

Dz  
**HACKEVENT**  
Compte-rendu



Professionnels, experts, étudiants, amateurs et passionnés autour d'une série de conférences, d'ateliers et de challenges sur des problématiques de sécurité informatique.

- La sécurité des illusions
- La sécurité des systèmes SCADA
- Exploiting RFID vulnerabilities using NFC phones
- Traitement du volet humain dans la sécurité numérique
- Protection des Infrastructures critiques industrielles
- Are we ready for the new CyberWar ?
- Reactions and learning From the SONY hack
- La protection du Cloud et de l'infrastructure virtuelle
- Offensive Python For Networkers
- La gouvernance de la Sécurité des SI dans les organisations
- Analytics malware
- Comment convaincre votre hiérarchie pour investir dans la sécurité informatique ?

**09 Mai 2015**  
Centre de formation CBA (Sonelgaz)  
IFEG - Ben Aknoun - Alger.  
[www.dz-hackevent.elit.dz](http://www.dz-hackevent.elit.dz)

**ELIT** El Djazair Information Technology

# Dz HACKEVENT

09 mai 2015

Centre de formation Sonelgaz  
IFEG - Ben Aknoun - Alger





Pour la première fois en Algérie, le Dz-HackEvent, organisé par ELIT et sponsorisé par les Sociétés du Groupe Sonelgaz, s'est déroulé le 09 mai 2015 au niveau des locaux du CBA à Ben Aknoune.

Cet évènement a regroupé d'éminents experts en sécurité informatique, et s'est vu être un lieu d'échange et de débats sur des thématiques

relatives à la sécurité IT, répondant à des défis et des préoccupations d'actualité.

Cette première édition a été marquée par le nombre et la qualité des participants (chercheurs, enseignants, étudiants, employés, dirigeants, etc.) qui témoignent, on ne peut mieux, de la pertinence des thématiques annoncées.

## SPONSORS



M. Noureddine BOUTARFA

Président Directeur Général de la Société Nationale de l'Electricité et du Gaz (Sonelgaz)



M. Abdelouahab BOUKHAROUBA

Président Directeur Général de El Djazaïr Information Technology (ELIT)



**M. Lamine OUYAHIA**

Vice-Président de l'AASSI et propriétaire d'OTEK. Animateur et conférencier spécialisé en sécurité IT.

**M. Bruce SCHNEIR**

Membre de "Berkman Center for Internet and Society" à l'université de Harvard. Cryptologue spécialiste en sécurité informatique.

**M. Dmitry KUZNETSOV**

Expert en sécurité des systèmes SCADA (Systèmes de contrôle et d'acquisition de données).

**M. Hafedh BEN HAMIDA**

Spécialiste en Piratage informatique et Investigations des Crimes Cybernétiques.

**M. Pavol LUPTAK**

Consultant en sécurité et propriétaire de Nethemba Slovaquie OWASP.

**M. Haythem EL MIR**

Consultant expert en sécurité informatique et Cybersécurité. Directeur technique à Positive Technologies pour la région MENA.

**M. Michel GERARD**

Consultant expert en sécurité informatique et CEO & propriétaire de RAPID AWARNESS, CONSCIO TECHNOLOGIES et HAPSIS.

**M. Boumediene KADDOUR**

Etudiant à "Pentester Academy".Animateur de conférences et d'ateliers traitant de la sécurité informatique.

**M. Rafik BENCHERAIET**

Conseiller senior en sécurité. Spécialiste en cybercriminalité et en cyber terrorisme.

**M. Battista CAGNONI**

Expert certifié, animateur et conférencier en sécurité des SI. Forensic Analyst

**M. Jorge SEBASTIAO**

Expert et conférencier international en sécurité informatique. Co-auteur du livre "La Face Cachée du Crédit".

**M. Thierry CHIOFALO**

Gestionnaire de la sécurité des SI. Administrateur Clusif.

