Kurzgutachten zur Re-Zertifizierung der Dataport Firewall Altenholz

im Auftrag von Dataport

datenschutz cert GmbH

Juni 2016

Inhaltsverzeichnis

Kurzgutachten zur Re-Zertifizierung der Dataport Firewall Altenholz

1. Gegenstand der Prüfung

Mit diesem Kurzgutachten wird die erneute datenschutzrechtliche Auditierung des IT-Produktes „Dataport Firewall Altenholz“ mit Funktionsstand vom März 2016 dokumentiert. Das IT-Produkt der Dataport Anstalt des öffentlichen Rechts wurde erstmals am 25.11.2003 erfolgreich durch das vom Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) zertifiziert und seit dem regelmäßig re-zertifiziert, zuletzt 2014[1].

Grundlage der Auditierung mit dem Ziel der Re-Zertifizierung ist der Anforderungskatalog des ULD in der Version 2.

Die Dataport hat eine Selbsterklärung gegenüber den Auditoren und dem ULD abgegeben, in der Änderungen gegenüber der letzten Zertifizierung vermerkt wurden. Eine aktuelle Dokumentation zum IT-Produkt hat der Hersteller den Auditoren zudem in Form eines DokuWiki bereitgestellt. Das Audit erfolgte anhand einer Dokumentenprüfung und der Durchführung von Plausibilitätstests sowie eines Vor-Ort-Audits in Altenholz zur Einsatzumgebung im Februar 2016.

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 Begutachtung erstreckte sich auf den Zeitraum von 01.12.2015 bis 24.05.2016.

3. Antragstellerin

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

4. Sachverständige Prüfstelle

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

5. Geringfügig veränderte Produktkomponente

Die „Dataport Firewall Altenholz“ besteht aus externen Router/Paketfiltern, internen Router/Paketfiltern sowie Bastion Hosts als Proxies (Ersatzdienste). Sie können von Kunden der Dataport zum Schutz ihrer eigenen Ressourcen im Netzwerk gegen unberechtigte Zugriffe aus dem Internet in Anspruch genommen werden. Die

[1] Rezertifiziert am 24.01.2014 unter der Zertifizierungsnummer 8-11/2003 (gültig bis 24.01.2016).

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.

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

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. Ebenfalls *nicht* zum Auditgegenstand gehören die Regelungen zur SPAM-Abwehr und zum Virenschutz.

Der Aufbau des IT-Produktes hat sich gegenüber der letzten Rezertifizierung 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 betreffen Tools, die für Tests und Freigabeverfahren eingesetzt werden, den Abbau von Reverse-Proxies sowie Dokumentationen. Die (Reverse-)Proxies sind Teil der jeweiligen Fachanwendung und daher, wie auch bei den bisherigen Zertifizierungen, nicht Gegenstand dieser Auditierung.

