

# Dienstleistungen zum Sicherheitscheck

# Übersicht

- Öffentliche Stellen
- Dienstleistungen:
  - Outsourcing
  - Penetrationstests
  - Consulting
  - Schulungen
  - Zertifikate und Signaturen
  - IT- Forensik
  - Hardware vernichten

# Finanzvolumen

- 2003 wurden 11 Milliarden US\$ für Sicherheitssoftware ausgegeben
- Schäden durch MSBlaster und SQLSlammer betragen ca. 35 Milliarden US\$
- Markt für IT-Sicherheit wächst
- Nach Schätzungen erhöhen sich die Ausgaben für IT-Sicherheit bis 2007 um jährlich 18%

3/42

Quelle: Studien von Marktforschungsunternehmen Merrill Lynch und IDC

# Öffentliche Stellen

- Bundesamt für Sicherheit in der Informationstechnik
- Statistisches Bundesamt

# BSI

- Def des BSI Sicherheit
- Historie
- Aufgaben
- Themen
- Dienstleistungen
- Produkte/ Tools

## Bundesamt für Sicherheit in der Informationstechnik

- Zentraler IT-Sicherheitsdienstleister des Bundes
- Für die IT-Sicherheit in Deutschland verantwortlich
- Ziel: sicherer Einsatz von Informations- und Kommunikationstechnik
- Kunden: Verwaltungen in Bund, Ländern und Kommunen, Unternehmen und Privatanwender

6/42

# Aufgaben

- Bewertung der Auswirkungen und Folgen neuer Entwicklungen
- Festlegung von Sicherheitsstandards
- Dienstleistungen in den Bereichen:
  - Information
  - Beratung
  - Entwicklung
  - Zertifizierung

7/42

Informationen zu den wichtigen Themen der IT-Sicherheit

Beratung in Fragen der IT-Sicherheit und Unterstützung bei der Umsetzung geeigneter Maßnahmen.

Entwicklung: Konzeption und Entwicklung von IT-Sicherheitsanwendungen und –produkten

Zertifizierung: Prüfung, Bewertung und Zertifizierung von IT-Systemen auf die Sicherheitseigenschaften, ebenso Zulassung für Systeme zur Verarbeitung von geheimen Daten

# Geschichte

- 1986: Zentralstelle für Chiffrierwesen bekommt Arbeitsbereich „Computersicherheit“ hinzu
- 1989: Umwandlung in die Zentralstelle für die Sicherheit in der Informationstechnik
- Gründung des BSI
- 2001: BSI wird zum zentralen IT-Sicherheitsdienstleister des Bundes

# Themen

- Biometrie
- ePass
- E-Government
- Internet- Sicherheit
- IT- Grundschutz
- Zertifizierung und Akkreditierung

9/42

Die Themen etwas ausführlicher:

Biometrie: Untersuchung wie sicher biometrische Daten sind und wie man diese Daten nutzen kann

ePass: Hinzufügen biometrischer Daten in den Personalausweis und den Reisepass. Was sind Probleme, die dafür beseitigt werden müssen.

E-Government: Soll die Möglichkeit bieten, dass Bürger viele Behördengänge vom PC zu Hause erledigen können. Das BSI sorgt für sichere Standards

Internet-Sicherheit: Das BSI berät, wie man sicher im Internet surfen kann

IT-Grundschutz: Gibt Tipps, welche Sicherheitsmerkmale ein System mindestens haben sollte

Zertifizierung und Akkreditierung: Das BSI zertifiziert Firmen, die ihrerseits Sicherheit als Dienstleistung anbieten. Zertifizierte Firmen arbeiten nach den Standards des BSI.

