REPORT

FG BENIN
Forum sur la Gouvernance de l'Internet

5eme Forum sur la Gouvernance de l'Internet au Bénin

16 & 18 juin 2016
Cotonou - BENIN

"La Sécurité des infrastructures & des individus sur Internet"

ICANN · iGFSA Internet Governance Forum Support Association · Internet Society · @betic TIC au service du développement · BENIN TELECOMS

be. Fixe - Mobile - Internet

PBEF · IT-num

f : Forum sur la gouvernance de l'internet au Bénin
Tél : +229 6309 4066 / Email : bureau@fgi.bj /www.fgi.bj

5th Benin Internet governance Forum

Theme: "*Infrastructures & endusers security on Internet*"

The fifth edition of the Internet Governance Forum in Benin took place in two phases namely, a pre-conference with the private sector and a forum with all stakeholders in Internet governance ecosystem in Benin. Both activities were organized by the office of Internet Governance Forum in Benin (IGF Benin) under the patronage of the President of the Association of Banks and Financial Professionals Institutions (APBEF Benin) for activity that mobilized the private sector. These events were respectively held on June 16 & 18, 2016 at Novotel in Cotonou and in the conference hall at Benin Telecoms SA.

Lunch discussion of June 16, 2016

On Thursday, June 16th, 2016 was held at Novotel in Cotonou the private sector's meeting organized in the framework of activities of the national Internet governance forum in Benin. The meeting was chaired by the President of the Association of Banks & Financial professionals Institutions in Benin. It was an opportunity to make two presentations followed by discussions on the main theme of this edition of the IGF which is: « **Infrastructures and endusers Security on Internet** ».

Two introductory interventions marked the official opening ceremony of the event before the presentation of communications.

➔   **The phase of the opening ceremony**

 At the beginning of her speech, the president of the IGF.BJ welcomed the participants and wished that they actively take part in exchanges in order to enable the IGF.BJ to collect specific concerns to be used for advocacy.

She encouraged them to inform the public on activities carried out for preserving the trust of their monetary services users by credit cards, mobile phones and internet.

As for the president of APBEF, he welcomed the relevance of the IGF 2016's edition theme. He notified that digits are in the heart of data used by banks. He acknowledged that banks are increasingly concerned by the security of infrastructure and enduserson the internet. It is a major issue for the sustainability of banks actions in Benin. The establishment of an adequate legislative

framework is important to locate the responsibilities of actors. The importance of activity resumption plan is also acceptable. Then he declared open the meeting of the private sector as part of the fifth edition of the Internet Governance Forum in Benin.

➜ **The phase of speech delivery**

From Jacques HOUNGBO's speech, some strong ideas deserve to be highlighted. They are related to the following:
Malicious acts are increasingly organized. All countries that have successfully reduced malicious acts have built the capacities of all stakeholders. Malicious acts have become a cancer. Many countries have set up tools and actors to control the actions of the perpetrators. There are several sites whom host malware in Africa. We are not entirely protected. There worms on our banking networks. The IGF suggests the clean-up of the whole environment. To that effect, it can help to establish protection tools for bank resources.

• **From Djalil ASOUMA's communication**, the key elements are the following:

The cyber war has started for several years now. We have not yet reached any import digitization level in Benin but we'll get by 2020. In Benin cyberspace, the customer experience will make a difference among banking companies. We should bear in mind that security challenges will be significant. The level of positioning chief information officer (CIO) or chief security officers (CSO) or people in charge of securing the information system (RSSI) should more and more head towards the Top Level Manager. We shall talk more about cyber security because we are entering a global digitization space. The hacker increasingly acts form the inner part of information system. There are three fundamental goals to reach: confidentiality, availability and the integrity of information. These three goals are important and will be simultaneously aimed. Let's keep them as the security goals. These goals are based on the trilogy of profit, risk and loss. Their impacts are increasing in the digital world. Security is primarily a matter of growth in business. Security is not just about technology, it is integrated in business growth strategy. Security faults must be corrected. Without security policy, repression

is unsupportable in case of fault. Business continuity is pillar of security. By 2020, a large population will be under digital influence.

