"Les cybermenaces à l'horizon 2020"

Table ronde :
Menaces et protection des infrastructures

Podiumsdiskussion : Gefahren und Absicherung der Infrastrukture

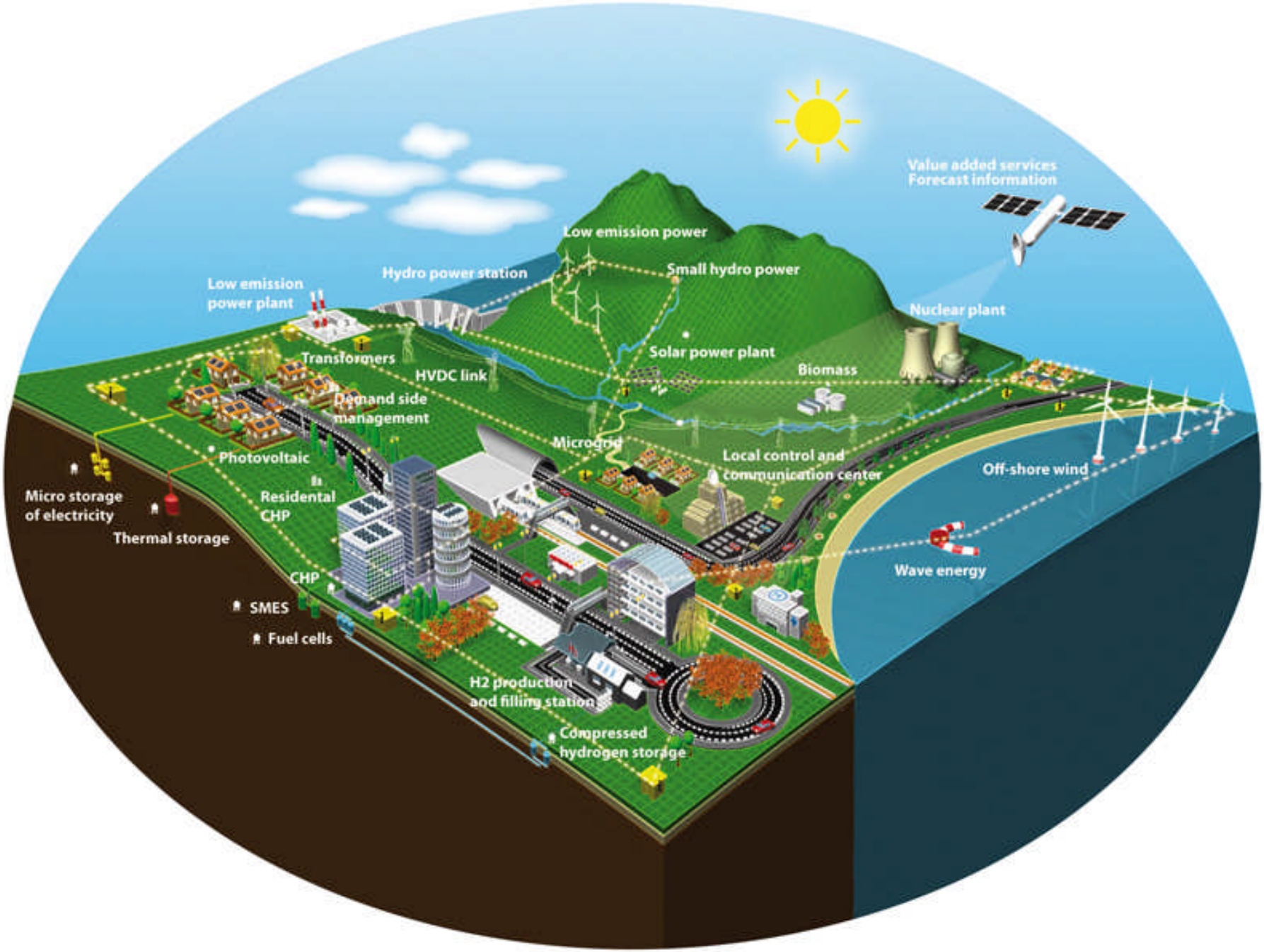
Animation par René ECKHARDT

Réseaux électriques intelligents et cybermenaces

Email : j.monereau@gmail.com

par Julien MONEREAU

Chargé de mission projet européen Greenov, ADEC

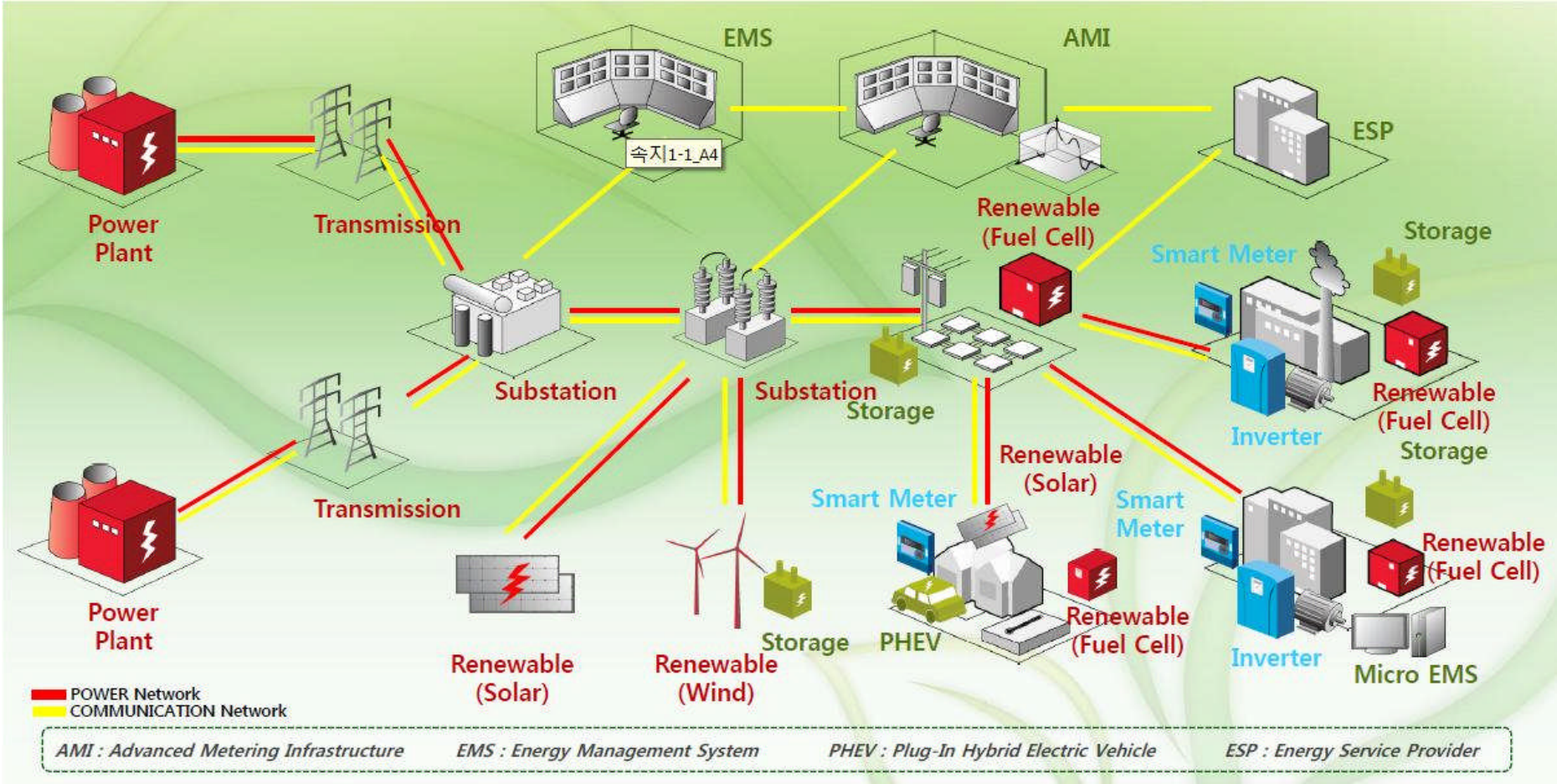

Value added services
Forecast information
Low emission power
Small hydro power
