MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

LANDSKAP KESELAMATAN SIBER MALAYSIA 2020:

APAKAH PERSIAPAN MENGHADAPI CABARAN KESELAMATAN SIBER MENDATANG?

CONTENTS

PENGENALAN

Kepesatan peredaran ilmu pengetahuan dan kemajuan teknologi telah berkembang dengan begitu mendadak sejak beberapa tahun kebelakangan ini. Kemajuan teknologi ini telah memberi impak dan berupaya mengubah cara hidup dan peradaban manusia termasuk melakukan aktiviti rutin dalam kehidupan seharian kita. Perkembangan teknologi digital menunjukkan bahawa pencapaian manusia dalam kehidupan seharian semakin lancar, mudah dan cepat. Malah, perubahan teknologi dan kebergantungan terhadap Internet yang semakin tinggi ini juga telah mempengaruhi aktiviti seharian individu, pendidikan, kesihatan, perniagaan dan pentadbiran.

Pada masa sekarang terdapat isu-isu yang mendesak dalam persekitaran digital negara yang boleh menjejaskan keselamatan negara. Ancaman siber terbukti memberi kesan buruk kepada negara kerana ia menggalakkan aktiviti jenayah dan ketidakadilan sosio-ekonomi di kalangan masyarakat. Selari dengan perkembangan teknologi semasa dan tahap kecerdikan masyarakat, salah laku tersebut juga menjadi kian kompleks sekaligus menyukarkan kegiatan mereka ditangani oleh pihak berkuasa.

Jenayah siber dilihat lebih praktikal kepada penjenayah dan menyebabkan jenayah siber ini menjadi pilihan berbanding jenayah tradisional. Malah, jenayah siber dilihat memberikan keuntungan yang lebih besar kepada penjenayah. Namun, kerugian yang besar pula dialami oleh organisasi, perniagaan dan individu sekiranya menerima serangan siber. "Jenayah sebagai satu perkhidmatan" semakin berkembang menjadi trend dalam talian.

Antara jurang yang menyebabkan berlakunya jenayah siber seperti berikut:

a. Manusia – Sifat manusia yang inginkan keseronokan melayari internet, tanpa memahami ilmu keselamatan siber, sifat manusia yang ingin tahu dan juga kecuaian.

b. Proses – Merujuk kepada tiadanya garis panduan dan polisi yang dapat melindungi dari serangan siber dan tiada audit dalam menentukan tahap keselamatan siber.

c. Teknologi – Perkembangan dan percambahan teknologi yang canggih dan pesat.

ANALISIS PERSEKITARAN SIBER SEMASA

Persekitaran Siber Semasa. Peningkatan globalisasi dan digitalisasi telah membuka peluang kepada perkembangan jenayah siber. Daripada jenayah siber biasa seperti penipuan pembelian dalam talian, ucapan kebencian, gangguan siber dan lain-lain lagi. Jenayah siber kini memperlihatkan perkembangan ke arah jenayah siber terancang. Malah, jenayah ini mempunyai struktur organisasi yang mempunyai kelengkapan peralatan, kemahiran dan latihan bagi menjalankan operasi jenayah mereka.

Munurut Cybersecurity Ventures, kerugian jenayah siber pada tahun 2021 secara global akan mencapai $6 trilion. Malah, menurut PurpleSec, jenayah siber meningkat 600 peratus disebabkan Covid-19 pada tahun 2020. Serangan siber yang canggih dengan situasi semasa yang mendesak dan kekurangan profesional dalam keselamatan siber memberikan cabaran kepada keselamatan negara.

Di Malaysia, berdasarkan *Malaysia Cyber Emergency Response Team* (MyCERT) telah membahagikan pecahan insiden siber kepada dua kategori iaitu insiden teknikal dan insiden berkaitan kandungan. Insiden siber seperti berikut:

Revolusi Perindustrian Keempat (4IR) yang melibatkan teknologi memuncul seperti Data Raya, Realiti Terimbuh, Realiti Maya, *Blockchain*, Internet Benda, Pengkomputeran Awan, Kecerdasan Buatan dan sebagainya dilaksanakan bagi mentransformasikan Malaysia menjadi negara maju dan berpendapatan tinggi. Malahan juga menjadi negara peneraju serantau dalam bidang ekonomi digital.

Terdapat beberapa dasar dan pelan tindakan berkaitan digital yang telah dibangunkan dan dilaksanakan. Antaranya ialah **Strategi Keselamatan Siber Malaysia (MCSS)** yang telah diluluskan pada 15 Januari 2020 yang mana ia telah dibangunkan oleh Majlis Keselamatan Negara (MKN) melalui Agensi Keselamatan Siber Nasional (NASCA). Melalui dasar ini, Kerajaan telah menyenaraikan beberapa garis panduan dan peraturan yang perlu dipatuhi untuk organisasi, perniagaan dan masyarakat.

Unit Pemodenan Tadbiran dan Perancangan Pengurusan (MAMPU) juga telah membangunkan **Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)** pada April 2016 di bawah Teras Strategik ke 3 Pelan Strategik ICT Sektor Awam 2016-2020. Objektif RAKKSSA adalah untuk memberi panduan asas kepada agensi dalam merancang perlindungan yang diperlukan bagi ruang siber masing-masing dan memastikan keselamatan penyampaian perkhidmatan sektor awam serta meningkatkan tahap keyakinan pemegang taruh.

Selain itu, pihak Kementerian Komunikasi dan Multimedia Malaysia membangunkan **Program Penilaian Keselamatan Siber (PPKS)** untuk menilai tahap kesediaan keselamatan siber organisasi sektor awam di peringkat operasi dan teknikal. Program ini adalah untuk memberi panduan kepada organisasi sektor awam kaedah meningkatkan keselamatan siber organisasi mereka secara menyeluruh.

