"Les cybermenaces à l'horizon 2020"

Table ronde :
Menaces et protection des données personnelles

Podiumsdiskussion : Gefahren und Schutz der Privaten Daten

Animation par René ECKHARDT

Gesamt Diebstahl der Privat Daten

Mail: mkuhr@iusec.de

Martin KUHR

LL.M., Attorney for IT-Law
Data Protection Officer
Manager IUSEC Datenschutz

Ausgangslage

- Im Jahr 2010 in Deutschland **250.000** Fälle von Internetkriminalität, 20% mehr als in 2009.
- **Vollständige Identität** interessant für Kriminelle
- **Vorgaben der EU** gewinnen auch für Datenschutz an Bedeutung
- Datenschutz (leider) **kein eigener Aufgabenbereich der EU**
- Kein verbindlicher Grundrechtskatalog in EU
- **EuGH** hat bzgl. Art 8 EMRK erklärt, dass das Recht auf Achtung des Privatlebens „ein von der Gemeinschaftsordnung geschütztes Grundrecht“ darstellt.
- Aber: EuGH im Jahr 2006: Übermittlung personenbezogener Daten ist **keine "unmittelbar beschwerdende Maßnahme"**
- 2000: **Charta der Grundrechte** der EU : Art. 8 Datenschutz

Ausgangslage

- Da Charta nicht bestätigt wurde in nationalen Gesetzen hat sie nur "soft law"- Bedeutung, EuGH oder nationale Gerichte können sie als Erkenntnisquelle nutzen, aber nicht direkt anwenden.
- **Datenschutz ist als Grundrechtsschutz** auf EU-Ebene und vor dem EuGH anerkannt
- **Europäische Datenschutzrichtlinie 95/46/EG** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr personenbezogener Daten innerhalb der EU
- **Richtlinie 2002/58/EG** zum Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation
- **Europäischer Datenschutzbeauftragter :** nur Empfehlungen

Ausgangslage

- **Personenbezogene Daten** :
  - **§ 3 Abs.1 BDSG** Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, so auch
  - **Art. 2 Richtlinie 95/46/EG**, wonach eine Person bestimmbar ist, wenn diese direkt oder indirekt identifiziert werden kann, z.B. durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, psychologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.
- Personenbezogene Daten z.B. : Name, Geburtsdatum, E-Mail-Adresse, Kontoverbindung

Informationspflichten ...

- **§ 42a BDSG** seit 1.4.2010 in Kraft
- Vorbild: USA sog. Breach Notification
- **Benachrichtigung des Betroffenen und Aufsichtsbehörden**
- Greift Vorschlag der EU-Kommission auf zur Änderung der Richtlinie 2002/58/EG
- Dient der **Prävention** (sonst negative Wirkung in Öffentlichkeit)
- Gilt **nur für nichtöffentliche Stellen**, nicht für Verwaltung
- Informationspflicht **begrenzt auf besonders sensible Daten**
  - Rassische/ethnische Herkunft; politische Meinung; Religiöse Überzeugung; Gewerkschaftszugehörigkeit; Gesundheit; Videoaufnahmen
  - Personenbezogene Daten bzgl. Berufsgeheimnis

Informationspflichten bei unrechtmäßiger Kenntniserlangung

Informationspflichten …

- Personenbezogene Daten bzgl. Strafbare Handlung
- Personenbezogene Daten bzgl. **Bank- u. Kreditkartenkonten**

- **Unrechtmäßige Kenntniserlangung**: z. B. unberechtigte Weitergabe oder sonst gegen Willen des Benachrichtigungspflichtigen.
- **Nachricht an Betroffenen**: unverzüglich, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden und Strafverfolgung nicht gefährdet ist.
- **Nachricht muss für Betroffenen erklären**: Art der Verletzung und Empfehlung für Maßnahmen zur Minderung möglicher nachteiliger Folgen
- Benachrichtigung kann schriftlich oder elektronisch erfolgen

Informationspflichten bei unrechtmäßiger Kenntniserlangung

Informationspflichten ...

