Menu

- Beranda
- RFC 2350
- Berita
- Kontak
- Bahan Bacaan
- Dukungan
- Tentang Kami

TENTANG KAMI

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

PROFILES

I. Introduction

CERT (Computer Emergency Response Team) is a technical coordination team regarding to internet network incident in the whole world. Recently, the team is improved by RFC 2350 <http://tools.ietf.org/html/rfc2350> and name it as CSIRT (Computer Security Incident Response Team).

CERT or CSIRT in every country is built by community. Though some of them is supported by their country such as KrCERT (South Korea), JPCERT (Japan), AusCERT (Australia), etc. In each country, CERT has various job authority and constituent. Some CERTs have a little bit different pattern one from another.

For example, CERT in South Korea has authority in the national cybernetiquette security; meanwhile CERT Australia has constituent and membership so that it got fund to support its activity. There are also CERTs/CSIRTs built by limited community or country with

limited scope for limited circle, such as MilCERT (Military), GovCERT (Government), BankingCERT (Banking), ISPCERT (ISP), etc. CERT/CSIRT does coordination not only in a country internally (among CERT/CSIRT or organizations) but also internationally.

Many times a coordination needed among CERT/CSIRT when involving internet network incident. A good relationship is important to have among CERT/CSIRT, and to facilitate it a regional forum is built by all CERTs in Asia Pacific, named APCERT (Asia Pacific CERT), including ID-CERT as one of the founder.

II. ID-CERT

ID-CERT (Indonesia Computer Emergency Response Team) is an independent team which is from and for community. ID-CERT is the first CERT in Indonesia and founded by DR. Budi Rahardjo in 1998. ID-CERT together with JP-CERT (Japan), AusCERT (Australia) is one of the founders of the APCERT (Asia Pacific Computer Emergency Response Team) forum.

In 1998 there was no CERT in Indonesia. Based on that DR. Budi Rahardjo, an internet security expert, encouraged himself to establish ID-CERT. At the same time countries around Indonesia began to establish their own CERTs and this continued into Asia- Pacific forum which later became the APCERT.

First APCERT Meeting was attended by DR. Budi Rahardjo and Andika Triwidada in Tokyo, Japan in 2001. APCERT Meeting became annual agenda held taking turn between its members. Japan and Australia are two most active members in APCERT. ID-CERT has a difficulty to attend this annual meeting, that is funding, which always depends on sponsorship.

ID-CERT wishes to remain standing as a non-governmental organization, independent, but received an allocation of government funding as a contribution to the CERT. ID-CERT is just being reactive (not active) in responding and handling a case of incoming or reported incident by complainers. ID-CERT does not have the authority to investigate a case thoroughly, but just become a liaison who can be trusted, especially by those who reported incident.

III. Mission

1. ID-CERT's purpose is to coordinate the incidents handling involving community locally and internationally.
2. ID-CERT does not have operational authority to its constituency, it only informs a variety of complaints to network incidents, and depends entirely on the cooperation with all those involved in incidents related networks.
3. ID-CERT is built from community and the results will be given back to the community.
4. ID-CERT helps increasing the internet security awareness in Indonesia.
5. ID-CERT has research in internet security which is needed by the Indonesia internet community.

IV. Activity

ID-CERT is being reactive, that is doing the job based on incident reports received by ID-CERT. The most incident reports received by ID-CERT is phishing. The reports were received personally by DR. Budi Rahardjo, Andika Triwidada, and Ahmad Alkazimy, then sent on to the reported site or to the related provider. Mailing list is also used to explain some cases and their progress.

Now, ID-CERT has a "helpdesk" to manage incoming reports and resolving progress. At this time, ID-CERT is run by professionals and supported by volunteers. Demand of "helpdesk" is related to improve services and handle the incident complaints, also in the need of presenting a statistic of handling cases, that always presented at APCERT Meeting.

1. Incident Monitoring Report

ID-CERT in the last three years have done a research related to incident handling based on complaints, named Incident Monitoring Report, that involve ISP, NAP, Telecommunication Operator, and non-ISP such as Government and company. It was started in 2012 with name Internet Abuse Research, ID-CERT was one of the supporters of the research. Since March 2012, the research became permanent activity for ID-CERT. It hopes to be continuous so that Indonesia will have a primary data of Incident Monitoring Report occuring in Indonesia. In 2010 the research involved 13 organizations of respondent, and in 2011, it's been 38 organizations of respondent joined the research. The amount of complaints received is about 290,297 per month:

2010

NO	Kategori Komplain	Rating (%)
1	SPAM	90,3
2	INTELLECTUAL PROPERTY RIGHTS/HaKI	5,41
3	MALWARE	1,95
4	NETWORK INCIDENT (Deface, DDos Attack, etc)	1,74
5	SPOOFING/PHISHING	0,05
6	KOMPLAIN SPAM	0,01
7	RESPON ADUAN	0,001

2011

NO	Kategori Komplain	Rating (%)
1	**NETWORK INCIDENT (Deface, DDos Attack, etc)**	**75,45**
2	**SPAM**	**17,40**
3	**INTELLECTUAL PROPERTY RIGHTS/HaKI**	**5,33**
4	**MALWARE**	**1,62**
5	SPOOFING/PHISHING	0,11
6	**RESPON ADUAN**	**0,07**
7	**KOMPLAIN SPAM**	**0,03**

