Identification & Exploitation des failles humaines par les prédateurs informationnels…

Michel Iwochewitsch – 04/06/2008

<u>Avertissement :</u> le cadre temporel de cette conférence ne permet pas de développer l'ensemble des outils, méthodologies, ou concepts concernant cette riche problématique !

Le conférencier se tient à disposition des participants pour tout renseignement complémentaire concernant les sujets abordés au cours de cette conférence.
(mi@stratinternational.com)

De la notion de “prédateur” ?

Qui sont-ils ? Qu’ont-ils en commun ..?

3

Le prédateur « one-shot » ! Un objectif simple : obtenir très vite une information sensible. Des méthodes efficaces mais peu pérennes dans le temps! Les principales catégories sont :

Le social engineer, certains journalistes, l’opérateur IE, le désinformateur, l’escroc…

Le prédateur « long-terme » ! Un objectif simple : obtenir un flux d’informations sensibles en s’établissant durablement. Redoutable et bien formé ! Contrairement à une légende savamment entretenue : tout le monde peut-être la cible ! Les principales catégories sont :

Le spooke (renseignement industriel), le traitant d’un SR, l’activiste, le criminel rattaché à une organisation transnationale de criminalité organisée…

Page ▪ 4

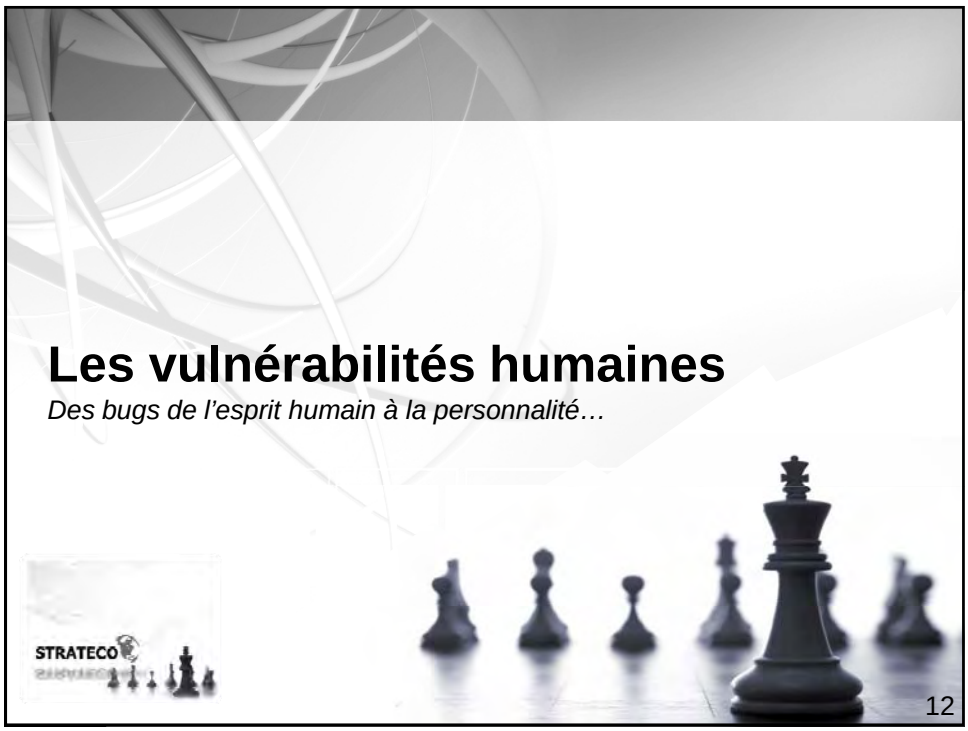
- Confidentiel -

Le concept phare du prédateur : la valeur réelle d'une information

Les « valeurs » de l'information !

- La valeur pécuniaire… Directe ET indirecte !
- La valeur liée à l'intégrité de l'information : un exemple, les CRM dans la distribution
- La valeur liée à la confidentialité : un exemple, les informations financières de fusac
- La valeur liée à la disponibilité : des exemples, SABRE, les opérations bancaires, etc.
- Le coût de nuisance : la perte d'un PC portable, le « vol d'identité », le temps passé à recréer l'information, etc.
- La valeur pour « l'opposition » : quelle est la valeur de l'information pour le criminel ? L'officier traitant ? Le concurrent ?


STRATECO


Les vulnérabilités humaines
Des bugs de l'esprit humain à la personnalité…
STRATECO
12

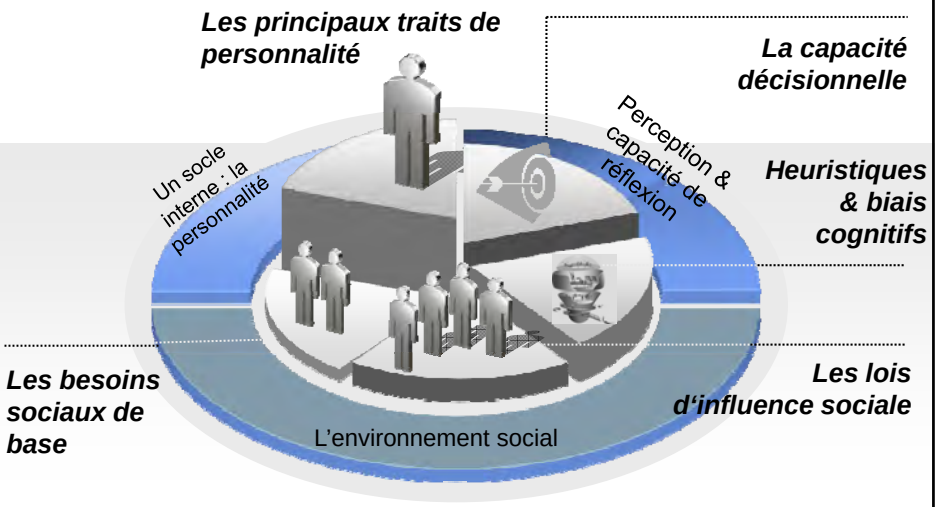
Les grandes familles de vulnérabilités …

Techniquement, ces vulnérabilités sont exploitées selon deux angles différents…

Le prédateur informationnel pourra en effet soit :

1. Exploiter une faille pour obtenir un effet (manipulation de l'individu/ création d'une action/ collecte d'information) …
2. Disposer d'outils lui permettant de mieux appréhender sa cible et donc de prendre l'ascendant…

Failles humaines & environnement…



Heuristiques & biais cognitifs

De la survie de l'homme préhistorique à

Quid de l'heuristique ?
C'est un modèle mental automatique que nous appliquons pour comprendre une situation rapidement et plus particulièrement lors de choix incertains.

Les heuristiques sont très utiles dans notre vie car ils interviennent chaque fois que nous manquons de temps et/ou d'information pour prendre une décision…
Cependant, ils peuvent être biaisés !

Heuristiques (2)

l'heuristique de disponibilité qui nous pousse à estimer une fréquence ou une probabilité en fonction de la facilité avec laquelle des exemples et/ou des associations nous viennent à l'esprit. Ainsi, lorsque nous avons un jugement à faire, ce dernier se fera en tenant compte des informations les plus facilement accessibles.