Hydro power station
Low emission
power plant
Nuclear plant
Transformers
Solar power plant
HVDC link
Biomass
Demand side
management
Microgrid
Photovoltaic
Local control and
communication center
Off-shore wind
Micro storage
of electricity
Residental
CHP
Thermal storage
Wave energy
CHP
SMES
Fuel cells
H2 production
and filling station
Compressed
hydrogen storage

Smartgrids : Définition

- "Les "smart grids", ou réseaux "intelligents", visent à intégrer de manière efficiente les actions de l'ensemble des utilisateurs (producteurs et consommateurs) afin de garantir un approvisionnement électrique durable, sûr et au moindre coût".

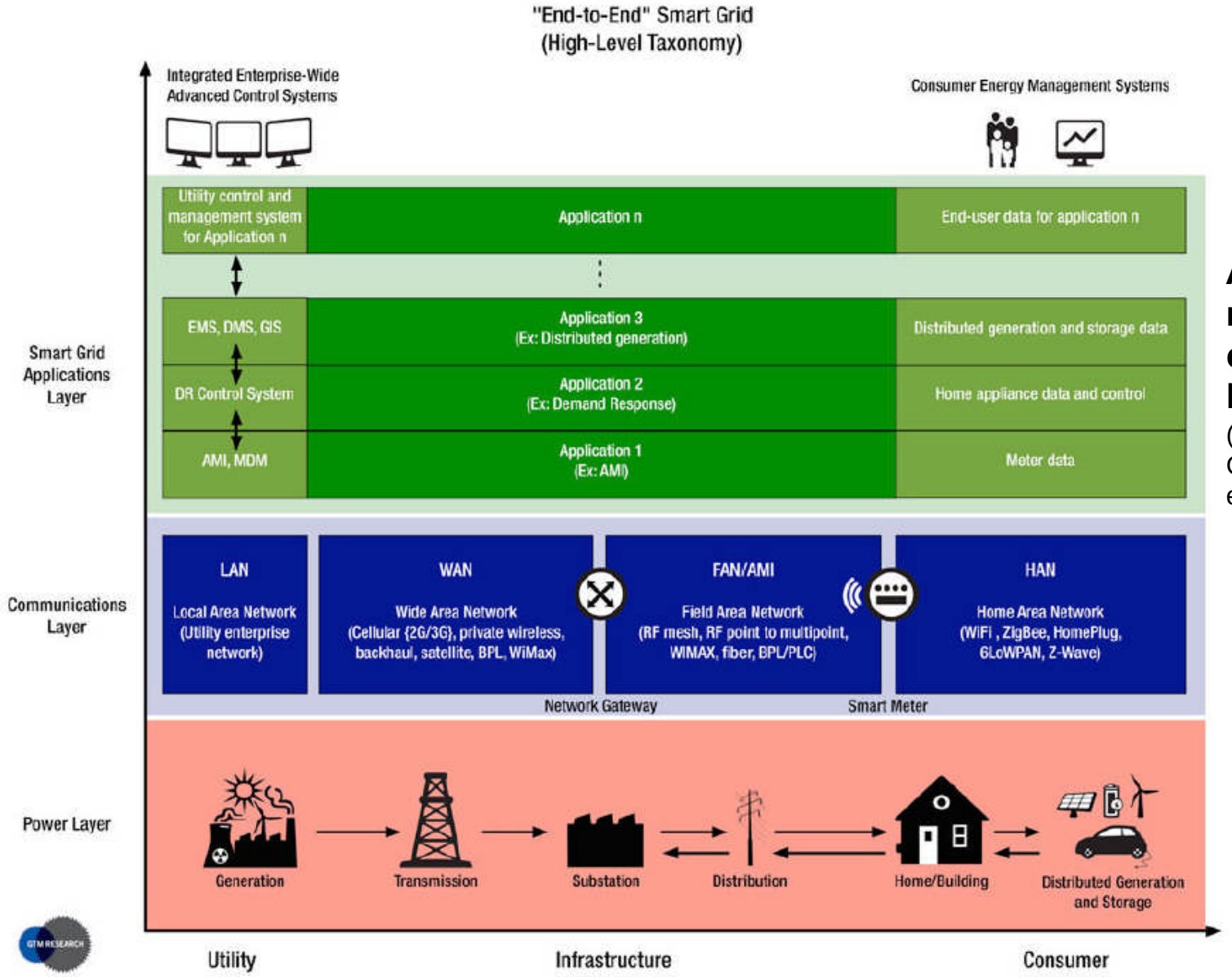
- Les "smart grids" associent les technologies de l'information et de la communication (TIC) aux réseaux. Les systèmes communiquant, en parallèle des réseaux de distribution, ainsi que l'intelligence embarquée doivent permettre un meilleur ajustement entre production et consommation d'électricité et l'intégration des énergies renouvelables.

