"Les cybermenaces à l'horizon 2020"

Table ronde :
Menaces et protection des données des organismes

Podiumsdiskussion : Gefahren und Schutz der Daten

Animation par René ECKHARDT

Diebstahl von strategischen Daten und Verletzung des geistigen Eigentums

frederic.sanuy@dalim.com

Frederic SANUY

Dr. in Physik
DALIM Software GmbH
Lösungen Enginieur Manager

DALIM® SOFTWARE

Wer wir sind

Sotfware Design und Engineering-Unternehmen

Hauptsitz in Kehl, Deutschland

Entwicklung hochproduktiver Workflow-Systeme

Für die medienverarbeitende Industrie

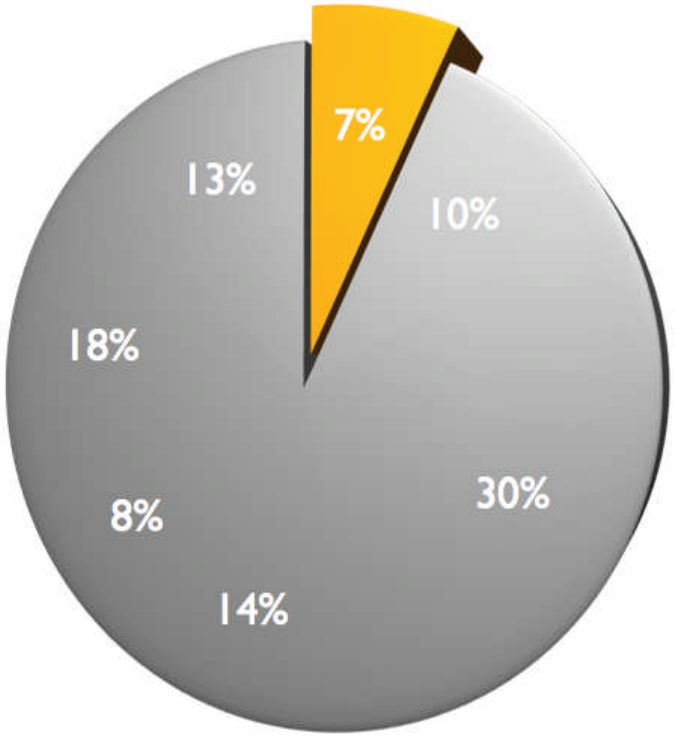
Innovative Lösungen für unsere Kunden seit 1985 für die medienverarbeitende Industrie

Von den renommiertesten, global agierenden Unternehmen

Bis zu deren entlegensten und vielfältigsten Zulieferern auf der ganzen Welt

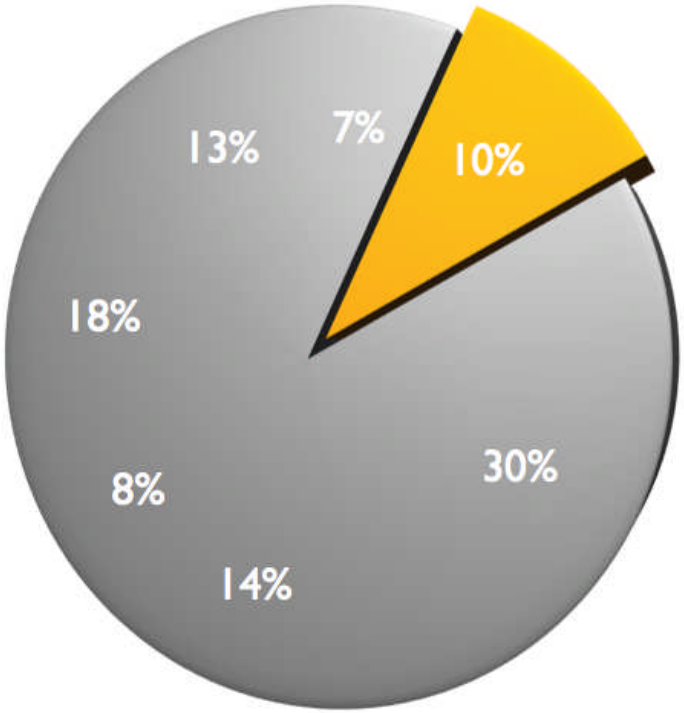
Für wen wir es tun

Creative Professionals

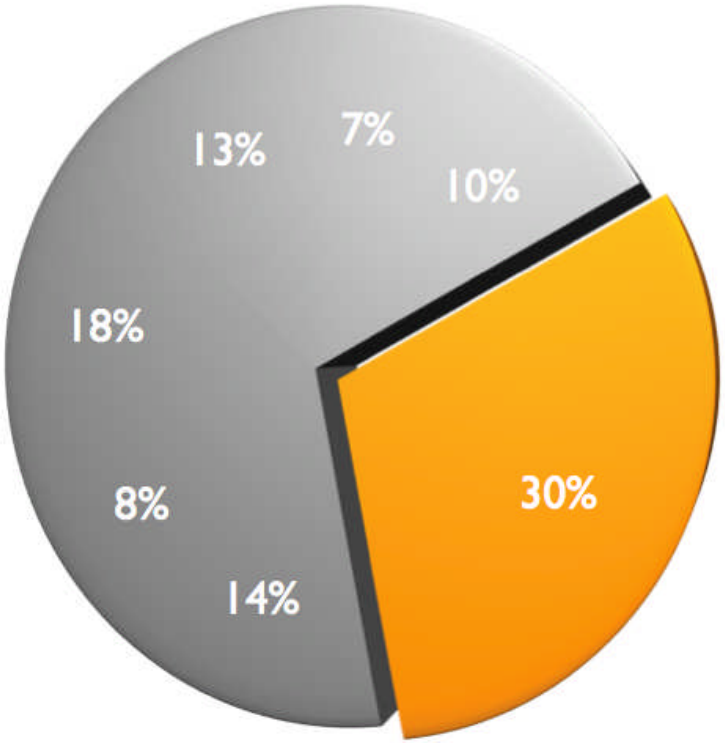


WPP · IPG · HAVAS · PUBLICIS GROUPE · OmnicomGroup · SAATCHI & SAATCHI · M&CSAATCHI · Y&R · ogilvy · DDB · 2009 ANOS DM9DDB · TBWA\ · Tag: · thelab · Deutsch · mundcom MAÎTRE D'ŒUVRE DE L'IMAGE · JWT · McCANN-ERICKSON