Ancaman Siber Semasa. Penggunaan digital transformasi dalam teknologi yang diguna pakai kini secara tidak langsung telah turut meningkatkan pelbagai ancaman siber di Malaysia seperti penipuan dalam talian, pencerobohan, kebocoran data dan lain-lain lagi. Perkembangan teknologi yang semakin canggih telah mendedahkan kepada persekitaran yang tidak selamat yang mengundang penjenayah untuk mengeksploitasi krisis semasa untuk mendapatkan wang dan maklumat demi untuk kepentingan sendiri. Makin ramai orang bergantung dan berurusan dengan Internet, semakin besar pula peluang penjenayah siber untuk mengambil kesempatan menimbulkan kekacauan terutamanya terhadap mereka yang berada dalam kesukaran lebih-lebih lagi dalam persekitaran pandemik Covid-19 kini. Mereka yang mudah menjadi mangsa adalah disebabkan tidak arif menggunakan Internet, kurang berpengetahuan mengenai isu semasa siber atau terlalu leka melayari Internet.

Pandemik dan Norma Baharu. Tahun 2020 dunia telah menyaksikan bagaimana pandemik Covid-19 yang melanda telah menyebabkan meningkatnya penggunaan digital teknologi disebabkan perintah kawalan pergerakan dan norma baharu penjarakkan sosial. Peningkatan digitalisasi telah membawa organisasi dan institusi pendidikan untuk mengamalkan kaedah bekerja dari rumah. Perintah kawalan pergerakan dan bekerja dari rumah telah menyebabkan masyarakat terpaksa memilih internet untuk tujuan berkomunikasi, berinteraksi dan meneruskan tanggungjawab mereka berkerja dari rumah. Penggunaan teknologi seperti sidang video, media sosial, platform membeli-belah dalam talian juga turut semakin meningkat dan merupakan pilihan yang terbaik dalam situasi Covid-19 kini. Bukan sahaja Covid-19 ini telah mengubah cara kita menghadapi teknologi digital semasa, tetapi turut mengubah cara kita menerapkan keselamatan siber. Perkara ini telah memberikan cabaran kepada masyarakat di seluruh dunia.

CABARAN ANCAMAN SIBER MEMUNCUL

Menurut laporan A.T Kearney yang bertajuk *The ASEAN Digital Revolution*, kerajaan di rantau ini sedang melaksanakan pembangunan infrastruktur komunikasi dan maklumat bagi tujuan digital ekonomi. Menurut laporan ini juga, Persatuan Negara-negara Asia Tenggara (ASEAN) mempunyai potensi menduduki tempat kelima antara digital ekonomi di dunia pada tahun 2025. Perkara ini turut melibatkan Malaysia yang kini sedang membangunkan polisi dan infrastruktur ke arah digitalisasi ekonomi ini. Selain itu, terdapat pendapat dari pakar mengenai rantau ASEAN akan membangun dan berkembang ke arah bandar pintar. Pembangunan bandar pintar ini telah disokong oleh kerajaan Malaysia menerusi pembangunan Cyberjaya sebagai 'Bandar Pintar dan Selamat'.

Namun begitu, cabaran dalam menuju digital ekonomi dan bandar pintar ini melibatkan pembangunan infrastruktur di kawasan pendalaman yang kini sedang dialami oleh Malaysia apabila anak-anak yang tinggal di kawasan pendalaman sukar untuk mendapatkan liputan internet bagi tujuan pembelajaran secara atas talian ketika Covid-19. Selain dari itu, Malaysia juga turut mengalami kekurangan tenaga kerja dalam bidang keselamatan siber dan wujudnya jurang pakar dalam pelbagai sektor. Kekurangan profesional keselamatan siber akan menjadikan organisasi mudah terdedah kepada ancaman siber. Apabila penggunaan Internet Benda dan teknologi digunakan dengan lebih meluas di bandar pintar, ia

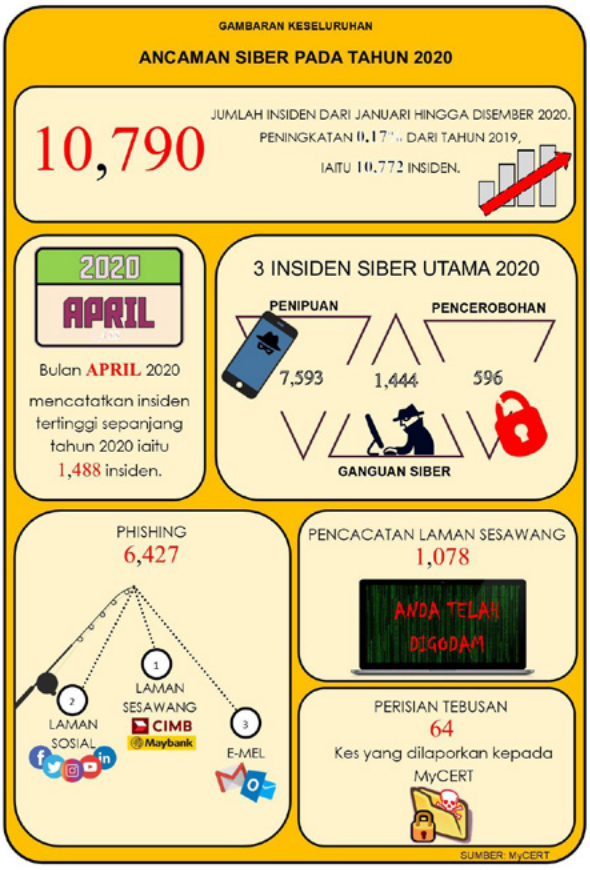
terdedah kepada tahap ancaman keselamatan. Perkara ini dapat menarik perhatian penjenayah siber untuk menceroboh sistem dan boleh melumpuhkan aspirasi bandar pintar tersebut.

