2.4 BSI-Lagebericht zur IT-Sicherheit 2018

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 11.10.2018 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=5 den Bericht zur Lage der IT-Sicherheit in Deutschland 2018 veröffentlicht, aus dem nachfolgend einige Auszüge entnommen sind.

Mit dem „Bericht zur Lage der IT-Sicherheit in Deutschland 2018“ legt das BSI einen umfassenden Überblick über die Bedrohungen Deutschlands, seiner Bürgerinnen und Bürger und seiner Wirtschaft im Cyber-Raum vor.

Aus dem Bericht geht hervor, dass die Gefährdungslage im Bereich der Cyber-Sicherheit in Deutschland in den vergangenen Monaten vielschichtiger geworden ist. WannaCry, NotPetya, Efail oder Spectre/Meltdown sind Ausdruck einer neuen Qualität von Cyber-Angriffen und IT-Sicherheitsvorfällen, die sich gegen die Grundpfeiler der Informationstechnologie richten. Gleichzeitig schreitet die Digitalisierung und Vernetzung von IT-Systemen, Alltagsgegenständen und Industrieanlagen voran, wodurch sich die potenzielle Angriffsfläche und auch die Abhängigkeit von Staat, Wirtschaft und Gesellschaft von funktionierenden IT-Systemen täglich vergrößert. Diese Kombination aus neuer Angriffsqualität und zunehmender Digitalisierung hebt die Gefährdungslage auf ein neues Niveau.

So beobachtet das BSI eine hohe Dynamik der Angreifer bei der Weiterentwicklung von Schadprogrammen und Angriffswegen. Bekannte Schadsoftware-Familien werden fortlaufend verändert, weiterentwickelt und mit zusätzlichen Schadfunktionen ausgestattet. Auf Seiten der Verteidiger erfordert dies hohe Aufmerksamkeit und Flexibilität zur Gewährleistung der Informationssicherheit.

Im Unterschied zu den Vorjahren sind im Berichtszeitraum 2017/2018 größere Angriffswellen mit Verschlüsselungssoftware (Ransomware) ausgeblieben. Dennoch bleibt Ransomware eine massive Gefährdung, wie die Angriffe mit der Schadsoftware Petya/NotPetya eindrucksvoll gezeigt haben, die auch in der deutschen Wirtschaft Schäden in Millionenhöhe verursachten. Als neue Gefährdung hat das BSI im Lagebericht das Thema „illegales Krypto-Mining“ näher betrachtet. Aufgrund der hohen finanziellen Attraktivität und der Unauffälligkeit der Infektionen ist illegales Krypto-Mining als signifikant zunehmendes Cyber-Risiko zu bewerten.

4.1.24 Art. 24 DSGVO: Verantwortung des für die Verarbeitung Verantwortlichen

1. Gesetzestext

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.
(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

2. Bedeutung des Artikels

Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Vorgaben der Datenschutz-Grundverordnung verantwortlich. Ihm obliegt es somit, die Rechtmäßigkeit der von ihm verantworteten Verarbeitungen personenbezogener Daten zu gewährleisten. Er haftet für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt.

a) Absatz 1

Der Verantwortliche hat im Hinblick auf die jeweilige Verarbeitung und unter Berücksichtigung der mit ihr einhergehenden **Risiken** für die Rechte und Freiheiten natürlicher Personen **angemessene** und **geeignete** technische und organisatorische Maßnahmen umzusetzen. Dabei muss er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen.

Risiken

Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen,

materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft (ErwGr. 75 zur DSGVO).

Risikoanalyse und -bewertung

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollen in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer **objektiven Bewertung** beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt (ErwGr. 76 zur DSGVO).

Es muss daher eine formale Risikoanalyse bei der Einführung eines neuen Verfahrens durchgeführt werden. Die Risikoanalyse ist zudem Grundlage für die Entscheidung, ob eine **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO nötig ist.

Im Rahmen der Risikoanalyse muss insbesondere abgewägt werden, in welchem Umfang und zu welchem Zweck personenbezogene Daten erhoben werden sollen, welchen Schutzbedarf die Daten haben und welche Gefahren/Risiken (genannt werden in Art. 32 Abs. 2 DSGVO insbesondere Risiken durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten) dies für die betroffenen Personen mit sich bringen kann. Dabei muss sowohl geprüft werden, wie schwerwiegend mögliche Nachteile für die betroffenen Personen sind, als auch, mit welcher

Wahrscheinlichkeit diese eintreten können. Anschließend muss geprüft werden, mit welchen Maßnahmen das jeweilige Risiko reduziert werden kann.
Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter geeignete Maßnahmen durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist, insbesondere was die Ermittlung des mit der Verarbeitung verbundenen Risikos, dessen Abschätzung in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für dessen Eindämmung betrifft, könnten insbesondere in Form von genehmigten **Verhaltensregeln**, genehmigten **Zertifizierungsverfahren**, **Leitlinien des Ausschusses** oder **Hinweisen eines Datenschutzbeauftragten** gegeben werden (ErwGr. 77 Satz 1 zur DSGVO).