Verlage

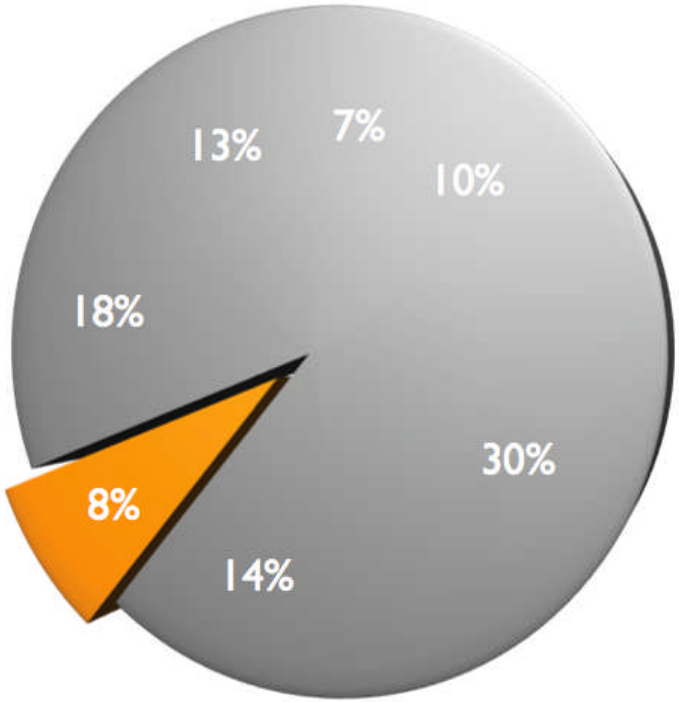


Marketing & Media Services



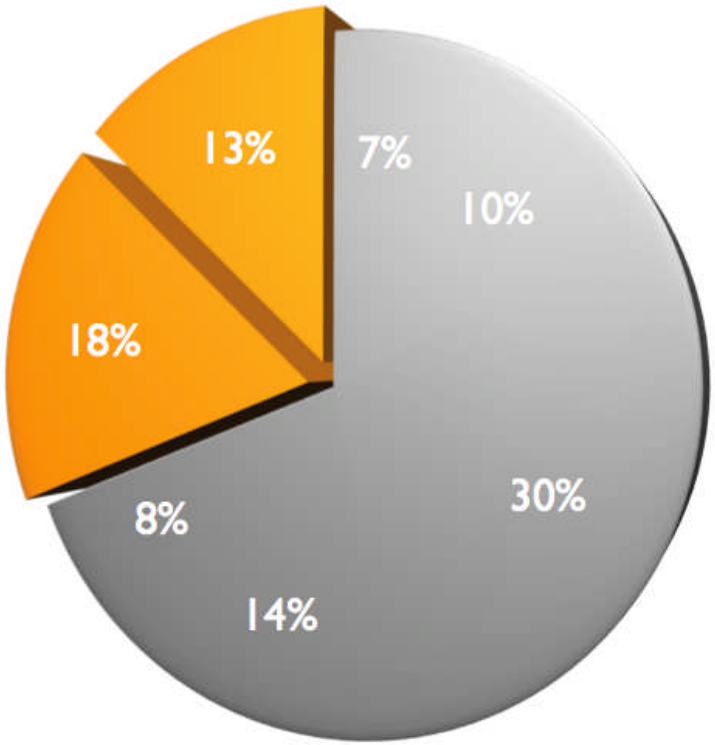
vertis communications
arizona
zinio
Burti
Laudert
vio
w&co MediaServices
QuadGraphics
Tag:
ALTAVIA
Meyle Müller
eupro
EXAPRINT
websend
xerox
BLACK DOT GROUP
sendmyad smart ad portal

Etiketten & Verpackung



janoschka
Pen&Inc.
tapas
BG-PACK
kroha
amcor
beck
Adare Packaging Solutions
spinnler emballage cylindrique
WANFRIED-DRUCK KALDEN
Sunbranding
GRS
Carey color incorporated
Pelgrims
RR DONNELLEY
WALL. A MeadWestvaco Resource
SCHAWK
BERRY PLASTICS CORPORATION
diadeis
PACKPOOL.
CPC PACKAGING

Akzidenz- & Verlags-Druckereien



Geistige Eigentum des Unternehmen

Die Daten unsere Kunden sind im Mittelpunk unsere Politik und die Sicherheit

- Patente
- Geschäftsmethoden
- Productionprozesse
- Produktdesign
- Software codes gehören

Unsere Bericht über Geistige Eingentum

- **Teilen – Tauschen**

- Alles geistiges Eigentum hat eine Sache gemein: Sein Wert steigt, wenn dieser geteilt wird und umso mehr geistiges Eigentum sicher ausgetauscht werden kann, desto mehr steigt auch der Wert.

- **Zusammenarbeit**

Der Wert des geistigen Eigentums hängt stark davon ab, wie einfach es in einem stark geprägten Umfeld der Zusammenarbeit umgesetzt werden kann.

Unsere Bericht über Geistige Eingentum

Effizienz des Unternehmens

- Unternehmen tun sich schwer, die richtige Balance beim Austausch von geistigem Eigentum zu finden und dadurch die Zusammenarbeit zu optimieren, die Effizienz des Unternehmens zu verbessern und die Risiken abzuwägen, die mit einem Austausch verbunden sein können.

Kompromisse eingehen

- Um ihr geistiges Eigentum zu schützen, müssen Unternehmen häufig schwierige und teure Kompromisse eingehen. Dabei geht es zum einen um den Austausch sensibler Informationen, um die Zusammenarbeit und Produktivität zu steigern und zum anderen um die Einführung von strengen Sicherheitsmaßnahmen, um das Risiko des Daten-Missbrauchs zu reduzieren.

Geistige Eigentum des Unternehmen

Was wir unsere Kunde um ihre Daten zu Schutzen empfehlen

- VPN Verbindung
- Firewall Verwendung
- Unsere Lösungen sind Websicherheit serienmäßig eingebaute eben für die API (“https”)
- Alle Eingänge und Zugriffe sind untergebracht
- Wir brauchen keine plugins um die Daten zu senden
- Alle server sind synchronisiert und die Daten aufbewahrend
- Die Schutzziele unsere Software sind basiert auf Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit, Verfügbarkeit und Schutz der Privatsphäre
- Kleine und mittlere Unternehmen können ihre IT-Sicherheit durch Cloud-Computing erhöhen.

Geistige Eigentum des Unternehmen

Sicherheit in der Wolke : Cloud Computing

- Seit einigen Jahren haben wir auch SAAS Lösungen für die Daten und Anwendungen

- Auf der einen Seite ermöglicht die Strategie des Auslagerns in die Wolke den Unternehmen, sich auf ihre Kernkompetenzen zu konzentrieren und neue Geschäftsmöglichkeiten zu erschließen.

- **Verwalten von Risiko-und Compliance :** Unternehmen, die einen Teil ihrer Aktivitäten-Schalter auf der Wolke sind verantwortlich für Compliance, Sicherheit und Risiken für ihre Operationen.

- **Identity Management und Access :** Der Dienst kann solche Identitäten an ihre Kunden liefern. Diese Anbieter sind dann in der Lage, den Zugang zu Dienstleistungen über Cloud-Infrastruktur verwalten und ermöglichen die Zusammenarbeit ohne Zwang Grenze.

Geistige Eigentum des Unternehmen

Sicherheit in der Wolke : Cloud Computing

- **Integrität von Dienstleistungen an :** Cloud-basierte Dienste müssen so konzipiert und umgesetzt mit der Priorität auf Sicherheit, während die Business-Prozesse in das System des Sicherheitsmanagements des Unternehmens integriert werden müssen.