➔ **The phase of debate followed by lunch**

At the end of the communications, an open debate enabled to share experiences and questions whose substance is as follows:

Among questions are:
- What are the tools and means for improving security on internet?
- How do we reduce the risks?
- What measures are put into place at national level to filter national information?
- Is there an authority that regulates security in Benin?
- May the IGF help to set up legislative tools?
- When will the law on electronic signature be voted in Benin?

Among experiences shared:
- Security call on reflexes. The fact of displaying for instance, LEPI data is already a personal data security problem. Just using a USB key in a conference to expose oneself to the risks. IGF office is invited to continue to mobilize all the stakeholders on cyber security issues.
- When we publish breaches of national big organizations' security, we shall know. It is through information sharing that we shall know the security threat.
- There was also a sensitization campaign on the adhesion to the DSI club in Benin that brings together all DSI from public and private sectors in order to share national experience on IT issues.
- There is a nice initiative of the Central Bank to force banks to observe the security levels. Also, the central bank organizes the evaluation of bank shares.
- In Benin, operators and internet services providers are not allowed to do filtering on internet. Operators do not have the right to trace the contents that pass on the internet. The related devices are to envisage at the legislative level.

- We do not invest enough in technology. There are some cases of data copy in some banks in Benin. We must say that it is an entire chain.
- There is the need of telling the truth about the faults observed in information system.
- We often appoint people who are good at techniques but do not have enough capacity for leadership position at decision making level. It would be useful to review the positioning and collaboration between IT managers and decision makers to discuss IT in terms of profit.
- To ensure good security, there is the need of support from public sector. Physical attacks are also frequent in Benin. When talking about IT and its cost, it is a major concern for decision makers. General expenses have seriously increased in the past twenty years. Sometimes, there is communication problem between technicians and banks leaders but the bridge is being created between them.
- There are scanners that bad people use to scan data entered by money distributors.

Before the lunch offered to participants in this meeting, a communication opportunity was given to Benin Telecom SA to talk about internet offers that are marketed to big companies.

Were present ::

APBEF
Banque Atlantique Bénin
BCEAO
BE TÉLÉCOMS SA
BENIN TÉLÉCOMS SA
BGFIBANK BENIN
CBAO
CCEI BANK BENIN
CCIB
Conseil Économique & Social
CIPB

DIAMOND BANK-BÉNIN
E-MONEY
FLUDOR BÉNIN
MOOV
MTN
ORABANK
Société Général Bénin

The FORUM of JUNE 18, 2016

On Saturday, June 18th, 2016 in Benin was held in Benin Telecom Infrastructures SA conference hall, the fifth edition of National Internet Governance Forum. Have taken part all actors of internet ecosystem in Benin. It was enhanced by the effective presence of the vice President of the National Assembly and the vice President of ICANN for Africa. It took place in several phases namely: the opening ceremony, speech delivery, committee/group work and general debate.

The opening ceremony
The opening ceremony was marked by the welcome note of the President of IGF.BJ and the opening speech of Vice president of ICANN Africa. Related documents are attached to this report.

Presentation of communications.
Four communications were presented during this forum and are appended to this report. The synthesis of key information for each of them is as follow.

The first communication: national cyber security

There is a lack of statistical information on cyber security at national level. It is useful to have an observatory for the combination of statistics.
The more a country has a high penetration rate, the more it is exposed to cyber attacks.

In Benin, there is a law on the protection of personal data that highlights cybercrime. Many laws should be voted on it.

In terms of organizational structure, there are CNIL, ARCEP, HAAC, central office for cybercrime. There is a need of setting up a national coordination framework among those stakeholders.

