Universiti Kebangsaan Malaysia
The National University of Malaysia

Menangani SERANGAN RANSOMWARE

LANGKAH PENCEGAHAN

Sentiasa laksana proses sandar (backup) untuk mengurangkan impak kehilangan data serta mempercepatkan proses pemulihan data.

Sentiasa pastikan sistem operasi (cth: Windows), perisian, Java, Shockwave dan Flash dikemaskini.

Berhati-hati apabila membuka sebarang fail yang dilampirkan melalui e-mel. Jangan buka fail yang dihantar oleh pengirim yang mencurigakan.

Gunakan perisian yang dikenalpasti selamat sahaja untuk menghalang perisian bersifat hasad dijalankan.

Perisian antivirus/antimalware mestilah dikemaskini dan imbas semua perisian yang dimuat turun daripada internet.

Jangan klik pautan mencurigakan yang dikongsi melalui e-mel, media sosial atau laman web.

JADI MANGSA? APA PERLU SAYA BUAT?

- Asingkan server atau komputer yang dijangkiti ransomware daripada rangkaian.
- Imbas komputer/server menggunakan perisian antivirus versi terkini untuk mengesan dan menghapus malware.
- Tukar semua kata laluan akaun atas talian dan rangkaian selepas komputer/server diasingkan daripada rangkaian.
- Tukar semua kata laluan sistem setelah malware berjaya dihapuskan.
- Imbas semula dengan perisian antivirus versi terkini untuk memastikan komputer/server tersebut berjaya dibersihkan sebelum ia disambung semula ke rangkaian.
- Kembalikan semula data daripada sandaran (backup).

Rujukan: Hebahan media CyberSecurity Malaysia 14 Nov 2018

BAHAGIAN KESELAMATAN ICT
PUSAT TEKNOLOGI MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA