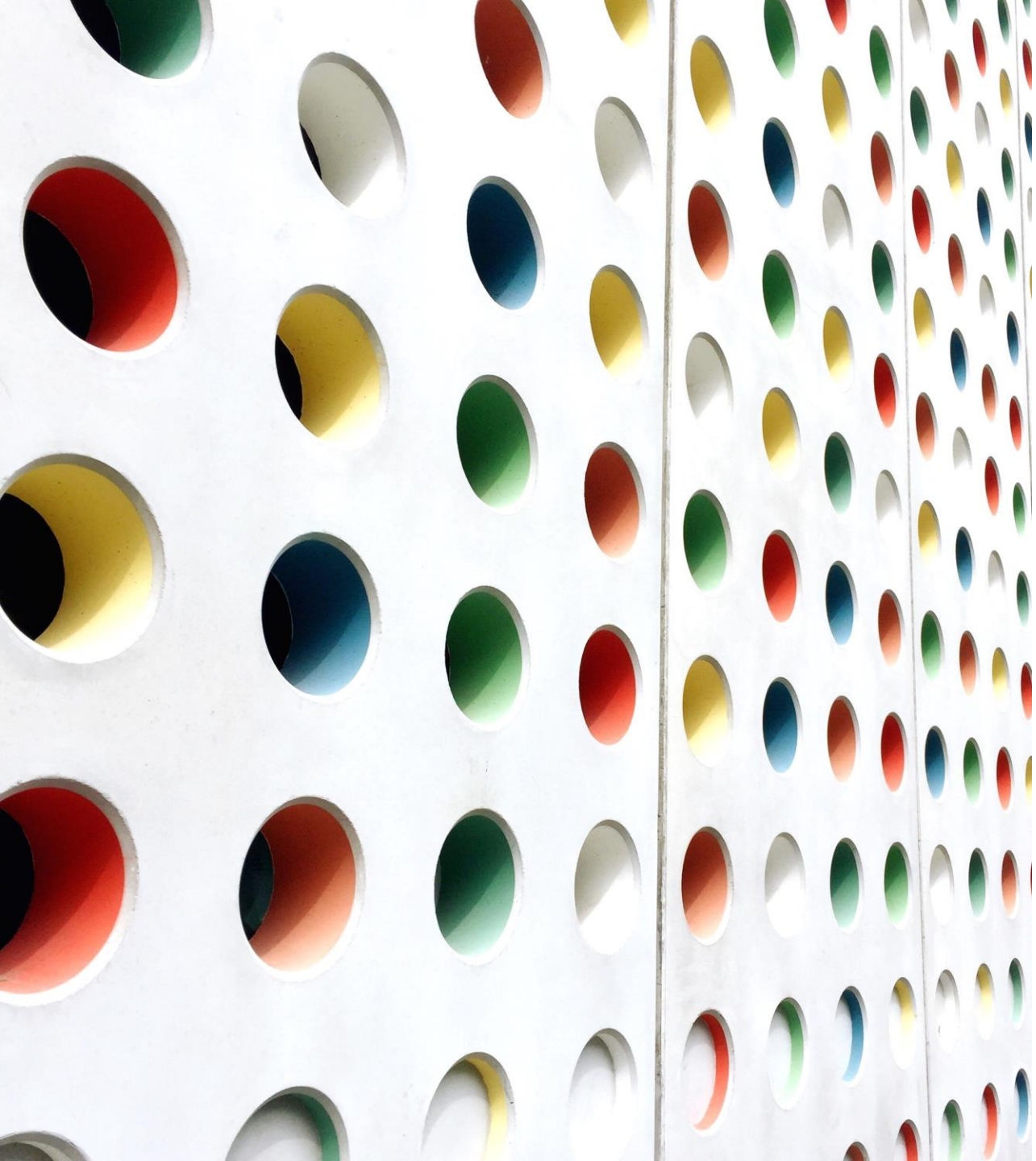

Cyber Kill Chain

APA TUH? MARI CARI TAU

Pengertian

Cyber Kill Chain merupakan tahapan-tahapan yang dilakukan para *hacker* untuk melancarkan serangan mereka kepada target dengan beberapa tujuan tertentu, seperti : bentuk spionase pemerintahan antar negara, orang yang memiliki dendam, orang yang disewa untuk menyerang target, dan orang yang ingin mengeksploitasi data target atau bahkan orang yang hanya iseng melakukan serangan kepada target.

Tahapan dalam *Cyber Kill Chain*

1. ENVIRONMENTAL AWARENESS

Pada fase ini sangat berkaitan dengan kepedulian dari pengguna terhadap sistem yang dimiliki, karena kelemahan pengguna ini bisa saja menjadi pintu serangan. Seperti contohnya klik link pada sembarang iklan digital, atau menerima email spam, dll.

Lalu bisa juga didapatkan kelemahan pada aplikasi pengguna seperti contohnya dalam jaringan, autentikasi dan otorisasi juga adanya aplikasi bajakan yang dipakai.

2. RECONNAISANCE & SCANNING

Fase pengintaian dan pemindaian ini bertujuan untuk mengumpulkan informasi dari target. Informasi bisa didapatkan dengan berinteraksi dan tanpa interaksi dengan korban. Seperti halnya cara yang biasa dilakukan adalah penetrasi ke port yang terbuka, IP address korban, dll.

Tahapan dalam *Cyber Kill Chain*

3. DELIVERY & ATTACK

Dalam pengiriman serangan kepada korban, penyerang dapat menyerang sistem korban dengan beberapa cara seperti salah satunya *broken authentication* yang dapat mengetahui *user authentication* menggunakan *brute force.*

Sebelum melakukan penyerangan, penyerang harus mengetahui informasi target, seperti OS yang digunakan, servis pada sistem target, dan target *software* atau port yang terbuka ke public.

4. EXPLOITATION & INSTALLATION

Exploitation bertujuan untuk mendapatkan akses kepada sistem korban. Biasanya setelah melakukan *Exploitation* dilakukan juga *Installation* yang akan menginstall malware yang sudah disisipkan pada aplikasi ataupun *software.* Kedua hal tersebut bertujuan agar penyerang bisa mendapatkan akses dan mempertahankan akses pada sistem korban.

Tahapan dalam *Cyber Kill Chain*

5. SYSTEM COMPROMISE

Pada fase ini penyerang bisa mengakses informasi pada *unauthorized access*. Pada fase ini penyerang bisa memodifikasi, merusak, atau menghilangkan sumber daya. Pada fase ini penyerang juga bisa mendapatkan akses untuk *command and control* (C2s). Tentunya fase serangan ini sangat berbahaya dan mengakibatkan kehilangan dan kerusakan data pada aset yang dimiliki perusahaan.

Pencegahan terhadap *Cyber Kill Chain*

- Melakukan PenTest secara berkala sebagai tindakan preventif
- Melakukan pelatihan untuk membangkitkan rasa *aware* terhadap *cyber security*
- Memperbarui *software* yang digunakan
- Menggunakan kata sandi yang kuat
- Membuat rencana *System Security*
- Enkripsi dan backup data yang sensitif secara rutin
- Menggunakan *Web Application Firewall*

Referensi

- https://cyberthreat.id/read/11619/Memahami-Taktik-Pengintaian-Peretas-dalam-Cyber-Kill-Chain
- https://beritakomputer.com/tutorial/5-fase-hacking-cyber-kill-chain/