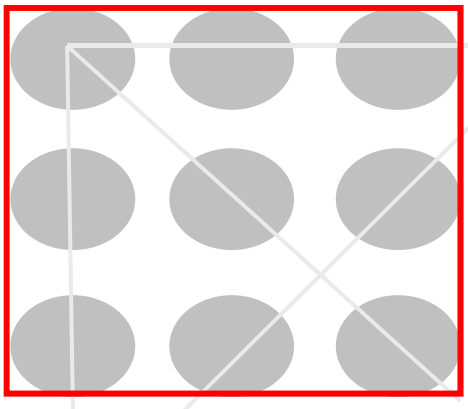
l'heuristique de représentativité qui permet par exemple à un médecin d'analyser vos symptômes en les comparant rapidement à des cas types de maladies. Nous cherchons en effet naturellement à rapprocher le cas particulier d'un cas général.

l'heuristique d'ancrage : nous avons une tendance naturelle à estimer des valeurs incertaines en les rapprochant d'une valeur délivrée antérieurement. De fait, dès qu'un chiffre a été donné, il influencera les estimations qui suivront.

Les émotions (primaires et secondaires) : qui sont des raccourcis heuristiques fondamentaux. Simple à provoquer, et facile à exploiter…

Un exemple ….

Le perturbateur : l'heuristique de disponibilité



Quelques biais cognitifs exploitables…

L'effet de primauté : nous retenons plus aisément une 1ère information que celles qui suivront (rôle de l'archicortex)

L'effet de Halo : consiste à étendre à l'intégralité d'un ensemble un jugement – positif ou négatif – qui aura été porté à son encontre à partir d'un seul élément.

Le biais de connaissance rétrospectif : consiste à projeter de nouvelles connaissances dans le passé et à se les réapproprier. Ce biais est à l'origine d'une auto-manipulation de la mémoire.

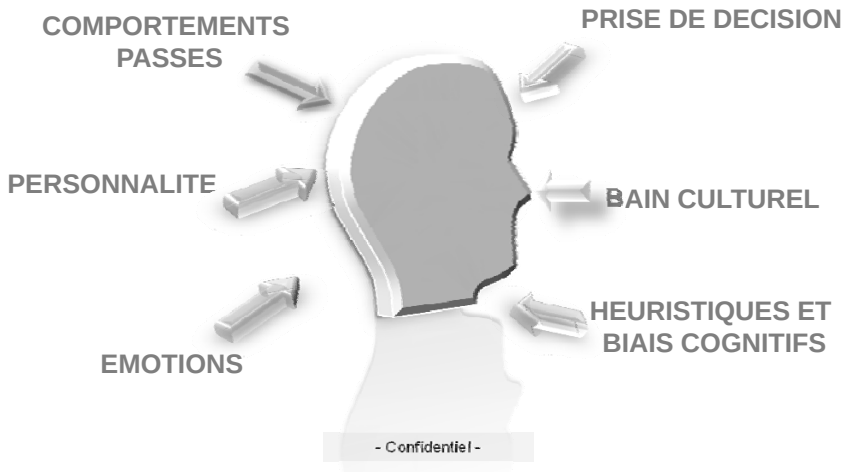
Le biais de complaisance égocentrique : nous avons une fâcheuse tendance à nous approprier nos réussites et à refuser nos échecs. En limitant notre capacité d'analyse sur les causes de nos échecs et de nos réussites, ce biais nous « aide » à réaliser de mauvaises analyses…

Les perceptions sont rapides à se former … Et difficile à changer !

La personnalité et son exploitation

Du rôle central de l'humain ….

Principaux éléments conditionnant la perception d'un individu…



- Confidentiel -

Les principaux outils …

- Les *Big Five Factors* : *considérés comme l'approche de la personnalité la plus rigoureuse et la plus pertinente*
- Le système de défense de l'Ego : ***lié à la Political Psychology … Cet outil facilite grandement la compréhension des phénomènes concernant une cible sous stress !*** *Trois composantes principales : personnalités à composante paranoiaque, narcissique, ou obsessionnel-compulsive*
- Les besoins sociaux de base : ***identifiés et traités au travers d'outils spécialisés comme le Fundamental Interpersonal Relations Orientation (FIRO-B) au travers de 3 fondamentaux:*** le besoin de reconnaissance; le besoin d'influence; le besoin pour la proximité humaine
- Les caractéristiques de la prise de décision : ***nombreuses théories, peut d'outils opérationnels. Notre choix se porte sur l'Executive Decision Making Style (EDS)*** *qui permet d'analyser 2 éléments essentiels dans la prise de décision : l'utilisation des informations disponibles et le degré de focalisation*

Page ▪ 18

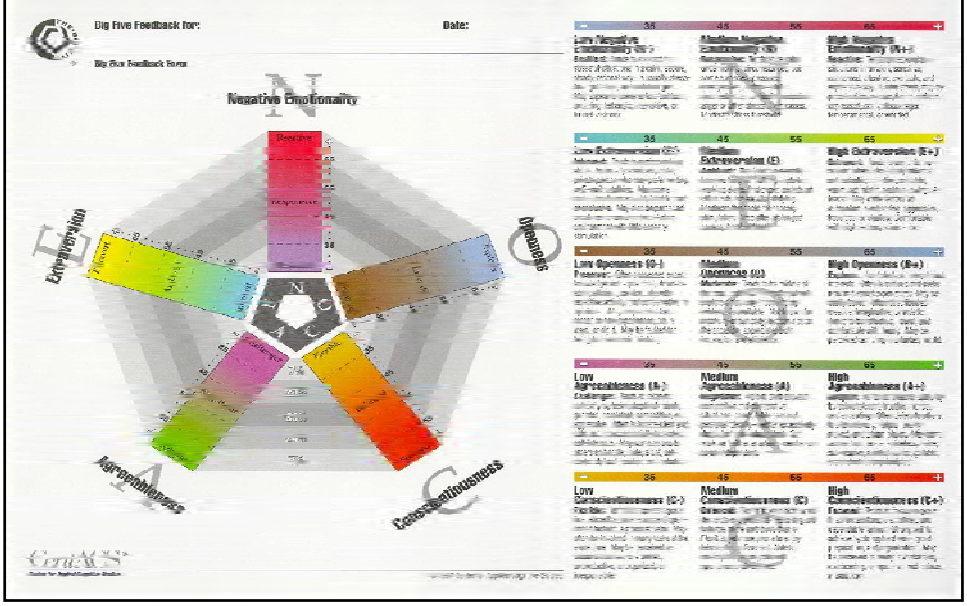
- Confidentiel -

Les *Big Fives* : le NEO-PI R

Points–clés

- Les *big fives* (5 facteurs) sont considérés comme l'approche de la personnalité la plus rigoureuse et la plus pertinente
- Plusieurs instruments ont été développés autour de cette approche: la plus réputée est le NEO-PI-R
- L'outil se compose de 5 axes déclinés chacun en 6 facettes…

Les 5 axes …



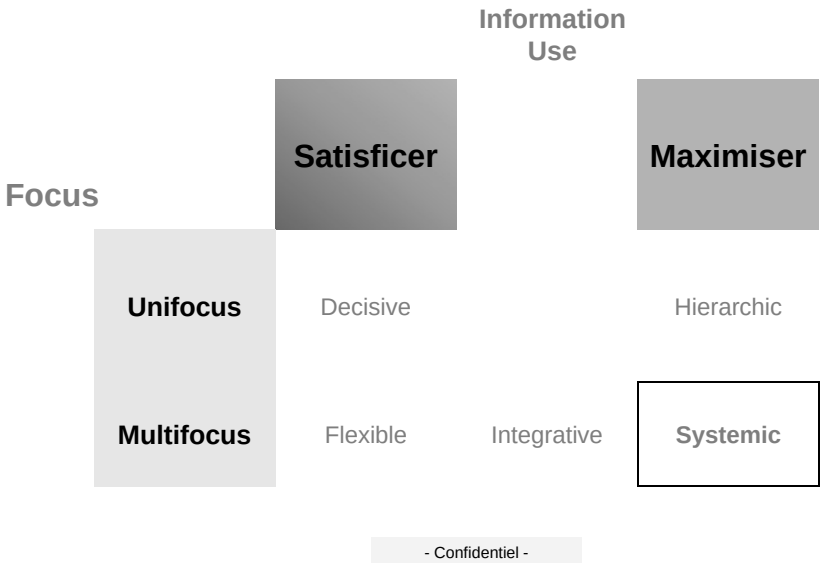
Exploiter les *Big Fives* (fortement simplifié!!!)

