SANS SECURITY AWARENESS

OUCH!

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Pencarian Maklumat Diri Sendiri Atas Talian

Pengenalan

Umum mengetahui kepentingan untuk melindungi privasi dan maklumat yang dikongsi di atas talian. Satu kaedah baru untuk mengetahui maklumat diri anda di atas talian ialah dengan melakukan pencarian mengenai diri anda di atas talian, dengan menggunakan maklumat diri anda, melalui sumber terbuka. Cara ini adalah dengan menggunakan OSINT atau nama lainnya Open Source Intelligence. Ini bermaksud mencari maklumat menggunakan sumber terbuka untuk mendapatkan sebanyak mungkin maklumat mengenai alamat IP, sesebuah syarikat dan juga diri anda sendiri. Sentiasa berwaspada bahawa kebanyakan penjenayah alam siber juga menggunakan teknik dan alatan yang sama untuk mencari maklumat dengan menggunakan kaedah OSINT. Sekiranya penjenayah ini berjaya mencungkil banyak maklumat mengenai diri anda, maka serangan siber yang ditujukan untuk anda akan lebih kemas dan terperinci. Walaupun konsep ini telah lama wujud, penggunaan alatan di atas talian menjadikan pencarian maklumat lebih mudah.

Cara Mendapatkan Maklumat

Pencarian maklumat bermula dengan satu laman sesawang. Dapatkan beberapa maklumat di satu laman sesawang dan dengan menggunakan maklumat tersebut, anda boleh mendapatkan maklumat seterusnya di laman sesawang lain. Perkara ini boleh dilakukan berterusan sehinggalah anda boleh menggabungkan dan membuat perbandingan antara maklumat yang telah di kumpul bagi membentuk satu profil atau dossier mengenai subjek yang dicari. Tempat pertama yang boleh anda mulakan pencarian mengenai diri anda adalah dengan menggunakan enjin carian seperti Google, Bing dan DuckDuckGo. Setiap enjin carian ini mempunyai indeks maklumat yang berbeza mengenai sesuatu maklumat, ini bermaksud carian dari setiap enjin ini akan memberikan hasil carian yang berbeza. Pencarian juga boleh dimulakan dengan mencari kata kunci di dalam simbol petikan. Simbol pengendali yang lain juga boleh digunakan untuk mendapat maklumat yang lebih lanjut. Simbol pengendali adalah simbol atau teks tertentu yang boleh digunakan untuk menjelaskan secara lebih terperinci mengenai perkara yang anda cari. Perkara ini sangat penting sekiranya nama anda umum dan lazim, jadi carian boleh dilakukan dengan menambah maklumat lain seperti alamat e-mel atau bandar tempat tinggal anda. Anda boleh mengetahui lebih lanjut mengenai pengendali dan teknik carian di bahagian Sumber di penghujung artikel ini. Berikut merupakan contoh yang dimaksudkan:

⚠

- **“NamaPertama NamaAkhir” > maklumat yang boleh dicari mengenai individu ini.**
- **“NamaPertama NamaAkhir@” > mencari alamat e-mel yang boleh dikaitkan dengan nama ini.**
- **“NamaPertama NamaAkhir” filetype:doc > mencari dokumen yang mempunyai nama ini.**

Terdapat beberapa laman sesawang yang bertujuan untuk mencari seseorang individu. Anda boleh menggunakan mana-mana laman sesawang seperti di bawah untuk cuba mencari maklumat terbuka yang boleh diketahui mengenai diri anda. Walaubagaimanapun, ada kemungkinan maklumat yang diberikan adalah tidak tepat atau mungkin maklumat tersebut tertakluk kepada negara-negara tertentu sahaja. Anda boleh menggunakan beberapa laman sesawang untuk mengenal pasti kesahihan maklumat yang ditemui.

- https://pipl.com
- https://cubib.com
- https://familytreenow.com

Akhir sekali, terdapat banyak lagi laman sesawang yang boleh digunakan untuk mencari lebih banyak maklumat seperti Google Images, Google Maps, pelbagai laman media sosial dan lain-lain. Anda boleh mendapatkan senarai laman web yang boleh digunakan untuk mencari diri anda di atas talian di OSINT Framework di alamat URL https://osintframework.com.

Keperluan Melakukan Pencarian Diri Anda Atas Talian

1. **Kenal pasti semua maklumat yang telah dikumpulkan, dipaparkan atau dikongsikan mengenai diri anda oleh individu atau organisasi lain (sekolah, kelab sukan atau mana-mana laman web komuniti tempatan).**
2. **Ambil maklum bahawa setiap sumber yang anda temui di atas talian boleh ditemui oleh orang lain, termasuk penjenayah siber yang boleh menggunakan maklumat yang sama untuk menujukan sesuatu serangan terhadap anda. Sentiasa berhati-hati dan berwaspada. Contohnya, jika anda menerima panggilan telefon yang kedengaran penting daripada bank dan bank tersebut menyebut beberapa maklumat mengenai diri anda, hal ini tidak membuktikan bahawa pihak bank yang sebenar telah menghubungi anda. Sebaliknya, letakkan panggilan tersebut dengan berhemat dan membuat panggilan telefon semula ke nombor telefon bank yang sebenar. Begitu juga dengan e-mel, sekiranya terdapat e-mel yang dikatakan daripada bank anda hanya kerana terdapat beberapa maklumat mengenai diri anda tidak bererti e-mel tersebut adalah sahih.**
3. **Selidik maklumat yang anda kongsikan secara umum dan impak maklumat yang telah dikongsikan kepada diri anda, keluarga dan majikan anda.**

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Editor Jemputan

Nico Dekens *(@dutch_osintguy) ialah seorang pakar penggunaan OSINT. Beliau banyak meluangkan masanya dengan aktiviti perisikan siber dan analisis. Nico merupakan salah seorang pensyarah antarabangsa yang mengajar subjek OSINT, IoT dan Operasi Sekuriti di syarikat-syarikat Fortune 500 dan agensi-agensi kerajaan.*

Sumber

Social Engineering:	https://www.sans.org/u/LW6
Social Media:	https://www.sans.org/u/LWb
Search Engine Operators:	https://support.google.com/websearch/answer/2466433
OSINT Framework:	https://osintframework.com/
SANS OSINT Course SEC487:	https://www.sans.org/u/LWZ