



OSSIR – 07/07/2003



Exemple de scénario catastrophe technologique

Mise en péril d'une entreprise



Patrick CHAMBET
EdelWeb

patrick.chambet@edelweb.fr

<http://www.edelweb.fr>

<http://www.chambet.com>

- **Objectifs**
- **Généralités**
 - Les différents risques informatiques
 - Les risques logiques
- **Scénario catastrophe**
 - Présentation du scénario
 - Les différentes étapes du scénario
- **Recommandations**
 - Mesures préventives
 - Détection, réaction
- **Conclusion**



Objectifs



- **Différencier les attaques logiques des autres risques informatiques**
- **Décrire un exemple de scénario catastrophe dans une grande entreprise**
- **Effectuer une analyse technique et organisationnelle à chaque étape du scénario**
- **Présenter des recommandations permettant de contrer certaines étapes du scénario**
- **Conclure sur la probabilité d'un tel scénario**



- Objectifs
- ✓ • Généralités
 - Les différents risques informatiques
 - Les risques logiques
- Scénario catastrophe
 - Présentation du scénario
 - Les différentes étapes du scénario
- Recommandations
 - Mesures préventives
 - Détection, réaction
- Conclusion



- **Les différents risques informatiques**
 - **Désastres naturels (feu, inondation, cyclone, tremblement de terre)**
 - **Catastrophes humaines (manifestations, pillage)**
 - **Coupures de courant**
 - **Dysfonctionnements physiques**
 - Disques, ventilateurs, ...
 - **Dysfonctionnements logiques**

- **Ajout récent: terrorisme**
 - **Enseignements du 11 septembre 2001**

Généralités (2/3)



- **Les risques logiques**
 - Erreurs de manipulation / d'exploitation
 - Bugs logiciels
 - Mauvaise configuration du réseau et/ou des applications
 - Attaques logiques délibérées
- Nous nous intéresserons ici uniquement aux attaques délibérées
- Nous laisserons de côté la « guerre de l'information » au sens large (par, pour, contre l'information)

- **Le but des attaques logiques**
 - **Délit crapuleux**
 - Profit financier immédiat
 - **Vengeance**
 - Suite à des plans sociaux, des mesures disciplinaires
 - **Activisme / « hacktivism »**
 - Entreprises liées à l'environnement, à l'énergie, ...
 - **Concurrence économique**
 - Dévalorisation de l'image de marque d'un concurrent
 - Récupération de secrets de fabrication
 - **Renseignement**
 - Entreprises et organisations du domaine de la Défense
 - **Terrorisme**
 - Déstabilisation d'une population, d'un état
 - Attentat et attaque informatique combinés
 - **Cyber-guerre**
 - Destruction de l'économie d'un pays

- Objectifs
- Généralités
 - Les différents risques informatiques
 - Les risques logiques
- ✓ • Scénario catastrophe
 - Présentation du scénario
 - Les différentes étapes du scénario
- Recommandations
 - Mesures préventives
 - Détection, réaction
- Conclusion



Vécu ou imagination ?



Aéroport d'Orly

Présentation du scénario catastrophe



- **Les différentes étapes du scénario contre l'entreprise « *Maybe Airlines* »**
 1. **Envoi d'un mail piégé à un utilisateur interne ciblé**
 2. **Lancement de la charge utile**
 3. **Propagation**
 4. **Implantation sur la cible finale et mise en veille**
 5. **Réveil et exécution de la tâche finale**
 6. **Impacts immédiats et à retardement**

Déroulement du scénario (1/6)

Envoi d'un mail piégé à un utilisateur interne



- **Ciblage:** un utilisateur innocent et/ou un administrateur du système cible
- **Identification**
 - Par recherche sur les sites Web de l'entreprise, dans les newsgroups, les listes de diffusion, ...
 - Par ingénierie sociale
 - Par complicité interne
- Développement d'un code hostile sur mesure
- Enrobage dans une pièce attachée innocente ou furtive
- **Envoi**
 - Par l'intermédiaire d'un remailer anonyme
 - En usurpant l'identité d'un correspondant habituel
 - Grâce à un outil fragmentant le message afin de tromper la passerelle anti-virus
- **Les firewalls ne voient rien !**



Étapes du scénario (2/6)

Lancement de la charge utile



- **Par une vulnérabilité logicielle**
 - Exécution de la pièce attachée lors de l'ouverture du mail
 - Parfois même lors de la simple prévisualisation
 - Ou bien serveur Web hostile

- **Par ingénierie sociale**
 - Mail au contenu attirant
 - Expéditeur connu
 - « Manipulation » de l'interlocuteur
 - Ex: vente d'une voiture peu chère

Etapes du scénario (3/6)

Propagation



- **Propagation du ver sur le réseau interne de l'entreprise**
 - Exploration du réseau
 - Examen des partages de fichiers
 - Infection de fichiers (MS Office, exécutables)
 - Envoi d'autres mails
 - Infection de pages Web internes (-> pages hostiles)
 - Infection d'applications vulnérables
 - Exemple: CodeRed, Nimda
- **Contrôle de la propagation du ver pour éviter un effet « boule de neige » et donc une détection**

Etapes du scénario (4/6)

Implantation sur la cible finale



- **Sur un serveur d'application**
 - Implantation en mémoire seulement (plus furtif)
 - Analyse des données et des processus métiers
- **Sur une console d'administration**
 - Masquage des fichiers et des processus du ver (rootkit)
 - Analyse du trafic réseau
- **Sur un poste de travail**
 - Démarrage automatique
 - élévation de privilèges
 - Récupération de mots de passe

Etapes du scénario (5/6)

Réveil et exécution de la tâche finale



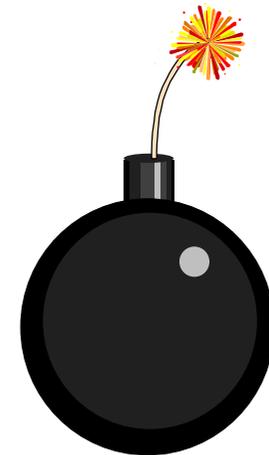
- **Réveil**
 - A une date précise
 - Sur un événement précis (trigger)
 - Sur un paquet IP précis
 - Sans avoir forcément un port ouvert (ICMP, carte en mode promiscuous)
- **Pilotage, mises à jour, récupération d'ordres et de cibles**
 - Par connexion sortante (reverse Back Orifice)
 - Par IRC, newsgroup, ...
 - Par mail
 - Par canal caché (ICMP, DNS, ...)
- **Effacement automatique une fois la mission accomplie**

Etapes du scénario (6/6)

Impacts immédiats et à retardement



- **Défiguration de sites Web**
 - Atteinte à l'image de marque
- **Récupération d'informations**
 - Sniffer
 - Keylogger (ex: virus Klez)
- **Dénis de service**
 - Simples (DoS)
 - Distribués (DDoS)
- **Destruction d'informations**
- **Modification furtive d'informations**
- **Modification des backups**
 - Restauration d'un système corrompu
 - Impossibilité de restaurer les systèmes
- **Implantation d'autres bombes logiques**
 - Modification à la volée au moment opportun
 - Attaques coordonnées ultérieures en profondeur



Conséquences

- Paralysie de longue durée
- Perte de confiance des clients
- Licenciements
- Faillite

- Conséquences **physiques**
d'une attaque **logique**



- **Objectifs**
- **Généralités**
 - Les différents risques informatiques
 - Les risques logiques
- **Scénario catastrophe**
 - Présentation du scénario
 - Les différentes étapes du scénario
- ✓ • **Recommandations**
 - Mesures préventives
 - Détection, réaction
- **Conclusion**



Recommandations (1/4)



- **Mesures préventives**
 - **Rédiger une politique de sécurité adaptée**
 - Dispositifs humains (cellule de crise)
 - Dispositifs organisationnels (rôles, procédures, indicateurs)
 - Dispositifs techniques
 - **Sensibiliser / former les utilisateurs finaux**
 - **Partitionner le réseau interne en zones de confiance séparées par des firewalls**
 - **Sécuriser à la fois le réseau, les OS et les applications**
 - Mises à jour, veille technique
 - **Développer les applications Web de manière sécurisée**



Recommandations (2/4)



- **Mesures préventives (suite)**
 - Ne pas oublier la sécurité des postes de travail
 - Mettre à jour les anti-virus (messagerie, Web et postes de travail)
 - Mettre à jour et configurer les navigateurs et clients de messagerie
 - Etape la plus difficile
 - Ref: <http://www.chambet.com/publications/ie-oe-security/>
 - Plan de secours – plan de reprise
 - **Effectuer des backups**
 - Contrôler l'intégrité des backups
 - Plan de gestion et de sortie de crise



Recommandations (3/4)



- **Détection**
 - **Analyse des logs**
 - Récupération, centralisation, consolidation, analyse, sauvegarde des logs
 - **IDS**
 - Adapter leur configuration aux particularités de réseau afin de minimiser les faux positifs
 - **Analyse des flux réseaux inhabituels**
 - Signe qu'une infection a eu lieu
 - **Contrôle d'intégrité des fichiers**
 - Exemple: tripwire
 - **Passage périodique « au magasin » des postes de travail**
 - Analyse, nettoyage, mise à jour ou réinstallation (ex: ordinateurs portables)



Recommandations (4/4)



- **Réaction**

- Génération de fiches d'alertes
- Distribution des rôles et des tâches (selon politique de sécurité)
- Suivi des alertes
- Résolution et clôture des alertes

- **Résolution**

- But: éviter l'effet domino
- Déconnexion du réseau du (des) système(s) mis en cause
- Basculement vers système(s) de secours
- Backup du système et analyse post-mortem
- Nettoyage ou réinstallation
- Restauration saine des données
- Remise en exploitation du système
- Surveillance temporairement accrue



Conclusion



EdelWeb

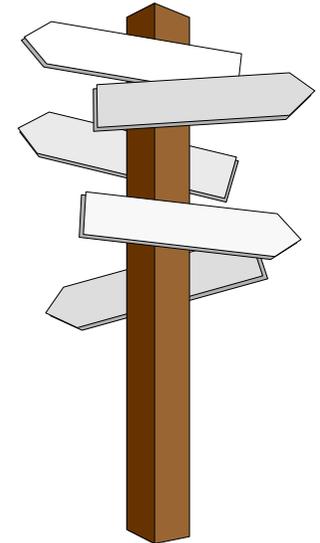
- **Le scénario étudié vous a-t-il paru invraisemblable ?**
- **La probabilité d'un tel scénario est de plus en plus forte**
- **Il est important de s'y préparer**
- **Les firewalls ne suffisent pas (« ligne Maginot »)**
- **Il faut prendre en compte la sécurité de manière globale**
 - **Sécurité organisationnelle**
 - **Sécurité technique**
 - **Physique**
 - **Logique**
 - **Evolution de la sécurité vers la **défense** des SI**
- **Importance du rôle des tests d'intrusion: seule façon d'évaluer un niveau de sécurité en grandeur nature**

Pour aller plus loin... (1/2)



EdelWeb

- **OSSIR**
 - <http://www.ossir.org>
- **CLUSIF**
 - <http://www.clusif.asso.fr>
- **SCSSI**
 - <http://www.ssi.gouv.fr>
- **UREC**
 - <http://www.urec.fr/securite>
- **SecurityFocus**
 - <http://www.securityfocus.com>
- **SANS Institute (System Administration, Networking and Security)**
 - <http://www.sans.org>

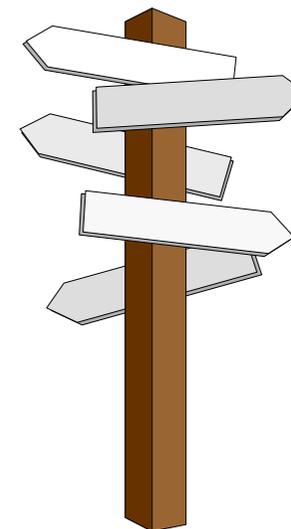
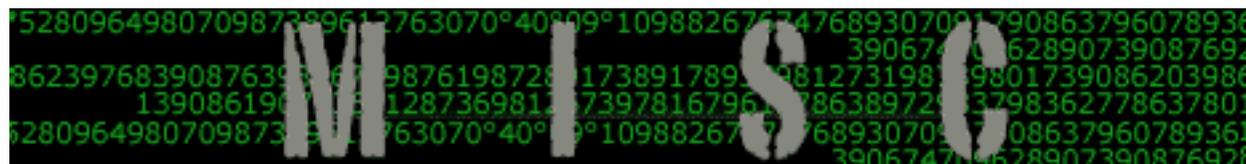


Pour aller plus loin... (2/2)



EdelWeb

- <http://www.edelweb.fr/EdelStuff/EdelPages/>
- **MISC** (premier journal technique français sur la sécurité des SI)



- <http://www.miscmag.com>
- La guerre de l'information (scénario itératif) :
<http://www.miscmag.com/articles/index.php3?page=404>
- Cyber-terrorisme :
<http://www.chambet.com/publications.html>

Questions

