Pembentukan Platform Risikan Ancaman Siber Sektor Kewangan (FinTIP)

Serangan siber boleh menimbulkan risiko yang besar terhadap kestabilan kewangan dengan industri kewangan dijangka menghadapi peningkatan ancaman dari segi kekerapan, kecanggihan dan skop. Perkembangan ini bukan hanya berlaku di Malaysia. Pada peringkat global, terdapat peningkatan jumlah serangan siber yang telah menjejaskan operasi perniagaan utama. Yang penting, sebahagiannya dirancang oleh pelaku ancaman menggunakan taktik canggih untuk mengeksploitasi bilangan laluan masuk (*entry points*) rangkaian dan sistem institusi kewangan. Hal ini berlaku disebabkan oleh penerapan sistem yang boleh diakses melalui Internet (*Internet-facing*) serta pendigitalan perkhidmatan kewangan yang pesat. Pelaku ancaman ini beroperasi dalam ekosistem rahsia yang aktif untuk berkongsi maklumat, menyelaraskan serangan, merekrut penggodam, menjual data yang dicuri (*compromised data*) dan menyediakan perkhidmatan jenayah siber.

Peningkatan jumlah serangan tersebut dan sifatnya yang cukup tersusun memerlukan tindak balas sektor kewangan yang terselaras. Institusi kewangan terus membuat pelaburan besar bagi menyediakan perlindungan IT dan daya tahan siber dalam institusi masing-masing. Namun, satu strategi pihak berkepentingan berbilang dalam seluruh industri untuk mempertahankan sistem kewangan daripada ancaman siber yang lazim diperlukan bagi memperkukuh usaha setiap institusi kewangan. Bagi tujuan ini, Bank telah berusaha mewujudkan platform risikan dan kerjasama ancaman siber untuk industri kewangan. Platform Risikan Ancaman Siber Sektor Kewangan (Financial Sector Cyber Threat Intelligence Platform), atau FinTIP, mula beroperasi pada bulan September 2021.

FinTIP akan memperkukuh kerjasama industri dan menggalakkan perkongsian maklumat

FinTIP bertujuan untuk mencapai tiga matlamat utama:

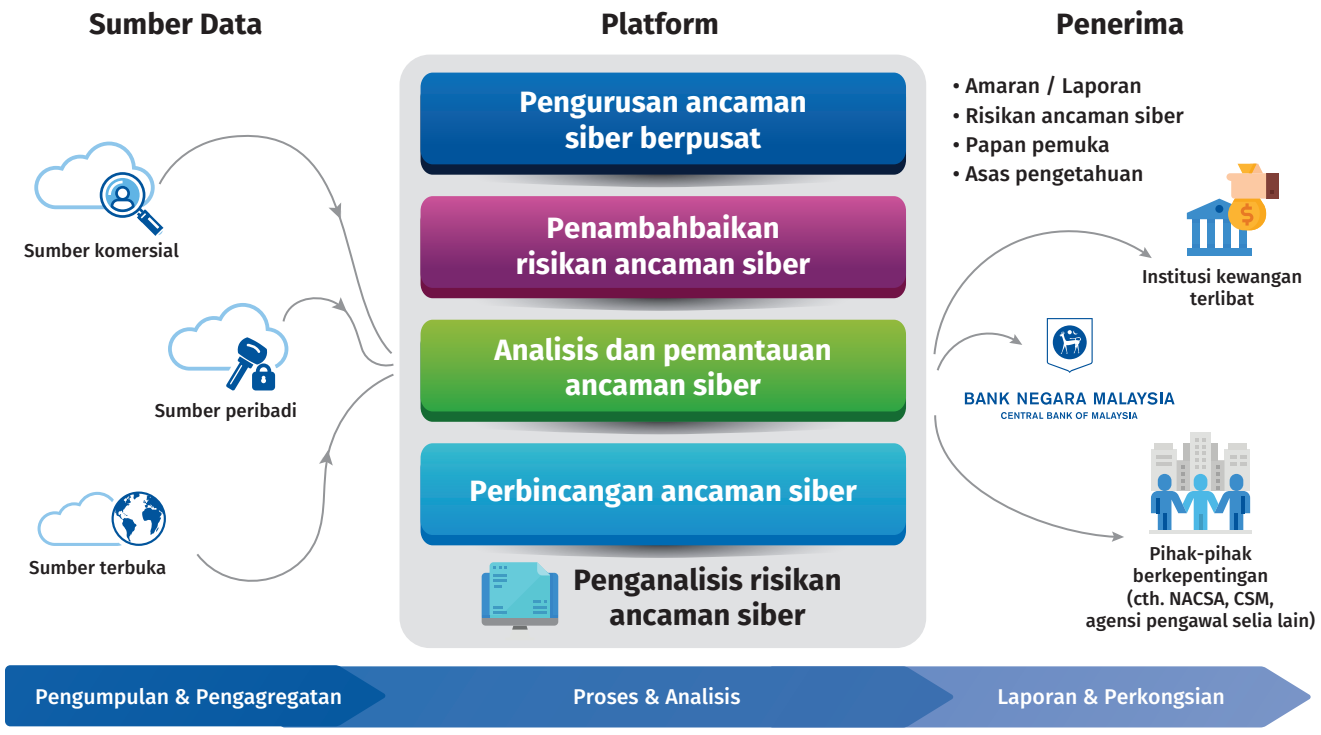
- Melaksanakan penilaian dan penyebaran maklumat secara pantas mengenai ancaman siber yang muncul dan kelemahan IT yang kritikal;
- Menggalakkan perkongsian maklumat dan kerjasama merentas industri melalui platform yang selamat dan dipercayai; dan
- Meningkatkan kesedaran situasi siber bagi membantu proses membuat keputusan yang strategik.