- Chacun des 5 grands traits possèdent des fragilités intrinsèques !
- Ces fragilités sont soit des augmentations de stress liées à la nature du trait (par ex : un introverti en situation publique/ Un extraverti « privé » d'interactions);
- Soit sont des qualités du trait « perverties » par le prédateur :
  1. Un extraverti est ainsi « exploité » en multipliant ses interactions…
  2. Un *reactive* peut être « forcé » à parler en créant un stress artificiel (ex : dans un avion avant le décollage, lui parler du nombre élevé d'accidents ces derniers mois…)

Page ▪ 22

L'Executive Decision Making Style: un exemple…

EDS : un exemple ….



Exploiter l'EDS

- L'EDS permet facilement de connaitre les flux informationnels nécessaires à un individu pour soutenir sa prise de décision !
- L'objectif du prédateur est de BLOQUER la capacité décisionnelle normale en faveur d'un glissement vers le mode heuristique !!
- Pour augmenter le stress de la décision, deux grandes méthodes cohabitent :
  1. Supprimer l'accès à l'information (*satisficier* par ex.);
  2. Surcharger l'individu (maximiser par ex.)

Les "boutons universels"

Universelles, ces failles sont aisées à mettre en oeuvre par le prédateur ! Ces "boutons" semblent évident ! Et tout le monde est persuadé de ne pas "tomber dans un piège aussi grossier" … POURTANT, régulièrement, nous voyons des individus se "faire avoir" par ces boutons ! Dans des proportions considérables (+ de 70% des cas)…

STRATECO

Les caractéristiques humaines …

- Le désir ou le besoin de reconnaissance.
- Une tendance naturelle à l'effacement.
- Une tendance naturelle à corriger les autres.
- Une tendance naturelle à vouloir prouver que l'autre à tort.
- L'absence d'«oreille» dans notre monde.
- Une tendance naturelle à parler de sujets qui ne nous concernent pas directement.
- Une tendance à ne pas évaluer correctement la valeur de l'info.
- Une volonté d'être reconnu comme expert dans son domaine.
- Des travers professionnels qui dérivent d'occupations secondaires (mentors, formation).
- Une tendance aux indiscrétions en cas de tension émotionnelle.

Les principales lois d'influence

Universelles, simples à mettre en oeuvre, les principales lois d'influence font partie de la panoplie des outils, régulièrement utilisée par le prédateur pour obtenir un effet sur la cible …

L'autorité : célèbre depuis l'expérience de Milgram… le principe d'autorité reste à ce jour l'un des plus simples à mettre en œuvre ! Prenons un exemple : quand avez-vous la dernière fois remis en cause le jugement de votre médecin lorsqu'il vous a prescrit un médicament?

Le recadrage ou *framing* : fondé entre autres approches sur les travaux de Kahneman et Tversky. Il s'agit d'une des techniques les plus versatiles ! Ses variantes sont multiples (positifs ou négatifs, de positionnement, par contraste, par attribution, etc.). L'approche la plus fréquente dans les tests de failles informationnelles, consiste à exploiter un cadre gains/pertes. En effet, il apparaît que la forme du message (*framing*) permet d'obtenir plus facilement l'adhésion d'un individu.

La dissonance cognitive : théorisée en 1957 (Festinger), cette loi repose sur un principe simple : les individus agissent de façon conforme à leurs valeurs/croyances et sont mal à l'aise lorsqu'ils sont en dissonance. En cas de dissonance, les individus adaptent leurs comportements futurs pour les supprimer ! Différentes approches de réduction de la dissonance sont utilisés : refus/rationalisation/séparation/modification du cadre de référence.

Réciprocité et obligation sociale : comme le dit un proverbe japonais : « rien n'est plus coûteux que quelque chose donné gratuitement…»! La théorie s'appuie sur le principe de réciprocité entrainant un besoin de retourner la faveur… C'est la loi la plus simple à mobiliser ! Les grandes approches sont : l'échange de secrets/ les concessions réciproques/ les « cadeaux » en phase initiale.

La validation sociale : de l'appartenance à un groupe, au besoin d'être accepté, en passant par l'effet d'apathie.

L'effet de rareté : pensez à Parmentier et à Catherine II lorsqu'ils imposèrent les pommes de terre : le « bulbe du diable » étant refusé par les paysans, ces deux individus ont décrété que la pomme de terre était un légume royal interdit au peuple (puni d'une peine d'emprisonnement en Russie) tout en disposant des gardes armés autour des champs. En quelques semaines, les vols ont débuté, et la pomme de terre s'est imposée. Il est facile d'obtenir une action à partir de ce principe. Techniquement, il s'appuie sur des deadlines, une perte potentielle, réduire la liberté d'action.

L'usage du contraste : fondé entre autres éléments sur les réactions quasi-automatiques de l'archicortex, cette loi est simple à mettre en œuvre ! La technique la plus connue s'appuyant sur ce principe est « la porte au nez ». Sans rentrer dans le détail de cette dernière, il s'agit grosso modo de commencer par exposer l'individu à une requête trop « coûteuse » (argent, temps, implication, etc.) afin d'obtenir un refus. Puis dans un second temps d'exposer la véritable requête. Le premier refus permettant généralement d'obtenir satisfaction sur la seconde requête qui parait tout à la fois plus raisonnable en terme de « coût » (logique du contraste) et qui permet à l'individu qui a refusé quasiment par réflexe la première requête de proposer une alternative (contraste appliqué à la dissonance cognitive).

La loi d'expectation : de l'art du placebo, de l'étiquetage, et de l'ancrage. Qui tous reposent sur une expectation d'un résultat/état par un individu ! Ainsi, l'étiquetage consiste à créditer un individu d'une valeur donnée. Testez par exemple les deux derniers outils en :

> *Expliquant à un enfant qu'il est particulièrement doué en mathématiques et qu'il dispose d'un esprit logique… Avant de lui demander de réaliser des équations qu'il réalise en général plus facilement.*
> *Ou dites lui que vous n'avez jamais rien compris aux dites mathématiques quand vous étiez jeune et que cela doit-être de famille (approche par ancrage négatif) et obtenez un résultat totalement inverse.*

Les grandes failles universelles…

Il s'agit des failles typiques exploitées par les SR et les spookes… Simples, faciles à mettre en oeuvre ! ET disposant d'un pouvoir coercitif non négligeable !