Critical infrastructures are, the Financial Ministry datacenter, the ACE cable, the SAT3 cable, internet exchange point (BENIX), the GOUV.BJ. Infrastructures security is not coordinated. We should work together to be protected against attacks. The sites on dot BJ have at least a vulnerability. After a study, the communicator has demonstrated the existence of critical security fault on many website hosted or not in Benin. He recommends the establishment of a security fault resolution mechanism. The studies conducted by e-benin project for setting up a response centre for nonprofit computer incidents should also be reviewed.

The second communication: digital security in company

All companies using internet and digital data are the heart of their operation. When talking about the security of information system, we seek to ensure the authenticity, confidentiality, integrity, the availability of data and infrastructures. Digital security also includes the protection of company's property, either digital or not. The threats of Information Systems are especially, attacks to the availability of systems and data, illicit use of the system or network, the use of compromised system to attack other targets and stealing equipments.
The sources of the threats are either human nature or related to natural disasters.
To act, we must manage the user access rights. We must separate the privileges. We must impose to users to authenticate themselves with centralized antivirus updates. We must establish intrusion detection system. One must know its network and quantify the risks. We must put in place IT security policy and manage incidents. Set up back up in order to manage activities taken. It is important to take measures in order to deal with the threats.

Briefly, the weak link of critical infrastructures security and digital security in companies is of human origin.

The third communication: endusers' security on internet

Security makes think of a possible threat to prevent. Digital revolution has become a reality in Benin. The development tool which is internet is also used to harm the victims. There is endusers insecurity on the net. There is for instance the blackmail video. Blackmails are numerous and make the victims waste money. There are false scholarships online. The damages are in the order of several million of local money according to the kind of infraction. There are intrusion attacks, by unauthorized access, by alteration, by sabotage, by destroying the database, information system, operating system. 87 % of attacks are carried out using computer tools as the means of action.

It is advised to change passwords every 90 days. Avoid using the same password for accounts on all platforms. Install on computers antivirus and reliable firewall.

The security measures set up by the state are mainly:
- The law on the protection of personal data;
- The law on corruption that is used to deal with cybercrime issues;
- The code of electronic communication and mail in Benin.

Combating strategies were set up in 2005 in Benin with the establishment of an anti-cybercrime brigade. In 2009, an anti-cybercrime committee was established. Afterward there was the establishment of an office for combating cybercrime. The office works with internet service providers.

The fourth communication: the contribution of IPv6 and DNSSEC to the security of infrastructures and endusers on internet

Security has become a necessity, an obligation with the proliferation of risks. With IPv6, we can easily identify the sources of the attacks. IPv6 enables to ensure the encryption from one to the other.

DNSSEC enables to certify the validity of the host address. In case of DNS resolution, it enables to exchange with the authentic host. The DNSSEC does not encrypt information. It contributes to the credibility of trust on internet. It reduces some risks of attack.

Benin DNS Forum is a forum organized in partnership between IGBANET and ISOC Benin. It helps to create an exchange framework on the DNS. It aims at organizing trainings on the importance of the DNS in promoting the dot BJ.

Following communications, commission works took place.

Participants were divided in workshop in order to make suggestions of reform to undertake in term of security. At the end of the works, the following syntheses have been retained:

At the workshop on infrastructures' Security on internet

Wherever, IT Security has evolved, there was a strong leadership with an appropriate institution anchorage. Critical internet infrastructures and of energy were listed with proposals of actions to undertake. It is recommended to hold a national meeting on internet infrastructures' security in Benin. It is foreseen to have a national authority in charge of internet security under the responsibility of the Head of state. Studies conducted by e-benin project should be implemented. Review the training curricula in Benin universities in order to better build the capacities of the stakeholders.

At the workshop on digital security in company

It is recommended to ensure the certification of information system in Benin. There must be Security Policy in companies. We must raise the staff's awareness and set up business continuity plan in case of disaster.

