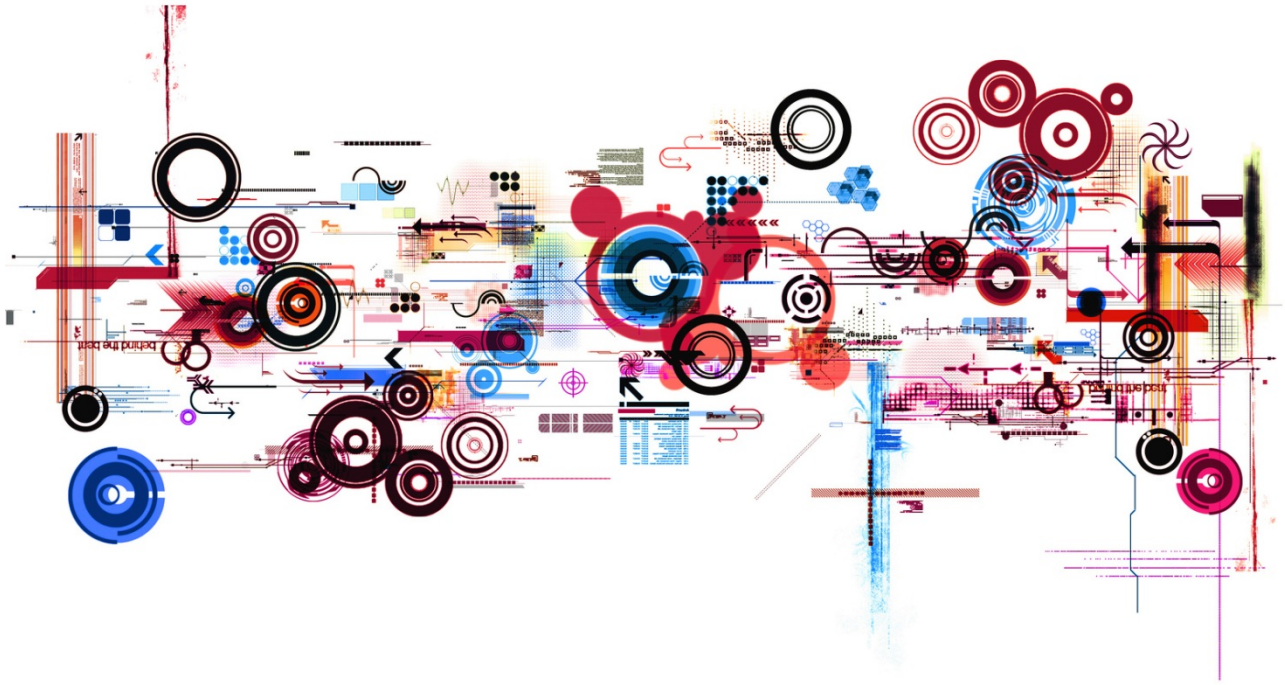
Überwachung von Unternehmenskommunikation

Am Beispiel von SSL Verbindungen



Überwachung von Unternehmenskommunikation

- Warum Überwachung?
- Technische Grundlagen
- Nutzerwahrnehmung von SSL-Verbindungen
- Schutzbereiche in der Kommunikation
- Vertragliche Verpflichtungen zur Sicherheit?
- Umsetzungsmöglichkeiten in Unternehmen

Überwachung von Unternehmenskommunikation

- Warum Überwachung?
- Technische Grundlagen
- Nutzerwahrnehmung von SSL-Verbindungen
- Schutzbereiche in der Kommunikation
- Vertragliche Verpflichtungen zur Sicherheit?
- Umsetzungsmöglichkeiten in Unternehmen

Warum Überwachung?

- Einsatz von Web-Anwendungen für unternehmenskritische Prozesse
- Hosting solcher Webanwendungen durch Dritte
- Einsatz von SSL Verschlüsselungen dadurch notwendig
- die Unternehmens-IT verliert durch Verschlüsselung den Einblick in Anwendungen und Transaktionen
- Verbreitung „gefährlicher“ Inhalte durch SSL-Tunnel oder Umgehung von Sicherheitsrichtlinien

Anwendungsbeispiele

- salesforce.com

- Einwahl über Browser mit HTTPS Verschlüsselung
- Einstellen unternehmenskritischer Daten in das System möglich
- Download z.B. der Kundendatenbank ohne Berechtigung

Anwendungsbeispiele

- facebook.com

- Einwahl über Browser mit HTTPS Verschlüsselung
- Nutzung z.B. nur als Social Network Manager im Unternehmen zulässig
- Malware/Virenüberwachung bei Nutzung durch Mitarbeiter erforderlich

Anwendungsbeispiele

- http://aws.amazon.com

- Einwahl unter anderem über Browser mit HTTPS Verschlüsselung
- Nutzung zur Komplettverwaltung von virtuellen Umgebungen
- z.B. Überwachung der Einhaltung der Sicherheitsrichtlinien

Überwachung von Unternehmenskommunikation

- Warum Überwachung?
- Technische Grundlagen
- Nutzerwahrnehmung von SSL-Verbindungen
- Schutzbereiche in der Kommunikation
- Vertragliche Verpflichtungen zur Sicherheit?
- Umsetzungsmöglichkeiten in Unternehmen

Transportprotokolle

HTTPS (Hypertext Transfer Protocol Secure)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Verschlüsselte Datenübertragung
Port:	443/TCP

HTTPS im TCP/IP-Protokollstapel:

Anwendung	**HTTP**				
Transport	**SSL/TLS**				
	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standards:	RFC 2818 (HTTP Over TLS, 2000)

[Docs] [txt|pdf] [draft-ietf-tls-rf...] [Diff1] [Diff2] [IPR] [Errata]

Updated by: 5746, 5878, 6176 — PROPOSED STANDARD, Errata Exist

Network Working Group — T. Dierks
Request for Comments: 5246 — Independent
Obsoletes: 3268, 4346, 4366 — E. Rescorla
Updates: 4492 — RTFM, Inc.
Category: Standards Track — August 2008