Angemessenheit
Die Sicherheitsmaßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.
Schutzzweck und Aufwand sind also maßgeblich für die Festlegung der Einzelmaßnahmen. Als Aufwand sind insbesondere zu berücksichtigen:
– die Kosten der Maßnahmen
– die organisatorischen Aufwendungen
Ob eine Maßnahme als angemessen betrachtet werden kann, ist immer vom Einzelfall abhängig. Anhaltspunkte für die Angemessenheit sind:
– Art der zu schützenden personenbezogenen Daten
– Anzahl der Betroffenen
Dies bedeutet: Je **sensibler** die Daten sind und je mehr Personen von der Erhebung, Verarbeitung und Nutzung der Daten betroffen sind, desto umfassendere technische und organisatorische Schutzmaßnahmen sind zu ergreifen. Es bedeutet aber umgekehrt nicht, dass bei wenig sensiblen Daten gänzlich auf Sicherheitsmaßnahmen verzichtet werden kann. Ein gewisser Grundschutz muss immer vorhanden sein.
Es ist ferner schwierig zu erkennen, wie die mit der Sicherheit verbundenen Kosten dem Schutzzweck im Verhältnis zu setzen sind. **Kosten-Nutzen-Analysen** sind nicht immer problemlos und auch nicht frei von Risiken, da eintretende Schäden, insbesondere wenn sie immaterieller Art sind, in ihrem Umfang kaum bezifferbar vorauszusehen sind.
Als Maßstäbe für eine Kosten-Nutzen-Analyse können
– die ein bestimmtes Risiko absichernde Kosten,
– die eventuelle Schadenshöhe,
– die Eintrittswahrscheinlichkeit eines Schadens,
– die Attraktivität der Daten für Unbefugte und
– die Sensibilität der zu schützenden Daten
dienen.

Geeignetheit
Die Maßnahmen müssen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, der jeweiligen Eintrittswahrscheinlichkeit und der Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignet sein. Dies verlangt nicht, dass es sich dabei um die bestmöglichen Datensicherheitsmaßnahmen handelt, sondern nur um geeignete Maßnahmen.

Rechenschaftspflicht
Die Einhaltung der sich aus der Datenschutz-Grundverordnung ergebenden Pflichten ist durch den Verantwortlichen angemessen zu dokumentieren („Rechenschaftspflicht").

Überprüfung und Aktualisierung
Die Überprüfungs- und Aktualisierungspflicht erfordert, auch bestehende Verfahren regelmäßig in Augenschein zu nehmen, insbesondere im Hinblick auf geänderte Rechtsvorschriften, auf wesentliche Verfahrensänderungen (etwa durch Hinzunahme neuer Datenarten), auf veränderte Zuständigkeiten sowie auch auf Weiterentwicklungen hinsichtlich des Standes der Technik (beispielsweise geänderte Anforderungen an Verschlüsselungsverfahren). Die insoweit durchgeführten Prüfungen müssen ebenfalls schriftlich dokumentiert werden und dürfen nicht aus Kostengründen unterbleiben.

b) Absatz 2
Im Sinne des Abs. 2 müssen Richtlinien und konkrete Handlungsanweisungen zum Umgang mit personenbezogenen Daten als geeignete Datenschutzvorkehrungen erlassen werden. Diese Richtlinien und Anweisungen sollten Bestandteil des zu erstellenden **Datenschutzmanagementsystems** sein.

c) Absatz 3
Der Verantwortliche muss die Einhaltung der Verarbeitungsgrundsätze (durch Zertifizierungen und Verhaltensregeln) nachweisen können.

3. Nähere Erläuterungen

– „Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche bzw. die bestimmten Kriterien sei-

