Zwischen dem Land Schleswig-Holstein, vertreten durch das Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung des Landes Schleswig-Holstein – Land -

einerseits

und

- dem DBB Beamtenbund und Tarifunion
Landesbund Schleswig-Holstein –

- dem Deutschen Gewerkschaftsbund
Bezirk Nord -

- Vereinbarungspartner – andererseits

wird die folgende **Vereinbarung nach § 59 Mitbestimmungsgesetz** des Landes Schleswig-Holstein (MBG) geschlossen.

Richtlinie zur Nutzung von Internet und E-Mail

1. Geltungsbereich

Diese Richtlinie gilt für die Beschäftigten (Beamtinnen und Beamten sowie Arbeitnehmerinnen und Arbeitnehmer) der unmittelbaren Landesverwaltung im Sinne des § 3 in Verbindung mit § 2 Abs. 1 Mitbestimmungsgesetz des Landes Schleswig-Holstein (MBG), deren PC-Arbeitsplatz an das Landesnetz angeschlossen ist und denen über diesen Anschluss die Dienste Internet und E-Mail zur Verfügung gestellt werden.

Sie gilt nicht für die Gerichte und Staatsanwaltschaften.

Sie gilt nicht für die Beschäftigten der Landtagsverwaltung und des Landesrechnungshofes.

Soweit die Präsidentin oder der Präsident des Landtages beziehungsweise des Landesrechnungshofes das Einvernehmen nach § 59 Abs. 4 MBG Schl.-H. erklärt, gilt diese Vereinbarung auch für die Beschäftigten des jeweiligen Bereiches.

Anlagen 1 bis 3 sind Bestandteil dieser Vereinbarung.

2. Umfang

Diese Richtlinie regelt die dienstliche und private Nutzung der dienstlich zur Verfügung gestellten Services Internetzugang und E-Mail[1].

Die Regelungen dieser Vereinbarung müssen durch die Dienststellen für ihren Zuständigkeitsbereich in entsprechenden Dienstanweisungen oder Dienstvereinbarungen präzisiert und ergänzt werden.

3. Grundsätze der Nutzung von Internet und E-Mail

3.1. Internetzugang und E-Mail sind Arbeitsmittel, die an allen PC-Arbeitsplätzen, die an das Landesnetz angeschlossen sind, zur Verfügung gestellt werden.

3.2. Die Nutzung von Internetzugang und E-Mail durch die Beschäftigten muss eigenverantwortlich und der jeweiligen dienstlichen Aufgabenstellung angemessen erfolgen.

3.3. Die Nutzung von E-Mail ist ausschließlich für dienstliche Zwecke zulässig.

3.4. Für private Zwecke ist den Beschäftigten die unentgeltliche Nutzung des dienstlichen Internetzugangs ausschließlich zum Nutzen von Web-Seiten (Dienste http / https) gestattet, soweit dienstliche Interessen nicht entgegenstehen.

3.5. Der lesende und schreibende Zugriff auf ein privates, bei einem externen Dienstanbieter geführtes E-Mail-Postfach (Web-Mail) ist den Beschäftigten gestattet, soweit dienstliche Interessen nicht entgegenstehen.

3.6. Die Zulassung der Nutzung des Internetzugangs nach Nr. 3.4 und 3.5 kann – für einen bestimmten Verwaltungsbereich oder im Einzelfall – widerrufen werden.

3.7. Die Nutzung von Internetzugang und E-Mail im Rahmen der Vereinigungsfreiheit entsprechend Artikel 9 Grundgesetz ist zulässig.

---

[1] Einzelheiten des Diensteumfangs sind jeweils aktuell der Anlage 1 zu entnehmen.

3.8. Die Beschäftigten werden in der Nutzung der angebotenen Dienste bedarfsgerecht geschult und fortlaufend sowie anlassbezogen über mögliche Risiken informiert.

3.9. Die Dienststellen haben im Rahmen ihrer Zuständigkeit die Nutzung der angebotenen Dienste unter Beachtung der in Nr. 6 und Anlage 1 dieser Vereinbarung festgelegten Grundsätze zu überwachen.

3.10. Die Sicherheitsmaßnahmen der vom Zentralen IT-Management Schleswig-Holstein über Dataport betriebenen zentralen Komponenten entbinden die Dienststellen nicht von der entsprechenden Verantwortung für ihren jeweiligen Zuständigkeitsbereich.

3.11. Die Regelungen der Abgabenordnung (insbesondere § 87 a Elektronische Kommunikation) und der Landesverordnung über die Verarbeitung personenbezogener Daten in Schulen (Schul-Datenschutzverordnung - SchulDSVO) bleiben unberührt.

4. E-Mail

4.1. Für den Dokumentenverkehr ist, soweit keine rechtlichen, wirtschaftlichen oder technischen Gründe entgegenstehen, die elektronische Post vorrangig gegenüber der Briefpost und dem Fax einzusetzen. Ein paralleler Versand mit Briefpost soll unterbleiben.

4.2. Der E-Mail-Eingang soll regelmäßig, mindestens einmal arbeitstäglich auf eingegangene E-Mail gesichtet werden.

4.3. E-Mail wird wie eingehende Post gewertet und weiterbearbeitet. Ziffer 5.2.1 der Gemeinsamen Geschäftsordnung für die Ministerien des Landes Schleswig-Holstein (GGO) ist nicht anzuwenden.

4.4. Wenn bei einer eingehenden E-Mail die absendende Stelle, der Inhalt oder die Anlage zweifelhaft erscheint, ist unverzüglich die zuständige Stelle[2] zu informieren. Diese entscheidet über die weitere Behandlung.

4.5. Eine elektronische Post mit vertraulichem Inhalt oder mit personenbezogenen Daten darf an eine E-Mail-Adresse mit anderer Endung als …@...landsh.de oder weiteren, vom zentralen IT-Management freigegebenen Endungen nur versandt werden, wenn der schützenswerte Inhalt oder die Nachricht insgesamt ihrem Schutzbedarf entsprechend geschützt, gegebenenfalls verschlüsselt ist. Die Vorgaben der Verschlusssachen-Anweisung für Schleswig-Holstein bleiben unberührt.

5. Internet

5.1. Unzulässig ist jede absichtliche oder wissentliche Nutzung des Internetzugangs, die gegen geltende Rechtsvorschriften verstößt oder geeignet ist, den Interessen der Landesregierung oder deren Ansehen in der Öffentlichkeit zu schaden oder die Sicherheit des Landesnetzes zu beeinträchtigen. Das Land behält sich vor, den Internetzugriff auf entsprechende Seiten generell oder für einzelne Bereiche zu sperren.

5.2. Unzulässig ist die Internetnutzung für Glücksspiele, Wetten und ähnliche Internetaktivitäten, die ein Suchtpotential und damit gesundheitliches Gefährdungspotential für Nutzer besitzen (Glücksspiele, Online-Poker, Sport-/Wetten, Lotto u.ä.).

5.3. Die Nutzung von Anonymisierungsdiensten ist verboten.

5.4. Mit der Erlaubnis zur privaten Nutzung des Internetzugangs ist kein Anspruch auf Verfügbarkeit des Dienstes und Betreuung begründet.

---

[2] Wer diese Aufgabe vor Ort wahrnimmt, ist in den Dienststellen festzulegen, zum Beispiel im jeweiligen Sicherheitskonzept.

6. Protokollierung und Kontrolle

6.1. Eine Protokollierung der Nutzung der Dienste (Nutzungs-, Verkehrs- und Inhaltsdaten) erfolgt und ist erforderlich

6.1.1. aus Gründen der Daten- und Systemsicherheit,

6.1.2. aus Gründen der Systemtechnik (z.B. zur Fehlerverfolgung) und

6.1.3. aus Gründen der Arbeitsorganisation (z.B. zur Feststellung von Art und Umfang der Nutzung und zur Missbrauchskontrolle)

Protokolldaten, die gemäß 6.1.1 aus Gründen der Daten- und Systemsicherheit verarbeitet werden, unterliegen zum Teil deutlich längeren Speicherfristen als jene unter 6.1.2 und 6.1.3.

Die Protokolldaten gemäß 6.1.1 werden von Protokolldaten für die Zwecke gemäß 6.1.2 und 6.1.3 technisch und organisatorisch getrennt verarbeitet und stehen für andere Zwecke als 6.1.1 nicht zur Verfügung.

Einzelheiten der Protokollierung (Art, Umfang, Verarbeitung - je nach Zweck) sind insbesondere in Anlage 1 in der jeweils aktuellen Fassung festgelegt und Grundlage des Auftrages an Dataport (Anlagen 2 und 3).

Über die nachstehend genannten Nutzungen hinaus werden die Protokolldaten nicht zur Leistungs- und Verhaltenskontrolle genutzt. Dies gilt gemäß § 15 Landesdatenschutzgesetz im Besonderen für die Protokolldaten gemäß Ziffer 6.1.1.

Die Rechte der Beschäftigten, für die diese Vereinbarung gilt, gemäß Art. 15 DSGVO bleiben unberührt.

Die Daten- und Systemsicherheit der Dienste und damit der gesamten Standard-ITSH sowie weiterer Dienste und IT-Verfahren haben sehr hohe Priorität.

Sollte nach dem Inkrafttreten dieser Vereinbarung und gemäß Zweck 6.1.1 und damit aus Gründen der Daten- und Systemsicherheit der Dienste eine längere oder kürzere Aufbewahrungsdauer für Protokolldaten erforderlich werden, wird das Land dies den Vereinbarungspartnern einschließlich der dafür maßgeblichen

Gründe und der vorgesehenen Befristung der Änderung unverzüglich mitteilen und um Zustimmung bitten. Das Land macht die geänderte Aufbewahrungsdauer und deren Befristung den Beschäftigten bereits zu diesem Zeitpunkt im Extranet (SHIP) bekannt. Sollte keine Zustimmung erreicht werden, nimmt das Land mit den Vereinbarungspartnern unverzüglich Verhandlungen auf.

Das Land wird die Vereinbarungspartner um Zustimmung in Textform bitten. Die geänderte Vereinbarung wird nach der Zustimmung der Vereinbarungspartner gemäß Ziffer 8 Schlussbestimmungen bekannt gemacht.

6.2. Auf Protokolldaten hat grundsätzlich nur Dataport Personal Zugriff, insbesondere im Rahmen der Zwecke gemäß Ziffern 6.1.1 und 6.1.2. Einzelheiten zur Protokollierung sind der Anlage 1 zu entnehmen.

6.3. Personal, das Zugang zu Protokollinformationen hat, ist besonders auf die Sensibilität dieser Daten hinzuweisen und auf Einhaltung von Datenschutz zu verpflichten. Bei der Auswahl des Personals ist dies entsprechend als Eignungsvoraussetzung zu berücksichtigen. Dafür ist auch Sorge zu tragen (zum Beispiel durch vertragliche Vereinbarung), wenn und soweit es sich nicht um eigenes Personal handelt.

6.4. Auswertungen von Protokolldaten gemäß Ziffer 6.1.3 erfolgen grundsätzlich zunächst anonymisiert als Monatsstatistiken nach Anzahl der Aufrufe und nach Volumen der übertragenen Datenmengen. Eine weitergehende Auswertung von Protokolldaten muss die Grundsätze einer datenschutzgemäßen Kontrolle berücksichtigen, insbesondere den Grundsatz der Verhältnismäßigkeit. Eine individuelle Verhaltens- und Leistungskontrolle durch eine Auswertung der Protokolldaten ist grundsätzlich unzulässig.

6.5. Ergeben sich insbesondere aus den statistischen Auswertungen eindeutige Hinweise auf unzulässige Zugriffe oder auf eine deutliche Überschreitung der erlaubten privaten Nutzung (Stufe 1), ist der betroffene Kreis der Beschäftigten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hinzuweisen (Stufe 2). Gleichzeitig wird darüber unterrichtet, dass bei Fortdauer der Verstöße zukünftig eine gezielte Kontrolle (Stufe 3) nach einem gesondert festzulegenden Verfahren

stattfinden kann. An der Festlegung des Verfahrens und Auswertung von Protokolldaten sind die zuständige Gleichstellungsbeauftragte, Personalvertretung, Schwerbehindertenvertretung und die oder der behördliche Datenschutzbeauftragte zu beteiligen. Das Verfahren ist den Beschäftigten bekannt zu machen.

