OFFICIAL OPENING CEREMONY OF CARICERT

Speech Mr. J.D. De Canha
20 March 2012

Honorable Minister, Mr. Charles Cooper
Members of the Media,
Dear guests,
Ladies and Gentlemen,

The minister already told you about the background of the foundation of a CERT in the Caribbean area. Today we are celebrating the opening of CARICERT and I would like to point out a few issues about the operational aspects of it.

A CERT is not just an office with some security specialists in it,…monitoring the threats coming from the Internet. It is an institution which has to comply with international standards, set by the CERT-community worldwide.
Standards concerning techniques, procedures, monitoring, tooling, knowledge and trust. About trust, I will elaborate later on.

Today is the day that I have been looking forward to for months. (A brief Historical preview of the activities carried out for establishing the CARICERT in Curacao).
We at Bureau started this CARICERT effort in 2008 when the Minister of the Telecommunications, Mr. Maurice Adriaens instructed BT&P on July 24th 2008 to investigate the possibility to start with an own national CERT. This was a result of the CTU meeting in 2008 that was hosted in Curacao by BT&P.
In early 2009 we approached international consultants in this matter and on March 17th, 2009 we had the initial discussions with mr. Roeland Reijers and the GOVECERT in Holland.

On July 30th 2009 we signed the first offer to start the organization of the national CERT in Curacao. During 2010 Bureau Telecommunication and our consultant "Roeland Reijers" deployed a lot of work to establish this CARICERT effort. This resulted in that on November 16th 2010 we signed a joined venture agreement (protocol) with the GOVCERT of Holland to help CARICERT in Curaçao with the organization, know-how and expertise.

On December 1st 2011 we started with the implementation of the CARICERT and this resulted that today March 20th 2012 we officially inaugurate the CARICERT which is now fully operational.
This effort took us over 3 years to come to this point that we have today. I would like to thank Mr. Roeland Reijers and the team of experts that have contributed to this endeavor because it has been a great effort to find professionals to work in this CERT, to meet up to the standards of physical and digital security, to draw the work processes of prevention, detection and incident handling and to purchase the right tools and equipment.

However, we must take time to let CARICERT grow and be able to offer all the services a CERT should offer. We can not do this in one day. We have to prioritize the activities of this CERT.
Worldwide, there are four (4) main tasks for a Cyber Emergency Response Team.
These tasks are: 1. Prevention, 2. Detection, 3. Resolution of incidents and 4. Advice on cyber security matters.

From tomorrow on, CARICERT will start offering services with regards to the first two tasks.

Which are they?

1. First of all CARICERT focuses on prevention. It will provide information, training and all that is needed for its constituents to prevent being the victim of cyber attacks, hacking or disruptions coming from ICT. To do that, CARICERT has insight in the systems the constituents work with and can provide them with the specific information they need.

2. Secondly, CARICERT will focus on detection. Detection means that CARICERT registers cyber related incidents, in order to be able to analyze them, get insight in techniques, trends and upcoming threats and improve prevention. To do this, we use Taranis, a tool made by one of CARICERT partner-CERTs, NCSC in the Netherlands.

3. Later this year, CARICERT will start her incident response, a very essential and important CERT-service. This means that CARICERT is the single point of contact for the Caribbean area when it comes to cyber related incidents. Once an incident is reported and it effects more then 1 constituent – or it may even effect society as a whole- CARICERT will coordinate the handling and if possible the solution of it.
I want to emphasize that CARICERT's security officers will coordinate the handling of incidents on a larger scale when they form a threat to the stability of vital sectors.

Last but not least, CARICERT will offer tailored advice to constituents. It might take some time to get there, as this is very time consuming. But in the end, a constituent must be able to get advice in specific situations when it foresees a threat or disruption.

I am talking about constituents, who are they?

Constituents is another word for participants in the CERT-world. These organizations can come from all sectors and are part of the structure of CARICERT.
They share information, they exchange ideas and solutions, and they meet on a regular basis. They are the main target group for CARICERT.
However, CARICERT will share relevant information with others too. To do so, it will mainly use the website Caricert.cw. On this site CARICERT will publish surveys, reports, alerts and other publications. Information about threats specifically for constituents will not be made public.

Concept relationship CARICERT and BTPU:

I was talking about trust. This is a key word when it concerns cyber security. By sharing knowledge and incident information, constituents open up to each other, not bothered by the fact that they are competitors in the same markets. Cyber security is an issue with national impact and that makes the need to be open and trustworthy even more important. CARICERT is part of a trusted community, nationally and internationally.

Also I want to talk about another kind of trust. CARICERT is situated on the premises of Bureau Telecommunicatie and Post, a regulator. This does not mean that all information will be shared with BTPU.
CARICERT is independent when it comes to its knowledge of incidents and constituents. When an incident with national impact happens, the head of CARICERT will inform me.

But CARICERT officers will not give further details about the parties involved, systems involved or the exact losses they suffer. CARICERT will give me the information I need to take action or probably to be able to adjust or create cyber security policy. That is where the information stops. We call it a Chinese wall. I think it is important to emphasize that we built this wall.

And finally, about trust: we have to work to establish and maintain the trust in Internet as a safe and efficient way to work, to shop, bank and communicate. This is also one of the aims of CARICERT: to create awareness among the general public about cyber security. You will hear from this initiative later this year.

I have given you a lot of background information. It all comes down to the fact that we work very hard to improve the quality and the integrity of the Curacao Internet infrastructure and we have succeeded in that. Now, we have come to the point that we have to realize that cyber-security is of utmost importance for Curacao and the Caribbean economy and society.
Today we make a promising start with CARICERT. I hope in a year from now you can see the results. Or actually, I hope you do not, because if CARICERT works well on prevention and awareness, no cyber-related incidents will happen in or coming from the Caribbean area!

Thank you for your attention.