


Gestion des vulnérabilités

« Back to basic » ou
nouvelle tactique face à l'évolution des attaques ?

Xavier PANCHAUD
Juin 2012, Paris


 **BNP PARIBAS** | La banque d'un monde qui change

Le groupe BNP Paribas



Le Groupe
BNP Paribas en bref

Présent dans **78** pays
près de **195.200** collaborateurs, dont **152.400** en Europe,
15.000 en Amérique du Nord, **13.500** en Asie*
*(31/03/2012)

 **BNP PARIBAS** | La banque d'un monde qui change 2

Organisation du BNP Paribas

Trois domaines d'activité, organisée en « pôles » ou « entités opérationnelles » ou « métiers », répartis sur différents « territoires » (pays ou régions).
Neuf « fonctions » assurent un appui transversal à l'ensemble des activités.
Les collaborateurs de ces domaines travaillent ensemble pour être au plus près des besoins du client.

Retail Banking La Banque de détail	Investment Solutions* Les solutions intégrées pour les investisseurs	Corporate and Investment Banking - CIB* Les métiers de financement et d'investissement
<p>Une présence dans 52 pays - Plus de 124 000 collaborateurs Près de 6 000 agences bancaires - 250 000 points de contact clients</p> <p>BOF - Banque de détail en France 31 000 collaborateurs 2 200 agences 20 centres d'affaires entreprises 220 centres de banque privée</p> <p>BNP - Retail - BNP Entreprises - Opérations Agence-vente - Banque Privée France - Banque de détail - BNP Paribas Factor - Personal Finance - BNP Paribas Développement</p> <p>BNL - Banque de détail en Italie 14 000 collaborateurs Plus de 400 points de vente 27 centres d'affaires entreprises 2 centres de Banque Privée 2 centres de détail en Italie et 12 Italian Retail Units</p> <p>BNP - Retail - Retail et Private (Banque de détail et banque privée) - Corporate (entreprises et institutions) - Argentinians, BNL, France</p> <p>BNP West - Banque de détail en Espagne 11 000 collaborateurs dans 20 Etats de l'Espagne et Gibraltar 742 agences 2 centres d'affaires Bank of the West First Tennessee Bank</p> <p>Europe Méditerranée Banque de détail dans 30 pays émergents Plus de 30 000 collaborateurs 2 000 agences</p> <p>Finances d'Etat - Le Moyen Orient - Le Moyen Méditerranéen - Espagne, Italie - France et le Moyen-Orient - Afrique - Les ODM TOM</p> <p>Personal Finance Crédit aux particuliers - crédit à la consommation et crédit immobilier Plus de 31 000 collaborateurs dans 39 pays Cibacross BNP Paribas International Buyers, Cash Management BNP Paribas Personal Finance, Fiduciaries, UCI, Lohr</p> <p>Equilibrium Solutions Solutions locales aux entreprises et aux professionnels 7 000 personnes dans 24 pays BNP Paribas Leasing Group, Aviva</p>	<p>Présent dans 61 pays - Plus de 26 000 collaborateurs 6 expertises complémentaires</p> <p>BNP Paribas Wealth Management (Banque Privée) 4 500 collaborateurs répartis dans 30 pays Propose à ses clients fortunés et à des familles fortunées une gamme étendue de produits et services sur mesure</p> <p>BNP Paribas Investment Partners (Classe d'actifs) 2 600 collaborateurs répartis dans 34 pays Gestion d'actifs</p> <p>BNP Paribas Personal Investors (Epargne et courtage en ligne) 4 200 collaborateurs dont plus de 90% en ligne Conseil Brocureur et courtage via ses trois acteurs-clés : Cortol Concorce, FORTIS, Crédit</p> <p>BNP Paribas Securities Services (Services Titris) Plus de 6 000 collaborateurs répartis dans 28 pays Services liés pour un éventail de sociétés de gestion, d'institutions financières et d'entreprises</p> <p>BNP Paribas Real Estate (Immobilier) 9 200 collaborateurs couvrant un réseau de 28 pays (avec les affiliés) 6 métiers complémentaires : Protection / Transaction / Counsel / Support / Investment management / Property management</p> <p>BNP Paribas Assurance 8 000 collaborateurs dans 64 % hors de France notamment sous le régime local Produits et services dans les domaines de l'assurance, la prévoyance et l'investissement</p>	<p>Présent dans plus de 60 pays - 17 000 collaborateurs 13 000 clients</p> <p>METIERS DE FINANCEMENT 2 100 collaborateurs</p> <p>Bankers Finance 2 100 collaborateurs</p> <p>Corporate & Transaction Group Gestion de flux bancaires Corporate Management des Corporates, Trade Finance, Cash Management, plain vanilla, Structured Finance</p> <p>ACTIVITE DE COMMERCE ET MARCHES DE CAPITAL 2 500 collaborateurs</p> <p>Corporate Finance Fournit à ses clients, opérations sur marchés primaires actions, conseils aux entreprises cotées, conseils en restructuration</p> <p>Global Equities & Community Derivatives Activités de recherche, structuration, trading et vente sur actions volatiles et dérivés actions, indices et fonds d'actifs mondiaux, sur les marchés émergents</p> <p>Fixed Income Activité "cash", swap et "change" est à l'appui sur une expertise mondiale en termes d'intégration, recherche, distribution, Sales et Trading sur les marchés des taux d'intérêt, crédit, dérivés et produits structurés</p> <p>Capital & Balance Sheet Management</p> <p>ALM Treasury</p> <p>Coverage 1 300 collaborateurs</p> <p>Global & Transaction Group Gestion de flux bancaires Corporate Management des Corporates, Trade Finance, Cash Management, plain vanilla, Structured Finance</p> <p>Client Marketing Unité commerciale au quotidien des clients via les produits de flux</p> <p>Fonctions CIB 9 800 collaborateurs dont 2 200 chefs de métiers Technology & Operations</p>