6.6. Für die gezielte Kontrolle (personenbezogene Verarbeitung der Protokolldaten) entsprechend Stufe 3 müssen der genaue Zweck, der Umfang, der Zeitraum der von Dataport zu übermittelnden Protokolldaten und deren Auswertung vorab in einem Konzept festgelegt werden und der zentral für den Internetzugang verantwortlichen Stelle übermittelt werden. Der Umfang der von der Protokollierung erfassten Personen muss dabei auf den Kreis der Verdächtigen begrenzt werden. Es dürfen nicht pauschal alle Beschäftigten kontrolliert werden. Die zentral für den Internetzugang verantwortliche Stelle beauftragt Dataport mit der Lieferung der Protokolldaten an die anfordernde Stelle. Die Protokolldaten sind von der anfordernden Stelle nach der Auswertung zu löschen, soweit sie nicht Bestandteil von Akten werden und damit den diesbezüglichen Aufbewahrungsfristen unterliegen. Die Ergebnisse sind den Betroffenen bekannt zu geben. Entsprechend der Ergebnisse ist das weitere Vorgehen abzuwägen:

- Einstellen der Lieferung von Protokolldaten,
- erneutes Ermahnen des betroffenen Personenkreises und Fortführen der gezielten Verarbeitung oder
- Verschärfen der Kontrolle, in dem die Protokollierung bezogen auf den beziehungsweise auf dem Arbeitsplatzrechner stattfindet (Stufe 4).
  Für die Protokollierung auf dem Arbeitsplatz gelten dieselben Anforderungen wie in Stufe 3 mit Ausnahme der Ankündigung. Die Mitarbeiterinnen und Mitarbeiter müssen über diese Maßnahme aufgeklärt werden. In diesem Stadium ist auch zu erwägen, ob bereits eine Strafanzeige zu stellen und eine Strafverfolgungsbehörde hinzuziehen ist, um bei der Beweissicherung keine Fehler zu machen.

6.7. Bei fortgesetzten Verstößen sind dienst- oder arbeitsrechtliche Maßnahmen gegen die betreffenden Beschäftigten nicht ausgeschlossen.

6.8. Unzulässig sind Auswertungen insbesondere von Protokolldaten (Nutzungs-, Verkehrs- und Inhaltsdaten), um Informationen über die Nutzung des Dienstes Internet und die E-Mail-Kommunikation in Zusammenhang mit besonders zu schützenden Funktionen (zum Beispiel Personalvertretungen, Gleichstellungsbeauftragte, Schwerbehindertenvertretungen, behördliche Datenschutzbeauftragte und ähnliche) sowie über die Kommunikation im Sinne von Ziffer 3.7 zu gewinnen.

6.9. Bei Verdacht von Straftaten ist die Auswertung von Protokolldaten den zuständigen Strafverfolgungsbehörden zu überlassen.

7. In-Kraft-Treten

Diese Richtlinie tritt am 01.01.2021 in Kraft und löst damit die Fassung vom 01.01.2010 ab.

8. Schlussbestimmungen

Die zu dieser Vereinbarung gehörenden Anlagen

- Anlage 1 Einzelheiten der Protokollierung
- Anlage 2 SLA Leistungsbeschreibung E-Mail SH
- Anlage 3 SLA Leistungsbeschreibung FW-Infra SH

können in der Weise aktualisiert werden, dass das Land den Vereinbarungspartnern einen entsprechenden Änderungsvorschlag vorlegt, der beschlossen ist, sobald von allen Beteiligten in Textform zugestimmt wurde. Sollte keine Zustimmung erreicht werden, nimmt das Land mit den Vereinbarungspartnern unverzüglich Verhandlungen auf.

Diese Vereinbarung kann mit einer Frist von einem Jahr zum Jahresende und erstmalig zum 31. Dezember 2022 von beiden Seiten gekündigt werden.

Wenn diese Vereinbarung gekündigt wird, gilt sie in allen Punkten so lange weiter, bis eine neue Vereinbarung abgeschlossen wurde, die die hier geregelten Sachverhalte neu regelt. Dies gilt auch für den Fall, dass die gesetzlichen Regelungen zur Mitbestimmung oder zum Beschäftigtendatenschutz geändert werden.

Diese Vereinbarung und deren Aktualisierungen werden im Extranet SHIP der Landesregierung und im Amtsblatt veröffentlicht. Die Anlagen und deren Aktualisierungen werden im Extranet SHIP veröffentlicht.

Kiel, 8. Dezember 2020

Ministerium für Energie, Landwirtschaft, Umwelt, Natur und Digitalisierung des Landes Schleswig-Holstein

Staatssekretär V StE

Gez. Tobias Goldschmidt

Tobias Goldschmidt

Hamburg, 16. Dezember 2020

Deutscher Gewerkschaftsbund

- Bezirk Nord –

Gez. Uwe Polkaehn

Uwe Polkaehn

Kiel, 17. Dezember 2020

dbb beamtenbund und tarifunion e.V.

- Landesbund Schleswig-Holstein-

Gez. Kai Tellkamp

Kai Tellkamp

Teil 1 – Überblick über die Dienste

1. Der Internet-Dienst umfasst
   1.1. http (hypertext transport protocol) – Surfen
   1.2. https (hypertext transport protocol secure) – verschlüsseltes Surfen
   1.3. ftp (file transport protocol)– Download (ggf. Upload) von Dateien

   Der Zugang wird grundsätzlich rund um die Uhr angeboten (erreichte Verfügbarkeit größer als 98,5% im Jahresmittel). Grundsätzlich kann die Firewall vom Netz getrennt werden, wenn Angriffe von extern auftreten oder die Vermutung besteht, dass Systeme unberechtigt genutzt werden.
2. Der E-Mail-Dienst umfasst Mailen im Bereich des Landesnetzes und in sicher gekoppelten, anderen Verwaltungsnetzen (z.B. Netz des Bundes, CNPON, ParlaNet, …) sowie im Internet.
3. Unterstützung und Wartung sind über das Dataport Call-Center verfügbar. Die Störungsannahme erfolgt Montag bis Freitag von 6:30 – 18:00 Uhr.
4. Aus externen Netzen eingehende E-Mails werden von der zentralen Firewall geprüft auf
   - ausführbare Dateien anhand der Datei-Endungen,
   - soweit sie im html-Format eingehen, auf Sprunganweisungen,
   - Viren und auf
   - SPAM.

   Aus dem Internet eingehende E-Mails mit der Absendeadresse .landsh.de werden abgewiesen.
   E-Mails, die bestimmte Dateiformate als Anhänge enthalten, die potentiell Schadcode enthalten könnten, werden ebenfalls abgewiesen.
   Als gefährdend oder belästigend erkannte Mails werden an der Firewall mit einer Fehlermeldung an den Absender abgewiesen.
5. Von den Verkehrsdaten der E-Mail werden an der Firewall protokolliert:
   - Datum / Uhrzeit
   - Adressen von Absender und Empfänger
   - Übertragene Datenmenge
   - IP-Nummer des unmittelbaren Eingangs- und Ausgangs-Servers.

   Von den Inhaltsdaten der E-Mail werden an der Firewall protokolliert:
   - Betreff der E-Mail
   - Dateinamen von Anhängen

Die E-Mail-Protokolldaten werden 10 Tage aufbewahrt und dann gelöscht.
Art und Umfang der Aufbewahrung und Verwendung von E-Mail-Inhaltsdaten durch die Dienststellen sind von diesen für ihren jeweiligen Zuständigkeitsbereich festzulegen und den Beschäftigten bekannt zu machen.

6. Von den Nutzungsdaten des Internets werden protokolliert und für die genannten Zwecke verarbeitet:
   HTTP(S):
   - Zeitpunkt des Aufrufs (Datum, Uhrzeit)
   - IP-Adresse des Arbeitsplatzes
   - http-Methode (nicht bei HTTPS)
   - Status / Fehlercode
   - Übermittelte Datenmenge (der übermittelten Informationen)
   - Ziel-URL (bei verschlüsselten Verbindungen nur die Domain selbst, ohne Parameter)
   - IP-Adresse des Zielsystems
   - Bei Downloads Datentyp der heruntergeladenen Datei (nur bei HTTP)

   FTP:
   - Zeitpunkt des Aufrufs (Datum, Uhrzeit)
   - IP-Adresse des Arbeitsplatzes
   - Ziel-IP
   - Status / Fehlercode
   - Menge der übertragenen Daten
   - Namen der übertragenen Dateien.

   Die hier aufgezählten Werte sind nicht abschließend und können von Dataport aus Gründen der Daten- und Systemsicherheit und aus Gründen der Systemtechnik angepasst werden. Ausdrücklich ausgeschlossen hiervon sind aufgrund des hohen Schutzwertes Inhaltsdaten der Verbindungen.
   Dataport holt die Zustimmung des Verantwortlichen zu Änderungen unverzüglich ein. Der Verantwortliche bindet je nach Inhalt der Änderung Informationssicherheits-beauftragte und behördliche Datenschutzbeauftragte ein und holt die Zustimmung der Vereinbarungspartner zur Änderung ein (siehe Ziffer 8 der 59er-Vereinbarung).
7. Diese Festlegungen gelten für die zentralen Komponenten und entsprechend für die lokalen Komponenten, soweit dort keine weitergehenden Regelungen getroffen, vereinbart und bekannt gemacht worden sind.

Teil 2 Verarbeitung von Logdateien im Rahmen der Internetnutzung

1. Notwendigkeit der Protokollierung im Rahmen der Internetnutzung

Im Rahmen der Nutzung des dienstlichen Internetzugangs werden auf den zentralen Systemen, die den Zugriff ins Internet realisieren, unterschiedliche Logdaten verarbeitet. Die Verarbeitung dieser Protokolldaten erfolgt mit folgender Zweckbestimmung:

1. aus Gründen der Daten- und Systemsicherheit,
2. aus Gründen der Systemtechnik (z.B. zur Fehlerverfolgung) und
3. aus Gründen der Arbeitsorganisation (z.B. zur Feststellung von Art und Umfang der Nutzung und zur Missbrauchskontrolle)

Die Protokolldaten gemäß 1 werden von Protokolldaten für die Zwecke gemäß 2 und 3 technisch und organisatorisch getrennt verarbeitet und stehen für andere Zwecke als 1 nicht zur Verfügung.

Die Protokolldaten können auch im Rahmen des Auskunftsrechtes nach Nr.6 der Vereinbarung von den betroffenen Beschäftigten angefordert werden.

2. Protokolldaten des Internetzugangs und Zuordnenbarkeit zu Beschäftigten

Die Protokolldaten des Internetzugangs enthalten Informationen, die Beschäftigten zugeordnet werden können und damit personenbezogene Daten.

Um diese Protokollinformationen tatsächlich Rechnern oder Accounts zuordnen zu können, werden Daten aus der AD-Protokollierung benötigt, deren Verarbeitung je nach Zweck genauso lange erfolgen darf, wie die der Logdaten des Internetzugangs.

Die Verarbeitung der AD-Protokollierung, bezogen auf

- Datum, Uhrzeit
- IP-Adresse des Rechners
- Computername des Rechners
- Benutzerkonto, das zur Anmeldung am Rechner genutzt wurde

zu den Zwecken dieser Richtlinie erfolgt ebenfalls im Rahmen der technischen und organisatorischen Trennung je nach Zweck.

3. Erweiterte Darstellung zur Aufbewahrung gemäß Zweck je Anwendungsfall

In der folgenden Tabelle werden die einzelnen Anwendungsfälle, für die Logdaten der Proxys und anderer Quellen benötigt werden, den einzelnen Zwecken zugeordnet. Zusätzlich wird danach definiert, in welchen Fällen eine Beziehbarkeit zu einem Computer und zu einem AD-Konto (und damit im Regelfall zu einer natürlichen Person) notwendig ist und wie lange die Daten für den jeweiligen Anwendungsfall aufbewahrt werden müssen.

