CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

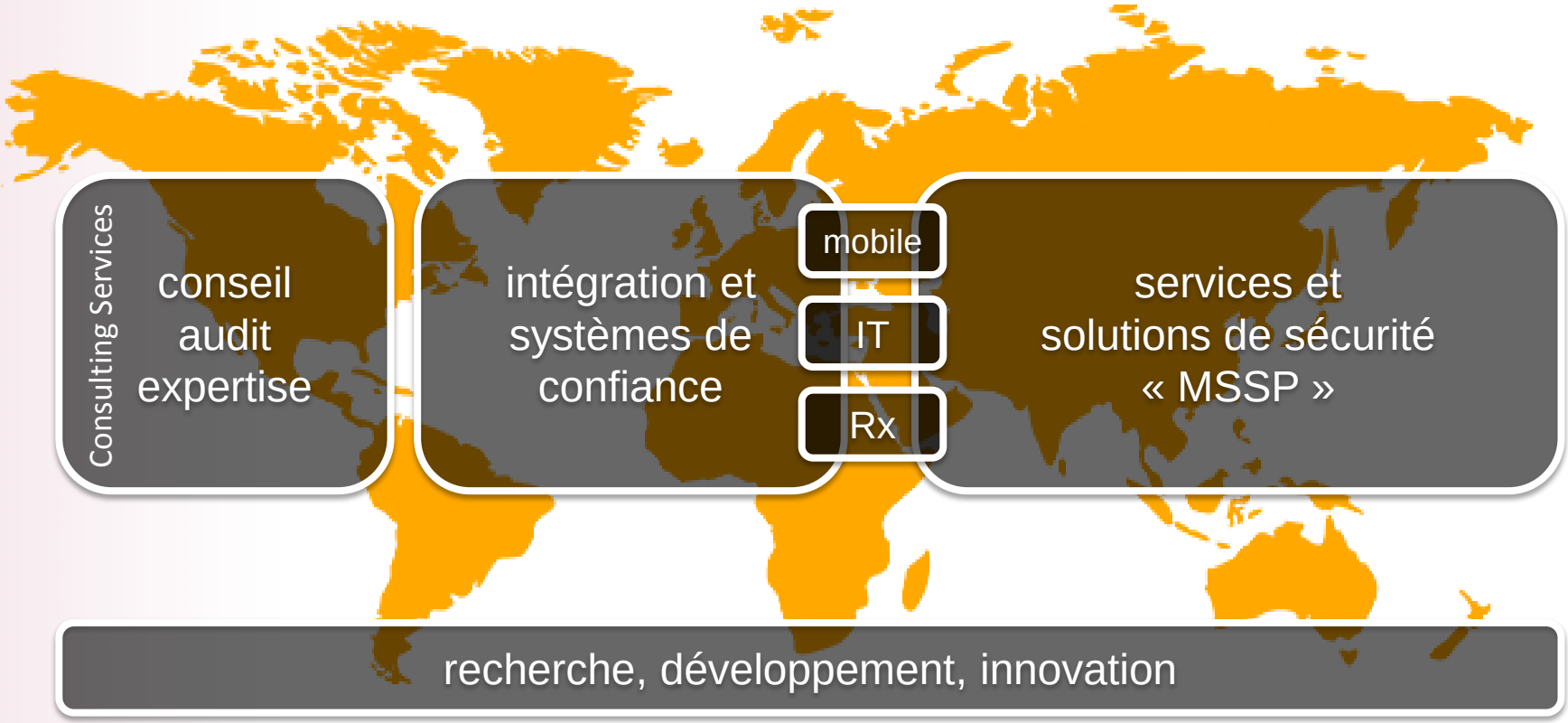
La sécurité des PABX IP

Panorama des risques et introduction des mesures de protection

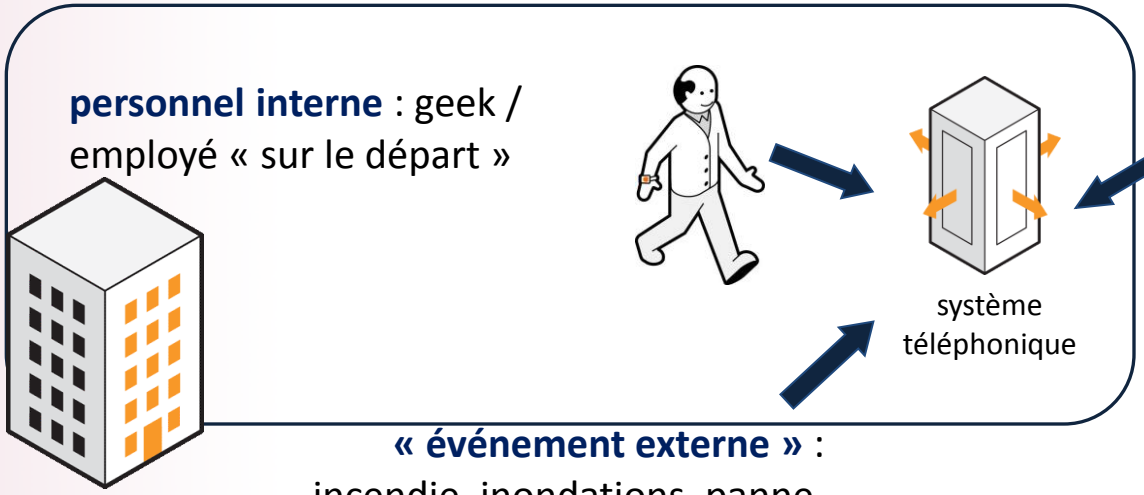
Marc LEFEBVRE – Consultant Sécurité – Orange Consulting - 25 avril 2013

cybersécurité by Orange

unité d'affaire « cybersécurité » d'Orange Business Services



quels attaquants ? quelles motivations ?



- nuire à l'entreprise: obtenir des informations confidentielles
- nuire à l'entreprise: atteinte à la disponibilité
- jouer avec les équipements
- nuire à l'entreprise: faire des gains / économies

des risques hérités de la téléphonie « numérique » reconduits sur la téléphonie sur IP

détournements de fonctionnalités téléphoniques légitimes ou des malversations sur les protocoles Voix et de Signalisation