Les principaux acronymes liés à la manipulation de sources

MICE

- *Money ; Ideology ; Coercion; Ego*
- *Ces quatre failles sont considérées comme les plus exploitables.*

ASIE

- *Argent, Sexe, Intellect, Ego*
- *Acronyme plus tactique récapitulant les grandes failles facilitant l'empiégage. L'acronyme intègre le sexe, une des grandes failles humaines (coercitif ou acte volontaire).*

SANSOUCIS

- *Solitude, Argent, Nouveautés, Sexe, Orgueil, Utilité, Contrainte, Idéologie, Suffisance*
- *Plus nuancé, ce dernier acronyme intègre des variables liés au fonctionnement de l'esprit humain…*

Quelques exemples de stéréotypes à risques…

La personne immature : cible facile pour un professionnel. Risque augmenté lorsque l'immaturité se combine au besoin « d'appartenir à ceux qui savent »

Le « héros » : ou plus précisément le « héros révélé » qui se voit offrir de changer la société alors que jusqu'alors sa vie était terne et banale…

L'amateur d'intrigue : attiré dans ce monde par son seul goût naturel…

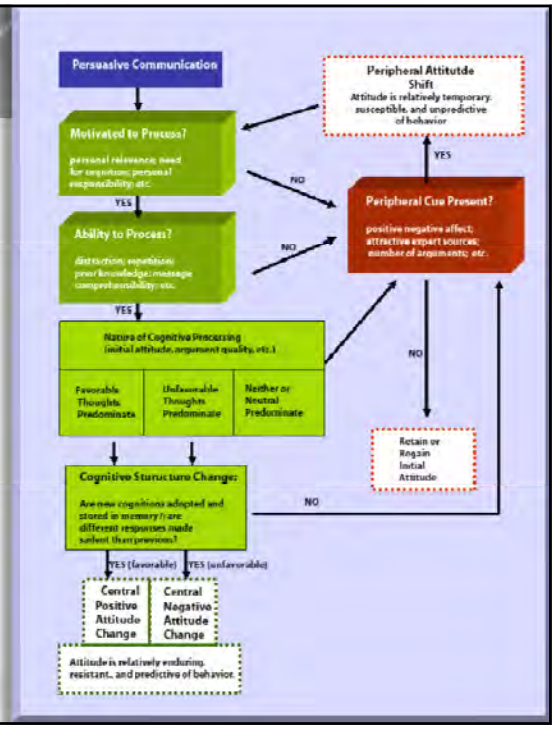
L'insatisfait : qui n'accepte pas de vivre une vie médiocre ! D'où une recherche perpétuelle de sensation capable de flatter son ego. Au-delà des produits, nos entreprises actuelles « fabriquent » des masses d'insatisfaits d'autant plus fragiles en période difficile (réduction de personnels, etc.)…

Le solitaire : dans une société de communicants, les personnes souffrant de solitude se retrouve marginalisées dans les sociogrammes. Ils sont une proie facile! Les SR soviétiques avaient ainsi monté une opération dédiée (Myosotis) auprès d'occidentaux … Les arnaqueurs russes font de même aujourd'hui avec les sites de rencontres !

L'intellectuel : qui de part son intelligence, a un besoin permanent d'évoluer. Si cette évolution est limitée et/ou lente : il ressent une frustration. Cette frustration se reporte généralement sur l'environnement (pays, société, famille, etc.)

Heuristique/systémique : le coeur des actions *one-shot* !

L'*Elaboration Likelihood Model …*



Page ▪ 35

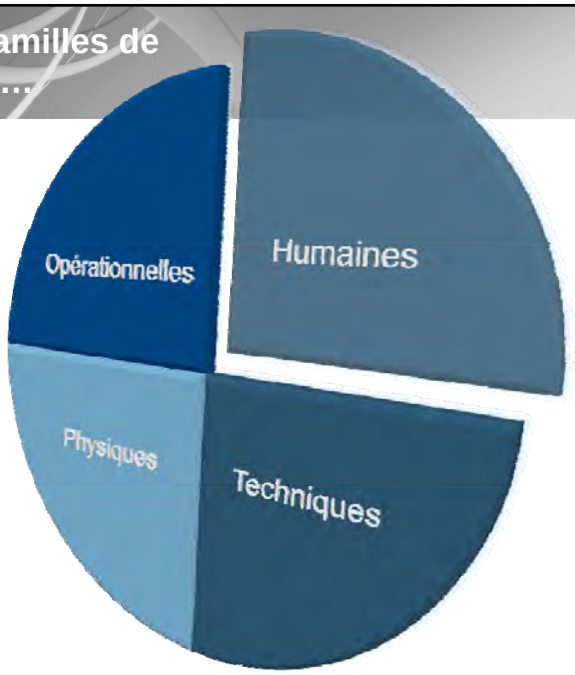
De la notion de vulnérabilité d'une entreprise

Présentation succincte des principales vulnérabilités..

STRATECO

4

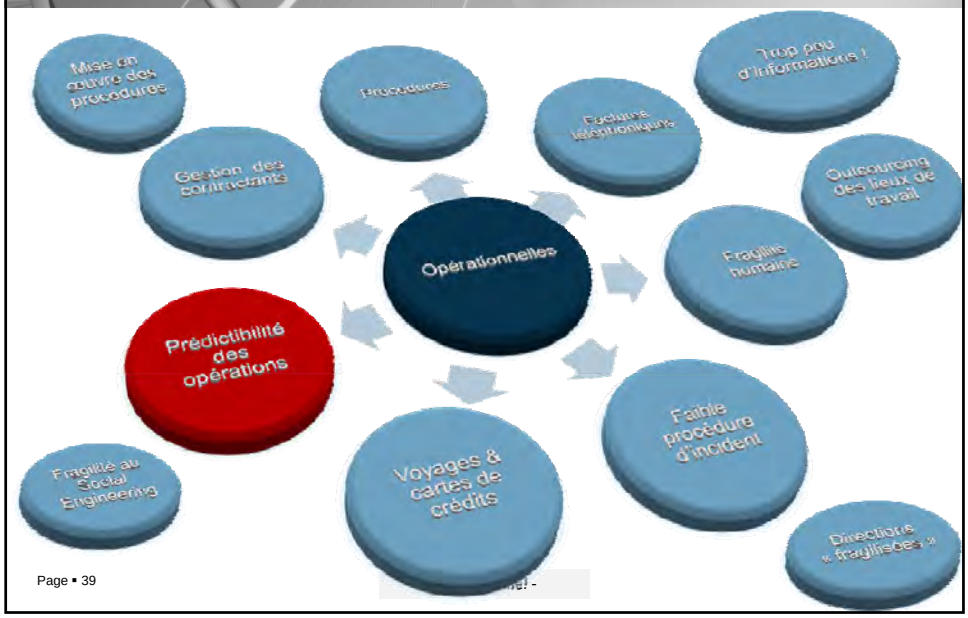
Les grandes familles de vulnérabilités …