The Transport Layer Security (TLS) Protocol Version 1.2

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Table of Contents

Transportprotokolle

- Transport Layer Security (TLS)
- Vorgängerbezeichnung Secure Sockets Layer (SSL)
- hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet
- Ursprüngliche Entwicklung im Jahre 1994
- Aktueller Stand aus 2008
- Standard im HTTPS Protokoll und VPN

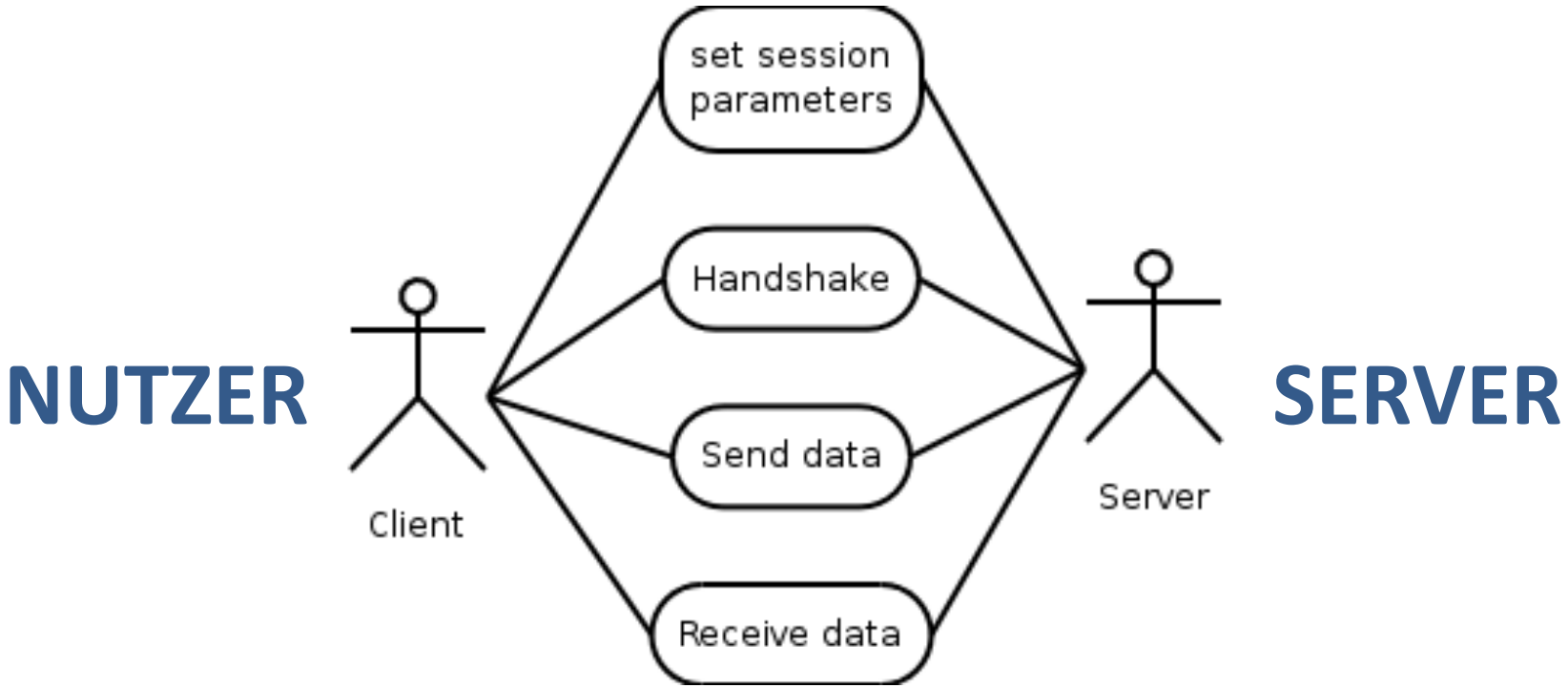
Funktionsweise des SSL/TLS Transportprotokolls

- Bei der Kommunikation werden folgende Ebenen angesprochen:

SSL im TCP/IP-Protokollstapel

Anwendung	HTTPS	IMAPS	POP3S	SMTPS	...
Transport	**SSL/TLS**				
	TCP				
Internet	IP				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Funktionsweise des SSL/TLS Transportprotokolls