Apabila teknologi memuncul berkembang, keselamatan siber juga sepatutnya seiring dengan teknologi tersebut. Namun, perkara yang sebaliknya berlaku. Malah, kesedaran keselamatan siber dikalangan organisasi, perniagaan dan individu masih ditahap yang rendah dan ini menjadi ancaman dalam teknologi memuncul.

TUJUAN

Tujuan kertas ini adalah untuk melihat sejauh mana ancaman siber yang berlaku dalam tahun 2020 dapat memberi implikasi kepada ancaman siber tahun 2021. Kemajuan teknologi jika tidak diuruskan dengan baik akan mewujudkan jurang dan kelompongan digital yang dapat menarik perhatian penjenayah. Berikutan pandemik Covid-19 yang melanda, ia telah mempengaruhi landskap keselamatan siber secara global dan domestik. Krisis Covid-19 ini telah mengubah masyarakat untuk bergantung kepada teknologi secara keseluruhan. Analisis mengenai ancaman siber tahun 2020 di Malaysia dibincangkan dan dihuraikan sebagai peringatan untuk menghadapi ancaman yang mendatang agar ancaman siber ini dapat diramal dan ditangani.

Laporan ini mengandungi empat bahagian yang membincangkan mengenai analisis ancaman siber tahun 2020 berdasarkan insiden siber yang berlaku di Malaysia, ancaman akan datang, ancaman siber ketika Covid-19 dan pendekatan keselamatan siber bagi menangani ancaman siber mendatang.



Statistik ini berdasarkan aduan insiden siber yang diterima daripada orang awam dan organisasi di dalam negara kepada CyberSecurity Malaysia (CSM) menerusi Jabatan Malaysia *Computer Emergency Response Team* (MyCERT). Laporan insiden keselamatan siber ini dirujuk kepada CSM melalui perkhidmatan Cyber999 yang disediakan oleh Jabatan MyCERT.

ANALISIS ANCAMAN SIBER 2020

Pada tahun 2020, terdapat peningkatan dalam kekerapan dan kepelbagaian ancaman siber seperti aktiviti penipuan dalam talian, perisian tebusan, kebocoran data, pengintipan siber, berita palsu dan ucapan kebencian di Malaysia. Ini berkemungkinan disebabkan pandemik Covid-19 yang berlaku ketika itu. Insiden keselamatan siber ini berdasarkan pemantauan CSM pada tahun 2020 yang merangkumi laporan yang disampaikan oleh pihak media. Ancaman siber boleh dibahagikan kepada dua iaitu insiden teknikal dan insiden bukan teknikal.

Insiden Berkaitan Kandungan

Penipuan. Berdasarkan laporan dari MyCERT, laporan penipuan yang diterima adalah sejumlah 7,593 insiden. Ini merupakan insiden paling tinggi dilaporkan dengan 70.37% daripada jumlah keseluruhan 10,790 insiden (9 kategori insiden). Jumlah penipuan ini menunjukkan penurunan sebanyak 2.33% berbanding tahun 2019 iaitu 7,774 insiden penipuan. Namun, insiden penipuan masih berlaku dalam berbagai bentuk. Malah pandemik yang melanda seluruh negara telah memperlihatkan peningkatan jenis penipuan siber yang berkaitan dengan Covid-19.

Penipuan Macau atau ***Macau Scam.*** Jumlah kerugian penipuan Macau pada tahun 2020 sehingga September adalah sejumlah RM232 juta dengan 4,764 kes. Berdasarkan fakta laporan yang berlaku, terdapat satu kes yang menyebabkan kerugian sejumlah RM 3.83 juta yang melibatkan seorang pesara berumur 90 tahun. *Macau Scam* antara penipuan yang semakin menjadi-jadi. Modus operandi mereka adalah dengan membuat panggilan telefon dan menyamar sebagai pihak penguatkuasa dari agensi-agensi kerajaan untuk memperdayakan mangsa bagi mendapatkan wang. Kemuncak insiden yang melibatkan *Macau Scam* ini yang telah mengakibatkan kerugian sejumlah RM85 juta adalah apabila tertangkapnya lima orang suspek antaranya yang bergelar Datuk dan Datuk Seri dalam bulan Oktober 2020.

Penipuan pelaburan dan juga **mata wang digital** mula menunjukkan peningkatan di kalangan rakyat Malaysia pada tahun 2020. Pada Januari 2020, seramai 87 orang warga China yang terbabit dalam sindiket penipuan pelaburan telah ditahan. Perkara ini berlaku kerana rakyat mula menunjukkan minat untuk melaburkan wang memandangkan situasi krisis Covid-19 yang mendesak kehidupan untuk mereka mencari jalan pintas. Susulan dari penipuan ini, penjenayah menjadi semakin kreatif dan mula membangunkan aplikasi di *Google Play* dan juga laman sesawang bagi meyakinkan mangsa.

Menurut kajian dari Telenor Group yang membuat kajian mangsa penipuan di Malaysia, India, Singapura dan Thailand, merumuskan bahawa rakyat Malaysia adalah yang paling terdedah kepada penipuan internet. Menurut laman web *Scam Watch* dari *Australian Competition & Consumer Commission*, terdapat 80,744 aduan yang diterima bagi insiden penipuan 2020 dengan kerugian $77,323,806.

Tiga trend penipuan yang sering dilaporkan ialah *phishing*, penipuan pembelian dalam talian dan kecurian identiti. Manakala, tiga jenis penipuan berdasarkan kerugian wang ialah penipuan pelaburan, *dating & romance* dan mengugut untuk mengancam nyawa dan lain-lain.

Phishing merupakan insiden yang paling banyak dilaporkan dengan 6,427 insiden siber iaitu 59.56% daripada jumlah keseluruhan insiden 10,790. Kebanyakan aktiviti *phishing* terutamanya melibatkan institusi kewangan, kemudian diikuti laman sosial dan emel. Menurut PDRM, Malaysia menerima lebih dari 100 laporan dalam sehari yang melibatkan *phishing* dan kategori yang banyak dilaporkan ialah *Vishing* (*Phishing* melalui panggilan telefon, *Smishing (Phishing SMS)* dan *Spear Phishing*.

