NOTA MAKLUMAN GCERT BIL. 2/2015
PADA 11 OGOS 2015

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**Ancaman Serangan Laman Web Kerajaan oleh Anonymous Malaysia.**
Tarikh Dikesan	**9 Ogos 2015**
Bilangan Agensi Terlibat	**Semua**

Sistem Pengoperasian/Aplikasi Berisiko

- Semua laman web kerajaan berisiko untuk diserang.

Keterangan Serangan

- Pihak Anonymous Malaysia telah mengeluarkan satu ancaman berbentuk video pada 4 Ogos 2015 untuk menyerang laman web kerajaan pada 29 hingga 30 Ogos 2015 (Sabtu dan Ahad) mulai 6.00pm hingga 11.00pm (5 jam).
- Ancaman ini dikeluarkan berikutan dengan cadangan untuk mengadakan Demonstrasi Jalanan Bersih 4.0
- Sasaran ancaman adalah terhadap laman web 1MDB, Najib Razak, PDRM dan SPRM.
- Sekiranya tiada tindakan diambil oleh kerajaan untuk menyelesaikan isu-isu yang dibangkitkan dalam tempoh 48 jam, serangan akan disasarkan terhadap 150 laman web kerajaan yang lain.

Kaedah Serangan

- Sasaran serangan adalah terhadap kelemahan yang terdapat di sistem rangkaian dan aplikasi laman web kerajaan.

Cadangan Tindakan Pengukuhan

- Pengukuhan dan pemantauan terhadap sistem rangkaian di agensi.
- Melaksanakan pengemaskinian patches terhadap semua peranti.
- Melaksanakan pengemaskinian patches terhadap semua komponen perisian laman web.
- Memasang IPS/IDS (sekiranya tiada).
- Aktifkan sistem log bagi semua sistem yang ada.
- Meningkatkan pemantauan terhadap pelaksanaan sistem dalam talian.
- Memasang agen pemantauan MyGSOC bagi semua server di agensi persekutuan sahaja.
- Memasang *Web Server Monitoring System* (WSM) kepada semua laman web agensi persekutuan.
- Melaksanakan tindakan pengukuhan terhadap penemuan ujian penembusan yang dijalankan.

Maklumat Lanjut

- *Government Computer Emergency Response Team* (GCERT) (http://gcert.mampu.gov.my/)