Smartgrids : Fonctionnement



(source: http://sentientwave.com/content.php?id=34&lang_id=1)

Smartgrids : Architecture



Architecture et réseaux de communication et leurs applications

(source : La smartgrid en Californie: acteurs et enjeux (GMT Research))

Une vulnérabilité accrue des réseaux

- "La superposition de l'infrastructure de réseau électrique et des systèmes de TI modernes augmente considérablement les vulnérabilités et les points d'accès que les criminels et les terroristes peuvent utiliser pour attaquer le système électrique"

  (source: www.css.drdc-rddc.gc.ca/pstp/proj-prop/call-appel/security-securite/security-securite_02-fra.asp)

- "la cybersécurité devrait représenter un marché de 21 milliards de $ entre 2010 et 2015 avec un revenu annuel de 3,7 milliards de $ en 2015.

  Les investissements relatifs à la sécurité devraient correspondre à 15% de l'investissement total dans le Smart Grid"

  (source: www.bulletins-electroniques.com/actualites/64468.htm)

Classes de vulnérabilités selon le NIST

- 50 classes de vulnérabilités ont été identifiées par le NIST

(NIST : National Institut of Standards and Technology ;
l'agence nationale américaine des normes et de la technologie)

- Exemples:
  - Insufficiently Trained Personnel
  - Inadequate Security Training and Awareness Program
  - Insufficient Identity Validation, Background Checks
  - Inadequate Security Policy
  - Inadequate Risk Assessment Process
  - Inadequate Incident Response Process
  - Code Quality Vulnerability (CWE-398)
  - Authentication Vulnerability (CWE-287)
  - Cryptographic Vulnerability (CWE-310)

(source : Guideline for Smart Grid cyber security, Aout 2010 : www.ardi-rhonealpes.fr/web/guest/publications-electronique/detail/-/journal_content/56_INSTANCE_T7Ow/10136/254263/0-ARDI-PUBLI-TEMPLATE;jsessionid=7E247871DBCF2BA23CC01C13F996B073?refererPlid=25520)

Le système SCADA

- **L'exemple du ver STUXNET**

  C'est le premier ver découvert qui espionne et reprogramme des systèmes industriels, ce qui comporte un risque élevé. Il a été écrit spécifiquement pour attaquer les systèmes SCADA qui sont utilisés pour le contrôle commande.