Menurut laporan FBI bagi jenayah internet pada tahun 2019, **penipuan phishing** adalah antara jenayah yang sedang meningkat naik dengan kerugian USD57.8 juta yang melibatkan lebih dari 114,000 mangsa di Amerika Syarikat. Apa yang lebih mengejutkan, *phishing* yang berlaku adalah kerana kebocoran data dengan 32% kebocoran data melibatkan *phishing* berdasarkan laporan *Wandera 2020 Mobile Threat Landscape*.

Insiden Teknikal

Perisian Tebusan. MyCERT menerima 64 insiden mengenai perisian tebusan terhadap organisasi. Menurut laman ID Agent, 65% jangkitan perisian tebusan adalah menerusi *phishing*. Pada tahun 2019, 51% organisasi telah terjejas disebabkan perisian tebusan. Penjenayah berjaya menyulitkan data dalam 73% serangan berkenaan. Menurut laporan *The State of Ransomware 2020* dari Sophos, trend serangan perisian tebusan pada tahun 2020 adalah mempunyai fokus tersendiri dan kebanyakan sasarannya adalah serangan ke atas rangkaian. Laporan tersebut juga menyatakan 13% organisasi Malaysia akan membayar wang tebusan bagi mendapatkan kembali data.

Perisian tebusan yang kini menyasarkan infrastruktur kritikal adalah sangat membimbangkan kerana kebanyakan sektor ini belum bersedia sepenuhnya untuk melindungi infrastruktur mereka.

Laporan atau aduan mengenai serangan perisian tebusan kepada pihak penguatkuasaan masih lagi rendah di kalangan organisasi di Malaysia. Perkara ini berikutan imej organisasi akan tercalar sekiranya laporan dilakukan. Organisasi digalakkan untuk melaporkan sebarang insiden siber kepada pihak penguatkuasaan dan agensi seperti CSM supaya dapat memberikan khidmat nasihat dan siasatan untuk menangani ancaman ini.

Serangan perisian tebusan bukan sahaja menyerang organisasi/syarikat besar malah telah memfokuskan kepada infrastruktur kritikal seperti insiden serangan perisian tebusan terhadap syarikat pembekal elektrik Johannesburg dalam bulan Julai 2019. Selain pembekal elektrik, infrastuktur lain seperti hospital juga turut menjadi sasaran penggodam. Namun, yang lebih mengejutkan apabila serangan perisian tebusan ke atas Hospital Düsseldorf di Jerman dalam bulan September 2020 telah menyebabkan kematian seorang pesakitnya.

PERISIAN TEBUSAN

64

Insiden yang dilaporkan kepada MyCERT pada tahun 2020

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

AP German Hospital Hacked, Patient Taken to Another City Dies

By Associated Press on September 17, 2020

Share Tweet Recommend 1 RSS

German authorities said Thursday that what appears to have been a misdirected hacker attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment.

The Duesseldorf University Clinic's systems have been disrupted since last Thursday. The hospital said investigators have found that the source of the problem was a hacker attack on a weak spot in "widely used commercial add-on software," which it didn't identify.

Kebocoran data dilihat akan terus menjadi ancaman utama di Malaysia. Antara isu yang mendapat perhatian ialah kebocoran data pada bulan Mac 2020 yang melibatkan 37,145 butiran kad kredit. Pada bulan September dan Oktober, kebocoran data berlaku melibatkan data peribadi 1,400 rakyat Malaysia yang didakwa didalangi oleh syarikat teknologi China Zhenhua. Insiden ini mendapat perhatian kerana membabitkan kebocoran maklumat milik orang kenamaan di Malaysia. Selain itu, terdapat isu pencerobohan terhadap sistem pelanggan ShopBack yang mengurus maklumat peribadi pelanggan bagi perkhidmatan pembelian dalam talian.

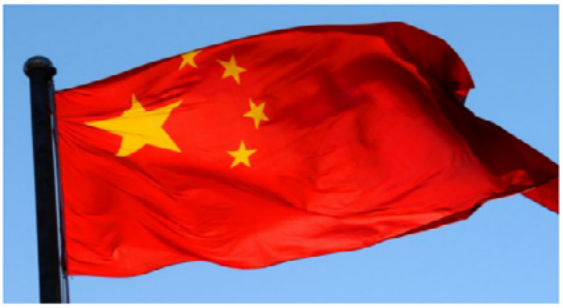
Kebocoran data juga dikaitkan dengan pengintipan siber oleh sesebuah negara bagi tujuan pertahanan negara mereka. Data mempunyai nilai yang strategik yang digunakan bagi menyerang negara lain dari segi ekonomi, politik dan sosial. Kebanyakan pengintipan siber ini dirancang dengan penuh teliti dan sukar untuk dikesan seperti kumpulan APT41 yang telah menjalankan aktiviti jenayah dan pengintipan sejak 2014 dan hanya dapat dikesan baru-baru ini.

Masyarakat hanya mengetahui bahawa negara kita turut menjadi mangsa pengintipan apabila terdapat laporan dari pakar keselamatan siber dari luar negara. Adalah dipercayai pengintipan siber ini akan berterusan untuk satu jangka masa yang panjang. Namun, untuk mengesan aktiviti pengintipan ini memerlukan keupayaan dan kesungguhan pihak-pihak yang berkenaan untuk menanganinya. Justeru itu, data termasuk data raya perlu dilindungi dengan lebih selamat melalui penggunaan kriptografi.