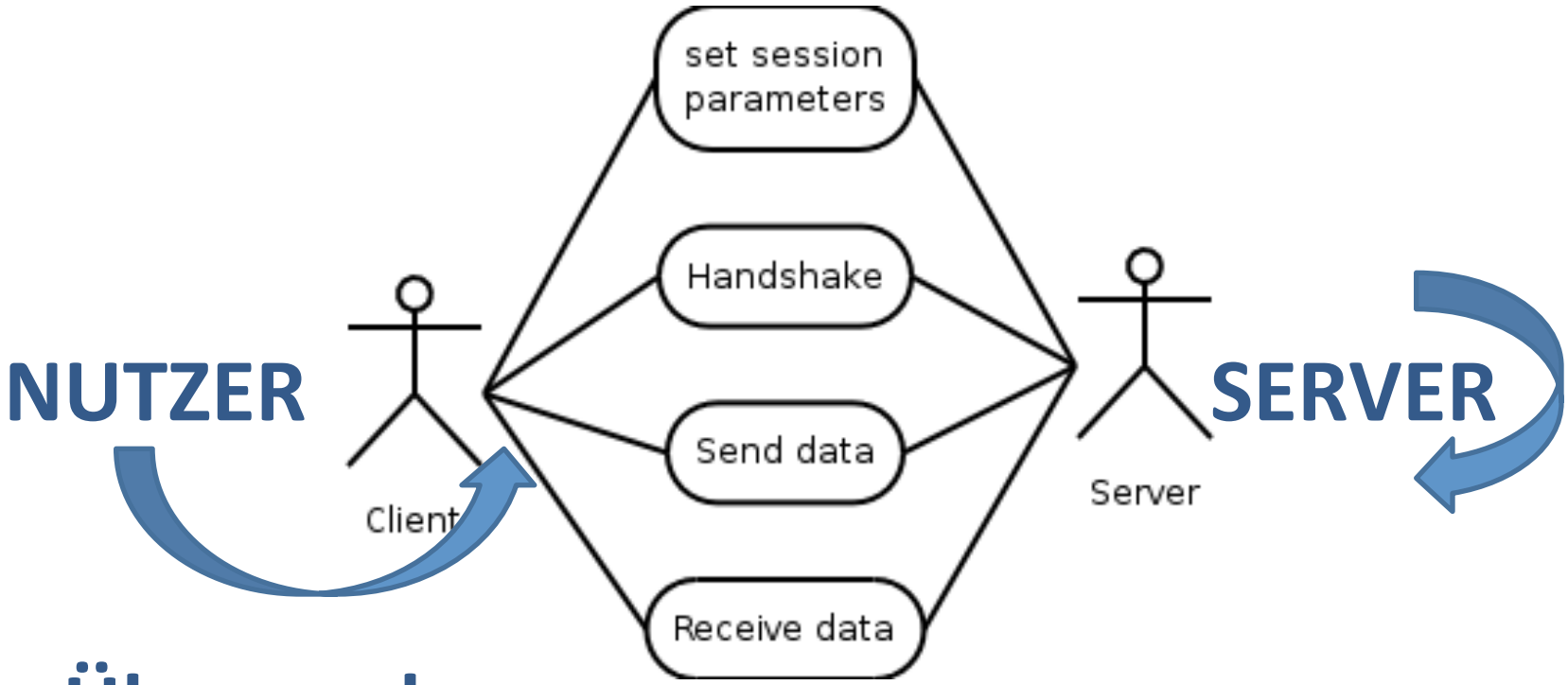


Übertragung

Funktionsweise des SSL/TLS Transportprotokolls

- Der Einsatz von SSL erfolgt dabei im TCP/IP-Protokollstapel nach dem Grundprinzip, dass ausgehend von der Anwendung (zum Beispiel der Browser), die vom Nutzer aufgerufen wird, das SSL/TLS Protokoll die Transportverschlüsselung zur Gegenstelle übernimmt.
- SSL verschlüsselt dabei nur die Kommunikation zwischen zwei Stationen.
- Es sind jedoch auch Szenarien (insbesondere in serviceorientierten Architekturen) denkbar, in denen eine Nachricht über mehrere Stationen gesendet wird.

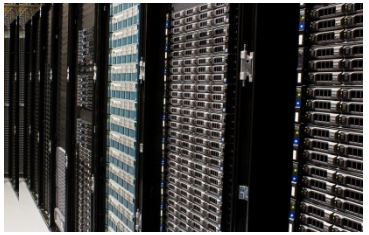
Überwachung des SSL/TLS Transportprotokolls



