**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

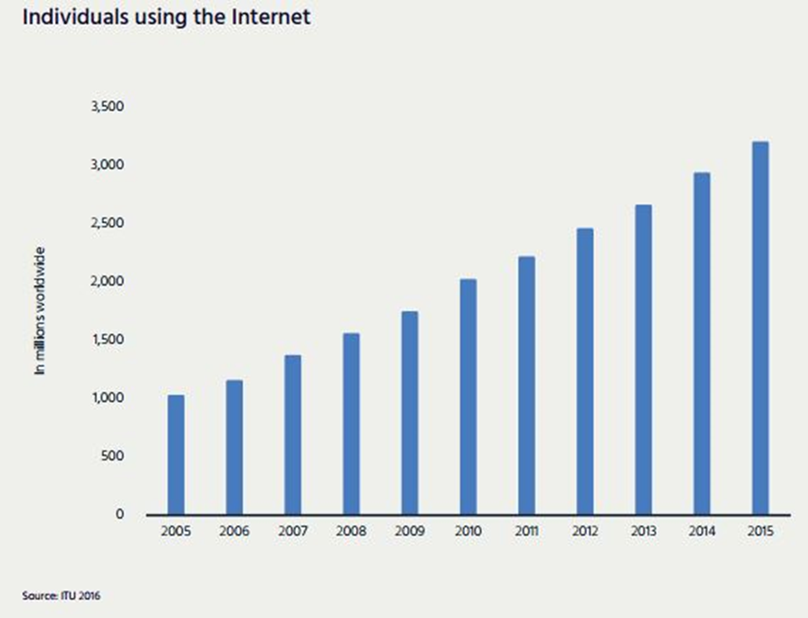
**KDS – Name SME**

**Session 08**

**IT Security and prevention**

1. **Pendahuluan IT Security**

Pada tahun 2016 ini, lebih dari separuh penduduk Indonesia sudah terhubung ke internet. Data ini adalah hasil dari survey yang dilakukan oleh Asosiasi Penyelenggara Jaringan Internet Indonesia (APJII). APJII menemukan bahwa di tahun 2016 ada 132,7 juta orang Indonesia sudah terhubung ke internet dengan total populasi penduduk Indonesia 256,2 juta orang. Dari angka tersebut dapat diambil kesimpulan bahwa sudah separuh penduduk Indonesia yang terhubung ke internet. Padahal pada tahun sebelumnya, di tahun 2015, APJII menemukan hanya 88 juta pengguna internet di Indonesia. Hal ini menunjukkan ada kenaikkan pengguna internet sebesar 51,8 persen dari tahun 2015 ke tahun 2016.



Gambar 1. Grafik pengguna internet di seluruh dunia

Survey juga menunjukkan bahwa lebih dari separuh pengguna internet mengakses internet dengan menggunakan peralatan yang dapat dibawa atau mobile yaitu smartphone atau perangkat gengam lainnya dan laptop, statistiknya sebagai berikut:

• 67,2 juta orang atau 50,7 persen mengakses melalui perangkat genggam dan komputer.

• 63,1 juta orang atau 47,6 persen mengakses dari smartphone.

• 2,2 juta orang atau 1,7 persen mengakses hanya dari komputer.

Kenaikkan jumlah pengguna internet ini akan terus bertambah. Tren kenaikkan ini bukan hanya terjadi di Indonesia, tetapi juga terjadi diseluruh belahan dunia. Ke depan nya di prediksi setiap orang didunia akan terhubung lewat internet. Kenaikkan jumlah pengguna internet ini dikarenakan semakin banyaknya aplikasi yang tersedia di internet yang dapat mempermudah dalam kegiatan sehari hari. Sehingga menarik masyarakat untuk menggunakannya.

Pada gambar 1 terlihat perkembangan pengguna internet yang selalu naik dari tahun 2005 sampai 2015. Dimana pengguna internet didunia sudah mencapai 3,2 milyar di tahun 2015.

**Tantangan dalam Information Security**

Seiring dengan meningkatnya jumlah aplikasi di internet dan jumlah pengguna internet, maka meningkat pula kejahatan yang menggunakan internet. Semakin beragam aplikasi yang ada di internet semakin beragam pula kejahatan yang ada di internet.

