# Ancaman Keamanan pada Sistem Informasi Manajemen Rumah Sakit

Abdul Kohar[1], Hanson Prihantoro Putro[2]

Magister Informatika, Universitas Islam Indonesia
Jl. Kaliurang Km14 Yogyakarta 55584
Telp (0274) 895287 ext 122
sheilamnh@gmail.com[1], hanson@uii.ac.id[2]

***Abstract.*** Sistem informasi manajemen rumah sakit merupakan sistem yang kritis menyangkut kehidupan seseorang. Upaya perlu dilakukan agar sistem tersebut dapat tetap aman, terjaga dari berbagai ancaman yang dapat menganggu keberjalanan sistem. Penelitian ini bertujuan untuk mengetahui ancaman terhadap keamanan sistem informasi kesehatan, khususnya pada Sistem Informasi Manajemen Rumah Sakit. Penelitian ini menggunakan metode *review* dengan teknik melakukan *review* dan menganalisis beberapa makalah yang berkaitan dengan topik pembahasan tentang keamanan sistem informasi kesehatan. Hasil penelitian yang diperoleh adalah bahawa ancaman yang paling tinggi terhadap keamanan sistem informasi kesehatan adalah ancaman dari peretas.

**Keywords**: *review*, ancaman keamanan, sistem informasi kesehatan, manajemen rumah sakit

## 1. Pendahuluan

Saat ini, menggunakan sistem informasi dalam layanan kesehatan dapat memberikan banyak manfaat yang potensial seperti meningkatkan kualitas pelayanan, mengurangi kesalahan medis, meningkatkan pembacaan ketersediaan fasilitas dan aksesibilitas informasi. Namun demikian, ancaman terhadap keamanan Sistem Informasi Kesehatan juga meningkat secara signifikan. Sebagai contoh, selama periode 2006-2007, terdapat lebih dari 1,5 juta kesalahan data yang terjadi di rumah sakit[1]. Oleh karena itu, menyimpan informasi kesehatan dalam bentuk elektronik dapat menimbulkan kekhawatiran bagi pasien maupun manajemen rumah sakit.

Pada dasarnya, ancaman dan tindakan yang disengaja dapat sangat merusak sistem informasi kesehatan dan akibatnya dapat mencegah profesional untuk menggunakannya di kemudian hari[2]. Selain itu, kurangnya perlindungan yang memadai dalam menopang aspek kerahasiaan, integritas dan ketersediaan untuk investigasi juga menjadi ancaman, terutama di domain sistem informasi kesehatan.Hal ini memerlukan pengelolaan lebih dalam keamanan informasi serta perhatian khusus dari sektor publik dan swasta.

Penyelidikan lebih lanjut diperlukan untuk mengidentifikasi ancaman keamanan sistem informasi kesehatan adalah wajib. Diperlukan suatu praktik industri yang baik

atau standar dalam pengembangan sistem informasi. Untuk alasan ini, penelitian dilakukan dengan melakukan peninjauan terhadap beberapa makalah yang berkaitan dengan perhatian para pengembang terhadap ancaman keamanan sistem informasi manajemen rumah sakit

