Bintang Yosafat Putra
119140185
Pemrograman Web Lanjut

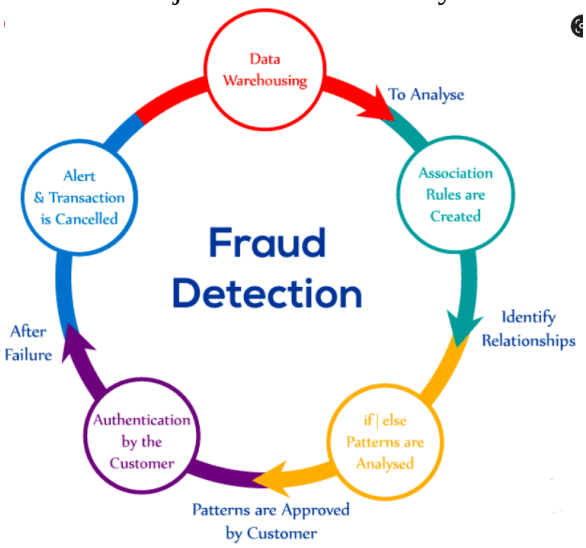
Tugas Individu 3

Teknik Keamanan Website

1. Gunakan SSL (Secure Socket Layer)
    - SSL merupakan sebuah sistem keamanan yang membuat website solah-olah telah tervalidasi oleh perusahaan tingkat dunia dan dapat meningkatkan kepercayaan pengunjung maupun calon pengunjung.
    - Dengan SSL, website dapat berubah otomatis menjadi HTPPS yang berarti website sudah memiliki keamanan yang memadai
    - Cara Kerja :
        1) Handshake Protocol
           Pada tahap ini hubungan antar client dan server atau web browser dan website, mulai dibangun. Client akan membangun koneksi awal melalui akses yang terdapat pada sertifikat SSL.
        2) Record Protocol
           Setelah client dan server terhubung, seluruh data yang masuk akan langsung terenkripsi oleh sistem. Kemudian server akan melakukan pengecekan dan konfigurasi data. Jika server dinilai aman, maka server akan memberikan public key yang berfungsi untuk mengenkripsi data yang akan dikirim kepada client.
        3) Alert Protocol
           Pada tahapan ini SSL akan memberikan tanda pada data yang dinilai mencurigakan dan tidak aman. Biasanya, ditandai dengan “Not Secure” pada laman website. Sebaliknya, jika website dinilai aman, maka pengunjung dapat mengakses website yang dimiliki tanpa adanya peringatan apapun.
    - Manfaat dan Keunggulan menggunakan SSL :
        1) Meningkatkan Keamanan Website
        2) Mencegah Serangan Phising
        3) Autentikasi
        4) Efisiensi Biaya
        5) Meningkatkan Ranking SEO

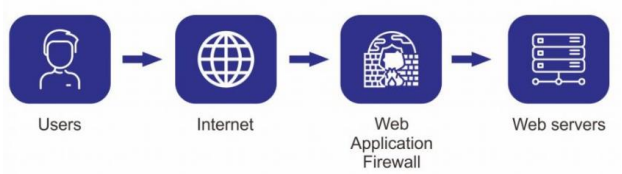
Sumber :
https://www.biznetgio.com/news/apa-itu-ssl-cara-kerja-dan-fungsinya#:~:text=Untuk%20memberikan%20tingkat%20keamanan%20data,dibaca%20dan%20diterjemahkan%20oleh%20hacker.

2. Pentingnya FDS (Fraud Detection System)
    - Fraud Detection System atau FDS berguna untuk memblokir setiap transaksi yang terdeteksi fraud/penipuan atau kecurangan dalam binisi. Penipuan bisa berupa jual beli, pencurian identitas atau transaksi online
        - Cara Kerja Fraud Detection System :



Sumber : https://blog.kredibel.co.id/fraud-detection-system-bagaimana-cara-kerjanya/#apaitu

3. Install Web Application Firewall (WAF)
    - Web Application Firewall (WAF) adalah sebuah firewall yang memonitor, filter, dan memblok data yang berasal dari client ke sebuah website atau aplikasi web. Sebuah WAF bisa berbasis jaringan, host-based atau cloud-based, dan kadang digunakan melalui proxy terbalik di depan sebuah website atau aplikasi.
    - Cara Kerja :
        - Whitelisting ➔ WAF akan menolak semua permintaan secara default dan hanya mengizinkan permintaan yang sudah dipercaya
        - Blacklisting ➔ penggunaan peraturan tertentu yang mampu mengindikasikan sebuah bahaya. Blacklisting lebih tepat untuk website publik karena banyak menerima traffic dari alamat IP yang tidak familiar, dan tidak diketahui apakah itu traffic berbahaya atau baik.
        - Hybrid Security
          Model ini menggunakan baik elemen whitelisting dan blacklisting



Sumber : https://indonesiancloud.com/apa-itu-web-application-firewall-waf/#:~:text=Cara%20kerja%20WAF&text=Bagian%20utama%20HTTP%20yang%20dianalisis,dan%20menyaring%20konten%20dari%20HTTP.