- **Integrity Endpunkt :** Da die Cloud-basierte Dienste angefordert werden und verbraucht auf der Baustelle, Sicherheit, Compliance und Integrität der Endpunkt muss sorgfältig geprüft werden.

- **Schutz von Informationen :** Cloud-Services benötigen zuverlässige Informationen verarbeiten Schutz vor, während und nach der Transaktion.

Merci!

Vielen Dank!

Classification et mesures de protection des données

Email : guinier@acm.org

par Daniel GUINIER

Dr. ès Sciences, Certifications CISSP, ISSMP, ISSAP, MBCI
Expert judiciaire honoraire près la Cour d'Appel de Colmar
Expert devant la Cour Pénale Internationale de La Haye
Lieutenant-colonel (RC) de la gendarmerie nationale

Quand l'information vaut plus que l'or!

Les informations **stratégiques** relèvent de données :

- **sensibles** - par elles-mêmes
- **vitales** - par leur nécessité

- 1 800 milliards de GO de données seront créées et répliquées en 2011
- Tous les deux ans, les données mondiales vont plus que doubler

(EMC (2011) : Extracting value from chaos)

$1{,}8 \cdot 10^{21}$

Toutes les informations

- n'ont pas la même valeur intrinsèque ou de nécessité
- ne nécessitent donc pas le même niveau d'attention

Croissance **QUALITATIVE** dans :

- l'aide aux processus décisionnels
- la génération de nouveaux revenus, etc.

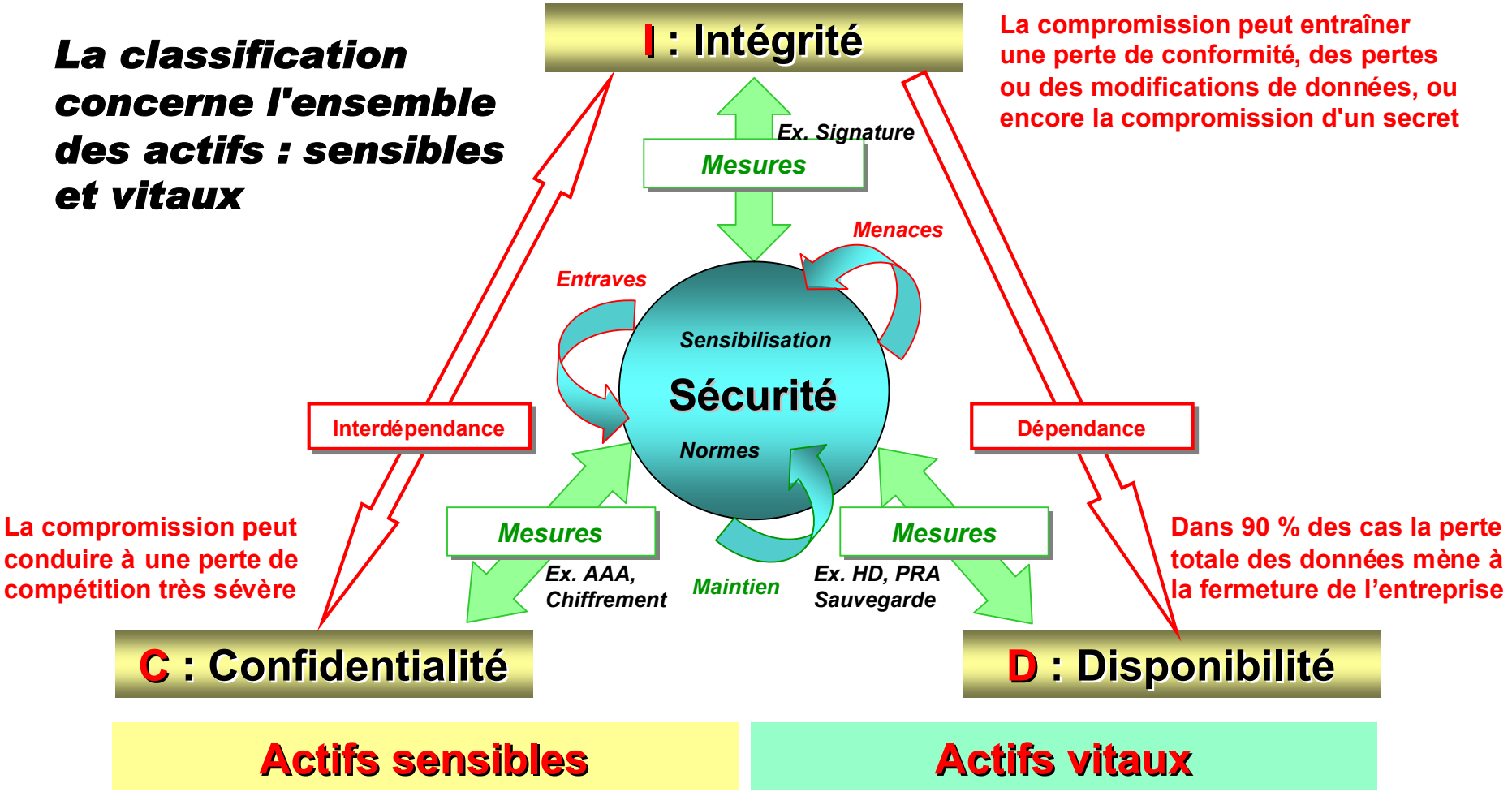
Croissance **QUANTITATIVE** dans :

- le stockage et la dispersion des données
- les transactions et flux de données, etc.

La perte ou la compromission d'informations stratégiques signifie la disparition ou la faillite dans la majorité des cas. Connaître leur valeur est une nécessité des organismes pour protéger l'essentiel.

Propriétés CID de la sécurité SI-info.

La classification concerne l'ensemble des actifs : sensibles et vitaux



En complément, l'impuTabilité (T) assure la traçabilité de fonctions ou d'opérations, comme moyen de preuve sans répudiation possible.

Qu'est-ce que la classification ?