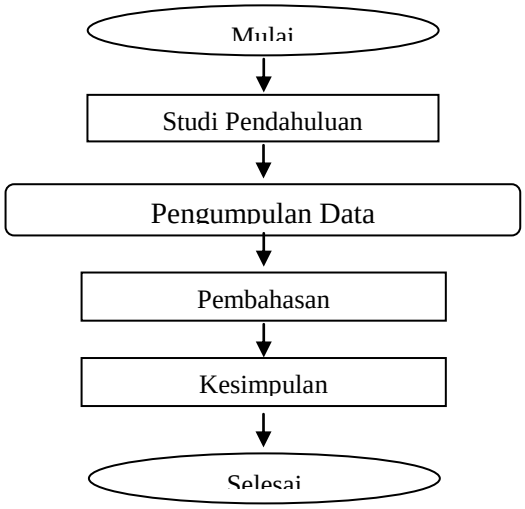
# 2. TINJAUAN PUSTAKA

Keamanan sistem informasi adalah segala betuk mekanisme yang harus dijalankan dalam sebuah sistem yang ditujukan agar sistem tersebut terhindar dari segala ancaman yang membahayakan keamanan data informasi dan keamanan pelaku sistem[3]. Ancaman mencakup berbagai jenis perilaku karyawan seperti keridaktahuan karyawan, kecerobohan, mengambil sandi karyawan lain dan memberikan *password* untuk karyawan lain. Untuk ancaman eksternal, yaitu virus dan serangan *spyware*, *hacker* dan penyusup di tempat. Selain itu, telah dikategorikan ancaman sistem informasi rumah sakit berdasarkan studi kasus dilakukan dengan menggunakan risiko yang dipilih dalam metode analisis.

Temuan menunjukkan bahwa yang ancaman yang paling potensial untuk sistem informasi rumah sakit adalah kegagalan daya server[2]. Selanjutnya, kegagalan daya dari *workstation* sistem dan kegagalan jaringan perangkat lunak dan perangkat lunak telemonitoring menjadi ancaman yang berisiko tinggi untuk sistem informasi rumah sakit. Kemudian, ancaman yang mungkin timbul dari kegiatan pengolahan informasi juga dapat berasal dari alam, yaitu: ancaman air, ancaman tanah, serta ancaman alam lain, seperti: kebakaran hutan, petir, tornado, angin ribut, dan lain sebagainya.

# 3. METODE PENELITIAN

Penelitian ini dilakukan dengan melakukan peninjauan (*review*) terhadap beberapa makalah yang memberikan perhatian pada ancaman keamanan sistem informasi manajemen rumah sakit. Selanjutnya setelah melakukan *review*, dilakukan pengelompokan mengenai apa saja yang menjadi ancaman bagi sistem informasi kesehatan. Terakhir, pembahasan dilakukan pada hasil pengelompokkan yang diperoleh. Adapun metodologi penelitian dibuat dalam beberapa langkah-langkah seperti pada Gambar 1.




**Gambar 1.** Alur metodologi penelitian

# 4. PEMBAHASAN

Dalam *review*, telah dipilih 7 makalah yang berasal dari berbagai sumber. Tabel 1 memperlihatkan beberapa makalah yang dijadikan bahan *review* dalam penelitian ini.

Tabel 1. Daftar makalah yang ditinjau

| No | Judul | Penulis |
|---|---|---|
| 1 | Analisa Database dan Keamanan Sistem Informasi SUP Fatmawati[4] | M. Fauzanul Hakim Abdurrahim |
| 2 | Kerangka Standar Keamanan Informasi: ISO17799[5] | Richardus Eko Indrajit |
| 3 | Peraturan Pemerintah Republik Indonesia Nomor 46 Tahun 2014 Tentang Sistem Informasi Kesehatan[6] | Pemerintah RI |
| 4 | Tantangan dan Etika Teknologi Informasi[7] | Ratri Purwaningtyas |
| 5 | Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik[8] | Kementerian Komunikasi dan Informatika RI |
| 6 | Threats to Health Information Security[9] | Ganthan Narayana Samy, Rabiah Ahmad. Dan Zuraini Ismail |
| 7 | An Integrated Approach in Risk Management Process for Identifying Information Security Threats using Medical Research Design[10] | Ganthan Narayana Samy, Rabiah Ahmad. Dan Zuraini Ismail |

Paper pertama mengidentifikasi adanaya ancaman terhadap keamanan sistem informasi kesehatan berupa, kelalaian pengguna (user), virus, *hacker* (peretas), serangan *spyware*, kegagalan daya server, kegagalan daya workstation system dan penyusupan/pencurian[4]. Kemudian makalah kedua mengidentifikasi adanaya ancaman terhadap keamanan sistem informasi kesehatan berupa *malicious code*, virus, *social engineering*, *hacker*, dan pencurian serta dipengaruhi juga oleh ancaman alam seperti ancaman air, ancaman tanah dan ancaman lain seperti kebakaran dan petir[5]. Selajutnya, materi ketiga mengidentifikasi adanaya ancaman terhadap keamanan sistem informasi kesehatan berupa, pencurian data, aktivitas spionase, *hacker*, dan tindakan vandalism serta dipengaruhi juga oleh ancaman alam seperti ancaman air, ancaman tanah dan ancaman lain seperti kebakaran, petir[6].