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

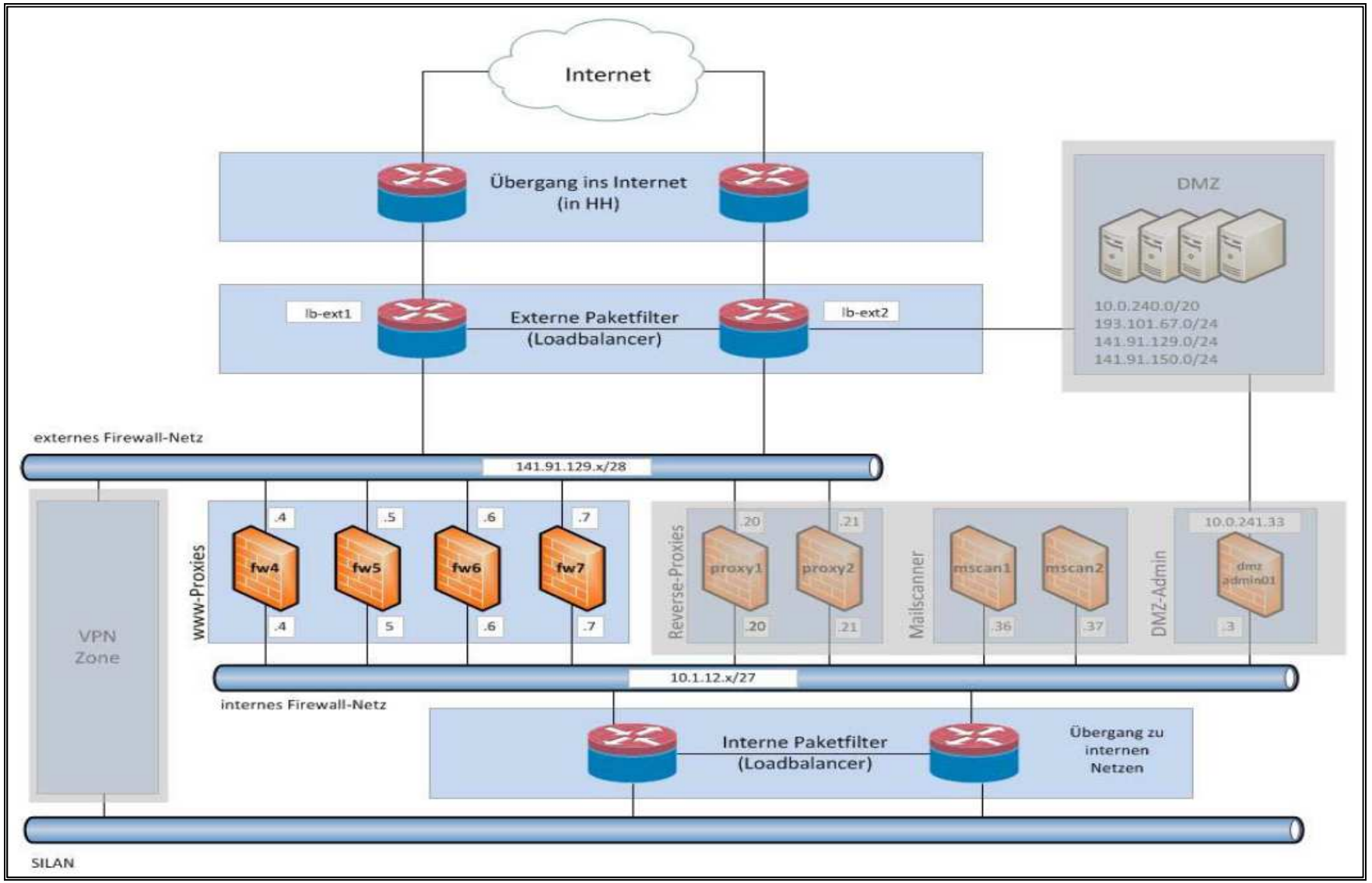


Abb. 1: Übersicht Struktur Dataport Firewall Altenholz

6. Bewertung anhand der technischen Anforderungen

6.1 Updates

Software und Tools, die für den Betrieb der Dataport Firewall am Standort Altenholz in Betrieb sind, werden fortlaufend auf den neusten Stand gebracht. Die Auditoren haben die hierzu angewandten Tests- und Freigabeverfahren eingesehen und die aktuellen Umstellungen als angemessen bewertet.

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 Auditierung des Rechenzentrums von Dataport am Standort Altenholz vor Ort durch den technischen Auditor geprüft und bestätigt.

7. Bewertung anhand der rechtlichen Anforderungen

Bei der Auditierung wurden insbesondere das Landesdatenschutzgesetz Schleswig-Holstein, das Telemediengesetz und das Telekommunikationsgesetz als Bewertungsmaßstab hinzugezogen. Diese Gesetze haben seit der Re-Zertifizierung keine für das IT-Produkt relevanten Veränderungen erfahren. Die oben genannten Änderungen an der Dataport Firewall Altenholz 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.

Erneut dargestellt und bewertet werden soll an dieser Stelle der Protokollierungsprozess, welcher die Verarbeitung sekundärer Daten, wie IP-Adressen beinhaltet.

Abrechnungs- und Statistikdaten werden, wie in der **Abbildung 2** unten gezeigt, täglich erfasst (z.B. verbrauchte Bandbreite aller Netze eines Auftraggebers, aufgerufene Domains aller Netze eines Auftraggebers für monatliche „top30“ Liste). Anschließend werden die Daten der HTTP/HTTPS Proxies (anonymisiert) sowie des SMTP Dienstes (Transportlog) 10 Tage lang für die Zwecke des Leistungsnachweises bzw. der Entstörung gespeichert und dann gelöscht.