At the workshop on endusers Security on internet

It is recommended to ratify ECOWAS and African Union's guidelines on cybercrime in Benin. Vote law on cybercrime. Encourage the systematic use of dot BJ for administrative communications. Systematize internet and IT patent in schools and universities. Encourage companies to adopt security protocols.

General comment

It is planned to make available a white book containing the proposals made during this forum in order to encourage the stakeholders of the ecosystem to implement the suggestions made. This white book will be forwarded to the government and the National Assembly, and will be published by press.

For achieving this, the participants wished to continue the work online in order to get a digestible and applicable document. An advocacy with executives is also planned in order to have concrete actions.

At the end of the general debate, the final release of the forum was read before taking the group photo and the sharing of the closing meal. The present release is here attached.

ANNEXES

COMMUNIQUÉ FINAL

Nous, les participants au cinquième Forum sur la Gouvernance de l'Internet au Bénin (FGIB), en collaboration avec les autres parties prenantes de l'écosystème de l'Internet au Bénin.

Rappelant :
- Que lors du quatrième Forum sur la Gouvernance de l'Internet au Bénin en 2015, une association dénommée « FGI Bénin » a été mis en place pour conduire et suivre les activités du forum sur la gouvernance de l'internet au Bénin ;
- Que l'organisation du Forum sur la Gouvernance de l'Internet est une action conduite par des bénévoles de l'écosystème de l'internet dans chaque pays ;
- Que l'internet est un espace ouvert et devrait le rester au profit de tous les multi-acteurs de la gouvernance de l'internet ;
- Qu'il s'agit du cinquième Forum sur la Gouvernance de l'Internet au Bénin, FGI Bénin 2016 ;
- L'engagement des multi-acteurs à tenir effectivement et régulièrement un Forum national annuel sur la Gouvernance de l'Internet au Bénin ;

Convenons :
- Que la sécurité laisse penser à une éventuelle menace à prévenir ;
- Que les origines des menaces sont soit de nature humaine ou liées à des catastrophes naturelles ;

- Que lorsque la progression de la pénétration de l'internet est acquise, elle s'accompagne d'un niveau élevé de risques d'attaques sur internet ;
- Qu'il y a nécessité de prendre des mesures pour faire face aux menaces qui adviennent au niveau national ;
- Qu'en matière de sécurité du système d'information, il faut assurer l'authenticité, la confidentialité, l'intégrité et la disponibilité des données et des infrastructures ;
- Qu'au regard des expériences vécues, le maillon faible de la sécurité des infrastructures critiques et la sécurité numérique en entreprise est d'origine humaine ;
- Qu'il y a nécessité de mettre en place un cadre national de concertation des acteurs en charge des questions relatives à la sécurité sur internet ;
- Qu'il est nécessaire de déployer en urgence au niveau national, l'IPv6 et le DNSSEC pour améliorer la sécurité des infrastructures et des individus sur Internet et faire la promotion de l'usage du « .bj » par les béninois ;
- Qu'il faut sécuriser l'accès aux ressources criques de l'internet notamment, le .BJ, le IXP, le backbone national d'accès internet, le câble SAT3, le câble ACE et le cache google ;
- Que pour impacter la communauté, les participants ont travaillé en commission et ont formulé des propositions d'actions contenues dans un livre blanc à soumettre au gouvernement et à la représentation nationale.

Remercions pour l'appui technique, financier et logistique apporté à l'organisation de cette édition du Forum sur la Gouvernance de l'Internet au Bénin :
- Le Gouvernement du Bénin ;
- ISOC Bénin et Internet Society (ISOC) International ;
- ICANN ;
- Benin Télécoms Infrastructures SA ;
- Bénin Télécoms service SA ;
- IGF support Association ;
- l'Association Professionnelles des Banques et Établissements Financiers du Bénin (APBEF) ;
- l'Agence Béninoise des Technologies de l'information et de la Communication (ABETIC).