5.1 Informationssicherheit, IT-Sicherheit, Datensicherheit, Datenschutz: Begriffe, Ziel, Umfang

Informationssicherheit, IT-Sicherheit, Datensicherheit und Datenschutz sind Begriffe, die stark miteinander verflochten sind.
Das Recht der Bürger, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen, ist verfassungsrechtlich garantiert. Aufgabe des **Datenschutzes** ist es, dieses Recht zu schützen. So enthält die Datenschutz-Grundverordnung (DSGVO) „Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ (Art. 1 Abs. 1 DSGVO). Gemäß Art. 1 Abs. 2 DSGVO müssen „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ geschützt werden.
Bei der Verarbeitung personenbezogener Daten sind zur Gewährleistung des Datenschutzes insbesondere die Art. 5 (Grundsätze für die Verarbeitung personenbezogener Daten) und 6 (Rechtmäßigkeit der Verarbeitung) DSGVO zu beachten.
Zur Gewährleistung des Datenschutzes und der **Datensicherheit** sind von den Verantwortlichen und Auftragsverarbeitern die geeigneten technischen und organisatorischen Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.
Datensicherheit wird häufig auch als Synonym für IT-Sicherheit verwendet, was aber nicht ganz zutrifft, da IT-Sicherheit weitreichender ist.
IT-Sicherheit umfasst natürlich auch den Schutz der Informationen, die durch IT-Geräte verarbeitet werden. Diese müssen aber – im Gegensatz zur Datensicherheit – nicht zwangsläufig personenbezogen sein. Außerdem sollen die IT-Geräte selbst ebenfalls geschützt werden.
IT-Sicherheit ist wiederum ein wesentlicher Teil der Informationssicherheit. **Informationssicherheit** hat als Ziel den Schutz von Informationen jeglicher Art und Herkunft. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert sein. (1) Während sich die IT-Sicherheit an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung beschäftigt, geht die Informations-

5.1.4.6 Übertragungskontrolle

Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle) (§ 64 Abs. 3 Nr. 6 BDSG).
Maßnahmen zur Übertragungskontrolle sind nur bei automatisierten Verarbeitungen zu ergreifen. Unter dem Begriff **automatisierte Verarbeitung** ist die Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen zu verstehen.
Im alten Recht (Nr. 6 der Anlage zu § 9 Satz 1 BDSG) war die Übertragungskontrolle – zusammen mit Transport- und Datenträgerkontrolle – Teil der Weitergabekontrolle.

Zielsetzung

Ziel der Übertragungskontrolle ist es, zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen der Datenübertragung übermittelt werden (können). Die Überprüfung und Feststellung müssen **nicht dauernd** erfolgen, sondern sie müssen jederzeit möglich sein.
Dabei kommt es nicht auf die tatsächliche oder theoretisch mögliche, sondern auf die nach der Verfahrenskonzeption vorgesehene Übermittlung an (auch im Rahmen von **automatisierten Abrufverfahren**).
Bei dem **Empfänger** kann es sich um eine natürliche oder juristische Person, eine Behörde, Einrichtung oder jede andere Stelle handeln, die Daten erhält.
Natürlich sollen auch die **Vertraulichkeit** und die **Integrität** der Daten bei der Datenübertragung gewährleistet werden. Dazu zählt auch, dass E-Mails mit (sensiblen) personenbezogenen Daten einschließlich eventueller Anhänge verschlüsselt übermittelt werden.

Maßnahmenkatalog

Das Bundesdatenschutzgesetz gibt lediglich das Ziel der Übertragungskontrolle vor und verzichtet auf eine detaillierte Festlegung der in diesem Rahmen zu ergreifenden Maßnahmen. Damit bleibt es den Unternehmen und Behörden überlassen, zu entscheiden, welche Maßnahmen ergriffen werden müssen.
Als Maßnahmen im Rahmen der Übertragungskontrolle kommt insbesondere Folgendes in Betracht:

5.1.6.2 Muster einer Bestellung zum IT-Sicherheitsbeauftragten

Ein IT-Sicherheitsbeauftragter muss nicht, sollte aber bestellt werden. Das nachfolgende Muster fußt auf dem „Muster für eine Bestellung des/der IT-Sicherheitsbeauftragten“ des BSI – abrufbar im Internet unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Muster/muster_bestellung_it-sibe_doc.doc?__blob=publicationFile&v=1.
Die *kursiv* gehaltenen Stellen sind zu ergänzen bzw. durch eigene Angaben zu ersetzen.

Bestellung zum IT-Sicherheitsbeauftragten

.....

(Name und Anschrift der Firma/des Unternehmens/der Institution)

Ich/Wir bestelle(n)

Frau/Herrn

.....

(Name und Anschrift *der/des* zukünftigen IT-Sicherheitsbeauftragten)

mit Wirkung vom ……/ab sofort zur/zum IT-Sicherheitsbeauftragten.
Ihre/Seine Abwesenheitsvertretung ist Herr/Frau *Name der Vertretung*.

1. Stellung

In der Funktion als IT-Sicherheitsbeauftragte(r) wird *sie/er* unmittelbar der *Geschäfts-/Behördenleitung* unterstellt und berichtet direkt an diese.
Es ist sicherzustellen, dass die Wahrnehmung der Rolle *der/des* IT-Sicherheitsbeauftragten zu keinen Konflikten mit weiteren von dieser Person wahrgenommenen Rollen führt.

