경제혁신 3개년 계획 3년의 혁신, 30년의 성장

창조경제

K-ICT International Conference on Information Security (ICIS) 2015

International Cooperation in the field of Cyber Security

Indian Computer Emergency Response Team (CERT-In)

미래창조과학부 Ministry of Science, ICT and Future Planning

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

Cyber attacks being observed

- Scanning and Probing of Critical Systems
- Targeted attacks
- Denial of Service (DoS) attacks
- Distributed Denial of Service (DDoS) attacks
- Website Defacements (Government and Private)
- Spread of Malwares/Bots
- Website Intrusion for Malware Propagation
- Phishing attacks (Banks & Government)

Key Elements of Cyber Security Strategy

- Security R&D
- Legal Framework
- Security Incident - Early Warning & Response
  - National Cyber Alert System
  - CERT-In and Sectoral CERTs
  - Information Exchange with international CERTs
- Security Policy, Compliance and Assurance
  - Security Assurance Framework
  - Cyber security drills
- Security Training
  - Skill & Competence development
  - Domain Specific training – Cyber Forensics, Network & System Security Administration
- International Cooperation

K-ICT International Conference on Information Security (ICIS) 2015

Issues for Discussion & Co-operation

- Information exchange on various aspects of cyber threats & attacks and their mitigation
- Discussions on elements of cooperation on Incident response, including CERT to CERT cooperation
- Cooperation on Security testing and on improving security of industrial control system
- Joint mock drills with public-private partnership and sharing of experience
- Exchange of experts/ visits to CERTs

K-ICT International Conference on Information Security (ICIS) 2015

Cyber threats and concerns

International level

- Cyber crime & cyber terrorism
- Deliberate and anonymous use of ICTs for attacks on critical Infrastructure
- Unhindered growth of botnets
- Absence of international mechanism to facilitate information sharing & counter action
- Risk of attack misperception due to uncertainty of positive attack attribution

National level

- Cyber crime & terrorism
- Attacks on Critical Infrastructure
- Website defacements
- Website intrusion and malware propagation
- Malicious Code & spread of botnets
- Scanning and probing for Cyber espionage
- Denial of Service & Distributed Denial of Service attacks
- Supply chain integrity

Organizational level

- Website intrusion/Defacement
- Domain stalking
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- Targeted attacks
- Phishing
- Data theft
- Insider threats
- Financial frauds

Individual level

- Social Engineering
- Email hacking & misuse
- Identity theft & phishing
- Financial scams
- Abuse through emails
- Abuse through Social Networking sites
- Device theft

Thank you

kkb@cert-in.org.in
bkkumar2000@gmail.com
www.cert-in.org.in