confidentialité: écoute / enregistrement de communications

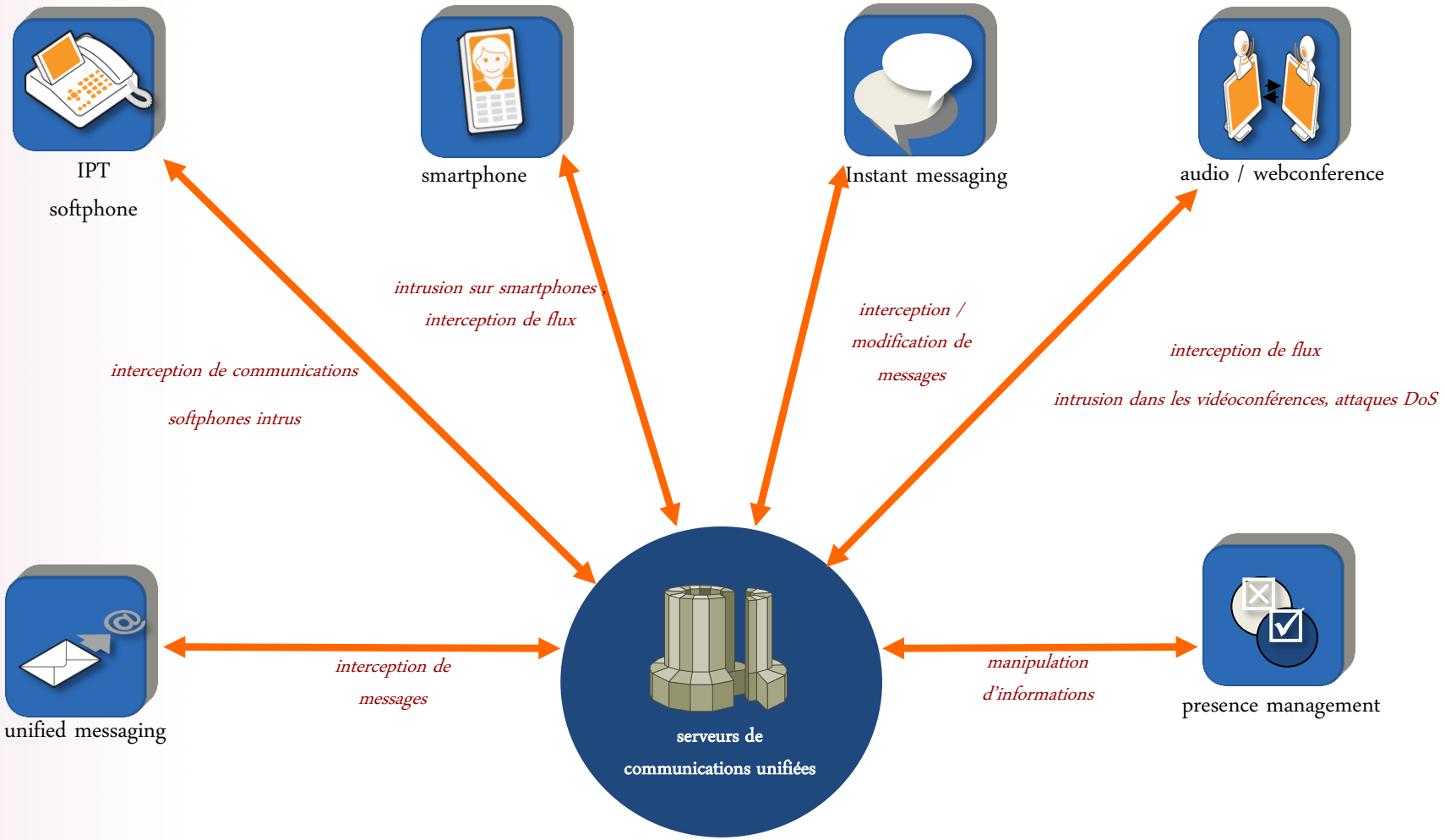
disponibilité: dénis de services

intégrité: usurpation d'identité, modification de paquets

fraudes financières

Intrusion sur les systèmes ToIP depuis l'externe pour atteinte au SI de l'entreprise

des nouveaux risques sur un écosystème « hyperconnecté »



des nouveaux risques sur un écosystème « hyperconnecté » : cas des smartphones / tablettes