  "Un porte-parole de Siemens a indiqué que le ver avait été trouvé sur 15 systèmes dont 5 sont situés en Allemagne dans des usines abritant des systèmes de contrôle de processus industriels"

Protection des données personnelles

- "La Commission (européenne) prévoit des dispositions juridiques et réglementaires afin de veiller à ce que la vie privée des consommateurs soit respectée. Elle va vérifier les législations nationales qui pourraient s'appliquer pour tenir compte des spécificités des réseaux intelligents en matière de protection des données. Les organismes européens de normalisation devront adopter une approche dite "*privacy by design*" pour élaborer les normes techniques des réseaux intelligents" (11 avril 2011)

(source:http://preprod.europolitique.abccom.cyberscope.fr/politiques-sectorielles/reseaux-intelligents-la-commission-envisage-des-mesures-reglementaires-artb301040-13.html)

Un déploiement dans l'urgence

- **Communication de la commission européenne**

  "Réseaux intelligents: de l'innovation au déploiement" (COM(2011) 202 final, 12 avril 2011):

  - "La Commission entend promouvoir un déploiement plus rapide et plus large des réseaux intelligents en Europe […] Sur la base des avis exprimés par les institutions et les parties prenantes sur la présente communication, elle entend prendre des initiatives appropriées dans le courant de 2011"

    (source: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/20110412_act_fr.pdf)

Pour aller plus loin

❑ Smart grids :

www.smartgrids.eu

www.smartgrids-cre.fr

www.projetpremio.fr

www.e-energy.de/en/animation/

.

❑ Smart grids et cyber sécurité :

National Institute of standard and technology (NIST), documents en anglais :

http://www.ardi-rhonealpes.fr/web/guest/publications-electronique/detail/-/journal_content/56_INSTANCE_T7Ow/10136/254263/0-ARDI-PUBLI-TEMPLATE;jsessionid=7E247871DBCF2BA23CC01C13F996B073?refererPlid=25520

Recherche et développement pour la défense Canada: http://www.css.drdc-rddc.gc.ca/pstp/proj-prop/call-appel/security-securite/security-securite_02-fra.asp

Merci!

Vielen Dank!

Les transactions et applications en ligne, le point de vue de la banque

Email : michel.wendling@alsace.banquepopulaire.fr

par Michel WENDLING

Directeur logistique
Banque Populaire d'Alsace

Sommaire

- Un peu de nostalgie
- Aujourd'hui
- Pourquoi cette ampleur ?
- Et le secteur bancaire ?
- Quelques risques
- En images

Un peu de nostalgie

- ORTF…l'archange
- virement international
- un bug dans une chaîne posé par un informaticien malveillant
- une empreinte de carte bleue récupérée par pression sur une nappe de table en papier au fond d'un restaurant

Aujourd'hui

- aujourd'hui le cyberespace est un "far west" virtuel pour hors la loi débordants d'ingéniosité qui font vivre un ‘underground’ économique dans des mondes invisibles
- la cybercriminalité aurait généré, en 2010, 1000 milliards de dollars dans le monde, soit plus que les revenus du trafic de stupéfiants
- et les technologies de l'information et de la communication sont devenues les cibles privilégiées de la malveillance

Pourquoi cette ampleur ?

- essor du e-commerce
- une offre technologique en explosion : téléphones portables , e-book , i…
- le développement du "cloud computing"
- des peines faibles au pénal
- une insuffisance de coopération internationale

Et le secteur bancaire ?

- exposé car
  - l'informatique = outil de production qu'il faut protéger physiquement :
    - en renforçant la robustesse des infrastructures informatiques et de télécommunication
    - en dupliquant les installations
    - en protégeant l'accès aux serveurs (firewall)
    - en ayant un PCA (Plan de Continuité d'Activité) opérationnel quelle que soit la défaillance
- exposé car
  - entre internet et intranet interne il y a une grande proximité (étanchéité)

Et le secteur bancaire ?

- exposé car
  - monde ouvert : clients, non clients, employés, partenaires, prestataires externes (maintenances)
- exposé car
  - toutes les technologies sont utilisées

    (la banque : c'est quand je veux, où je veux, comme je veux)
- exposé car
  - quelques automates "sympathiques" : gab: distribution d'argent hors des murs / cartes : moyen de paiement hors des frontières/…

Et le secteur bancaire ?