## Produkte und Tools

- Das BSI stellt zum Einen Software für Behörden und öffentliche Einrichtungen zur Verfügung
- Manche Softwareprodukte können auch von Firmen und Privatpersonen genutzt werden:
  - Chiasmus, Verschlüsselungssoftware für Windows- PCs

# Statistisches Bundesamt

- Einsatz von Sicherheitseinrichtungen in Unternehmen mit Internetzugang 2005(2004):

	Viren - SW	Firewall	Sichere Server	Ext. Festpl.	Dig. Unterschr.	Verschl. Datenübertr.
Insges.	91(89)	72(59)	31(33)	73(70)	7(10)	27(31)
Mineralöl- verarb.	100(100)	100(43)	72(38)	100(100)	28(68)	67(90)
F&E	92(77)	83(62)	41(59)	83(63)	11(6)	20(23)
Bau- gewerbe	87(84)	62(44)	19(19)	68(61)	6(8)	16(24)

11/42

Quelle: Tabellenband „Informationstechnologien in Unternehmen“ 2004 und 2005

# Dienstleistungen

- Outsourcing
- Penetrationstests
- Consulting
- Schulungen
- Zertifikate und Signaturen
- IT Forensik
- HW vernichten

# Outsourcing

- Zwei Arten von Outsourcing
  - Von IT Sicherheit
  - Von Daten als zusätzliche Sicherheit

# Outsourcing von Hardware

- Def.: in der Ökonomie: Abgabe von Unternehmensaufgaben und –strukturen an Drittunternehmen
- IT-Outsourcing-Markt hat ein Volumen von 8-10 Milliarden €
- Durchschnittliches Wachstum von 10-12% in den Jahren 2002 bis 2008

14/42

Quelle: [www.wikipedia.de](http://www.wikipedia.de)

# Outsourcing

- Formen des Outsourcings:
  - Out-tasking
  - Selective Outsourcing
  - Transitional Outsourcing
  - Comprehensive Outsourcing
  - Business Transformation Outsourcing
  - Business Process Outsourcing
  - Out-servicing

15/42

## Formen des Outsourcings

Es werden verschiedene Arten des Outsourcings unterschieden, wobei die Definitionen erheblich variieren:

**Out-tasking:** Einzelne Funktionen oder Prozesse eines Unternehmens werden an einen Dienstleister übertragen, Personal oder Assets gehen nicht über. Alternativ kann auf technischer Ebene das Out-tasking auch als das Auslagern einfacher elementarer Operationen, Funktionen und Methoden z. B. Lese-/Schreiboperationen oder Lookup-Methoden von Applikationen verstanden werden. Häufig wird diese Bezeichnung auch bei der Auslagerung bzw. Integration von Web Services, die von Service Providern angeboten werden, verwendet.

**Selective Outsourcing:** Spezielle Teile eines Bereiches werden an ein Drittunternehmen vergeben. Das primäre Ziel ist meist nicht Kosteneinsparung, sondern etwa die Kompensation mangelnden Wissens oder mangelnder kritischer Masse im Unternehmen. Werden z. B. IT-Applikation im Unternehmen eingeführt, ist dies oft der Anlass den Betrieb dieser Lösungen an ein Drittunternehmen zu vergeben und dieses Spezialwissen nicht aufzubauen. Outtasking und Selective Outsourcing werden jedoch häufig synonym verwendet.

**Transitional Outsourcing:** Ein Prozess wird während des Technologiewechsels in einem Unternehmen an einen Dienstleister übertragen, der sowohl Kompetenzen in der Ist- und Ziel-Technologie besitzt.

**Comprehensive Outsourcing** oder **Complete Outsourcing:** Ein ganzer *Unternehmensbereich* wird ausgelagert, beispielsweise die EDV eines Unternehmens wird an einen IT-Dienstleister für eine Vertragslaufzeit von 10 Jahren übergeben. Dabei wechseln nicht nur die „Assets“, sondern auch große Teile der betroffenen Belegschaft in das Drittunternehmen.

**Business Transformation Outsourcing** oder **Transformational Outsourcing** meint die integrale Verbindung von Business Consulting und Outsourcing. Ein übernommener Unternehmensteil oder -prozess wird nach „Best-in-Class“-Methoden reorganisiert und dann entweder betrieben oder rücküberführt. Im Gegensatz zu klassischem Business Consulting übernimmt der Dienstleister Verantwortung für die Realisierung der identifizierten Optimierungspotentiale. Eine Zwischenform zwischen Transformational Outsourcing und Business Process Outsourcing wird zum Teil auch unter dem Stichwort „Business Innovation and Transformation Partner“ (BITP) diskutiert.