FMT news

HOME NEWS BERITA OPINION

Data peribadi 1,400 rakyat Malaysia terdedah akibat kebocoran maklumat China



Data merupakan sesuatu yang bernilai, sulit dan bersifat peribadi untuk dilindungi daripada dicuri atau digunakan untuk tujuan jenayah. Data yang dikumpul dan data yang dibocorkan merupakan ancaman siber yang boleh memberikan kesan yang mendalam. Punca penipuan berlaku adalah disebabkan kebocoran data yang mana ianya boleh diperolehi di web tertutup (dark web), dibocorkan disebabkan tiada perlindungan keselamatan siber atau kecuaian pekerja. Data yang dikumpul oleh penjenayah membolehkan mereka untuk melakukan berbagai jenis penipuan. Malah, penipuan dilihat akan terus berlaku kerana penipuan siber lebih mudah untuk dilakukan dan mengambil masa yang lama untuk dikesan. Agenda atau motif penjenayah melakukan penipuan siber adalah untuk mendapatkan kewangan secara mudah dan haram. Data juga dicuri untuk tujuan pengintipan siber.


TheStar

StarPlus News Asean+ Business Sport Metro Lifestyle

JPDP to look into number of Malaysians affected by ShopBack data breach

TECHNOLOGY

Monday, 28 Sep 2020
6:30 PM MYT

By Angelin Yeoh

The company, which offers cashback rewards for online shopping, said that its services and business operations have not been affected by the incident. — ANGELIN YEOH/The Star

Kerjasama dengan pihak penguatkuasa untuk melaksanakan Data Analitik adalah bertujuan untuk mengetahui trend penipuan siber di Malaysia dari segi modus operandi mereka untuk mengekang penipuan siber. Kerjasama ini amat diperlukan dengan segera kerana Data Analitik mempunyai kemampuan untuk mengetahui trend dan masalah yang mungkin berlaku lebih pantas daripada manusia.

Pengintipan siber. Pada Februari 2020, laman berita ZDNet melaporkan mengenai kumpulan penggodam China telah menyasarkan rangkaian komputer Kerajaan Malaysia untuk mencuri dokumen sulit kerajaan. Kumpulan penggodam ini dipercayai dikenali sebagai APT40 yang ditaja oleh kerajaan China yang turut menyasarkan negara-negara lain bagi mendapatkan maklumat sulit yang strategik kerana ianya menyasarkan pegawai kanan dan orang berkepentingan dalam institusi kerajaan.


FMT news

HOME NEWS BERITA OPINION

FMT finds 1,400 prominent Malaysians listed in Zhenhua data leak

Imran Ariff - October 3, 2020 9:30 AM

The Chinese company Zhenhua Data is believed to have compiled the data in an intelligence-gathering effort.

Pada bulan September 2020, sekali lagi negara China menjadi bualan hangat apabila dikaitkan dengan pengintipan siber sebuah syarikat Zhenhua Data yang berkait rapat dengan pihak tentera dan perisikan China yang telah mengumpul data raya dan menyebabkan kebocoran data 1,400 data rakyat Malaysia. Susulan pendedahan ini, senarai data 1,400 rakyat Malaysia telah dijumpai yang didapati menyasarkan individu yang berkuasa seperti kerabat diraja, ahli parlimen, menteri, pemimpin perniagaan yang terkemuka, bekas anggota tentera terkenal dan juga termasuk keluarga ahli politik.


ZDNet

Malaysia warns of Chinese hacking campaign targeting government projects

MyCERT security alert points the finger at APT40, a Chinese state-sponsored hacking crew.

By Catalin Cimpanu for Zero Day | February 7, 2020 -- 01:25 GMT (09:25 GMT+08:00) | Topic: Security

MORE FROM CATALIN CIMPANU

Security

Selain itu maklumat berkenaan turut mengandungi data mengenai individu yang telah didakwa berkaitan jenayah atau kesalahan seperti penipuan, pengedaran dadah, penculikan dan keganasan. Dalam bulan yang sama, dua rakyat Malaysia yang terbabit dengan operasi penggodaman antarabangsa didakwa di Amerika Syarikat bersama-sama dengan lima orang penggodam China yang mempunyai kaitan dengan *Advanced Persistent Threat* (APT). Penggodam ini menjadikan pegawai kerajaan Malaysia dan beberapa orang yang berkedudukan penting menjadi sasaran mereka untuk mendapatkan maklumat seperti yang berlaku pada Februari 2020.

Kegiatan pengintipan masa kini telah beralih dari kaedah tradisional kepada digital menyebabkan ianya sukar dikesan. Keadaan ini amat membimbangkan kerana data dan maklumat rahsia yang diperolehi

dapat menggugat keselamatan dan kestabilan negara serta turut melibatkan organisasi yang lain. Penggunaan teknologi terkini seperti APT menyebabkan ianya sukar dikesan di dalam sistem dan persekitaran siber yang menjadi sasaran. Justeru, pihak kerajaan dan industri perlu menggandakan usaha dan inisiatif dalam meningkatkan pelaburan dan keupayaan dari segi penggunaan teknologi terkini, penambahbaikan proses serta meningkatkan pengetahuan semua kakitangan dalam menangani insiden serangan siber termasuk aktiviti pengintipan. Tindakan ini bukan sahaja boleh menjejaskan kredibiliti agensi kerajaan tetapi juga sektor infrastruktur kritikal dan ekonomi negara.

Aktivis Penggodam (Hacker Activist (Hactivist)). Serangan siber melalui pencacatan laman sesawang seperti Gangguan Perkhidmatan Teragih di Malaysia (*Distributed Denial of Service* – DDoS) pencacatan visual laman sesawang (*web defacement*) di Malaysia lebih cenderung bermotifkan isu semasa. Penyerang menggunakan isu semasa untuk menyuarakan rasa tidak puas hati dengan melancarkan kempen serangan dalam ruang siber secara terbuka dan mempromosikan serangan secara besar-besaran di media sosial bagi meraih sokongan sebelum dan selepas melancarkan serangan. Serangan penggodam antara negara jiran ini boleh menjejaskan hubungan dua hala antara negara.