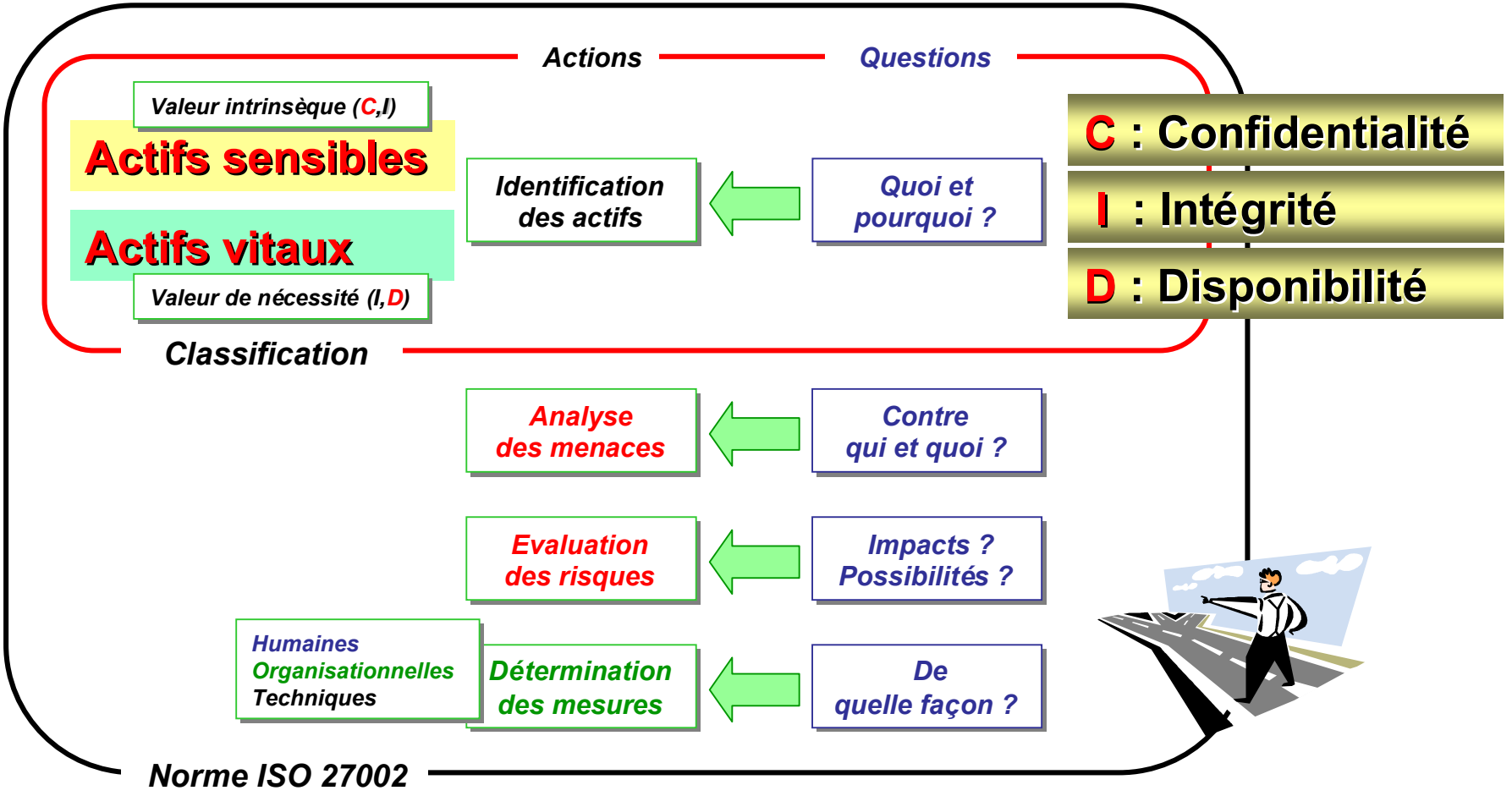
- Définition
  - La classification est **un processus de gestion** visant à assigner un **niveau de restriction formel** d'accès aux éléments à protéger
- Motifs
  - importance de **distinguer par valeur** les éléments du patrimoine informationnel **pour maintenir un niveau de sécurité approprié**
- Contexte
  - **tout organisme** : entreprise ou autre, de toute taille ou secteur d'activité, dans le cadre d'une **politique de sécurité**
- Prescriptions
  - **instruction** IGI n°1300 pour la protection du **secret de défense**
  - **norme** ISO 27002 - chapitre : **gestion des actifs** des organismes

SGDN (1990) : Guide pratique sur la protection du secret de défense, à l'usage des secrétariats et bureaux de courrier, 49 p.
SCSSI (1998) : Guide pratique pour la protection des supports informatiques classifiés de défense, 31 p.
Guinier D. (2006) : Les informations classifiées de défense - Conséquences sur la saisie et l'expertise. Revue *Experts,* n° 73, pp. 53-57

Les documents relatifs au secret de défense seront autant d'aides appréciables, avec d'autres, pour guider les entreprises.

Place de la classification

- Une première étape de la gestion de la sécurité



Au-delà, s'agissant de la préservation d'un capital intellectuel lié aux compétences et au savoir-faire, l'enjeu est également humain.

Types d'actifs informationnels

- Actifs d'information
  - bases et fichiers de données, archives, documentations, y compris plans, procédures et dispositions de substitution
- Actifs logiciels
  - systèmes de base et de développement
  - applications et utilitaires
- Actifs physiques
  - matériels informatiques et de communication
  - autres équipements fixes et mobiles, supports d'information
- Actifs de services
  - infrastructures informatiques et de communication
  - installations et commodités générales, espaces de travail

Une attention particulière est attendue concernant d'une part, les actifs "... as a Service" en nuages et en infogérance, et d'autre part, les personnes, au vu d'éléments classifiés.

Indices associés aux actifs

- Exemple de grille pratique d'indices **$C_x I_x D_x$**

Indice x	Cx : Confidentialité	Ix : Intégrité	Dx : Disponibilité
0	Sans conséquence	Sans conséquence	Sans conséquence
1	Conséquences défavorables Diffusion interne	Conséquences défavorables	Conséquences à long terme à plus d'une semaine
2	Conséquences dommageables Diffusion restreinte	Conséquences dommageables	Conséquences dommageables à moyen terme à plus d'un jour
3	Conséquences graves Classifié : "**confidentiel**"	Conséquences graves	Conséquences à court terme à moins d'une journée, ou graves
4	Conséquences extrêmes Classifié : "**très confidentiel**"	Conséquences extrêmement graves	Conséquences en temps réel, ou létales sans substitut

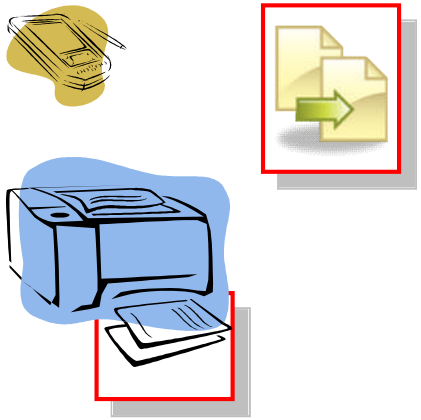
Indices de sensibilité | **Indices de vitalité**

Des indices seront affectés pour chaque type d'actifs, sous forme de triplet, selon une échelle de besoins de sécurité CID au vu de menaces et impacts divers : financiers, concurrentiels, image, etc.

Cycle de vie des actifs classifiés

1. Identification

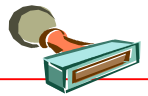
Inventaire



2. Caractérisation

Classifié ***"confidentiel"*** lié au secret : scientifique, industriel, technologique, commercial, ou à la vie privée, etc.

Peut être non classifié et ***"diffusion restreinte"*** : obligation de réserve ou de discrétion



3. Marquage

"confidentiel" et triplet d'indices **C**x**I**x**D**x pour préciser les niveaux de sensibilité et vitalité

Mentions spécifiques : domaine, propriétaire, habilitations, séparation des privilèges, *"besoin d'en connaître"*, AAA : Authentification, Autorisations, Auditabilité

Date : classification ; date et/ou événement pour déclassification et/ou destruction

4a. Utilisation

En l'état : classifié ou déclassifié, selon les règles et procédures.

