RISIKO OPERASI

Operasi sektor kewangan kekal berdaya tahan dalam keadaan persekitaran risiko yang berubah-ubah

Kerugian kewangan akibat risiko operasi yang dilaporkan oleh institusi kewangan kekal rendah, mencakupi hanya 0.04% daripada jumlah modal sistem perbankan (ST2 2024: 0.03%; ST1 2024: 0.05%). Pada masa yang sama, institusi kewangan terus mengekalkan daya tahan operasi serta mampu untuk menyediakan perkhidmatan kewangan asas yang cekap dan boleh dipercayai kepada pelanggan. Yang ketara, insiden melibatkan kegagalan teknologi dan gangguan serius yang berpanjangan terhadap perkhidmatan dalam talian untuk orang ramai telah berkurang sebanyak 38% pada tempoh ini. Penambahbaikan ini mencerminkan usaha tambahan serta pelaburan institusi kewangan dalam mengukuhkan daya tahan operasi bagi memenuhi standard ketersediaan perkhidmatan yang diharapkan oleh pengguna kewangan. Namun, usaha yang berterusan ini bukan sahaja penting untuk mengekalkan ketersediaan dan daya tahan sistem penting institusi kewangan, tetapi juga untuk menambah baik pengalaman pelanggan, termasuk apabila perkhidmatan kewangan tertentu tidak tersedia atau terganggu buat sementara waktu. Antara keutamaan termasuk meningkatkan kebolehpercayaan perkhidmatan dalam talian dan memupuk pendekatan yang lebih berfokuskan pelanggan dalam menguruskan gangguan perkhidmatan, disertai komunikasi yang berkesan dan tepat pada masanya kepada pelanggan yang terjejas bagi mengurangkan kesulitan.

Meskipun terdapat peningkatan bilangan insiden siber yang dilaporkan pada separuh pertama tahun 2025, kebanyakan insiden berada pada tahap keseriusan yang rendah. Peningkatan bilangan kes yang dilaporkan sebahagiannya mencerminkan tahap pelaporan insiden siber yang lebih menyeluruh oleh institusi kewangan, disokong oleh usaha yang berterusan oleh BNM untuk memupuk kesedaran dan berkongsi ilmu pengetahuan. Yang ketara, tiada insiden perisian tebusan (*ransomware*) dilaporkan pada tempoh ini. Berikutan ancaman siber yang berterusan, institusi kewangan terus meningkatkan kewaspadaan siber dan keupayaan tindak balas mereka secara berperingkat. Usaha ini dicerminkan oleh peningkatan keupayaan institusi kewangan dalam menjalankan fungsi pengawasan, pengesanan, tindak balas dan pemulihan ancaman yang membolehkan ancaman siber dibendung dan diuruskan secara lebih berkesan dengan gangguan operasi yang minimum.

Sebagai tindak balas terhadap trend peningkatan insiden siber yang dilaporkan serta untuk mengukuhkan lagi keupayaan institusi kewangan dalam menguruskan risiko siber baharu merentas sektor, BNM telah menjalankan tinjauan berfokus terhadap amalan pengurusan keselamatan institusi kewangan berhubung dengan Antara Muka Pengaturcaraan Aplikasi (Application Programming Interface, API). Tinjauan tersebut mendedahkan tahap kesiapsiagaan yang tinggi merentas sektor kewangan, dengan penerapan amalan terbaik yang meluas dalam pengurusan risiko keselamatan berkaitan API, khususnya dalam bidang seperti standard pembangunan, ujian dan penilaian keselamatan serta pengesahan dan kawalan akses API. Walau bagaimanapun, tadbir urus dalam pengurusan API dan pelaksanaan kawalan keselamatan automatik telah dikenal pasti sebagai bidang-bidang utama yang memerlukan penambahbaikan selanjutnya oleh institusi kewangan.

Walaupun langkah-langkah pencegahan penipuan yang telah diperhalus oleh industri berjaya membendung kes penipuan membabitkan transaksi tanpa kebenaran *(unauthorised transactions)*,[18] separuh pertama tahun 2025 menyaksikan peningkatan skim penipuan dengan kebenaran *(authorised fraud)* yang didorong oleh kejuruteraan sosial dan taktik manipulasi. Skim sebegini sering mengeksploitasi kepercayaan pelanggan dan berjaya memintas kawalan keselamatan. Bagi mengukuhkan pertahanan terhadap ancaman sedemikian, BNM dan industri kewangan telah mempergiat program pendidikan dan kesedaran pelanggan. BNM juga telah memperkenalkan langkah pencegahan penipuan yang ditambah baik bagi

[18] Transaksi tanpa kebenaran merujuk transaksi pembayaran yang tidak dipersetujui, dimulakan atau dibenarkan oleh pelanggan. Hal ini tidak termasuk transaksi yang membabitkan mangsa secara rela melakukan dan meluluskan pembayaran pada saat transaksi dibuat (contohnya penipuan cinta, penipuan pelaburan dan penipuan bungkusan).

mengukuhkan sistem pertahanan institusi kewangan terhadap penipuan. Kehendak utama daripada langkah-langkah ini termasuk:

- penghasilan profil risiko yang terperinci bagi setiap pelanggan melalui analisis tingkah laku untuk meningkatkan pengesanan penipuan;
- pengesanan dan penyekatan secara masa nyata terhadap transaksi yang mencurigakan atau penipuan transaksi;
- siasatan dan pengesahan yang pantas selepas sekatan;
- pengesanan dan penamatan segera sesi yang dirampas (*hijacked session*);[19] dan
- kemas kini dan penambahbaikan peraturan pengesanan penipuan yang berterusan.

Usaha memelihara kepercayaan pelanggan dan integriti sistem perbankan kekal menjadi keutamaan BNM. National Fraud Portal (NFP), platform utama yang digunakan oleh Pusat Respons Penipuan Kebangsaan (National Scam Response Centre, NSRC) untuk mengesan dana yang dicuri, akan ditambah baik dengan keupayaan analisis lanjutan untuk membolehkan pengesanan awal akaun keldai dan transaksi mencurigakan. Langkah ini menandakan satu kemajuan ketara dalam usaha peralihan industri ke arah pencegahan penipuan secara proaktif serta meminimumkan kerugian kewangan yang ditanggung mangsa.

Usaha-usaha ini dilengkapi dengan kempen kesedaran dan pendidikan tentang penipuan secara berterusan yang dianjurkan secara bersama oleh rakan kerjasama dalam sektor awam dan swasta, dengan tujuan untuk memperkasakan pengguna supaya menjadi lebih arif dan waspada khususnya apabila skim penipuan dengan kebenaran semakin berleluasa. BNM terus mendukung dasar Memastikan Layanan yang Adil kepada Mangsa Transaksi e-Perbankan Tanpa Kebenaran yang dikeluarkan pada tahun 2024. Dasar ini menegaskan keputusan yang konsisten dan adil bagi mangsa penipuan dengan menghendaki institusi kewangan menjalankan siasatan secara telus dan tepat pada masanya, memberikan pampasan yang wajar serta membuat semakan bebas sekiranya perlu.

Susulan berakhirnya tempoh maklum balas orang ramai mengenai Draf Dedahan Risk Management in Technology (RMiT) pada bulan Februari 2025, BNM akan menerbitkan dokumen dasar RMiT pada suku akhir tahun 2025. Sebagai tindak balas kepada perkhidmatan digital yang semakin meluas, dasar yang dikemas kini tersebut menggariskan kehendak baharu terhadap institusi kewangan untuk membina daya tahan perkhidmatan. Antaranya termasuk sasaran ketersediaan perkhidmatan yang dipertingkatkan bagi memenuhi jangkaan pelanggan yang lebih tinggi terutamanya bagi bank-bank yang mempunyai jumlah transaksi runcit yang besar, pengurusan isu perkhidmatan yang terputus-putus secara proaktif, penyelarasan yang lebih baik dengan penyedia perkhidmatan pihak ketiga untuk memastikan tindak balas insiden yang berkesan dan penetapan protokol komunikasi supaya pelanggan mendapat maklumat dan sokongan semasa berlakunya gangguan.