- Benachrichtigung an Aufsichtsbehörde muss mögliche nachteilige Folgen der Verletzung sowie die vom Betreiber nach der Verletzung ergriffenen Maßnahmen enthalten.
- Bei unverhältnismäßig hohem Aufwand an Kosten und Zeit: Benachrichtigung der Öffentlichkeit ausreichend:
  - mindestens ½ Seite in mind. 2 bundesweit erscheinenden Tageszeitungen oder ähnlich geeignete Maßnahmen (Website?)
- Aufsichtsbehörde kann Maßnahmen anordnen.
- Verletzung der Informationspflicht: bis zu 300.000 Euro Bußgeld.
- Bundesregierung hat bis zum 31.12.2012 dem Parlament über die Auswirkungen der Regelung zu informieren.
- Wünschenswert wäre ein umfassender EU-Rechtsrahmen zum Schutz vor Cyberkriminalität unter besonderer Berücksichtigung des Datenschutzes.

Informationspflichten bei unrechtmäßiger Kenntniserlangung

Merci!

Vielen Dank!

Vol et usurpation d'identité numérique

Email : expert.gilles.grimault@gmail.com

par Gilles GRIMAULT

Ingénieur ESEO – électronique et informatique
Expert judiciaire près la Cour d'Appel de Colmar
Membre de l'AFSIN et de la CNEJITA

Définitions, enjeux

- L'identité administrative **n'est pas** l'identité numérique.
  certains pseudos sont plus célèbres que l'original (ex: Me Eolas) !
- L'identité numérique est l'ensemble des informations qu'on donne quand on créé un compte :
  - Dans les messageries (adresses email, informations plus ou moins personnelles, mots de passe, phrases secrètes, etc);
  - Dans les réseaux sociaux (pseudo, coordonnées, avatars, "amis", préférences, détails plus ou moins intimes…);
  - Dans les blogs (comme auteur, ou comme simple commentateur);
  - Dans la multitude de sites marchand, les sites de banques, etc.
- Les informations confiées à des sites sont souvent *a priori* anodines, mais il est tellement facile de se confier à un ordinateur froid et anonyme ! Quand le *viol* de données survient, il est trop tard :
  - Données de carte bancaire détournées…
  - Photos privées envoyées aux quatre coins du cyberespace…
  - Messagerie rendue inutilisable…
  - Spam vers tous les Contacts…
  - Site web, compte Facebook défiguré (cf blog de Sarkozy en janvier 2011)…
  - Commentaires inappropriés dans les blogs…
  - Cyber-réputation, notoriété en ligne…
  - Chantage, ingénierie sociale, etc.

Evolution des textes de lois en France

- Au civil, on peut utiliser les articles 9 (respect de la vie privée) et 1382 / 1383 (dommage à autrui / négligence), si ces trois conditions sont réunies :
  - Faute (par exemple se faire passer pour quelqu'un d'autre).
  - Préjudice (financier ou d'image).
  - La faute est la cause du préjudice.
- Au pénal, on peut utiliser ces différents textes :
  - 433-19 du CP : usurper une identité pour obtenir un acte authentique.
  - 434-23 du CP : usurper une identité qui conduit à des poursuites pénales.
  - 313-1 du CP : escroquerie par l'usage d'une fausse qualité.
  - 323 du CP : altération volontaire d'un système informatisé.
- Depuis le 14 mars 2011 (LOPPSI 2), on peut utiliser l'extension -1 de l'article 226-4 du CP (celui-ci concernait l'introduction dans le domicile d'autrui à l'aide de manœuvres, de menaces, de contraintes…) :

  Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

  Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

(LOPPSI = Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure)

Techniques de vol d'identité (1/3)

- Vol physique :
  - Ordinateur, téléphone, clé USB, carte d'accès à puce…
  - Documents divers au bureau, dans une boite aux lettres, dans des poubelles…
  - Emprunt d'un ordinateur non protégé par mot de passe…
  - Vol de doigt (empreinte biométrique) !

