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

NUKLEAR MALAYSIA

TARIKH	JUMAAT, 7 JANUARI 2022
AKHBAR	BERITA HARIAN
TAJUK ARTIKEL	PELAKSANAAN AKTA ENKRIPSI TANGANI KETIRISAN DATA, MAKLUMAT
M/S	12
BIDANG	MANAGEMENT
KATA KUNCI	DATABASE MANAGEMENT

Pelaksanaan akta enkripsi tangani ketirisan data, maklumat

Oleh Dr Shekh Faisal Abdul Latip
bhrencana@bh.com.my

Pensyarah Kanan (Kriptografi dan Keselamatan Maklumat) di Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM)

Perkembangan pesat dalam dunia teknologi maklumat dan komunikasi menyebabkan pemprosesan maklumat dan aktiviti komunikasi semakin pantas.

Secara umum, perkembangan ini mematuhi dua hukum dikenali Moore's Law dan Nielsen's Law.

Moore's Law merumuskan bahawa kuasa komputer meningkat 60 peratus setiap tahun, manakala harga komputer berkurangan dalam kadar serupa bagi tempoh sama.

Bagi jalur lebar internet pula, Nielsen's Law merumuskan perkembangannya meningkat 50 peratus setiap tahun. Trend ini menyebabkan peningkatan kepada jumlah pengguna dan pemilik peranti digital yang semakin laju dan murah harganya.

Era Revolusi Perindustrian Keempat (IR 4.0) mencakupi pelbagai teknologi baharu seperti internet kebendaan (IoT) yang membabitkan pelbagai peranti digital yang terangkai dalam rangkaian internet dan penyimpanan maklumat di 'cloud' (awan), turut merancakkan penggunaan peranti digital dan mampu meningkatkan capaian data serta maklumat tanpa sempadan.

Walaupun secara dasarnya dilihat positif, ia juga boleh mengundang impak buruk jika maklumat dihasilkan, disimpan dan dipindahkan menggunakan peranti digital ini tidak dipelihara dari segi keselamatan, terutamanya dari aspek kerahsiaan.

Data dan maklumat daripada peranti digital ini merangkumi pelbagai bentuk termasuklah multimedia, audio, video, penstriman data, transaksi dalam talian, data rangkaian komunikasi, dokumen dan sebarang data mentah yang disimpan.

Secara prinsip, sistem keselamatan peranti digital perlu menjamin ciri CIA tiga serangkai merujuk 'confidentiality' (kerahsiaan), 'integrity' (integriti) dan 'availability' (ketersediaan).

Kes ketirisan data dan maklumat di negara ini yang sering berlaku dan semakin meningkat setiap tahun berpunca kurangnya kesedaran awam tentang kepentingan dan cara berkesan melindunginya. Perkembangan dalam dunia teknologi maklumat dan komunikasi berlaku secara eksponen ini, turut memudah dan mempercepatkan penyebaran data serta maklumat berkenaan.

Bagi menangani masalah ini, mekanisme paling ampuh untuk memelihara kerahsiaan data dan maklumat adalah menerusi penggunaan enkripsi - satu mekanisme dalam bidang kriptografi.

Enkripsi boleh difahami sebagai suatu bentuk algoritma yang menukarkan maklumat asal kepada kod tulisan rahsia atau lebih dikenali teks sifer yang tidak mampu difahami maknanya oleh pihak ketiga.

Bagi membolehkan maklumat asal diperoleh kembali daripada teks sifer, ia memerlukan algoritma dekripsi berserta satu kunci dekripsi rahsia yang hanya boleh diketahui individu yang diberikan autoriti untuk melihat data dan maklumat berkenaan.

Bagi menyokong penggunaan algoritma kriptografi, Dasar Kriptografi Negara digubal pada 2013, bertujuan menggariskan kaedah dan pendekatan strategik dari aspek penggunaan algoritma kriptografi, pembangunan produk kriptografi serta penyelidikan dan pembangunan maklumat kerajaan dan agensi.

Namun, sehingga kini tiada akta khusus berkaitan enkripsi bagi memastikan penguatkuasaan penggunaan enkripsi untuk melindungi data dan maklumat orang ramai, sektor awam, swasta dan pentadbiran kerajaan berserta mengelakkan enkripsi disalah guna sebagai instrumen melakukan jenayah.

Akta jenayah komputer sedia ada yang sering digunakan pihak berkuasa bagi menangani kes ketirisan data dan maklumat pula sekadar mampu digunakan selepas berlakunya jenayah dan kerosakan. Namun, kesan ketirisan maklumat sukar dipulihkan terutama apabila maklumat menular ke pengetahuan umum atau pihak berkepentingan sama ada dalam atau luar negara.