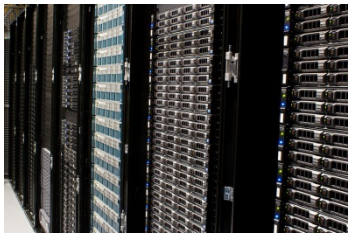
Überwachung

Überwachung des SSL/TLS Transportprotokolls

WWW über HTTPS

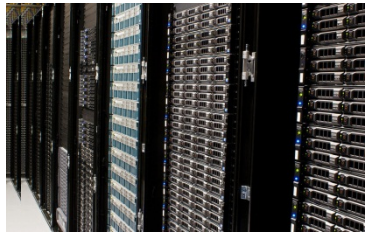


WWW
über HTTPS

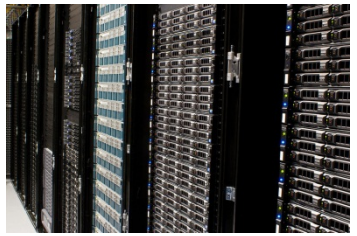


Überwachung des SSL/TLS Transportprotokolls

WWW über HTTPS



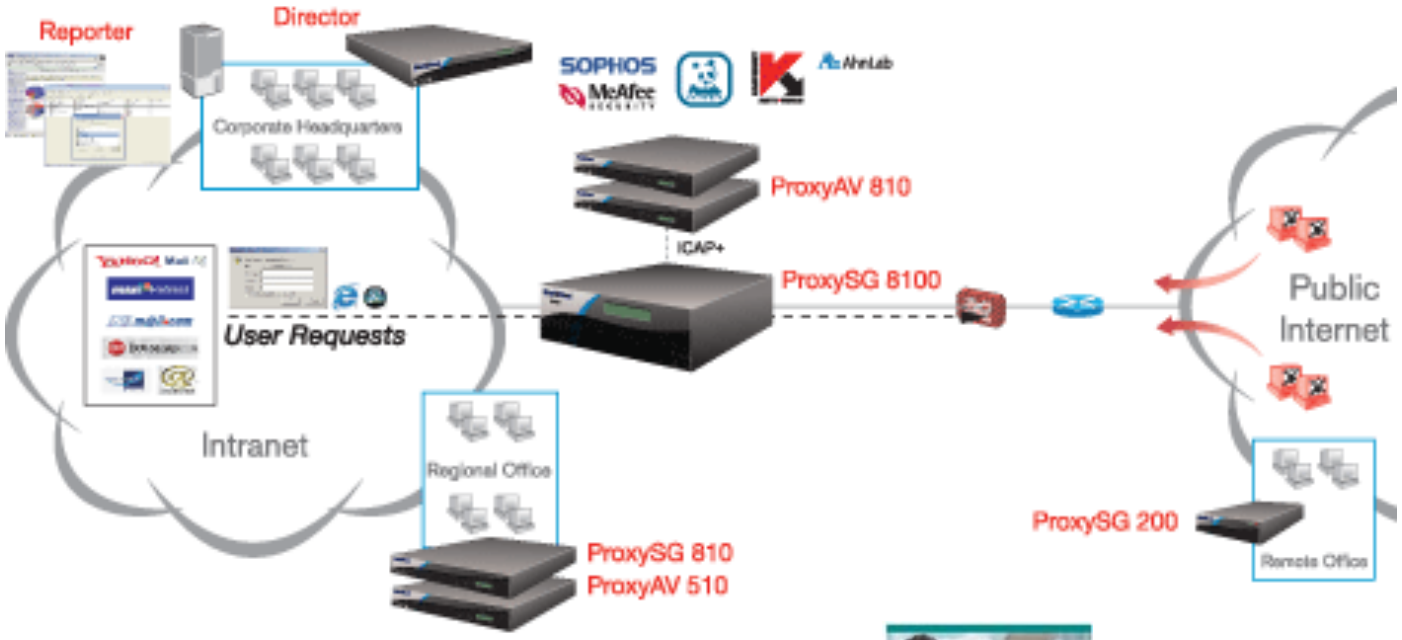
WWW
über HTTPS



Überwachung des SSL/TLS Transportprotokolls

- Die Möglichkeit innerhalb eines Netzwerkes den SSL/TLS Verkehr über mehrere Stationen zu leiten, nutzt die Überwachungstools und ermöglichen damit, die Inhalte innerhalb der Verbindung automatisiert technisch zu Überwachen und beispielsweise innerhalb der Verbindung nach Viren, Malware, Trojaner und vergleichbarer Schadsoftware zu scannen und gegebenenfalls die Verbindung bei Auftreten einer solche Schadsoftware zu unterbrechen, bevor sie beim Nutzer, der die ursprüngliche Anfrage ausgelöst hat, ankommt.

Marktanbieter mit SSL Überwachung



Marktanbieter mit SSL Überwachung

- WatchGuard® XTM 1050 und 2050
  - „Überprüfung aller Protokolle einschließlich HTTPS“
  - „Administratoren können genau feststellen, wann von wem eine Anwendung verwendet wird“
- Blue Coat ProxySG und ProxyAV Appliances
  - „der Proxy muss über Einblick in SSL-Verkehr die Kontrolle für (internen wie externen) SSL-Verkehr übernehmen“
  - „Prüfung des Wer, Was, Wann“
- Integralis Monitored SSL VPN
  - „Integralis überwacht Ihre SSL-VPN-Verbindung, analysiert ständig die Daten...“

VPN und andere verschlüsselte Verbindungen

- Ihrem Ursprung nach bilden VPNs innerhalb eines öffentlichen Wählnetzes in sich geschlossene virtuelle Teilnetze, wobei das VPN ein reines Softwareprodukt ist.
- Für die Kommunikation des zugeordneten Netzes mit einem seiner VPN-Partner werden am VPN-Gateway die ursprünglichen Netzwerkpakete in ein VPN-Protokoll gepackt und üblicher Weise mit SSL/TLS Verschlüsselung verschlüsselt.
- Auch wenn das virtuelle Teilnetz in einem „fremden“ Netz betrieben wird, ist grundsätzlich die Überwachung der Verbindung möglich.

Überwachung von Unternehmenskommunikation

- Warum Überwachung?
- Technische Grundlagen
- Nutzerwahrnehmung von SSL-Verbindungen
- Schutzbereiche in der Kommunikation
- Vertragliche Verpflichtungen zur Sicherheit?
- Umsetzungsmöglichkeiten in Unternehmen

Nutzerwahrnehmung von SSL Verbindungen

(Nicht nur) die Rente ist sicher!

Nutzerwahrnehmung von SSL Verbindungen

Aufgrund der hohen Verbreitung des SSL/TLS Protokolls, insbesondere durch standardmäßige Implementierung in allen verfügbaren Internet-Browsern, wird das Vorhandensein einer solchen Verbindung durch den Nutzer regelmäßig als sicher wahrgenommen.

Nutzerwahrnehmung von SSL Verbindungen

- Mit Secure Sockets Layer (SSL) können Sie auf sichere Webseiten zugreifen. Webseiten, die SSL verwenden, müssen "https" am Anfang ihrer Adresse führen. Die meisten Online-Banking-Seiten und Online-Shops verwenden SSL. (Hinweis aus Firefox)
- SSL/TLS-Protokoll soll gewährleisten, dass sensible Daten beim Surfen im Internet, beispielsweise Bankdaten, Kreditkarten-Informationen beim Online Shopping, oder sonstige persönliche Daten verschlüsselt übertragen werden. Somit soll verhindert werden, dass Dritt-Nutzer die Daten bei der Übertragung auslesen oder manipulieren können. Zudem stellt dieses Verschlüsselungs-verfahren die Identität einer Website sicher. (VeriSign Beschreibung)

Nutzerwahrnehmung von SSL Verbindungen

- Unsere Bank setzt sowohl technische als auch organisatorische Maßnahmen ein, um Ihre Daten vor zufälligen oder vorsätzlichen Manipulationen, Verlust, Zerstörung oder vor dem Zugriff unberechtigter Personen zu schützen. Unsere Sicherheitsmaßnahmen werden dem technologischen Fortschritt entsprechend weiterentwickelt. Organisatorisch sind alle Mitarbeiter unserer Bank im Rahmen des Bundesdatenschutzgesetzes auf das Datengeheimnis verpflichtet. Außerdem unterliegen sie dem Bankgeheimnis. (Auszug aus Bank AGB)

Nutzerwahrnehmung von SSL Verbindungen

Das Vertrauen des Nutzers in die SSL/TLS Verbindung wird dann grundsätzlich zunächst verletzt, wenn ein Eingriff in diese als „sicher“ angesehene Verbindung vorgenommen wird.

Überwachung von Unternehmenskommunikation

- Warum Überwachung?
- Technische Grundlagen
- Nutzerwahrnehmung von SSL-Verbindungen
- Schutzbereiche in der Kommunikation
- Vertragliche Verpflichtungen zur Sicherheit?
- Umsetzungsmöglichkeiten in Unternehmen

Schutzbereiche in der Kommunikation

- Die Integrität und die Vertraulichkeit von Daten, die im Rahmen von elektronischen Kommunikationsvorgängen übermittelt werden, sind durch verschiedene Ebenen des Rechts geschützt.
- Dabei ist bereits der Transportvorgang, in den durch die SSL/TLS Überwachung eingegriffen wird, Schutzgegenstand.
- Darüber hinaus unterliegen auch die entstehenden Daten über das Verhalten des Nutzers dem Schutz gesetzlicher Regelungen.