Dasar yang dikemas kini ini juga memperkukuh keperluan pertahanan siber selaras dengan amalan terbaik global, termasuk pelaksanaan pemantauan kawalan secara berterusan untuk mengurangkan risiko pihak ketiga. Keperluan dasar pengurusan risiko teknologi maklumat (*information technology,* IT) yang seragam ini juga akan diperluas untuk mencakupi pemeroleh peniaga besar dan institusi pengiriman wang pengantara, berdasarkan paras ambang tertentu, dengan tujuan untuk mengukuhkan keselamatan ekosistem perkhidmatan pembayaran secara keseluruhan. Sejajar dengan itu, proses semakan pengawalseliaan akan dipermudah dan diselaraskan untuk mempercepat penggunaan teknologi yang telah matang dan memudahkan penilaian teknologi yang pesat berkembang seperti pengkomputeran awan.

Sistem pembayaran dan penyelesaian kekal boleh dipercayai dan selamat

Sistem Pemindahan Dana dan Sekuriti Secara Elektronik Masa Nyata (Real-time Electronic Transfer of Funds and Securities System, RENTAS) dan sistem pembayaran runcit (*retail payment systems,* RPS) utama[20] kekal berdaya tahan dengan tahap ketersediaan sistem yang tinggi sepanjang separuh pertama tahun 2025. Tiada insiden operasi atau insiden siber yang serius berlaku pada tempoh ini. Walau bagaimanapun, satu insiden terpencil akibat gangguan global pada perkhidmatan pihak ketiga telah

[19] Sesi yang dirampas (*hijacked session*) berlaku apabila penipu mengambil alih kawalan sesi dalam talian pengguna yang sedang aktif digunakan.

[20] Platform Pembayaran Runcit Masa Nyata (Real-time Retail Payments Platform, RPP), GIRO Antara Bank (Interbank GIRO, IBG), Sistem Penjelasan Informasi Cek Kebangsaan secara Elektronik (eSPICK), Bursa Pemprosesan Kewangan (Financial Process Exchange, FPX), Rangkaian ATM Bersama (Shared ATM Network, SAN), Direct Debit (DD), MyDebit, Pembayaran Bil Elektronik Kebangsaan (JomPAY) dan Pindahan Segera (Instant Transfer, IBFT).

mengganggu sambungan ke RENTAS buat sementara waktu. Isu ini telah ditangani dengan segera setelah pusat operasi alternatif perkhidmatan pihak ketiga tersebut berjaya diaktifkan tepat pada masanya.

Sebagai sebahagian daripada usaha penyeliaan berterusan untuk mengukuhkan kestabilan dan daya tahan infrastruktur pembayaran utama, BNM telah menjalankan pemeriksaan penyeliaan terhadap Platform Pembayaran Runcit Masa Nyata (Real-time Retail Payments Platform, RPP) yang dikendalikan oleh PayNet.

Pelbagai usaha terus dilaksanakan untuk meningkatkan lagi daya tahan dan keselamatan keseluruhan RPP, khususnya dalam pengurusan kesinambungan perniagaan serta pengurusan penyedia perkhidmatan yang penting, peserta dan perkhidmatan rentas sempadan. Berikutan kesalinghubungan pembayaran Respons Pantas (Quick Response, QR) rentas sempadan serantau kini semakin meluas dan berkembang, BNM akan terus mempertingkatkan pengawasan terhadap pengaturan pembayaran rentas sempadan melalui usaha kerjasama dengan pihak berkuasa kawal selia yang berkaitan.