

Mourad LOUKAM – Département d'Informatique-UHBC/Chlef

# La sécurité informatique : enjeux et perspectives

# Pour commencer

7 الشروق

متابعة

الأحد 21 مارس 2010 / الموافق لـ 05 ربيع الثاني 1431 هـ / العدد 2880

تحضر للمتابعة القضائية للمتورطين في اختطاف "اسم النطاق"

## الشروق تسترجع موقعها الإلكتروني بعد معركة ضارية مع القرصنة

بعد معركة إلكترونية وإدارية ضارية تمكنت جريدة الشروق من استعادة اسم النطاق الخاص بموقع الجريدة (www.echoroukonline.com) بعد عملية السطو والاختطاف التي تعرض لها على يد قرصنة مصريين منذ أسبوع بطريقة مخططة لها بدقّة، وأثبتت التحريات أن أصحاب العملية تقف وراءهم جهات قوية يحتمل أنها استخباراتية.

لهذه الأسباب تم استهداف موقع "الشروق أون لاين"

عبد الرحمن م

أثارت قرصنة موقع "الشروق أون لاين" الكثير من التساؤلات عن السر وراء الهجوم إلى شرب الموقع العربي الأول للتخصص في الإعلام، حسب آخر تقارير موقع "اليكسا" العالمي، وكذا توقّعت هذه القرصنة النوعية التي حاولت من خلالها جهات مصرية مشبوهة القضاء على صوت الشروق التي صارت تمثل إخراجاً للنظام المصري، لأنها واجهته بغير ما ألف أن تواجهه به عادة الصحف العربية.

ورغم أن محاولات القرصنة المصرية قد بدأت بشكل لافت منذ شهر أكتوبر الماضي، إلا أن الطريقة التي عمد إليها القرصنة هذه المرة تختلف اختلافاً كبيراً عن محاولات الاختراق الكلاسيكية، وأدت تقنياتهم الحديثة إلى اختراق المؤسسة الأمريكية المسؤولة عن تأمين اسم نطاق الجريدة، ثم الاتصال بالشركة التي ترعى خوادم الشروق "السيرفرات" وعرض شرائها، وهي التي تُقدّر بمئات الآلاف من الدولارات (الخوادم لوحدها تُقدّر بما لا يقل عن 12 ألف دولار دون احتساب المادة الإعلامية)، وهذه المعطيات وردت من الشركة الراعية نفسها التي رفضت عرض الشراء، رغم حرص القرصنة في رسالة لاحقة نشرها على موقع "الشروق" على نفي هذه المعلومة، وهو أحد التناقضات التي وقع فيها القرصنة الذين غطوا على جريمتهم بدعاوى عريضة من بينها التأكيد على العروبة ورفض

عبد الرزاق بوالقمج

من يعتذر لمن؟

وكانت عملية السطو وما تبعها من تحقيقات قام بها الفريق التقني للشروق أون لاين وكذا تقنيو شركة جيكوس لتحديد الجهة التي تقف وراء العملية أثبتت بوضوح الاختطاف التي تحدثت يومياً عبر العالم، حيث يقوم الخاطفون بالكشف عن مطالبهم غداً كل عملية، إذ طلب القرصنة من جريدة الشروق تقديم "اعتذار للشعب المصري" كشرط أساسي لاستعادة اسم النطاق لكن هذا القرصان والجهة التي تقف وراءه والذين نصبوا أنفسهم كنطاق رسمي باسم الشعب المصري



في الإعلام الأبي تمكّنوا بعد تتبع قلعوا على إثرها بتحسين وحماية دفع كل هذه الأموال، إلى جانب

Cas du quotidien EChourouk

Mourad LOUKAM, 13 Avril 2010

# Pour commencer

الجمهورية الجزائرية الديمقراطية الشعبية - وزارة التعليم العالي و البحث العلمي  
 République Algérienne Démocratique et Populaire - Ministère de l'Enseignement Supérieur et de la Recherche Scientifique  
 المديرية العامة للبحث العلمي و التطوير التكنولوجي  
 Direction Générale de la Recherche Scientifique et du Développement Technologique DG-RSDT

Site en cours de maintenance jusqu'au 18 avril 2010

The image depicts a futuristic digital landscape. In the foreground, a blue and black robot with a human-like head and torso is shown from the side, looking towards the left. The background features a city skyline with tall buildings, several wind turbines, and solar panels. The scene is overlaid with various mathematical equations and data points, creating a high-tech, scientific atmosphere. The ground is a mix of orange and yellow, suggesting a desert or a digital terrain.

