

Improvements to CHIHT

Putting more value into the Clearinghouse Recent advances (Jan. - May 2004)

Marco Thorbrügge, DFN-CERT
12. TF-CSIRT meeting
28. May 2004 / Hamburg

-
- **Phase 1: Re-organisation (done)**
 - Moving basic tools into an own category (done)

 - **Phase 2: Adding more information**
 - Collect input: which additional information would be useful? (done)
 - Generate a new XML object (done)
 - Apply changes to the CHIHT framework (done)
 - Completing information for existing tools (ongoing)

-
- **What information we already had**
 - The name of the tool
 - Where one can get it (HTTP- or FTP-URL)
 - Which platforms it runs on
 - A short description

 - **What information we additionally have now**
 - Category
 - Detailed Info (Link to a local page)
 - Mailing Lists (Link, will probably be moved to DI)
 - In use by team (Name and URL)
 - XML file (for that tool)

Status Quo (II)

CHIHT - CSIRT procedures - Mozilla (Build ID: 2002091116-SuSE)

File Edit View Go Bookmarks Tools Window Help

http://chiht.dfn-cert.de/functions/csirt_pr Search

Home Bookmarks

encryption. PGP is widely used by CSIRTs around the world to communicate confidential/sensitive data. The official PGP program was purchased by NAI Labs, who have recently stopped supporting the program. PGP will be further developed by pgp.com, version 8.0 ist available and looks promising. A free version of older PGPversions is available at the link above.
XML-File: [pgp.xml](#)

Name: The GNU Privacy Guard (GPG)
Source: <http://www.gnupg.org/>
Platform: Unix, Windows
GPG is a powerful alternative to PGP from NAI Labs. Like PGP, GPG encrypts/decrypts mail or data with a mix of symmetric and asymmetric encryption. GPG is widely used by CSIRTs around the world to communicate confidential/sensitive data. GPG is a command-line tool, some graphical user interfaces and plugins for mailprograms exist. The program is sponsored by german government.
Category: CSIRT procedures - Communications
More Details: Local [gpg](#) Page
Mailinglist: [http://www.gnupg.org/\(en\)/documentation/mailling-lists.html](http://www.gnupg.org/(en)/documentation/mailling-lists.html)
Used by Team: DFN-CERT
XML-File: [gpg.xml](#)

Name: Listserv
Source: <http://www.lsoft.com/products/default.asp?item=manuals>
Platform: Windows
Listserv is a commercial mailing list package that can be used to maintain distribution lists for incident response teams.
XML-File: [listserv.xml](#)

Document: Done (0.109 secs)

- **Phase 3: Generate a new questionnaire (open)**
 - Overwork existing survey to gather new tools
- **Phase 4: Adding workflow descriptions**
 - Idea: Having clickable image maps guiding to the correct tools
 - See: <http://chiht.dfn-cert.de/workflow/>
 - Another form of navigation within the clearinghouse

-
- **Next steps**
 - Complete the informations for existing tools (Phase 2)
 - Generate a new questionnaire (Phase 3)
 - Send in all your workflows, ideas how to present them, etc. (Preparing Phase 4)

 - **Call for volunteers!**