

## KENYATAAN MEDIA

10 Ogos 2015

# KENYATAAN CYBERSECURITY MALAYSIA MENGENAI KEMUNGKINAN ANCAMAN SIBER DARI “ANONYMOUS”

**SERI KEMBANGAN (10 Ogos 2015)** - CyberSecurity Malaysia, pusat pakar teknikal keselamatan siber nasional dan agensi di bawah Kementerian Sains, Teknologi dan Inovasi (MOSTI) mengambil maklum mengenai kemungkinan ancaman serangan siber oleh sekumpulan penjenayah (penggodam) siber yang dikenali sebagai “Anonymous” melalui laman media sosial.

Menurut Dr. Amirudin Abdul Wahab, Ketua Pegawai Eksekutif CyberSecurity Malaysia, “CyberSecurity Malaysia telah mengambil tindakan sewajarnya dengan membuat analisa teknikal dan dalam masa yang sama bekerjasama rapat dengan pihak berkepentingan sama ada dalam negara mahupun luar negara dalam usaha menangani perkara ini.”

CyberSecurity Malaysia ingin menggesa agar semua pihak agar mengambil langkah segera seperti berikut:-

### Organisasi

- i. Organisasi digesa agar untuk memperkukuhkan sistem pertahanan siber bagi melindungi rangkaian komputer di organisasi mereka. *Firewall*, sistem pencegahan pencerobohan (Intrusion Prevention System), rangkaian dan sistem pengesanan pencerobohan berasaskan hos (Intrusion Detection System) boleh mencegah dan log kebanyakan serangan generik;
- ii. Pastikan sistem, aplikasi dan *add-ons* pihak ketiga diperkemas dan dinaiktaraf dengan perisian terkini dan “patch” keselamatan;
- iii. Jika beroperasi dengan menggunakan sistem atau perisian operasi versi yang lebih lama, maka disarankan agar mereka menaik taraf sistem dan perisian tersebut

**CyberSecurity Malaysia**  
(726630-U)



T +603 8992 6888  
F +603 8992 6841  
H 1 300 88 2999

Corporate Office:  
Level 5, Sapura@Mines  
No 7, Jalan Tasik  
The Mines Resort City  
43300 Seri Kembangan  
Selangor Darul Ehsan  
Malaysia.

[www.cybersecurity.my](http://www.cybersecurity.my)



kepada versi terkini. Ini disebabkan oleh sistem dan perisian versi lama mungkin mempunyai beberapa kelemahan yang boleh dimanipulasi oleh penceroboh. Selain itu, sila pastikan bahawa aplikasi web (web-based applications) anda dan peralatan rangkaian (Network-based appliances) dipasang dengan “patch” keselamatan sewajarnya;

- iv. Melaksanakan ujian penilaian kelemahan atau ujian penembusan secara berkala.
- v. Tingkatkan kemahiran pentadbir laman web serta pegawai yang bertanggungjawab dalam pengendalian insiden keselamatan siber melalui latihan kepakaran;
  - i. Menggunakan sistem pengurusan keselamatan maklumat atau ISMS;
  - ii. Laporkan insiden atau serangan siber kepada Pusat Bantuan Cyber999 melalui email: [cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my)

### **Individu / Perseorangan**

- i. Pastikan komputer dan pelayar anda dikemaskini dan “patch” keselamatan dipasang;
- ii. Pasang perisian Anti-Virus pada komputer anda untuk mengimbas dan menyekat mana-mana malware ke dalam PC. Anti-virus perlu sentiasa dikemaskini agar sistem komputer dapat dilindungi dari cecacing dan virus terkini;
- iii. Jangan klik pada pautan dan lampiran yang diterima melalui Rangkaian Sosial dan Emel di Telefon pintar atau komputer anda. Langkah berjaga-jaga tambahan perlu diambil apabila membuka pautan dan lampiran;
- iv. Melaksana pendua (backup) tetap pada semua maklumat penting untuk menghadkan kesan atau kerugian sistem atau data serta membantu mempercepatkan proses pemulihan. Sebaik-baiknya, pendua harus dilakukan pada setiap hari dan data perlu disimpan pada peranti yang berasingan atau disimpan di luar talian di lokasi yang sesuai;
- v. Laporkan insiden keselamatan siber dan serangan siber kepada pihak berkuasa yang berkaitan atau kepada Pusat Bantuan Cyber999 melalui email: [cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my)

CyberSecurity Malaysia juga menggesa orang ramai supaya membuat pengesahan ke atas maklumat yang diperolehi melalui aplikasi Internet dan dari pelbagai saluran media dan jaringan sosial sebelum mengambil sebarang tindakan seperti berkongsi maklumat tersebut dengan orang lain.

**CyberSecurity Malaysia** is the national specialist centre for cyber security, under the purview of the Ministry of Science, Technology and Innovation (MOSTI). For additional information, please visit our website at <http://www.cybersecurity.my>. For general inquiry, please email to [info@cybersecurity.my](mailto:info@cybersecurity.my). Stay connected with us on social networks: facebook/ CyberSecurityMalaysia, twitter/cybersecuritymy, youtube/cybersecuritymy, instagram/CyberSecurity\_Malaysia.

*For further enquiries about this document, please email: [media@cybersecurity.my](mailto:media@cybersecurity.my) or call +603-89926888, Mohd Shamil Mohd Yusoff (ext: 6978) or Sandra Isnaji (ext: 6977)*