smartphones / tablettes avec applications de « téléphonie d'entreprise » intrusion dans ces dernières pour récupération de messages vocaux, codes pin utilisateurs, traces d'appels, fraude financières par usurpation de compte.

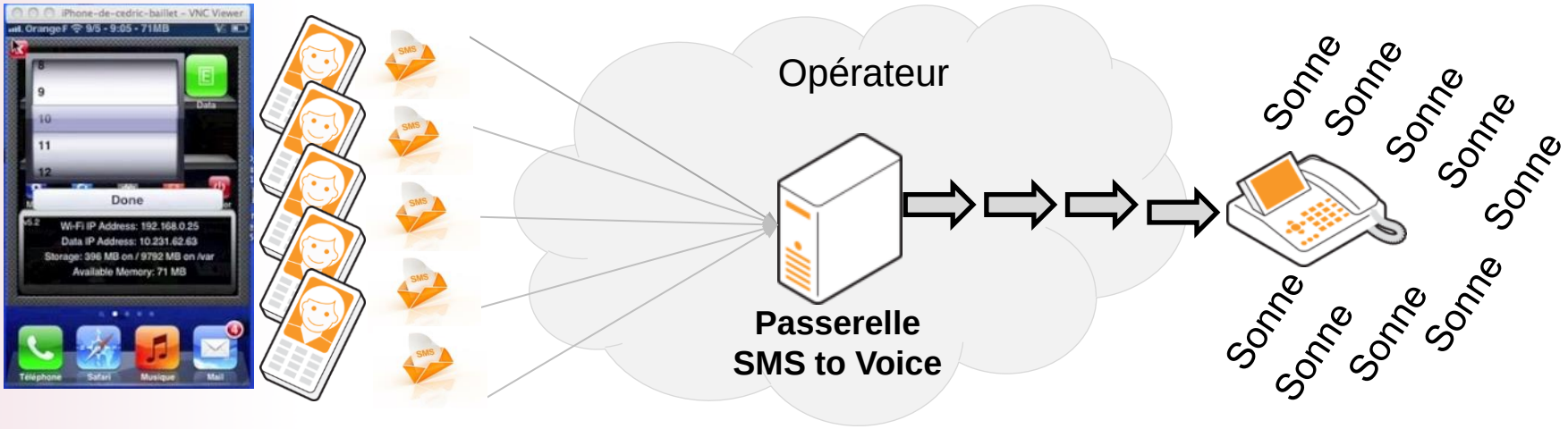
BYOD : quelle sécurité pour des Smartphones d'Employés sur lesquels sont installées les applications de téléphonie d'entreprise ?

