

Das Programm NetSPOC dient der policybasierten Erstellung von Konfigurationsbefehlen für Cisco IOS Produkte. Durch die Nutzung von Policies wird, im Gegensatz zur manuellen Erstellung der Konfigurationsbefehle, die Wahrscheinlichkeit von Konfigurationsfehlern verringert. Dies führt zu einer Verbesserung der Sicherheit der Komponenten.

5.1.4 Einsatz von pound als ULR-filternder Proxy

Für den in der DMZ betriebenen Governikus-Dienst wurde mit Pound ein zusätzlicher Proxy eingerichtet, der anhand von URLs filtern kann. Der Proxy ist Teil der zugehörigen Anwendung und daher nicht Gegenstand der Rezertifizierung.

5.1.5 Überführung der Governikus-DMZ in eine gewöhnliche DMZ

Die Governikus-DMZ ist Teil der zugehörigen Anwendung und daher nicht Gegenstand der Rezertifizierung.

6. Bewertung der Einsatzumgebung

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.

7. Bewertung anhand der rechtlichen Anforderungen

Bei der Auditierung wurden bei den vorherigen Begutachtungen folgende Rechtsnormen als Bewertungsmaßstab hinzugezogen:

- --- Landesdatenschutzgesetz Schleswig-Holstein
- --- Telemediengesetz
- --- Telekommunikationsgesetz

Die genannten Gesetze haben in der Zwischenzeit **keine für das Produkt relevanten Veränderungen** erfahren.

Die oben genannten Änderungen des Produktes 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 Firewall am Standort 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.

9. Literatur

[GRZDF08] datenschutz nord GmbH, „Gutachten zur Rezertifizierung der Firewall der Dataport am Standort Altenholz“. Dezember 2008