Di makalah keempat, penelitian mengidentifikasi adanaya ancaman terhadap keamanan sistem informasi kesehatan berupa *malicious code*, virus, *social engineering*, *hacker*, dan pencurian serta dipengaruhi juga oleh ancaman alam seperti ancaman air, ancaman tanah dan ancaman lain seperti kebakaran, petir[7]. Kemudian sumber kelima yang ditinjau, mengidentifikasi adanaya ancaman terhadap keamanan sistem informasi kesehatan berupa *malicious code*, virus, *social engineering*, *hacker*, dan pencurian serta dipengaruhi juga oleh ancaman alam seperti ancaman air, ancaman tanah dan ancaman lain seperti kebakaran, petir.

Selanjutnya, paper keenam mengidentifikasi adanaya ancaman terhadap keamanan sistem informasi kesehatan berupa *malicious code*, virus, *social engineering*, *hacker*, dan pencurian serta dipengaruhi juga oleh ancaman alam seperti ancaman air, ancaman tanah dan ancaman lain seperti kebakaran, petir[8]. Terakhir makalah ketujuh mengidentifikasi adanaya ancaman terhadap keamanan sistem informasi kesehatan berupa *malicious code*, virus, *social engineering*, *hacker*, dan pencurian serta dipengaruhi juga oleh ancaman alam seperti ancaman air, ancaman tanah dan ancaman lain seperti kebakaran, petir.

Tabel 2 memperlihatkan hasil pemetaan ancaman yang muncul sebagai perhatian pada makalah-makalah yang di*review*. Pengelompokkan dilakukan berdasarkan pengelompokkan yang dilakukan oleh salah satu makalah yang ada[6].

Berdasarkan hasil *review* dari berbagai makalah, ancaman yang sering terjadi berasal dari para peretas. Ancaman yang dilakukan para peretas terhadap sistem informasi dikarenakan sebuah sistem informasi bagi perusahaan atau individu digunakan untuk menyimpan data penting yang menyangkut privasi atau kerahasiaan perusahaan. Terlebih perusahaan yang menggunakan web, sangat rentan terhadap penyalahgunaan karena pada sebuah web dapat diakses oleh semua orang, Ancaman peretas menjadi sangat potensial saat tidak ada batas fisik dan kontrol yang dilakukan terpusat. Kemudian perkembangan jaringan yang amat cepat juga menjadi andil terhadap perbedaan ketrampilan pengamanan, di mana yang ahli akan mengancam yang kurang ahli. Selain itu, sikap dan pandangan pemakai yang kurang memberikan perhatian

terhadap sistem informasi tersebut membuat sistem dengan mudah mendapat serangan yang pada umumnya berasal dari pihak luar.

Tabel 2. Daftar ancaman yang disajikan di setiap makalah

| Kategori Ancaman | Makalah | | | | | | |
|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **1. Ancaman Manusia** | √ | | | | | | |
| a. Ketidaktahuan Karyawan | √ | | | | | | |
| b. Kecerobohan Karyawan | √ | | | | | | |
| c. Kegagalan Daya Server | √ | | | | | | |
| d. Malicious Code | | √ | | √ | √ | √ | √ |
| e. Virus | √ | √ | | √ | √ | √ | √ |
| f. Serangan *Spyware* | √ | | | | | | |
| g. *Hacker* | √ | √ | √ | √ | √ | √ | √ |
| h. Social Engineering | | √ | | √ | √ | √ | √ |
| i. Pencurian | √ | √ | | √ | √ | √ | √ |
| j. Pengkopian tanpa ijin | | | | | | | |
| k. Perang Informasi | | | | | | | |
| l. Pencurian Data | | | √ | | | | |
| m. Aktivitas Spionase | | | √ | | | | |
| n. Tindakan Vandalisme | | | √ | | | | |
| | | | | | | | |
| **2. Ancaman Alam** | | | | | | | |
| a. Ancaman air | | √ | √ | √ | √ | √ | √ |
| b. Ancaman Tanah | | √ | √ | √ | √ | √ | √ |
| c. Ancaman Angin | | √ | √ | √ | √ | √ | √ |
| d. Petir | | √ | √ | √ | √ | √ | √ |
| e. Kebakaran | | √ | √ | √ | √ | √ | √ |
| | | | | | | | |
| **3. Ancaman Lingkungan** | | | | | | | |
| a. Penurunan tegangan listrik | | √ | | √ | √ | √ | √ |
| b. Polusi | | √ | | √ | √ | √ | √ |
| c. Efek Bahan Kimia | | √ | | √ | √ | √ | √ |
| d. Kebocoran. dll | | √ | | √ | √ | √ | √ |