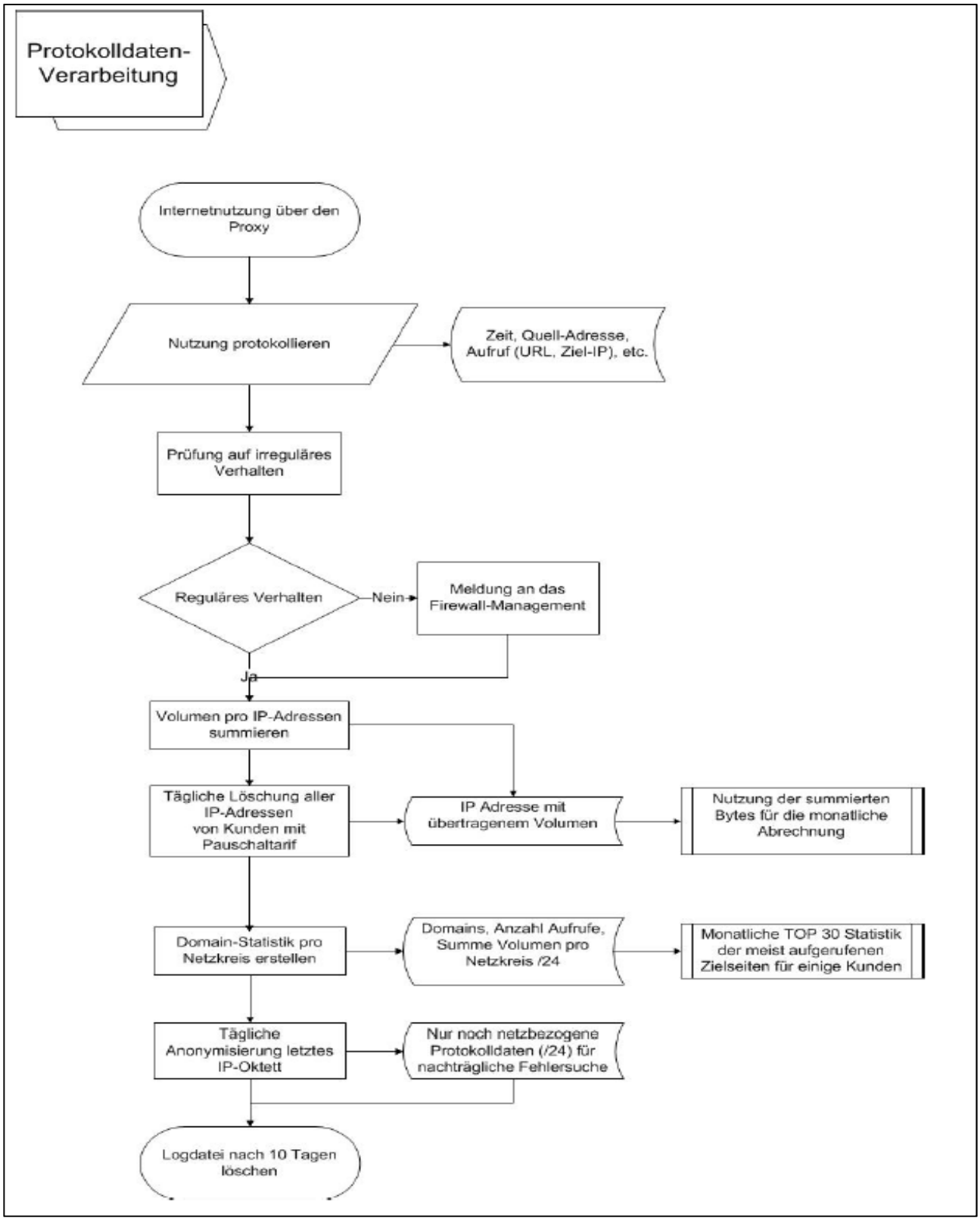


Abb. 2: Protokollierungs-Datenfluss

Aus den Protokollen wird ein zur Rechnungsstellung benötigter Teildatensatz erstellt. Der Teildatensatz enthält maximal

--- die IP-Adresse des anfragenden Rechners, gekürzt um das letzte Oktett,

--- die Menge der übertragenen Daten,

--- den Zeitpunkt der Verbindung und

--- die Dauer der Übertragung.

