Pentingnya Keamanan Informasi Di Industri 4.0

****

**Oleh:**

**FAREL MUFADAL PUTRA**

**11850115197**

**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI SUSKA RIAU  
PEKANBARU   
2021**

# KATA PENGANTAR

Puji syukur penulis ucapkan kehadirat Allah Swt. atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan makalah ini. Dalam makalah ini, penulis akan membahas mengenai “Pentingnya Keamanan Informasi Di Industri 4.0”. Penulis ucapkan terima kasih kepada pihak yang memberikan kontribusi materi dan pikirannya. Harapan penulis semoga makalah ini dapat menambah pengetahuan pembaca dan dapat mengembangkan makalah ini menjadi lebih baik kedepannya. Semoga makalah ini dapat dipahami bagi siapapun yang membacanya.

Tidak lupa penulis ucapkan terima kasih kepada dosen pengampu mata kuliah , Sonya Meitarice, S.T.,M,SC, Yang telah memberikan bimbangan kepada penulis agar dapat menyelesaikan makalah ini dengan baik. Karena keterbatasan pengetahuan dan pengalaman penulis, banyak kekurangan yang mendasar pada makalah ini. Oleh karena itu, penulis sangat mengaharapkan saran dan kritiknya dari pembaca demi kesempurnaan makalah selanjutnya.

Pekanbaru , 16 April 2021

Penulis

Contents

[BAB I 3](#_Toc69507899)

[PENDAHULUAN 3](#_Toc69507900)

[1.1 Latar Belakang 3](#_Toc69507901)

[1.2 Rumusan Masalah 3](#_Toc69507903)

[1.3 Tujuan Penulisan 4](#_Toc69507907)

[BAB II 5](#_Toc69507908)

[PEMBAHASAN 5](#_Toc69507909)

[2.1 Keamanan Informasi 5](#_Toc69507910)

[2.2 pengaruh keamanan informasi di industry 4.0 6](#_Toc69507911)

[2.3 Cara Menjaga Keamanan Informasi 7](#_Toc69507914)

[BAB III 8](#_Toc69507915)

[PENUTUP 8](#_Toc69507916)

[3.1 Simpulan 8](#_Toc69507917)

[DAFTAR PUSTAKA 9](#_Toc69507918)

# BAB I

# PENDAHULUAN

## Latar Belakang

Pada zaman teknologi informasi sekarang, data atau informasi merupakan suatu asset yang sangat berharga dan harus dilindungi. Hal ini juga diikuti oleh kemajuan teknologi komputer. Kemajuan teknologi komputer membantu semua aspek kehidupan manusia. Dari hal kecil sederhana sampai hal yang sangat rumit sekalipun bisa dikerjakan komputer. Keunggulan dari aplikasi komputer ini selain memberi kemudahan terhadap berbagai kegiatan pengolahan data dan informasi di berbagai bidang kehidupan, misalnya penggunaan komputer dalam bidang pemerintahan, organisasi social, militer, bank, pendidikan, transportasi, perdagangan, industri, dan lain sebagainya. Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka kemudian muncul masalah baru, yaitu masalah keamanan akan data dan informasi dan dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan.

Di era 4.0 ini, keamanan ini sangat penting, karna dengan adanya tenologi keamanan informasi, maka akan semakin terlindungi data-data penting. .dalam kesempatan ini penulis akan mencoba menjelaskan pentingnya keamanan informasi di industri 4.0.

## Rumusan Masalah

Berdasarkan latar belakang di atas, penulis akan menjabarkan rumusan masalah sebagai berikut:

1. Apa itu keamanan informasi ?
2. Apa pengaruh keamanan informasi di industry 4.0 ?
3. Bagaimana cara menjaga keamanan informasi ?

## Tujuan Penulisan

Tujuan pembuatan makalah ini penulis jabarkan sebagai berikut:

1. Mengetahui yang dimaksud dengan keamanan informasi
2. Mengetahui pengaruh keamanan informasi di industri 4.0
3. Mengetahui cara menjaga keamanan informasi

# BAB II

# PEMBAHASAN

## 2.1 Keamanan Informasi

Keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (*right information*), informasi dipegang oleh orang yang berwenang (*right people*), dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan memberikan informasi pada format yang tepat (*right form*). Dalam membuat program keamanan informasi ada prinsip dasar yang harus dipenuhi agar sistem tersebut handal. Prinsip dasar tersebut adalah:

1. Kerahasiaan artinya informasi dijamin hanya tersedia bagi orang yang berwenang sehingga pihak yang tidak berhak tidak bisa mengakses informasi. Contoh kerahasiaan adalah seorang administrator tidak boleh membuka atau membaca email milik pengguna. Selain itu kerahasiaan harus menjamin data-data yang harus dilindungi penggunaan dan penyebarannya baik oleh pengguna maupun administrator, seperti nama, alamat, tempat tanggal lahir, nomor kartu kredit, penyakit yang diderita, dan sebagainya.
2. Integritas artinya informasi dijaga agar selalu akurat, untuk menjaga informasi tersebut maka informasi hanya boleh diubah dengan izin pemilik informasi. Virus trojan merupakan contoh dari informasi yang integritasnya terganggu karena virus telah mengubah informasi tanpa izin. Integritas informasi ini dapat dijaga dengan melakukan enkripsi data atau membuat tanda tangan dijital (*digital signature*).
3. Ketersediaan artinya adanya jaminan ketika pihak berwenang membutuhkan informasi, maka informasi dapat diakses dan digunakan. Hambatan dalam ketersediaan ini contohnya adalah adanya *Denial of Service Attack* (DoS). DoS merupakan serangan yang ditujukan ke server, di mana banyak sekali permintaan yang dikirimkan ke server dan biasanya permintaan tersebut palsu yang menyebabkan server tidak sanggup lagi melayani permintaan karena tidak sesuai dengan kemampuan sehingga server menjadi *down*bahkan *error*.

Dengan terpenuhinya aspek-aspek sistem keamanan informasi dan prinsip dasar penyusunan program keamanan informasi tersebut maka sumber daya informasi terjamin dan terlindungi dari ancaman pihak-pihak yang tidak berwenang yang akan memanfaatkan data dan informasi untuk kepentingan yang merugikan organisasi atau perusahaan.

## 2.2 pengaruh keamanan informasi di industry 4.0

Revolusi industri 4.0 dan peningkatan konektivitas antara bisnis dengan kehidupan sehari-hari kini tengah mendorong transformasi bisnis dan memajukan para karyawan dan pelanggan di seluruh dunia. Akan tetapi fenomena revolusi industri 4.0 ini membawa banyak pengaruh, baik positif maupun negatif bagi masyarakat. Dimana semua lini tengah berlomba untuk melakukan digitalisasi agar tidak terlindas oleh teknologi yang terus berkembang. Terlebih lagi masyarakat millennials menjadi salah satu ujung tombak yang penting untuk di berikan ruang dan kesempatan untuk berinovasi. Salah satu dampak negative dibalik kecanggihan yang ada, yakni keamanan dan data pribadi yang rentan bocor kepada pihak-pihak yang tidak bertanggung jawab yang memanfaatkan kelengahan sistem keamanan.

Penelitian yang dilakukan oleh perusahaan security McAfee mengatakan bahwa Kejahatan cyber terjadi tanpa henti, jumlahnya tidak pernah berkurang dan terjadi begitu masif setiap saat di berbagai belahan dunia. Pelaku kejahatan internet memanfaatkan celah untuk mengeksploitasi sebuah sistem dan meminta sejumlah bayaran atas ulahnya. Mereka bergerak sangat cepat, mengadopsi teknologi cloud serta enkripsi yang sulit untuk diketahui jejaknya. Kejahatan cyber semakin berkembang dengan kurangnya security awareness perusahaan terhadap revolusi industri menjadikan perusahaan tersebut menjadi sasaran yang mudah sekali dimonetasi. Bank menjadi target favorit para penjahat dunia maya, dan hal ini telah terjadi lebih dari satu dekade. Kejahatan cyber dapat mengakibatkan kebocoran data nasabah serta uang yang besar. Hal tersebut tentunya menjadi ancaman serius oleh bank serta nasabah yang menyimpan uang.

## 2.3 Cara Menjaga Keamanan Informasi

Untuk memastikan bahwa aplikasi suatu perusahaan aman dari serangan siber, kita perlu melakukan uji keamanan yaitu dengan cara melakukan simulasi serangan siber fiktif yang dilakukan pada sistem komputer untuk mencari kelemahan pada aplikasi perusahaan kita.berikut cara menjaga keamanan informasi :

1. Menghubungkan para peneliti keamanan (bug hunter) dengan pihak perusahaan atau organisasi yang terkena dampak serangan siber;

2. Mengelola laporan kerentanan yang telah masuk;

3. Melakukan analisa terhadap dampak serangan siber tersebut;

4. Hingga memberikan hadiah (reward) kepada rekan-rekan yang telah berpartisipasi di dalam pelaporan.

5. Terakhir, memberikan pelatihan teknis serta awareness terkait dengan keamanan informasi dan siber.

# BAB III

# PENUTUP

## Simpulan

1. Keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik.
2. Pengaruh keamanan informasi terhadap industri 4.0 adalah semakin canggih nya zaman semakin mudahnya para cyber hacker untuk menembus pertahanan data dari perusahaan. Dengan begitu kemanan informasi sangatlah penting dan harus di tingkatkan.
3. Cara menjaga data dengan keamanan informasi
4. 1. Menghubungkan para peneliti keamanan (bug hunter) dengan pihak perusahaan atau organisasi yang terkena dampak serangan siber;
5. 2. Mengelola laporan kerentanan yang telah masuk;
6. 3. Melakukan analisa terhadap dampak serangan siber tersebut;
7. 4. Hingga memberikan hadiah (reward) kepada rekan-rekan yang telah berpartisipasi di dalam pelaporan.
8. 5. Terakhir, memberikan pelatihan teknis serta awareness terkait dengan keamanan informasi dan siber.

# DAFTAR PUSTAKA

Nazar firman pratama (full time instructor inixindo bandung)