Kejahatan yang paling banyak dilakukan pada saat ini adalah dengan melalui websites. Menurut acunetix, pada saat ini sebesar 70% dari websites dan networks berpotensial dapat diserang atau di eksploitasi oleh hacker.

Ada berbagai macam cara untuk menyerang website seperti:

1. Injection

Kelemahan injeksi, seperti SQL, OS, dan injeksi LDAP terjadi ketika data yang tidak dipercaya dikirim ke seorang hacker sebagai bagian dari perintah atau permintaan. Data penyerang ini dapat mengelabui interpreter untuk mengeksekusi perintah yang tidak diinginkan atau mengakses data tanpa otorisasi yang tepat.

2. Broken Authentication and Session Management

Fungsi aplikasi yang berhubungan dengan otentikasi dan manajemen sesi sering tidak diterapkan dengan benar, memungkinkan penyerang untuk kompromi password, kunci, atau token sesi, atau untuk mengeksploitasi kelemahan pelaksanaan lainnya untuk mengasumsikan identitas pengguna lain '.

3. Cross-site Scripting

XSS flaws terjadi ketika aplikasi mengambil data yang tidak dipercaya dan mengirimkannya ke web browser tanpa validasi yang tepat. XSS memungkinkan penyerang untuk mengeksekusi skrip di browser korban yang dapat membajak sesi pengguna, merusak situs web, atau mengarahkan pengguna ke situs berbahaya.

4. Insecure Direct Object References

Sebuah direct object reference terjadi ketika seorang pengembang menghadapkan referensi ke suatu objek implementasi internal, seperti file, direktori, atau kunci basis data. Tanpa pemeriksaan kontrol akses atau perlindungan lainnya, penyerang dapat memanipulasi referensi ini untuk mengakses data yang tidak sah.

5. Security Misconfiguration

Keamanan yang baik memiliki konfigurasi yang aman, didefinisikan dan digunakan untuk aplikasi, kerangka kerja, server aplikasi, web server, database server, dan platform. Pengaturan keamanan harus didefinisikan, diimplementasikan, dan dipelihara, karena default sering tidak aman. Selain itu, perangkat lunak harus selalu up to date.

6. Sensitive Data Exposure

Banyak aplikasi web tidak benar melindungi data sensitif, seperti kartu kredit, nomor pajak, dan kredensial otentikasi. Penyerang dapat mencuri atau memodifikasi data tersebut untuk melakukan penipuan kartu kredit, pencurian identitas, atau kejahatan lainnya. Data sensitif layak dibuat perlindungan ekstra seperti enkripsi baik dalam penyimpanan ataupun dalam perjalanan dalam jaringan, serta tindakan pencegahan khusus ketika ditukar dengan browser.

7. Missing Function Level Access Control

Sebagian besar aplikasi web memverifikasi level hak akses. Namun, aplikasi perlu melakukan pemeriksaan kendali akses yang sama pada server ketika masing-masing fungsi diakses. Jika permintaan tidak diverifikasi, penyerang akan dapat menempa permintaan untuk mengakses fungsi tanpa otorisasi yang tepat.

8. Cross-site Request Forgery (CSRF)

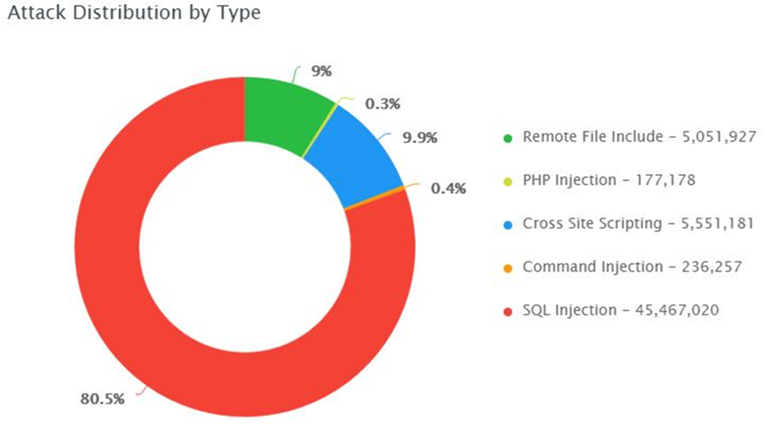
Sebuah serangan CSRF memaksa browser log-on korban untuk mengirim permintaan HTTP, termasuk cookie sesi dan informasi otentikasi, untuk aplikasi web yang rentan. Hal ini memungkinkan penyerang untuk memaksa browser korban untuk menghasilkan permintaan aplikasi yang menurutnya adalah permintaan yang sah dari korban.

