Les erreurs humaines

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Considérer les erreurs humaines comme des menaces peut sembler un peu indélicat et pourtant, comme le montrent les statistiques publiées par différents organismes, elles demeurent une cause très courante de sinistres informatiques. On considère comme « erreur humaine », tout comportement humain ne respectant pas le bon usage et pouvant conduire de façon involontaire à des préjudices divers.

Table des matières

1 C'est quoi ?
2 Qui est concerné ?
3 Comment cela fonctionne-t-il ?
4 Pourquoi se protéger ?
5 Comment se protéger ?
6 Statistiques

1 C'est quoi ?

On considère comme « erreur humaine », tout comportement humain ne respectant pas le bon usage et pouvant conduire de façon involontaire à des préjudices divers. Les actes volontaires réalisés dans un but malveillant ne sont pas qualifiés d'erreurs. Il est impossible de dresser une liste exhaustive des erreurs humaines. Bien qu'il soit impossible de quantifier toutes les possibilités en matière d'erreurs humaines, il est toutefois possible de dresser quelques critères distinctifs permettant de classifier les erreurs humaines.

1.1 Les erreurs de type « négligence »

On regroupe sous ce titre toutes les actions menées par des personnes bien informées mais ne respectant pas les règles. On pourrait donc associer la négligence à un acte volontaire. Toutefois le but de la négligence n'est généralement pas frauduleux.

Exemples:

- ne pas respecter les procédures prévues pour la sauvegarde des données,
- arrêter la mise à jour de la solution anti-virale au démarrage de la machine,
- confier son mot de passe à un collègue,
- utiliser l'architecture informatique de l'entreprise à usage privé,
- installer un logiciel « hors norme » sur une machine, notamment ordinateur ou serveur.

1.2 Les erreurs de type « incapacité »

Cette catégorie regroupe toutes les erreurs commises sans en avoir conscience. En effet, de nombreuses erreurs peuvent être commises « de bonne foi », sans que l'utilisateur ait conscience du non-respect du bon usage ou du règlement et sans qu'il mesure l'impact de son geste.

Exemples:

- le « social engineering » (voir point relatif à ce sujet),
- la mauvaise utilisation de l'outil informatique,
- l'effacement de données.

2 Qui est concerné ?

Tout utilisateur d'un équipement ou d'un système informatique est susceptible de commettre des erreurs humaines.

suite au verso

www.cases.lu

Les erreurs humaines

suite

3 Comment cela fonctionne-t-il ?

Les erreurs humaines sont des menaces non intentionnelles qui exploitent différentes vulnérabilités notamment :

3.1 La fainéantise et l'absence de conscience professionnelle

Dans cette catégorie sont repris tous les actes commis par négligence et contre lesquels il est très difficile de lutter, si ce n'est en agissant au niveau de la responsabilisation et des mécanismes de sanction.

3.2 Le manque de formation ou de sensibilisation à la sécurité

L'absence de conscientisation d'une personne représente bien sûr une énorme vulnérabilité dont la face cachée est l'absence de prise de conscience de l'erreur commise, et donc l'absence de détection et de correction par la personne elle-même.

Le manque de formation et de sensibilisation à la sécurité d'une personne présente une vulnérabilité pouvant être exploitée par une menace hautement dangereuse qui est le **social engineering** :

LE « SOCIAL ENGINEERING »

Cette technique a pour but d'extorquer des informations sensibles à des personnes. Contrairement aux autres attaques, elle ne nécessite pas de logiciel. La seule force de persuasion du cracker et la cupidité ou l'ignorance de sa victime sont les clefs de voûte de la réussite de cette attaque. Il y a quatre grandes méthodes de social engineering.

1. Par téléphone
Le cracker contacte sa cible par téléphone. C'est la technique la plus simple. Son but est d'avoir le renseignement le plus rapidement possible.

2. Par courrier
Le cracker adresse à sa victime une lettre très professionnelle. Il utilise très souvent la boîte postale d'une société fictive.

3. Par Internet
La méthode est comparable à celle utilisée par téléphone. Le cracker se fait facilement passer pour un opérateur système, un responsable informatique ou un ingénieur système.