**Business Process Outsourcing:** Bei dieser Spielart wird ein ganzer *Unternehmensprozess* an ein Drittunternehmen gegeben. Beispielsweise kann der Unternehmensprozess Einkauf ausgelagert werden, das heißt, das Drittunternehmen verhandelt und besorgt für den auslagernden Betrieb beispielsweise günstigere Konditionen bei der Beschaffung. Weitere Beispiele sind HR-Management, Payroll-Processing oder Transaktions-Banking. Oft handelt es sich um IT-intensive Prozesse, die an entsprechend spezialisierte Dienstleister abgegeben werden.

**Out-servicing:** Hierbei werden in Anlehnung an das *Business Process Outsourcing* Geschäftsprozesse oder Aggregationen von Geschäftsprozessen ausgelagert, die nach dem Paradigma Serviceorientierter Architekturen (SOA) gestaltet wurden. Hierbei können Services – gekapselte, wiederverwendbare und lose koppelbare betriebliche Funktionseinheiten – in unterschiedlichen Feinheitsgraden, d. h. sehr fein als Elementarfunktion und gröber als gesamthafter Geschäftsprozess ausgelagert werden. Out-servicing kann als Outsourcing bzw. Out-tasking unter Anwendung der Paradigmen des SOA verstanden werden.

[www.wikipedia.de](http://www.wikipedia.de)

# Outsourcing

- Risiken:
  - Qualität
  - Abhängigkeit von Drittunternehmen
  - Schutz des Know Hows

16/42

## Risiken

Ein entscheidender Punkt ist die **Qualität** der ausgelagerten Prozesse, die nur indirekt beeinflusst werden kann.

Durch das Outsourcing vor allem bei Schlüsselprozessen kommt es zu einer risikobehafteten **Abhängigkeit von Drittunternehmen**.

Weiterhin ist der **Schutz des Know-Hows** bei der Vergabe von Leistungen an Dritte oft nicht sicher gestellt.

[www.wikipedia.de](http://www.wikipedia.de)

# Outsourcing

- Gründe für Outsourcing:
  - Unternehmen benötigen hochqualifiziertes Personal und aktuelle Sicherheitsinfrastruktur  
Basistools: Anti-Spam, Anti-Viren-Lösungen
    - Dafür entstehen Kosten durch zus. HW und Lizenzgebühren oder Entwicklungskosten bei Inhouse-Entwicklung
    - Personalkosten durch Administration von Spam- und Virenfilter und Support.

17/42

T. Koehler

# Outsourcing

- **Alternative: Managed Security Services (MSS)**
  - Kosten werden von dem Dienstleister auf mehrere Kunden verteilt
  - Interessant gerade für kleinere Firmen
- **Fremdvergabe ist große Vertrauensfrage**
- **Bisher:**
  - Hauptsächlich große Firmen nutzen MSS
  - Großes Potential gerade für mittelständische Unternehmen

18/42

<http://www.competence-site.de/>

# Outsourcing

- Verisign Managed Security Services:
  - Managed Firewall
  - Managed Intrusion Detection
  - Managed Vulnerability Protection Service
  - Managed Vulnerability Alerting
  - Managed VPN
  - Managed Incident Response and Forensics
  - iDefense Security Intelligence Services
  - Phishing Response

19/42

Um die Rechner einer Firma sicher zu verwalten benötigt man eine 24-stündige Überwachung

Ein Beispiel für einen solchen Anbieter ist Verisign:

## **Managed Security Services**

**Managed Firewall:** Die Managed Firewall Services (MFS) von VeriSign bieten für die wichtigsten Informationsgüter eine fortschrittliche, vollkommen ausgelagerte Firewall zum Schutz von Netzwerken, Hosts, Anwendungen und Datenbanken. Die benutzerdefinierten Firewall-Services gewährleisten ein hohes Maß an Netzwerkzugriff sowie Verfügbarkeit, Integrität und Schutz von Informationen. Die permanente Firewall-Überwachung generiert unverzüglich Alarme und Reaktionen für Service-Ausfälle und Sicherheitsalarme, die mit kritischen Internetzugangspunkten verknüpft sind.

**Managed Intrusion Detection:** Der Managed Intrusion Detection Service (IDS) von VeriSign ermöglicht die Überwachung von Netzwerkverkehr rund um die Uhr. Der Service fungiert als Alarmsystem für ein Unternehmensnetzwerk und löst die erforderlichen Warnungen aus, wenn ein potenzieller Angriff erkannt wird. Die zertifizierten Sicherheitsexperten von VeriSign überwachen diese Warnungen aktiv im Security Operations Center (SOC) des Unternehmens.