**M. Abderrafiq KHENIFSA**

Informaticien de formation et journaliste multimédia. Directeur-Gérant de l'hebdomadaire it-Mag. Un magazine des professionnels IT

D  
Z  
H  
A  
C  
K  
E  
V  
E  
N  
T

**AGENDA**

Se déroulant sur deux volets, la première édition du DZ Hack Event a prévu dans son agenda :

- En diurne : des conférences et Work-Shops ;
- En nocturne : le challenge "Capture the Flag" CTF.

Une application mobile a été mise en service

par les ingénieurs-développeurs d'ELIT en vue de faciliter aux convives de cet évènement le suivi du programme de la journée et fournir des informations utiles, en temps réel, sur tous les aspects liés aux travaux de la journée (comme les différentes informations concernant les conférences, les intervenants, les ateliers, etc.) ainsi que la participation à un jeu en ligne.

08h00	<b>Accueil et réception</b>	
09h00	Allocution d'ouverture et mot de bienvenue	M. Abdelouahab BOUKHAROUBA
09h20	Allocution de Monsieur le PDG de Sonelgaz	M. Noureddine BOUTARFA
09h40	<b>La sécurité des Illusions</b>	M. Lamine OUYAHIA
10h20	<b>La sécurité des systèmes SCADA</b>	M. Dmitry KUZNETSOV
11h00	<b>Pause café</b>	
11h30	Exploiting RFID vulnérabilités using NFC phones	M. Pavol LUPTAK
12h10	Traitemet du volet humain dans la sécurité numérique	M. Gerard MICHEL
13h00	<b>Pause déjeuner</b>	
14h00	Protection des Infrastructures critiques industrielles	M. Rafik BENCHERIAT
14h40	Are we ready for the new CyberWar ?	M. Jeorge SEBASTIAO
15h20	Reactions and learning From the SONY hack	M. Bruce SCHNEIER
16h00	La protection du Cloud et de l'infrastructure virtuelle	M. Hafed BENHAMIDA
16h40	Table Ronde "Comment convaincre votre hiérarchie pour investir dans la sécurité informatique ?"	M. Abderrafiq KHENIFSA
17h40	<b>Clôture</b>	
	<b>Les ateliers</b>	
	La sécurité des systèmes SCADA	M. Haythem ELMIR
	Offensive Python For Networkers	M. Boumediene KADDOUR
	Hacking RFID devices using NFC smartphones	M. Pavol LUPTAK
	La gouvernance de la sécurité des SI dans les organisations	M. Thierry CHIOFALO
	Analytics malware	M. Battista CAGNONI
20h00	Nuit du challenge « Capture The Flag »	
06h00	Remise des prix	

## ACCUEIL ET RECEPTION DES CONVIVES

L'Auditorium Mohamed Djediani a commencé à accueillir les convives d'ELIT, dès 08 heures. En vue d'imprégner les invités dans l'ambiance de l'évènement, un quiz a été proposé aux invités qui le désirent pour stimuler leurs

connaissances IT et donner, du coup, un avant-gout sur le contenu de cette journée.

A noter que des cadeaux symboliques ont été remis aux participants gagnants.

## ALLOCUTIONS

M. Abdelouahab Boukharouba,

Président Directeur Général d'ELIT.



Le mot d'ouverture de cet évènement a été prononcé par le Président Directeur Général d'ELIT, en l'occurrence, M. Abdelouahab Boukharouba.

Il a remercié l'ensemble des convives hôtes d'ELIT d'avoir répondu à l'invitation et a souhaité aux experts venus d'ailleurs, un excellent séjour en Algérie.

M. Abdelouahab Boukharouba n'a pas caché son plaisir d'accueillir tous ces acteurs du monde de l'IT.

*« C'est un grand honneur que de pouvoir vous rassembler et un immense plaisir que de prendre la parole pour vous dire combien il est important de commencer à débattre entre pairs d'une préoccupation commune qui devrait interroger autant les professionnels de l'IT que les managers principaux de toutes les organisations,... ».*

Et d'enchaîner par un rappel « *des défis à relever, dans un nouveau contexte technico-économique, marqué par la numérisation et le cyberspace, qui relèvent tout particulièrement de la pérennité où les menaces et les risques qui pèsent sur nos systèmes sont en perpétuelle croissance...* »

En parlant du problème de la sécurité IT, M. Boukharouba s'est posé quelques questions sur nos capacités à déceler en ce moment même, d'éventuelles intrusions et/ou attaques sur nos SI.

