Bersama FIRKHAN
firkhan.uthm@yahoo.com

Cyber kill chain dalam keselamatan siber

ISTILAH *cyber kill chain* merujuk kepada satu model kitar hayat serangan siber yang dapat membantu dalam mengenal pasti dan mencegah berlakunya pencerobohan siber.

Dalam bidang ketenteraan, istilah *kill chain* atau rantaian bunuhan merujuk pada satu model serangan berfasa yang terdiri daripada fasa pencarian, pembetulan, penjejakan, sasaran, keterlibatan dan pencapaian.

Semakin dekat dengan permulaan rantaian bunuhan ini, sesuatu serangan itu boleh dihentikan dengan semakin baik.

Semakin kurang maklumat yang dimiliki oleh penyerang untuk membuat serangan, kemungkinan orang lain dapat melengkapkan dan menggunakan maklumat tersebut untuk menyelesaikan serangan itu pada kemudiannya.

Begitu juga dengan konsep *cyber kill chain* ini yang dikemukakan oleh Lockheed Martin, iaitu fasa serangan yang disasarkan diperjelas.

Begitu juga, sebaliknya model ini boleh digunakan untuk perlindungan keselamatan rangkaian bagi sesebuah organisasi.

Seterusnya dibincangkan fasa-fasa dalam model *cyber kill chain* ini.

1 Fasa Peninjauan atau *Reconnaisance* iaitu mendapatkan segala maklumat dari luar dan dalam berkaitan dengan infrastruktur rangkaian dan teknologi maklumat bagi sesebuah organisasi yang hendak diserang.

2 Fasa Persenjataan atau *Weaponization* iaitu pembinaan alat serangan seperti aplikasi *exploit* dan *backdoor* sebagai persediaan untuk masuk ke sistem siber sasaran.

3 Fasa Penghantaran (*Delivery)* dengan mengantar pakej persenjataan kepada sasaran serangan seperti menerusi pautan muat turun ke dalam e-mel sasaran dan lain-lain.

4 Fasa Pengeksploitasian (*Exploit)* apabila pakej persenjataan berjaya ditempatkan dan beroperasi dalam persekitaran siber sasaran.

5 Fasa Pemasangan (*Installation)* dengan memasang *malware* pada aset-aset teknologi maklumat tertentu kepunyaan sasaran.

6 Fasa Kawalan dan Arah (*Command and Control* iaitu saluran dibina daripada sasaran kepada pihak penyerang untuk kawalan secara jarak jauh terhadap aset siber sasaran.

7 Fasa Tindakan (*Actions)* iaitu penyerang akan berbuat apa yang telah diobjektifkan atau tindakan yang perlu terhadap sasaran seperti dapatkan maklumat tertentu, merosakkan prsarana teknologi maklumat tertentu, pesongkan maklumat tertentu dan lain-lain.