Diese Daten werden auf dem Bastion-Host maximal 31 Tage zur Rechnungslegung gespeichert. Für die volumenbasierte Abrechnung wird auf die Speicherung des letzten Oktetts der IP-Adresse verzichtet. Das letzte Oktett ist für die Abrechnung nicht erforderlich, da Kunden mindestens ein Klasse C Netz zugewiesen bekommen.

Die Daten sind nach der Anonymisierung nicht mehr als personenbezogene Daten anzusehen, da nur noch der Besitzer des Netzes (= Behörde) zu erkennen ist. Die Daten dienen zur Erkennung von Störungen (auch als Nachweis der Leistungserbringung, z.B., dass eine Störung auf dem Zielserver eines Drittanbieters vorliegt) und dem Nachweis von Schadcodebefall (Aufrufe von C&C Servern). Insbesondere Domains und IPs von C&C Servern werden erst mit Verzögerung erkannt / bekannt und dann z.B. über das BSI mitgeteilt. Dann muss auch nachträglich noch ermittelt werden können, ob ein entsprechender Datenabfluss stattgefunden hat.

Die Speicherung dieser Nutzungsdaten ist im Rahmen eines Auftragsverhältnisses zwischen den öffentlichen Stellen des Landes Schleswig-Holstein und Dataport zulässig, da diese Daten von den öffentlichen Stellen benötigt werden, um die private Internetnutzung durch ihre Mitarbeiter abzurechnen. Hierbei handelt es sich um einen Teledienst, den die öffentlichen Stellen gegenüber Ihren Mitarbeitern erbringen, sofern diese das Internet zu privaten Zwecken nutzen, nicht jedoch um einen Teledienst, den Dataport zur Verfügung stellt. Nutzungsdaten, die zu solchen Abrechnungszwecken gespeichert werden, sind als Abrechnungsdaten gemäß § 15 Abs. 4 TMG zu betrachten, ihre Speicherung ist innerhalb des in § 15 Abs. 7 TMG gezogenen Rahmens zulässig.

Ihre datenschutzkonforme Verarbeitung innerhalb der Rechnungsabteilung wird durch den betrieblichen Datenschutzbeauftragten von Dataport sichergestellt.

Die Logdaten des access.log und die Datei redir.log (squidguard, einige Kunden haben einen URL-Filter beauftragt) werden nach wenigen Stunden bereits anonymisiert. Dabei wird das letzte Oktett nach Mitternacht auf 000 gesetzt. Nach 10 Tagen werden alle übrigen Dateien komplett gelöscht.

Darüber hinaus sind Logs zur Gewährleistung der technisch-organisatorischen Sicherheit aktiviert. Die Logdateien syslog, mail.*, firewall.log, rinetd.log und sec.log werden (wie oben beschrieben) ebenfalls anonymisiert und nach 10 Tagen gelöscht.

Die rinetd.log enthält dabei Protokolle über Kundenzugriffe, also auch Kunden-IPs. Allerdings sind diese Verbindungen stark eingeschränkt. Es sind jeweils nur eine oder wenige Quell-IPs freigeschaltet. Zudem finden hierüber nur Verfahrenstechnische Zugriffe statt (keine privaten Zugriffe), die i.d.R. automatisiert sind (z.B. durch spezielle Geräte für Zahlungsverkehr oder e-pass-reader). Teilweise bleiben diese

Verbindungen ferner über lange Zeiträume bestehen und werden erst mit dem Abbau mitgeloggt.

Die Postfix- und Mailscanner-Logdateien auf Firewalls und mscan-Servern werden ebenfalls nach 10 Tagen gelöscht. Hier sind keine Client-IPs vorhanden.