Il n'a pas manqué d'attirer l'attention que le « maillon faible » du processus qui fait que la principale cause de vulnérabilité demeure l'être humain.

Il confirme, également, que les risques maîtrisables sont minimes par rapport aux risques ignorés, qui échappent à tout contrôle. « *Enfin, pour maîtriser ces risques, il est nécessaire de mettre en œuvre tous les moyens, les technologies et les processus appropriés* ».

En guise de conclusion de son mot d'ouverture, le Président Directeur Général d'ELIT a réitéré ses propos de bienvenue et a invité les présents à utiliser l'application mobile, mise à leur disposition, par les développeurs ELIT.

M. Noureddine Boutarfa,  
Président Directeur Général de Sonelgaz.



M. Noureddine Boutarfa a tenu à saluer l'ensemble des invités et a montré sa satisfaction de se retrouver à ce premier «Dz-HackEvent», organisé par ELIT.

Pour M. Boutarfa, il ne s'agit nullement d'un hasard car le numérique a, depuis plusieurs années, bouleversé toutes les transactions et, de ce fait, le mode de vie que nous avons mené jusque-là se transformera au gré du cyberspace, une sorte de toile qui est en train de nous embrigader.

Il précise que : « ...Nous sommes des industriels, nous sommes des sociétés qui exercent essentiellement dans le domaine des réseaux. Nos activités se prolongent depuis la chaîne de production des hydrocarbures, leur transport, leur transformation en électricité, jusqu'à la distribution et la consommation des énergies. »

Et de rajouter que : « ...toute l'économie nationale repose sur l'énergie et sans celle-ci nous reviendrons des siècles en arrière ... donc l'énergie est "un capital" qu'il faut sécuriser, au même titre que nos réseaux, d'où l'intérêt de se pencher sérieusement sur l'aspect de la sécurité informatique. »

M. Boutarfa a, également, rappelé que les actes malveillants en matière de sécurité informatique coutent très chers. Pour étayer ses propos, il a cité plusieurs exemples de failles de sécurité exploitées, à travers le monde, pour nuire à des sociétés et même à des états souverains. Il a cité entre autres l'affaire des centrifugeuses Bouchehr d'Iran, le Black-out de Turquie tout en insistant sur le rôle fondamental de la sécurité informatique qui va au-delà du simple fait de la sécurité industrielle et qui peut constituer une réelle crise nationale.

M. Noureddine Boutarfa, a conclu son intervention par des propos encourageants à l'endroit des organisateurs de l'évènement, en témoignant que ce DZ Hack Event est venu à point nommé.



## « La sécurité des illusions »

M. Lamine OUYAHIA

Plusieurs organisations exploitent des solutions de sécurité informatique et tentent de se conformer à des politiques et des standards. Mais serait-il possible que tout cela ne soit en réalité qu'une grande comédie sécuritaire dont le but est de se rassurer que l'on est à l'abri du croquemitaine numérique ?

Bien évidemment, l'idéal est un niveau de sécurité impossible à atteindre en pratique. Mais cela ne signifie pas que la sécurité informatique est en soi un mirage. La question de savoir si nous disposons d'une sécurité réelle ou si nous avons une sécurité faite d'illusions mérite d'être posée.

L'intervenant a parlé de l'excès de confiance par rapport aux standards, aux outils et aux architectures des systèmes qu'il a qualifié comme étant un ennemi redoutable. Il a fourni dans ce sens des recommandations concrètes.



## « La sécurité des systèmes SCADA »

M. Dmitry KUZNETSOV

L'orateur a commencé son intervention en annonçant que la sécurité des systèmes SCADA constitue un défi majeur à relever.

