## Memperkukuh Daya Tahan Teknologi

Dalam kepesatan transformasi digital, SC mendapati peningkatan ketara dalam serangan siber di seluruh dunia pada tahun 2022, seiring dengan peningkatan amalan kerja dari jauh dan pertumbuhan teknologi digital. Serangan siber ini juga telah menunjukkan bahawa mana-mana firma boleh terkesan, tanpa mengira saiz atau skala.

Sebagai tindak balas untuk memastikan risiko teknologi dan siber diurus serta dipantau dengan betul, SC mengeluarkan kertas perundingan mengenai rangka kerja kawal selia untuk Pengurusan Risiko Teknologi (TRM). Langkah-langkah pencegahan juga telah diambil untuk menyokong entiti pasaran modal menjadi lebih proaktif dalam menguruskan insiden keselamatan siber dan pelbagai program telah diadakan untuk meningkatkan kesedaran risiko siber dan kebersihan dalam pasaran modal. Dua acara utama yang berlangsung pada tahun 2022 ialah Simulasi Siber Pasaran Modal (CMCS) dan Latihan Di Meja Insiden Siber Pasaran Modal (Latihan CMCIT) dengan tujuan memastikan piawaian risiko siber didukung dalam pasaran modal. CMCS disasarkan untuk entiti yang mempunyai kebergantungan yang lebih tinggi pada teknologi dalam operasi perniagaan harian mereka manakala Latihan CMCIT membantu syarikat yang kurang bergantung kepada teknologi untuk memulakan perancangan dan menjadi lebih bersedia untuk serangan siber.

### Membina daya tahan terhadap risiko siber

- Simulasi Siber Pasaran Modal

Simulasi siber tahunan yang kelima untuk entiti pasaran modal telah dijalankan oleh SC dengan kerjasama Agensi Keselamatan Siber Kebangsaan (NACSA) dan CyberSecurity Malaysia (CSM).

**110 Entiti**
yang mempunyai kebergantungan yang lebih tinggi pada teknologi dalam operasi harian perniagaan mereka telah dijemput.

**Bertemakan 'Percaya Tetapi Sahkan'**
dengan tiga senario peristiwa siber dipilih untuk mengajuk keadaan yang mencabar pada tahun 2022.

| Senario | Cabaran |
|---|---|
| **Bekalan Rantaian** | SC mengakui bahawa penyerang menyelidiki pembekal sebagai titik penyusupan baharu ke dalam organisasi. Hasil daripada peningkatan potensi bagi penggodaman bekalan rantaian untuk menembusi sejumlah besar pengguna, menjadikan jenis serangan ini semakin lazim. Serangan ini kebanyakannya mensasarkan data pelanggan, termasuk data Maklumat Pengenalan Peribadi (PII) dan harta intelek. |
| **Kebocoran data** | Pekerja adalah kelemahan terbesar data syarikat. Kelemahan ini semakin meluas apabila ramai pekerja beroperasi di luar rangkaian korporat yang selamat. Walaupun penggodam telah membangunkan strategi dan alatan yang lebih canggih untuk mencuri data dan maklumat, pancingan data masih merupakan teknik yang lazim dan murah untuk mendapatkan akses kepada data organisasi. Penggodam menggunakan ketakutan orang ramai dan memanipulasi mereka untuk menyerahkan data, selalunya melalui e-mel atau laman web. |
| **Pencemaran dalam talian** | Pemilik laman web yang dicemari biasanya mengalami kerosakan reputasi, dan dalam beberapa keadaan, kerugian dari segi kewangan. Akibatnya, pemilik laman web mungkin hilang kepercayaan di kalangan pelanggan. |

**Objektif Utama**

- Mensimulasi proses tindak balas insiden siber dan pemulihan organisasi yang mengambil bahagian;
- Mengenal pasti potensi jurang dalam keupayaan teknologi;
- Latih keupayaan untuk mengekalkan kelancaran operasi pasaran dengan insiden siber yang berbeza; dan
- Membiasakan peserta dengan *SC Portal Vault*[4] untuk melaporkan dan mengemukakan laporan insiden.

**Keputusan**

- Penambahbaikan yang ketara berbanding dengan latihan tahun 2021 walaupun terdapat tahap kesukaran dalam senario penilaian dipertingkatkan; dan
- Sebahagian peserta menunjukkan kematangan dalam tahap ketahanan siber mereka dan lebih bersedia sekiranya berlaku serangan siber.

[4] Vault ialah sistem pengurusan kes yang membenarkan pengantara melaporkan, dan memudah cara SC menjejaki sebarang insiden siber atau teknologi yang berlaku dalam lingkungan pengantara. Ia juga berfungsi sebagai platform komunikasi di mana khidmat nasihat atau pemakluman dikeluarkan oleh SC kepada perantara yang berdaftar di platform Vault.



- Latihan Di Meja Kejadian Siber Pasaran Modal

Untuk membantu organisasi mengukuhkan usaha mengurangkan rintangan dalalm menghadapi potensi ancaman siber, *Guidance Note on Management of Cyber Incidents (Nota Panduan Pengurusan Insiden Siber SC)* telah dilancarkan kepada semua entiti pasaran modal pada tahun 2022 sebagai buku panduan asas untuk membimbing pengendalian dan pengurusan insiden keselamatan siber. Di samping itu, latihan di meja telah dianjurkan untuk memperhebatkan keberkesanan prosedur tindak balas insiden entiti pasaran modal dengan meningkatkan kesedaran dan pemahaman tentang ancaman siber. Hampir 200 peserta pasaran modal yang tidak pernah terlibat dalam acara CMCS SC menyertai latihan ini.


Baca lebih lanjut mengenai *Guidance Note on Management of Cyber Incidents.*
https://www.sc.com.my/api/documentms/download.ashx?id=272ca944-ede5-42ec-bd9d-e1e04184c39a