Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Private sowie dienstliche Internet- und E-Mail-Nutzung

Metadaten:

Version:	1.6
Ausgabedatum:	1. April 2014
Status:	☐ in Bearbeitung ☐ in Abstimmung ☑ Freigegeben
Ansprechpartner juristisch:	Dr. Sven Polenz 0431/988-1215 ULD4@datenschutzzentrum.de
Ansprechpartner technisch:	Dr. Thomas Probst 0431/988-1211 ULD3@datenschutzzentrum.de

1. Ausgangslage

Internetnutzung und E-Mail-Kommunikation sind feste Bestandteile in modernen Organisationen. Die Entscheidung über die Erlaubnis einer privaten Internet- und E-Mail-Nutzung durch die Beschäftigten trifft der Arbeitgeber. Schweigt der Arbeitgeber hierzu, so ist den Beschäftigten eine entsprechend private Nutzung nicht gestattet. Eine Erlaubnis zur Privatnutzung gegenüber den Beschäftigten durch schlüssiges Verhalten ist abzulehnen, da sich aus dem Verhalten des Arbeitgebers ein solcher Erklärungswert nicht ohne weiteres ergibt. Aus einer stillschweigenden Erklärung des Arbeitgebers wird sich kaum der konkrete zeitliche Rahmen ableiten lassen, in welchem die Beschäftigten eine Privatnutzung vornehmen dürfen. Weiterhin kann dem Arbeitgeber nicht unterstellt werden, er würde durch sein Verhalten den Anschein erwecken, er werde auf Kontrollen verzichten und bestehende Sicherheits- und Haftungsrisiken, die mit der Privatnutzung durch Beschäftigte im Zusammenhang stehen, akzeptieren. Eine Erlaubnis zur Privatnutzung muss daher vom Arbeitgeber ausdrücklich erfolgen. Eine Verpflichtung des Arbeitgebers, den Beschäftigten eine private Nutzung von Internet und/oder E-Mail zu gestatten, besteht nicht.

Der Einsatz von Internetnutzung und E-Mail-Kommunikation setzt eine funktionierende IT- und Sicherheitsdokumentation mit der Beschreibung der nötigen IT-Komponenten, deren Konfiguration, Datensicherheitsmaßnahmen und Kontrollflüssen voraus. Diese Anforderung ergibt sich für öffentliche Stellen in Schleswig-Holstein aus dem Landesdatenschutzgesetz (LDSG) und der Datenschutzverordnung (DSVO), für nichtöffentliche Stellen hingegen aus dem Bundesdatenschutzgesetz (BDSG). Die Entscheidung über den Umfang der Internet- und E-Mail-Nutzung durch Beschäftigte muss von der Dienststellen- bzw. Unternehmensleitung getroffen und dokumentiert werden.

Das Maß der erlaubten Internet- und E-Mail-Nutzung hat Auswirkungen auf die Verpflichtungen der Daten verarbeitenden Stelle nach dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz (TKG).

2. Rechtsvorschriften

2.1 Telekommunikationsgesetz (TKG)

Sobald ein Arbeitgeber seinen Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, erbringt er ihnen gegenüber geschäftsmäßig Telekommunikationsdienste, § 3 Nr. 6 TKG. Dabei kommt es nicht darauf an, ob der Arbeitgeber die private Nutzung gegenüber seinen Mitarbeitern abrechnet. Der Arbeitgeber ist den Beschäftigten gegenüber Diensteanbieter nach dem TKG und somit zur Einhaltung des Fernmeldegeheimnisses verpflichtet. Der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, unterliegen dem Fernmeldegeheimnis. Gemäß § 88 Abs. 3 TKG ist es dem Diensteanbieter untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Die Ver-

pflichtung zum Schutz des Fernmeldegeheimnisses gilt nicht nur für Telekommunikationsunternehmen, die ihre Dienste der Öffentlichkeit anbieten, sondern ebenso für öffentliche Stellen oder Unternehmen, die die betriebliche Telekommunikation auch für private Zwecke ihrer Mitarbeiter zur Verfügung stellen.