Et de poursuivre, qu'actuellement nous sommes face à plusieurs sortes de pirates : ceux qui agissent pour leur propre compte et d'autres qui sont sous les commandes d'une organisation, voire d'un gouvernement. Et quelle que soit leur obédience, ces pirates utilisent les mêmes armes pour perpétrer leurs attaques et disposent d'une capacité de destruction redoutable.

La conférence dans son ensemble s'est, essentiellement, focalisée sur les risques de sécurité liés aux systèmes « SCADA ».

L'orateur a présenté le sujet sous plusieurs facettes, de sorte à fournir le maximum d'informations sur cette problématique, relativement nouvelle et qui devrait intéresser tous les industriels dont les activités sont plus au moins automatisées.



## « Exploiting RFID vulnerabilities using NFC phones »

M. Pavol LUPTAK

L'animateur de cette conférence a débuté sa présentation par un rappel de l'importance accordée, de nos jours, au numérique. Il a fourni des exemples de pratiques frauduleuses récurrentes qui ont contraint les organisations et les gouvernements des pays occidentaux à mettre en œuvre des dispositifs parfois contraignants, voire très onéreux pour s'en prémunir. En guise d'exemple, il a parlé de la biométrisation de certains documents personnels, rendue obligatoire à travers le monde.

Il a également, longuement parlé de la généralisation de l'usage des smartphones et des éventuels menaces qu'ils génèrent tant pour leurs détenteurs que pour les organisations et les systèmes auxquels ils peuvent accéder.

L'orateur a aussi présenté et défini ce que représente, pour lui, la sécurisation des cartes de crédits en donnant des exemples concrets et en s'appuyant sur des démonstrations vidéo.



## « Traitement du volet humain dans la sécurité numérique »

M. Gerard MICHEL

La grande majorité des attaques s'appuie à un moment ou à un autre sur une défaillance, provoquée ou non, de comportement d'un utilisateur du SI. De ce fait, il ne saurait y avoir de stratégie de sécurité qui ne prenne pas en compte le volet humain. Une stratégie de sécurité efficace s'appuie sur des processus, des technologies et un développement d'une culture sécurité. Comme tout dispositif s'appuyant sur trois piliers, si on lui en enlève un c'est tout l'édifice qui s'écroule.

Développer une culture de sécurité numérique dans les entreprises est devenu indispensable. De plus, cela permet d'économiser de l'argent, ainsi PWC démontre dans sa dernière étude que le développement de cette culture permet de faire baisser le coût lié aux incidents de sécurité de 76%. C'est ce qu'a développé, entre autres, M. Michel.



## « Protection des Infrastructures critiques industrielles »

M. Rafik BENCHERAIET

Les menaces qui pèsent sur les infrastructures industrielles étant en hausse, tous les Etats et toutes les entreprises en détention de ce genre d'équipements sont fortement préoccupés.

Leur préoccupation majeure est de savoir comment protéger, contre des cyberattaques relevant du terrorisme, de l'espionnage et/ou de la criminalité, des équipements dont dépend le fonctionnement de leurs infrastructures de base (Energie, Télécoms, Transport, Eau, Assainissement...).

Présentement, il ne s'agit plus de savoir si l'on sera attaqué, mais plutôt si on ne l'a pas déjà été, quand les dégâts commenceront à apparaître et comment y remédier.

La conférence a porté, essentiellement, sur un retour d'expérience sur les risques et les menaces décelés à travers le monde, notamment en Amérique du Nord ainsi que les technologies et les solutions préconisées pour sécuriser les infrastructures critiques de type SCADA et DCS dont dépendent les réseaux d'énergie, de transport, etc.



## « Are we ready for the new CyberWar ? »

M. Jeorge SEBASTIAO

Comme l'indique l'intitulée de cette conférence, M. Sebastiao a orienté sa présentation sur la guerre cybérétique ou « Cyber War ». En prenant la région du moyen orient comme cas d'étude.

Il a parlé de l'influence des dommages informatiques sur la vie sociale et sociétale, en arguant ses propos par l'exemple de l'Egypte qui a connu une coupure d'Internet en 2008 et qui s'est transformé, par la suite, en un fief de révoltes qualifiées de "printemps arabe" (Janvier 2011 et 2013).