En parallèle de ces 3 domaines d'activité, des Sociétés d'Investissements | Mélière Immobilier commercial - Principal Investments Investissement pour compte propre de BNP Paribas

9 Fonctions Groupe - 200 000 collaborateurs
Affaires Fiscales Groupe - Affaires Juridiques Groupe - Conformité Groupe - Finances Développement Groupe - Group Risk Management
Inspection Générale - Technologies & Processus - Marque, Communication et Qualité - Ressources Humaines Groupe.

Fortis : Dans le cadre du rapprochement en cours, l'organisation intégrera prochainement les activités de Fortis



BNP PARIBAS | La banque d'un monde qui change

© 2015 BNP

La sécurité des SI au sein de BNP Paribas

OBJECTIF : maîtrise démontrée du risque sécurité lié aux SI conformément

- Aux lois et règlements de l'industrie bancaire et financière
- Les valeurs du groupe BNP Paribas : éthique, développement durable, valeur de la marque, maîtrise du risque opérationnel...
- L'appétence au risque propre à chaque métier dans chaque implantation

PÉRIMÈTRE : tout le groupe sur l'ensemble de ses territoires

COUVERTURE : la sécurité de l'information comme définie par l'ISO 27001

MOYENS : un cadre de management de la sécurité (politique, scorecard, gouvernance projet, veille...) et des actions permanentes

EFFECTIFS : sécurité groupe (~40 pers.) + un réseau de BISO / CISO (~30 pers.) + une communauté (~150 pers.) et des acteurs opérationnels repartis (~500 pers. soit 4% des informaticiens)

La maîtrise du risque de sécurité lié aux SI, c'est :

- Une dimension de la stratégie de Sécurité Globale
- La contribution au processus global de gestion des risques opérationnels
- Un moyen de contrôle permanent
- Une valeur du groupe BNP Paribas et de des métiers



BNP PARIBAS | La banque d'un monde qui change

Agenda

- **Inventaire et classification**
 - « Car nous ne pouvons protéger que ce que nous connaissons »
- **Veille**
 - « Car nous ne pouvons nous protéger que de ce que nous connaissons »
- **Patch management**
 - 0-days, ½-days et vulnérabilités humaines : lesquelles prioriser
- **Gestion des priorités**
 - Risk acceptance et dérogation
- **Contrôle**
 - Parce que « la confiance n'exclut pas le contrôle » (Lénine)



2011 en chiffre

721 avis de sécurité

84 mises à jours majeurs

2427 mises à jours mineurs

1150 produits

9248 versions



Inventaire et classification

« Car nous ne pouvons protéger que ce que nous connaissons »

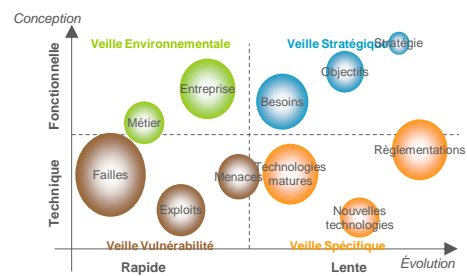
- **Un pré-requis pour :**
 - Connaître son parc
 - Identifier les priorités
 - Disposer d'état des lieux fiables
- **Souvent réduit à l'état d'objectif**
 - Limité par la taille des inventaires
 - L'indiscipline des acteurs
 - La limitation des outils



Veille

« Car nous ne pouvons nous protéger que de ce que nous connaissons »

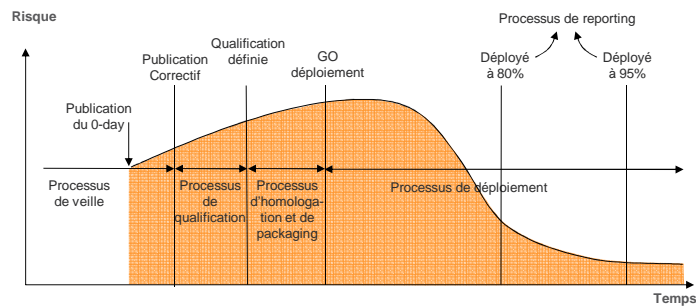
- **Indispensable sur les gros parcs**
 - **Veille Vulnérabilité**
 - Pour identifier les points faibles et les actions à réaliser
 - **Veille Environnementale**
 - Pour définir les priorités
 - **Veille Spécifique**
 - Pour anticiper