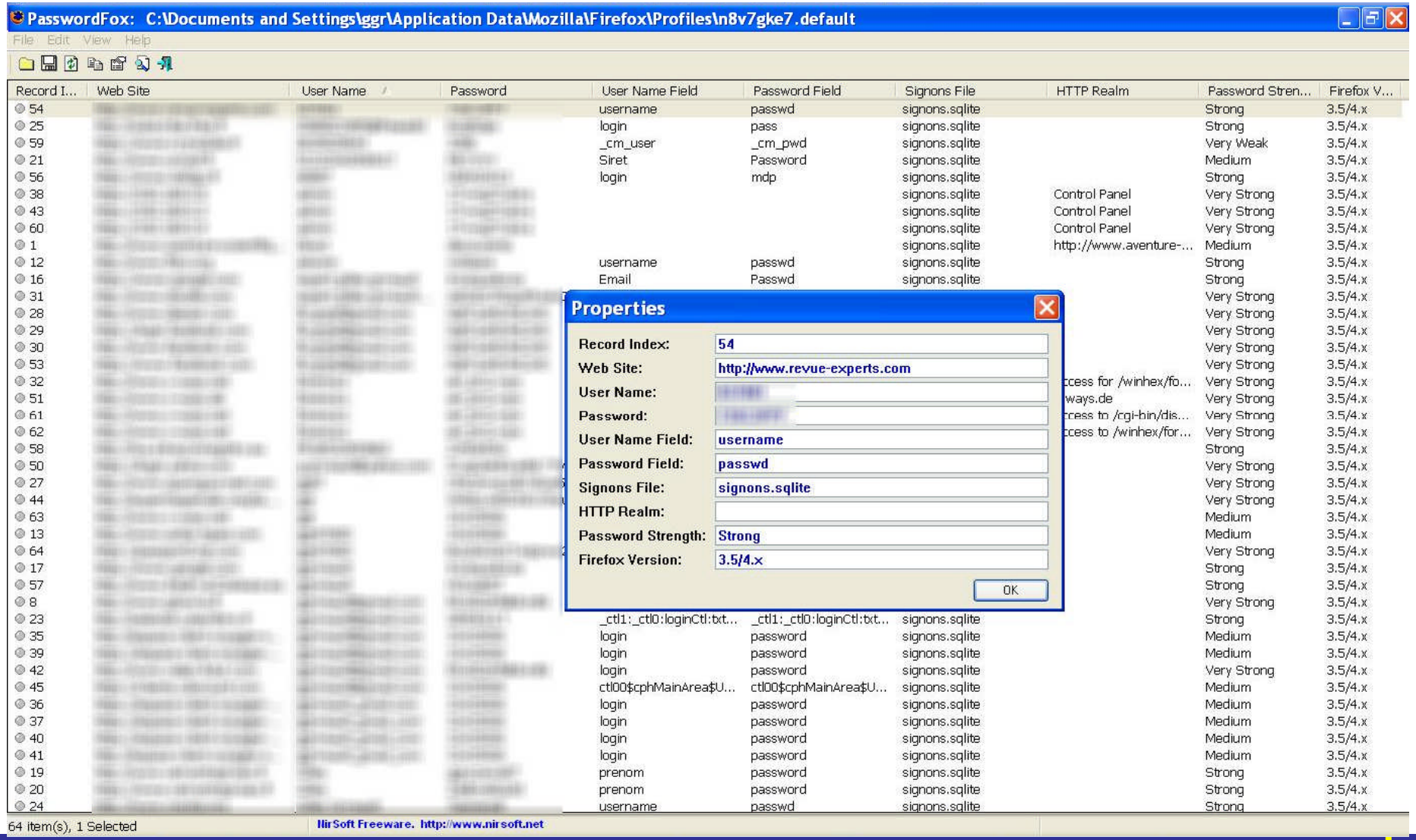
- Vol virtuel :
  - Sécurité simpliste :
    - Partage de répertoires sans contrôle;
    - Logiciels d'administration à distance;
    - Logins admin du poste confiés à tous;
    - Firewall et anti-virus, vulnérabilité des logiciels;
    - Méconnaissance de régles de base (veille techno, chartes)…
  - Utilisation de réseaux mal sécurisés (web-café, Wifi / WEP, etc.).

Techniques de vol d'identité (2/3)

- Vol virtuel :
  - Ingéniérie sociale :
    - Déterminer les bonnes cibles;
    - Infiltrer;
    - Interroger (par téléphone ou par email);
    - Utiliser l'accès obtenu (carnet d'adresse, etc).
  - Retrouver un mot de passe :
    - Post-it;
    - Mot de passe "azerty";
    - Caméra;
    - Keylogger;
    - Accès au poste non protégé (voir page suivante)…
  - Reprise de session d'un navigateur Internet;
  - Utiliser les défauts des systèmes :
    - Adresse de la source pas vérifiée par les prorocoles IP;
    - Sniffing de trames IP (la librairie "pcap" permet de sniffer et renvoyer);
    - Phishing (hameçonnage) de site;
    - Exploits" très bien documentés…

Techniques de vol d'identité (3/3)

Exemple d'utilisation d'un outil de récupération de mots de passe :



