Organisasi perlu siap siaga tangani ancaman jenayah siber

Konsep bekerja dari rumah yang digalakkan dalam mengehadkan pergerakan akibat penularan COVID-19 bukan budaya baharu.

Kerajaan sendiri sudah melancarkan konsep ini beberapa tahun lalu bagi sektor awam dalam kerjaya tertentu.

Bagaimanapun, ia terhad kepada bidang kerja dan perjawatan tertentu seperti arkitek serta pereka grafik.

Pada era pandemik ini, perkara ini menjadi norma baharu bagi hampir kesemua sektor pekerjaan.

Firkhan Ali Hamid Ali

Konsep bekerja dari rumah menuntut penggunaan peralatan digital dan perkhidmatan internet. Dengan situasi ini, ia mendedahkan pekerja kepada risiko keselamatan siber kepada diri sendiri dan organisasi atau majikan.

Menurut Cyber Security Malaysia (CSM), sebanyak 4,596 laporan dibuat terhadap kes jenayah siber, awal tahun ini hingga April.

Begitu juga laporan Majlis Keselamatan Pertubuhan Bangsa-Bangsa Bersatu (PBB) menyebut peningkatan kes jenayah siber ketika pandemik COVID-19.

Kesedaran keselamatan siber asasi seperti penggunaan kata laluan dan pengesahan diri selamat, kesedaran pelbagai jenis penipuan siber serta keselamatan penggunaan data.

Juga kesiagaan maklum balas kemalangan siber dan enkripsi maklumat rahsia berupaya mengurangkan risiko ancaman keselamatan siber kepada sebuah organisasi.

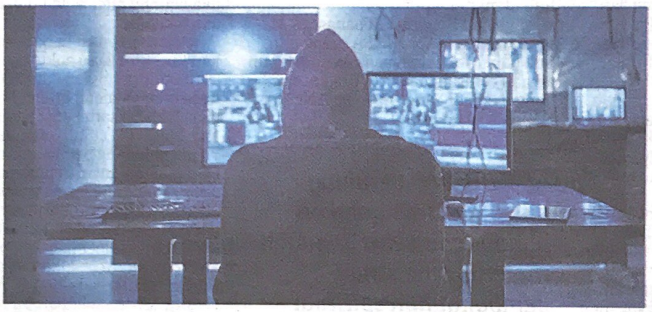
Pekerja yang bekerja secara jarak jauh berisiko kepada ancaman keselamatan siber bagi organisasi terbabit.

Keselamatan siber juga bergantung sejauh mana kecekapan organisasi menangani dan mengurus keselamatan siber serta maklumat.

Bagi memastikan keselamatan siber terjamin dalam situasi pekerja bekerja dari rumah, terdapat beberapa perkara boleh dilakukan organisasi.

Pertama, prasarana teknologi maklumat seperti komputer riba dan capaian internet perlu disediakan majikan dengan mengambil kira polisi keselamatan maklumat, penggunaan perisian keselamatan seperti perisian antivirus serta tembok api dikemas kini dan sistem komunikasi melalui proses enkripsi.

Kedua, penyediaan perimeter keselamatan oleh majikan dalam capaian data, rangkaian dan sistem maklumat sebuah organisasi seperti penggunaan rangkaian persendirian maya (VPN), penyediaan kata laluan dan sistem pengesahan kukuh, mekanisme keselamatan perlu dalam menangani capaian rangkaian organisasi mencurigakan.



Sekiranya kedua-dua perkara itu dapat dilaksanakan, risiko ancaman keselamatan siber akan berada pada tahap rendah. Dengan ini, pihak jabatan teknologi maklumat atau unit mengurus keselamatan siber boleh memberi fokus dalam menangani ancaman keselamatan siber dengan lebih spesifik.

Antaranya, pihak terbabit berupaya membuat jangkaan jenis serangan atau ancaman keselamatan siber lebih spesifik yang berupaya membuat lonjakan tinggi kehadirannya atau mengancam persekitaran digital organisasi.

Ia juga berupaya memberi fokus lebih kepada titik kritikal keselamatan siber bagi sesebuah organisasi seperti sistem kewangan dan perakaunan, storan digital penyimpanan fail dikongsi, pangkalan data pengguna serta korporat, sistem perkhidmatan e-mel organisasi, sistem maklumat dan komputer pelayan.

Ia juga berupaya menyediakan penyelesaian dan pengukuran teknikal dalam menangani aktiviti digital lebih selamat kepada pekerja seperti pengurusan kata laluan cekap serta selamat.

Begitu juga penggunaan storan melalui proses enkripsi bagi menyimpan maklumat sensitif, penggunaan pengesahan dua faktor, pelaksanaan polisi keselamatan siber dan pendidikan keselamatan siber.

Pihak berkenaan juga berupaya menangani perkongsian maklumat rahsia antara pekerja dengan cekap dan selamat. Banyak kaedah boleh digunakan untuk capaian ke rangkaian organisasi, penghantaran fail, kawalan sistem dari jarak jauh dan capaian perkhidmatan e-mel dengan penggunaan sistem enkripsi bersama-sama dengannya.

Contohnya, penggunaan protokol enkripsi S/MIME untuk penghantaran e-mel dan penggunaan VPN untuk capaian ke rangkaian organisasi.

Ia juga berupaya melihat keselamatan siber setiap struktur organisasi secara keseluruhan dan mengenal pasti kumpulan pekerja berisiko tinggi menyumbang ancaman keselamatan siber.

Pihak pengurusan perlu merencanakan strategi utuh, cekap dan berkesan dalam menangani ancaman keselamatan siber bagi membolehkan bekerja dari rumah sebagai norma baharu.

Penulis adalah *Pensyarah, Jabatan Keselamdtan Maklumat dan Teknologi Web, Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Tun Hussein Onn Malaysia*