L'orateur a poursuivi son intervention par l'énoncé des éléments de base à protéger : car les priorités sécuritaires varient d'un pays à un autre, en fonction des ressources dont dispose chaque d'eux.

L'entreprise ou l'organisation doit dans ce contexte, mesurer les risques en déterminant leurs degrés de dangerosité.

Les attaques informatiques ou CyberWar, ne se limitent guère au secteur économique, elle relève désormais de la sécurité et de la pérennité des peuples et des Etats.

Par ailleurs, Il a insisté sur le facteur humain qui a un grand impact sur tout ce qui relève de l'insécurité numérique.

Cette conférence a été ponctuée par deux démonstrations vidéo en rapport avec la thématique.



## « Reactions and learning From the SONY hack »

M. Bruce SCHNEIER

Surnommé le gourou de la sécurité informatique, M. Bruce Schneier a entamé son intervention par saluer l'assistance en utilisant la langue de Molière avant de revenir à l'anglais, la langue dont il a choisi pour sa communication.

Son intervention avait trait au hacking et s'est longuement étalée sur l'attaque du géant SONY, supposée par le gouvernement Nord-Coréen, qui a fait couler beaucoup d'encre et dont nul ne peut confirmer avec exactitude les tenants et aboutissants.

Il a expressément comparé l'affaire Sony aux attentats du 11 septembre et, cela, pour dire que la sécurité informatique revêt parfois un caractère vital notamment lorsque l'attaque cible une organisation d'envergure ou un Etat.

Selon l'orateur, le Hacking est tout acte d'intrusion ou d'attaque commis par un pirate informatique qu'il soit amateur ou qualifié.

Jusque-là, nul Etat n'a été qualifié « d'Etat Hacker », bien que ces opérations aient été orchestrées ou commanditées par certains gouvernements.

C'était la manière à M.Bruce Schneier d'alerter l'assistance sur les risques de hacking qui peuvent parfois aller au-delà des simples hackers agissant de leur propre gré et s'inscrire comme une action de piraterie orchestrée et bénie par des gouvernements et des Etats.

A la fin de sa conférence, M. Bruce Schneier a répondu à quelques questions. Nous vous en citerons ce qui suit :

Q : Réellement la Corée du Nord est-elle responsable, dans l'affaire SONY ? Ou, sommes-nous face à une autre opération de propagande ?

En d'autres termes, Pourrait-il s'agir tout simplement d'un mensonge, comme celui du conflit qui a opposé le monde occidental à l'IRAQ (Armes de destruction massive qui n'ont jamais existé) ?



R : Dans sa réponse l'orateur a fait comprendre que rien n'est sûr concernant l'implication directe et officielle du gouvernement de Pyong-yong. Et de rajouter une opinion personnelle dans laquelle il laisse entendre qu'il croit vraiment que la Corée du Nord a orchestré ce hacking.

Q : Sony a-t-elle évalué l'impact financier qu'a provoqué cette affaire ?

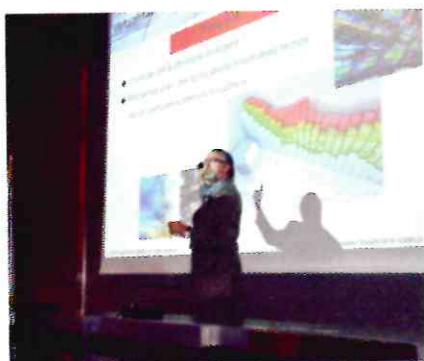
R : M.Bruce a dit qu'il n'a pas de détails ou d'éléments de réponse à fournir sur le point financier. Bien que SONY a publié des chiffres qui lui semblent ridiculement en deçà de la réalité.

## « La protection du Cloud et de l'infrastructure virtuelle »

M. Hafed BENHAMIDA

L'orateur s'est focalisé, dans un premier temps, sur la sécurité du Cloud. Il a présenté les bonnes pratiques du CSA (Cloud Security Alliance) liées à la protection du Cloud telles que celles édictées pour la sécurité des réseaux, du matériel ainsi que les stratégies de contrôle déployées pour protéger les données, les applications et les infrastructures associées au Cloud Computing.