4b. Déclassification

Procédure de déclassification des actifs classifiés sensibles et vitaux

Par le propriétaire ou sur délégation formelles ou arbitrées par RSSI

5. Destruction

Procédure de destruction effective des supports et/ou de l'information

Autorisation particulière et par RSSI concernant les actifs vitaux

Les mentions spécifiques visent le cloisonnement de l'information pour l'accès exclusif à ceux ayant besoin de la connaître, les conditions d'accès et les procédures aux différentes étapes.

Concernant les TPE, PME / PMI

- La valeur des actifs informationnels
  - reste souvent à déterminer et non prioritaire
- L'information est hétérogène
  - enregistrée, sous formes numérique et imprimée
  - répartie et dupliquée, sous différents formats
  - diffusée et archivée, avec peu de contrôle
- Des freins sont identifiés
  - multiplicité des problèmes quotidiens à gérer
  - compétences et moyens internes limités
  - culture de recherche d'une solution immédiate
    - facilité apparente d'une solution technique
    - beaucoup de promesses dans les offres

Déterminer cette valeur, c'est s'attacher au caractère fonctionnel et à l'impact sur le fonctionnement de l'entreprise. Toute solution requiert une volonté forte, une conduite de projet et diverses aides.

Nouvelle infraction pénale en vue

- **But** : Protéger les actifs ***"confidentiels"***
- **Cadre** : Atteintes au secret des affaires des entreprises
- **Marquage** : Documents et autres objets mettant en jeu :
  - les intérêts de l'entreprise ou ses positions stratégiques
  - son potentiel technologique ou concurrentiel
  - ses intérêts commerciaux ou financiers, et autres
- **Infractions actuelles** : *difficultés hors domaine de la défense*
  - violation du secret de défense *(Art. 413 du Code pénal)*
  - violation du secret professionnel *(Art. 226-13 du Code pénal)*
  - abus de confiance *(Art. 314-1 du Code pénal)*
  - concurrence déloyale *(Arts. 1382 et 1383 du Code civil)*
- **Infraction nouvelle** : *projet de loi en direction des entreprises*
  - révélation volontaire d'informations ***"confidentiel entreprise"***
  - existence d'un tel marquage sur leurs supports

Le ministre de l'Industrie, de l'Energie et de l'Economie Numérique, a récemment annoncé le 20/09/11 l'initiative d'un projet de loi concernant la protection et la défense des entreprises.

Conclusion

- **La classification** : Une étape indispensable

  Sans cette étape, il est difficile de mettre en œuvre une politique de sécurité globale adaptée aux besoins, sans connaître les actifs sensibles et vitaux et leur valeur.

- Existence de guides et de normes
- Adaptations attendues :
  - prise en compte des actifs vitaux, en plus des actifs sensibles
  - des méthodes à chaque type d'organisme : TPE, PME / PMI, etc.
  - du droit au *"confidentiel entreprise"* distinct du secret de défense
- Difficultés et enjeux à attendre
  - avec les services externalisés et *"en nuages"*
  - avec l'homme, comme talon d'Achille, *faible en dépit de sa force*

Dans l'entreprise, chacun a la responsabilité de s'assurer, à son niveau, que l'information dispose d'un niveau approprié de sécurité au vu de la classification préalablement approuvée par la direction.

Merci!

Vielen Dank!

Cyberkrimminalität und Angriffe auf (geheime) Organisationen

Email : roger.klose@she.net

Roger KLOSE

Senior Security Consultant

SHE AG, Ludwigshafen, Germany

Disclaimer

- *Nachfolgende Informationen sind öffentlich verfügbar.*
- *Einige der gezeigten Methoden sind nur nur zur Demonstration und können ggf. als Straftat geahndet werden. Der Autor übernimmt hierfür keine Haftung.*

Definition und Scope

- *Computerkriminalität:*
  - *ist im engeren Sinne die Bezeichnung für Straftaten bei denen der Computer als Tatmittel oder als Gegenstand der deliktischen Handlungen eine wesentliche Rolle spielt.*
- *Geheime Organisationen:*
  - *Der Begriff Geheimbund oder Geheimgesellschaft bezeichnet eine Organisation oder auch Vereinigung mit einem konspirativen Hintergrund. Geheime Gesellschaften bilden ein Sammelbecken verschiedener gemeinsamer Interessen, die von aufklärerischen, politischen, ökonomischen, spirituellen, religiösen, mystizierenden, okkultistischen oder esoterischen Zielen motiviert sein können.*
- *Problemstellung:*
  - *Da geheime Organisationen nur solage geheim sind, bis sie enttarnt werden, können diese auch nur dann betrachtet werden (z.B. Gladio)! Daher werden in diesem Vortrag zudem Vorfälle im Bezug mit vermeintlich „geheime“ Daten aufgezeigt.*

Facts ‘n’ Fiction

- Film und Fernsehen zeigen immer wieder sensationelle Hackermethoden…
- … welche nicht immer der Realität entsprechen
- Die breite Öffentlichkeit nimmt dies aber oft als gegeben an.

Siehe auch: Johnny Long – Hacking Hollywood
(http://www.youtube.com/watch?v=aGTsOLhLaAU)

- Angreifer lassen sich inspirieren…
  - *Hacktivisten*
  - *Stromausfälle*
  - *NSA*
  - *CIA*
  - *Waffensysteme*
  - *Pentagon*

Beziehungen der Bedrohungen

Gut

Unternehmen

Regierungen

(geheim)
Organisationen

Hacker

politisch motivierte Gruppierungen
(Hacktivists)