Sebanyak 1,078 laman sesawang di Malaysia menerima serangan dalam tahun 2020 seperti yang dilaporkan kepada MyCERT. Kebanyakan insiden serangan menyasarkan laman sesawang kerajaan, industri dan lain-lain. Pada penghujung tahun 2020, terdapat serangan pencacatan laman sesawang dari penggodam Indonesia dengan lebih dari 200 laman web dengan domain.my dan gov.my yang menjadi mangsa serangan ini. Sebagai balasan, penggodam dari Malaysia turut membalas dengan menyerang 300 VPN korporat Indonesia dengan mendedahkan senarai akses ID yang digodam. Serangan pencacatan laman web sesawang dari Indonesia ini pernah berlaku pada tahun 2019 berikutan isu penangkapan nelayan Indonesia di sempadan maritim antara Malaysia dan Indonesia, dan isu penyedia perkhidmatan pengangkutan awam Gojek.

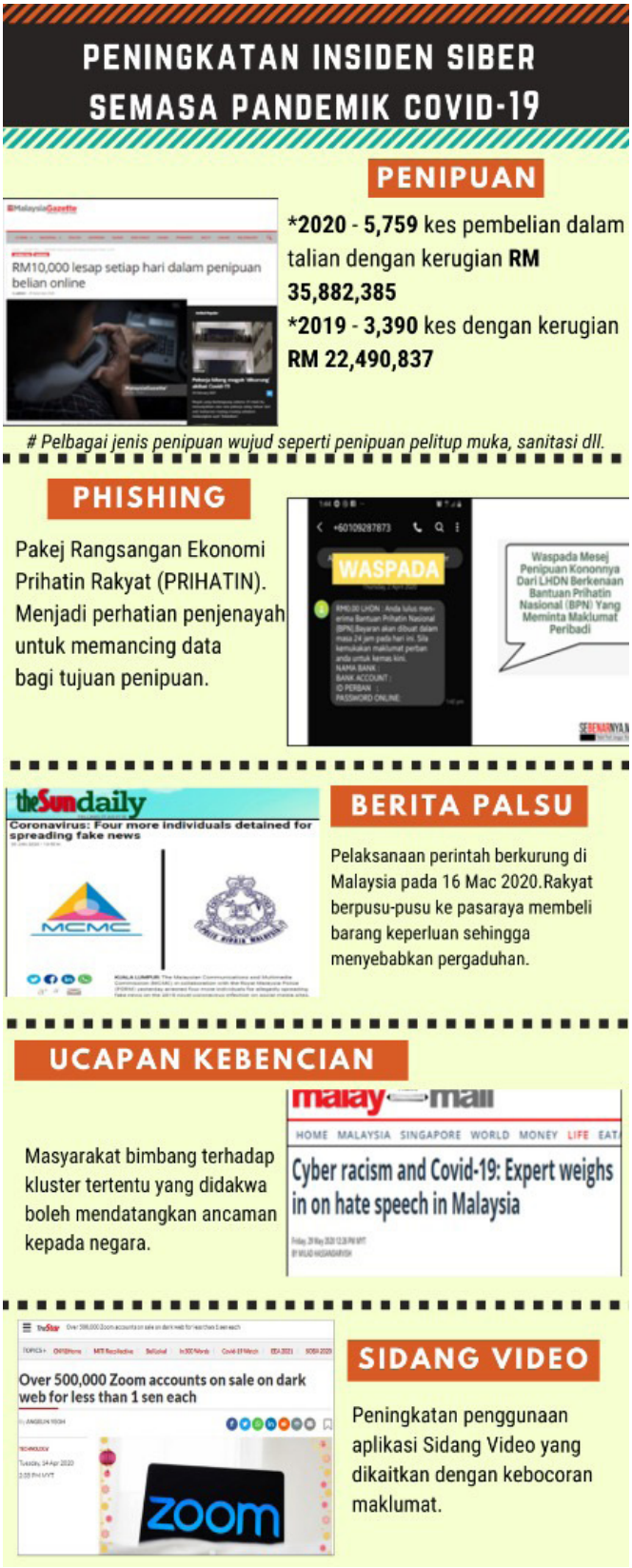
Berkaitan insiden pencacatan laman sesawang yang melibatkan dua negara berjiran, kerjasama keselamatan siber dua hala Malaysia dengan negara-negara rantau Asia perlu diwujudkan bagi memberi fokus dan memperkasakan kerjasama keselamatan siber di peringkat diplomatik. Sebagai contoh

hubungan dua hala berkaitan keselamatan siber di antara negara Jepun-India yang telah mengadakan Perbincangan Siber (*Cyber Dialogue*) bagi membincangkan keselamatan siber dan jenayah siber dalam konteks keselamatan dan ekonomi kedua-dua negara.

ANCAMAN SIBER KETIKA COVID-19

Wabak Covid-19 ini telah mengubah ekosistem dunia secara drastik, menjejaskan semua lapisan masyarakat dan memberi ruang kepada penjenayah siber mengambil kesempatan dalam suasana krisis yang dihadapi. Pelaksanaan Perintah Kawalan Pergerakan (PKP) menyebabkan rakyat Malaysia yang keluar bekerja diarahkan untuk bekerja dari rumah. Keadaan ini telah meningkatkan kebergantungan masyarakat terhadap teknologi dan juga peranti bagi tujuan komunikasi, berita, hiburan, perniagaan dan interaksi sosial.