4. Par contact direct
C'est le social engineering le plus rarement utilisé et ce en raison de la complexité et des risques encourus de la part du cracker. Toutefois, la plupart des sociétés fournissant des services informatiques n'auraient pas besoin d'insister beaucoup pour exploiter le social engineering.

4 Pourquoi se protéger ?

⚠ Les erreurs humaines constituent une menace considérable pour tous les utilisateurs des systèmes d'information et de communication et peuvent causer des préjudices financiers ainsi que des pertes de réputation importants.

5 Comment se protéger ?

La loi de « non-fiabilité » de Gibbs (mathématicien américain) stipule que « Tout système qui dépend de la fiabilité de l'homme n'est pas fiable ».

Il existe de multiples moyens de lutter contre les erreurs humaines. Toutefois, il est conseillé de consacrer beaucoup d'énergie à la limitation de l'impact des erreurs humaines et de ne pas partir du principe que l'on va être en mesure d'éviter toutes les erreurs humaines. Les principales contre-mesures sont les suivantes :

5.1 La sensibilisation

C'est dans ce domaine qu'il est facilement possible de diminuer de manière sensible le risque.. En effet, la majorité des êtres humains sont de bonne volonté et si on les informe de l'importance de leurs gestes quotidiens ainsi que de la valeur des données traitées, ils prendront à cœur de les gérer en bon père de famille.

5.2 La formation

Le meilleur moyen d'éviter de mauvaises manipulations au niveau des données et des logiciels, est de former les utilisateurs sur les logiciels et sur la manipulation des supports.

5.3 La mise en place et le contrôle de procédures

Il est primordial de mettre en place des procédures qui couvrent tous les aspects importants (accès, sauvegarde...) touchant à la sécurité. Ces procédures doivent être contrôlées de façon cyclique et leur non respect devrait entraîner des sanctions.

suite au verso

Les erreurs humaines

suite

5.4 La double validation

Afin d'éviter des erreurs de saisie au niveau des logiciels critiques (paiement électronique...), il est prudent de mettre en place une double saisie des données ou une double validation.

5.5 La gestion et le suivi des erreurs

Les erreurs n'étant pas entièrement inévitables, il faut en tirer les conséquences afin de ne pas les reproduire. Seule une analyse pointue des erreurs commises, ainsi que des causes à l'origine de ces erreurs permet d'en éviter la répétition.

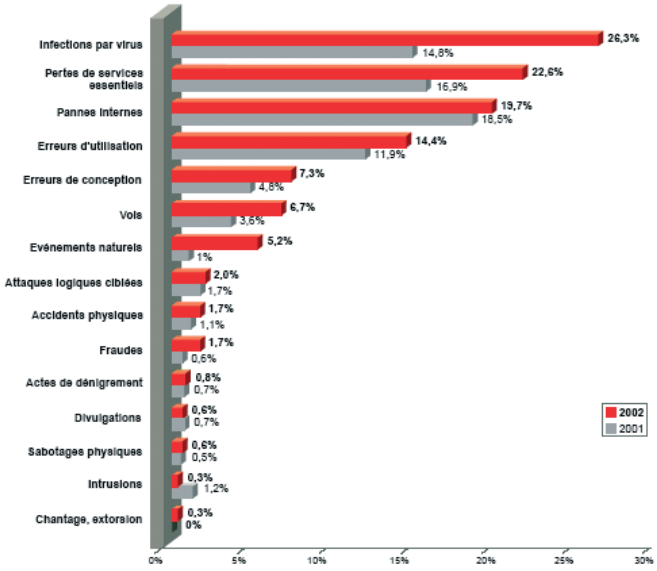
5.6 L'administration centralisée

Pour minimiser les erreurs humaines, il est conseillé que vous limitiez strictement les accès aux logiciels et aux données aux seules personnes qui en ont vraiment besoin.

6 Statistiques

En 2002 en France, 24% des sinistres informatiques sont dus à un accident, 14% à des erreurs humaines et 62% à la malveillance (source: CLUSIF - Club de Sécurité Informatique Français).

Le ci-après donne un aperçu de l'incidence des erreurs humaines par rapport aux autres menaces.



CASES,
pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois

OFFICE LUXEMBOURGEOIS D'ACCREDITATION ET DE SURVEILLANCE

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Economie et du Commerce extérieur