IGF Best Practices Forum on "Establishing and Supporting CERTS for Internet security"

Report 5. Tooling

Note. This report joins the comments on the online forum. As there were distinctive topics that were discussed, they are presented separately. Entries are presented in the order of arrival. First the contributor is mentioned and where appropriate within brackets the person responding to is mentioned, e.g. (Wout). The affiliation of a respondent is not mentioned, as he/she may be giving a personal point of view or not. As consultant to the group this is impossible and not necessary to ascertain.

Jerome Athias (on Wout)

You could be interested by the survey in this report


Sylvain Baya

I'm sure that I've missed much on passed discussions about this important WG main topic: "Establishing and supporting Computer Emergency Response Teams (CERTs) for Internet security". But I just want to mention a good existing toolkit for beginners: Cert-In-A-Box. Many thanks to the Dutch CERT | govcert.nl

http://www.first.org/assets/resources/guides/cert-in-a-box.zip

<quoted> CERT-in-a-box

NCSC-NL (National Cyber Security Centre of The Netherlands)

The project 'CERT-in-a-Box' and 'Alerting service-in-a-Box' is an initiative of GOVCERT.NL/NCSC to preserve the lessons learned from setting up GOVCERT.NL and 'De Waarschuwingsdienst', the Dutch national Alerting service.

The project aim is to help others starting a CSIRT or Alerting Service by:

- Getting them up to speed faster
- Taking the benefits and not making the same mistakes

cert-in-a-box.zip
Format: application/zip
Size: 8.42 Mb </quoted>

www.first.org/resources/guides#bp21

So, for those who needs to establish a National or Local CSIRT/CIRT/CERT I think it's necessary to begin with a toolkit like the Cert-In-A-Box; maybe it looks too old and not maintained since the
beginning.

I propose that we suggest that a open projet, if not existent, be created to update by adding new tools and options in the initial cert-in-a-box.