Kebergantungan yang tinggi kepada Internet ketika Covid-19 telah menyebabkan berlakunya peningkatan jenayah siber. Krisis sebegini membuka peluang kepada penjenayah untuk mengaut keuntungan terutamanya melalui alam siber atau alam maya. Antara ancaman keselamatan siber ketika krisis Covid-19 yang mengubah landskap keselamatan siber adalah seperti di bawah :



ANCAMAN SIBER YANG MEMBIMBANGKAN DI MALAYSIA

Teknologi dan situasi semasa banyak mempengaruhi potensi aktiviti yang berniat jahat untuk dijalankan oleh pihak-pihak yang tidak bertanggungjawab. Berikut merupakan beberapa ancaman yang akan terus berlaku pada masa akan datang berdasarkan insiden yang lepas untuk persediaan kita menghadapinya di Malaysia:

a. Jenayah siber – paling menonjol ialah scam dan juga pelaburan atas talian seperti bitcoin. Oleh kerana kekerapan orangramai menggunakan aplikasi atas talian, ianya lebih banyak mendedahkan '*attack surface*' untuk penjenayah mengambil kesempatan. Insiden seperti **penipuan** akan terus berlaku pada masa akan datang dan tidak menunjukkan sebarang penurunan lebih-lebih lagi dalam situasi Covid-19 kini. Penambahan kepelbagaian jenis penipuan seperti penipuan pelaburan, penipuan mata wang kripto dilihat akan terus meningkat. Malah, penggunaan aplikasi dan laman sesawang untuk tujuan penipuan akan terus berlaku.

b. Insiden **kebocoran data** pula, penggodam lebih menyasarkan organisasi besar atau kerajaan yang mempunyai simpanan data yang bernilai dan data-data rahsia bagi sesebuah negara.

c. **Perisian Tebusan** juga akan terus berlaku dengan menyasarkan organisasi yang besar dan mampu untuk membayar wang tebusan. Malah, penjenayah siber akan turut menyasarkan infrastruktur kritikal negara terutamanya penjagaan kesihatan yang merupakan aset kritikal ketika Covid-19 kini. **Sindiket kumpulan jenayah siber** sudah mula memperlihatkan struktur urusan jenayah mereka yang begitu tersusun dengan mencari rakan kongsi untuk melakukan jenayah dan hasil keuntungan akan dinikmati bersama, penjenayah atau penggodamnya diberikan peralatan dan latihan untuk melakukan jenayah seperti sindiket serangan perisian tebusan *Netwalker*.

d. **Pengintipan Siber** oleh penggodam aktor negara luar terhadap Malaysia sangat signifikan kepada keselamatan negara Malaysia berdasarkan insiden Zhenhua Data yang diulas di bahagian atas. Tambahan lagi, dengan jumlah wang yang dilaburkan untuk projek digital telah menarik perhatian penggodam bukan sahaja pengintipan siber, malah jenayah siber. Pengintipan menyasarkan kepada perkhidmatan kritikal yang memberikan implikasi yang besar kepada keselamatan negara dan awam.

e. Berdasarkan insiden **hactivism** yang berlaku antara dua negara iaitu Malaysia dan Indonesia. Isu hacktivism ini tidak akan terhenti begitu sahaja. Perkara ini berlaku kerana ianya seakan satu cabaran di antara satu pihak dengan pihak yang lain untuk menunjuk-nunjuk keupayaan dan kebolehan masing-masing untuk membuat penggodaman.

Pendekatan Keselamatan Siber Bagi Menangani Ancaman Siber Mendatang

Pendekatan aspek keselamatan siber perlu berubah kepada pendekatan secara holistik dan bukan sekadar pendekatan berdasarkan teknologi semata-mata. Pendekatan yang lebih strategik ini perlu merangkumi tiga komponen iaitu proses, teknologi dan manusia. Ketiga-tiga komponen ini boleh dikategori juga sebagai *Defense in Depth* (DiD) iaitu satu siri mekanisme pertahanan berlapis untuk melindungi data dan maklumat yang berharga. Sekiranya satu mekanisme gagal, terdapat langkah-langkah keselamatan lain untuk segera menghalang serangan. Tiga (3) komponen pendekatan holistik keselamatan siber diterangkan di bawah.

Proses. Satu daripada tiga komponen pendekatan holistik adalah aspek proses iaitu dari sudut garis panduan atau undang-undang atau peraturan. Ianya perlu direka seiring dengan objektif organisasi dan merangkumi kesemua elemen keselamatan organisasi dari segi keselamatan fizikal mahupun siber. Kerajaan Malaysia telah membangunkan Dasar Keselamatan Siber Nasional atau *National Cyber Security Policy* (NCSP) pada tahun 2006 dan telah ditambahbaikkan dengan Strategi Keselamatan Siber Malaysia pada tahun 2020 yang menangani risiko terhadap Infrastruktur Maklumat Nasional Kritikal (CNII) yang terdiri daripada sistem maklumat rangkaian sepuluh sektor kritikal, perniagaan, industri dan masyarakat.

Strategi ini dibuat untuk mewujudkan kepercayaan dalam persekitaran siber bukan hanya untuk keselamatan negara tetapi juga untuk menyokong agenda Kerajaan dalam ekonomi digital, Industri 4.0 dan penggunaan teknologi yang berkaitan untuk kemajuan Malaysia. Elemen penguatkuasaan, perundangan dan peraturan perlulah diperkasakan dan digunapakai oleh semua sektor. Ini adalah penting kerana serangan siber dan pencerobohan data tidak hanya tertumpu kepada aspek perseorangan atau individu tetapi akan melibatkan impak kepada keselamatan awam, perkembangan ekonomi dan kedaulatan negara.

Teknologi. Tidak dapat dinafikan bahawa perkembangan teknologi terkini antaranya teknologi yang berasaskan *Financial Technology (Fintech)*, 4IR, Internet Benda, *Blockchain*, kecerdasan buatan, kriptografi, matawang digital dan lain-lain lagi. Namun, kecanggihan teknologi tersebut boleh juga disalah gunakan oleh mereka yang tidak bertanggungjawab untuk melakukan pelbagai perbuatan jenayah siber bagi mengganti kaedah tradisional. Malahan, ia akan menjadi kian rumit apabila dilakukan menerusi pasaran gelap Internet *(Internet black market)*.