Pelaksanaan FinTIP oleh Bank dapat membantu membina kepercayaan, sekali gus mengurangkan halangan utama terhadap perkongsian maklumat dan kerjasama yang meluas antara institusi kewangan dengan pihak berkepentingan utama yang lain. Pihak berkepentingan dalam sektor awam dan swasta boleh mengambil bahagian dan memberikan sumbangan kepada FinTIP dengan berkongsi maklumat secara sulit mengenai ancaman siber, insiden dan kelemahan IT pada masa hampir nyata (*near real-time*). Pada peringkat kebangsaan, FinTIP berfungsi untuk menghubungkan dan memudahkan pertukaran maklumat rentas sektor antara sektor kewangan dengan sektor ekonomi yang lain, melalui entiti seperti Agensi Keselamatan Siber Kebangsaan (National Cyber Security Agency, NACSA), CyberSecurity Malaysia (CSM), Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dan Suruhanjaya Sekuriti Malaysia.

Penilaian dan penyebaran maklumat yang pantas

FinTIP, yang beroperasi secara 24x7x365, akan mengumpulkan, menggabungkan dan menganalisis risikan ancaman siber dan kelemahan IT daripada pelbagai sumber, serta menyebarkan maklumat yang relevan kepada pihak berkepentingan tepat pada masanya (Gambar Rajah 1.3). Platform analisis ini memanfaatkan gabungan algoritma mesin dan kepakaran manusia untuk menghubungkaitkan, menyelaraskan, memperkaya, dan memurnikan data terkumpul untuk menghasilkan risikan yang boleh diambil tindakan pada masa nyata. Institusi kewangan boleh menggunakan maklumat yang disediakan oleh FinTIP untuk tindak balas insiden, operasi keselamatan, pemburuan ancaman, pengurusan kelemahan dan analisis risiko mereka sendiri. Mereka juga boleh mendapatkan perkhidmatan profesional untuk bantuan mengenai pemulihan insiden siber dan analisis ancaman. Gambar Rajah 1.4 menerangkan ciri-ciri penting FinTIP.

Gambar Rajah 1.3: Model Penggunaan FinTIP



Sumber: Bank Negara Malaysia

Gambar Rajah 1.4: Ciri-Ciri FinTIP

Pemantauan landskap ancaman berterusan

Papan pemuka masa nyata – papan pemuka yang boleh diubah suai terdiri daripada pelbagai jenis data dan rajah.

Tahap dedahan – hubungkan inventori aset yang dihantar dengan kelemahan yang diketahui pada masa nyata.

Penanda aras rakan setara – tahap prestasi atau tahap dedahan institusi kewangan ditanda aras dengan rakan setara dalam industri.

Laporan landskap ancaman – muat turun laporan landskap ancaman berkala dengan mudah secara terus daripada portal FinTIP.

Komunikasi dan penyebaran kepada industri

Penyebaran amaran dan khidmat nasihat tepat pada masanya kepada pihak yang berkaitan.

Saluran perbincangan yang dipercayai – untuk memudahkan perkongsian maklumat dan kerjasama dalam organisasi dan industri.

Analisis menyeluruh oleh penganalisis ancaman siber

Analisis perisian hasad dan *shellcode* – permohonan analisis terperinci untuk mengenal pasti dan memahami tingkah laku kod yang mungkin berbahaya dengan memuat naik artifak ke FinTIP.

Sandbox – buka dan uji program atau fail yang tidak dipercayai melalui sandbox FinTIP (persekitaran yang selamat).

Perkongsian risikan ancaman siber setempat

Perkongsian risikan setempat yang selamat – sumber risikan peribadi yang dimuat naik ke FinTIP akan dikumpulkan, dilaraskan dan dibuang identiti sebelum dikongsikan dengan lebih banyak pihak.

Sumber: Bank Negara Malaysia

Meningkatkan kerjasama industri

FinTIP juga menyediakan platform yang selamat kepada institusi kewangan dan pihak berkepentingan lain merentas industri untuk bertukar-tukar maklumat mengenai langkah-langkah bertahan yang diambil dan iktibar yang dipelajari daripada insiden siber. Sebagai contoh, institusi kewangan boleh mengambil bahagian dalam perbincangan yang diadakan oleh komuniti untuk bekerjasama dan saling belajar daripada pengalaman masing-masing dalam menangani ancaman lazim. Institusi kewangan juga dapat memperoleh pemahaman yang objektif mengenai prestasi risiko siber atau tahap dedahan mereka, yang ditanda aras berdasarkan rakan setara dalam industri.

Meningkatkan kesedaran situasi siber

FinTIP meningkatkan kesedaran situasi siber industri secara keseluruhan dengan memberikan pandangan yang lebih holistik mengenai pelaku ancaman yang menjadikan industri tempatan sebagai sasaran serta membantu institusi kewangan memahami dengan lebih baik tentang taktik, teknik dan prosedur pelaku ancaman. Data terkumpul mengenai ancaman dan kelemahan IT dipadankan dengan aset IT yang digunakan dalam industri untuk memberikan maklumat yang tepat tentang tahap dedahan siber tempatan. Maklumat ini akan membolehkan Bank mengenal pasti kelemahan khusus dan menilai potensi kesan ancaman siber kepada seluruh sistem.

Laporan yang dihasilkan oleh FinTIP bersifat taktikal, operasi dan strategik untuk memenuhi keperluan khalayak yang pelbagai. Pada peringkat taktikal, laporan teknikal memberikan data terperinci mengenai penunjuk ancaman siber yang dapat disepadukan oleh institusi kewangan dalam instrumen keselamatan siber mereka bagi mengenal pasti dan mengurangkan ancaman siber. Pada peringkat operasi, institusi kewangan akan dapat menjejak kempen serangan dan melakukan pemprofilan pelaku ancaman untuk mendapatkan pemahaman yang lebih baik mengenai pelaku ancaman yang menjadikan institusi kewangan sebagai sasaran. Hal ini akan membolehkan institusi kewangan memberikan keutamaan dan melaksanakan operasi keselamatan siber yang lebih bersasar. Akhir sekali, pada peringkat strategik, institusi kewangan boleh menggunakan data FinTIP untuk membuat keputusan perniagaan yang bijak dengan lebih memahami cara peristiwa global dan tempatan, serta landskap ancaman yang berubah-ubah dapat mempengaruhi tahap ketersediaan keselamatan siber sesebuah institusi kewangan.

FinTIP melengkapi strategi pertahanan pelbagai lapisan sedia ada

FinTIP mencerminkan perkongsian tanggungjawab untuk keselamatan siber dengan memudahkan pendekatan seluruh industri ke arah meningkatkan daya tahan siber. Penting dinyatakan bahawa FinTIP berfungsi untuk melengkapi dan menambah, dan bukannya menggantikan, perkhidmatan risikan ancaman siber sedia ada dalam institusi itu sendiri. Bank menjangkakan FinTIP akan menyokong perkongsian maklumat dan kerjasama secara lebih mendalam dan lebih pantas yang seterusnya memperkukuh keupayaan tindak balas industri kewangan terhadap ancaman siber yang berubah-ubah dan menjejaskan sistem kewangan.