50 % des utilisateurs souhaitent n'avoir qu'un seul terminal (une convergence entre ligne fixe et mobile, et équipement personnel et professionnel *(source : Entretiens menés par TNS Sofres pour Orange)*

39% des entreprises ont déjà connu des failles de sécurité en raison de l'utilisation d'appareils personnels non autorisés *(source : Entretiens menés pat TNS Sofres pour Orange)*

des nouveaux risques sur un écosystème « hyperconnecté : focus sur le TDoS

TDoS : SMS Bombing : Spam de plateforme téléphonique par envoi de SMS massifs sur postes téléphoniques



Autres risques sur un écosystème « hyperconnecté »

messagerie instantanée : interception de messages, récupération de contacts, logins / mots de passe de comptes (XMPPloit)

Internet : scan d'équipements ToIP pour intrusion, écoutes, dénis de Service ou reroutage d'appels

exemple http://www.shodanhq.com
- moteur de recherche
- 19 $ pour 10 000 références et l'accès au filtrage et à l'export via xml
- 5 heures de travail de tri des résultats (script, scan, analyse)
- détection de postes SIP, équipements Visio connectés sur Internet avec mots de passe par défaut

écrans téléphoniques évolués / interfaces web utilisateurs : intrusions pour atteinte aux données métiers ou défacement d'interfaces

plans d'actions de sécurité

- Équipements, applications pour exploitants et utilisateurs
  - Renforcer la sécurité des contrôles d'accès, restreindre les droits d'accès au réseau public et classe de services, redonder les systèmes critiques
- Réseaux voix et données
  - Cloisonner les flux, implémenter des systèmes de sécurité VoIP (SBC, IDS/IPS Voix), faire des choix de sécurité LAN (802.1x, chiffrement, etc.)
- Organisation
  - Mettre en place une gouvernance SSI pour la Voix : audits des architectures et configuration de postes, processus de changements de mots de passe, suivi des mises à jour de sécurité, analyse des flux suspects.

prendre en compte la Téléphonie sur IP dans la PSSI d'Entreprise

et la sécurité de la téléphonie en mode Cloud ?

des enjeux importants : risques d'atteinte « à grande échelle » à la confidentialité des données de différents clients, de conversations, de la disponibilité des services, de l'intégrité et de la conformité des données

- nécessité de contrôler l'existence des mesures de sécurité « adéquates » au cloud

confidentialité : chiffrement des données au repos / en transfert entre client / fournisseur

confidentialité : cloisonnement des serveurs téléphoniques / séparation des flux réseaux pour différents clients

authentification fortes pour les accès Internet

disponibilité : protection contre TDoS, plans de reprises, plateforme de pré-production pour mises à jour, portails web de protection

merci

Marc LEFEBVRE – Consultant Sécurité – Orange Consulting
marc.lefebvre1@orange.com +33(0)6 45 75 94 38