2.2 Telemediengesetz (TMG)

Bei einer erlaubten privaten Internet- und/oder E-Mail-Nutzung ist der Arbeitgeber seinen Beschäftigten gegenüber ferner Diensteanbieter nach dem TMG, da er den Zugang zur Nutzung dieser Dienste vermittelt. Bei der Internet- und E-Mail-Nutzung handelt es sich um Informations- und Kommunikationsdienste, die nur teilweise in der Übertragung von Signalen über Telekommunikationsdienste bestehen. Neben dem Transport von Daten, der dem Anwendungsbereich des TKG unterfällt, stehen nach den Vorschriften des TMG die transportierten Inhalte im Vordergrund (sog. Telemedien).

Bei einer Erlaubnis zur privaten Internet- und/oder E-Mail-Nutzung sind nur einige besondere Regelungen des TMG von Bedeutung, vgl. § 11 Abs. 3 TMG. Müssen die Beschäftigten etwa ein Entgelt für die private Nutzung von Internet und E-Mail entrichten, so hat der Arbeitgeber als Diensteanbieter etwa die Befugnis, personenbezogene Daten der Beschäftigten über das Ende des Nutzungsvorgangs hinaus für Zwecke der Rechtsverfolgung zu verwenden, wenn zu dokumentierende tatsächliche Anhaltspunkte vorliegen, dass seine Dienste von bestimmten Beschäftigten in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten.

Soweit die Bereitstellung solcher Dienste im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt, gelten gem. § 11 Abs. 1 Nr. 1 TMG die datenschutzrechtlichen Regelungen des TMG für die Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien nicht.

3. Gestaltungsfragen

Das Fernmeldegeheimnis stellt den Inhalt und die näheren Umstände der Kommunikation unter einen besonderen Schutz, so dass diese Informationen über den in § 88 Abs. 3 TKG zulässigen Umfang hinaus durch den Arbeitgeber nur mit Einwilligung des Beschäftigten zur Kenntnis genommen werden dürfen. Es schützt aber nicht nur den privat kommunizierenden Beschäftigten, sondern im Falle des E-Mail-Verkehrs auch den Kommunikationsempfänger oder -absender außerhalb der Dienststelle bzw. des Unternehmens. Für diesen kann der Beschäftigte keine Einwilligung erklären, so dass eine fehlende Unterscheidung gegebenenfalls dazu führen würde, dass die gesamte dienstliche bzw. betriebliche Kommunikation dem Fernmeldegeheimnis unterfällt. Im Bereich der E-Mail-Nutzung kann das Problem etwa so gelöst werden, dass den Beschäftigten erlaubt wird, ausschließlich über sog. Webmailer oder andere Web-Frontends private E-Mails zu versenden. Dienstliche E-Mail-Adressen sollten nie für private Kommunikation genutzt werden. Hier empfiehlt sich eine strikte Trennung.

Es bleibt die Frage, ob der Arbeitgeber im Falle der Erlaubnis einer privaten Internet- und/oder E-Mail-Nutzung gegenüber den Beschäftigten Maßnahmen der Verhaltenskontrolle durchführen darf, um einer missbräuchlichen Nutzung des dienstlichen Internetzugangs entgegen zu wirken. Ihm ist ein berechtigtes Interesse zuzubilligen, den Umfang der erlaubten privaten Nutzung zu beschränken und diese Einschränkungen auch kontrollieren zu können.

Entschließt sich der Arbeitgeber also dazu, die private Nutzung zu erlauben, so kann er diese Erlaubnis an einschränkende Voraussetzungen knüpfen. Diese sollten im nichtöffentlichen Bereich in einer Betriebsvereinbarung und im öffentlichen Bereich in einer Dienstvereinbarung festgehalten werden. Soweit keine Personalvertretung existiert, sollte eine Festlegung z. B. in Form einer Dienstanweisung oder in Richtlinien erfolgen.

Es kann etwa geregelt werden, dass die private Nutzung nur während der Pausenzeiten gestattet ist. Eine Erlaubnis kann sich auch auf die gesamte Dienstzeit beziehen. Auf unbestimmte Begrifflichkeiten, wie z.B. „Nutzung in angemessenem Umfang“ oder „Nutzung in geringem Umfang“ sollte zur Gewährleistung von Rechtsklarheit für alle Beschäftigten verzichtet werden. Letztlich sind konkrete Formulierungen schon für die Prüfung der Zulässigkeit von Verhaltenskontrollen im Einzelfall und für darauf aufbauende arbeitsrechtliche oder disziplinarische Entscheidungen von Bedeutung.