Remercions les participants au cinquième Forum sur la Gouvernance de l'Internet au Bénin (FGI Bénin 2016) pour leur disponibilité ;

Remercions les hôtesses et les communicateurs pour leur appui et disponibilité ayant permis le bon déroulement des travaux du cinquième Forum sur la Gouvernance de l'Internet au Bénin.

Fait à Cotonou, le 18 juin 2016.

Vue partielle des participants

DISCOURS DE BIENVENUE PRESIDENTE FGI Bénin

Mesdames et Messieurs,

- Les représentants du secteur public,
- Du secteur privé,
- Des acteurs techniques,
- De la société civile,
- Du secteur académique,
- Des organisations internationales,
- Cher(e)s Participantes et Participants,

Bienvenue dans cette salle de conférence de Bénin Télécoms. L'un des fidèles sponsors du Forum sur la Gouvernance de l'Internet au Bénin avec ISOC, ICANN, IGFSA.

La sécurité des biens et des personnes sur internet est un sujet brulant d'actualité au plan international. Mais au Bénin, rien ! Personne n'en parle vraiment, en tout cas pas publiquement. C'est un peu comme si le pays était en dehors du cyber danger.

On oublie que les incidents de sécurité sur internet ne sont découverts que longtemps après qu'ils aient commencé, un peu comme l'hypertension ou le cancer. Et que contrairement à ce qui se passe dans la «vraie vie », le voleur a eu largement

le temps de sévir avant que le gendarme ne commence à lui courir après. L'intérêt des échanges de ce matin c'est de poursuivre ce que le FGI Bénin a entamé depuis plusieurs années, à savoir : œuvrer pour un internet de qualité ! Et cette qualité implique aussi un usage sécurisé.

Au fait, une petite question :

Q > Beaucoup d'internautes ont au moins 2 terminaux (smartphone et tablette) en plus de leur PC. Combien de personnes ont un antivirus sur les terminaux (smartphone et tablette) ?

Encore une autre question :

Q > Combien de personnes ont des mots de passe différents sur chaque terminal et pour son compte email et ses réseaux sociaux ?

Les réponses à ces questions sont des indications sur la responsabilité de l'individu pour ce qui est de sa sécurité dans le monde du numérique. Tout le monde sait aujourd'hui que c'est un marché planétaire et tout le monde sait que lorsque l'on s'aventure sur un marché, il y a un minimum de dispositions à prendre pour se protéger et protéger ses biens !

Mais ceux qui nous offrent des services dans ce monde du numérique ont aussi leurs responsabilités, elles ne sont pas uniquement individuelles. Il y a plusieurs SIG dans l'administration publique. Mais on entend très peu l'administration publique a sujet de la sécurité de l'information.

Les fichiers des impôts, ceux de la fonction publique, la LEPI, etc. Il y a quelques années, un petit bug a donné quelques indications : des professeurs d'université n'ont pas eu leurs salaires parce qu'une application les avait mis d'office à la retraite ! Combien de cas intentionnels de ce style sévissent actuellement ?

Que fait-on pour s'assurer qu'il n'y a pas de virus colporté et distribué par tous les « transitaires » qui s'affairent autour des déclarants en douane. Combien d'entreprises ont des antivirus à jour sur leurs PC ? Combien d'entreprises utilisent des versions authentiques de logiciels ?

La sécurité de l'information, c'est un peu comme une question de santé publique ; la sécurité de tous repose sur l'hygiène observée par chacun. Il faut que chaque entreprise assainisse son environnement pour éviter que l'économie du pays ne soit indexée comme zone « insalubre », zone avec laquelle on ne peut faire affaires qu'en portant des « préservatifs » en kevlar ! Zone dont on black liste les adresses IP. Il faut que chaque utilisateur de smartphone, tablette, ordinateur comprennent que sa responsabilité est engagée.

Voilà ce sur quoi porteront nos échanges aujourd'hui. Je vous remercie d'avoir fait le déplacement en ce samedi matin. Je vous souhaite un FGI Bénin 2016 des plus intéressants et des plus productifs.

Numériquement vôtre !