BERITA HARIAN 20/3/2024 M.S 11

Negara perlukan 30,000 tenaga mahir keselamatan siber

Timbalan Naib Canselor (Penyelidikan dan Inovasi), Universiti Tun Hussein Onn Malaysia (UTHM)

Oleh Prof Dr Rabiah Ahmad
bhrencana@bh.com.my

Ancaman keselamatan maklumat lebih tertumpu kepada keselamatan siber meskipun ia juga boleh membabitkan perkakasan, perisian, komunikasi dan data. Laporan Techwireasia menunjukkan sebanyak 22 juta ancaman siber disekat di negara ini pada 2023, manakala laporan insiden keselamatan siber daripada Cybersecurity Malaysia pula merekodkan 567 *insider* berkaitan ancaman ini sekitar Januari tahun ini sahaja.

Ini menunjukkan keperluan keselamatan siber dijadikan bidang keutamaan negara dalam konteks bakat, teknologi dan dasar. Transformasi dunia digital memerlukan pelan tindakan lebih strategi agar Malaysia mempunyai ruang siber lebih selamat dan terlindung.

Justeru, untuk memperhebat strategi keselamatan siber, Kementerian Pendidikan Tinggi (KPT) dengan model quadra helix turut merancakkan kerjasama bidang berkaitan bagi melaksanakan aktiviti penyelidikan, pembangunan bahan dan peningkatan tenaga mahir.

Penyelidikan berkaitan ancaman siber dapat diklasifikasikan dengan pelbagai kategori seperti kajian metod bersesuaian untuk mengenal pasti ancaman, kajian analisis impak daripada insiden serangan, penghasilan teknologi baharu dalam pengecaman dan pembangunan polisi mengatasi ancaman.

Kerjasama universiti bersama industri memberi peluang kepada potensi penyelidik untuk meneroka ancaman keselamatan siber menerusi model quadra helix. Penulis sendiri berpengalaman mengetuai penyelidikan asas dan membuka ruang mengenal pasti aset serta risiko keselamatan siber.

Penyelidikan bersama kumpulan penyelidik universiti awam (UA) menggunakan responden dalam kalangan perusahaan kecil dan sederhana (PKS) itu, menghasilkan model struktur maklumat penting membantu melaksanakan analisis risiko.

Kenal pasti aset, potensi ancaman

Penghasilan ilmu baharu akan dipraktikkan antaranya kemahiran mengenal pasti aset dan potensi ancaman siber yang mula diajarkan kepada pelajar sarjana muda sekitar 2000 bagi universiti menawarkan program 'Keselamatan Komputer'.

Pensijilan seperti Sistem Maklumat Pengurusan Keselamatan ditawarkan bersama rakan industri pula boleh menjadi inisiatif strategik penghasilan bakat memiliki kecekapan dalam bidang ini.

Ini membolehkan pelbagai kemahiran menggunakan perkakasan diajar seperti penggunaan aplikasi OWASP dalam mengenal pasti kelemahan sistem komputer, yang menjadi antara proses analisis risiko pada aset.

Realitinya, Malaysia memerlukan tenaga mahir keselamatan siber seramai 30,000 menjelang 2030. Dalam usaha meningkatkan modal insan ini, Universiti Tun Hussein Onn Malaysia (UTHM) menerusi Fakulti Sains Komputer dan Teknologi Maklumat (FSKTM) turut membantu Agensi Keselamatan Siber Negara (NACSA).

Bagi menjayakan bidang keselamatan siber ini, penerokaan secara silang disiplin perlu dilakukan. Justeru, analisis risiko ancaman siber perlu membabitkan bidang baharu seperti teknologi rel, dron dan marin.

Peningkatan pesat dalam penggunaan teknologi internet benda (IoT) dalam bidang pengangkutan juga menuntut kepada penerokaan ancaman keselamatan siber secara model quadra helix.

Bagaimanapun, usaha menangani ancaman siber negara bukan sahaja memerlukan kerjasama terpandu antara universiti, industri dengan agensi kerajaan, bahkan perlu sampai kepada komuniti melalui pelbagai saluran media sosial, cetak dan digital.