L'orateur a également, démontré comment un problème de sécurité dans une plateforme sur le Cloud peut engendrer une perte économique ou une mauvaise réputation pour l'entreprise.



Dans la deuxième partie de sa communication, il a présenté quelques outils permettant de gérer et de surveiller l'ensemble d'une infrastructure virtuelle depuis un emplacement central, de réduire le temps de provisionning des nouveaux serveurs et d'allouer des ressources informatiques partagées avec plus de flexibilité. Il a aussi énuméré les techniques permettant la surveillance, la visibilité des opérations et l'optimisation des capacités afin d'améliorer l'utilisation de la capacité et les ratios de consolidation tout en réduisant les coûts matériels et le temps nécessaire au diagnostic et à la résolution des problèmes.



Un débat animé par M. Abderrafiq KHENIFSA propriétaire d'un magazine IT à parution hebdomadaire «It-Mag» et modérateur rompu aux questions et débats IT.

Le thème choisi pour cette table ronde est :

## « Comment convaincre votre hiérarchie pour investir dans la sécurité informatique ? »

Comme le veut l'objectif de cette table ronde plusieurs questions ont été posées et ont eu à chaque fois des réponses groupées, fournies par l'ensemble des conférenciers. Chacun a, à sa manière, répondu pour enrichir au maximum les réponses données et être à la hauteur des attentes de ceux qui l'ont posées.

Une reprise synthétisée de quelques questions est présentée ci-après :

**Q1 : M. KHENIFSA :** Sur le cyber space pouvons-nous faire confiance ou non, ou simplement-dit est ce que nos systèmes d'information sont sécurisés ou non ?

**M. BENCHERAIET :** La sécurité totale n'existe pas, donc nous ne pouvons pas faire entièrement confiance aux dispositions mises en place pour la sécurité des Systèmes d'Information.

**M. CAGNONI :** Nous devons savoir quels sont les risques pour choisir les bonnes mesures à mettre en place. Ensuite il faut sensibiliser et être attentif aux menaces.

**M. OUYAHIA :** La sécurité absolue n'existe pas, mais nous devons faire confiance, à un certain degré, sinon nous déconnectons tous nos systèmes du réseau et d'Internet ce qui est impossible. Nous devons continuer à faire des efforts de sensibilisation, de promotion des compétences et des efforts en matière de législation.

**M. EL MIR :** La sécurité est inversement proportionnelle à la confiance. Ces deux concepts sont intimement liés. De ce fait, la confiance joue un rôle prépondérant dans le choix des mesures sécuritaires à mettre en œuvre.

**M. BENHAMIDA :** Il faut d'abord savoir que le risque est fonction de trois éléments : le produit à protéger, la vulnérabilité et les menaces. A défaut de biens à protéger et de menaces persistantes, on parle de Zéro risques.

**Q2 :** On parle de sécurité dans plusieurs domaines. Est-ce la sécurité internet, celle des infrastructures, des systèmes, des données, etc... Pouvez-vous nous éclairer ?

**M. CHIOFALO :** Il ne sert à rien de sécuriser les infrastructures si on laisse les bureaux d'une entreprise ouverts aux étrangers. Donc, on parle de l'ensemble : les utilisateurs, la donnée, les infrastructures et les systèmes. La sécurité est un concept global.

**Q3 :** Comment convaincre un décideur pour investir dans la sécurité SI.

**M. BENCHERAIET :** Pour ce faire, il faut aborder avec lui le volet financier, voir les coûts et convaincre ce décideur du retour sur investissement lié à la mise en place des mesures de sécurité.



Aussi, informer le décideur sur des incidents survenus dans d'autres entreprises exerçant dans le même domaine constitue un moyen efficace de persuasion.



