RESUME

SEMINAR KOMUNITAS CSI

AISHA FITRIA SALSABILA

CASSANDRA

DEPARTEMEN ILMU KOMPUTER

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

IPB UNIVERSITY

2023

“Why Hackers Want Your Data and The Importance of Protecting It”

Heri Susanto (*heri@bangunindo.com*)

RESUME

Domain Keamanan *Cyber*

1. Edukasi Pengguna
   Pengguna sering kali menjadi mata rantai terlemah dalam keamanan siber.

2. Kerangka & Standar
   Metodologi untuk menilai dan mengelola risiko keamanan.

3. Arsitektur Keamanan
   Arsitektur keamanan yang kuat melibatkan perancangan dan penerapan langkah-langkah keamanan di seluruh infrastruktur TI organisasi.

4. Keamanan Aplikasi
   Aplikasi dapat memiliki kerentanan yang dieksploitasi oleh penyerang.

5. Operasi Keamanan
   Operasi keamanan mencakup pemantauan, deteksi, dan respons berkelanjutan terhadap insiden keamanan.

Tujuan Pelanggaran Data

- Tantangan Intelektual, misalnya peretasan topi putih.
- Keuntungan Finansial, misalnya kredensial login data pribadi sensitif data kartu kredit.
- Membuat Poin Sosial atau Politik, misalnya melalui *hacktivisme*.
- Spionase, misalnya memata-matai pesaing untuk mendapatkan keuntungan yang tidak adil.

Ancaman Umum Keamanan Siber

1. Perusak Perangkat Lunak
   Perangkat lunak berbahaya yang dapat menginfeksi komputer dan jaringan, menyebabkan kerusakan atau akses tidak sah.

2. Phising
   Penjahat dunia maya berupaya menipu individu agar memberikan informasi sensitif, seperti kata sandi atau rincian kartu kredit.

3. Serangan Penolakan Layanan (DoS)
   Membanjiri jaringan dengan permintaan palsu untuk mengganggu operasi bisnis.

4. Rekayasa Sosial
   Memanipulasi individu untuk mendapatkan akses tidak sah ke sistem atau informasi.

5. Pemalsuan
   Aktor jahat menyamar sebagai entitas atau sumber yang sah. untuk menipu target, mendapatkan akses tidak sah, atau memanipulasi data.

6. Serangan Berbasis Identitas
   Memanfaatkan kerentanan dalam sistem otentikasi dan otorisasi pengguna untuk mendapatkan akses tidak sah ke informasi atau sistem sensitif.

7. Serangan Injeksi Kode
   Kode berbahaya dimasukkan ke dalam aplikasi, mengeksploitasi kerentanan untuk mendapatkan kontrol tidak sah atau melakukan tindakan yang tidak diinginkan.

8. Serangan Rantai Pasokan
   Menyusup ke sistem melalui vendor pihak ketiga yang telah disusupi, mengeksploitasi hubungan tepercaya mereka untuk menyebarkan malware atau kerentanan.

9. Penerowongan DNS
   Penerowongan DNS secara diam-diam mentransfer data melalui permintaan dan respons DNS, menghindari tindakan keamanan.

10. Serangan Berbasis IoT
    Menyerang perangkat Internet of Things yang rentan untuk mendapatkan akses tidak sah, mengganggu layanan, atau melancarkan serangan siber yang lebih luas.

Konsekuensi Pelanggaran Data

- Dampak Finansial dan Reputasi.
- Akibat Hukum dan Sanksi Peraturan.
- Gangguan Operasional dan Downtime.
- Kekayaan Intelektual dan Dampak Inovasi.
- Kejatuhan Pribadi dan Konsekuensi Jangka Panjang.