Page ▪ 38

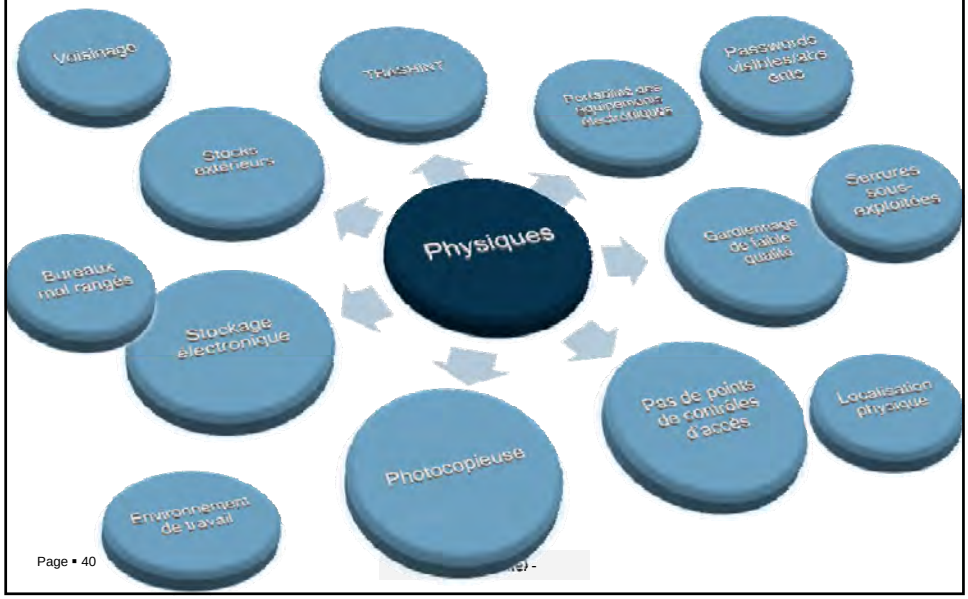
- Confidentiel -

Les vulnérabilités opérationnelles correspondent à des failles provenant des opérations habituelles des entités et/ou personnes



Page ▪ 39

Les vulnérabilités physiques : « facilitateurs » des autres approches, et exploitables quelque soit la taille…



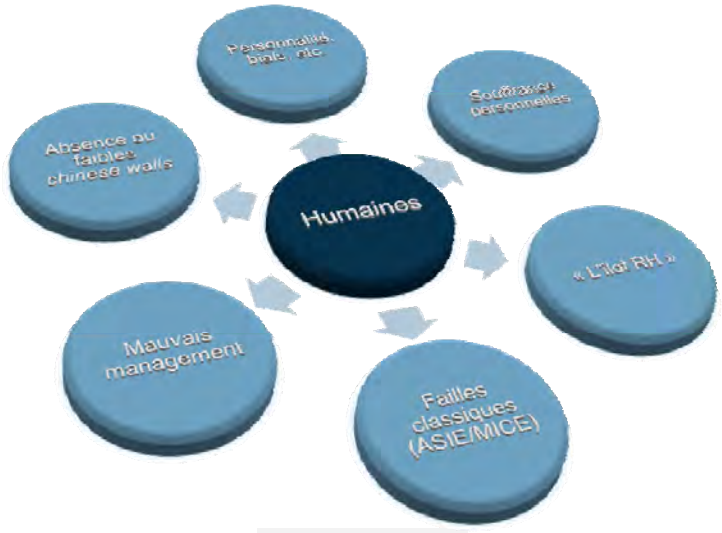
Page ▪ 40

Vulnérabilités techniques : surestimées pour l'informatique ! (20% max des pertes informationnelles en « solo ») … Et le rare « génie » !

Page ▪ 41

- Confidentiel -

Les vulnérabilités humaines sont de loin les plus efficaces à exploiter ! Universelles, renforçant toutes les autres…



Page ▪ 42

- Confidentiel -

Un exemple de prédateur qui a « le vent en poupe » la criminalité organisée & les entreprises…

- Les menaces contre l'entreprise : par exemple les différentes formes de chantages (ex : EMP dans les milieux financiers), etc.
- Les problématiques de blanchiment : la fausse sous-traitance, les faux contrats, les bureaux d'études bidons, etc.
- Les menaces contre les personnes : chantages (ex: aux emails en UK), menaces (ex: passeport en Allemagne), exploitation massive de failles (Myosotis), etc.
- Le « vol organisé » : les équipes de doublettes aux aéroports, les rats d'hôtels spécialisés dans le vol de portable et la revente des informations, etc.

Des prédateurs “one-shot”

Présentation succincte des principales approches..

11

Les principales catégories de prédateurs « one-shot »

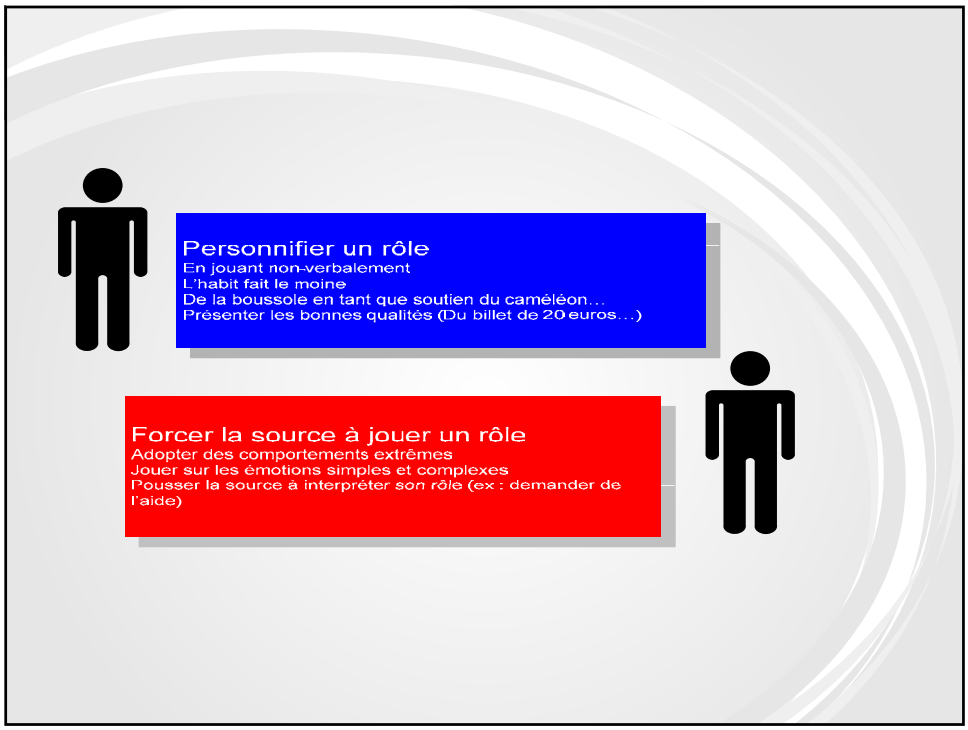
- **Le *social engineer*…** Intuitif, mais peu formé ! Méthodologie (quand elle existe!) reposant sur très peu de principes efficients contrairement à la légende qui entoure ses exploits…
- **Le « *con artist* »…** Généralement très bien formé! Un cœur méthodo tournant autour des failles les plus simples (argent/sexe/ego) rigoureusement documentées !
- **L’opérateur IE/*Competitive Intelligence :*** allant de peu formé à parfaitement opérationnel ! D’éthique à quasiment illégal… Généralement, plus l’opérateur respecte l’éthique, plus il dispose d’une technicité importante…
- **Certains journalistes** (paparazzi, investigation)…Qui agissent souvent comme les autres prédateurs « one-shot » !

Page ▪ 46

- Confidentiel -

Les grands principes !

- Choisir le point le plus fragile !
- Agressivité et rapidité : les deux maitres mots du one-shooter
- Le cœur méthodologique : élicitation/Social engineering, lois d'influences sociales, maitrise des « points d'eau »
- De l'importance des rôles dans le « one-shot »



La méthodologie de *screening* simplifiée*

La sélection des cibles …

La recherche secondaire : **cette recherche permet d'identifier des sources potentielles, de détecter leurs goûts, de les «profiler », et de connaître leurs points d'eau…**

La « surface utile » : **dans le même temps, l'opérateur va détecter au sein de l'entreprise cible les canaux et flux de communication. Il va se servir de ces derniers pour identifier la «surface utile » sur laquelle il va concentrer ses efforts. Ensuite, l'opérateur utilisera différents outils (dont des sociogrammes) pour connecter cette « surface utile » aux *Who's Who* réalisés précédemment…**

- Confidentiel -

La sélection des cibles …(2)

L'analyse des risques : **en fonction du degré d'illégalité de son action, l'opérateur va ensuite appliquer une matrice d'analyse de risques pour identifier les « points d'entrée » les plus sûrs pour ses actions d'élicitation…**

La matrice de sélection des sources : **l'opérateur déterminera ensuite un panel de sources potentielles pour obtenir les informations dont il a besoin… Pour mettre en adéquation ses collecteurs/relais avec les sources, il s'appuiera sur des matrices. Ces dernières analysent par exemple le degré de proximité de l'individu avec la cible et avec le collecteur…**

- Confidentiel -

L'élicitation & le *social engineering*

Remarque : ***malgré sa réputation, le Social engineering est une « pâle copie » des approches d'élicitation (ou autres) développées par les services spécialisés. Notre propre travail de screening n'a fait apparaitre que des individus certes doués mais dépourvus de méthodologie rigoureuse…***

De fait, nous nous focaliserons essentiellement sur l'élicitation dans les slides suivantes.

Rappelons néanmoins que malgré sa faiblesse méthodologique, de nombreuses opérations de SE « passent » sous les radars des entreprises ! Imaginez simplement ce qu'un opérateur spécialisé pourrait réaliser dans un cas de figure identique !

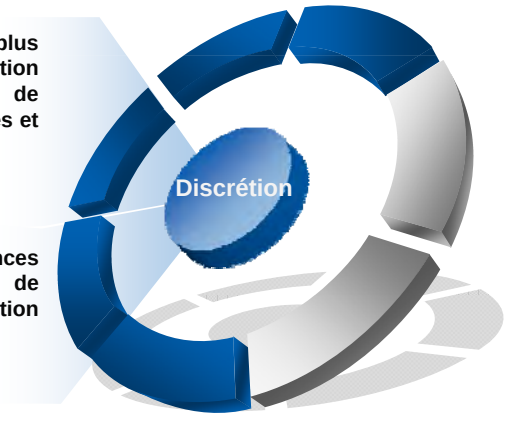
Eliciter **:** obtenir l'information d'une personne, qui a – ou n'a pas admis - avoir cette information, et qui ne connaît pas la motivation et les objectifs du collecteur. L'interaction n'est jamais agressive. La motivation de la source repose sur les techniques, la flexibilité et l'astuce du collecteur.

Points-clés de l'élicitation...

Fondamentalement, l'élicitation n'est efficace que si :

L'élicitation recherche le ratio le plus efficient entre efficacité et adaptation ! Son objectif est clairement de "passer sous le radar" des sources et des observateurs éventuels ...

L'opérateur intégre les différences entre le processus volontaire de l'élicitation et une conversation informelle classique !



L'élicitation : action légale ou illégale.. ?

...Les deux car l'outil est utilisé par un vaste panel d'opérateurs dont certains naviguent en pleine illégalité...

Le cadre d'utilisation…

Le renseignement : **l'élicitation est l'outil principal lors des phases de *spotting* et d'évaluation des sources (ex: l'échelle 1000-100-10-1 du GRU)**

L'accès à l'information : **l'élicitation en combinaison avec des prétextes/légendes permet d'obtenir un accès illégal à des sources d'informations confidentielles (ex: le *social engineering*)**

La collecte d'information en face-à-face : **l'élicitation est une des techniques les plus employées par les professionnels étant donné son ratio efficacité/discrétion (ex: la collecte lors d'une conférence)**

Les principales techniques

Les approches de maintien du flux conversationnel : une vingtaine de techniques permettent de maintenir le flux conversationnel actif. Un exemple connu est l'approche par répétition de mots…

Les amplificateurs émotionnels : un cœur d'une dizaine de techniques a été défini pour amplifier le flux conversationnel d'une source sous le coup d'une émotion. L'exemple de la colère est symptomatique de ces approches…

Les approches par opposition : une dizaine de techniques exploitent les réactions découlant d'une opposition à un point de vue défendu par la source. Les approches vont de la critique modérée à l'opposition franche…

Les principales techniques

Les techniques liées à l'Ego : une dizaine de techniques exploite les fragilités égotiques des sources. Un exemple typique est le recours à la flatterie…

Les techniques adaptées à des traits de personnalités : un corps d'une vingtaine de techniques est adapté aux caractéristiques personnelles de la source. Un exemple : le silence utilisé avec des extravertis

La technique « reine » de l'élicitation : le sablier …

Questions

Test des caractéristiques

Techniques d'Elicitation

Questions

Quelques exemples de "*one-shot*"*

*tirés de cas réels mais évidemment démarqués…

Reconstituer un organigramme … Quelques approches « *one-shot* » !

- ***Appels systématiques de nuit sur les boites vocales des employés … Et reconstitution des services par proximité des terminaisons !***
- ***Observer les restaurants dans les zones industrielles : obtenir les CV par élicitation et/ou récupération dans les paniers « free meal »***
- ***Personnifier un rôle de consultant auprès d'une standardiste (devenu meilleure nouvelle amie) et accéder à l'annuaire interne …***
- ***Passer des annonces de recrutement avec des postes spécialisés : analyser les réponses (IP, zone géographique, etc.)…***

Reconstituer les déplacements d'un cadre… Quelques approches en « *one-shot* »!

- ***Prétexte de sondage auprès de la famille : collecte des destinations …***
- ***Collecte de la banque sur un salon. Recrutement et exploitation d'un agent d'accès dans la banque pour avoir la copie des relevés CB…***
- ***Vérification dans la BdD SABRE du nom de l'individu via un agent d'accès recruté en agence de voyage…***
- ***Via un agent d'accès et/ou SE (code en 4 chiffres), récupération des miles sur les programmes de fidélisation du cadre !***
- ***En grande vogue actuellement : placement d'une prostituée lors d'un déplacement à l'étranger. L'agent d'accès valide l'inscription du portable du cadre sur un service de localisation permanent durant la nuit ! …***

De l'art de récupérer des informations financières … Quelques approches « *one-shot* »

- ***Connaitre la banque par élicitation, et disposer d'un agent d'accès pour les relevés CB … Et les soldes du CC***
- ***Proposer à la source directement ou via un tiers, un montage de réduction d'impôts ! Puis collecter les éléments nécessaires…***
- ***« Lire » les adresses d'expéditeur, ainsi que le courrier par dépôt de gaz inerte… Éliciter les amis et connaissances !***
- ***Analyser le parking de l'entreprise pour identifier les véhicules (anciens ou trop coûteux)..***
- ***Analyser le mode paiement de l'individu (CB ou cash – petites ou grandes coupures)… Suivre l'individu lorsqu'il achète ses courses (analyse du mode de paiement)***
- ***Etc… Etc.***

Page • 65

- Confidentiel -

Des prédateurs “long-terme”

Plus redoutables… Heureusement moins présents … Mais en forte recrudescence !

12

Les principales catégories de prédateurs « long terme »

- **L’insider …!** Souvent oublié et pourtant : il sait ce qui peut vous faire mal …Et surtout il maitrise le « comment » de l’accès à l’information !
- **Le « *spooke* »,** spécialiste du renseignement industriel … généralement très bien formé et financé, il sait comment *spotter* des sources et les recruter sur leurs failles ! Il est d’autant plus dangereux que ces motivations sont liées à celles de vos concurrents : vous « sortir » du marché ! De plus en plus présent !
- **L’opérateur des SR :** le mieux formé! Le plus efficace ! Sa dangerosité est atténuée par le fait qu’il ne cherche pas à « vous sortir du jeu concurrentiel » mais accéder à de l’information sensible .. Le cas est rare mais en forte progression !

Les grands principes !

- **NE PAS SE FAIRE PRENDRE !**
- Patience et créativité : les deux maitres mots du prédateur informationnel !
- Le cœur méthodologique : élicitation, surveillance, observation, OPSEC, méthodologie de recrutement…
- De l'importance du recrutement sur les failles humaines dans le « long terme »

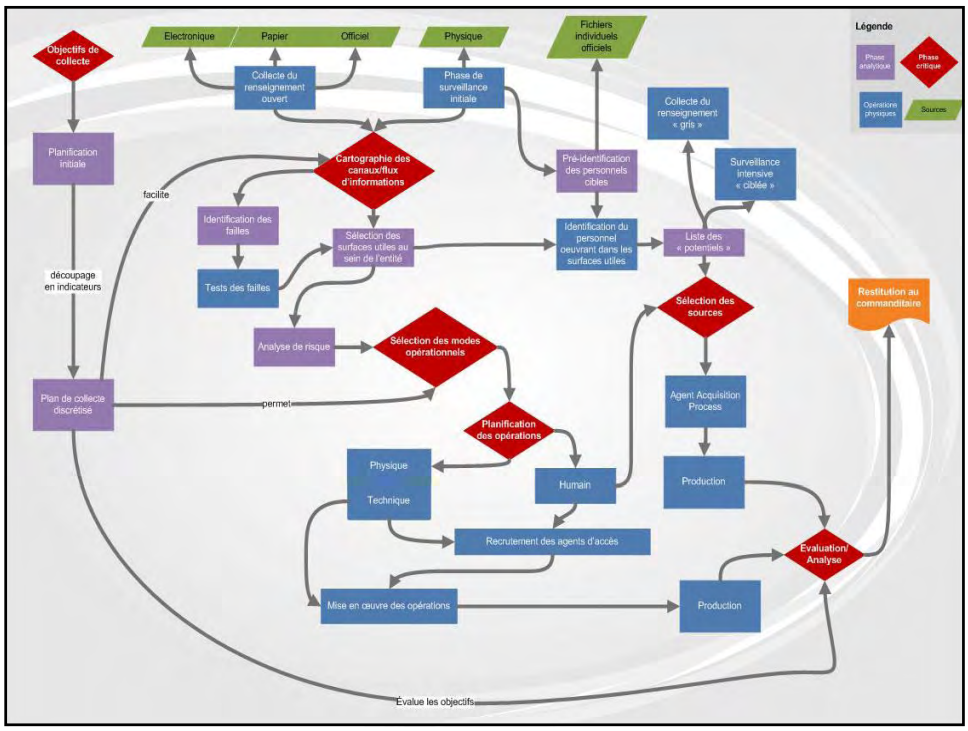
Les menaces liées au renseignement industriel…

Quelques constats..!

- Le renseignement industriel est très largement sous-estimé !
- Si peu de *blackbag operations* et tant de « désensibilisation » des sources ….
- Une TRES GRANDE professionnalisation des opérateurs ! (un exemple : les opérateurs ex-bloc de l'Est)
- Une règle : l'information n'est pas dépendante de sa forme ! (un exemple : password sur un post-it, éliciter, compromission de communication > résultat identique !)

Un exemple de méthodologie des prédateurs “long terme”

* Méthodologie propriétaire STRATECO@2007



*L'Agent Acquisition Process**

* et/ou l'Asset Acquisition Process…

Le cycle du recrutement …. Ou le *Agent acquisition process* en vigueur dans les SR US

Page ▪ 76

- Confidentiel -

Quelques exemples !

Les cas célèbres (au grand dam des opérateurs!)

- La pénétration de la société Erickson par les SR russes… Une seule source, des sous-agents ! Résultats : l'équivalent informatique de 20 « 33T de papier »
- Le cas GM-Volkswagen avec le recrutement de l'équipe des achats de GM..
- La mission de Diligence qui a recruté une source au sein de KPMG pour obtenir des copies des rapports d'audit de ce *Big Four* sur un groupe audité. Cas tout récent de « faux drapeau » pour le recrutement !

Un service de R&D dans une PME… Ou l'argent est au centre de la manipulation !

- 1-Collecte de l'organigramme par social engineering (multiples méthodes) et identification des cadres clés sur les projets intéressants le client du *spooke*.
- 2-Une shell-company fait passer une annonce de recrutement dans un journal spécialisé. L'annonce correspond précisément aux caractéristiques des cadres identifiés. Réception des CV des ingénieurs intéressés.
- 3-Relance des ingénieurs n'ayant pas réagit par une « chasseuse de tête » du faux cabinet.
- 4-Une salle est louée dans un Regus pour la semaine, les ingénieurs sont convoqués. Les entretiens permettent d'éliciter les informations nécessaires sur les projets intéressants le client, ils ont également filmés discrètement.
- 5-Une offre financière « optimale » est proposée aux cadres les plus intéressants et les plus fragiles. Plusieurs débriefings sont réalisés sur les cibles les plus fragiles.
- 6-L'offre est annulée au bout de quelques temps, car le poste est dans une société qui travaille sur un rachat de l'entreprise cible et que c'est incompatible avec les normes éthiques de recruter sur cette société. Certains ingénieurs sont heureux déjà de ne pas avoir été « dénoncés» à leur direction !
- 7-Pour les plus fragiles, il leur est proposé d'aider le futur acheteur en donnant des informations sensibles en échange d'un contrat de consulting !

Un simple exemple qui passe sous le radar … De l'art de renouveler les PC d'une PME… !