Darüber hinaus muss den Beschäftigten transparent gemacht werden, auf welche Art und Weise eine Kontrolle des Umfangs der privaten Nutzung stattfindet. Auch das Verfahren einer datenschutzkonformen Protokollierung und Missbrauchskontrolle sollte in einer Betriebs- oder Dienstvereinbarung festgelegt werden. Dies gilt im Übrigen nicht nur für den Fall der erlaubten Privatnutzung. Auch bei der ausschließlich dienstlich erlaubten Nutzung von E-Mail und Internet handelt es sich bei der Bereitstellung der Kommunikationsmittel um organisatorische und sonstige innerdienstliche Maßnahmen, die die Beschäftigten der Dienststelle insgesamt, Gruppen von ihnen oder einzelne Beschäftigte betreffen oder sich auf sie auswirken, sowie um technische Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Damit unterliegen diese Maßnahmen der Mitbestimmung des Personalrates gem. § 51 Personalvertretungsgesetz Schleswig-Holstein bzw. der Mitbestimmung des Betriebsrates gem. § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz. Bei der erlaubten privaten Nutzung des Internets muss der Beschäftigte zusätzlich zustimmen, dass der Arbeitgeber über das für die Erbringung der Telekommunikationsdienstleistung bzw. über das für eine Abrechnung erforderliche Maß hinaus Kenntnis von den näheren Umständen der Kommunikation (z. B. über die Zeiträume der Nutzung) erhält.

Die Anforderungen an eine Betriebs- bzw. Dienstvereinbarung werden im Abschnitt 6 beschrieben.

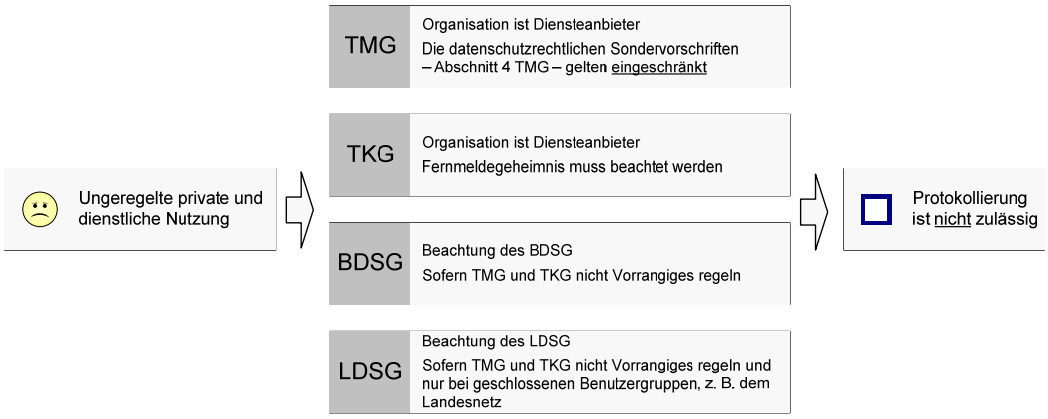
4. Datenschutzkonforme Protokollierung

Bei der Einführung einer Protokollierung muss darauf geachtet werden, dass es zu keinen Verstößen gegen die oben genannten Normen kommt. Die Internet- und E-Mail-Nutzung in einer Daten verarbeitenden Stelle kann in drei Szenarien unterteilt werden:

- ungeregelte private und dienstliche Nutzung
- geregelte rein dienstliche Nutzung

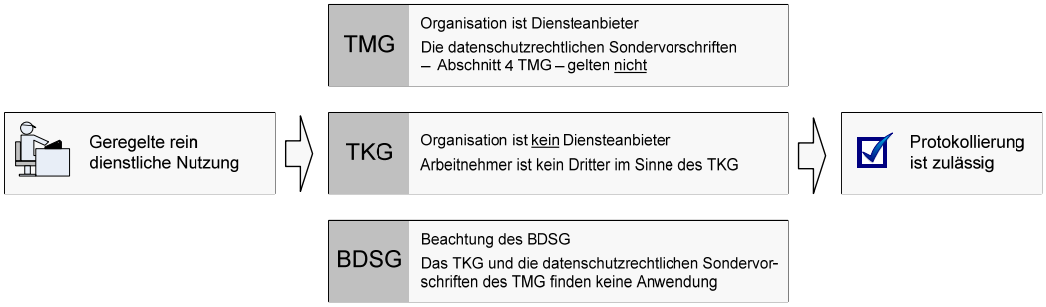
- geregelte private und dienstliche Nutzung

Ist die Internet- und E-Mail-Nutzung ungeregelt und wird die Privatnutzung durch den Arbeitgeber aber offensichtlich geduldet, ist die Daten verarbeitende Stelle insgesamt an das Fernmeldegeheimnis gebunden. Eine Protokollierung der Nutzung ist nicht zulässig (siehe die folgende Abbildung).