Folgende Anwendungsfälle mit in diesem Sinne personenbeziehbaren Daten ergeben sich:

Daten- und Systemsicherheit

1. **Echtzeiterkennung:** Aufgrund der Schnelligkeit und Gefährlichkeit aktueller Angriffe ist es notwendig, Angriffe so früh wie möglich zu erkennen, um die Schäden zu minimieren. Zum Beispiel erfolgt bei einer Emotet-Infektion sofort der Beginn der Datenextraktion, und innerhalb von wenigen Tagen

kann es sein, dass die Angreifer sich auf dem übernommenem System direkt anmelden und den gewonnen Zugang ausbauen. Eine Echtzeiterkennung wird mittels spezialisierter Sicherheitssysteme, zum Beispiel mittels eines Security Information and Event Management (SIEM) durchgeführt, da die eigentlichen Proxys hierzu nicht in der Lage sind.

2. **Rückwirkende Erkennung von Angriffen:** Die Echtzeiterkennung bietet jedoch nicht die Möglichkeit, Angriffe, für die Indikatoren zur Erkennung erst nach langer Zeit bekannt werden, zu detektieren. Fortgeschrittene, gezielt vorgehende Angreifer sind dafür bekannt, dass sie übernommene Systeme nach der Erreichung ihrer Ziele wieder säubern, um so zu verhindern, dass sie entdeckt werden. So hat der Bundesverfassungsschutz im Dezember 2019 erstmalig vor der chinesischen Gruppe Winnti gewarnt, die nachweislich seit 2011[1] in Deutschland aktiv war. Im Rahmen dieser Warnung wurden URL-Aufrufe, an denen man die Erstinfektion durch diese Gruppe erkennen kann, bekannt gegeben. Diese Informationen können jedoch gewinnbringend nur in Verbindung mit weit zurückreichenden Log-Dateien genutzt werden.

3. **Rückwirkende Erkennung Phishing**: Phishing, insbesondere Spearphishing, zielt darauf ab, Zugangsdaten von Endanwendern zu erhalten. Oft erfolgt dies, indem Anwender auf echten Seiten nachempfundene Webseiten gelockt werden und sich dort dann anmelden müssen. Da gerade Spearphishing sehr zielgerichtet erfolgt, ist die Erkennungsrate durch Endanwender sehr gering. Falls die gefälschte Webseite doch einem Anwender oder durch andere Mittel auffällt, kann nur mittels langfristig aufbewahrter Logdateien festgestellt werden, ob weitere Anwender angegriffen wurden.

Arbeitsorganisation

4. **Auswertung wegen missbräuchlicher Nutzung:** Gemäß der 59er Vereinbarung zur Nutzung von Internet und Email erfolgt ab der Stufe 3 eine personenbeziehbare Auswertung der Logdaten ab Beginn der Stufe 3.
5. **Entlastung von Mitarbeitern:** Sofern personenbeziehbare Daten aus den zuvor genannten Gründen langfristig aufbewahrt werden, sollten diese auch zur Entlastung von Mitarbeitern durch die betroffene Person angefordert werden können.

Nachfolgend sind in einer Tabelle die Anwendungsfälle zu Zweck und resultierender Aufbewahrungszeit zugeordnet worden. Ergänzend sind stabiler Betrieb und Fehler- und Störungsbehebung in der Tabelle aufgelistet, eigene Anwendungsfälle erübrigen sich hierfür.

Anwendungsfälle	Personen-bezogene Zuordnung notwendig	Zweck 1: Daten -und Systemsicherheit	Zweck 2: Systemtechnik (z.B. Fehlerverfolgung)	Zweck 3: Arbeitsorganisation (z.B. Nutzung, Missbrauchskontrolle)
Anwendungsfall 1 Echtzeiterkennung	Ja	10 Tage		
Anwendungsfall 2 rückwirkende Erkennung von Angriffen	Ja	365 Tage		
Anwendungsfall 3	Ja	365 Tage		

[1] https://web.br.de/interaktiv/winnti/index.html

rückwirkende Erkennung Phishing				
Stabiler Betrieb	nein		30 Tage	
Fehler- und Störungsbehebung	nein		30 Tage	
Anwendungsfall 4 Anomysierte Statistiken	nein			30 Tage
Anwendungsfall 4 Auswertung wegen missbräuchlicher Nutzung	Ja, ab Stufe 3 der 59er			30 Tage für die zunächst anonymisierte Kontrolle. Bei Feststelung eines Verdachtsfalles dann für die Dauer der Aufklärung.

4. Organisatorische und technische Trennung nach Zwecken

Für Zweck 1 und für die Zwecke 2 und 3 sieht Dataport unterschiedliche Aufbewahrungssysteme vor.

Die Regelungen für den Zugang zu diesen Aufbewahrungssystemen sind vertraglich vereinbart und in der Arbeits- und IT-Organisation von Dataport entsprechend ausgeprägt.

Durch die unterschiedlichen Aufbewahrungssysteme und die zugehörigen Regelungen für den Zugang gewährleistet Dataport, dass die zu Sicherheitszwecken für einen längeren Zeitraum aufbwahrten Protokolldaten nicht für andere Zwecke genutzt werden können, für die nur eine kürzere Aufbewahrungsdauer vereinbart ist.

Personal, das mit Fehlerverfolgung sowie Auftragsverarbeitung im Rahmen der Arbeitsorganisation des Verantwortlichen (zum Beispiel Statistik, Nutzung, Missbrauchskontrolle) befasst ist, gehört nicht der Sicherheitsorganisation von Dataport an und hat daher maximal für 30 Tage rückwirkend Zugang zu der beschriebenen Internetprotokollierung. Für den Fall einer gezielten Kontrolle (ab Stufe 3 der Internet-Richtlinie) liefert das Personal für den beauftragten IP-Bereich, eventuell genannte URLs und während der beauftragten Zeit die beschriebene Internetprotokollierung an die zuständige Dienststelle. Eine längere Aufbewahrung ist bei Dataport auch in diesen Fällen nicht notwendig, diese obliegt der zuständigen Dienststelle selbst.

5. Begründung der benötigten Daten

Da sich die Angriffsarten unterscheiden, ergeben sich zwangsläufig unterschiedliche benötigte Informationen mit hohen Überschneidungen, um die IT-Infrastruktur und die Daten des Landes und damit auch die Daten der Mitarbeiterinnen und Mitarbeiter zu schützen. Unabhängig von der Art der Entdeckung lassen sich zwei Angriffsarten unterscheiden. Angriffe zielen entweder direkt auf IT-Systeme oder auf die Zugangsdaten von Personen.

5.1 Angriff auf IT-System

In diesem Fall versucht der Angreifer, die Kontrolle über ein System zu erlangen. Nachdem er die Kontrolle über ein System erlangt hat, kann er entweder versuchen, dieses System als Sprungbrett zu weiteren Systemen zu nutzen, die Daten dieses Systems anzugreifen oder das System zu nutzen, um

Zugangsdaten der Anwender*innen zu erbeuten und somit mittels der zugeordneten Rechte der Anwender*innen Daten zu entwenden, zu manipulieren oder zu verschlüsseln.
In diesem Fall sind folgende Informationen zur Bekämpfung und Feststellung des eingetretenen Schadens notwendig:

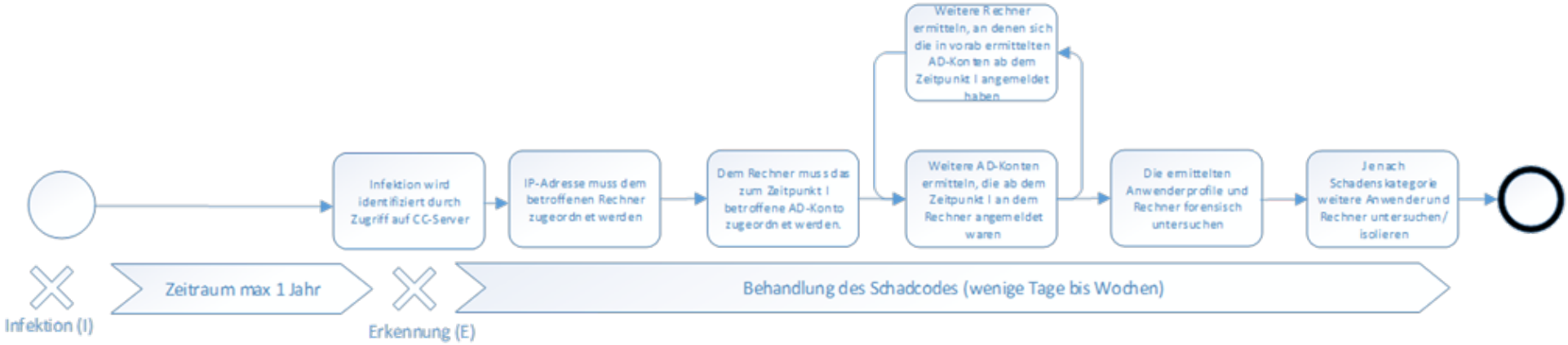
- Die IP-Adresse zum Zeitpunkt des Angriffs, um das eigentlich angegriffene System zu identifizieren
- Der Name des angegriffenen Systems, um dieses zu isolieren und betroffene Anwenderkennungen des Active Directorys (AD) zu identifzieren
- Die Anwenderkennungen, die sich im Zeitraum des Angriffs auf dem System angemeldet haben, um Betroffene zu warnen
- Weitere Rechner, an denen sich Betroffene angemeldet haben, um die Ausbreitung eines Angriffs zu bestimmen
- Die Organisation, der die betroffenen Anwender*innen aktuell angehören, um diese über den Angriff zu informieren und damit zu ermöglichen, dass diese eventuellen Meldepflichten (z. B. nach DSGVO/LDSG) nachkommen können.

5.2 Angriff auf Zugangsdaten (Phishing)

In diesem Fall versucht der Angreifer, Zugangsdaten von Personen zu erbeuten. Mittels der erbeuteten Zugangsdaten wird sich Zugriff in einem Netzwerk verschafft, um die regulär erteilten Rechte auf Systeme und Daten auszunutzen, um dann diese zu entwenden, zu manipulieren oder zu verschlüsseln.
In diesem Fall sind folgende Informationen zur Bekämpfung und Feststellung des eingetretenen Schadens notwendig:

- Die IP-Adresse zum Zeitpunkt des Angriffs, um die betroffene Kennung zu identifizieren
- Die Kennung, um diese zu deaktivieren und betroffene Anwender*innen zu informieren. Zusätzlich die durch die betroffene(n) Kennung(en) genutzten Systeme ab Zeitpunkt des Angriffs
- Weitere Rechner, an denen sich mit der betroffenen Kennung angemeldet wurde, um die Ausbreitung eines Angriffs zu bestimmen
- Die Organisation, der die betroffnene Anwender*innen aktuell angehören, um diese über den Angriff zu informieren und damit zu ermöglichen, dass diese eventuellen Meldepflichten (z. B. nach DSGVO/LDSG) nachkommen können

6. Erweiterte Darstellung zu der Aufbewahrung gemäß Zweck 1



7. Erfordernis für die Verarbeitung der Protokolldaten für Zweck 1 (Daten- und Systemsicherheit)

Für eine hinreichende Daten- und Systemsicherheit ergeben sich aus den obigen Anwendungsfällen folgende zu verarbeitende Daten mit den zugehörigen Aufbewahrungsfristen.

Entstehung	**Information**	**Verwendung**	**Aufbewahrungs-dauer in Tagen**
Firewall Protokoll http(s)	Datum, Uhrzeit	Ja unmittelbar	365
Firewall Protokoll http(s)	IP-Adresse des Arbeitsplatzes	Ja unmittelbar	365
Firewall Protokoll http(s)	HTTP-Methode[2]	Ja unmittelbar	365
Firewall Protokoll http(s)	Status/Fehlercode	Ja unmittelbar	365
Firewall Protokoll http(s)	Ziel URL	Ja unmittelbar	365
Firewall Protokoll http(s)	IP des Zielsystems	Ja unmittelbar	365
Firewall Protokoll http(s)	Datentyp[2]	Ja unmittelbar	365
Firewall Protokoll http(s)	Menge der übertragenen Daten	Ja unmittelbar	365
Firewall Protokoll ftp	Datum, Uhrzeit	Ja unmittelbar	365
Firewall Protokoll ftp	IP-Adresse des Arbeitsplatzes	Ja unmittelbar	365
Firewall Protokoll ftp	IP des Zielsystems	Ja unmittelbar	365
Firewall Protokoll ftp	Status/Fehlercode	Ja unmittelbar	365
Firewall Protokoll ftp	Menge der übertragenen Daten	Ja unmittelbar	365
Firewall Protokoll ftp	Namen der übertragenen Dateien	Ja unmittelbar	365
AD-Logdatei	Datum, Uhrzeit	Ja Verarbeitung	365
AD-Logdatei	IP-Adresse des Arbeitsplatzes	Ja Verarbeitung	365
AD-Logdatei	Computername des Arbeitsplatzes	Ja Verarbeitung	365
AD-Logdatei	Anmeldung Benutzerkonto am Arbeitsplatz	Ja Verarbeitung	365

[2] Bei HTTPS Zugriffen können die HTTP-Methode und der Datentyp nicht protokolliert werden.