organisiertes Verbrechen

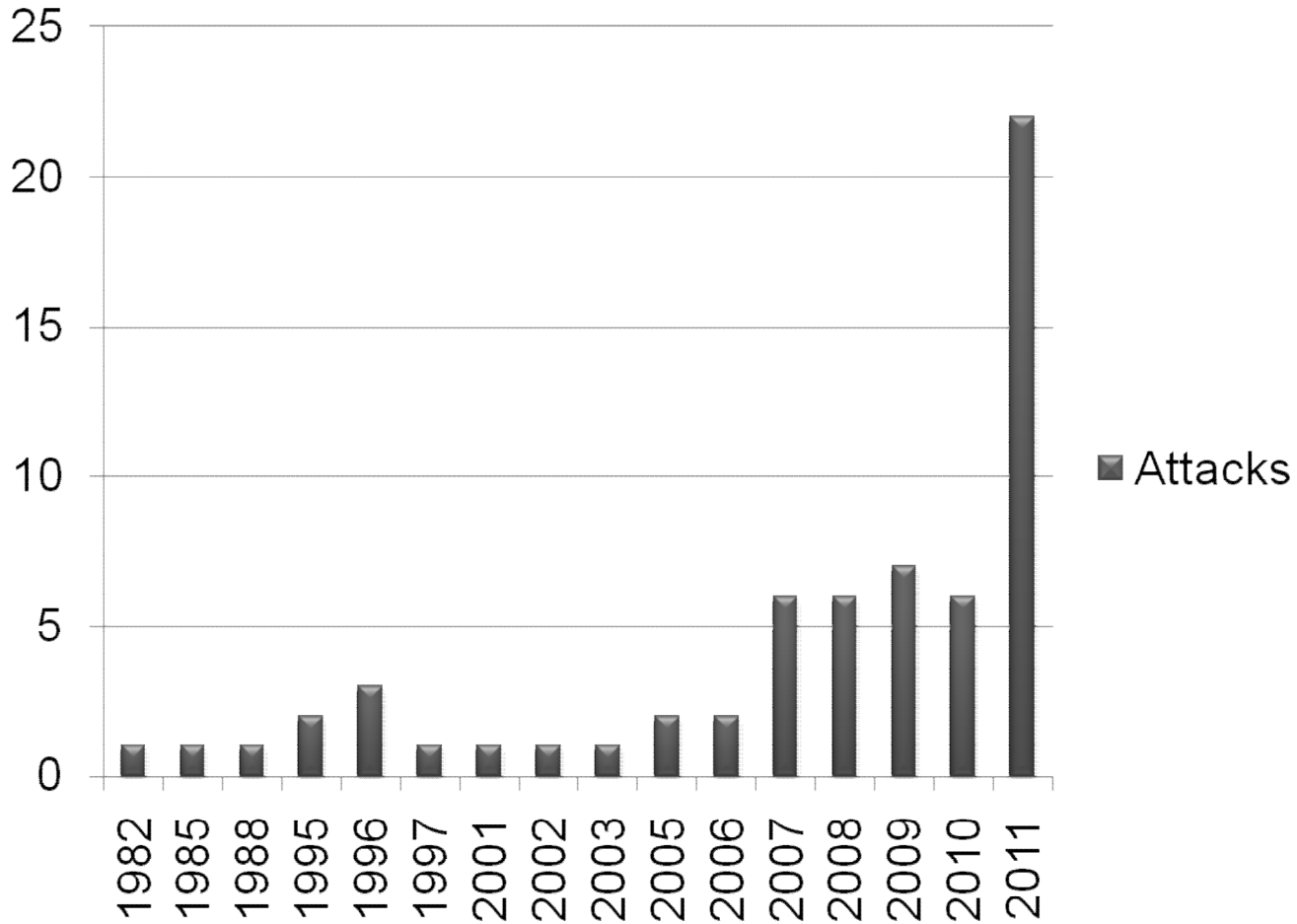
Böse

Bekannte Vorfälle (Auszug)

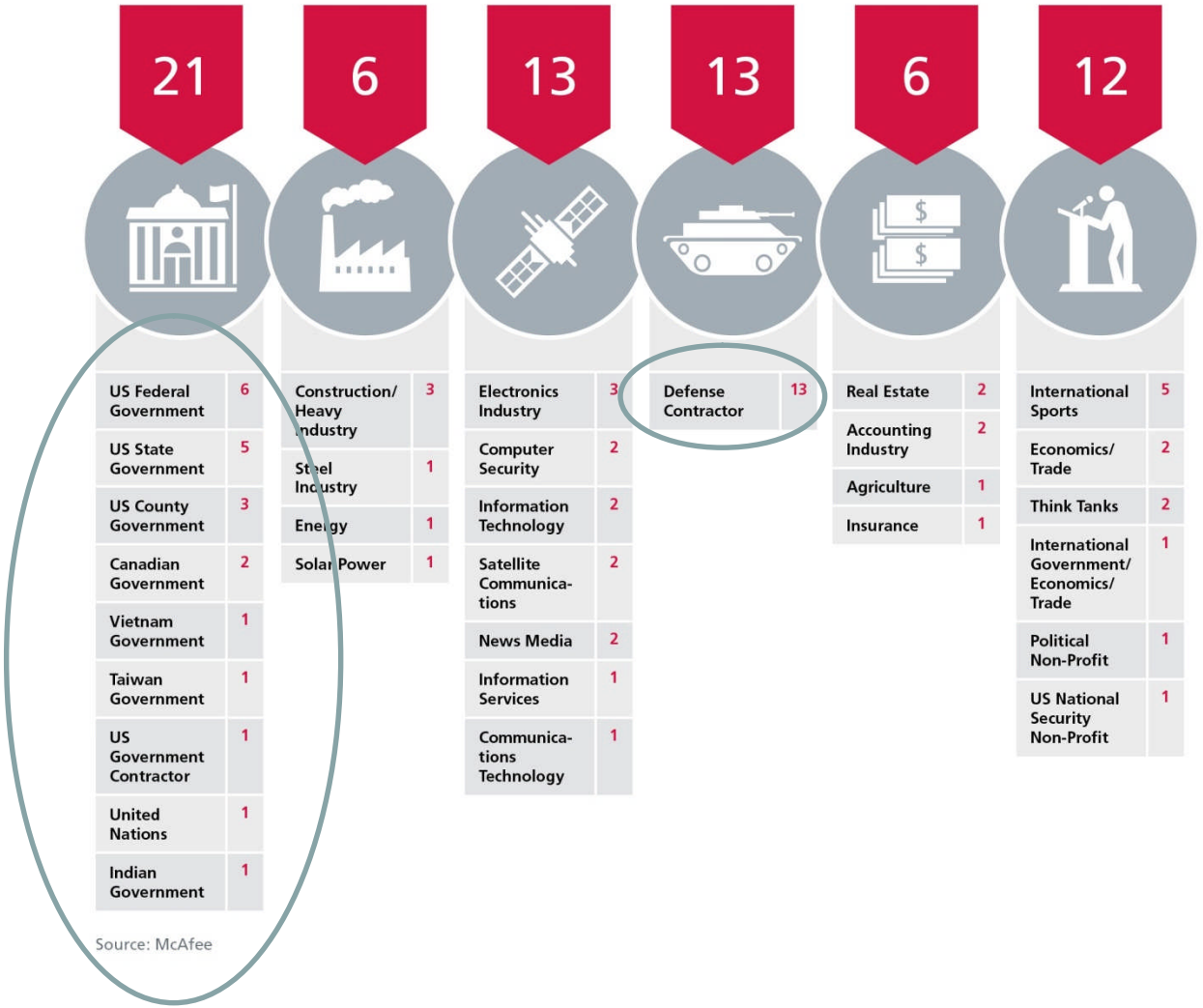
- 1982 – Los Almos Labs
- 1985 – KGB-Hack
- 1988 – The Morris Worm
- 1995 – U.S General Accounting Office, BND
- 1996 – U.S. Department of Justice, CIA, U.S. Air Force
- 1997 – U.S. Air Force
- 2001 – U.S. Air Force
- 2002 – NASA
- 2003 – Mossad, NSA
- 2005 – Great Britain, Secret Service
- 2006 – Weapons Division ;U.S. Naval Air Warfare Center
- 2007 – Estonia Case, DoD, United Nations, Pentagon, Great Britain, Germany, Oak Ridge National Laboratory, Los Almos Labs, U.S. Satellites
- 2008 – Department of Homeland Security, Multi-City Power Outage, White House, Georgia, Russia,
- 2009 – Conficker , Ames Research Center NASA, Australian Department of communication, Ghostnet, U.S. Air Force F-35, Israel, Palestina, Bundeswehr
- 2010 – UN department of safety and security, Stuxnet, Wikileaks, AT&T, Austria, India,
- 2011.01 – Canada
- 2011.02 – HBGary
- 2011.03 – U.S. weapon system ,(24.000 Files), White House Gmail Hack, RSA, G20 (France)
- 2011.04 – Deutscher Bundestag – 5 Angriffe täglich (17/5677)
- 2011.05 – Lockheed Martin,
- 2011.06 – C.I.A, FBI, U.S. Senate, Malaysian Gouvernment, Northrop Grumman
- 2011.07 – German Federal Police, Booz Allen Hamilton, DigiNotar (CIA, MI6, Mossadd), NATO
- 2011.08 – Syrian Defence Ministery
- 2011.09 – Japan lower house, Mexico Security and Defence. Mitsubishi, U.S. Navy
- 2011.10 – U.S Air Force

Trend

- Trend der (öffentlich bekannten) Angriffe gegen Systeme mit (geheimen) Daten.