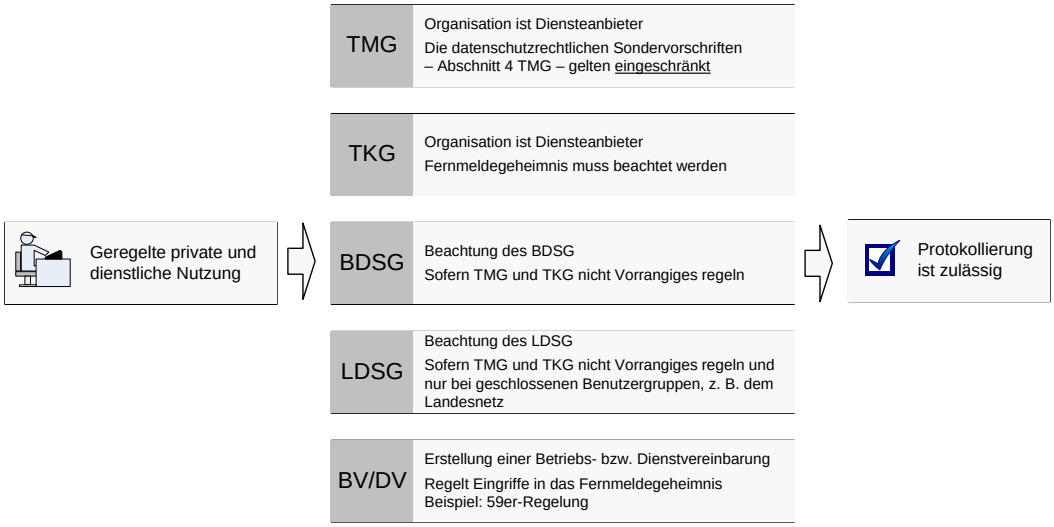


Die Orientierungshilfe „Protokollierung“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder liefert umfangreiche Informationen zum Thema Protokollierung und kann unter dem Link http://www.lfd.m-v.de/dschutz/informat/protokol/oh-proto.pdf abgerufen werden.

Wird die Internet- und E-Mail-Nutzung nur zu rein dienstlichen Zwecken erlaubt, darf die Daten verarbeitende Stelle die Benutzeraktivitäten im Rahmen von technisch-organisatorischen Datenschutzkontrollen prüfen (siehe die folgende Abbildung).



Wird die private Internet- und E-Mail-Nutzung eingeschränkt erlaubt, so ist die Daten verarbeitende Stelle ebenfalls an das Fernmeldegeheimnis gebunden. Durch Einwilligung der betroffenen Beschäftigten sowie durch eine Betriebs- bzw. Dienstvereinbarung können aber Eingriffe in das Fernmeldegeheimnis zulässig sein (siehe die folgende Abbildung).



Gemäß §§ 5 und 6 Landesdatenschutzgesetz (LDSG) darf eine Protokollierung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren notwendig ist. Werden die Daten ausschließlich zu den genannten Zwecken gespeichert, ist die strenge Zweckbindung nach § 13 Abs. 6 LDSG zu beachten. Die protokollierten Daten dürfen nicht für andere Zwecke verwendet werden. Dies unterstreicht die Notwendigkeit einer klaren Regelung über Umfang und Reichweite der Protokollierung zu Zwecken der Verhaltens- und Leistungskontrolle. Es ist unzulässig, Daten, die nur zur Datenschutzkontrolle, Datensicherung oder Sicherung des ordnungsgemäßen Betriebs der Verfahren aufgezeichnet werden, zu anderen Zwecken zu verwenden. In einem eventuellen arbeitsrechtlichen Verfahren müssten solche Daten als unzulässige Beweismittel abgelehnt werden. Das gleiche gilt nach § 31 Bundesdatenschutzgesetz für nichtöffentliche Stellen. Sollen diese Daten für den weiteren Zweck der Missbrauchskontrolle, d. h. einer Verhaltenskontrolle, genutzt werden, so muss dieses Vorgehen für die Beschäftigten von vornherein transparent gemacht werden.