Service Level Agreement

E-Mail SH (Fullmail)

Anlage 4 zu V2020-7 E-Mail für SH

Version: 2.0
Stand: 11.11.2020

Inhaltsverzeichnis

1 Einleitung

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Regelung von allgemeinen Rechten und Pflichten von Auftraggeber und Auftragnehmer.

Leistungsbeschreibungen (Kapitel 3): Inhaltliche Beschreibung der beauftragten Leistungen sowie der für einen reibungslosen Betrieb erforderlichen Dienstleistungen.

1.2 Leistungsgegenstand

Gegenstand dieses Service Level Agreements ist die Leistung E-Mail SH (Fullmail).

Die Leistungen werden hinsichtlich der Leistungsqualität und des Leistungsumfangs im Kapitel 3 beschrieben.

2 Rahmenbedingungen

2.1 Rollen

Es gibt folgende Rollen:

- Auftragnehmer und Auftragsverarbeiter (Dataport)
- Auftraggeber und Verantwortlicher laut DSGVO (ZIT SH)
- Beteiligte Stellen (am Landesnetz Anschlussberechtigte mit angebundenen Mailservern)

Der Auftraggeber kann gleichzeitig beteiligte Stelle sein, sofern er auch angebundene Mailserver verantwortet.

2.2 Mitwirkungsrechte und –pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Der Auftraggeber hat das Recht, globale Anpassungen zu beauftragen.

Die vom Auftragnehmer zugesagten Leistungen erfolgen daneben auf Anforderung einer beteiligten Stelle im Rahmen der globalen Festlegungen des Auftraggebers.

Die beteiligte Stelle hat das Recht, Dienstanpassungen im Rahmen der globalen Festlegungen des Auftraggebers für ihre eigene E-Mail-Domain zu beauftragen.

Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers sowie der beteiligten Stellen erforderlich.

Die beteiligte Stelle muss folgende Daten liefern und aktuell halten:

- Nennung der zum E-Mail-Versand genutzten Domains und Mailserver-IP-Adressen
- Name und E-Mail-Adresse des IT-Verantwortlichen der beteiligten Stelle, der berechtigt ist, Dienstanpassungen für die eigene E-Mail-Domain zu beauftragen, zum Beispiel, Einstellungen des E-Mail-Filters zu verändern bzw. zu beauftragen. Änderung der zentral vom Auftraggeber (ZIT SH) vorgegebenen Einstellungen und Filterungen sind nur in Abstimmung mit dem ZIT SH zulässig. Beauftragungen sind zu senden an dataportMailrouting@dataport.de
- Aktivierung der Empfänger-Validierung am Mailserver der beteiligten Stelle (wird empfohlen)
- Anpassen der DNS-Einträge, sofern die E-Mail-Domain von der beteiligten Stelle selbst verwaltet wird.

Die beteiligte Stelle darf ausschließlich das Dataport Mailrelay für ihren ausgehenden E-Mail-Versand nutzen, da nur so die Anschlussbedingungen des NdB-Netzverbundes eingehalten werden (§ 4 IT-NetzG).

2.3 Ansprechpartner

2.3.1 Störungsbearbeitung

Auftraggeber und beteiligte Stellen können sich bei technischen Störungen an das Dataport-Callcenter unter der Rufnummer 0431 3295-444 wenden. Der Auftragnehmer wird in seinem ITSM einen Incident erstellen.

Störungsannahme: Montag bis Freitag von 6:30 – 18:00 Uhr

Betriebszeit: Montag bis Donnerstag von 8:00 – 17:00 Uhr, Freitag von 8:00 – 15:00 Uhr

Kann die Störungsbehebung nicht innerhalb der normalen Bearbeitungszeit beendet werden, so wird die Bearbeitung am nächsten Werktag (Mo-Fr) fortgesetzt.

2.3.2 Technischer Ansprechpartner

Auftraggeber und beteiligte Stellen können sich bei technischen Fragen zum Produkt an dataportMailrouting@dataport.de wenden.

2.3.3 Vertraglicher Ansprechpartner

Bei vertraglichen Fragen wenden sich beteiligte Stellen an das ZIT SH.

3 Leistungsbeschreibung

3.1 E-Mail Transport

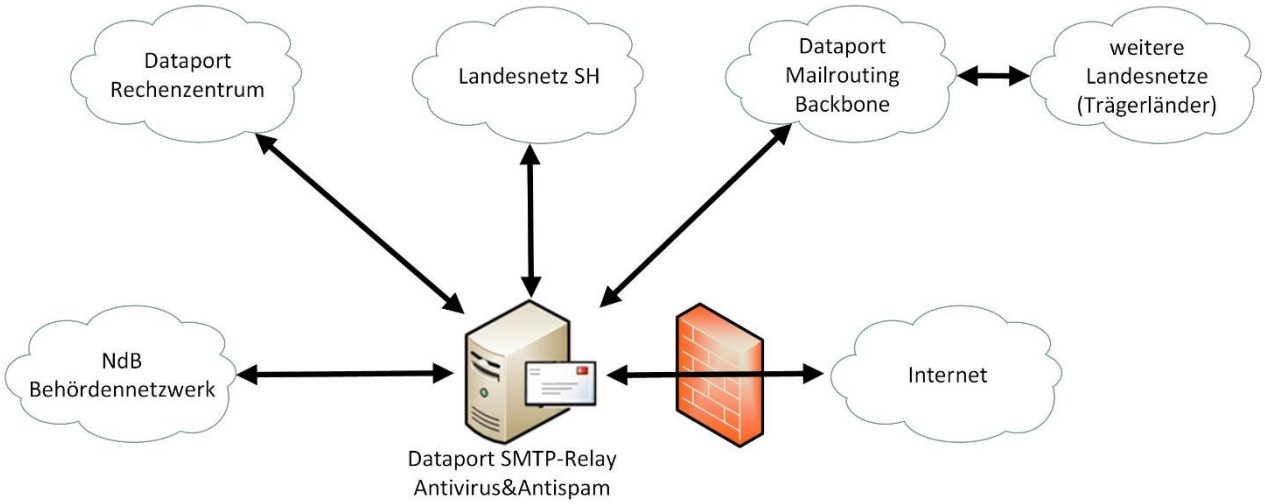
Die Ziele des Dienstes E-Mail SH lauten:

- Die Kommunikation ist so einfach wie möglich und unterstützt die Nutzer bei ihrer Arbeit
- Die Sicherheitsanforderungen des Landesnetzes SH werden erfüllt
- Sichere Kommunikation ist auch mit Teilnehmern außerhalb des Landesnetzes möglich.

In den folgenden Abschnitten wird beschrieben, welche Maßnahmen der Auftragnehmer im Auftrag des Verantwortlichen oder der beteiligten Stellen ergreift, um diese Ziele zu erreichen.

3.1.1 Übersicht

Der Auftragnehmer ermöglicht die E-Mail-Kommunikation der Systeme der beteiligten Stellen mit dem Internet. Hierbei betreibt die beteiligte Stelle i.d.R. einen eigenen E-Mail-Server im Landesnetz oder nutzt weitere Dienstleistungen des Auftragnehmers, welche ihm E-Mail-Server oder E-Mail-Postfächer zur Verfügung stellen. Beim E-Mail-Routing stellt der Auftragnehmer sicher, dass E-Mails aus verschiedenen Netzen (Internet, NdB, usw.) empfangen werden und an die Mailserver/Postfächer der beteiligten Stellen im Landesnetz weitergeleitet werden. Ebenso werden E-Mails von Clients oder Mailservern der beteiligten Stellen entgegengenommen und an ihr Ziel weitergeleitet.



Damit E-Mails aus dem Internet korrekt an die Mailserver der beteiligten Stellen übermittelt werden können, liefert die beteiligte Stelle neben ihrem Domainnamen die IP-Adresse des zuständigen Mailservers, an den die E-Mails durch den Auftragnehmer weitergeleitet werden. Sofern die DNS-Einstellungen der beteiligten Stelle selbst verwaltet werden, stellt Dataport diesem die korrekten Einstellungen hierfür zur Verfügung. Sofern die DNS-Einstellungen durch den Auftragnehmer verwaltet werden, nimmt der Auftragnehmer diese Änderungen selbständig vor.

3.1.2 Routing nur von gültigen Absenderadressen

Der Auftragnehmer prüft anhand der ihm bereitgestellten Informationen vom Auftraggeber bzw. der beteiligten Stelle, dass Absenderdomains gültig sind, bevor diese vom Mailrelay des Auftragnehmers angenommen und weitergeroutet werden. So werden ausschließlich gültige Domains als Senderadresse aus internen Netzen akzeptiert.

Der Auftragnehmer implementiert die Regel, dass Senderdomains nur von den Eigentümern der jeweiligen Domains verwendet werden dürfen.
Die beteiligte Stelle teilt dem Auftragnehmer mit, welche Kombinationen von IP-Adressen und Domains zum Versand von E-Mails verwendet werden. Der Auftragnehmer transportiert nur E-Mails mit diesen genannten Kombinationen.

3.1.3 Routing an existierende Zieladressen

Es ist für den Auftragnehmer aufgrund der dezentralen Organisation der Mailserver im Landesnetz nicht ohne weiteres möglich, bei der Annahme einer E-Mail festzustellen, ob das Postfach auf dem Zielserver auch existiert. Der Mechanismus der Empfänger-Validierung ermöglicht es, die Existenz der Zielpostfächer schon vor Annahme der E-Mail zu überprüfen und nur bei erfolgreicher Rückmeldung zuzustellen.

Die beteiligten Stellen sind verpflichtet, sofern technisch möglich, die Empfängervalidierung auf ihren Mailservern zu aktivieren.

3.1.4 Ablehnen von internen Adressen/Domains aus dem Internet

Der rechtmäßige Ursprung einer E-Mail mit einer Landesnetz-Adresse kann nur im Landesnetz liegen, denn nur diese Systeme sind berechtigt, Nachrichten im Namen dieser Domänen zu versenden. Im Einzelfall betreiben jedoch auch beteiligte Stellen Webserver im Internet, die im Einzelfall autorisiert werden sollen, die Landesnetz-Domäne der beteiligten Stelle als E-Mail-Absender von definierten IP-Adressen aus dem Internet zu verwenden.

Der Auftragnehmer nimmt standardmäßig keine E-Mails mit internen Absenderadressen aus dem Internet entgegen. Die E-Mail wird direkt am Internetübergang durch einen REJECT-Fehlercode abgewiesen und gelangt nicht in den Verantwortungsbereich des Auftragnehmers bzw. eines Systems der beteiligten Stelle. Die beteiligte Stelle kann für einzelne Internet-IP-Adressen eine Ausnahme von dieser Regel per E-Mail an Dataport beauftragen, um einzelne Kombinationen aus Quell-IP-Adresse und Domain des Teilnehmers im Einzelfall zu autorisieren.

3.1.5 Kennzeichnung von Nachrichten aus externen Netzen

Der Auftragnehmer kennzeichnet eingehende E-Mails aus Drittnetzen (Internet oder NdB) im Betreff durch ein vorangestelltes [EXTERN] im Betreff der E-Mail.

3.1.6 Routing in NdB (Netze des Bundes)

Alle Domains, die Bestandteil dieses Vertrages sind, werden durch den Auftragnehmer automatisch als Teilnehmer am NdB-Netz gemeldet. Somit ist es möglich, dass deutsche Verwaltungen bundesländerübergreifend über die sichere Infrastruktur der deutschen Verwaltungen ihre E-Mails austauschen, ohne dass diese über das Internet gesendet werden.