Patch management

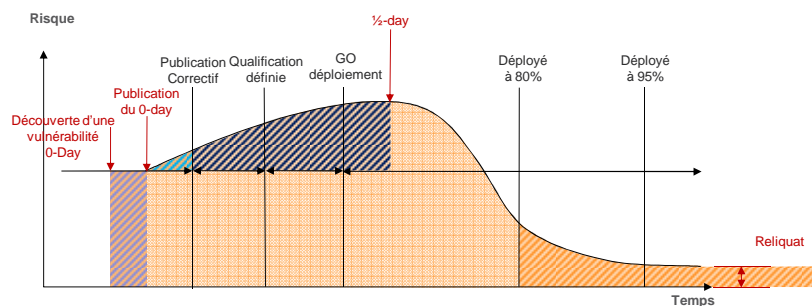
0-days, ½-days et reliquat: lesquels prioriser

- **Rappel sur le cycle de patch-management**



La vérité sur le patch management

- **Zone de risque non maîtrisable avant la connaissance du 0-day**
- **Zone de risque liée à la publication du 0-day**
- **Zone de risque subie jusqu'au patch de la moitié des équipements**
- **Zone de risque résiduelle : « reliquat »**



Gestion des priorités

- **Le patch management n'est possible que si un correctif existe**
 - Les zones de risque induites par un 0-Day doivent être gérées par des mesures de sécurité autre que le patch management
- **La zone de risque subie pendant le déploiement du correctif doit être couverte par des mesures de sécurité complémentaires**
 - Priorisation de déploiement (actifs critiques ou très exposés)
 - Monitoring accru
- **Le risque porté par le reliquat doit continuer à être réduit**
 - Identification des équipements vulnérables non inventoriés (scans)
 - Suivi du déploiement et identification des anomalies
 - En dernier recours acceptation du risque et définition de mesures complémentaires si impossibilité de passer le correctif sur un serveur



Un processus complexe

La gestion des vulnérabilités est un processus complexe intégrant un nombre important de mesures

- **Organisationnelles**
 - Veille
 - Gestion des inventaires
 - Classification
 - Suivi du déploiement
 - Réalisation de tableaux de bord
 - Acceptation du risque
- **Techniques**
 - Détection d'événements et signatures (SMC)
 - Identification et implémentation de mesures de sécurité complémentaires
 - Déploiement de correctif
 - Scans de vulnérabilité

L'efficacité de ce processus ne peut être garanti que si toutes ces mesures sont déployées



Des contrôles pour assurer l'efficacité du processus

« Implémentation »

« Efficacité »

« Pérennité »

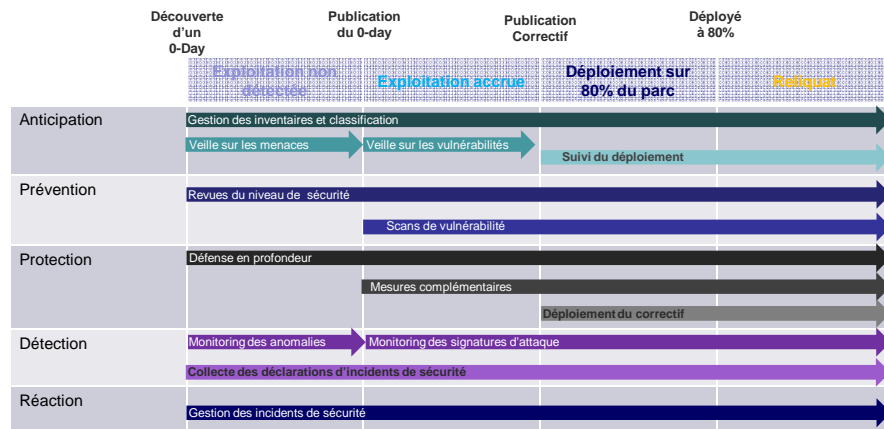
- **Trois niveaux de contrôle**
 - Contrôle de premier niveau par les équipes opérationnelles
 - Contrôle permanent par le contrôle interne
 - Contrôle périodique par l'audit interne
- **Ciblant l'ensemble du processus sécurité**
 - Du physique à l'organisation de la sécurité
 - Du technique à l'organisationnel



En revenant aux basiques

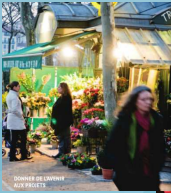


Une nouvelle tactique face à l'évolution des attaques : Ne pas oublier ses basiques





Questions



BNP PARIBAS | La banque d'un monde qui change