GENERAL

Lindungi data dan waspada ancaman siber dalam talian

19 May 2021

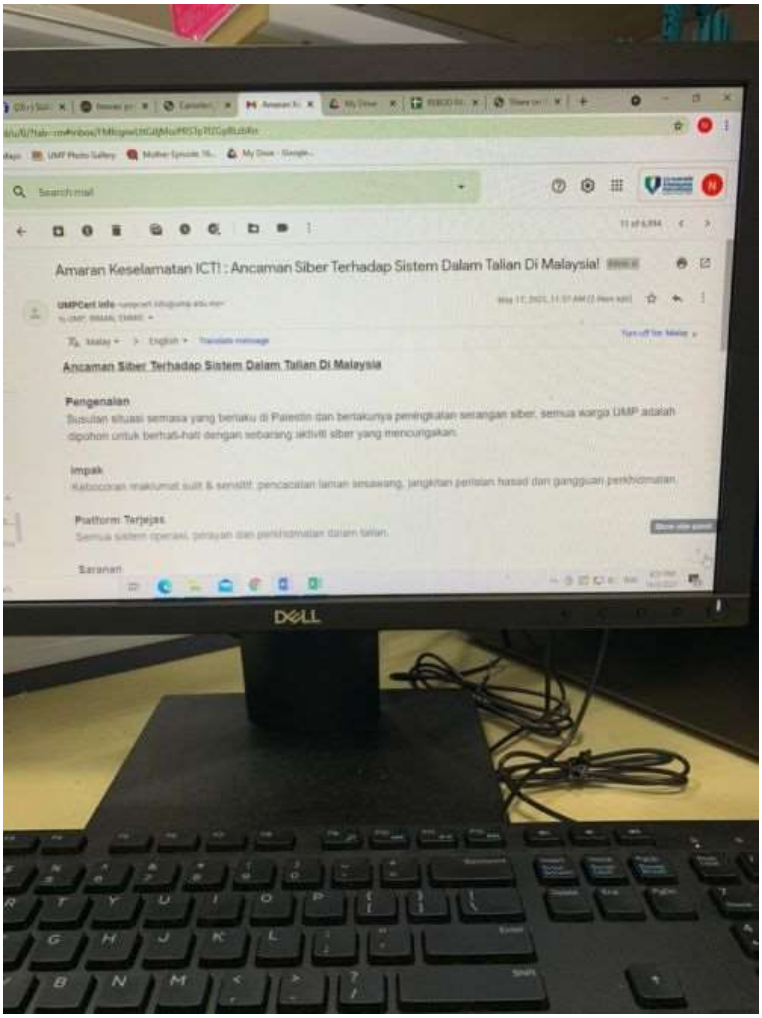
Disediakan Oleh: Irman Khalil, Pusat Teknologi Maklumat dan Komunikasi dan Mimi Rabita Haji Abdul Wahit, Unit Komunikasi Korporat, Pejabat Naib Canselor. (PNC)

PEKAN, 18 Mei 2021 - Universiti Malaysia Pahang (UMP) menerusi Pusat Teknologi Maklumat dan Komunikasi (PTMK) menasihatkan warga universiti agar sentiasa memastikan semua aplikasi yang berkaitan dengan internet dikemas kini dan dinaik taraf dan sentiasa berhati-hati dengan e-mel dan pautan dari sumber yang mencurigakan.

Ia boleh mengakibatkan kebocoran maklumat sulit dan sensitif, pencacatan laman web, jangkitan perisian hasad (*malware*) dan gangguan perkhidmatan.

Ancaman siber di Malaysia ini bermula susulan situasi tegang di Palestin berikutan siri kempen hacktivist yang menyerang akaun media sosial tokoh-tokoh, para pemimpin dan selebriti Israel dengan komen berunsur cercaan disulami tanda pagar #shameonIsrael dan #IsraelKoyak.

Berdasarkan peringatan daripada Agensi Keselamatan Siber Negara (NACSA) yang dikeluarkan pada 16 Mei 2021, terdapat peningkatan aktiviti tindak balas dari pihak Israel yang menyasarkan organisasi Malaysia.



Setiap organisasi pelu mengambil tindakan sewajarnya bagi mengelak daripada menjadi mangsa serangan ini sehingga mengakibatkan gangguan operasi organisasi.

Menurut Irman Khalil yang menjalankan tugas Pengarah PTMK berkata, terdapat juga kumpulan yang melakukan penggodaman terhadap laman web dan pangkalan data milik Israel yang mengakibatkan ratusan laman web dan pangkalan data berjaya digodam dan dicacatkan.