9. Using Components with Known Vulnerabilities

Komponen, seperti perpustakaan, kerangka kerja, dan modul perangkat lunak lain, hampir selalu dijalankan dengan hak penuh. Jika komponen rentan dieksploitasi, dapat mengakibatkan kehilangan data atau server dapat diambil alih.

10. Unvalidated Redirects and Forwards

Aplikasi web sering mengarahkan dan meneruskan pengguna ke halaman lain dan website, dan menggunakan data yang tidak dipercaya untuk menentukan halaman tujuan. Tanpa validasi yang tepat, penyerang dapat mengarahkan korban phishing atau malware situs, atau menggunakan depan untuk mengakses halaman yang tidak sah.



Gambar 2. Distribusi tipe serangan

Dari berbagai macam serangan tersebut, menurut Akamai, serangan dengan SQL injection merupakan yang paling banyak. Seperti dapat terlihat pada gambar 2, serangan SQL injection mencapai 45,467.021 atau sebesar 80.5% dari semua serangan di tahun 2015.

**Definisi Information Security**

Menurut Committee on National Security Systems (CNSS) information security is the protection of information and its critical elements, including systems and hardware. Apabila diterjemahkan adalah sebagai berikut: keamanan informasi adalah sebuah perlindungan terhadap informasi dan elemen elemennya termasuk perangkat keras dan sistemnya.

Sementara itu apabila kita mengacu kepada konsep segitiga C.I.A. dimana konsep berdasarkan tiga karakteristik informasi yaitu:

– Confidentiality

– Integrity

– Availability

Apabila digabung maka information security adalah sebuah perlindungan informasi dari confidentiality, integrity, and availability baik dalam penyimpanan, saat di proses atau pada saat ditransmisikan.

**Penyerang, Hacker, atau Attacker**

Berikut adalah definisi definisi yang akan digunakan dalam kelas ini

• Hacker adalah seseorang atau sekumpulan orang yang berbuat untuk kebaikkan pada hal hal yang berhubungan dengan software atau program computer. Misalnya mencari dan mendapatkan kelemahan pada suatu program memperbaikinya dan memberitahu kepada orang yang bersangkutan dengan program tersebut.

• Cracker adalah seseorang yang sengaja mencoba mencari kelemahan dari sebuah system security dengan tujuan untuk mendapatkan keuntungan pribadi. Misalnya mengcrack sebuah software, mencuri data data, menghilangkan atau merusak data dan system.

• Script kiddies adalah sebuah program jahat yang tersedia dimana dapat digunakan oleh orang orang yang tidak berpengalaman. Biasanya program jahat ini bertujuan untuk merusak computer atau system. Juga program ini dapat mudah didownload.

**Security Strategy**

Beberapa konsep strategi untuk system keamanan dapat di lihat seperti dibawah ini.

• Layering: Menciptakan penghalang dari beberapa pertahanan yang dapat dikoordinasikan untuk menggagalkan berbagai serangan.

• Limiting: Membatasi akses ke informasi akan mengurangi ancaman terhadap informasi itu sendiri.

• Diversity: Apabila satu lapisan keamanan terserang tidak akan mengorbankan seluruh system keamanan.

• Obscurity: Menghindari pola karakteristik perilaku atau kebiasaan akan membuat serangan dari luar lebih sulit.

• Simplicity: Membuat sebuah sistem yang sederhana dari dalam tetapi kompleks di luar akan sangat bermanfaat besar.