Der Auftragnehmer implementiert das Routing zum NdB laut dem Leitfaden „Sichere E-Mail-Kommunikation im VN“ der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS).
Da die beteiligte Stelle ausschließlich das Dataport Mailrelay für ihren ausgehenden E-Mail-Versand nutzen darf (laut Abschnitt 2.2), ist ein synchrones Routing sichergestellt.
Der Auftragnehmer stellt dem Auftraggeber ein Verzeichnis aller Domains, die Bestandteil dieses Vertrages oder Teilnehmer am NdB-Netz sind, zur Verfügung.

3.2 E-Mail Filterung

3.2.1 Mögliche Gefahren

Die E-Mail-Kommunikation ist mit einer Vielzahl an möglichen Gefahren verbunden, welche durch die E-Mail-Filterung eingedämmt werden sollen. Unerwünschte E-Mails, z.B. SPAM, Viren/Trojaner (nachfolgend Schadsoftware/Malware genannt) oder ausführbare Dateien werden hierbei besonders betrachtet.

Der Auftragnehmer hat die Einhaltung gesetzlicher Vorgaben insbesondere des TKG sicherzustellen. Dies bedeutet u.a. dass:

- empfangene E-Mails dem Empfänger stets zugestellt werden
- Inhalte von E-Mails niemals verändert werden
- der Auftragnehmer sich über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus keine Kenntnis vom Inhalt der Kommunikation verschafft

Dies macht es erforderlich, möglichst viele SPAM-E-Mails und E-Mails mit gefährlichen Inhalten schon vor dem Empfang abzulehnen. In den nachfolgend dargestellten Verfahren erfolgen Überprüfungen bzw. Auswertungen ausschließlich automatisiert.

3.2.2 Maßnahmen gegen gefährliche Anlagen

Anlagen von E-Mails stellen ein potenzielles Sicherheitsrisiko dar, insbesondere wenn es sich hierbei um ausführbare Dateien z.B. (.exe, .com, .pif, .scr, usw.) handelt. Bei diesen Dateien kann es sich um Schadcode handeln, der unbemerkt den PC des Empfängers infizieren und z.B. schutzwürdige Daten stehlen könnte.

Dateiformate, die Makros oder andere aktive Inhalte enthalten können, stellen ein erhöhtes Sicherheitsrisiko dar. Der Auftragnehmer gewährleistet, dass E-Mails mit solchen Anlagen gemäß einer bedarfsgerecht nach Möglichkeit mit den zentralen Informationssicherheitsbeauftragten der Trägerländer abgestimmten Liste an der Firewall abgewiesen werden. Für SH trifft der Auftraggeber die Entscheidung über abzuweisende Formate. Das direkte Abweisen der Mail führt zu einer Fehlermeldung an den Absender.

Eine vollständige Liste der gesperrten Dateierweiterungen kann tagesaktuell beim Auftragnehmer angefordert werden. Der Auftraggeber stellt je nach Bedarf diese Liste den Anwenderinnen und Anwendern zur Verfügung.

Erlaubte Dateianhänge werden im nächsten Schritt mithilfe eines Virenscanners untersucht. Sofern Schadsoftware erkannt wurde, führt dies ebenfalls zum direkten Abweisen der E-Mail mit einer Fehlermeldung an den Absender.

Der Auftragnehmer gewährleistet, dass der Virenscanner stets auf dem neuesten Stand ist.

Die vorstehend beschriebenen Prüfungen und Abweisungen von potenziell gefährlichen Anlagen führt der Auftragnehmer am Übergang aus dem Internet und dem NdB durch.

3.2.3 Maßnahmen gegen SPAM

Neben den direkten Gefahren durch Anlagen werden im Folgenden alle weiteren Formen unerwünschter Inhalte wie z.B. Massenwerbung oder auch E-Mails mit gefährlichen Links allgemein als SPAM bezeichnet.

Der Auftragnehmer setzt im Auftrag des Auftraggebers eine Vielzahl von Maßnahmen ein, die eng miteinander verzahnt sind und in ihrer Summe zu einem wirksamen Spamschutz beitragen. Zu diesen Maßnahmen gehören u.a. die Prüfung auf die Einhaltung des SMTP-Protokolls laut RFC-Vorgaben, DNS-Blacklists, Greylisting, Content-Filterung, Reputationsdatenbanken sowie manuell erstellte Filter.
Der Auftragnehmer führt selbständig Feinanpassungen durch, um die vereinbarte Leistung angepasst an die aktuelle Bedrohungslage zu erbringen.
Da sich die Muster der SPAM-Mails oftmals stündlich verändern, ist es nicht auszuschließen, dass – insbesondere zu Beginn einer neuen Welle - einige der ersten SPAM-Mails an die Empfänger zugestellt werden. Für diesen Fall stellt der Auftragnehmer dem Auftraggeber und den beteiligten Stellen ein Service-Postfach zur Verfügung, über das SPAM-Mails gemeldet werden können, um die Filterregeln der Spam-Erkennung zu verbessern. (siehe 3.2.7).

3.2.4 Ablehnen von unerwünschten E-Mails gemäß Ziffern 3.2.1 – 3.2.3

Die Erkennung auf unerwünschte E-Mails führt der Auftragnehmer während des Empfangsprozesses durch, bevor dieser abgeschlossen wurde. Entscheiden die umfangreichen Prüfmechanismen, dass es sich um eine unerwünschte E-Mail handelt, so erhält der aus dem Internet einliefernde Mailserver umgehend (vor der Empfangsquittierung) eine entsprechende Fehlermeldung (REJECT), sodass die E-Mail nicht in den Verantwortungsbereich des Auftragnehmers und somit auch nicht nachgelagert in den Verantwortungsbereich der beteiligten Stellen gelangt. Laut RFC-Vorgaben erhält der Absender von seinem Provider (E-Mail-Dienstleister) eine entsprechende Fehlermeldung, dass die E-Mail nicht zugestellt werden konnte. Sollte es sich hierbei um eine Fehleinstufung handeln, so stehen die in 3.2.6 beschriebenen Maßnahmen zur Verfügung, um die E-Mail bei einem erneuten Zustellungsversuch dennoch zuzustellen.

3.2.5 Ausnahmedefinition

In einigen Ausnahmefällen kann es jedoch gewünscht sein, dass bestimmte Postfächer von der zuvor beschriebenen Filterung ausgenommen werden. Gemäß Abschnitt 2.2 kann der jeweils berechtigte Ansprechpartner der beteiligten Stelle über das Funktionspostfach dataportMailrouting@dataport.de eine Filter-Ausnahme beantragen. Hierbei ist es möglich für einzelne Empfängeradressen oder Domains die Spam-Filterung, die Filterung von gefährlichen Anhängen (banned content) oder auch die Virenfilterung abzuschalten, sodass die Inhalte ungefiltert das Empfängerpostfach erreichen. Dataport informiert das zentrale Informationssicherheitsmanagement des Auftraggebers über das Funktionspostfach sicher@melund.landsh.de unverzüglich über derartige Ausnahmen.

Das erhöhte Risiko trägt der berechtigte Ansprechpartner der beteiligten Stelle.

3.2.6 Zustellung von Mails im Ausnahmefall / False-Positives

Es kann im Einzelfall vorkommen, dass eine E-Mail fälschlicherweise als SPAM klassifiziert und abgelehnt wird. Ebenso kann der Fall eintreten, dass z.B. eine legitime .exe Datei an einen Empfänger im Landesnetz zugestellt werden soll.

Um Anlagen aus dem Internet zu empfangen, die aufgrund der in 3.2.2 bis 3.2.4 beschriebenen Maßnahmen generell blockiert werden würden, z.B. „programm.exe“ ist es ausreichend, wenn der Absender die Datei z.B. in „programm.xxx“ umbenennt. Der Empfänger muss die ursprüngliche Benennung wiederherstellen, um das Programm ausführen zu können. Eine weitere Möglichkeit stellt die Verschlüsselung der Anlage mit einer zusätzlichen Software dar (z.B. WinZIP). Bei Versand einer Datei z.B. „programm.exe“ in einer verschlüsselten Archivdatei z.B. „archiv.zip“ oder „archiv.rar“ ist darauf zu achten, dass auch die Dateinamen verschlüsselt werden, da ansonsten die Prüfung des Archives die erhaltene „.exe“ Datei anhand des Namens erkennen würde.

Sollte eine E-Mail aus anderen Gründen nicht den Empfänger erreichen, wird der Auftragnehmer das Problem nach Erstellung eines Störungstickets durch das Dataport Callcenter zu beheben versuchen.

3.2.7 SPAM melden

Da sich die Muster der SPAM-Mails oftmals stündlich verändern, ist es nicht auszuschließen, dass dennoch gelegentlich eine SPAM-Mail zugestellt wird. ZIT SH und beteiligte Stellen gewährleisten durch entsprechende Informationen und Sensibilisierungen der Postfachnutzer, dass die betreffende E-Mail zur Analyse an spam@landsh.de gesendet werden. Es ist hierbei wichtig, dass die E-Mail als Anhang versandt wird (nicht mittels „weiterleiten“), damit die ursprünglichen Kopfzeilen der SPAM-E-Mail erhalten bleiben (In Outlook ist die betreffende Mail zu markieren und dann STRG+ALT+F zu drücken, um die E-Mail als Anlage weiterzuleiten). Der Auftragnehmer wird so besser in die Lage versetzt, die Filterregeln zu verbessern.

3.2.8 Regelmäßige Anpassung der Filterregeln

Der Auftragnehmer passt im Rahmen des laufenden Betriebs die bestehenden Filterregeln entsprechend diesem SLA eigenständig an. Dies umfasst u.a. die Erstellung und Anpassung von Content-Filter Regeln, das manuelle Erstellen von Blockier-Regeln von Spam-Versendern, z.B. anhand der Absenderadresse, der einliefernden IP-Adresse bzw. des IP-Subnetz aus dem Internet, etc. Eine gesonderte Benachrichtigung des Auftraggebers bzw. der beteiligten Stellen bei Anpassungen dieser Regeln ist nicht vorgesehen.

3.2.9 Zukünftige Anpassungen

Grundlegende Änderungen der Filtermaßnahmen, z.B. dem Einsatz neuer Techniken, werden dem Auftraggeber zur Anwendung empfohlen und nach Beauftragung durchgeführt.

3.2.10 Filterregeln abhängig von der Quelle

Die vorhergehende Beschreibung bezieht sich im Regelfall auf E-Mails, die aus dem Internet empfangen werden, da hier die Hauptbedrohung zu erwarten ist.

Auch E-Mails aus Drittnetzen, wie z.B. dem NdB (Netze des Bundes) werden auf Bedrohungen untersucht, jedoch mit toleranteren Filterregeln bearbeitet.

Auch ausgehende E-Mails von Mailservern, die Bestandteil dieses Vertrages sind, an andere Teilnehmer im Landesnetz oder an Drittnetze, wie z.B. das Internet, werden auf SPAM/Schadsoftware untersucht, jedoch ebenfalls mit toleranten Filterregeln. Dies ist notwendig, um einen ausgehenden SPAM-Versand zu vermeiden und dient gleichzeitig der Reputationssicherung der beteiligten Stellen als Absender von E-Mails. Die Filterung von ausgehenden E-Mails erfolgt z.T. im Post-Queue Verfahren, d.h. die E-Mail wird ggf. zunächst durch das Mailsystem des Auftragnehmers angenommen und nach Spam-Einstufung zurückgewiesen (BOUNCE). Dieses Verhalten ist jedoch nur in Sonderfällen (ausgehender SPAM-Versand) zu erwarten.

3.3 Protokollierung

Von einer transportierten E-Mail werden folgende Daten in eine Logdatei geschrieben: Datum, Uhrzeit, Einliefernder Host (Name+IP) , Absender-Adresse, Empfänger-Adresse, Menge der übertragenen Daten, Statuscode, Mail-ID auf dem nächsten Mailserver, Prüfungen der Spambewertung (welche Regeln haben angeschlagen) + Diagnoseinformationen zur Spam/Virenprüfung, bei Anhängen (Dateiname und Typ des Anhangs), Betreff der E-Mails.

Nach 10 Tagen werden die protokollierten Daten gelöscht. Sofern Logdaten sich im Verlauf der 10 Tage als relevant für die Bearbeitung eines Incidents herausstellen, werden diese von der Löschung ausgenommen und erst nach Abschluss des Incidents gelöscht.