Studi Kasus 1

Kasus:

Jaringan internet di Pusat Tabulasi Nasional Komisi Pemilihan Umum sempat down (terganggu) beberapa kali. KPU menggandeng kepolisian untuk mengatasi hal tersebut. “Cybercrime kepolisian juga sudah membantu. Domain kerjasamanya antara KPU dengan kepolisian”, kata Ketua Tim Teknologi Informasi KPU, Husni Fahmi di Kantor KPU, Jalan Imam Bonjol, Menteng, Jakarta Pusat (15 April 2009). Menurut Husni, tim kepolisian pun sudah mendatangi Pusat Tabulasi Nasional KPU di Hotel Brobudur di Hotel Brobudur, Jakarta Pusat. Mereka akan mengusut adanya dugaan kriminal dalam kasus kejahatan dunia maya dengan cara meretas. “Kamu sudah melaporkan semuanya ke KPU. Cybercrime sudah datang,” ujarnya. Sebelumnya, Husni menyebut sejak tiga hari dibuka, Pusat Tabulasi berkali-kali diserang oleh peretas.” Sejak hari lalu dimulainya perhitungan tabulasi, samapai hari ini kalau dihitung-hitung, sudah lebuh dari 20 serangan”, kata Husni, Minggu(12/4). Seluruh penyerang itu sekarang, kata Husni, sudah diblokir alamat IP-nya oleh PT. Telkom. Tim TI KPU bias mengatasi serangan karena belajar dari pengalamn 2004 lalu. “Memang sempat ada yang ingin mengubah tampilan halaman tabulasi nasional hasil pemungutan suara milik KPU. Tetapi segera kami antisipasi.”

Penjelasan:

Kasus di atas memiliki modus untuk mengacaukan proses pemilihan suara di KPK. Motif kejahatan ini termasuk ke dalam cybercrime sebagai tindakan murni kejahatan. Hal ini dikarenakan para penyerang dengan sengaja untuk melakukan pengacauan pada tampilan halaman tabulasi nasional hasil dari Pemilu. Kejahatan kasus cybercrime ini dapat termasuk jenis data forgery, hacking-cracking, sabotage and extortion, atau cyber terorism. Sasaran dari kasus kejahatan ini adalah cybercrime menyerang pemerintah (against government) atau bisa juga cybercrime menyerang hak milik (against property).

Penanganan:

Internet Firewall: untuk mencegah akses dari pihak luar ke sistem internal. Firewall dapat bekerja dengan 2 cara, yaotu menggunakan filter dan proxy. Firewall filter menyaring komunikasi agar terjadi seperlunya saja, hanya aplikasi tertentu saja yang bisa lewat dan hanya komputer dengan identitas tertentu saja yang bisa berhubungan. Firewall proxy berarti mengizinkan pemakai dalam untuk mengakses internet seluas-luasnya, tetapi dari luar hanya dapat mengakses satu komputer tertentu saja.

Studi Kasus 2

Kasus:

Dunia perbankan dalam negeri juga digegerkan dengan ulah Steven Haryanto, yang membuat situs asli tetapi palsu layanan perbankan lewat Internet BCA. Lewat situs-situs “Aspal”, jika nasabah salah mengetik situs asli dan masuk ke situssitus tersebut, identitas pengguna (user ID) dan nomor identifikasi personal (PIN) dapat ditangkap. Tercatat 130 nasabah tercuri data-datanya, namun menurut pengakuan Steven pada situs Master Web Indonesia, tujuannya membuat situs plesetan adalah agar publik memberi perhatian pada kesalahan pengetikan alamat situs, bukan mengeruk keuntungan.

Persoalan tidak berhenti di situ. Pasalnya, banyak nasabah BCA yang merasa kehilangan uangnya untuk transaksi yang tidak dilakukan. Ditengarai, para nasabah itu kebobolan karena menggunakan fasilitas Internet banking lewat situs atau alamat lain yang membuka link ke Klik BCA, sehingga memungkinkan user ID dan PIN pengguna diketahui. Namun ada juga modus lainnya, seperti tipuan nasabah telah memenangkan undian dan harus mentransfer sejumlah dana lewat Internet dengan cara yang telah ditentukan penipu ataupun saat kartu ATM masih di dalam mesin tiba-tiba ada orang lain menekan tombol yang ternyata mendaftarkan nasabah ikut fasilitas Internet banking, sehingga user ID dan password diketahui orang tersebut.

Penjelasan :

Modus kejahatan ini adalah penyalahgunaan user_ID dan password oleh seorang yang tidak punya hak. Motif kegiatan dari kasus ini termasuk ke dalam cybercrime sebagai kejahatan “abu-abu”. Kasus cybercrime ini merupakan jenis cybercrime uncauthorized access dan hacking-cracking. Sasaran dari kasus ini termasuk ke dalam jenis cybercrime menyerang hak milik (against property). Sasaran dari kasus kejahatan ini adalah cybercrime menyerang pribadi (against person).

Penanganan:

Penggunaan enkripsi yaitu dengan mengubah data-data yang dikirimkan sehingga tidak mudah disadap (plaintext diubah menjadi chipertext). Untuk meningkatkan keamanan authentication (pengunaan user_id dan password), penggunaan enkripsi dilakukan pada tingkat socket. Hal ini akan membuat orang tidak bias menyadap data atau transaksi yang dikirimkan dari/ke server WWW. Salah satu mekanisme yang popular adalah dengan menggunakan Secure Socket Layer (SSL) yang mulanya dikembangkan oleh Nerscape. Selain server WWW dari netscape, server WWW dari Apache juga dapat dipakai karena dapat dikonfigurasikan agar memiliki fasilitas SSL dengan menambahkan software tambahan, sperti open SSL

Penggunaan Firewall Tujuan utama dari firewall adalah untuk menjaga agar akses dari orang tidak berwenang tidak dapat dilakukan. Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang keluar dan masuk harus melalui atau melewati firewall. Firewall bekerja dengan mengamati paker Intenet Protocol (IP) yang melewatinya.