Nous contacter....

Webmail...

DG-RSDT National Administration of Scientific Research NASR-DZ DPREP

## Cas de la DGRS

## Pourquoi faut-il + de sécurité informatique ?

Développement  
d'internet et  
Informatique  
nomade



de plus en plus d'organismes  
**ouvrent** leur systèmes  
d'informations à leurs partenaires  
(fournisseurs , clients, ...)



il est donc essentiel de connaître les ressources de l'entreprise à  
**protéger** et de maîtriser le **contrôle d'accès** et les **droits des**  
**utilisateurs** du système d'information

## Quelques concepts

La **menace** (threat) : toute action susceptible de nuire.

La **vulnérabilité** (*vulnerability*) : représente le niveau d'exposition face à la menace.

La **contre-mesure** : représente l'ensemble des actions mises en œuvre en prévention de la menace.

## Quelques concepts

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité}}{\text{Contre-mesure}}$$



**Le risque augmente lorsque les contre-mesures diminuent  
(sont insuffisantes)**

## Objectifs de la sécurité informatique

**L'intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;

**La confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;

**La disponibilité**, permettant de maintenir le bon fonctionnement du système d'information ;

**La non répudiation**, permettant de garantir qu'une transaction ne peut être niée ;

**L'authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

**La sécurité informatique, n'est pas qu'un mot de passe !**

**Il est inutile de blinder la porte alors que les  
fenêtres sont ouvertes !**



**Il est nécessaire d'entreprendre la sécurité  
informatique dans un cadre global : il faut une  
politique de sécurité**

## La politique de sécurité

La politique de sécurité est l'ensemble des orientations suivies par une organisation en terme de sécurité

Elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système

## Mise en place d'une politique de sécurité :

1/ **Identifier les besoins** en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;

2/ **Elaborer des règles et des procédures** à mettre en oeuvre dans les différents services de l'organisation pour les risques identifiés ;

3/ **Surveiller et détecter les vulnérabilités** du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;

4/ **Définir les actions à entreprendre** et les personnes à contacter en cas de détection d'une menace ;

## Mise en place d'une politique de sécurité :

### Analyse des besoins : faire l'inventaire

- Personnes et fonctions ;
- Matériels, serveurs et les services qu'ils délivrent ;
- Cartographie du réseau (plan d'adressage, topologie physique, topologie logique, etc.) ;
- Liste des noms de domaine de l'entreprise ;
- Infrastructure de communication (routeurs, commutateurs, etc.)
- Données sensible

## Mise en place d'une politique de sécurité :

**Analyse des risques** : Répertorier les risques possibles, estimer leur probabilité et leur coût (dommages).

Exemple d'échelle :

