KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

SIARAN MEDIA

KUKUHKAN PERTAHANAN SIBER. LINDUNGI SEKTOR MAKLUMAT KRITIKAL NEGARA

SERI KEMBANGAN (11 Ogos 2015) - Kementerian Sains, Teknologi dan Inovasi (MOSTI) hari ini menggesa semua organisasi di bawah Infrastruktur Maklumat Kritikal Negara (CNII) supaya terus memperkukuhkan sistem pertahanan siber bagi melindungi rangkaian komputer di organisasi masing-masing. Selain itu, organisasi CNII juga diingatkan agar menaiktaraf sistem komputer dengan perisian terkini dan "patch" keselamatan.

Ini berikutan dari kemungkinan wujudnya serangan siber oleh sekumpulan penjenayah dan penggodam yang dikenali sebagai "Anonymous" seperti yang dilaporkan.

"Sebagai sebuah Kementerian yang dipertanggungjawab bagi memastikan keselamatan ruang siber negara agar selamat serta terhindar dari pelbagai ancaman dan serangan siber, MOSTI melalui CyberSecurity Malaysia dan MIMOS Berhad ("MIMOS") sentiasa berusaha dan bertindak secara pro aktif dalam menangani isu-isu berkaitan keselamatan siber." Kata YB. Datuk Madius Tangau, Menteri Sains, Teknologi dan Inovasi.

Dalam konteks keselamatan siber, CyberSecurity Malaysia sentiasa memberi sokongan serta perkhidmatan berbentuk bantuan teknikal kepada 10 sektor CNII yang terdiri daripada sektor Pertahanan & Keselamatan, Perbankan dan Kewangan, Maklumat dan Komunikasi, Tenaga, Air, Pengangkutan, Kesihatan, Makanan & Pertanian, Perkhidmatan Kerajaan, dan Perkhidmatan

Kecemasan sebagaimana yang termaktub di dalam Dasar Keselamatan Siber Negara (NCSP).

Selain daripada itu, MIMOS sebagai agensi R&D ICT Negara juga turut berusaha ke arah menjaga kedaulatan Negara (e-*Sovereignty*) dengan membangunkan teknologi keselamatan yang terkehadapan *(advanced).* Ia dibangunkan bagi melindungi infrastruktur IT di sesebuah organisasi daripada serangan dalaman atau luar dan menjejak (*track*) pergerakan dokumen atau maklumat yang dibocorkan.

Selain itu, Datuk Madius juga menekankan bahawa pentadbir rangkaian komputer perlu mempunyai kemahiran dan kecekapan dalam mengendali sesuatu insiden atau ancaman siber yang dihadapi oleh organisasi mereka. Justeru, mereka perlu menjalani latihan kepakaran bagi mendapatkan *skill* kepakaran yang berkaitan.

Skill kepakaran boleh diperolehi melalui program-program latihan kepakaran professional yang ditawarkan oleh CyberSecurity Malaysia seperti latihan kepakaran dalam bidang forensik digital dan latihan kepakaran tindak balas keselamatan siber.

Orang ramai juga diminta supaya melaporkan insiden keselamatan siber dan serangan siber kepada pihak berkuasa yang berkaitan atau kepada Pusat Bantuan Cyber999 melalui email: cyber999@cybersecurity.my.

~ Tamat ~

Untuk maklumat lanjut sila hubungi +603-89460999, Mohd Shamil Mohd Yusoff (ext: 895), atau Sandra Isnaji (ext: 867), email media@cybersecurity.my

Maklumat lanjut berkaitan teknologi yang dibangunkan MIMOS, sila hubungi melalui emel: info@mimos.my