§ 88 TKG – Schutzbereich des Fernmeldegeheimnisses ?

- (1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
- (2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

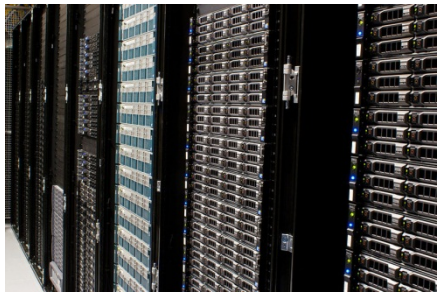
§ 88 TKG – Schutzbereich des Fernmeldegeheimnisses ?

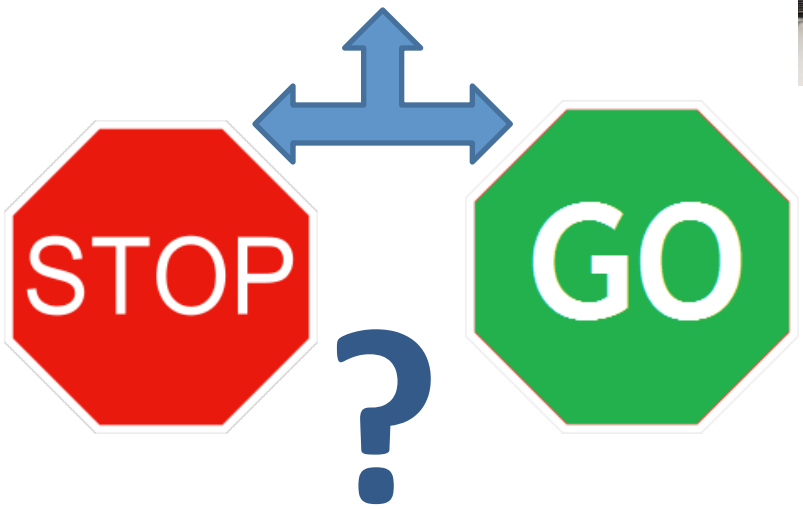
- Das Telekommunikationsgesetz (TKG) ist auf die Überlassung eines Internetzuganges nur dann anwendbar, wenn es sich bei dem Dienst um einen gewerblichen Telekommunikationsdienst für die Öffentlichkeit handelt.
- § 6 Abs. 1 TKG ist dabei Grundlage der Abgrenzung, da das TKG einerseits die „Öffentlichkeit“ des Dienstes erfordert und andererseits die „Gewerblichkeit“, die jedoch bei unentgeltlicher Leistungserbringung für einen beschränkten Personenkreis nicht angenommen wird.
- § 88 TKG gilt also nicht direkt für die Überlassung eines Internetzuganges im Rahmen eines Arbeitsverhältnisses, da der Arbeitgeber insoweit nicht als Diensteanbieter gilt.

Einwilligung in die Überwachung?

WWW

über HTTPS





§ 202a StGB Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202a StGB Ausspähen von Daten

- Schutzbereich:

  Die Vorschrift schützt nicht nur den persönlichen und den Geheimbereich des Nutzers, sondern auch das Interesse des Berechtigten, die in den übertragenen und/oder gespeicherten Daten verkörperten Informationen vor unberechtigtem Zugriff zu schützen. Die Vorschrift steht dabei in möglicher Tateinheit mit § 43 BDSG, soweit die übermittelten Daten personenbezogene Daten sind .

- Anwendbarkeit:

  Die Vorschrift ist auf elektronische Datenübermittlungen in Netzwerken und Fernmeldenetzen anwendbar und greift dann ein, wenn die übermittelten Daten durch besondere Sicherungen geschützt sind. Die Verschlüsselung durch das SSL/TLS Protokoll ist eine solche besondere Sicherung.

§ 202a StGB Ausspähen von Daten

- Einwilligungsfähigkeit:

Tatbestandsmerkmal des § 202a StGB ist, dass die Daten nicht für den „Täter“ bestimmt sind; für die Vollendung (oder den Versuch) des Delikts kommt es also auf die Rechtsmacht zur Verfügung über die Daten an. Willigt der Nutzer also in die Überwachung des Datenverkehrs ein, fehlt es schon an einem Tatbestandsmerkmal, wobei die Einwilligung ausdrücklich und unter Bezug auf den geschützten Bereich erfolgen muss und eine bereits, zum Beispiel nach § 4 Abs. 1 BDSG erteilte Einwilligung nicht ausreichend ist, da § 202a StGB keine Datenschutzvorschrift im Sinne des BDSG ist.

§ 202b StGB Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202b StGB Abfangen von Daten

- Schutzbereich:

  Die Vorschrift schützt Daten, die Gegenstand einer nicht öffentlichen Datenübermittlung sind. Die Regelungen der §§ 89, 148 TKG sind gegenüber § 202b StGB subsidiär, genauso wie § 202b StGB zu §§ 201, 202a StGB in Subsidiarität steht.

  - Anwendbarkeit:

  Die Vorschrift ist auf elektronische Datenübermittlungen in Netzwerken und Fernmeldenetzen anwendbar, wenn und soweit die Übermittlung noch nicht abgeschlossen ist und greift unabhängig davon ein, ob die übermittelten Daten durch besondere Sicherungen geschützt sind. Für das Tatbestandsmerkmal des Verschaffens ist es notwendig, dass die Daten abgefangen, kopiert oder umgeleitet werden oder jedenfalls in einen Arbeitsspeicher zur Darstellung auf einem Monitor geladen werden.