Etude de cas (1/2)

- (Au cours d'une procédure de divorce) Monsieur Albert connaît le mot de passe de messagerie de Madame Albert. Il utilise l'adresse de sa femme pour créer des fausses preuves d'infidélité ou de mauvaise santé mentale.
  - Au début, Madame ne produit que des emails imprimés.
  - Pour démontrer l'usurpation, il faudra corréler agendas et date des emails, retrouver les adresses IP utilisées par l'émetteur…
  - La limite de un an pour l'archivage des journaux de connexion est très courte…
- Monsieur Bernard récupère les données du profil Facebook d'une jeune collégienne (nom, photo, amis). Il créé un compte homonyme puis invite en son nom tous ses amis, puis en obtiens des faveurs qu'il fait fructifier de proche en proche.
- Charles reçoit un jour un email provenant apparemment de son service de messagerie (Gmail). On lui demande son mot de passe de messagerie. Un peu (!) crédule Charles répond. Quelques heures plus tard, sa messagerie est devenue inaccessible, son mot de passe a été modifié, et quelqu'un utilise sa messagerie pour envoyer à tous ses contacts des messages de ce style :

Etude de cas (2/2)

Bonjour,

Excuse moi de t'importuner avec ce mail, mais je souhaiterais que tu me rendes un service d'une importance capitale. Je suis présentement en Afrique plus précisément en cote d'ivoire ou je suis venue d'urgence ainsi que Caroline parce que nous avons été informe du décès d'une grande amie qui date de longtemps et qui me tenais à cœur raison pour cela nous avons effectué le déplacement jusqu'ici.

Nous nous somme rendu ici afin de présenter nos condoléances a sa famille et voila que nous nous somme fait agressé sauvagement par des bandits qui m'ont tout pris : argent, téléphone portable, carte de crédit... Le plus grave c'est que Caroline se trouve en ce moment même a l'hôpital grièvement blessée.

J'ai donc besoin que tu m'aides en me faisant un transfert de 1800 euros afin que je les règle et que je puisse nous sortir de cette situation pénible le plus rapidement possible et rentrer urgemment. De plus je risque d'être déféré a la police pour non paiement de mon séjour.

Je t'en prie je ne veux pas durer dans cette situation alors fait le paiement pour moi, je te rembourserais dès que je rentre. J'ai confiance en toi et je veux que tu me promettes dans parler a personne de peur qu'il s'inquiète trop, raison pour la quelle je t'ai contacte.

Alors pour l'amour de Dieu fais parvenir ces 1800 euros via WESTERN UNION afin de vite les réceptionner et gérer les derniers détails afin de rentrer. Les informations pour m'expédier l'argent sont les suivantes.

NOM: Crédule

PRENOM: Charles

VILLE: ABIDJAN

PAYS: COTE D'IVOIRE

ADRESSE : 10 BP 321 Abidjan 10

Envoie-moi les références du mandat par mail.

Charles et Caroline

Conclusion

- L'usurpation d'identité est vécu comme un véritable viol, très difficile à prouver et à faire reconnaître.

- En situation de crise, dans un monde ou les « devoirs » ont été remplacés par des « droits », les barrières techniques et légales sont souvent insuffisantes pour lutter contre la cybercriminalité.

- La prise de conscience ne peut passer que par la formation, l'étude de cas pratiques et l'autocritique…

Merci!

Vielen Dank!

Développement subtil du "skimming"

Email : cyril.debard@gendarmerie.interieur.gouv.fr

par le Capitaine Cyril DEBARD

Unité d'Expertise Extraction de Données
Institut de Recherche Criminelle de la Gendarmerie Nationale
Pôle Judiciaire de la Gendarmerie Nationale

Sommaire

- Le Skimming : c'est quoi ?
  - Processus technologique
  - Où trouve-t-on des skimmers ?
  - Catégorisation
- Utilisation frauduleuse des données capturées
  - Fabrication de carte
  - Retrait d'argent ou transaction chez un commerçant
  - Revente des données
- Nouvelles menaces
  - Anti-skimmer vs skimmer
  - Faille EMV _ migration de la fraude
  - Nouveaux moyens de paiement
- Conclusion

Le Skimming : c'est quoi ?

