

Artikel 1:

3 Lapisan "Internet Iceberg" dan Potensi Bahaya yang Mengintai

Internet seperti sebuah “gunung es” yang besar, dimana hanya sebagian kecil yang terlihat di permukaan. Di bawah permukaannya, terdapat lapisan-lapisan yang lebih dalam yang penuh dengan potensi bahaya dan ancaman yang mengintai. Dari sinilah muncul istilah “**Internet Iceberg**”, dimana terdapat tiga lapisannya. Mari kita eksplorasi tiga lapisan dari “**Internet Iceberg**” dan bahaya yang mungkin ada di dalamnya.



Surface Web

[Surface web](#) adalah bagian dari internet yang dapat diakses melalui *search engine* seperti Google, Bing, dan Yahoo. Ini adalah bagian yang paling mudah dijangkau dan sering digunakan oleh pengguna internet untuk mencari informasi, berbelanja online, dan berkomunikasi melalui media sosial. Meskipun begitu, bahaya juga ada di sini.

Potensi Bahaya:

- **Phishing Attacks:** Penyerang dapat membuat situs web palsu yang menyerupai situs web asli untuk mencuri informasi sensitif pengguna, seperti kata sandi dan informasi keuangan.
- **Malware Distribution:** Situs web yang tidak aman dapat menyebarkan malware ke perangkat pengguna, menyebabkan kerusakan pada sistem atau pencurian data.
- **Pencurian Identitas:** Informasi pribadi pengguna dapat diretas atau dicuri melalui situs web yang rentan, digunakan untuk pencurian identitas atau penipuan.

Deep Web

[Deep web](#) adalah bagian dari internet yang tidak diindeks oleh *search engine* dan tidak dapat diakses secara langsung oleh pengguna biasa. Berbeda dengan surface web yang dapat dijelajahi dengan mudah, deep web terdiri dari halaman web yang tidak diindeks oleh *search*

engine atau memerlukan otentikasi khusus untuk diakses. Ini termasuk basis data *online*, halaman web yang dilindungi kata sandi, dan konten/dokumen rahasia yang tidak untuk dipublikasikan secara umum. Meskipun tidak terlihat, *deep web* memiliki potensi bahaya tersendiri.

Potensi Bahaya:

- Pencurian data pribadi dan perusahaan: Tindakan mengambil informasi sensitif pribadi maupun perusahaan tanpa izin, dapat mencakup data identitas, informasi keuangan, atau rahasia perusahaan. Hal ini dapat mengakibatkan kerugian finansial, pelanggaran privasi, dan penurunan reputasi bagi korban.

Dark Web

Dark web adalah bagian terdalam dan paling gelap dari internet, di mana aktivitas ilegal dan kriminalitas sering kali terjadi tanpa jejak digital. Di sini, pengguna menggunakan jaringan anonim seperti Tor untuk berkomunikasi secara rahasia dan anonim. *Dark web* merupakan tempat yang sangat berbahaya dan tidak diatur dengan baik. Maka itu, *data breach* sangat marak terjadi di lapisan ini, mulai dari jual beli data, hingga pembocoran data secara gratis..

Potensi Bahaya Dark Web:

- Black Market: *Dark web* adalah tempat di mana barang-barang ilegal seperti senjata, narkoba, hingga kredensial data pribadi maupun korporasi dijual secara bebas.
- Pasar Informasi Pribadi: Informasi pribadi, seperti nomor kartu kredit, *password*, dan SSN (*Social Security Number*), dijual di pasar gelap untuk tujuan penipuan atau pencurian identitas.
- Jasa Kriminalitas: Layanan kriminalitas, seperti sewa *hacker*, pencurian identitas, dan serangan DDoS, tersedia untuk siapa saja yang bersedia membayar.
- Eksploitasi Anak: Situs-situs yang menampilkan konten eksploitasi anak dan perdagangan manusia dapat ditemukan di *dark web*.

Dalam menjelajahi internet, penting bagi pengguna untuk memahami bahaya yang mungkin tersembunyi di setiap lapisan "*Internet Iceberg*". Dengan waspada dan berhati-hati, kita dapat mengurangi risiko jatuh ke dalam jebakan online dan menjaga diri kita dan informasi pribadi kita tetap aman. Salah satu hal yang bisa dilakukan adalah *dark web monitoring*. Mari tingkatkan keamanan data pribadi maupun perusahaan dimanapun Anda berada!