certin
Handling Computer Security incidents
Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
(Government of India)

CCAOI™
Representing the ecosystem of Internet -Bharat Model

Security Newsletter 28th February, 2011

As internet is becoming an integral part of our lives, it is important that we are aware of the threats we face in the Cyberspace. Cybercrime is on the rise as is evident from the number of cases that are reported in the media. The need of the hour is to be aware and adequately equipped to protect ourselves online.

In fact countries today are getting ready to establish specific armies to counter Cyber terrorism. Recently Turkey announced that they would be establishing a Cyber Army Command to counter cyber-terrorism attacks against the country. Preparations for creating a special unit within the General Staff to deal with cyber threats have been completed in cooperation with the Defense Ministry, the Scientific and Technological Research Council of Turkey (TÜBİTAK) and Middle East Technical University (ODTÜ).

Looking at the gravity of the situation, with the support of Indian Computer Emergency Response Team (Cert IN), Department of Information Technology, VeriSign India and Sify Technologies Ltd, we are releasing this edition of our Security Newsletter.

Computer Security and Safety Measures to Secure Oneself Online

Computer security is important for all -small businesses, home based networks and large organizations and there is a need to establish good computer security practices. Many of these practices also serve as good advice to follow in order to limit the effects of disasters, accidents and cybercrimes other than terrorism.

- **Always have a plan**

It is always advisable to have an actionable plan for yourself and other users in your network to follow in case your network appears/ is attacked. Response plans, therefore, should go into effect as soon as a system appears to have been compromised, and then the source of the problem –whether accidental or malicious—can be sought.

- **Take a Back up of Critical Information**

It is always advisable to have a system for backing up critical information and databases.

- **Always Authenticate Network Users**

Make sure your user authentication system is appropriate for your system. If you are a private or home networked user, make sure you change your passwords at least every 3 months. If you run a small organization, make sure that you know who goes in and out of your workplace, virtually and physically. In larger organizations, it is recommended that passwords be combined with physical hardware and well-implemented biometric systems to ensure that computers are accessible only to authorized users.

- **Create a mechanisms for Reporting Problems in the Workplace.**

Ensure you have a formal and informal mechanism to report issues. The organization should foster an atmosphere of support for full reporting as it will save companies potentially critical and costly losses.

- **In case of Attack have a plan to Reduce the System's Vulnerability**

Always have a mechanism in place such that you can reduce the system's vulnerability in case of an attack. Reduce the number of users, run less software and limit communication between systems. All of these actions close off possible places where the system has been or can be breached further.

- **Make Sure that Everyone Knows What to Do and Expect**

The employees, system operators, managers, should be trained on how to respond in case of an attack. Response plans need to be practiced and made part of an overall prevention strategy. Staging mock attacks or "red teaming" is an excellent way to identify weaknesses and areas to be strengthened in existing response strategies, while reinforcing proper response methods.

- **Prevent Public Relations Crises by Preparing Communications Strategies**

The information of attacks need to be public as Researchers, developers, and operators need this information to redesign systems and procedures to avoid future incidents, and national security and law enforcement agencies need it to defend the nation. Fearing for their reputations, many organizations keep attacks under wraps. This is detrimental to the safety of all. Instead, a well planned communications strategy can both ensure future safety and protect organizations' reputations.

- **Report Attacks to Government Authorities**

If you suspect that a terrorist attack is the source of a slowdown or disruption in your system, it should be reported to the Cert In team.

CCAOI, 258 Okhla Industrial Estate, Phase III, New Delhi – 110020. Visit us online at: www.ccaoi.in
For any comments/suggestions email: info@ccaoi.in