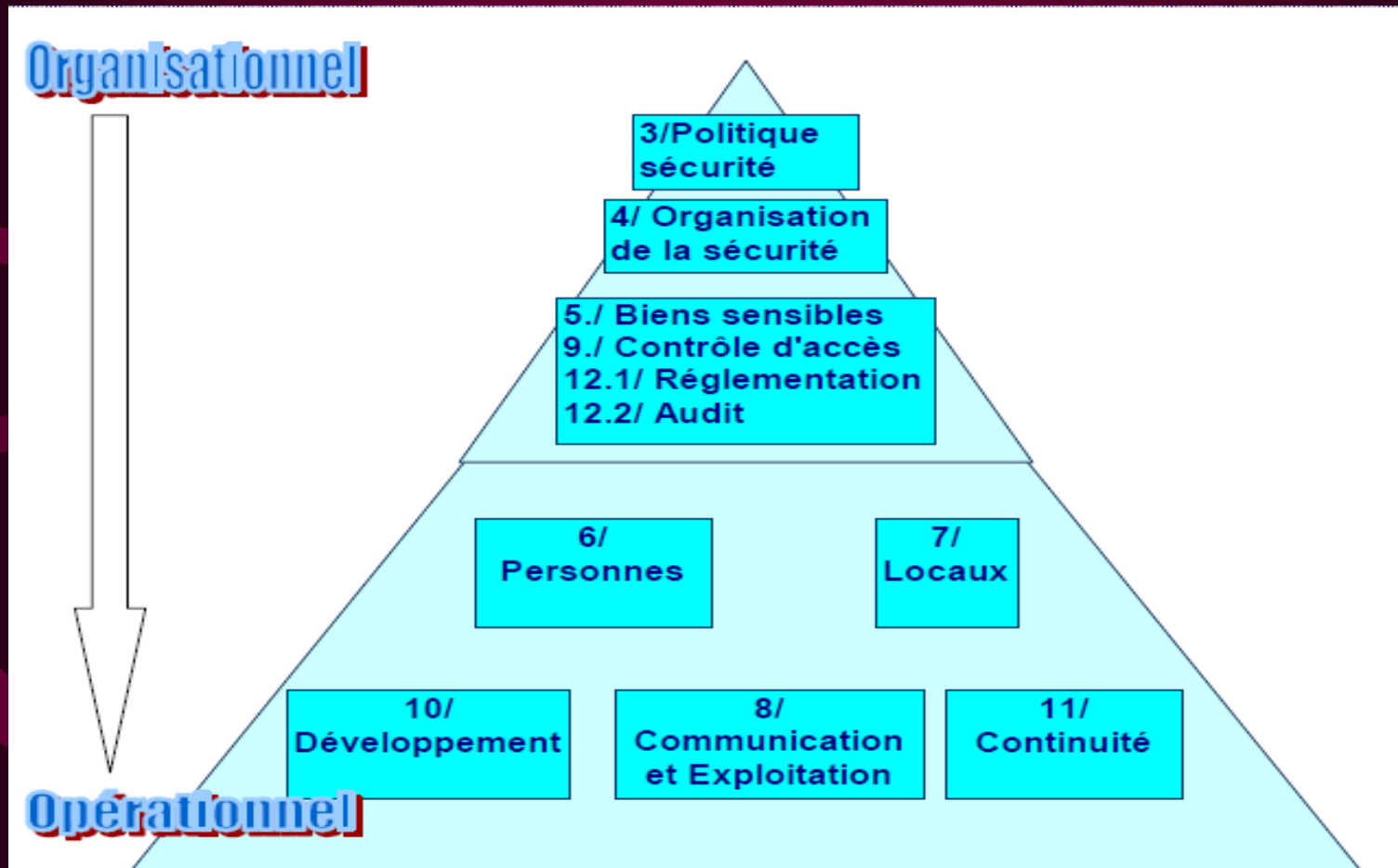
- Sans objet (ou improbable) : la menace n'a pas lieu d'être ;
- Faible : la menace a peu de chance de se produire ;
- Moyenne : la menace est réelle ;
- Haute : la menace a de grandes chances de se produire.

## Quelques Méthodes :

1. **MARION** (*Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux*);
2. **MEHARI** (*MEthode Harmonisée d'Analyse de RIques*) ;  
<https://www.clusif.asso.fr/fr/production/mehari/>
3. **EBIOS** (*Expression des Besoins et Identification des Objectifs de Sécurité*), mise au point par la DCSSI (*Direction Centrale de la Sécurité des Systèmes d'Information*) ;  
<http://www.ssi.gouv.fr/fr/confiance/ebios.html>
4. **La norme ISO 17799.**

## La norme ISO 17799

Norme concernant « la sécurité de l'information », publiée en 2000 par ISO, (mise à jour en 2005).



## Aspects techniques

Les principaux dispositifs permettant de sécuriser un système d'informations

Les antivirus

Les pare-feu

Les algorithmes cryptographiques

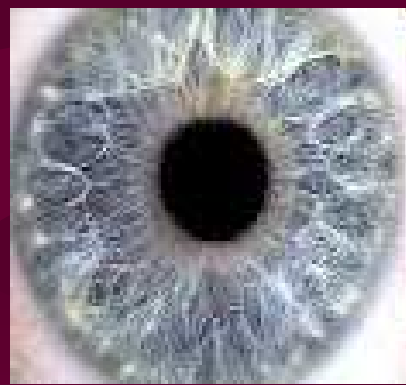
Les VPN (tunnels sécurisés)

...

Les méthodes biométriques

## Aspects techniques

### Les méthodes biométriques



## Conclusion

- Nécessité de la mise en place d'une politique de sécurité
- Se conformer aux normes de sécurité
- ...
- Introduire la « sécurité informatique » dans le cursus de formation des informaticiens

## Liens utiles

**MEHARI** (*M*éthode *H*armonisée d'Analyse de *R*isques) ;

<https://www.clusif.asso.fr/fr/production/mehari/>

**EBIOS** (*E*xpression des *B*esoins et *I*dentification des *O*bjectifs de *S*écurité), mise au point par la **DCSSI** (*D*irection *C*entrale de la *S*écurité des *S*ystèmes *d'*Information) ;

<http://www.ssi.gouv.fr/fr/confiance/ebios.html>

Merci !