MalaysiaGazette
SPROUT YOUR MIND

Gangguan IT: Keperluan melindungi infrastruktur kritikal

Oleh **Pendapat** - 21 July 2024

Perkhidmatan KTMB antara yang terjejas akibat gangguan IT global baru-baru ini.

DUNIA dikejutkan dengan isu gangguan perkhidmatan IT global yang menyebabkan operasi sektor kritikal seperti lapangan terbang, kereta api, saluran televisyen, lapangan terbang dan bank terjejas. *CrowdStrike*, salah satu firma keselamatan siber terkemuka di dunia, telah mengakui bahawa salah satu kemaskininya menyebabkan sistem pengendalian Microsoft Windows gagal berfungsi dan memaparkan skrin biru, biasanya dikenali sebagai Skrin Biru Kematian atau *the Blue Screen of Death.*

Ketua Pegawai Eksekutif serta Pengasas CrowdStrike Inc, George Kurtz, mengesahkan bahawa ia bukan insiden keselamatan atau serangan siber. Agensi Keselamatan Siber Negara (NACSA). Walau bagaimanapun berkata, ia memberi kesan negatif kepada pengguna Microsoft di seluruh dunia termasuk Malaysia terutamanya kepada pelbagai sektor kritikal, termasuk operasi di Terminal 2 Lapangan Terbang Antarabangsa Kuala Lumpur (KLIA) terjejas, menyebabkan daftar masuk secara manual dan masa menunggu yang panjang. Gangguan tersebut turut mengganggu transaksi dan perkhidmatan perbankan. Walaupun gangguan ini bukan serangan siber, NACSA menekankan bahawa hal ini menimbulkan isu keselamatan siber yang membimbangkan kerana ia telah

memberi kesan negatif kepada pengoperasian dan keselamatan siber sektor kritikal negara.

Hal ini membuktikan betapa pentingnya untuk melindungi aset-aset sektor kritikal negara melalui pelbagai kaedah, seperti perundangan, tadbir urus, teknologi dan sebagainya. Akta Keselamatan Siber 2024 telah diwartakan secara rasmi oleh Jabatan Peguam Negara pada 26 Jun 2024. Perundangan ini merupakan satu usaha dan pencapaian yang penting dalam mengukuhkan pertahanan siber Malaysia dan meningkatkan daya tahan terhadap ancaman yang muncul.

Akta Keselamatan Siber 2024 memperkenalkan beberapa ciri penting seperti penubuhan Jawatankuasa Keselamatan Siber Negara. Ia menggariskan tugas dan kuasa Ketua Eksekutif NACSA, serta fungsi dan tugas ketua sektor infrastruktur maklumat kritikal negara atau national critical information infrastructure (NCII) dan entiti NCII.

Akta ini juga menangani pengurusan ancaman keselamatan siber dan insiden yang berkaitan dengan NCII. Selain itu, ia termasuk peruntukan untuk mengawal selia penyedia perkhidmatan keselamatan siber melalui pelesenan. Adalah penting untuk ambil perhatian bahawa walaupun Akta itu telah diwartakan, ia masih belum dikuatkuasakan.

Jika kita imbau kepada insiden keselamatan siber yang berlaku pada 19 Julai 2024, beberapa sektor kritikal NCII telah terjejas dan memberi kesan besar kepada rakyat
secara amnya. Kebergantungan pengendalian infrastruktur NCII kepada perisian dan peranti yang berasaskan teknologi maklumat seperti CrowdStrike membuka ruang
kepada pihak-pihak yang tidak bertanggungjawab untuk menceroboh infrastruktur tersebut dengan mengambil kesempatan ke atas apa jua kelemahan yang wujud
dalam sistem yang digunakan.

Oleh itu, adalah sangat penting untuk memastikan infrastruktur maklumat kritikal negara sentiasa berada di tahap perlindungan yang terbaik melalui prosedur pengurusan risiko dan kaedah tindak balas yang berkesan dan berterusan.

Lantaran itu, Akta Keselamatan Siber 2024 digubal agar pendekatan yang strategik dan menyeluruh dapat dilaksanakan ke atas semua infrastruktur maklumat kritikal

negara yang merentasi semua sektor penting. Hal ini kerana apa-apa pencerobohan atau serangan ke atas infrastruktur kritikal boleh memberi impak yang besar kepada
negara dan rakyat khususnya dalam aspek keselamatan, ekonomi, kesihatan dan sosial.

Dr. Mahyuddin Daud
Profesor Madya (Undang-undang Siber) di Kulliyyah Undang-Undang Ahmad Ibrahim, Universiti Islam Antarabangsa Malaysia.