**Q4 : Comment convaincre le décideur pour réinvestir dans la sécurité ?**

**M. BENHAMIDA :** C'est l'analyse des risques quantitatifs ; elle est certes, difficile à réaliser mais elle est indispensable et c'est la raison pour laquelle elle est définie dans la norme ISO 27005 et ISO 27001 portant « Risques Management » qui exige l'analyse des risques. Cette analyse n'est pas figée, elle est cyclique. Toutes les trois années, on se doit de la refaire pour redéfinir les besoins. Et ensuite, il faut adapter l'outil selon le besoin.

Un bon manager de sécurité est un manager qui aide son entreprise à faire du chiffre, à produire... donc chaque Dinar doit faire l'objet d'une analyse ; c'est comme ça qu'on peut convaincre un décideur.

**M. OUYAHIA :** Quand on investit dans le domaine de la sécurité c'est comme si on investit dans une police d'assurance. On investit pour éviter de perdre de l'argent pas pour en gagner. C'est difficile de démontrer cela à un décideur, car il ne voudra pas investir s'il ne voit pas la nécessité de le faire.

**M. BENCHERAIET :** Il faut expliquer aux décideurs que la sécurité n'est pas un produit, c'est un processus.

**Q5 : comment s'assurer que les solutions acquises par les entreprises et les institutions Nationales de souveraineté (sachant que nous en sommes à 100% consommateurs) sont dignes de confiance et qu'elles ne comprennent pas un cheval de Troie ou autres programmes malveillants et qu'elles ne sont pas raccordées au gré et à la volonté des fournisseurs de solutions ?**

**M. OUYAHIA :** Il faut savoir tout d'abord, que cela dépend de la technologie utilisée. En ce qui concerne le chiffrement, il existe des méthodes qui permettent plus ou moins de vérifier que le cryptage se fait de manière convenable.

Aussi, il faut savoir qu'en théorie lorsqu'on prend un bloc d'informations et qu'on le chiffre avec une solution propriétaire au moyen d'une clé spécifique, on devrait avec une implémentation, même si elle s'avère lente, obtenir le même message chiffré octet par octet.

Pour les autres solutions à l'instar des pare-feu, c'est compliqué de s'assurer du degré de confiance à placer dans les solutions.

**Q6 : Comment pourrait-on gagner la confiance des collaborateurs ? N'est-il pas opportun de penser à une politique de motivation de la ressource humaine, pour en tirer plus d'avantages en matière de sensibilisation ?**

**M. GERARD :** Les facteurs de motivation sont importants certes, et il convient de noter en ce sens, que ces facteurs diffèrent d'une entreprise à une autre et d'un projet à un autre.

Cependant, il importe de noter que l'engagement du management est en soi un facteur essentiel et non négligeable en matière de motivation du personnel.

Egalement, il faut donner envie à la RH, pour qu'elle s'implique pleinement.

**Q7 : Le cyberspace. Est-il sécurisé ou pas ? Peut-on faire confiance ou pas ?**

L'ensemble des conférenciers se sont mis d'accord sur le fait qu'un niveau de sécurité garanti et absolu reste inatteignable.

Cependant, il est nécessaire d'avoir en soi un certain degré de confiance, car à défaut il faut se déconnecter du monde numérique.



Q8 : Par rapport au système SCADA et d'une manière générale, aux systèmes de télé-conduite isolés, déconnectés d'Internet ; Peut-on dire qu'ils sont en sécurité ?

Et à quel moment peut-on dire qu'un réseau est prêt à être connecté en toute sécurité à Internet sachant que les SCADA vont migrer vers le protocole IP ?

**M. EL MIR :** L'évolution technologique est telle que nous ne pouvons que suivre ou être rejétés.

Dans ce sens et en relation avec le système SCADA, il y a une évolution technologique qui doit se faire pour pouvoir interconnecter ces systèmes-là.

A noter que les vulnérabilités qui le caractérise, actuellement, peuvent mener jusqu'à son arrêt total, voire l'arrêt, le dysfonctionnement ou la destruction du réseau et/ou des infrastructures qu'il gère.

On aura, à terme, besoin de connecter le système avec l'ERP, avec des applications métiers et là, la menace sera globale. Et nous ne pourrons que suivre.