Teknologi digital yang dibangunkan atau digunakan perlu memenuhi beberapa kriteria termasuk pematuhan piawaian antarabangsa, kaedah perlindungan yang diperakui, pensijilan, penilaian kepada kerentanan sistem dan sebagainya. Penggunaan teknologi termaju di dalam bidang Data Analitik juga mampu memberi impak ketara terhadap keselamatan siber. Ini boleh dilihat dari aspek pengumpulan maklumat risiko, ancaman serta serangan yang berlaku di seluruh dunia. Pengumpulan maklumat yang berobjektif mampu memberi maklumat tertentu samada mengenai serangan siber, ancaman perisian jahat (malware), motif dan pelbagai informasi berguna yang lain. Sehubungan itu, Dasar Kriptografi Negara yang telah diluluskan pada tahun 2013 perlu dikuatkuasakan dan dilaksanakan dengan lebih agresif dan secara menyeluruh merangkumi aspek keselamatan dalam ekosistem kriptografi negara.

Manusia. Hampir kesemua pakar keselamatan siber bersetuju bahawa elemen manusia adalah titik kelemahan terbesar. Ini terbukti apabila insiden-insiden pencerobohan ke atas bank-bank besar di dunia melibatkan elemen *phishing* e-mel. Ianya adalah perangkap e-mel yang dihantar kepada pekerja bank yang direka bagi menarik minat seseorang untuk membuka e-mel dan mengikut arahan yang diberikan. Dalam hal ini, langkah pencegahan seperti program kesedaran dan latihan perlu sentiasa diadakan dengan lebih kerap dan berkala. Pendekatan ni juga perlu diadakan terhadap segenap lapisan hirarki organisasi termasuk pihak atasan. Ini perlu kerana serangan siber tidak mengira sesiapa pun dan penggodam akan menyerang dari segenap sudut bagi mencapai objektif niat jahat mereka.

Bagi merapatkan jurang ini, CSM sedang membangunkan program Kerangka Pembangunan Kapasiti Keselamatan Siber. Di dalam program Kerangka Pembangunan Kapasiti Keselamatan Siber ini, terdapat tiga (3) program yang menyasarkan kumpulan tertentu mengikut keperluan iaitu;

a. **Global Accredited Cybersecurity Education (ACE) Scheme**. Melahirkan profesional keselamatan siber yang mampu merancang dan melaksanakan inisiatif keselamatan siber.

b. **Cyberguru**. Melahirkan pengamal keselamatan siber yang berkeupayaan teknikal dan mahir dalam operasi.

c. **Cyber Security Awareness For Everyone (SAFE)**. Memupuk pengetahuan keselamatan siber terhadap kumpulan atau individu yang berdaya tahan terhadap insiden keselamatan siber.

PENUTUP

Ancaman siber akan berlaku secara berterusan selagi teknologi dan internet itu digunakan. Malah, keadaannya mungkin menjadi lebih mencabar dan merumitkan kepada keselamatan siber terutamanya dalam situasi pandemik Covid-19 ini. Tambahan pula, tahap keselamatan siber di Malaysia juga masih rendah dan mudah terdedah terhadap serangan siber.

Kesemua fakta dan insiden yang dilaporkan di atas boleh digunakan sebagai pendedahan dan maklumat kepada masyarakat agar sentiasa berwaspada dan beringat sewaktu melayari internet agar segala urusan yang dibuat secara atas talian dapat dilakukan dengan selamat, tanpa kebocoran data dan tidak terdedah kepada sebarang serangan siber.

Kepada pihak organisasi pula, adalah penting untuk sentiasa memberi tumpuan dan perhatian agar keselamatan maklumat sentiasa terjaga dan diberi kawalan keselamatan yang sewajarnya agar tidak berlaku sebarang kebocoran maklumat lebih-lebih dari dalam organisasi itu sendiri.

Rujukan:

[1] https://www.kosmo.com.my/2020/10/03/sprm-siasat-datuk-seri-datuk/

[2] https://www.bharian.com.my/rencana/lain-lain/2020/10/739938/macau-scam-hanya-satu-daripada-banyak-penipuan

[3] https://www.thestar.com.my/news/nation/2020/02/14/man-loses-rm65000-in-online-investment-scam

[4] https://www.nst.com.my/news/crime-courts/2020/12/650499/police-cripple-aliexchange-crypto-currency-investment-syndicate

[5] https://www.freemalaysiatoday.com/category/bahasa/2020/09/14/data-peribadi-1400-rakyat-malaysia-terdedah-akibat-kebocoran-maklumat-china/

[6] https://www.thestar.com.my/tech/tech-news/2020/09/28/jpdp-to-look-into-number-of-malaysians-affected-by-shopback-data-breach

[7] https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies

[8] https://www.freemalaysiatoday.com/category/nation/2020/10/03/fmt-finds-1400-prominent-malaysians-listed-in-zhenhua-data-leak/

[9] https://www.zdnet.com/article/malaysia-warns-of-chinese-hacking-campaign-targeting-government-projects/

[10] https://omghackers.com/300-vpn-korporat-indonesia-digodam-rilekscrew/?fbclid=IwAR2Um3rlmtrWvV59ArZ-6KIGCdEJLWiJ_D1zz_bvnWFyVXhUit1Pz8xAEBM

[11] https://www.malaymail.com/news/life/2020/05/29/cyber-racism-and-covid-19-expert-weighs-in-on-hate-speech-in-malaysia/1870481

[12] https://www.thesundaily.my/local/coronavirus-four-more-individuals-detained-for-spreading-fake-news-FJ1946456

Corporate Office:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

Tel: +603 8800 7999
Fax: +603 8008 7000
Email: info@cybersecurity.my
www.cybersecurity.my

@cybersecuritymy
CyberSecurityMalaysia
cybersecurity_malaysia
CyberSecurityMy

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : ISMS 00114

ACB ISMS 02
SAMM 456

Status Company

WSIS PRIZES 2020 WINNER
www.wsis.org