- exposé car
  - entre internet et intranet interne il y a une grande proximité (étanchéité)
- exposé car
  - les outils et applications sont de plus en plus mis à disposition du monde extérieur, pour faire des simulations par exemple
- exposé car
  - le matériau est riche : données clients nombreuses, adresses, mise à disposition de transactions pour faire des opérations
- exposé car
  - si l'exploitation des failles techniques est un axe d'attaque, la faiblesse humaine en est un autre et ô combien plus sensible, car il s'agit d'argent

Quelques risques

- vols de données
- carte usurpée
- mots de passe récupérés
- usurpation d'identité
- piratages d'adresses courriel (pour procéder à l'envoi de courriels (spams)) ou envoi de messages d'arnaque
- botnets : réseau d'ordinateurs infectés qui, quand ils sont réveillés, deviennent des robots (ordi zombies) / inondation de requêtes / serveurs inopérants
- phishing contraction : fishing (pêcher) et phreaking (pirater)
- pharming redirection vers de faux sites internet pour infecter les programmes par des codes malveillants
- skimming

Conclusion

Le monde bancaire va vivre dans une nouvelle dimension de la malveillance :

du hold up physique
on est passé
au hold up virtuel

Merci!

Vielen Dank!

L'informatique de production, talon d'Achille des entreprises

Email : dominique.schoenher@gendarmerie.interieur.gouv.fr

par Dominique SCHOENHER

Officier-professeur
du Centre d'enseignement supérieur de la gendarmerie
Lieutenant-colonel de la gendarmerie nationale

Différences entre systèmes

- Il existe deux systèmes informatiques en entreprise
  - L'un de gestion (paie, RH, site internet, etc.)
  - L'autre de production qui lui permet de produire ce qu'elle vend

- Leurs degrés de protection diffèrent
  - L'informatique de gestion est (mieux) protégée car bien identifiée comme une cible dont les attaques sont davantage médiatisées
  - L'informatique de production ne l'est qu'insuffisamment, car longtemps préservée par sa spécificité

Révélation du point faible

- Black Hat 2010 : SCADA systems far more insecure than enterprise IT systems
  - *In its analysis of approximately 120 critical infrastructure facilities, researchers at the firm discovered 38,753 vulnerabilities, Jonathan Pollet, founder and principal consultant for Red Tiger Security, said during a session Wednesday at the Black Hat conference in Las Vegas.*
  - *Moreover, there was a 331 day-gap between the time a vulnerability was disclosed in the public and when it is discovered in an industrial control systems assessment, Pollet said. One system contained a vulnerability that was disclosed three years prior to when it was discovered in the SCADA environment.*
- **L'informatique de production est à présent clairement identifiée comme un point faible de la sécurité informatique des entreprises mais aussi des infrastructures vitales, ce qui élève encore les enjeux.**

Conséquences des différences

❑ **Si les finalités divergent, les deux systèmes informatiques convergent** par le double phénomène de standardisation et d'intégration :

- Des matériels ; des OS ; des logiciels.

Et ce, pour des raisons de coût et d'amortissement de la part des éditeurs et constructeurs.

- Une connexion à Internet en expansion pour faciliter la maintenance

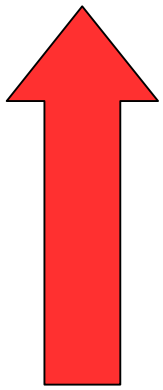
- Une interconnexion des deux réseaux (gestion et production) pour des raisons de rapidité de remontée de l'information vers les dirigeants

❑ **Il en résulte des vulnérabilités de plus en plus partagées alors que le différentiel de sécurisation fait de l'informatique de production une cible aisée.**

Vulnérabilités et capacités

- Si les vulnérabilités sont à présent partagées,

- les contraintes de sécurité ne sont pas les mêmes entre la production et la gestion