4 Glossar

Content-Filterung – eine E-Mail besteht aus Kopfzeilen (Header) mit Angaben zum Transport der E-Mail und dem eigentlichen zu übertragenden Inhalt (Content). Dieser Inhalt kann automatisiert von Anti-Spam- und Anti-Viren-Software untersucht und bewertet werden.

DNS – (Domain Name System) – ein Namensdienst, der die Zuordnung von Domainnamen (z.B. landsh.de) zu ihren IP-Adressen verwaltet. Für die Zustellung von E-Mails ist es erforderlich, dass im DNS zum Domainnamen die richtige IP-Adresse des zuständigen Mailservers hinterlegt wird.

DNS-Blacklist (RBL) - eine Liste von IP-Adressen, die dafür bekannt sind, dass über die zugehörigen Server unerwünschte Spam- oder Schadcode-Mails versendet werden. Wird laufend erneuert und nicht mehr aktive Server werden meist nach 24 Stunden wieder von der Liste entfernt.

DOI – Deutschland-Online-Infrastruktur. Der Begriff DOI ist veraltet. Das Netz wurde durch das NdB (Netze des Bundes) abgelöst.

Greylisting – eine RFC-konforme Möglichkeit die Annahme von E-Mails von unbekannten Servern zu verzögern. Bis zum Zeitpunkt des erneuten Einlieferungsversuchs ist der einliefernde Server eventuell bereits als Spamversender in einschlägigen Reputationsdatenbanken erkannt worden. Diese Maßnahme trägt zur Spamvermeidung bei und hat keine Auswirkungen auf regelmäßige Kommunikation.

Phishing E-Mail – E-Mails, ähnlich wie Spam-E-Mails versendet, aber einen seriösen Hintergrund vortäuschend, um den Empfänger zu Eingabe persönlicher Daten (Bankdaten, Passwörter aller Art) zu bewegen und somit „abzufischen“. Oft wird ein gewisser Zeitdruck vorgetäuscht, damit der Empfänger nicht zu lange über die Authentizität nachdenkt.

Mailrelay – ein Mailserver, der E-Mails für nachgelagerte Server entgegennimmt und an diese weiterleitet.

NdB – Netze des Bundes, eine deutschlandweite Kommunikations-Infrastruktur für alle Behörden der Deutschen Verwaltung, siehe auch http://www.bva.bund.de.

MX-Record – der MX-Record einer Domain zeigt im DNS auf den Namen bzw. die IP-Adresse des Servers, der E-Mails für diese Domain entgegennimmt.

Reputationsdatenbanken – Eine öffentliche Datenbank, welche typische Merkmale von Spam-Versendern oder Spam-Mails enthält. Dies sind z.B. IP-Adressen von Spam-versendenden Servern oder eine Datenbank mit Hash-Werten bekannter Spam-Signaturen.

REJECT – bezeichnet die Abweisung einer E-Mail vor der endgültigen Empfangs-Quittierung. Dies hat nicht nur Performance-Gründe, sondern verhindert auch, dass eine E-Mail in den Verantwortungsbereich des Auftragnehmers gerät und nach dem Telekommunikationsgesetz zwingend zugestellt werden muss.

RFC – Request For Comment, aber deutlich mehr als nur ein Vorschlag für die Umsetzung eines Internet-Dienstes, sondern eher eine Referenz bzw. Spezifikation wie dieser Dienst umzusetzen ist, damit alle Internet-Teilnehmer diesen Dienst nutzen können (RFC-Konformität).

Routing – Weiterleitung, Beförderung, z.B. von E-Mails durch ein Mailrelay

Schadcode – Programmcode (aber z.B. auch bösartige Office-Macros), der für den Benutzer unerwünschte bzw. schädliche Aktionen oftmals unbemerkt ausführt. Der Schadcode kann z.B. Daten

löschen oder schutzwürdige Daten (Zugangsdaten, personenbezogene Daten) an Dritte im Internet senden.

Spam – Spam- oder Junk-Mail sind unerwünschte E-Mails, die meistens in Massen verschickt werden und unverlangte Werbung, meist mit unseriösen Angeboten, enthalten. Die Grenze zu Phishing-Mails ist fließend.

TKG – Telekommunikationsgesetz – Das TKG regelt technische Aspekte der Telekommunikation, insbesondere sollen das Fernmeldegeheimnis und der Datenschutz bei einer Telekommunikation gewährleistet werden.

Service Level Agreement

Internet-Zugang über die Dataport FW-Infra SH

Anlage 4 zum Vertrag V15861 zur Internet-Nutzung SH

Version: 1.0
Stand: 01.01.2021

Inhaltsverzeichnis

1 Einleitung

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Regelung von allgemeinen Rechten und Pflichten von Verantwortlichem und Auftragsverarbeiter im Rahmen dieser Leistungsbeschreibung.

Leistungsbeschreibungen (Kapitel 3): Inhaltliche Beschreibung der bereitgestellten Leistungen sowie der für einen reibungslosen Betrieb erforderlichen Dienstleistungen.

1.2 Leistungsgegenstand

Gegenstand dieses Service Level Agreements ist die Leistung „Internet-Zugang über die Dataport FW-Infra SH“.

Die Leistungen werden hinsichtlich der Leistungsqualität und des Leistungsumfangs im Kapitel 3 beschrieben.

2 Rahmenbedingungen

2.1 Rollen

Es gibt folgende Rollen:

- Auftragnehmer und Auftragsverarbeiter (Dataport)
- Auftraggeber und Verantwortlicher laut DSGVO (ZIT SH)
- Beteiligte Stellen
  Das sind am Landesnetz Anschlussberechtigte, die den Internetzugang über die mit diesem Vertrag beauftragte Firewall-Infrastruktur nutzen.
  a) Dies sind in erster Linie Behörden und Dienststellen der unmittelbaren Landesverwaltung.
  b) Beteiligte Stellen, die nicht der unmittelbaren Landesverwaltung angehören, können den Internetzugang im Rahmen eigener Verträge mit Dataport nutzen. Das im Rahmen dieses Vertrages vorgegebene, generelle Regelwerk ist dabei zu beachten. Auf Anforderung des Auftraggebers stellt Dataport diesem die Information über diese beteiligten Stellen zur Verfügung.

2.2 Mitwirkungsrechte und –pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen im Rahmen dieser Leistungsbeschreibung sowie auf gesonderte Anforderung des Auftraggebers. Der Auftragnehmer ist berechtigt, technisch notwendige Anpassungen an der Leistung „Internet-Zugang über die Dataport FW-Infra SH“ vorzunehmen. Der Auftragnehmer informiert den Auftraggeber unverzüglich und stimmt sich nach Möglichkeit mit dem Auftraggeber ab. Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers erforderlich. Der Auftraggeber muss folgende Daten liefern und aktuell halten:

- Name und E-Mail-Adresse des IT-Verantwortlichen, der berechtigt ist, generelle Einstellungen der Proxy-Konfigurationen zu beauftragen. Beauftragungen sind zu senden an DataportZentralerInternetzugang@dataport.de

- Nennung der beteiligten Stellen entsprechend 2.1 a) und der dort Verantwortlichen. Der Auftraggeber ist selbst gleichzeitig beteiligte Stelle.

- Nennung und fortlaufende Aktualisierung der für den Internet-Zugang genutzten IP-Adressen bzw. Netzkreise einschließlich der jeweiligen organisatorischen Zuordnung zur Behördenhierarchie des Landes und der Netzverantwortlichen (Kommunikationskoordination - KomKo), damit die aus diesen Strukturen abgeleitete Datenverarbeitung, insbesondere gesonderte URL-Filterung, Erstellung der TOP 30 Listen usw., verwaltungsorganisatorisch korrekt erfolgen kann.

Die beteiligten Stellen arbeiten bei der Säuberung von infizierten Clients (Schadcode / Malware) mit. Auch bei technischen Änderungen gemäß Absatz 1 besteht auf Seiten der beteiligten Stelle eine Mitwirkungs- und Anpassungspflicht auf ihrer Seite und zu ihren Lasten, soweit erforderlich.

2.3 Ansprechpartner

2.3.1 Störungsbearbeitung

Bei technischen Störungen wenden sich Verantwortliche der beteiligten Stellen an das Dataport-Callcenter unter der Rufnummer 0431 3295-444.
Callcenter Störungsannahme: Montag bis Freitag von 6:30 – 18:00 Uhr

Betreute Betriebszeit: Montag bis Donnerstag von 8:00 – 17:00 Uhr, Freitag von 8:00 – 15:00 Uhr

Kann die Störungsbehebung nicht innerhalb der normalen Bearbeitungszeit beendet werden, so wird die Bearbeitung am nächsten Werktag (Mo-Fr) fortgesetzt.

2.3.2 Technischer Ansprechpartner

Bei technischen Fragen zur vereinbarten Leistung wenden sich Verantwortliche der beteiligten Stellen an DataportZentralerInternetzugang@dataport.de.

2.3.3 Vertraglicher Ansprechpartner

Bei vertraglichen Fragen zum Produkt wendet sich der Auftraggeber an Vertrieb@dataport.de

3 Leistungsbeschreibung

3.1 Internet-Dienste

Der Zugang zum Internet wird über eine mehrfach gesicherte Firewall-Infrastruktur zentral für das Landesnetz Schleswig-Holstein bereitgestellt. Das vorliegende Dokument beschreibt die Leistungsmerkmale der zentral implementierten Dienste.

Dataport bietet den Zugang zu ausgewählten Diensten (http, https, ftp) des Internet.
Die Planung und den Betrieb dieser Infrastruktur verantwortet Dataport als Auftragsverarbeiter im Auftrage des Landes Schleswig-Holstein, vertreten durch den Auftraggeber.

3.2 Leistung

Das Produkt "Dataport FW-Infra SH" besteht aus mehreren Komponenten: Externe und interne Paketfilter sichern das dazwischenliegende Netzsegment, in dem Proxies (Application Layer Gateways) für Dienste auf Basis der Protokolle http(s) und FTP bereitgestellt werden. Alle Komponenten sind zur Erhöhung der Verfügbarkeit redundant ausgelegt (teilweise mehrfach zwecks Lastverteilung).

Dataport betreibt die erforderlichen Netz- und Systemkomponenten in sicheren Systemräumen. Durch technische und organisatorische Maßnahmen ist der Zugang zu diesen Komponenten streng reglementiert. Der administrative Zugang ist auf wenige Personen beschränkt und wird vollständig protokolliert.

Die Produktkomponenten (Paketfilter und Proxies) schützen das Netz von Dataport und die Teilnehmernetze am Landesnetz Schleswig-Holstein durch Einschränkung der Verbindungen zum Internet. Dies geschieht durch unterschiedliche Maßnahmen, die auf verschiedenen Ebenen Sicherheitsfunktionalitäten implementieren. Hierzu gehören unter anderem die Beschränkung auf zulässige Dienste, die Einhaltung definierter Protokolle, die Erzwingung des technisch konformen Verbindungsaufbaus sowie die Überprüfung der Zugehörigkeit von IP-Paketen zu bestehenden Verbindungen.

Eine Protokollierung der Nutzung der Dienste (Nutzungs-, Verkehrs- und Inhaltsdaten) erfolgt und ist erforderlich

1. aus Gründen der Daten- und Systemsicherheit,
2. aus Gründen der Systemtechnik (z.B. zur Fehlerverfolgung) und
3. aus Gründen der Arbeitsorganisation des Auftraggebers (z.B. zur Feststellung von Art und Umfang der Nutzung und zur Missbrauchskontrolle)

Die unter den Punkt 3 erhobenen Daten werden anonymisiert zu statistischen Zwecken in Protokollen gespeichert. Die Analyse und Erstellung von Statistiken erfolgt durch die Firewall-Administration.
Eine Herausgabe von Daten an den Auftraggeber ist außer aus dem Grund 3. ausdrücklich ausgeschlossen.

Die sicherheitstechnischen Rahmenbedingungen, das Schutzniveau und die protokollierten Informationen des hier beschriebenen Produktes sind im Sicherheitskonzept Dataport-Firewall 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. Das Sicherheits- und Betriebskonzept kann auf Wunsch bei Dataport eingesehen werden.