**M. SEBASTIAO :** Il y a lieu de savoir qu'une machine qui n'est pas connectée à un réseau ne signifie pas forcément qu'elle est sans risque. Ex : cas du : STUXNET qui a contaminé les ordinateurs et la centrale nucléaire de Bouchehr (IRAN), bien qu'ils n'étaient pas connectés.



## CLÔTURE

M. Kamel GHEBOUB, Directeur Sécurité des Systèmes d'Information a salué l'assistance et tenu à remercié l'ensemble des collaborateurs d'ELIT.

« Ce que je retiens, c'est cet esprit de solidarité, cette confiance, cette entraide, ce dévouement qui ont caractérisé les préparatifs de cet évènement ».

Les conférences et les Workshops ont été cloturés avec ce mot de M. Gheboub et la remise du cadeau à M. Meftah BAKOUR, un des participants qui ont honoré ELIT de leur présence et vainqueur du quiz.

Pour rappel, ce quiz est composé d'une série de questions en relation avec les thématiques présentées lors des conférences ainsi que d'autres d'ordre général sur les technologies IT.



## LA NUIT DU CHALLENGE 'CAPTURE THE FLAG'

A 20h00, et dans une ambiance conviviale, voire familiale les compétiteurs, hôtes d'ELIT, ont annoncé tous ensemble, avec le Président Directeur Général d'ELIT, le commencement du challenge.

Le coup d'envoi du challenge tant attendu par les organisateurs que prisé par les compétiteurs a été donné, et a mis aux prises, sept équipes d'« Ethical Hackers » à savoir :

Hackliss	M'hamed naceredine BELHOUCINE Youcouf MEZARI Said ARAB Mohamed KRIM
Phantom	Zakaria BRAHIMI Tarek IDRES Mustapha BELLAL Amine BADAOUI

Sudo	Zakaria AROUI Ismail CHERIFIYOUSSEF Abdesselam GUERROUDJ
Th3jackers	Omar LAHBES Abderraouf BOUTHIBA Hakim DRAI Aymen KHENNACHE Abderrahmane OURAB
The Jouney	Akila BOUGUERRA Khaled el mehdi REBAH MOHAMED
T.I.T	Emir Fares BELMAHDI Hamza TAHMI Hani BENHABILES Brahim Fouad GUIA Hamza BENSMAIL
Goliath	Salaheddine BEALGGOUN Nassim CHAKROUN

## Fait marquant du « CTF »

Enfant prodige ou Génie précoce ?

Quel qu'il soit le qualificatif accordé, Rabah Khaled EL MEHDI a été bel et bien présent, comme compétiteur au CTF et prenant pour coéquipière sa maman dans l'optique d'aller le plus loin possible dans cette compétition.

Ce qui est marquant c'est, une fois de plus et à travers ce jeune adolescent de 14 ans, que l'on vient à confirmer combien regorge notre patrie de compétences et de potentialités fortes dans tous les domaines et à toutes les catégories d'âge.



### Déroulement du challenge

Etalé sur toute la nuit, le « CTF » a permis aux équipes de s'affronter, avec la ferme volonté de chacune d'elle de remporter le challenge.

A noter que ce challenge a été agrémenté par des cadeaux au mérite des lauréats.

### Les scores tout au long de la nuit

Equipe	23h30	03h30	06h00
T.T.T	528 pts	928 pts	1596 pts
Hacklish	156 pts	408 pts	1020 pts
Th3jackers	156 pts	623 pts	977 pts
Phantom	0 pts	205 pts	406 pts
The Jountey	108 pts	108 pts	159 pts
Sudo	0 pts	152 pts	152 pts
Goliath	0 pts	0 pts	0 pts



**ÉLIT** الهندسة المعلوماتية للأذربيجان  
El Dzair Information Technology

1011011010101

DZ  
**HACKEVENT**

09 mai 2015

Centre de formation Sonelgaz  
IFEGB - Ben Aknoun - Alger

01010110011010101110

1011011010101  
1001101010101010

110  
01110  
10010001101011110

101110001010111

01110  
10011010101110

01010110011010101110