**Managed Vulnerability Protection Service (MVPS):** Der Managed Vulnerability Protection Service (MVPS) von VeriSign ist die ideale Lösung für Organisationen, die kundenspezifischen, kosteneffektiven und ununterbrochenen Schutz vor der Ausnutzung von Sicherheitslücken suchen. Zu seinen Bausteinen zählen eine Vorabrisikoanalyse und regelmäßiges Scannen nach Sicherheitslücken, Sicherheitslückenbeurteilungen sowie Penetrationsprüfungen.

**Managed Vulnerability Alerting:** VeriSign stellt als Ergänzung zum Managed Vulnerability Protection Service (MVPS) einen Warndienst bereit, der aufkommende Bedrohungen mit einer hostbasierten MVPS-Datenbank abgleicht, die Kunden absolut aktuelle Hintergrundinformationen zu Sicherheitslücken bereitstellt.

**Managed VPN:** Der VeriSign Managed Virtual Private Network (VPN) Service verwaltet die Client-Autorisierung und die Zugangskontrolle für Organisationen, die eine sichere, kosteneffiziente Methode benötigen, um den Fernzugang zu kritischen Onlineinformationen zu erhöhen.

**Managed Incident Response and Forensics:** Basierend auf den fünf Hauptkomponenten des effektiven Zwischenfall-Managements – Erkennung, Bewertung, Forensik, Eindämmung und Wiederherstellung – nutzen die Managed Incident Response and Forensics Services von VeriSign die Best Practices der Branche, um eine vollständige und angemessene Reaktion auf Sicherheitsverletzungen zu gewährleisten.

**VeriSign iDefense Security Intelligence Services:** Dank der großartigen Erweiterung der VeriSign MSS-Funktionen um VeriSign iDefense, kann VeriSign erstklassige Dienste anbieten, die proaktiv und unmittelbar Informationen zur Verfügung stellen, auf deren Basis unsere Kunden auf Bedrohungen und Schwachstellen reagieren können.

**Phishing Response:** Der VeriSign Phishing Response Service nutzt die weit reichende Erfahrung von VeriSign im Bereich Internet-Betrug sowie das internationale Unternehmensnetzwerk von Kontakten in Rechts-, Regierungs- und ISP-Gemeinschaften in dem Bestreben, Quellen von Phishing-Angriffen zu identifizieren und Websites sowie Konten schnell zu schließen.

[www.verisign.de](http://www.verisign.de)

## Auslagern von Daten

- Daten können aus verschiedenen Gründen verloren gehen
- Deshalb gibt es Backups
- Wenn es in einer Firma brennt, bringt ein solches Backup nichts
- Deshalb bieten Firmen die Möglichkeit Daten auf ihren Rechnern zu speichern

20/42

# Auslagern von Daten

- Es gibt verschiedene Arten des Backups:
  - Differentielles Backup
  - Inkrementelles Backup
  - Vollständiges Backup
- Beispiel für einen Anbieter EUnet:
  - Backup 512: 500MB Speicher 19,-€/Monat
  - Backup 1024: 1GB Speicher 29,-€/Monat
  - Zuzüglich MwSt.

21 / 42

## Backupversionen:

**Differentielles Backup:** Hier werden die seit dem letzten vollständigen Backup geänderten Daten vollständig gespeichert.

**Inkrementelles Backup:** Hier werden nur die Daten gesichert, die sich seit der letzten (meist dem letzten inkrementellen Backup) verändert haben.

**Vollständiges Backup:** Diese Art bezeichnet man als die Sicherung aller Daten unabhängig vom Datum ihrer letzten Sicherung.

## Bsp.: EUnet.at:

Bei der Basisvariante EUnet Backup-Flex ersparen sich Kunden die gesamte monatliche Grundgebühr und bezahlen nur den tatsächlich genutzten Speicherplatz und Datentransfer - entwickelt für Firmen, die ihr Datenaufkommen genau kennen und volle Kostentransparenz schätzen.

Für nur EUR 19,- (exkl. MwSt.) pro Monat erhalten Kunden mit EUnet Backup 512, der idealen Lösung für kleine und mittlere Unternehmen, 500 MB Speicherplatz.

EUnet Backup 1024 inkludiert für nur EUR 29,- (exkl. MwSt.) pro Monat 1 GB Speicherplatz - konzipiert für Firmen mit größeren Datenvolumina.

Speziell für Unternehmen mit einem bestehenden Backup-Server wurde EUnet Backup-Server entwickelt. Diese Lösung inkludiert für monatlich EUR 160,- (exkl. MwSt.) eine spezielle Server-Software und 1 GB Speicherplatz.

## Backup im Tresor

- Für besondere Sicherheit
- Grundgebühr: 149,00 EUR/Monat
- inkl. 1 Client und 1 GB Speicherplatz
- *Einrichtungsgebühr: 199,00 EUR*

22/42

<http://www.it-workgroup.com/de/sites/start.php>

## Der eigene Tresor

Typ	Oslo 1	Oslo2
Aussenmaße	635x540x620	635x540x755
Innenmaße	400x380x387	400x380x522
Gewicht	185kg	201kg
Preis	1254,33€	1456,41€



23/42

# Penetrationstests

- **Definition:**
  - Bezeichnung für eine Sicherheitsüberprüfung eines Netzwerk- oder Softwaresystems aus Sicht eines Hackers
- **Zielsetzung:**
  - Identifikation von Schwachstellen
  - Erhöhung der Sicherheit
  - Bestätigung der Sicherheit durch einen Dritten
- **Einschränkung:**
  - Ein Test ist nur Momentaufnahme

24/42

## **Testaufbau und Durchführung**

Das Bundesamt für Sicherheit in der Informationstechnik Deutschland (BSI) hat ein Klassifikationsschema entwickelt, anhand dessen sich ein Test beschreiben lässt. Im Wesentlichen werden sechs verschiedene Kriterien betrachtet:

Informationsbasis

Aggressivität

Umfang

Vorgehensweise

Technik

Ausgangspunkt

Anhand dieser Kriterien wird dann zusammen mit dem Kunden ein individueller Test zusammengestellt. In der Praxis werden meist mehrstufige Tests durchgeführt, bei denen mehrere Kriterien nacheinander zur Anwendung kommen. Beispielsweise wird zuerst ein Blackbox-Test und danach ein Whitebox-Test durchgeführt. Im Test selbst werden einzelne Testmodule ausgeführt. Bei den Testmodulen werden I- und E-Module unterschieden. I-Module bezeichnen Testschritte die zur reinen Informationsbeschaffung dienen, E-Module bezeichnen aktive Eindringungsversuche. Einem E- Modul geht entsprechendes meist ein I- Modul voraus.

# Penetrationstests

- Risiken
  - Es kann zu Störungen des normalen Betriebs kommen (DoS-Attacken)
  - Es kann evtl. auch zu Abstürzen von Systemen kommen
  - Tester könnten an unternehmenskritische Informationen kommen

25/42

Quelle: [www.wikipedia.de](http://www.wikipedia.de)

# Penetrationstests

- Secorvo Security Consulting
  - Analyse der Architektur
  - Ist-Aufnahme
  - Black-Box Analyse
  - White-Box Analyse
  - Auswertung und Priorisierung
  - Maßnahmenvorschläge
  - Dokumentation

26/42

Ist-Aufnahme: Feststellung des Ist-Zustandes

Black-Box Analyse: Technische Überprüfung ohne genauere Systemkenntnisse unter Verwendung unterschiedlicher Analyse-Tools

White-Box Analyse: Technische und organisatorische Überprüfung der Sicherheitssysteme, auch nach BSI "Grundschutzaudit"

Auswertung und Priorisierung: Bewertung aufgedeckter Schwachstellen

Erarbeitung von technischen und organisatorischen

Maßnahmenvorschlägen zur Behebung von etwaigen Schwachstellen

Ausführliche Dokumentation der Analyse und Ergebnisse

Quelle: [www.secorvo.de](http://www.secorvo.de)

# Penetrationstests

- **"tajanas" Security-Scanner**

<b>Anzahl Systeme</b>	<b>Rabatt</b>	<b>Preis pro IP (netto)</b>
• 1-10	Basispreis	125,00 €
• 11-20	20%	100,00 €
• ab 51	50%	62,50 €