3.3 Eingesetzte Hard- und Software

Das Produkt basiert auf Open Source Komponenten und kommerziellen Produkten, mit deren Hilfe sich die gewünschten Leistungsmerkmale erzielen lassen. Bei der Auswahl werden viele Kriterien wie z.B. Sicherheit, Updatezyklen, Leistungsfähigkeit usw. von Dataport bewertet und dann eine Entscheidung von Open Source Programmen oder kommerziellen Produkten getroffen. Diese Bewertung wird in gewissen Abständen oder angesichts neuer Anforderungen neu durchgeführt, so dass sich die eingesetzten Pakete und Produkte ändern können. Dataport stimmt Änderungen mit dem Auftraggeber ab.

3.4 Funktionsumfang

Angeboten wird der Zugang zu den Diensten Internet („surfen“, also http, https), und Dateitransfer (FTP). Für beide Dienste erfolgt der Zugriff über sogenannte Proxy-Server. Der Proxy-Server setzt die Kommunikation zwischen dem Endanwender und dem Ziel im Internet um. Dadurch kommt es zu keiner direkten Verbindung zwischen dem genutzten Client und dem Internet.

Dataport ist mit zwei redundanten Verbindungen an das Internet angeschlossen. Dataport überwacht die Auslastung zum Internet und rät dem Auftraggeber bei langfristig höherem Bedarf, einen Ausbau der Infrastruktur und Bandbreite zu beauftragen.

3.5 Sicherheit

Um gegen aktive Angriffe aus dem Internet gesichert zu sein, betreibt Dataport die FW-Infra SH als geschützte und schützende Infrastruktur. Durch diesen Zugang können aus dem Internet keine direkten Zugriffe in die internen Netze und damit auch nicht bis zu einem Arbeitsplatzrechner vordringen. Ein Außenstehender kann keine Verbindung zu einem internen Server oder Client aufbauen.

Das Firewall-System bietet nur für von den im Rahmen des Betriebs des Landesnetzes benannten Netzverantwortlichen zugelassene Netzwerke und Clients den Zugriff auf das Internet. Die Verbindung eines internen Netzes bzw. eines Clients aus diesem Netz zum Internet erfolgt nicht direkt, sondern stellvertretend durch die Proxy-Server.

Wird Dataport davon in Kenntnis gesetzt oder erhält Dataport durch eigene Überwachungsmaßnahmen davon Kenntnis, dass Clients im Landesnetz von Schadcode befallen sind, informiert Dataport den zuständigen Informationssicherheitsbeauftragten oder, sofern dieser nicht ermittelt oder erreichbar ist, benannten IT-Verantwortlichen.
Dataport hat als Auftragsverarbeiter das Recht, aus Gründen der Daten- und Systemsicherheit Clients umgehend zu sperren. Dataport informiert den Verantwortlichen und dessen Informationssicherheitsbeauftragte unverzüglich über solche Maßnahmen. Die Sperrung dient dem Schutz vor Datendiebstahl aus dem Landesnetz sowie der Reputationssicherung der Dataport Firewalls (Gefahr des IP-Blacklistings).
Ebenso behält sich Dataport vor, in Zusammenarbeit mit dem Verantwortlichen und dessen Informationssicherheitsbeauftragten Webseiten zu sperren, die mit hoher Wahrscheinlichkeit Schadcode anbieten, verteilen oder aus internen Netzen gestohlene Daten annehmen. Sollte eine Abstimmung nicht zeitnah möglich sein oder eine hohe Bedrohungslage bestehen, sperrt Dataport die Webseiten eigenständig und informiert im Nachgang den Verantwortlichen und dessen Informationssicherheitsbeauftragten.

3.6 Sicherheitskonzept

Dataport betreibt die Dataport FW Infra SH angelehnt an BSI Grundschutz.

3.7 Systemausfälle

Der Zugang zum Internet ist durchgehend verfügbar. Durch technische Maßnahmen (redundante Auslegung aller Systeme (automatische Überwachung und automatisches Fallback auf Backup-Systeme) wird versucht, die Auswirkung von Systemausfällen zu minimieren.

Dataport behält sich vor, Firewalls vom Netz zu trennen, wenn Angriffe aus dem Internet auftreten oder die konkrete Vermutung besteht, dass Systeme unberechtigt genutzt werden, um z.B. interne Netze anzugreifen. Dataport informiert unverzüglich den Verantwortlichen und dessen Informationssicherheitsbeauftragten.

3.8 Protokollierung

Folgende Verbindungsdaten werden laufend protokolliert zu folgenden Zwecken:

1. aus Gründen der Daten- und Systemsicherheit,
2. aus Gründen der Systemtechnik (z.B. zur Fehlerverfolgung) und
3. aus Gründen der Arbeitsorganisation des Auftraggebers (z.B. zur Feststellung von Art und Umfang der Nutzung und zur Missbrauchskontrolle)

HTTP(S): Datum, Uhrzeit, IP-Adresse des Arbeitsplatzes, HTTP-Methode, Status/Fehlercode, Menge der übertragenen Daten, URL (bei verschlüsselten Verbindungen nur die Domain selbst, ohne Parameter), IP des Zielsystems, Datentyp von heruntergeladenen Dateien.

Bei HTTPS Zugriffen können die HTTP-Methode und der Datentyp nicht protokolliert werden, da diese Bestandteile im verschlüsselten Datenstrom übertragen werden und für den Proxy nicht auswertbar sind.

FTP: Datum, Uhrzeit, IP-Adresse des Arbeitsplatzes, Ziel-IP, Status/Fehlercode, Menge der übertragenen Daten, Namen der übertragenen Dateien

Die hier aufgezählten Werte sind nicht abschließend und können von Dataport aus Gründen der Daten- und Systemsicherheit und aus Gründen der Systemtechnik angepasst werden. Der Auftraggeber muss der Anpassung zustimmen.
Ausdrücklich ausgeschlossen hiervon sind aufgrund des hohen Schutzwertes Inhaltsdaten der Verbindungen.

Die Aufbewahrung der Daten erfolgt je nach Zweckbindung unterschiedlich, sowohl hinsichtlich des Speicherortes als auch hinsichtlich der Speicherdauer. Dataport vergibt die Zugriffsrechte auf die Protokolldaten restriktiv.
Dataport gibt die Protokolldaten nur auf Grundlage richterlicher Beschlüsse oder gesetzlicher Grundlagen an Dritte heraus.
Die Herausgabe an den Auftraggeber und an die beteiligten Stellen erfolgt ausschließlich aus Gründen der Systemtechnik im Rahmen einer Störungsbearbeitung und aus Gründen der Arbeitsorganisation. Letzteres beinhaltet die Herausgabe anonymisierter Statistiken (gemäß 4.).

Für die Herausgabe nicht-anonymisierter Daten im Falle der missbräuchlichen Nutzung müssen der genaue Zweck, der Umfang, der Zeitraum der von Dataport zu übermittelnden Protokolldaten und

deren Auswertung festgelegt sein. Der Auftraggeber beauftragt Dataport mit der Lieferung dieser Protokolldaten an die anfordernde, beteiligte Stelle gemäß 2.1 a).

Um zu ermitteln, welche Clients und Konten von potentiellen Angriffen betroffen sind, kann es notwendig sein, weitere Datenquellen zur Kontextherstellung hinzuziehen. Dataport ist ermächtigt, die bereits erhobenen Daten des zentralen Authentifizierungsdienstes (Active Directory) im Rahmen von Untersuchungen zur Sicherstellung der Daten- und Systemsicherheit zu verarbeiten.

Folgende Anwendungsfälle mit in diesem Sinne personenbezogenen Daten ergeben sich:

Daten- und Systemsicherheit

a) **Echtzeiterkennung:** Aufgrund der Schnelligkeit und Gefährlichkeit aktueller Angriffe ist es notwendig, Angriffe so früh wie möglich zu erkennen, um die Schäden zu minimieren. Eine Echtzeiterkennung wird mittels spezialisierter Sicherheitssysteme, zum Beispiel mittels eines Security Information and Event Management (SIEM) durchgeführt.

b) **Rückwirkende Erkennung von Angriffen:** Die Echtzeiterkennung bietet jedoch nicht die Möglichkeit, Angriffe, für die Indikatoren zur Erkennung erst nach langer Zeit bekannt werden, zu detektieren. Fortgeschrittene, gezielt vorgehende Angreifer sind dafür bekannt, dass sie übernommene Systeme nach der Erreichung ihrer Ziele wieder säubern, um so zu verhindern, dass sie entdeckt werden.

c) **Rückwirkende Erkennung Phishing**: Phishing, insbesondere Spearphishing, zielt darauf ab, Zugangsdaten von Endanwendern zu erhalten. Oft erfolgt dies, indem Anwender auf echten Seiten nachempfundene Webseiten gelockt werden und sich dort dann anmelden müssen. Da gerade Spearphishing sehr zielgerichtet erfolgt, ist die Erkennungsrate durch Endanwender sehr gering. Falls die gefälschte Webseite doch einem Anwender oder durch andere Mittel auffällt, kann nur mittels langfristig aufbewahrter Logdateien festgestellt werden, ob weitere Anwender angegriffen wurden.

Arbeitsorganisation

d) **Auswertung wegen missbräuchlicher Nutzung:** Gemäß der 59er Vereinbarung zur Nutzung von Internet und Email erfolgt ab der Stufe 3 eine personenbeziehbare Auswertung der Logdaten ab Beginn der Stufe 3.

Anwendungsfälle	Personen-bezogene Zuordnung notwendig	Zweck 1: Daten -und Systemsicherheit	Zweck 2: Systemtechnik (z.B. Fehlerverfolgung)	Zweck 3: Arbeitsorganisation (z.B. Nutzung, Missbrauchskontrolle)
Anwendungsfall a) Echtzeiterkennung	Ja	10 Tage		
Anwendungsfall b) rückwirkende Erkennung von Angriffen	Ja	365 Tage		
Anwendungsfall c) rückwirkende Erkennung Phishing	Ja	365 Tage		
Stabiler Betrieb	nein		30 Tage	

Fehler- und Störungsbehebung	nein		30 Tage	
Anwendungsfall d) Anomysierte Statistiken	nein			30 Tage
Anwendungsfall d) Auswertung wegen missbräuchlicher Nutzung	Ja, ab Stufe 3 der 59er			30 Tage für die zunächst anonymisierte Kontrolle. Bei Feststellung eines Verdachtsfalles dann für die Dauer der Aufklärung.

Trennung nach Zwecken

Für die beiden Anwendungsbereiche **Daten- und Systemsicherheit** und **Arbeitsorganisation** stellt Dataport eine technische und organisatorische Trennung der Zugriffsberechtigten sicher.
Personal, das mit Fehlerverfolgung sowie Auftragsverarbeitung im Rahmen der Arbeitsorganisation des Verantwortlichen (zum Beispiel Statistik, Nutzung, Missbrauchskontrolle) befasst ist, gehört nicht der Sicherheitsorganisation des Auftraggebers an und hat daher maximal für 30 Tage rückwirkend Zugang zu der beschriebenen Internetprotokollierung.

4 TOP30-Auswertung

Der Auftraggeber und auch Netzverantwortliche können für ihre Netze eine sogenannte TOP30-Auswertung beauftragen. Dies ist eine monatliche Auswertung, die per Email an ein vom Auftraggeber benanntes Postfach gesendet wird.

Die TOP30-Auswertung listet für den jeweils vergangenen Monat die 30 Domains auf, für die die meisten Aufrufe verzeichnet wurden, sowie die 30 Domains, die den meisten Traffic erzeugt haben. Die 30 Positionen enthalten nur den Namen der Domain (keine Subdomains und keine URL-Bestandteile), die Anzahl der Aufrufe bzw. das übertragene Volumen in MB und eine Liste der Netze des jeweiligen Verantwortungsbereichs. Es sind keine Zeitangaben oder IP-Adressen oder sonstige Angaben gelistet, die auf einzelne Nutzer oder Arbeitsplätze schließen lassen könnten. Die auszuwertenden Netze müssen ausreichend groß sein, um die Anonymität sicherzustellen (Netzmaske mindestens 255.255.255.0, bzw. /24, also minimal 254 IP-Adressen).

5 URL-Filter

Der optionale Zusatzdienst „URL-Filter“ wird von Dataport für beteiligte Stellen angeboten.