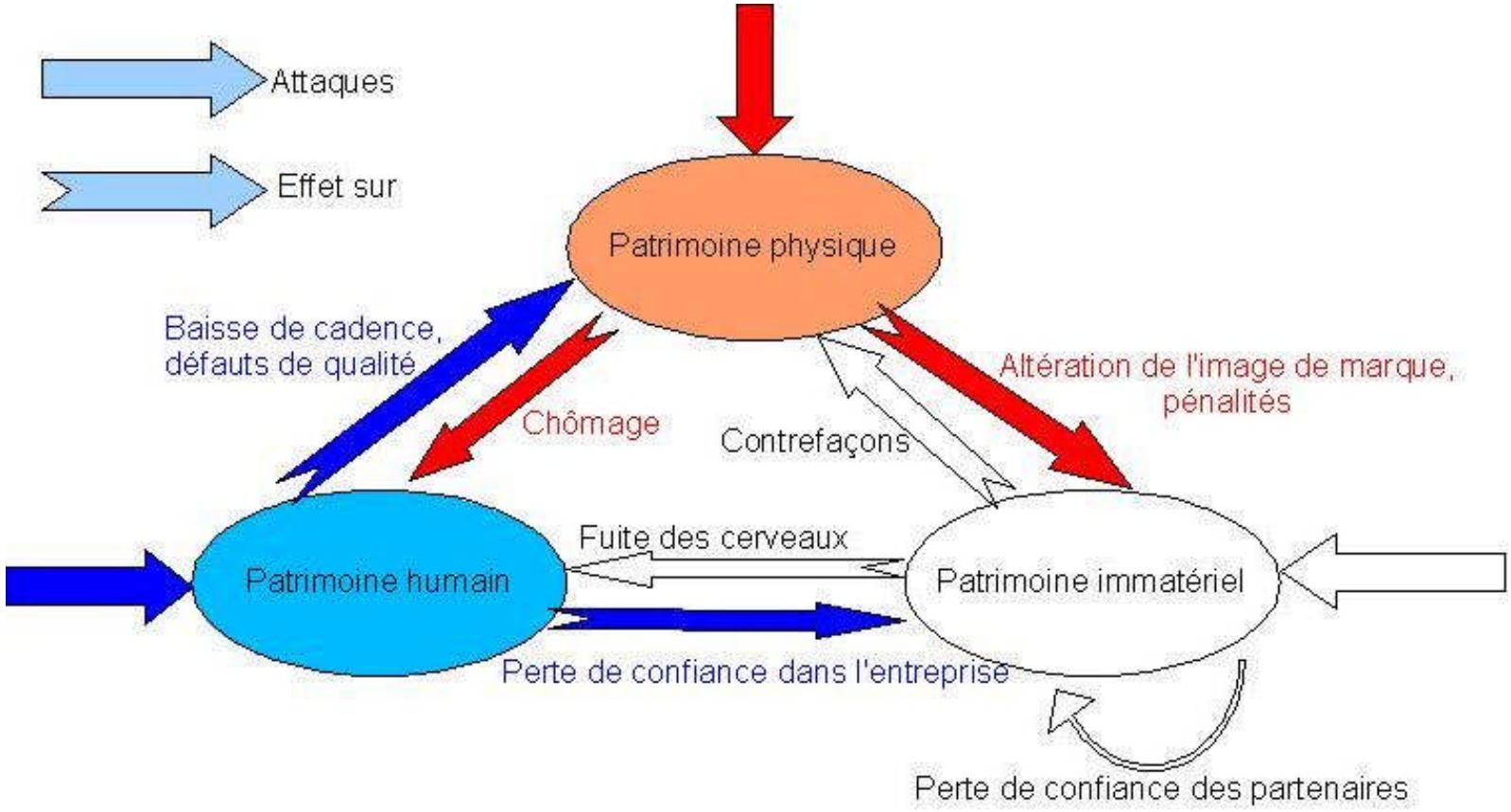


Gestion	Production
Confidentialité	Disponibilité
Intégrité	Intégrité
Disponibilité	Confidentialité

- les capacités des deux systèmes restent différentes et les solutions "gestion" ne sont pas transposables à la "production"

Conséquences globales

- Une attaque visant l'informatique de production peut avoir des conséquences directes ou par rebond sur les trois patrimoines de l'entreprise :



Merci!

Vielen Dank!

Questions

"Les cybermenaces à l'horizon 2020"