§ 202b StGB Abfangen von Daten

- Einwilligungsfähigkeit:

Tatbestandsmerkmal auch des § 202b StGB ist, dass die Daten nicht für den „Täter“ bestimmt sind; für die Vollendung (oder den Versuch) des Delikts kommt es also auf die Rechtsmacht zur Verfügung über die Daten an. Willigt der Nutzer also in die Überwachung des Datenverkehrs ein, fehlt es schon an einem Tatbestandsmerkmal, wobei die Einwilligung ausdrücklich und unter Bezug auf den geschützten Bereich erfolgen muss und auch hier eine bereits, zum Beispiel nach § 4 Abs. 1 BDSG erteilte Einwilligung nicht ausreichend ist, da § 202b StGB keine Datenschutzvorschrift im Sinne des BDSG ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

- Schutzbereich:

  Die Vorschrift umfasst die Schutzbereiche der §§ 202a und 202b StGB

  •Anwendbarkeit:

  Tatbestandsmerkmal des § 202c StGB ist, dass eine Straftat nach § 202a und/oder § 202b StGB vorbereitet werden soll, also der „Täter“, der eine Software im Sinne von § 202c StGB erwirbt (der Überwachungsmethoden umfassen Hard- und Softwarekomponenten), einen auf die Begehung einer Straftat nach §§ 202a, 202b, 303a, 303b StGB gerichteten Vorsatz hat . Die Vorbereitung der Straftat muss also gerade vom Vorsatz umfasst sein .

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

- Dabei ist davon auszugehen, dass so genannte „dual use“ Software, also Software die sowohl für rechtmäßige, wie auch für rechtswidrige Zwecke eingesetzt werden kann, vom Anwendungsbereich des § 202c StGB nicht umfasst ist:

„Nach alledem ließe es sich nicht vertreten, im Rahmen des § 202c Abs. 1 Nr. 2 StGB für die Bestimmung des Zwecks eines Computer-programms auf dessen Eignung oder auch spezifische Eignung abzustellen. Eine solche Auslegung würde dem Wortlaut der Norm und dem Willen des Gesetzgebers widersprechen und stellte damit gleichzeitig einen Verstoß gegen Art. 103 Abs. 2 GG dar. Die ... teilweise vertretene Auffassung, der objektive Tatbestand des § 202c Abs. 1 Nr. 2 StGB erfasse allgemein auch so genannte dual use tools, lässt sich nicht halten.“ (BVerfG Urteil vom 18.05.2009)

Rechtfertigungsgrund „berufliche Kommunikation“?

- Tatbestandsmerkmal der §§ 202a und 202b StGB:
  „*nicht für ihn bestimmt*“
- Ist von den beruflich genutzten Rechnern keinerlei private Kommunikation gestattet, könnten die vom Mitarbeiter aufgerufenen Daten als „im Namen des Arbeitgebers“ aufgerufen gelten.
- „Die Entscheidung über die Bestimmung trifft die zur Verfügung über die Daten berechtigte Person“. Ist aber der Arbeitgeber jeweils „zur Verfügung über die Daten“ berechtigt?
- Falls der Anwendungsbereich von §§ 202a und 202b StGB nicht eröffnet sind, kann auch keine Strafbarkeit nach § 202c StGB vorliegen.

Sonstige Schutzregelungen (§§ 203, 204 StGB)

- Die §§ 203 und 204 StGB erfassen im Schutzbereich eigentlich nicht den Eingriff in Daten, wie er im Rahmen der SSL/TLS Überwachung erfolgt und die Vorschrift ist nur dann direkt anwendbar, wenn der Nutzer einen der Katalogberufe des § 203 Abs. 1 Ziffern 1 bis 6 ausübt.
- Soweit im Einzelnen die Vorschrift anwendbar ist, ist der persönliche Lebens und Geheimbereich geschützt, also solche Tatsachen, die nicht allgemein bekannt sind und vom Betroffenen auch nicht allgemein bekannt gegeben werden wollen.

Sonstige Schutzregelungen (§§ 203, 204 StGB)

- Schutzbereich
  - Die §§ 203 und 204 StGB erfassen im Schutzbereich eigentlich nicht den Eingriff in Daten, wie er im Rahmen der SSL/TLS Überwachung erfolgt und die Vorschrift ist nur dann direkt anwendbar, wenn der Nutzer einen der Katalogberufe des § 203 Abs. 1 Ziffern 1 bis 6 ausübt.
  - Soweit im Einzelnen die Vorschrift anwendbar ist, ist der persönliche Lebens und Geheimbereich geschützt, also solche Tatsachen, die nicht allgemein bekannt sind und vom Betroffenen auch nicht allgemein bekannt gegeben werden wollen.
  - Die Tätigkeit als Syndikusanwalt ist von § 203 Abs. 1 Nr. 3 StGB nicht umfasst (EuGH C-550/07, AnwBl. 2010, 796)

Sonstige Schutzregelungen (§§ 203, 204 StGB)

- Anwendungsbereich
  - Anwendbar ist die Vorschrift insbesondere für als Rechtsanwälte tätige Mitarbeiter, die von ihrem Arbeitsplatz aus zulässiger Weise berufsbezogene Kommunikation betreiben, sowie zum Beispiel sämtliche Angehörige einer betriebsärztlichen Einrichtung im Hinblick auf deren Kommunikation.
  - Hierbei sind vom Schutzbereich sämtliche Informationen (ein- und ausgehend) umfasst, wenn durch die SSL/TLS Überwachung deren Geheimhaltung eingeschränkt wird.
  - Vom Schutzbereich umfasst ist dabei auch schon das Bestehen einer Kommunikationsverbindung, da eine solche auf eine anwaltliche Vertragsbeziehung oder betriebsärztliche Inanspruchnahme hindeutet.