Lantas, satu akta baharu yang bersifat preventif (mencegah) dan punitif (menghukum) amat diperlukan untuk tujuan ini. Akta enkripsi dibentuk perlulah mengguna pakai Dasar Kriptografi Negara bagi memastikan hanya kaedah dan algoritma sesuai dan selamat digunakan.

Ia juga seharusnya menggariskan larangan dan hukuman bagi individu yang mendedahkan kunci dekripsi kepada pihak ketiga yang tidak mempunyai autoriti sama ada secara sengaja atau sebaliknya.

Bagi mengelak pendedahan kunci dekripsi berlaku secara tidak sengaja akibat kecuaian pengguna, kaedah penyimpanan kunci dekripsi selamat dan sukar dicapai pihak ketiga tidak berautoriti haruslah dikuatkuasakan. Sebagai contoh, kunci dekripsi disimpan dalam peranti tahan gangguan.

> "Isu ketirisan data dan maklumat dalam negara sememangnya semakin serius dan membabitkan semua peringkat sama ada orang awam, rekod perubatan, institusi kewangan, ahli politik, kerajaan mahu pun swasta

Bagi menangani kes penyalahgunaan enkripsi untuk tujuan jenayah, hukuman tegas perlulah dibentuk seperti ketegasan dalam undang-undang siber Malaysia. Harus difahami reka bentuk algoritma enkripsi moden berdasarkan Kerckhoff's Principle menyatakan, kekuatan algoritma enkripsi mestilah hanya bergantung kepada kerahsiaan kunci dekripsi, bukannya bergantung kerahsiaan reka bentuk algoritma digunakan.

Tanpa pengetahuan tentang kunci dekripsi, mustahil proses dekripsi dilakukan bagi mendapatkan maklumat asal walaupun peranti menggunakan algoritma enkripsi berada di tangan pihak berkuasa.

Tambahan pula, saiz kunci dekripsi diperuntukkan bagi algoritma enkripsi moden menghalang kunci ini daripada dapat dikenal pasti, walaupun menggunakan sebarang teknologi moden dan canggih masa kini.

Justeru, bagi mengatasi masalah penyalahgunaan enkripsi untuk tujuan jenayah, ketegasan hukuman terhadap penjenayah hanyalah satu-satunya jalan penyelesaian.

Dalam keadaan tertentu - terutama atas sebab kepentingan negara dan keselamatan awam - data atau maklumat dalam bentuk teks sifer perlu dilakukan dekripsi oleh pihak ketiga berautoriti seperti kerajaan, bagi membolehkan kandungan data dan maklumat asal diperoleh.

Bagi tujuan ini, akta enkripsi harus menggariskan pelaksanaan eskrow (dokumen sah yang memuat perjanjian mengenai aset) kunci dekripsi bagi membolehkan perkara ini dilakukan pihak ketiga berautoriti dalam keadaan sangat terkawal, contohnya di bawah perintah mahkamah.

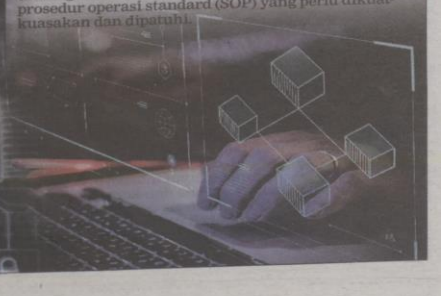
Namun demikian pelaksanaan eskrow kunci dekripsi ini mempunyai beberapa masalah teknikal dan kontroversi tersendiri yang perlu diberi perhatian sekiranya ingin dilaksanakan. Banyak negara cuba melaksanakannya, tetapi menemui kegagalan. Oleh itu, kajian mendalam diperlukan bagi mengkaji kesesuaian pelaksanaannya di negara ini.

Isu ketirisan data dan maklumat dalam negara sememangnya semakin serius dan membabitkan semua peringkat sama ada orang awam, rekod perubatan, institusi kewangan, ahli politik, kerajaan mahu pun swasta.

Ia memberi impak besar terhadap keselamatan awam, sistem demokrasi dan semestinya menggangu kestabilan politik, kesejahteraan dan ekonomi negara, malah turut memberi kesan terhadap reputasi dan kredibiliti individu dan institusi terbabit.

Masalah ini seharusnya dibendung segera bagi mengelakkan keadaan semakin parah seperti menularnya wabak COVID-19 di serata dunia.

Ia hanya dapat diatasi jika enkripsi dijadikan vaksin bagi melindungi data dan maklumat, manakala undang-undang menerusi akta enkripsi dijadikan prosedur operasi standard (SOP) yang perlu dikuatkuasakan dan dipatuhi.



DISEDIAKAN OLEH	**1-PN NOR SURIANI BINTI MOHD ZIN (S44), BPM** **2-CARLOS LINTON (S19), BPM** UNIT PERPUSTAKAAN, BPM