5.1.1 Universelle und individuelle Listen

Dataport bezieht von einem Drittanbieter eine sogenannte Blacklist, die ca. 800.000 Domains und URLs mit pornografischen Inhalten enthält („adult content“, Stand Anfang 2020). Über Webseiten dieses Themenbereichs besteht allgemeiner Konsens, dass diese Seiten dienstlich nicht benötigt werden und auch in Pausenzeiten nicht von dienstlichen Arbeitsplätzen aufgerufen werden sollten. Diese allgemeine Blocklist wird täglich automatisch aktualisiert.

Jede beteiligte Stelle hat die Möglichkeit, für sein Netz zusätzliche Domains und URLs sperren zu lassen oder explizit freizugeben.

5.1.2 Filterung

Der URL-Filter ist eine per Auftrag einschaltbare Funktion des Dataport HTTP-Proxies (Dienstprogramm zur Weiterleitung von Daten auf dem Dataport Firewall, siehe auch Glossar). Die Sperre von Zugriffen erfolgt zentral auf dem Dataport Proxy.

Wird eine unerwünschte Seite aufgerufen, leitet der URL-Filter den Browser auf eine Hinweis-Seite um (siehe Abb. 1, nicht erlaubter Zugriff auf http://www.porno.dk). Aus dem Hinweis geht hervor, dass der Dataport URL-Filter den Zugriff gesperrt hat. Es wird außerdem darauf hingewiesen, dass **nicht** Dataport, sondern ein lokaler Administrator die Verantwortung für die Filtereinstellungen hat und die Seite freigeben könnte, falls sie versehentlich gesperrt wurde.

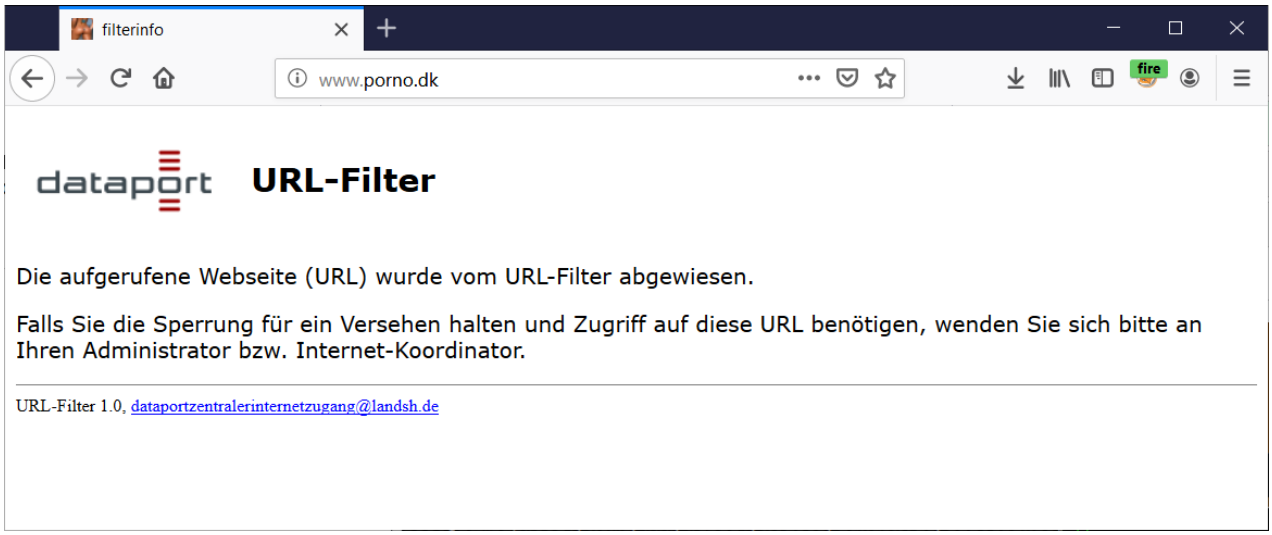


Abb. 1: Hinweis beim Aufruf einer unerwünschten Webseite

5.2 Filterregeln

Der benannte Netzverantwortliche legt einmalig fest, welche seiner Netze gefiltert werden und ob z.B. IP-Adressenbestimmter Arbeitsplätze von der Filterung ausgenommen sein sollen. Er kann Dataport jederzeit beauftragen, zusätzliche Domains und URLs für seinen Verantwortungsbereich blockieren oder aber explizit freischalten zu lassen. Die Filterung geschieht nach folgender Regel:

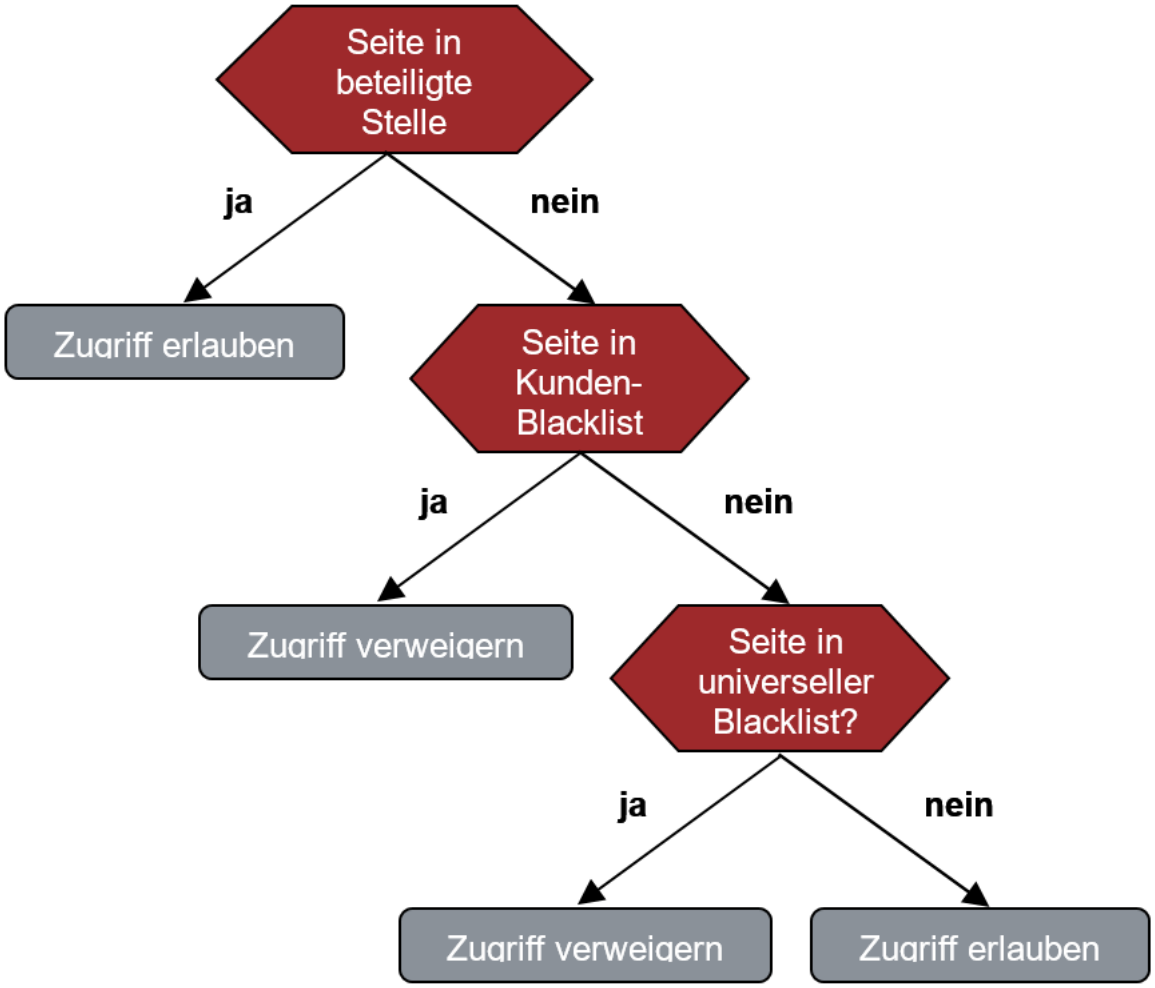


Abb. 2: Regelwerk

6 Betreuung und Pflege

Ein automatischer Prozess lädt und installiert täglich die aktuelle universelle Blacklist. Fehlerbehebungen, Aktualisierung und Verbesserung werden zentral auf den Servern von Dataport durchgeführt. Änderungen an den kundenspezifischen Filterregeln können von den beteiligten Stellen per Auftragsformular bei dataport über das Service Center Netze per Email beauftragt werden.

7 Protokollierung

Für den Zugriff auf nicht erlaubte Seiten (Blacklist) gibt es keine besondere Protokollierung. Umleitungen auf die URL-Filter Informationsseite werden im Rahmen des Internet-Zugangs protokolliert.

8 Redirects

Einige wenige Endgeräte sind nicht in der Lage über einen Proxy mit dem Internet zu kommunizieren und benötigen eine direkte Verbindung ins Internet. Ein Beispiel sind sogenannte e-Cash-Reader, also Geräte, die Bankkarten einlesen und elektronische Zahlungen steuern können, aus Sicherheitsgründen aber nicht über Proxies verbunden sein dürfen.

In solchen Fällen prüft Dataport zusammen mit dem Hersteller, ob die Verbindung trotzdem über die FW-Infra SH Netzstruktur mit Hilfe eines sogenannten „Redirect“ hergestellt werden kann. Parallel dazu wird geprüft, ob die Lösung den Sicherheitsanforderungen genügt.

Für Redirects gilt, dass die Kommunikation nur aus dem internen Netz (Landesnetz SH) aufgebaut werden darf und an einer fest eingestellten IP-Adresse im Internet terminieren muss.

Die Verbindungsdaten werden – so weit wie möglich - in ähnlicher Form wie der normale Internet-Verkehr geloggt (Datum, Uhrzeit, Quelle, Ziel, Anzahl übertragener Bytes bzw. Fehlercodes)

9 Glossar

DNS – (Domain Name System) – ein Namensdienst, der die Zuordnung von Domainnamen (z.B. landsh.de) zu ihren IP-Adressen verwaltet.

Domain – ein Namensraum im Internet (englisch domain). Es gibt verschiedene Domainlevels, z.B. den Top-Level (.de ist die Top-Level-Domain für Deutschland). Im Zusammenhang mit dem URL-Filter wird in diesem Dokument meist mit Second-Level-Domains gearbeitet (z.B. „dataport.de“).

FTP – File Transfer Protocol, englisch für Dateiübertragungsprotokoll. Mittels FTP können Dateien mit Hilfe einer FTP-Client-Software vom Client ins Internet oder vom Internet auf den Client übertragen werden.

HTTP – aus Wikipedia, der freien Enzyklopädie: Das Hypertext Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung von Daten über ein Netzwerk. Es wird hauptsächlich eingesetzt, um Webseiten und andere Daten aus dem World Wide Web (WWW) in einen Webbrowser zu laden. Beim Protokoll HTTPS werden die übertragenen Daten zusätzlich verschlüsselt.

Malware – siehe Schadcode

Proxy – Ein Proxy ist ein Dienstprogramm zur Weiterleitung von Daten. In Zusammenhang mit diesem Dokument wird darunter der Dataport-Proxy verstanden, der auf den Dataport Firewall-Servern dafür sorgt, dass Webseiten aus dem WWW mittels Browser aufgerufen werden können. Der Proxy-Dienst dient der Zugangskontrolle, Datensicherheit und Filterung, indem nur zugelassene Anwender den Proxy erreichen, nur das HTTP-Protokoll (bzw. HTTPS) zugelassen und Aufrufe vom URL-Filter geprüft werden.

Schadcode – Programmcode (aber z.B. auch bösartige Office-Macros), der für den Benutzer unerwünschte bzw. schädliche Aktionen oftmals unbemerkt ausführt. Der Schadcode kann z.B. Daten löschen oder schutzwürdige Daten (Zugangsdaten, personenbezogene Daten) an Dritte im Internet senden.

URL – Uniform Resource Locator, engl. „einheitlicher Quellenanzeiger“. URLs identifizieren eine Ressource über das Zugriffsprotokoll (häufig http oder ftp) und den Ort (engl. location) in Computernetzwerken, also z.B. http://www.google.de (Protokoll http, location www.google.de).