5. Eskalierendes Stufenmodell

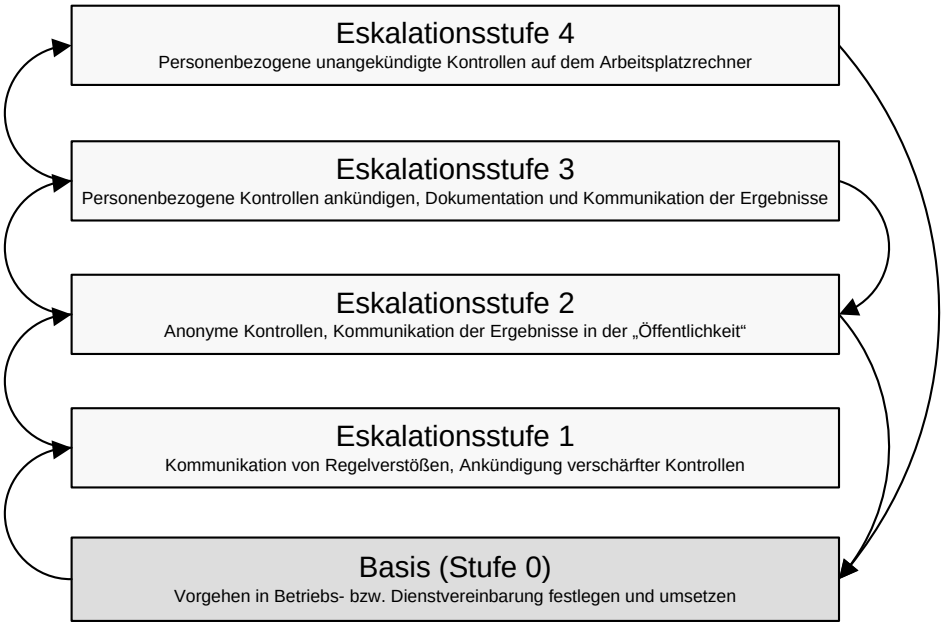
Das Ziel von Kontrollen besteht vorrangig darin, unerwünschte Handlungen zu unterbinden und Verdächtige zu überführen. Entsprechend dieser Vorgabe wurde das nachfolgende Stufenmodell entwickelt.

Heutige Organisationen betreiben typischerweise an ihrer Schnittstelle zum Internet einen Proxy. Mit dessen Hilfe können die Inhalte des Datenverkehrs ins und aus dem Internet automatisiert geprüft werden, um beispielsweise

- die Filterungen von Inhalten mit Schadfunktion vorzunehmen,
- eine Authentisierung und Autorisierung von Beschäftigten durchzuführen,
- die Internet- und E-Mail-Nutzung zu protokollieren oder
- an dieser zentralen Stelle bestimmte Regelungen, beispielsweise bezüglich der Anbindung mobiler Geräte, durchzusetzen.

In einer Betriebs- bzw. Dienstvereinbarung (siehe auch Abschnitt 6) müssen die technischen und organisatorischen Vorgaben vereinbart werden, die die verantwortliche Stelle zur Kontrolle umsetzt.

Wie kann ein transparentes und zielführendes Kontrollverfahren zur Aufdeckung von Missbräuchen und Regelverstößen aussehen? Es sollte zumindest über vier Eskalationsstufen verfügen:



Basis (Stufe 0):

Zunächst sind Zweck und die akzeptablen Anlässe einer Kontrolle als Bestandteile der Dokumentation schriftlich festzulegen, dann die Verfahrensabläufe, wie Kontrollen durchzuführen sind, zu beschreiben sowie eine Betriebs- bzw. Dienstvereinbarung zu schließen, die die Beschäftigten darüber in Kenntnis setzt.

Eskalationsstufe 1:

Innerhalb der Organisation wird kommuniziert, dass Fälle von Missbrauch oder Regelverstößen vorgekommen sind. Es werden weitergehende Sanktionen entsprechend den Ausführungen in der Betriebs- bzw. Dienstvereinbarung (dies entspricht den nachfolgenden Stufen) angekündigt, sofern weiterhin Missbräuche und Regelverstöße festgestellt werden.

