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

Report 3. Regional differences

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.

Maarten van Horenbeeck

One topic which we have not yet covered extensively on this list is the regional difference between how CSIRT's operate and partner with each other.

Yurie Ito, chair of the APCERT Steering Committee, contributed the attached APCERT Best Practices document, which summarizes their vision and the key initiatives they are working on in their region. Thank you Yurie and APCERT for sharing your experience.

What is happening in your region? Do you see initiatives that APCERT is developing which have worked well, or perhaps were less effective in your particular region?

Andrew Cormack (on Maarten)

It's really interesting to compare the APCERT approach with our European TF-CSIRT (http://www.terena.org/activities/tf-csirt/).

We first got together a couple of years before they did, following our EuroCERT pilot (which I managed for its last few months in 1999) which had explored providing “top-down” CERT services to academic networks in Europe. The pilot concluded that wasn’t particularly useful, because those networks already had well-established CERTs and the incidents that couldn’t be resolved within those existing trust networks were probably insoluble anyway as key systems were in one of the many unresponsive commercial networks that we had in those days.

So we went back to our wish list, removed all the ones that required permanent staff or other fixed resources (roughly the "operational" stuff), and came up with a list of things that could be done by informal collaboration among interested volunteers. That's still the basis for most of the Task Force's activities. One of the first products was the TRANSITS training course, nowadays projects include technical tools such as abuse helper and passive DNS, but also more top-down (though "top" for us is still the CSIRT community) things like accreditation and certification.

When APCERT started they drew up their own wish list and Yuri met with us to talk about it. It turned out that the two wish lists were pretty much identical, but opposite ways up! They started with the top-down operational stuff, we started with the bottom-up volunteer collaborations. We concluded
that indicated a perfect fit: each of us was starting with the stuff that the other thought was hardest. So we've been swapping experiences ever since :-) I also talked to Yuri about why I felt EuroCERT hadn't worked, and we concluded that the APCERT region was sufficiently different that they probably wouldn't run into the same challenges.

So if you want an example that there's more than one way to do CSIRT collaboration, I don't think you could find a much better one :-) 

Mirek Maj (on above)

Once again the ENISA stuff regarding this point. Few years ago my colleagues from my former organisation (CERT Polska) and myself - we have prepared the report for ENISA "CERT cooperation and its further facilitation by relevant stakeholders". It is available here: https://www.enisa.europa.eu/activities/cert/background/coop

The examples of the regional cooperation (including well evaluated by Andrew - EuroCERT) are mentioned. I believe that not too much has changed since that time and maybe "Ideas for Future facilitation of CERT Cooperation" (chapter 8 of the document) are still valid:)

Wout

Reply on regional differences.

The document we are trying to produce is also to point to potential multi stakeholder involvement concerning CSIRTs. What could be a way forward here? Let me start with a personal experience and then come to the point.

In Nov. 2010 I attended and presented at an anti-spam meeting of AfriNIC in South Africa. In response a government official from a large sub-Saharan country said: "Our national bank was under attack for 36 hours recently and there was no one in the country who knew how to deal with it. We waited till it stopped". I'll skip the part on the devastating effects on the country's payment system.

My guess is that an attack like that will have happened in many developing and developed country and that people responsible for decisions have become much more aware of cyber attacks because of attacks like this. But did they start acting on it?

Did incidents/emergencies like this give priority to CSIRTs in your country in recent years? Have CSIRTs started to appear, whether private or public? Is the topic on the national agenda?

As the discussion in this group shows, there are large regional differences here.

What I am trying to get at, is to find out how the IGF can, if and where necessary, get the topic of CSIRTs on agendas that allow the discussion on urgency, on the necessity for, the need for funding of CSIRTs and the availability of trainings, assistance and grants, etc. to start in the right places with the right people. The places where the need is high, but action insufficient so far. Where multistakeholder participation can make a difference. No external advice or training is going to help, when, either on the side of private companies or on government level, no urgency is perceived to act first. Change starts there.
To start. Is this topic worth following up on? If so, please share your thoughts on how the IGF could help after Istanbul and what the topics to raise awareness should be in your view and who/what organisations need to become involved in the debate that are missing at present in your opinion. If we can make the distinction between the initial discussion on urgency/initiative/initial funding and the need for assistance, etc., we might make a difference here.

Andrew Cormack (on Wout)

While I suspect an attack like that is probably the most immediate way to get the need for CSIRTs on the radar (compare how CERT-CC or JANET-CERT started, after all!) there are some instances where peer-pressure has helped too. And I suspect that's a lot less painful for the recipients.

Generalising hugely (hey, I was originally a mathematician) I've seen two different types of message:

a) your failure to deal with problems causes us direct problems as a "trading" partner;

b) your failure to deal with problems is causing us indirect problems by damaging the external reputation of our "sector".

Both "trading" and "sector" should be interpreted widely, because I've seen those messages used, apparently successfully, within groups of economies or in countries as well as within business sectors. So I suspect (without ever having been to one of the meetings) that this might indeed be a good message for all the groups represented at the IGF: if your peers are having more difficulty with internet security than you are, try to use your knowledge and those of your economy/sector/whatever to help them to improve.

I smile to myself that pretty much everyone's "cyber-security strategy" has the ambition of making "us" the safest place to live/trade/research/etc on-line. Positive competition to do better is fine, but the Internet is so interconnected that significant differences in cyber-security actually harm all of us. So by all means try to be a bit better than everyone else, but you'll have fewer problems if you also help them (nearly) keep up ;-)  

Jacques Beugre

I think Robert JR reflection is important in the evolution of cision or certs in different African countries.
Language is an important ban and especially for non English speaking team members.
during treatment or analysis tansmises from other teams the time to identify incidents is long because of the language.

I also suggest a good budget for the training of technicians.

I also want to give them scholarships to participate in international forum.

Maarten van Horenbeeck

One topic which we have not yet covered extensively on this list is the regional difference between how CSIRT's operate and partner with each other.

Yurie Ito, chair of the APCERT Steering Committee, contributed the attached
APCERT Best Practices document, which summarizes their vision and the key initiatives they are working on in their region. Thank you Yurie and APCERT for sharing your experience.

What is happening in your region? Do you see initiatives that APCERT is developing which have worked well, or perhaps were less effective in your particular region?