“Sebagai pengguna, kita perlu memastikan kata laluan bagi aplikasi internet adalah kuat dan selamat serta penggunaan 2-step factor authentication juga sangat digalakkan bagi penggunaan akaun e-mel dan media sosial.

“Selain itu juga, organisasi dinasihatkan untuk berwaspada dan mengambil tindakan terhadap kemas kini aset kritikal ICT dengan tampalan keselamatan terkini (*update patch*), berhati-hati dengan e-mel yang mencurigakan dan pautan dengan/atau tanpa lampiran dan pastikan anti-virus bagi komputer peribadi dan komputer makmal telah dikemas kini dan berfungsi dengan baik,” katanya.

Pihaknya juga menasihatkan pengguna agar jangan sesekali membuka pautan dari sumber yang tidak dipercayai yang boleh menyebabkan serangan siber, jangkitan virus komputer atau pencurian identiti atau maklumat akaun.
“Tutup sepenuhnya semua stesen kerja sebelum meninggalkan pejabat sama ada komputer peribadi atau pun komputer makmal serta laksanakan pengemaskinian dan naik taraf pada semua aplikasi internet.

“Dalam pada itu, pengguna juga hendaklah memutuskan rangkaian komputer (komputer peribadi dan komputer makmal) dari internet jika tidak digunakan dan pastikan kata laluan sistem, portal fakulti dan jabatan anda kuat dan selamat.

“Ini termasuklah pentadbir akaun media sosial fakulti dan jabatan UMP (Facebook, Twitter, Instagram dan lain-lain) yang dikehendaki membuat *two-factor authentication* pada akaun media sosial masing-masing,” ujarnya.

Antara kaedah serangan siber yang dijangka bagi tindak balas serangan tersebut adalah pencerobohan, percubaan penggodaman, penafian perkhidmatan tersebar (DDoS), pencacatan laman web dan jangkitan perisian hasad.

Aktiviti pencerobohan merupakan cubaan untuk memasuki sesuatu laman web secara tidak sah dengan niat untuk melakukan kerosakan atau mencuri data tertentu.

Percubaan penggodaman pula merupakan aktiviti yang bertujuan untuk mendatangkan kerosakan kepada sesuatu laman web.

Serangan DDoS merupakan satu kaedah untuk melumpuhkan sesuatu rangkaian atau pelayan dengan bilangan trafik yang tinggi hingga mengakibatkan sumber memori dan pemproses perkakasan berkenaan terjejas.

Pencacatan laman web pula melibatkan pihak penceroboh bertindak melakukan kerosakan kepada laman web sedia ada.

Antara kaedah yang popular ialah dengan cara menukarkan muka depan laman web berkenaan kepada tulisan atau gambar-gambar yang tidak sepatutnya.

Manakala *malware* pula merupakan satu program kecil yang dibangunkan dengan tujuan untuk mendapatkan akses kepada sesuatu sistem, merosakkan data, mencuri data dan sebagainya.

Terdapat banyak jenis perisian hasad antaranya ialah virus, trojan, spyware dan ransomware.

Pihak universiti melarang warganya sama ada staf atau pun pelajar terlibat dalam sebarang aktiviti pencerobohan siber menggunakan rangkaian UMP (*UMP network*).

Mereka hendaklah melaporkan sebarang anomali yang berlaku di dalam rangkaian dan persekitaran mereka kepada pihak UMPCERT melalui e-mel umpcert@ump.edu.my.

Pihak NACSA juga telah mengeluarkan panduan bagi organisasi dalam menghadapi situasi serangan siber meliputi saranan bagi pengguna dan pentadbir sistem dan rangkaian.
Langkah-langkah keselamatan siber secara kendiri juga telah pun dikeluarkan oleh kerajaan Malaysia yang terdiri daripada sepuluh langkah mudah iaitu:

1. Gunakan KATA LALUAN
2. KEMAS KINI perisian keselamatan
3. SIMPAN dan LINDUNGI maklumat
4. ELAK terpedaya
5. BERETIKA menggunakan internet dan media sosial
6. WASPADA jenayah siber
7. FIKIR sebelum klik
8. LAPORKAN
9. AMBIL TAHU
10. PATUHI

Sumber: Agensi Keselamatan Siber Negara (NACSA) https://www.nacsa.gov.my/doc/10LangkahMudah-v8.pdf

TAGS / KEYWORDS

Ancaman Siber