Eskalationsstufe 2:

Es werden anonyme oder pseudonyme Protokollierungen zentral am Proxy vorgenommen:

- Beteiligung des/der Datenschutzbeauftragten und der Personalvertretung,
- Analyse der Protokolldaten,
- Kommunikation der Ergebnisse innerhalb der Organisation, z. B. in Form einer Top-Ten-Liste der aufgerufenen Webseiten,
- Hinweis, dass bei fortgesetztem Missbrauch personenbezogene Kontrollen oder Protokollierungen durchgeführt werden,
- mögliche technische Unterstützung, z. B. können im Fall einer Internetnutzung mit unerwünschten Webseiten deren Adressen in eine „Blacklist“ eingetragen werden, so dass die entsprechenden Server nicht erreichbar sind.

Die Auswertung der Daten kann dazu führen, dass sich als Quelle eines Missbrauchs beispielsweise eine bestimmte Abteilung identifizieren lässt. Über das Ansprechen dieser Abteilung kann dann ein Versuch gestartet werden, einen Appell an die Beschäftigten zu richten, die unerwünschten Handlungen zu unterlassen.

Eskalationsstufe 3:

Es wird eine personenbezogene Protokollierung auf dem Proxy angekündigt. Hierbei sollten folgende Regelungen vorgesehen werden:

- Beteiligung des/der Datenschutzbeauftragten und der Personalvertretung,
- Ankündigung einer personenbezogenen Protokollierung innerhalb der Organisation,
- Festlegung des genauen Zwecks, des Umfangs und des Zeitraums der Protokollierung und deren Auswertung in einem Konzept; der Umfang der von der Protokollierung erfassten Personen muss dabei auf den Kreis der Verdächtigen begrenzt werden; es darf nicht das gesamte Personal überwacht werden,

- Auswertung der Protokolldaten nur unter Beteiligung des/der Datenschutzbeauftragten und der Personalvertretung,
- vollständige Dokumentation der Auswertung,
- Löschung der personenbezogenen Daten nach Auswertung,
- Kommunikation der Ergebnisse,
- Abwägung des weiteren Vorgehens unter den Beteiligten entsprechend der Ergebnisse, beispielsweise:
  - Beenden der Kontrollen, keine weitere Überwachung,
  - Rückkehr zur Stufe 2, wenn man nach wie vor mit Verstößen rechnen muss,
  - nochmaliges Verschärfen der Kontrolle, indem die Protokollierung auf dem Arbeitsrechner der Verdächtigen stattfindet (Eskalation auf Stufe 4).

Eskalationsstufe 4:

Es wird eine personenbezogene Protokollierung auf den Arbeitsrechnern der Verdächtigen ohne Ankündigung durchgeführt.

Hierfür gelten dieselben Anforderungen wie für die Stufe 3 mit Ausnahme der Ankündigung. Diese Protokollierung darf ebenfalls nur dann geschehen, wenn die Beschäftigten in der Betriebs- bzw. Dienstvereinbarung darüber aufgeklärt wurden, dass diese letzte Eskalationsstufe unter bestimmten Bedingungen zum Einsatz kommen kann. In dieser äußersten Eskalationsstufe sollte man erwägen, bereits eine Strafanzeige zu stellen und eine Strafverfolgungsbehörde hinzuzuziehen, um bei der Beweissicherung keine Fehler zu machen.

Ergänzende Hinweise zu allen Eskalationsstufen:

Wichtig ist die zeitnahe Abwägung, wann wieder auf eine niedrigere Eskalationsstufe bzw. auf die Basisstufe zurückgefahren wird. Auch das Verfahren der „Zurückstufung“ sollte im Vorweg als Prozess beschrieben sein.

Weiterhin sollte festgelegt werden, wie lange die Protokolldaten und die Dokumentationen der Auswertungen aufbewahrt werden. Nach Ablauf der Aufbewahrungsfrist muss sichergestellt werden, dass die entsprechenden Daten gelöscht werden.

6. Anforderungen an eine Betriebs- bzw. Dienstvereinbarung

In der arbeitsgerichtlichen Rechtsprechung ist anerkannt, dass im Wege betrieblicher Rechtsetzung, also durch Betriebs- bzw. Dienstvereinbarungen, angepasste datenschutzrechtliche Regelungen aufgestellt werden können.

