pada pautan berbahaya, penggodam mampu mendapatkan capaian kepada akaun bank, data korporat atau maklumat peribadi mangsa yang sangat sensitif.

Penggodam juga menggunakan pelbagai teknik antiforensik yang canggih dalam menjalankan serangan siber. Situasi ini boleh dianalogikan seperti perang digital antara seekor kucing dengan tikus. Semakin canggih teknologi teknik, semakin canggih juga teknik antiforensik yang digunakan oleh penggodam untuk mengelakkan jejak digital mereka dikesan. Tindakan ini termasuklah pemadaman fail secara kekal, pengubahan metadata atau penggunaan alat untuk menutup rekod aktiviti mereka.

Pemulihan Data Siber: Rangka Kerja yang Diperlukan

Apabila serangan siber berlaku, bagaimanakah sesebuah organisasi atau individu boleh memulihkan sesuatu data? Pemulihan data bukan sahaja bermaksud mendapatkan kembali capaian kepada maklumat, tetapi memastikan data tersebut tidak rosak atau tercemar oleh serangan. Proses ini memerlukan pendekatan yang sangat teliti.

Langkah pertama dalam pemulihan data yang efektif adalah dengan melakukan sandaran data (data backup) secara berkala. Organisasi besar seperti hospital dan bank harus mempunyai sistem automatik yang melakukan sandaran data harian, terutamanya data kritikal.

Sandaran data ini juga harus disimpan di lokasi yang berbeza, misalnya melalui perkhidmatan awan (cloud) dalam pasaran seperti AWS atau Microsoft Azure. Dengan adanya sandaran data yang terkini, sesuatu data itu dapat dipulihkan dengan cepat sekiranya berlaku sebarang serangan siber.

Diakui bahawa sandaran data mewujudkan ruang pemulihan yang besar, namun pengujian sistem pemulihan merupakan mekanisme yang perlu diberikan penekanan. Pengujian berkala terhadap keupayaan untuk memulihkan data dapat memastikan organisasi bertindak dengan cepat apabila berlakunya sesuatu krisis. Pepatah "cegah sebelum parah" perlu dipraktikkan kerana kerosakan kritikal boleh terjadi sekiranya tiada tindakan tuntas dilakukan sewaktu masa genting pemulihan data.

Teknologi terkini seperti kecerdasan buatan atau pembelajaran mesin boleh digunakan untuk memantau dan mengesan anomali dalam sistem data. Teknologi ini dapat mengesan aktiviti yang mencurigakan lebih awal dan memberikan peluang kepada organisasi untuk bertindak balas sebelum serangan siber berlaku. Sistem ini juga berupaya membantu proses pemulihan data dengan mempercepat analisis data dan memastikan kesahihan maklumat selepas berlakunya serangan siber.

Satu daripada faktor yang lemah dalam mana-mana sistem keselamatan ialah sikap pengguna itu sendiri. Oleh hal yang demikian, sesebuah organisasi hendaklah melatih para pekerja tentang ancaman siber dan cara untuk mengenali taktik pancing data atau e-mel palsu. Perkara ini boleh menjadi garis pertahanan pertama yang paling berkesan dalam menangani serangan siber.

Peranan Kerajaan dalam Keselamatan Data dan Pemulihan Siber

Kerajaan bertanggungjawab untuk menggubal undang-undang, menyediakan infrastruktur dan memastikan organisasi mematuhi piawaian keselamatan tertentu. Di Malaysia, langkah keselamatan siber dipantau oleh agensi khusus seperti Agensi Keselamatan Siber Negara serta Suruhanjaya Komunikasi dan Multimedia Malaysia.

Dasar Keselamatan Siber

Malaysia mempunyai Polisi Keselamatan Siber Kebangsaan atau National Cyber Security Policy (NCSP) yang diperkenalkan untuk melindungi infrastruktur kritikal negara dan memacu kesedaran keselamatan siber. NCSP memberikan tumpuan kepada perlindungan sistem maklumat kritikal dalam sektor awam dan sektor swasta serta berfungsi memastikan setiap entiti memahami kepentingan keselamatan data.

Sebagai tambahan, inisiatif seperti Cyber999 Help Centre yang dikendalikan oleh Malaysia Computer Emergency Response Team (MyCERT) menawarkan perkhidmatan bantuan kepada organisasi yang menjadi mangsa serangan siber. MyCERT bukan sahaja membantu dalam pemulihan data, malah menyediakan latihan dan panduan pencegahan kepada syarikat dan individu untuk mengelakkan serangan siber pada masa hadapan.

Undang-undang Perlindungan Data

Dalam konteks pemulihan data siber, kerajaan memainkan peranan melalui penggubalan undang-undang perlindungan data. Di Malaysia, Akta Perlindungan Data Peribadi 2010 mewajibkan organisasi untuk melindungi data peribadi pengguna. Akta ini bukan sahaja melindungi hak individu tetapi memaksa syarikat untuk mengambil langkah lebih proaktif dalam melindungi dan memulihkan data selepas berlakunya serangan siber.

Dalam dunia yang semakin bergantung pada teknologi, keselamatan dan pemulihan data merupakan isu yang tidak boleh diabaikan. Serangan siber akan terus meningkat dalam skala kecanggihan. Masyarakat harus bersiap sedia untuk menghadapinya. Data yang hilang berupaya mengakibatkan kerugian yang besar kepada sesebuah organisasi dan individu. Oleh hal yang demikian, pemulihan data siber yang pantas dan cekap perlu menjadi semakin kritikal.