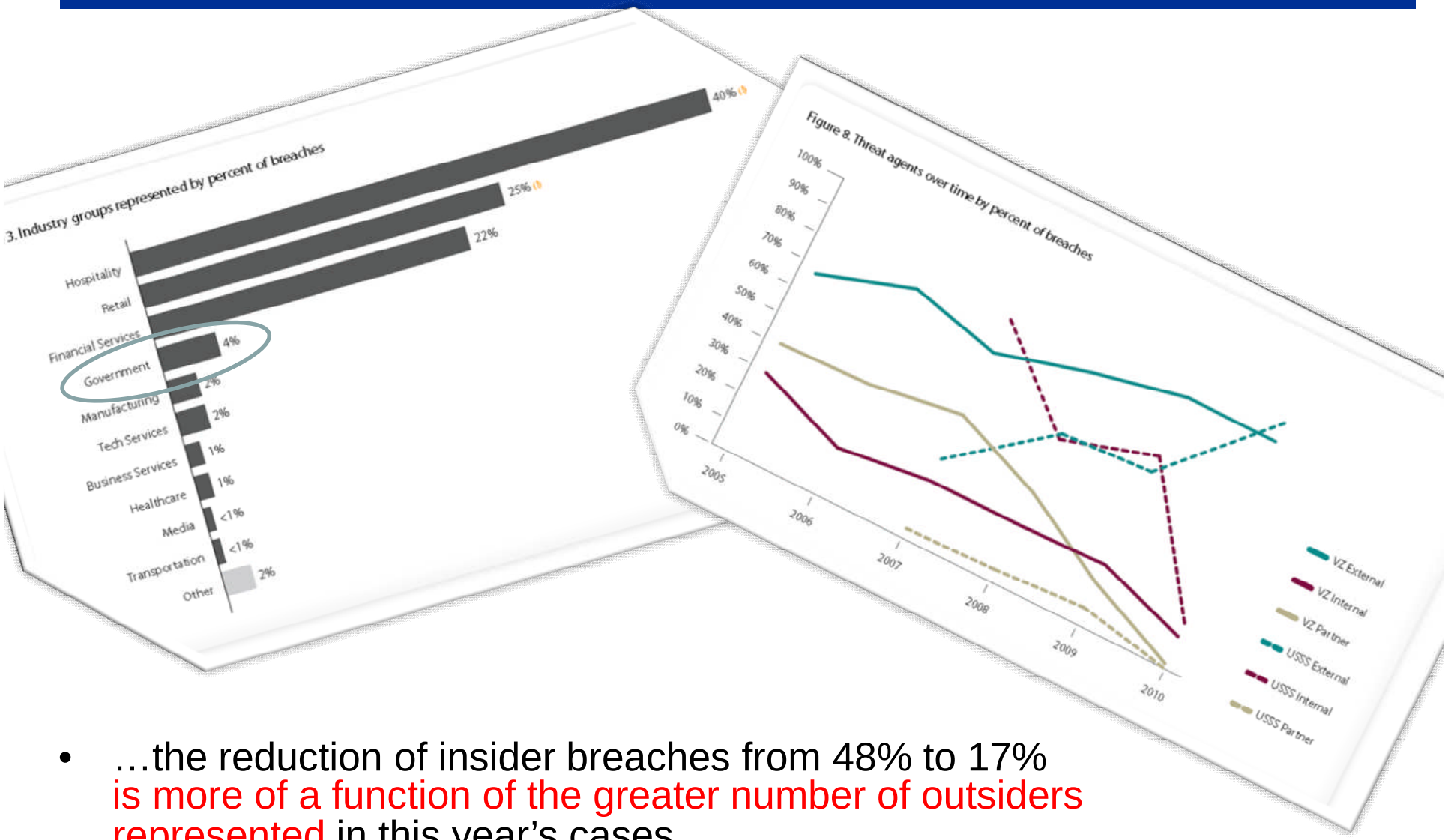


Ein Beispiel "Shady RAT"



Quelle: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

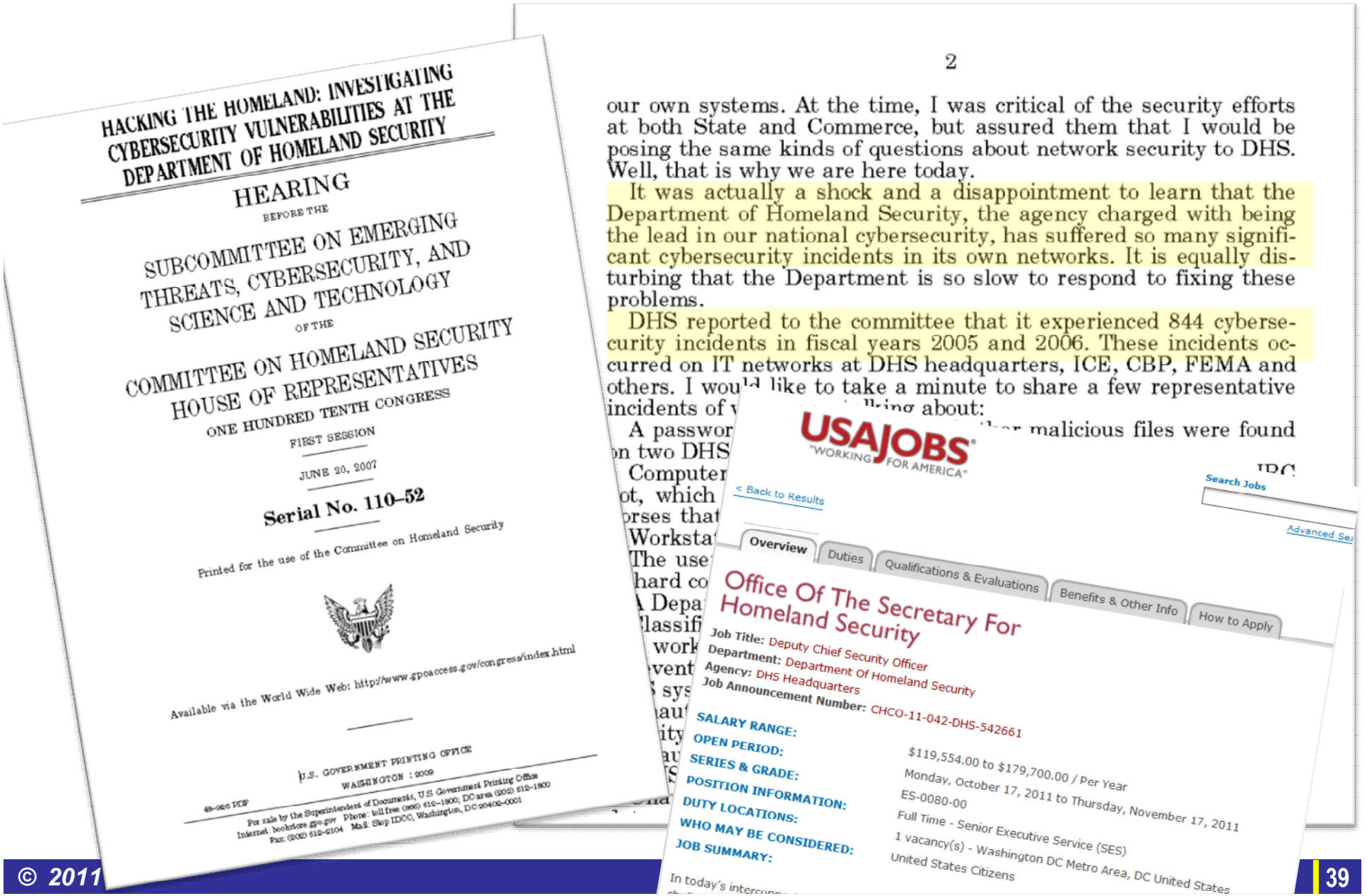
Ein Beispiel "Secret Service"