E-Mail-Transportdaten werden ebenfalls 10 Tage lang gespeichert und dann komplett gelöscht. Im Gegensatz zu HTTP/HTTPS sind private E-Mails von Beschäftigten der Kunden von dataport nicht erlaubt und daher immer als dienstlich, bzw. unaufgefordert zugesandte Spam- bzw. Schadcodemails anzusehen. Die Angaben von Internet-Mailservern sind nicht vertrauenswürdig, während die Angabe des Empfängers im Landesnetz das wichtigste Suchkriterium ist und nicht anonymisiert werden kann.

Diese Daten sind wichtig für den Leistungsnachweis bzw. für die Entstörung. "Störungen" bedeuten in diesem Fall so gut wie nie den kompletten Ausfall des Dienstes, der ja sofort erkennbar wäre (Senden und Empfangen von E-Mails nicht möglich). Vielmehr sind die Störungen von der Art „einzelne E-Mail aus dem Internet ist nicht eingegangen“ oder „einzelne E-Mail an Empfänger im Internet ist dort nicht angekommen“. Bei erwarteten oder angekündigten E-Mails fällt dies erst nach einigen Tagen auf, bei nicht erwarteten E-Mails kann die Verzögerung noch länger sein. Wichtig ist hier der Nachweis, ob sich die E-Mail im Verantwortungsbereich von Dataport befand, gegen welche Policy verstoßen wurde und ob ggf. eine qualifizierte Fehlermeldung zurückgegeben wurde.

Bezüglich der Sicherheit bei Schadcodewellen, die seit 2015 erheblich zugenommen haben, ist es sehr sinnvoll, nach Erkennung einer neuen Schadcodewelle zu prüfen, ob einzelne E-Mails dieser Art bereits vor der Erstellung eines Sperrmusters zugestellt wurden, um effektivere Erkennungsmuster zu erzeugen und ggf. den Empfängerkreis warnen zu können. Nach Erkennung eines Schadcodebefalls kann über die Logdaten untersucht werden, ob der Befall auf eine Schadcode-E-Mail zurückzuführen ist (falls ja, dann ist auch Zeitpunkt, Art der Welle und weitere Empfänger bei Bedarf ermittelbar).

Von einer transportierten E-Mail werden folgende Daten in eine Logdatei geschrieben: Datum, Uhrzeit, Einliefernder Host (Name + IP des einliefernden Host der Behörde), Absender-Adresse, Empfänger-Adresse, Menge der übertragenen Daten, Statuscode, Mail-ID auf dem nächsten Mailserver, Prüfungen der Spambewertung (welche Regeln haben angeschlagen) und Diagnoseinformationen zur Spam/Virenprüfung, bei Anhängen (Dateiname und Typ des Anhangs), Betreff der E-Mails (nur anlassbezogen zur Gefahrenabwehr insbesondere bei Spamfluten). Auch diese Daten werden nach 10 Tagen gelöscht. Auch hier erfolgt die Speicherung zur Abwehr von Gefahren, zur Fehleranalyse und Gewährleistung der IT-Sicherheit. Dabei erfolgt die Speicherung der Betreffzeilen nur nach Freigabe durch den Auftraggeber.

Die Speicherfrist dieser Protokolldaten von ebenfalls 10 Tagen ist, wie oben erläutert, auch angemessen. Laut Auskunft muss Dataport in dem verbleibenden Zeitraum von 10 Tagen recht oft Fragen über den Verlauf oder die Abweisung einer E-Mail (per

Incident über ITSM) nachgehen, so dass eine vorherige Anonymisierung diese Leistungen zunichtemachen würde.

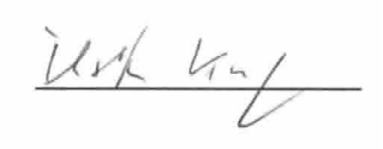
Die Datei sudo.log wird zur quartalsweisen Überprüfung der Administratoren aufgehoben. Dies ist im Hinblick auf die geforderte Revisionskontrolle als unkritisch zu betrachten.

Die Protokollierung der benannten Logs ist eine sicherheitstechnische Maßnahme nach § 5 Abs. 1 LDSG-SH und somit nach §11 Abs. 1 Nr.3 LDSG-SH zulässig.

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 15.06.2016



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

Thorsten Kamp
datenschutz cert GmbH