MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

# SIARAN MEDIA

**21 MEI 2019**

**UNTUK SIARAN SERTA MERTA**

## BERWASPADA DENGAN ANCAMAN KESELAMATAN SIBER DI MUSIM PERAYAAN AIDILFITRI

**CYBERJAYA** – Sempena musim perayaan Hari Raya Aidilfitri, CyberSecurity Malaysia, pusat pakar teknikal keselamatan siber dan agensi di bawah Kementerian Komunikasi dan Multimedia Malaysia (KKMM) hari ini mengeluarkan amaran *(alert)* kepada Pentadbir Sistem dan juga pengguna Internet untuk pertingkatkan keselamatan sistem dan rangkaian komputer serta gajet digital agar terhindar dari sebarang ancaman siber.

"Sehingga bulan April tahun ini, sebanyak 4,596 insiden keselamatan siber telah dilaporkan oleh pengguna Internet ke Pusat Bantuan Cyber999 berbanding 2,977 pada tahun 2019, di mana insiden Penipuan, Pencerobohan dan Kod Berbahaya adalah antara tiga yang tertinggi. Kita juga dapati insiden Penipuan telah meningkat secara mendadak terutamanya sepanjang tempoh Perintah Kawalan Pergerakan (PKP) bermula bulan Mac 2020 akibat penularan wabak COVID-19." kata Dato' Ts Dr Haji Amirudin Abdul Wahab, Ketua Pegawai Eksekutif, CyberSecurity Malaysia

Sepanjang tempoh empat bulan beberapa amaran dan nasihat amalan terbaik berkaitan pelbagai isu serta insiden keselamatan siber seperti *bogus scam email,* phishing, penggunaan *tele-conferencing* dalam talian, kerentanan perisian serta kemas kini produk seperti Microsoft, Adobe, Penyemak Imbas Internet dan lain-lain telah dikeluarkan bagi memberi panduan kepada Pentadbir Sistem dan pengguna Internet. (sila rujuk: https://www.mycert.org.my/ )

"Kami ingin mengesa Pentadbir Sistem dan pengguna Internet untuk merujuk kepada amaran dan nasihat yang dikeluarkan dengan mengikuti langkah-langkah yang perlu dilaksanakan bagi mencegah dan meminimumkan kesan atau risiko terhadap sebarang insiden keselamatan siber." ujar Dato' Dr Amirudin.



CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

Pentadbir Sistem harus melakukan pencegahan tambahan terhadap kemungkinan pencerobohan, serangan phising dan aktiviti perisian hasad seperti ransomware pada musim perayaan ini dengan mengamalkan langkah pencegahan yang tepat terhadap ancaman ini.

Antara langkah yang perlu dilaksanakan oleh Pentadbir Sistem ialah:

1. Pastikan sistem, aplikasi dan alat tambah pihak ketiga *(third party add-ons)* dikemas kini dengan peningkatan dan *patch* keselamatan terkini;
2. Pastikan aplikasi berasaskan web serta peralatan berasaskan rangkaian ditampal dengan sewajarnya;
3. Pastikan perisian Anti-virus yang beroperasi di *host* dan *gateway* e-mel dikemas kini dengan fail tandatangan terkini dan diaktifkan untuk mengimbas semua fail;
4. Pastikan sistem anda dikonfigurasi dengan betul untuk mengelakkan kejadian seperti pendedahan maklumat, penyenaraian direktori yang disebabkan oleh salah konfigurasi sistem;
5. Pastikan log sistem dan pelayan sentiasa diaktifkan;
6. *Backup* semua maklumat kritikal secara berkala untuk menghadkan kesan kehilangan data atau sistem serta untuk membantu mempercepat proses pemulihan. Sebaik-baiknya, *backup* dilakukan setiap hari pada media yang berasingan dan disimpan di luar talian di laman web alternatif;
7. Organisasi disarankan untuk mengamalkan strategi pertahanan secara menyeluruh bagi melindungi sistem rangkaian. *Firewall*, sistem pencegahan pencerobohan (IPS), sistem pengesanan pencerobohan berasaskan rangkaian dan host (IDS) dapat mencegah dan mencatat sebahagian besar serangan generik.

Manakala untuk pengguna Internet, berikut adalah nasihat yang disarankan:

1. Pastikan gajet dan penyemak imbas dikemas kini dengan *patch* keselamatan terkini;
2. Pasang perisian Anti-virus pada gajet untuk mengimbas dan menyekat sebarang perisian hasad. Anti-virus juga harus dikemas kini secara berkala dengan fail tanda tangan terkini untuk mengesan cacing / virus baharu;
3. Jangan klik pada pautan atau lampiran yang diterima melalui media sosial atau e-mel. Sentiasa berhati-hati semasa membuka pautan dan lampiran (jika perlu);
4. Jangan menjadi mangsa penipuan dalam talian. Sentiasa berhati-hati terhadap ancaman penipuan dalam talian yang menyasarkan pengguna Internet;

5. Pengguna Internet disaran untuk merujuk kepada amalan terbaik serta panduan mengenai penggunaan Internet secara selamat di portal CyberSAFE: http://www.cybersafe.my
6. Lakukan *backup* secara berkala untuk semua maklumat penting bagi menghalang dari kehilangan data atau sistem serta membantu percepatkan proses pemulihan.

Sila rujuk laman web MyCERT untuk mendapatkan maklumat mengenai amaran dan nasihat terbaharu CyberSecurity Malaysia:
https://www.mycert.org.my/portal/advisories?id=431fab9c-d24c-4a27-ba93-e92edafdefa5

Laporkan insiden keselamatan siber ke Pusat Bantuan Cyber999 menerusi saluran berikut:-

i. E-mel: cyber999@cybersecurity.my
ii. No. Kecemasan: 1-300-88-2999 (9.00 pagi – 9.00 malam)
iii. Telefon Mudah alih: +6019-2665850 (24 jam)
iv. SMS: CYBER999 <LAPOR INSIDEN> ke 15888
v. Muat turun aplikasi "Cyber999 App" di Appstore / Google Play
vi. Borang dalam talian di: https://www.mycert.org.my

~ Tamat ~

---

*Untuk maklumat lanjut mengenai siaran media ini, sila emel: media@cybersecurity.my atau hubungi +603-8008 7237, Mohd Shamil Mohd Yusoff / Zul Akmal Abdul Manan +603-8008 7242*