- …the reduction of insider breaches from 48% to 17% is more of a function of the greater number of outsiders represented in this year's cases.

Quelle: http://www.secretservice.gov/Verizon_Data_Breach_2011.pdf

Hacking the Homeland



HACKING THE HOMELAND: INVESTIGATING CYBERSECURITY VULNERABILITIES AT THE DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES
ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 20, 2007

Serial No. 110–52

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

2

our own systems. At the time, I was critical of the security efforts at both State and Commerce, but assured them that I would be posing the same kinds of questions about network security to DHS. Well, that is why we are here today.

It was actually a shock and a disappointment to learn that the Department of Homeland Security, the agency charged with being the lead in our national cybersecurity, has suffered so many significant cybersecurity incidents in its own networks. It is equally disturbing that the Department is so slow to respond to fixing these problems.

DHS reported to the committee that it experienced 844 cybersecurity incidents in fiscal years 2005 and 2006. These incidents occurred on IT networks at DHS headquarters, ICE, CBP, FEMA and others. I would like to take a minute to share a few representative incidents of

A passwor malicious files were found on two DHS

Computer

USAJOBS "WORKING FOR AMERICA"

< Back to Results

Search Jobs

Advanced Se

Overview | Duties | Qualifications & Evaluations | Benefits & Other Info | How to Apply

Office Of The Secretary For Homeland Security

Job Title: Deputy Chief Security Officer
Department: Department Of Homeland Security
Agency: DHS Headquarters
Job Announcement Number: CHCO-11-042-DHS-542661

SALARY RANGE: $119,554.00 to $179,700.00 / Per Year
OPEN PERIOD: Monday, October 17, 2011 to Thursday, November 17, 2011
SERIES & GRADE: ES-0080-00
POSITION INFORMATION: Full Time - Senior Executive Service (SES)
DUTY LOCATIONS: 1 vacancy(s) - Washington DC Metro Area, DC United States
WHO MAY BE CONSIDERED: United States Citizens
JOB SUMMARY:

In today's interconn

Wähle deine Waffen!

- Angriffe erfolgen auf div. Arten:
  - APT (Advanced Persistend Threat)
  - (D)DoS
  - Social Engineering (Robin Sage http://www.youtube.com/watch?v=4pnKbibi6QY)
  - 0-Day
  - Common Exploits
  - Web-Attacks
  - Google-Hacking
  - Filesharing
  - Phishing (E-Mails)

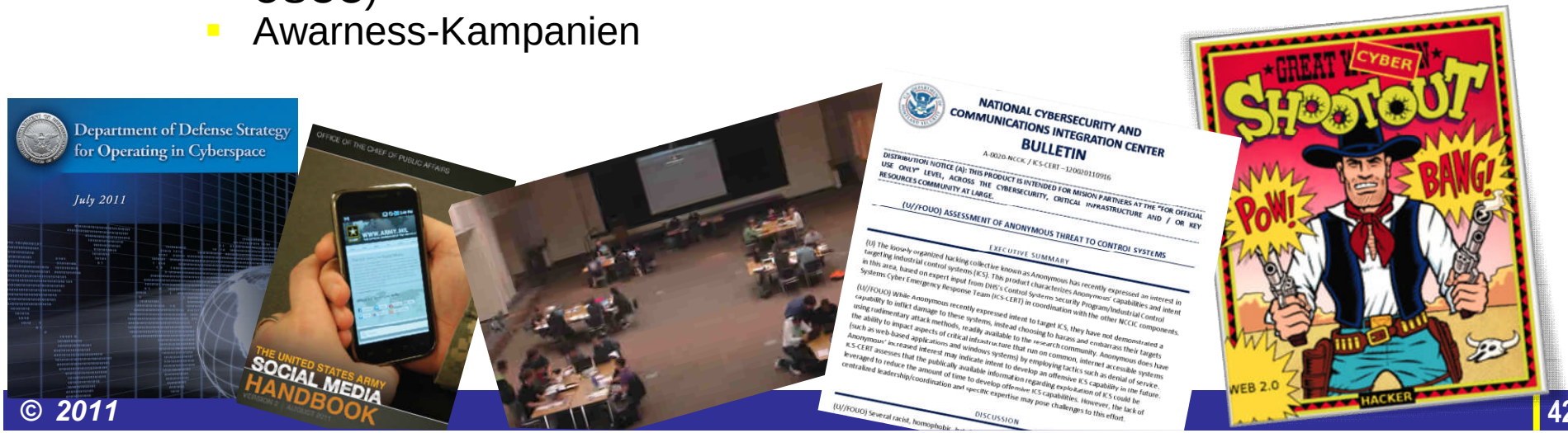
Einige Beispiele

Maßnahmen

- European Network and Information Security Agency (EU)
- Bundesamt für Sicherheit in der Informationstechnik (BRD)
- *Agence nationale de la sécurité des systèmes d'information* (Frankreich)

- *Cooperative Cyber Defence Centre of Excellence (NATO)*
- *Informations- und Computernetzwerkoperationen* des Kommandos Strategische Aufklärung (Deutsche Bundeswehr)
- Nationale Cyber-Abwehrzentrum (BRD)
- United States Cyber Command (U.S. Militär & NSA)

- Anwerben von Rekruten auf Konferenzen und druch Wettbewerbe. (z.B. USCC)
- Awarness-Kampanien



Merci!

Vielen Dank!

Questions

"Les cybermenaces à l'horizon 2020"