Sonstige Schutzregelungen (§§ 203, 204 StGB)

- Anwendungsbereich
  - Gemäß § 203 Abs. 2 StGB ist weiter Ausnahme der betriebliche Datenschutzbeauftragte, der den Katalogberufen bezüglich der Informationen gleichgestellt wird, die ihm in seiner berufliche Eigenschaft anvertraut oder sonst bekannt geworden sind und von welchen er bei der Erfüllung seiner Aufgaben Kenntnis erlangt hat. Vom Schutzbereich umfasst sind hier also die Daten, die der betriebliche Datenschutzbeauftragte aus der SSL/TLS Überwachung erhält.
  - Anwendbar könnten die §§ 203, 204 StGB auch indirekt auf die Kommunikation von Mitarbeitern mit externen Personen, die unter § 203 Abs. 1 StGB fallen, sein, wenn durch die SSL/TLS Überwachung eine Verletzung des Geheimnisschutzes erfolgt, denn die externe Person wählt möglicher Weise die Übertragung in der SSL/TLS Verbindung gerade um ihrer Schutzverpflichtung nach §§ 203, 204 StGB nachzukommen.

Sonstige Schutzregelungen (§§ 203, 204 StGB)

- Einwilligungsfähigkeit
  - Die Einwilligung des Geschützten schließt die Strafbarkeit nach §§ 203, 204 StGB aus, wobei die Einwilligung ausdrücklich oder konkludent erfolgen kann und sich auf konkret bestimmte Geheimnisse beziehen muss.
  - Bei Anwendung auf die Kommunikation von Mitarbeitern mit externen Personen, die unter § 203 Abs. 1 StGB fallen, ist die Einwilligung des Mitarbeiters notwendig.
  - Problematisch ist die Kommunikation einer Person, die unter § 203 Abs. 1 StGB fällt aus einem „überwachten Netz“ heraus mit „Schutzberechtigten“, da hier wohl kaum eine entsprechende Einwilligung vorliegen dürfte. Beispielsfall: medizinischer Dienst bei Krankenversicherungen

§ 303a Datenveränderung

- Schutzbereich:

§ 303a StGB erfasst im Schutzbereich das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von fremden Daten.

- Anwendbarkeit:

Anwendbar ist die Vorschrift jedoch nur für gespeicherte Daten, nicht jedoch auf den Eingriff in den Datenübermittlungsvorgang als solchen, auch wenn eine technisch bedingte Zwischenablaufe auf Arbeitsspeichern oder in Netzwerken erfolgt.

- Einwilligungsfähigkeit:

Die Einwilligung des Geschützten schließt die Strafbarkeit nach §§ 303a StGB tatbestandsmäßig aus.

Datenschutzrechtliche Regelungen

- Schutzbereich:

Gemäß § 43 Abs. 1 Ziffer 3 BDSG handelt der ordnungswidrig, der vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft. Dabei kommt es weder auf die unmittelbare „Entnahme“ von personenbezogenen Daten, noch sonst auf einen bestimmten Kommunikationsweg oder eine Bestimmte Darstellung an, sondern nur darauf, dass die Information einer nur beschränkten Personenzahl bekannt oder zugänglich ist. Soweit die SSL/TLS Überwachung daher solche Daten zugänglich macht, ist der Schutzbereich dieser Regelung eröffnet.

Datenschutzrechtliche Regelungen

- Anwendbarkeit:

Eine Strafbarkeit nach §§ 44, 43 BDSG wegen der Verwendung personenbezogener Daten kommt nur dann in Betracht, wenn eine vorsätzliche Verwirklichung einer in § 43 Abs. 2 BDSG aufgezählten Tathandlung in Bereicherungs- beziehungsweise Schädigungsabsicht begangen wird . Eine Ordnungswidrigkeit im Sinne von § 43 BDSG kann jedoch auch fahrlässig begangen werden.

- Einwilligungsfähigkeit:

Die Einwilligung des Geschützten nach § 4 Abs. 1 BDSG schließt die Strafbarkeit/das Vorliegen einer Ordnungswidrigkeit nach §§ 44, 43 BDSG aus .

Überwachung von Unternehmenskommunikation

- Warum Überwachung?
- Technische Grundlagen
- Nutzerwahrnehmung von SSL-Verbindungen
- Schutzbereiche in der Kommunikation
- Vertragliche Verpflichtungen zur Sicherheit?
- Umsetzungsmöglichkeiten in Unternehmen

Vertragliche Vereinbarungen

- Neben den straf- und datenschutzrechtlichen Vorschriften kommen auch noch vertragliche (oder quasi vertragliche) Vereinbarungen in Betracht, die einen besonderen Schutz und/ oder ein Interesse der Vertragspartei an der „Unversehrtheit“ der SSL/TLS Verbindung begründen.

- Beispiele von Regelungen:
  - Um die Sicherheit Ihrer Informationen bei Übertragung zu schützen, benutzen wir Secure Sockets Layer Software (SSL). Diese Software verschlüsselt die Informationen, die von Ihnen übermittelt werden. (Beispiel aus Amazon und Banking AGB)
  - Du wirst dein Passwort (oder deinen geheimen Schlüssel, wenn du ein Entwickler bist) nicht weitergeben, eine andere Person auf dein Konto zugreifen lassen oder anderweitige Handlungen durchführen, die die Sicherheit deines Kontos gefährden können. (Facebook AGB)
  - Regelungen zur Geheimhaltung von Pin und Tan in den AGB für Onlinebanking.

Vertragliche Vereinbarungen

- Soweit diese vertraglichen oder quasi-vertraglichen Regelungen einseitig zugunsten des jeweiligen Nutzers gelten, kann dieser einseitig auf einzelne vertragliche Rechte verzichten. Daher ist in diesen Fällen eine Zustimmung oder Einwilligung der anderen Vertragspartei und somit des Betreibers des entsprechenden Webdienstes nicht erforderlich.
- Ein einseitiger Verzicht bei zweiseitigen Verpflichtungen der Vertragsparteien oder bei einer einseitigen Verpflichtung des Nutzers gegenüber der anderen Vertragspartei ist nach BGB jedoch nicht möglich. Hier wäre es erforderlich, dass die andere Vertragspartei zustimmt, also die Zustimmung oder Einwilligung dahingehend erteilt, dass der Nutzer die entsprechende vertragliche Verpflichtung nicht erfüllt.