- **tajanas Security-Scanner Appliance**

<b>Installation auf vorhandener Hardware</b>	<b>Preis (netto)</b>
• <b>Leistung</b>	
• Preis 1. Jahr inkl. Installation und Updates	6500,00 €
• Preis jedes weitere Jahr für Updates	3500,00 €
• Einspielen der Updates pro Jahr per Remote-Access	1500,00 €

27/42

Quelle: <http://www.security-scans.de>

# Consulting

- Analyse der vorhandenen Netzwerkumgebung
- Bewertung der vorhandenen Netzwerksicherheit und –leistung
- Überwachung der System- und Netzwerkleistung
- Backupkonzepte
- System-Recovery-Konzepte
- Inhaltsprüfung (Virenschutzlösungen, Webfiltering, Content Scanning und Spamfilter)
- Durchführung von Sicherheitsbewertungen
- Sicherheitsplanung
- Beratung bei der Auswahl von Sicherheitssystemen
- Systemüberwachung und Fernwartung

28/42

[www.unimeco.com](http://www.unimeco.com)

[www.envel.com](http://www.envel.com)

# Schulungen

	Dauer	Preis
Ausbildung zum IT-Sicherheitsbeauftragten mit Prüfung	4 Tage	2350,00 EUR
Checkpoint Grundlagen der Netzwerksicherheit	3 Tage	1750,00 EUR
IT-Sicherheit im Brennpunkt des Rechts	2 Tage	1250,00 EUR
IT-Sicherheit nach BSI-Richtlinien	3 Tage	1650,00 EUR
IT-Sicherheits- und Risk Management	2 Tage	1250,00 EUR
Backup und Disaster – Recovery	2 Tage	1795,00 EUR
Mobile Security	1 Tag	678,00 EUR
Wireless Security	1 Tag	819,00 EUR

29/42

# Bereitstellung von Zertifikaten und Signaturen

- Elektronische Signaturen sind eine Art „digitale Unterschrift“
- Richtlinien nach dem deutschen Signaturgesetz
- Es wird öffentlicher Signaturschlüssel benutzt
- Man sieht ihm nicht an, ob er von dieser Person kommt
- Nachweis über Echtheit:
  - Man benötigt qualifizierte Zertifikate, die bestätigen, dass die Signatur tatsächlich zu der Person gehört
  - Zertifikate werden von Firmen angeboten
  - Diese müssen ihre Echtheit nachweisen
  - Rekursiv bis zur Wurzel, die Bundesnetzagentur

30/42

Zur Prüfung einer qualifizierten elektronischen Signatur wird ein öffentlich verfügbarer Signaturprüf Schlüssel ([Public Key](#)) benutzt. Diesem Prüf Schlüssel ist jedoch nicht anzusehen, ob er möglicherweise von einer nicht autorisierten Person stammt. Eine nicht autorisierte Person könnte einen Signaturschlüssel zur Erstellung einer Signatur und einen zugehörigen Prüf Schlüssel z. B. mit einer Software wie [PGP](#) selbst erstellen und anschließend Signaturen mit dieser Software unter falschem Namen erstellen und als qualifizierte elektronische Signaturen einer anderen Person ausgeben.

Daher wird ein Nachweis der Echtheit des Prüf Schlüssels benötigt. Zu diesem Zweck sieht das SigG für qualifizierte elektronische Signaturen ein qualifiziertes [elektronisches Zertifikat](#) vor, das eine qualifizierte elektronische Signatur des Ausstellers enthält.

Dies bedeutet für qualifizierte Zertifikate mit freiwilliger Anbieterakkreditierung (§15 SigG): Zertifizierungsdiensteanbieter wie beispielsweise D-TRUST oder die DATEV etc. erhalten ein Zertifikat vom Betreiber der obersten deutschen Root. Dieser Betreiber ist die Bundesnetzagentur. Sie ist auch gleichzeitig Aufsichtsstelle für alle Anbieter von Zertifikaten, Soft- und Hardware im Markt. Der jeweilige Zertifizierungsdiensteanbieter gibt nun seinerseits ein Zertifikat an eine Person aus die damit unterschreiben will. Somit kann nun jeder jede Unterschrift nachprüfen, da alle Zertifikatsketten auf die Bundesnetzagentur zurückzuführen sind.

