NOTIS PERINGKATAN KESELAMATAN ICT BIL. 2/2013
PADA 30 APRIL 2013

KETERANGAN KETERDEDAHAN	
Nama dan Jenis Keterdedahan	Ancaman Serangan Siber Keatas Server Kerajaan Sempena PRU-13
Tarikh Pengumuman Asal	30 April 2013
Bilangan Aset ICT Terlibat	Semua pengguna.

GAMBARAN KESELURUHAN

Bagi memastikan sistem penyampaian kerajaan beroperasi secara berterusan terutama di dalam tempoh Pilihan Raya Umum Ke-13 (PRU-13) bermula pada tarikh penamaan calon pada 17 April 2013 sehingga tarikh akhir bantahan pada 26 Mei 2013, pihak agensi adalah disarankan untuk sentiasa di dalam keadaan berjaga-jaga dan memberi lebih perhatian terhadap keselamatan aset ICT bagi memastikan agensi dilindungi dari sebarang ancaman siber.

CADANGAN PENYELESAIAN

- Menukar dan memastikan penggunaan kata laluan yang kukuh.
- Memastikan perisian antivirus dikemaskini dengan signature terkini dan menetapkan imbasan secara berkala pada server. (Malware Scanner bagi Linux : http://www.rfxn.com/projects/linux-malware-detect/)
- Mengimbas, menyemak dan menghapuskan fail-fail yang mencurigakan didalam folder web server secara berkala dengan NeoPI (https://github.com/Neohapsis/NeoPI)
- Pengukuhan XAMPP : http://robsnotebook.com/xampp-security-hardening , http://www.apachefriends.org/en/xampp-windows.html#1221
- Pengukuhan server Apache : http://www.symantec.com/connect/articles/securing-php-step-step
- Memasang ModSecurity (Application Firewall) : http://www.modsecurity.org/
- Memasang GreenSQL (Database Firewall) : http://www.greensql.net/
- Mengaktifkan fail log server (rujuk Surat Arahan Ketua Pengarah MAMPU bertarikh 23 Mac 2009 di http://www.mampu.gov.my/web/guest/suratarahanketuapengarahmampu)
- Menaiktaraf aplikasi PHP dan CMS seperti Joomla dan sebagainya ke versi terkini.
- Memastikan *'third party component'* CMS dikemaskini kepada versi terkini.
- Memastikan IDS/IPS dan firewall dikonfigurasi dengan betul dan berfungsi dengan baik
- Menutup port-port yang tidak diperlukan/digunakan pada server.
- Melakukan pemantauan pada aktiviti di dalam rangkaian dan server.
- Mengemaskini dan memastikan sistem pengoperasian dilengkapi dengan security patches yang terkini.

MAKLUMAT LANJUT

Pautan berkaitan:

1. http://www.ictsecurity.gov.my
2. http://gcert.mampu.gov.my

Sila e-mail kepada keselamatan.jpkn@sabah.gov.my untuk keterangan lanjut mengenai keterdedahan ini.

Disediakan Oleh:

Edi Abdul Majid
Security Audit & Assessment Team, sgCERT
Urusetia sgCERT
Bahagian Keselamatan
Jabatan Perkhidmatan Komputer Negeri