- Processus technologique :

  - Capture des données de la piste ISO2 du bandeau magnétique

  - Capture du code confidentiel

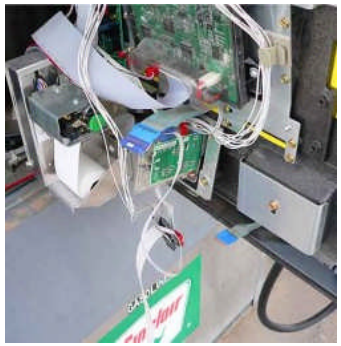
  - Copie des données capturées sur une carte "white plastic" ou un support volé.

Où trouve-t-on des skimmers ?

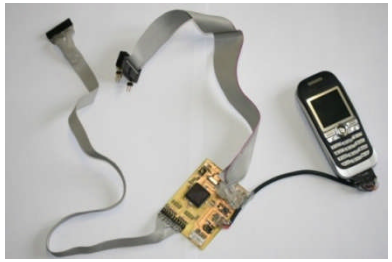
- Distributeur Automatique de Billets (DAB)
- Stations Essences
- Terminaux de paiements
- Porte d'entrée de banque
- Personnels (restaurants, commerçants…)

Catégorisation

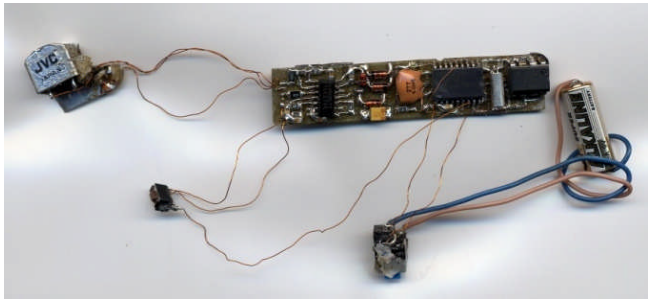
- Installation :
  - Montage,
  - Plug-in.



- Récupération des données :
  - Stockées dans le skimmer,
  - Envoyées par un transmetteur.



- Fabrication :
  - Commercial,
  - Commercial modifié,
  - Artisanal.



Utilisation frauduleuse des données

- Fabrication de cartes de paiements contrefaites :

- Retrait d'argent ou transaction chez un commerçant :

Utilisation frauduleuse des données

- Revente des données capturées :

http://vandump.biz/

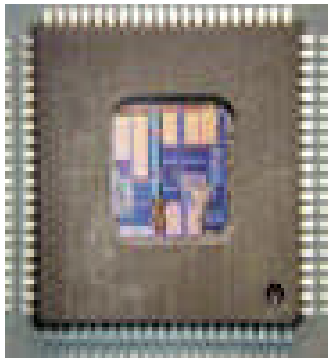
http://www.goldendump.com/dumps

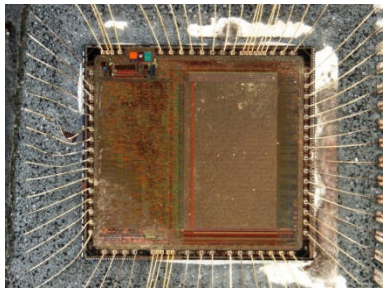
Nouvelles menaces

- Anti-Skimmer vs Skimmer :

Nouvelles Menaces

- Faille EMV _ Migration de la fraude ? :
  - 2010 : Ross Anderson démontre une faiblesse des spécifications EMV : attaque relais type "man in the middle". La puce n'authentifie jamais le processus de vérification du code PIN.
  - Réalisation d'une transaction avec saisie d'un code confidentiel quelconque. ("Yes-Card").
  - Aucune trace de cette fraude sur le réseau bancaire.
  - La skimmer piste magnétique "mute" en un skimmer puce et donc vers des pays non encore EMV !





Nouvelle Menaces

- Nouveaux moyens de paiement :
  - Sans contact - NFC : Paiement mobile, Carte contacless

  - Smart-phone : en tant que TPE, google Wallet…

Conclusion

- Skimmers de plus en plus sophistiqués et miniatures,
- Ressemblance Skimmers et anti-skimmers,
- Migration de la fraude (technologique, géographique)
- L'expertise forensique de plus en plus complexe,
- Chiffrement-cryptage des données (quasi)systèmatique.

* * *

- Veille technologique permanente,
- Dialogue expert-magistrat-enquêteur,
- Coopération Nationale et Internationale indispensable,
- Réseaux d'experts et laboratoires.

Merci!

Vielen Dank!

Questions

"Les cybermenaces à l'horizon 2020"