

Minutes of the 2nd meeting on September 13th, 13:00-16:00, Utrecht (NL)

ATTENDEES

AusCERT: Matthew McGlashan
CERT-FI: Johani Eronen
CERT Polska: Pjotr Kijewski
DFN-CERT: Klaus-Peter Kossakowski
GOVCERT.NL: Menno Muller (chair), Dave Woutersen, Carol Overes
NISCC: Dan Bailey, Will Alexander
SITIC: Stephen Rossi
SURFNet: Wim Biemolt, Rogier Spoor, Sjaak Schuurman
SWITCH-CERT: Peter Haag
Team Cymru: Neil Long

OPOLOGIES

- EWA-Canada/CanCERT: Ken Armstrong
- NU-CERT: Roger Safian
- KrCERT/CC: Arnold Yoon
- CNCERT/CC: Yonglin Zhou
- National Policy Agency Japan: Toshihiko Kamon
- ISS Atlanta: Peter Allor
- PRESECURE: Till Dorges
- DePaul Uni : Bill Eaheart

1. OPENING AND INTRODUCTION

Menno Muller opens the meeting thanking everyone for attending the meeting at SURFnet in Utrecht. A special thanks to Sjaak Schuurman who made it possible for those unable to attend, to have the ability to join using video-conferencing made available by SURFnet. (despite the unfortunate fact that no one made actual use of it).

2. UPDATE ON ACTION POINTS

Action point 'questionnaire' (250606.03)

One quick comment was made regarding the questionnaire that was send on the NM-SIG mailing list. It was not clear for everyone that the last questionnaire was actually the final version. This is probably why not every member filled in the questionnaire that was send on the list. Menno Muller will resend the final questionnaire on the list.

Action point 'SIG web-presence' (250606.02)

A webpage has been created by Liliana Solha. Its currently in the evaluation stage, comments are welcome on the list. Neil Long asks who is allowed to see the closed part of the website. Currently all FIRST members can see the submitted data on the closed part of the website, general consensus is that discussion on this matter should follow on the mailinglist. Maybe it would be nice to have the closed information only be available for NM-SIG-members. Action point added for Menno Muller to start the discussion on the mailinglist regarding the closed part of the website.

Action point 'Rules and Procedures' (250606.07)

General consensus is to keep things simple. <see point 4>

Action point 'Update list of members' (250606.05)

Arnold will be asked to do a crosscheck to see if proposed members are actually still FIRST member.

3. PRESENTATION CERT-POLSKA

Piotr Kijewski of CERT-POLSKA gives an interesting presentation on their ARAKIS Early Warning system. Please find the presentation been attached to this document. It will also be made available on the FIRST NM-SIG website (action point 250606.02: pending).

4. DISCUSSION / DECISION: RULES AND PROCEDURES

This proved to be a brief discussion as the general consensus is to avoid unnecessary hassle and red tape. We endeavour to keep focused on achieving the NM-SIG goals, rather than setting up all kinds of rules&procedures beforehand.

Decision-making can be done via the e-mail list. Thus providing an opportunity for everyone to take notice and contribute to the process. When unforeseen issues arise, it will be dealt with on the fly.

The conclusions (and decision) on rules and procedures:

- We don't start with setting up a rules&procedure's framework;
- Unforeseen issues are dealt with on the fly;
- The e-mail list is also used for decision-making.

5. DISCUSSION / DECISION: SHORT & LONG TERM ACTION TO ACHIVE NM-SIG GOALS

Regarding short-term actions, the following items have been discussed:

The idea is to have more presentations like the one from CERT-POLSKA. This is to be believed a valuable aspect of the face-to-face meetings. More particular we'll try to arrange a number of brief presentations, rather than one or two extensive ones. It 's all about generating ideas, rather than elaborating on details (these can be discussed bilateral e.g.). All material will be made available online (members only part on FIRST website). Regarding the website; this matter is pending and being worked on.

Long term actions items needs more discussion via the mailinglist. The idea is to investigate and discuss actions that are of personal interest of NM-SIG members and actions that are of interest for the FIRST community as a whole. For example, NM-SIG members are invited to bring their ideas of personal interest to the table which are an added value for their operational monitoring tooling. If other NM-SIG members are interested in this same feature, an action item can be created to start the development of this feature. An example of an actions item that could be of interest for the FIRST community, is the setup of an infrastructure for reporting security incidents. FIRST members can submit data, like logfiles which meet certain criteria, to this reporting infrastructure. And batched incident reports are sent out to the FIRST members.

The idea rose to have a closed Wiki page on the NM-SIG web space. This will make it easy for members to add and share there own products, comments and ideas. This will also create an NM-SIG archive. The idea gets positive feedback. What remains is the WHO, WHAT and HOW question (=action point).

One of the things to discuss is the NM-SIG funding. Can the NM-SIG be funded by FIRST? Menno Muller will inquire the FIRST Steering Committee about this matter. The same story goes for the arrangements of locations/room for (NM-)SIGs meetings at FIRST meetings. The FIRST Steering Committee will be asked whether rooms can be reserved for SIG in general in conjunction with (eg.) the general meeting.

The conclusions (and decision) on action points:

- Use face-to face meetings for brief (monitoring) presentations;
- Long-term action points need more input (via mailing list);
- Research the pro's and cons of a NM-SIG Wiki.

6. Discussion: future collaboration with organisations outside FIRST (e.g. CAIDA)

Due to lack of time this point is transferred to a discussion on the e-mail list.

7. Wrap up

Next meetings: One idea is to have the next NM-SIG meeting arranged in conjunction with FIRST TC in Hungary (January 2007). Also Arnold Yoon should be asked for the possibility for a NM-SIG meeting in Australia / Asia. Neil Long suggest a NM-SIG meeting in conjunction with the APCERT conference (Feb. 8-10 Malaysia).

Menno Muller kindly thanks SURFnet for providing the facilities and all attendees for their participation in this fruitful NM-SIG gathering and closes the meeting at 16:15.

ACTIONS

Action item*	Description	Who	End date	Status* 2
250606.01	Process comments on Birth Certificate	Menno Muller	End July	DONE
250606.02	Creation web-presence of NM-SIG	Liliana Solha (workinggroup)	End Oct	Pending
250606.03	Creation of a questionnaire for inventory of monitoring activities within the NM-SIG	Bill Eaheart (workinggroup)	Mid July (draft)	DONE
250606.04	Propose a new date and agenda for the next meeting	Menno Muller	Mid July	DONE
250606.05	Update list of members and the mailing-list of the NM-SIG	Arnold Yoon	End July	DONE
250606.06	Draw up minutes of the kick-off meeting	Hans Petri & Menno Muller	Early July	DONE
250606.07	Creation of 'Rules and Procedures'-document for the NM-SIG	Carol Overes	Early Aug	DONE
250606.08	Comment on the draft minutes, website outline and questionnaire / template	ALL	When asked for	DONE
130906.09	Resending the questionnaire on the NM-SIG mailinglist	Menno Muller	Early Oct	DONE
130906.10	Start a discussion via the mailinglist on who should get access to which information	Menno Muller	Mid Oct	DONE
130906.11	Query SC about SIG funding	Menno Muller	Oct	Pending
130906.12	Research to possibilities of using a WIKI for the NM-SIG	Dave Woutersen	Oct	Pending
130906.13	Suggest new meeting via list	Menno Muller	Oct	Pending
130906.14	Discus possible future collaboration via NM-SIG list	Carol Overes	Nov	Open

* day; month; year.number

*2 DONE: action point has been taken care of Pending: the action is being dealt with Open: action required.