Pihak kerajaan melalui inisiatif yang berterusan seharusnya memainkan peranan penting dalam memastikan keselamatan data dan memacu pemulihan data selepas serangan siber. Oleh itu, perlindungan terhadap data harus menjadi keutamaan bagi memastikan aset digital ini terus dilindungi dan integritinya terpelihara.

Nor Ika Shahirah Ramli dan Tarmizi Mohammad Shukri

ADAKAH DATA CUKUP DILINDUNGI?

Data merupakan teras kepada setiap aspek kehidupan. Manusia, sama ada dalam sektor awam, sektor swasta ataupun kehidupan peribadi kini beroperasi sepenuhnya dalam dunia yang berlandaskan maklumat.

Perkembangan teknologi digital pada masa ini telah menyebabkan kemajuan yang pesat. Ancaman terhadap keselamatan data juga semakin meningkat seiring dengan perkembangan tersebut. Serangan siber seperti perisian tebusan (ransomware), kecurian data dan serangan pancing data (phishing) yang semakin canggih mengakibatkan perlindungan dan pemulihan data siber kini menjadi satu daripada keutamaan yang kritikal.

Dalam dekad terakhir ini, ledakan teknologi digital telah menyebabkan berlakunya fenomena yang dikenali sebagai data raya. Data raya merujuk pengumpulan, penyimpanan dan pemprosesan jumlah maklumat yang besar. Data ini meliputi setiap sudut kehidupan manusia, termasuklah data perbankan dan perubatan sehinggalah tingkah laku dalam media sosial.

Sebagai contohnya, apabila setiap kali pengguna membuat pembelian secara dalam talian, syarikat seperti Amazon atau Lazada akan menyimpan maklumat transaksi yang dilakukan. Data ini merangkumi maklumat kad kredit, alamat penghantaran dan butiran produk yang dibeli. Dalam dunia perubatan pula, rekod pesakit disimpan secara elektronik untuk memudahkan capaian dan perkongsian maklumat antara hospital dengan doktor. Kesemua hal ini menunjukkan betapa pentingnya data dalam operasi harian.

Pada masa yang sama, cabaran keselamatan siber semakin membarah seperti cendawan tumbuh selepas hujan. Serangan siber menjadi lebih kompleks selain menyasarkan maklumat peribadi dan komersial dengan cara yang lebih licik. Pelbagai serangan siber yang menjejaskan fungsi hospital, sekolah dan kerajaan di seluruh dunia menjadi kayu ukur bahawa ancaman ini sememangnya berbahaya.

Ancaman Siber: Serangan dan Implikasinya

Malaysia tidak terlepas daripada menjadi sasaran serangan siber yang semakin canggih. Menurut Menteri Pertahanan, Yang Berhormat Dato' Seri Mohamed Khaled Nordin yang tersiar dalam *Berita Harian* pada 30 Mac 2024 lalu, negara ini menerima lebih daripada 3000 ancaman serangan siber pada setiap hari.

Serangan ini bertujuan untuk membolosi sistem keselamatan negara, sekali gus menimbulkan risiko yang serius. Ancaman keselamatan negara kini bukan sahaja berbentuk fizikal, malah melibatkan ancaman siber.

Statistik ini jelas menunjukkan bahawa isu keselamatan siber tidak boleh dipandang remeh kerana berpotensi menggugat kestabilan nasional. Oleh hal yang demikian, pengukuhan infrastruktur digital dan kesedaran masyarakat tentang kepentingan keselamatan siber perlu dipertingkat bagi mengurangkan risiko serangan siber.

Serangan perisian tebusan merupakan bentuk serangan yang paling ketara dan berterusan pada masa ini. Sebagai contohnya, serangan perisian tebusan WannaCry pada tahun 2017 telah melumpuhkan lebih daripada 200 ribu komputer di seluruh dunia, termasuklah sistem kesihatan di United Kingdom dan 150 negara lain. Keadaan ini membuktikan bahawa rentannya organisasi besar terhadap serangan siber, sekali gus mendedahkan kelemahan dalam infrastruktur digital global.

Lebih membimbangkan, banyak organisasi di negara membangun, termasuklah Malaysia mungkin tidak mempunyai perlindungan yang mencukupi untuk menghadapi serangan siber seumpama ini. Tanpa langkah pencegahan dan tindak balas yang berkesan, negara akan terus berhadapan dengan risiko yang kian meningkat.

Dalam kes perisian tebusan, data sering disulitkan tanpa pengetahuan pemilik. Dalam erti kata yang lebih mudah, data pengguna "diculik", dikunci dan dikodkan dengan bahasa asing. Tanpa kunci penyulitan yang tepat, data tersebut sukar untuk dipulihkan. Pengguna pula diugut untuk membuat bayaran tebusan bagi "membebaskan" data mereka. Sekiranya tidak, data tersebut akan dihapuskan atau dijual dalam pasaran gelap.

Selain itu, serangan pancing data yang menyamar sebagai mesej e-mel atau teks sah kian meluas penyebarannya. Dengan menipu mangsa untuk berkongsikan maklumat peribadi atau mengklik