2012

NO	Kategori Komplain	Rating (%)
1	NETWORK INCIDENT (Deface, DDos Attack, etc)	76,53
2	**MALWARE**	8,63
3	INTELLECTUAL PROPERTY RIGHTS/HaKI	6,99
4	**SPAM**	**4,78**
5	**KOMPLAIN SPAM**	**1,94**
6	**SPOOFING/PHISHING**	**0,64**

7	**RESPON ADUAN**	**0,48**

2013

NO	Kategori Komplain	Rating (%)
1	**SPAM**	**40,40**
2	**NETWORK INCIDENT (Deface, DDos Attack, etc)**	**27,81**
3	**MALWARE**	**10,07**
4	**INTELLECTUAL PROPERTY RIGHTS/HaKI**	**8,71**
5	KOMPLAIN SPAM	2,50
6	SPOOFING/PHISHING	1,65
7	RESPON ADUAN	0,86

2014

NO	Kategori Komplain	Rating (%)
1	SPAM	51,78
2	**INTELLECTUAL PROPERTY RIGHTS/HaKI**	**24,14**
3	**KOMPLAIN SPAM**	**6,74**
4	**NETWORK INCIDENT (Deface, DDos Attack, etc)**	**6,61**
5	**SPOOFING/PHISHING**	**4,67**
6	**MALWARE**	**4,57**
7	RESPON ADUAN	**1,49**

Note: in **Bold**: position rating

Most cases are from abroad because they found difficulty to contact the site administrator of the problem site. They trusted ID-CERT to report the case. ID-CERT has been made good relationship with neighbourhood CERTs and some of them have visited ID-CERT in Indonesia.

2. Statistics of Indonesia Malware

ID-CERT plans to have Statistics of Malware in Indonesia. The research is to find out the direct impact and readiness of Indonesia internet society to virus/worm/malware.

Some methods to use are:

1. Survey by using empty USB Flashdisk. Then bringing it back to the Laboratory and the USB Flashdisk is scanned by various antivirus.
2. Survey by using USB Flashdisk which installed by portable apps (an antivirus application which no need to be installed to computer when inserting it to the computer, and can be used to scan the PC and also the network directly).
3. After farming the virus, our team will make a note of time, name of the virus, and

location where the virus founded. Then, name of the virus will be saved to the database and statisics will create. This method will be improved so that can be done report parsing automatically.
4. Other method is by using honeypots server to collect various malware around Indonesia.

V. ID-CERT Agenda

The most ID-CERT's attention is: what exactly will be expected by society from ID-CERT.

1. ID-CERT will prepare the workflow and Standard Operation Procedures (SOP) and a detal jobdesk to develop/improve and add some staffs, at least to respond in helpdesk.
2. ID-CERT will deploy a system to manage and handle incidents better.
3. ID-CERT will prepare several other researches and studies, required by Indonesia internet community. ID-CERT also plans to add personnel in the field of research and collaboration with leading universities in developing any necessary research.
4. ID-CERT will publish regular research reports per month, per bi-monthly, per semester, and annual report.

VI. Community Support

ID-CERT hopes that many more respondent to participate in various researches run by ID-CERT, for greater good of Indonesia internet in the future. ID-CERT also hopes that in establishing it ID-CERT gets support especially in operational matters.

1. ID-CERT Constituent Membership of ID-CERT is available for all Indonesia internet communities which care for internet security , either for ISP or non-ISP, such as governmental organizations (department, Pemda, BUMN, BUMD, etc) or private sections.
2. ID-CERT Respondent From the research of Internet Abuse 2011, ID-CERT has 38 organizations of respondent. However, ID-CERT always welcome to new respondents whom want to participate in researches run by ID-CERT.
3. ID-CERT Supporting/Affiliation ID-CERT define its supporter or affiliation as organizations which give their support in ID-CERT researches. ID-CERT invites Indonesia internet communities to give their support in sponsorship, donation or membership fee (will define later).
4. ID-CERT Volunteer From the first day, ID-CERT got many supports from volunteers in contributing their energy and care for Indonesia internet security. Most of ID-CERT volunteers are individual. ID-CERT is wide open to everyone who wants to contribute in Indonesia internet security by joining ID-CERT research team, or being ID-CERT helpdesk.

VII. Our Team

Volunteers:

1. DR. Budi Rahardjo (Coordinator of ID-CERT)
2. Andika Triwidada (Vice Coordinator of ID-CERT) Finger print=5568 7C7D E898 4F33 A594 A996 DA4B C29F E22D FEE7

3. Maman Sutarman
4. Rizky Ariestiyansyah
5. Ikhlasul Amal
6. Samuel Cahyawijaya
7. Andreas Wenra Alfa
8. Denny Nugraha
9. Ridwan Akbar
10. Rizky Ariestiyansyah
11. Andri Aprijal
12. Nurwin Hermansyah
13. Indra Suryana
14. Oki Bagja
15. Setia Juli Irzal

Professional Staffs:

1. Ahmad Alkazimy, (Manager of ID-CERT)

   ahmad@cert.or.id

   M: +62-838-74-9292-15

   Finger print= 39B2 87BA 3DD6 7832 D56F 0344 FCE4 3A7C FE38 CC96

2. Rahmadian L. Arbianita, (Incident Response Team – HelpDesk Officer of ID-CERT)

   rahmadian@cert.or.id

   M: +62-811-227703

   Finger print= 414A 1183 199E 8BA5 E0D1 C234 08BF 8BDE 1766 2CC7