- **Par élicitation ou SE, le *spooke* identifie le nom de la société en charge de la gestion des ordinateurs auprès de la société cible.**
- **Cette société est située dans une zone industrielle. Il recrute ensuite au sein de la société de gestion une source en proposant de l'argent sous un prétexte quelconque.**
- **L'agent installe sur tous les PC, un dispositif technique ou physique.**
- **Les PC sont livrés au fil du temps. La collecte d'information est lancée. Le *spooke* peut en plus recruté des jeunes casseurs pour forcer les bureaux et voler les PC non infectés… Afin d'accélérer la procédure de renouvellement des PC !**

Le bonheur des grandes conférences dans les hôtels…

- **Saviez-vous que chaque conférencier est *buggé* ? .. Un simple scanner œuvrant dans les 300Mhz permet de se fixer sur les micro cravates de ces derniers ! Permettant ainsi de disposer des conférences, des discussions avant et après les interventions …**
- **Un *spooke* utilise les toilettes des conférences en y disposant un « préparateur » qui distribue des serviettes en papier aux représentants des sociétés …**
- **Un autre exploite les petits déjeuners en y plaçant un jeune opérateur sur les tables les plus grandes .. Qui ne fait qu'écouter tout en ne « comprenant pas » la langue !**
- **La chance souris aux *spookes* qui fume et retrouve leurs camarades dans les espaces fumeurs ! Souvent aussi, la seule présence du fumeur permet de rentrer dans des zones normalement fermées au public !**
- **Quelles sont les chances de voir un « compatriote » qui vous a abordé au bar de l'hôtel, de refuser de vous suivre pour un verre dans un endroit sympathique ? .. Évidemment, la source est le fameux compatriote qui vous a entendu parler sa langue !**

Ne croyez pas que ces collectes soient anodines !

- **Un détective privé US est recruté en Californie sous un faux prétexte (contrefaçons). Il équipe les camions du logisticien de la société cible de transpondeur GPS pour suivre les déplacements de ces derniers. Les stop des camions correspondent aux déchargements. Par recoupement, la liste des clients est identifiés. (illégal dans beaucoup de pays, autorisé en Californie)**
- **Dans le cadre d'un réseau social d'un commercial, ce dernier se voit offrir a des prix défiant toute concurrence des téléphones portables dernière génération sous Symbian. Il en prends pour lui, et en revend à d'autres collègues et amis avec une marge confortable (A et E de ASIE)… Les tél sont équipés d'un troyen….**
- **Une opération de désinformation qui a désorganisé une filiale d'un grand cabinet de conseil :**
  - Collecte par élicitation des numéros de tél portable des associés/seniors/juniors et des habitudes de communication de ces derniers.
  - Sélection des individus utilisant les SMS.
  - Faux SMS envoyés aux différentes personnes en changeant des lieux de réunions, des dates, des ordres, en mettant des messages personnels (liaison, personne se détestant, licenciement, démission), etc.


STRATECO


Se défendre !
Présentation succincte des principales approches défensives..
STRATECO
8

Les grands principes !

- Faire des *pen tests* sans les failles humaines est l'équivalent de se préparer au combat de rue avec une pratique interdisant les « coups pourris » et n'autorisant pas le contact !
- Le cadre éthique et opérationnel doit encore être plus strict que pour les *pen tests* informatiques si les failles humaines sont testées (ne serait ce que dans l'anonymat des employés qui sont volontairement « poussés à la faute !!) !
- Comme dans le domaine informatique, la protection des failles humaines doit s'appuyer sur une défense en profondeur avec de multiples couches de protection !!!...
- Il est relativement aisé de compliquer la tâche des prédateurs avec une série de mesures peu coûteuses !

Auditer les failles humaines !

Objectif n°1 : imiter le comportement de prédateurs!

Objectif n°2 : trouver de la « matière » pour réaliser des programmes de sensibilisation réalistes ! ET tester les contremesures actuelles

Objectif n°3 : réaliser des *pen tests* complets « sans gants » … Mais en respectant évidemment l'intégrité de la société cible !

Modus operandi : soit créer des actions typiques des prédateurs (téléphone, accès aux zones sécurisées, TRASHINT, etc.), soit se focaliser sur un objectif précis (accès àà une salle donnée, agenda du dirigeant, etc.).

La méthodologie repose systématiquement sur des scénarii et suis une courbe progressive de plus en plus « visible » pour tester les sécurités en place !

Exemple d'audit de failles humaines

- **Imiter le comportement d'un SE lors d'un *pen test* informatique ;**
- **Accéder physiquement au site de l'entreprise en dehors des horaires de travail;**
- **Simuler une action coordonnée physique/technique/humaine pour pénétrer un site**
- **Rechercher une catégorie spécifique de données (un projet sensible, cadres dirigeants par ex.) en exploitant les failles humaines**
- **Simuler le comportement d'un *insider***
- **Tester les employés contractants « *in situ* »**
- **Mettre en place une procédure d'observation sur un site industriel puis analyser les données afin d'appréhender la phase 1 d'une pénétration sous « l'angle du braconnier et non du garde-chasse »;**
- **Etc.**

Quelques contre-mesures en vrac !*

* Les CM techniques ne sont pas présentées. Les personnes présentes en connaissent nettement plus sur l'informatique que l'auteur et les autres CM techniques nécessitent des experts de ces sujets et sont plus rares dans la majorité des entreprises !

Quelques contre-mesures opérationnelles

Le point le plus important : programmes de sensibilisation réguliers !

- **Classification de l'information avec protection systématique des informations jugées sensibles après l'audit de vulnérabilité**
- **Catégorisation des employés et des « in situ » en fonction des besoins d'accès à l'information**
- **Système de détection des incidents : ex: ligne télé et/ou remontée par email**
- **Politique de « récompenses » : pécuniaires et/ou de reconnaissance par le management**
- **Politique de sécurité informationnelle en particulier par téléphone :**
  - Vérification de l'identité du correspondant
  - Vérification de son accès à l'information
  - Vérification par call-back
- **Suppression des logo, noms sur les badges d'accès**
- **Politique de protection lors des déplacements à l'étranger (portable/personnel/chambre/etc.)**

CM Ops 2 :

- **Politique de validation des documents quittant la société (PR, conférences,, etc.)**
- **Politique stricte liée à la classification des services ventes et marketing**
- **Pour les informations électroniques :**
  - minimiser le stockage sur les postes via une politique de check régulier
  - Disposer de DD en rack pour les informations sensibles (avec mises sous clé)
  - Exploiter les logs
- **Disposer de lignes téléphoniques non rattachées à la société pour les dossiers sensibles. Idem pour les moyens de paiement**
- **Modifier son comportement lors du traitement de sujets sensibles (limiter l'approche par analyse de patterns)**
- **Réaliser des *pen tests* complets régulièrement**
- **Réaliser des *background checks* des employés**
- **Coordonner les départements RH, IT et sécurité en particulier lors de la fin d'un contrat de travail !**

Contre-mesures physiques

- **Mettre sous clé les informations sensibles (salles, DD en rack, etc.)**
- **Mettre en place ET exploiter des serrures sur les bureaux !!**
- **Installer des logiciels de protection des écrans de veille**
- **Mise en place d'une politique de clean desk !**
- **Fixer les PC sur sites (câbles ou autres)**
- **Mettre en place des contrôles sur les copieurs/imprimantes en réseaux**
- **Disposer des *shredders* dans l'ensemble de la société**
- **Verrouiller les poubelles (TRASHINT). Audit régulier**
- **Si possible, exploiter des badges d'accès et des portes électroniques avec des zones d'accès délimitées en fonction des employés**
- **Disposer de gardes de sécurité réellement formés !!**
- **Couvrir lors des patrouilles de ces gardes, les zones extérieures au site avec procédure de remontée d'incident (camionnette, présence fréquente du même véhicule, etc.) …**


“Une personne normale voit sans regarder, écoute sans entendre, touche sans ressentir, mange sans goûter… Et parle sans réfléchir..”*
* Leonardo da Vinci
Merci de votre attention !
STRATECO