Bei der Erarbeitung einer Betriebs- bzw. Dienstvereinbarung ist Folgendes zu beachten:

- Erlaubt eine Daten verarbeitende Stelle die private Internet- oder E-Mail-Nutzung, wozu sie nicht verpflichtet ist, so kann sie die Erlaubnis an einschränkende Voraussetzungen knüpfen. Die Kontrollmechanismen müssen datenschutzkonform sein.
- Eine Nutzung von Internet und E-Mail, die den Interessen der Daten verarbeitenden Stelle entgegensteht oder gegen strafrechtliche bzw. urheberrechtliche Vorschriften verstößt, sollte untersagt werden.
- Eingehende private E-Mails sind wie private (Papier-)Post zu behandeln. Fälschlich als Dienstpost behandelte E-Mails sind den betroffenen Beschäftigten unverzüglich zur alleinigen Kenntnis zu geben.
- Die Inanspruchnahme kostenpflichtiger Angebote zu Lasten der verantwortlichen Stelle sowie die Verfolgung kommerzieller Zwecke im Rahmen der privaten Nutzung sollten untersagt werden.
- Für die private Nutzung von Internet und E-Mail kann ein separates Benutzerkonto zur Verfügung gestellt werden. Durch Protokollierung und ausschließlich summarische Auswertung der Nutzungszeiträume des privaten Benutzerkontos kann festgestellt werden, ob zeitliche Vorgaben eingehalten werden. Dies darf aber nur mit Einwilligung der Betroffenen erfolgen.
- Die Protokollierung zu Zwecken der Datenschutzkontrolle, der Abrechnung, der Datensicherheit oder zur Vorbeugung strafrechtlich relevanten Verhaltens ist zulässig. Für darüber hinausgehende Kontrollen sind eine Betriebs- bzw. Dienstvereinbarung und/oder die Einwilligung des Betroffenen nötig.

Zusätzlich müssen für die Protokollierung am Proxy zumindest folgende Aspekte berücksichtigt und in der Betriebs- bzw. Geschäftsvereinbarung beschrieben werden:

- Umfang der erlaubten Nutzung,
- Zweck und mögliche Anlässe sowie Umfang von Kontrollen und Protokollierungen (Aufnahme einer konkreten Zweckbindungsregel, z. B. in Form einer Bindung auf den Zweck der Missbrauchskontrolle unter Ausschluss der darüber hinausgehenden Leistungskontrolle),
- Aufbewahrungsfristen von Protokolldaten,
- Ausgestaltung personenbezogener Auswertungen,
- Regelungen zu Sperrungen von Kommunikationspartnern oder Webseiten,
- Berechtigungen des Zugriffs auf Hard- und Software sowie
- Verfahren, unter welchen Umständen Administratoren auf personenbezogene Datenbestände zugreifen dürfen.

Beispiel: In Schleswig-Holstein regelt die Richtlinie zur Nutzung von Internet und E-Mail nach dem Mitbestimmungsgesetz des Landes (MBG) die dienstliche und private Nutzung der dienstlich zur Verfügung gestellten Services Internet und E-Mail (59er Regelung).

Diese gilt für die Beschäftigten der unmittelbaren Landesverwaltung, deren PCs an das Landesnetz angeschlossen sind (Amtsblatt für Schleswig-Holstein 2009, S. 415 ff. oder http://shvv.juris.de/shvv/vvsh-2015.6-0001.htm). Diese Richtlinie kann für den Bereich der Kommunalverwaltung als Vorbild dienen.

7. Zusammenfassung

Bei einer Regelung der Internet- und E-Mail-Nutzung für die Beschäftigten eines Unternehmens oder einer Behörde sollten die folgenden Maßnahmen berücksichtigt werden:

- Fragen der Erlaubnis einer privaten Nutzung von Internet- und E-Mail-Nutzung und einschränkende Voraussetzungen durch Betriebs- bzw. Dienstvereinbarung festlegen
- Beschäftigte durch Arbeits- oder Dienstanweisungen über Festlegungen in den Betriebs- bzw. Dienstvereinbarungen informieren
- Zu Kontrollen:
  - Gestuftes Kontrollverfahren durch Betriebs- bzw. Dienstvereinbarung festlegen
  - Insbesondere bei E-Mail: Kontrollen datensparsam und mit minimalisierter Eingriffstiefe durchführen
  - Kontrollen und Ergebnisse dokumentieren
  - Protokolldaten nach definierter Frist löschen