[www.wikipedia.de](http://www.wikipedia.de)

# Zertifikat

- D-Trust
  - Tochterfirma der Bundesdruckerei
  - Für die Registrierung ist persönliche Identifizierung nötig
  - Beantragung z.B. in den Registrierungsstellen der IHK
  - Signaturkarte, gültig für 18 Monate 126,44€
  - Folgekarte, gültig 18 Monate 97,44€

31/42

[www.d-trust.net](http://www.d-trust.net)

# IT Forensik

- Teilgebiet der Forensik
- Beschäftigt sich mit der Untersuchung von verdächtigen Vorfällen bei IT-Systemen
- Feststellung des Tatbestandes
- Überführung des Täters

32/42

[www.wikipedia.de](http://www.wikipedia.de)

# IT Forensik

- Gründe für Forensik:
  - Betrugsfälle, missbräuchliche Nutzung von Internet/Mail, Verbreitung von Pornographie, Ermittlung in Mordfällen, Terrorismus
- Wichtig: Beweismaterial darf nicht beschädigt, zerstört oder auf eine andere Weise in Mitleidenschaft gezogen werden
- Sonst führt dies zur Nichtzulassung als Beweismittel

33/42

Quelle: [www.vogon.de](http://www.vogon.de)

# IT Forensik

- Angebot
  - Hardware zum spiegeln der Daten



# IT Forensik

- Außerdem wird angeboten:
  - Software
  - Schulungen
  - Sachverständigengutachten

35/42

, SW, Schulung zur Forensik von Firmen:

Datenträger kopieren, Image erstellen

Erstellte Images auslesen und am Computer betrachten

SW zur Abbilderstellung, -verarbeitung und –untersuchung

Sachverständigengutachten

# IT Forensik

- Richtlinien zur Sicherung von Beweismitteln (In GB):
  - Daten müssen vor Ort korrekt sichergestellt werden
  - Ist dies nicht der Fall sind die Daten vor Gericht evtl. unbrauchbar
  - Deshalb Kopie des kompletten Systems
  - Daten dürfen nicht verändert werden ;-)
  - Alle Vorgänge müssen protokolliert werden

36/42

# IT Forensik

- Open Source?
  - Es gibt einige Tools:
    - dd als Imagingtool
    - Sleuth Kit: Analysetool
  - Vorteil von Open Source:
    - Freier Code
    - Dadurch können Fragen beantwortet werden wie:
      - „Funktioniert ihre SW auch?“
      - „Können Sie das auch belegen?“

37/42

# IT Forensik

- **Kameras hinterlassen Fingerabdrücke**

**Anhand der individuellen Signatur der Chips von Digitalkameras wollen britische Forscher Kinderpornografen überführen. Das für jeden Chip typische Bildrauschen soll Fotos eindeutig der Kamera zuordnen, mit der sie angefertigt wurden.**

[www.spiegel.de](http://www.spiegel.de)

38/42

# Vernichtung von HW

- Daten sind auch nach Gebrauch eines Datenträgers noch vorhanden
- Es gibt mehrere Möglichkeiten diese zu löschen:
  - Entsorgung an Spezialfirma outsourcen
  - Bei Festplatten kann man die Daten überschreiben, wenn sie noch funktioniert
  - Wenn sie nicht mehr funktioniert kann man sie entmagnetisieren

# Probleme

- Selbst starke Magnete sind heute zu schwach
- Nur ein sehr starkes Magnetfeld ist in der Lage die Daten zu löschen
- Ein Gerät, das ein solches Feld erzeugt wäre ein Kernspintomograph
- Zerstört aber evtl. mehr als nur die Daten

## Vernichtung durch Fremdfirmen

- Entsorgen die Datenträger, allerdings besteht die Möglichkeit, dass Mitarbeiter die Daten noch auslesen können
- Festplatten werden physikalisch vernichtet

# Zusammenfassung

- Das BSI ist für Sicherheitsrichtlinien verantwortlich
- Outsourcing der IT-Sicherheit ist in Deutschland ein Wachstumsmarkt
- Penetrationstests können zur Sicherheit beitragen
- Die IT-Forensik dient der digitalen Spurensuche