Überwachung von Unternehmenskommunikation

- Warum Überwachung?
- Technische Grundlagen
- Nutzerwahrnehmung von SSL-Verbindungen
- Schutzbereiche in der Kommunikation
- Vertragliche Verpflichtungen zur Sicherheit?
- Umsetzungsmöglichkeiten in Unternehmen

Strafrechtlicher Schutzbereich

- Im Hinblick auf die Schutzbereiche der §§ 202a und 202b StGB sind vor dem Einsatz einer SSL/TLS Überwachung im Unternehmen individuelle, nachvollziehbare und dokumentierte Einwilligungserklärungen der betroffenen Mitarbeiter einzuholen, die ausdrücklich SSL/TLS Überwachung umfassen und über den tatsächlichen, technischen Vorgang Auskunft geben müssen.
- Die Erteilung oder Nicht-Erteilung einer Einwilligung ist zu dokumentieren, wobei eine Dokumentation in der Personalakte empfohlen wird.

Strafrechtlicher Schutzbereich

- Im Hinblick auf §§ 203 und 204 StGB ist sicherzustellen, dass solche Mitarbeiter des Unternehmens, die in den Katalog der geschützten Berufe fallen (insbesondere betriebs-medizinische Dienste), nicht der SSL/TLS Überwachung unterliegen, deren Arbeitsplätze also von der Überwachung ausgenommen werden.

- Bezüglich der nach §§ 203 und 204 StGB geschützten Geheimnisse kann empfohlen werden, die Kommunikation mit entsprechenden Webseiten und Diensten von der SSL/ TLS Überwachung auf Domainbasis auszunehmen.

Strafrechtlicher Schutzbereich

- Generell sollte in die Einwilligungserklärung auch bezüglich den §§ 203 und 204 StGB eine Einwilligung sowie ein Hinweis aufgenommen werden, so dass der Nutzer aufgrund dieser Informationen entscheiden kann, ob er die am Arbeitsplatz bestehende Verbindung für solche Kommunikationsvorgängen nutzen möchte, oder nicht.

Strafrechtlicher Schutzbereich

- Weiter sollte die Einwilligungserklärung auch den Schutzbereich des § 303a StGB im Hinblick auf das Merkmal „Unterdrücken“ umfassen, da durch die SSL/TLS Überwachung jedenfalls für eine gewisse, wenn auch kurze Zeit, die Übermittlung der Daten an den Nutzer ausgesetzt wird. Dazu wird vorgeschlagen, dass im beschreibenden Teil der Einwilligungserklärung auf die Verzögerung hingewiesen wird und sich dann die generelle Einwilligung auch auf diesen Bereich erstreckt.

Datenschutzrechtlicher Schutzbereich

- Die Einwilligung des Nutzers muss neben den Einwilligungen aus dem strafrechtlichen Bereich auch die datenschutzrechtliche Einwilligung enthalten, wobei hier die allgemeinen Grundsätze des § 4 Abs. 1 BDSG gelten und insbesondere über den tatsächlichen, technischen Vorgang sowie die anfallenden Daten und deren Speicherung und Verwendung Auskunft geben werden muss.

Besonderheiten der Einwilligung

- Die Einwilligung muss dem Nutzer, der die Einwilligung erteilen soll, einen ausreichenden und für ihn verständlichen Überblick über das, wozu er zustimmt gegeben werden, so dass eine entsprechende Überschaubarkeit der Tragweite seiner Entscheidung besteht.
- Wesentlich dabei ist, dass die Einwilligung – und zwar sowohl die für die strafrechtlichen, wie auch die für die datenschutzrechtlichen Schutzbereiche – jeweils auf freiwilliger Basis erfolgt und der klare zustimmende Wille des Nutzers erkennbar und dokumentiert ist.

Umsetzungsbezogene Besonderheiten

- Anpassung/Erstellung von Betriebsvereinbarungen

Zur Umsetzung des Konzepts der Einwilligungserklärungen und eines abgestuften Überwachungskonzeptes mit Ausnahmeregelungen für einzelne Datenströme oder Ziele sind bestehende Betriebsvereinbarungen anzupassen oder neu zu erstellen.

- Einbindung des Datenschutzbeauftragten und Betriebsrates

Bei der Umsetzung eines Konzepts von Einwilligungserklärungen und eines abgestuften Überwachungskonzeptes mit Ausnahmeregelungen für einzelne Datenströme oder Ziele ist der betriebliche Datenschutzbeauftragte einzubinden und die Zustimmung des Betriebsrates einzuholen. Dabei ist auch abzustimmen, wie die jeweilige Zustimmung des einzelnen Nutzers erfolgt und dokumentiert wird. Die Personen, die Zugang zu den entstehenden Daten haben, sind auszuwählen und zu überwachen; für den Umgang mit den Daten sind Anweisungen zu erlassen.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT !

FÜR RÜCKFRAGEN

ANWALTSCONTOR

RECHTSANWALT CHRISTIAN R. KAST
WWW.ANWALTSCONTOR.DE
ITANWALT @ TWITTER

Literatur zum Thema

- Beck´sches Mandatshandbuch IT Recht, Hassemer § 36 Rz. 58 ff.
- Kusnik, Abfangen von Daten, MMR 2011, 720ff.,
- Fischer, StGB, § 201 Rz. 9, § 202a Rz. 12
- Lencker/Winkelbauer, Computerkriminalität, CR 1986, 485f.
- Ernst, Das neue Computerstrafrecht, NJW 2007, 2661, 2662 f.
- BVerfG Urteil vom 18.05.2009, 2 BvR 2233/07, Randziffer 60 http://www.bundesverfassungsgericht.de/entscheidungen/rk20090518_2bvr223307.html
- Fischer, StGB, § 303a Rz. 3
- Simitis/Ehrmann, BDSG, § 43 Rz. 54/61, § 44 Rz. 3, 5 ff.
- Kind/Werner, Rechte und Pflichten im Umgang mit Pin und Tan, CR 2006, 353, 354
- Münchner Kommentar, BGB § 397 BGB Rz. 19
- *Helmes/Pohle*, Beck´sches Mandatshandbuch IT Recht, § 29 Rz. 40