2. Aufgaben

Zu *ihren/seinen* Aufgaben gehört es insbesondere,

- die Informationssicherheitsziele mit den Zielen *des Unternehmens/der Behörde* abzustimmen,
- die Leitlinie zur Informationssicherheit zu erstellen und diese mit der Führungsebene abzustimmen,

8.1.2.3 Checkliste für die Anschaffung, die Installation und den Betrieb einer Firewall

Firewalls bieten eine Reihe von Möglichkeiten, um den Datenverkehr in das und aus dem Internet zu kontrollieren, externe Angriffe abzuwehren und damit das Schutzniveau gegenüber dem Internet wesentlich zu erhöhen.
Insbesondere gut konfigurierte und administrierte Firewall-Systeme können die Gefahren, die durch einen Anschluss an öffentliche Netze entstehen, wirkungsvoll begrenzen, auch wenn selbst große und mit erheblichem Aufwand betriebene Firewall-Installationen nicht gegen sämtliche Gefahren aus dem Internet schützen können.
Die nachfolgende Checkliste enthält Prüfungsansätze für die Anschaffung, Installation und den Betrieb einer Firewall.
Die Checkliste erhebt keinen Anspruch auf Vollständigkeit und sollte durch eigene Erkenntnisse erweitert und ergänzt werden.

a) Fragen zur Produktauswahl

Frage	Ja	Nein	Anmerkungen
Wird darauf geachtet, dass nur erprobte und anerkannte Firewall-Produkte erworben werden?	☐	☐	
Wurde die Firewall bereits zertifiziert?	☐	☐	
Liegt eine ausführliche und aktuelle Beschreibung der Einsatzmöglichkeiten, Komponenten und der Funktionen der Firewall vor (z. B. reine Hardwarelösung, Router mit Firewall-Funktionalitäten, Proxyserver, Desktop-Firewall)?	☐	☐	

8.4 Datenschutz bei Suchmaschinen

Suchmaschinen durchforsten mithilfe von speziellen Programmen, sog. Robots oder Crawlern, das World Wide Web und speichern Informationen von gefundenen Seiten in einer eigenen Datenbank, dem Index. Wird eine Anfrage an eine Suchmaschine gerichtet, so recherchiert diese in ihrer Datenbank, ob sie das Gesuchte findet.
Bei Suchmaschinenanfragen fallen nicht nur die IP-Adressen der anfragenden Computer an, sondern weitere Angaben über den Rechner der Nutzenden, z. B. benutzter Browser und Betriebssystem. Außerdem stehen die Suchbegriffe zur Verfügung sowie das Datum und die Uhrzeit der Anfrage. Schließlich ist erkennbar, welche Webseite der Nutzende aus den gelisteten Resultaten tatsächlich ausgewählt und aufgerufen hat. Schon allein aus diesen Daten lässt sich ableiten, wofür sich eine Person wann interessiert hat. Werden viele solche Anfragen gemeinsam ausgewertet, lassen sich hieraus präzise Interessenprofile erstellen, also mit welchen Themen eine Person sich zu welcher Zeit beschäftigt hat. Werden diese Angaben einer konkreten Person zugeordnet, so lässt sich aus dem Anfrageprofil zumindest bei Personen, die regelmäßig Suchmaschinen nutzen, ein langfristiges Interessenprofil erstellen. Somit stellen Suchmaschinen ein großes Datenschutzproblem dar.

1. Gefahr durch die Veröffentlichung von Mitarbeiterdaten

Viele Unternehmen veröffentlichen Fotos, Telefonnummern und Lebensläufe ihrer Mitarbeiter auf ihren Webseiten.
Dadurch soll die fachliche Qualifikation der Beschäftigten herausgestellt sowie bei den (potenziellen) Kunden die Hemmschwelle für einen Anruf bei der Firma abgebaut und ein persönlicher Draht zu den Kunden aufgebaut werden.
Auf der anderen Seite haben immer mehr Mitarbeiter Angst um den Schutz ihrer Privatsphäre, da sie befürchten, dass anhand dieser Angaben und mithilfe von Suchmaschinen im Internet Persönlichkeitsprofile von ihnen erstellt werden könnten.

a) Erstellung von Persönlichkeitsprofilen

Diese Bedenken sind durchaus nicht unbegründet. Mithilfe der Auswerte- und Verknüpfungsmöglichkeiten von Suchmaschinen (wie beispielsweise Google) können sämtliche im Internet anzutreffenden Daten über eine Person problemlos verknüpft werden, indem man alle Internetangebote auswertet, in denen der Betroffene vorkommt (eine Art von Rasterfahndung).