Area Keamanan Perusahaan

1. Keamanan Jaringan
   Melindungi infrastruktur jaringan organisasi dari akses tidak sah dan ancaman dunia maya.

2. Keamanan Aplikasi
   Memastikan bahwa aplikasi perangkat lunak bebas dari kerentanan dan terlindungi dari serangan.

3. Keamanan Titik Akhir
   Mengamankan perangkat individu (titik akhir) yang terhubung ke jaringan.

4. ID & Manajemen Akses (IAM)
   Mengontrol dan mengelola identitas pengguna dan akses mereka ke sumber daya.

5. Perlindungan Data
   Melindungi data sensitif dari akses dan pelanggaran yang tidak sah.

PERSPEKTIF BARU

Perspektif baru yang diperoleh setelah mengikuti seminar ini adalah bahwa keamanan siber bukan hanya masalah teknis, tetapi juga melibatkan aspek-aspek seperti pendidikan pengguna, kerangka dan standar, dan arsitektur yang kuat. Selain itu, ancaman keamanan siber bervariasi dan memiliki tujuan yang beragam, sehingga organisasi harus siap dengan strategi yang berbeda untuk menghadapinya. Selain itu, pentingnya melindungi berbagai area, termasuk jaringan, aplikasi, titik akhir, identitas pengguna, dan data sensitif, menyoroti perlunya pendekatan holistik dalam mengelola keamanan siber.

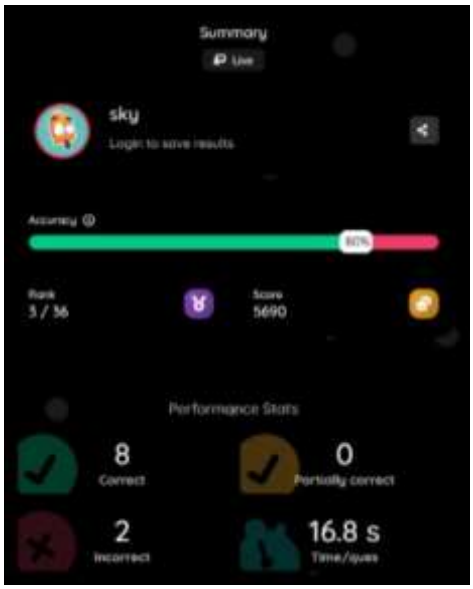
KERELEVAN SEMINAR

Materi tersebut sangat relevan dengan bidang IT karena membahas aspek-aspek kunci dalam keamanan siber yang esensial dalam melindungi sistem dan data dalam lingkungan teknologi informasi. Mencakup pemahaman tentang peran pengguna, adopsi kerangka

dan standar, perancangan arsitektur keamanan, perlindungan aplikasi, operasi keamanan berkelanjutan, serta pengenalan berbagai ancaman umum dan tujuan pelanggaran data. Selain itu, materi ini juga menguraikan berbagai area fokus dalam keamanan perusahaan, termasuk keamanan jaringan, aplikasi, titik akhir, manajemen akses, dan perlindungan data, yang semuanya relevan dalam konteks pengelolaan keamanan teknologi informasi.

PEMIKIRAN DAN TANGGAPAN PRIBADI

Seminar ini tidak hanya memberikan insight yang luar biasa namun juga memiliki susunan acara yang santai dan tetap produktif juga diakhiri dengan sesi QnA yang menyenangkan.



Gambar: Ketika saya mengikuti Quizizz di sesi akhir acara namun juara 3 *NT ☹

Saran: Memilih moderator yang tidak semaniez ini krn sy agak salfok trs selama pembicaranya menyampaikan materi 😊

KETERTARIKAN TERHADAP KOMUNITAS

Sebetulnya saya tertarik mengikuti CSI namun alangkah baiknya saya tidak gegabah dalam mengikuti komunitas karena sedang join daming *eaak. Smoga sy diberi hidayah dan kemantapan hati bila suatu hari ingin mengikuti CSI. AAMIINN…

RENCANA KONTRIBUSI

Jujurly this is the part of makin me think the most krn kan literally klo berencana hrs penuh ide cemerlang dan merenung di toilet or another peaceful place but yeah untuk saat ini blm kepikiran mw ngapain tp yg jelas I pray success for the entire ITToday events 💔