Untuk ancaman yang diakibatkan oleh alam adalah ancaman air, ancaman tanah, ancaman angin dan ancaman lain seperti petir dan kebakaran. Dikarenakan oleh terkadang tidak mempertimbangkan ancaman alam ini. Selain itu, ancaman virus komputer juga merupakan hasil karya seorang programmer yang punya niat jahat atau hanya untuk memuaskan nafsu programmingnya yang berhasil menyusupkan virus kedalam sistem komputer orang lain. Virus menyusup masuk ke dalam sistem komputer melalui berbagai cara, antara lain:

1. Pertukaran file, misalnya mengambil file (*copy-paste*) dari komputer lain yang telah tertular virus.

2. E-mail, membaca e-mail dari sumber yang tidak dikenal bisa berisiko tertular virus, karena virus telah ditambahkan (*attach*) ke file e-mail.
3. IRC, saluran *chatting* bisa dijadikan jalan bagi virus untuk masuk ke komputer.

Sedangkan resiko pencurian hanya sebagian kecil saja, dikarenakan setiap penyedia atau pengguna terkadang lebih mengutamakan dalam ancaman yang ini.

Dengan melihat beberapa aspek yang menjadi ancaman bagi keamanan sistem infomasi kesehatan yang disampaikan dalam makalah-makalah yang ditinjau, beberapa hal yang perlu diperhatikan oleh pengelola sitem informasi yaitu:

1. Melakukan perlindungan yang memadai dalam menopang aspek kerahasiaan, integritas dan ketersediaan untuk investigasi. Penyelidikan lebih lanjut untuk mengidentifikasi ancaman keamanan di kesehatan sistem informasi.
2. Melakukan perlindungan yang menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman
3. Melakukan analisis resiko keamanan untuk melindungi aset informasi menjamin keamanan sistem informasi.

# 5. KESIMPULAN

Secara umum penelitian ini telah sesuai dengan tujuan yang diharapkan yaitu, untuk mengetahui ancaman terhadap keamanan jaringan sistem informasi kesehatan. Adapun hasil dari berbagai *review* beberapa makalah, pembahasan dan analisa dapat disimpulkan bahwa ancaman yang paling tinggi terhadap keamanan sistem informasi kesehatan adalah ancaman dari *hacker*.

# Pustaka


1. HIMSS Analytics, Kroll Fraud Foundation (2008). HIMSS Analytics Report: Security of Patient Data. Chicago, IL : HIMSS Analytics.
2. Maglogiannis, Ilias. Elias Zafiropoulos (2006). "Modeling risk in distributed healthcare information systems", *The 28th Annual International Conference of the IEEE on Engineering in Medical and Biology Society (EMBS)*, IEEE.
3. ISO (2008). ISO 27799:2008 about Health Informatics – Information Security Management in Health using ISO/IEC 27002. Geneva : ISO.
4. Abdurrahim, M.F.H. (2011). Analisa Database dan Keamanan Sistem Informasi SUP Fatmawati. Bogor: IPB.
5. Indrajit, R.E. (2011). Kerangka Standar Keamanan Informasi: ISO17799. Jakarta : IDSIRTII.
6. Peraturan Pemerintah RI (2014). Sistem Informasi Kesehatan., Jakarta : Presiden Republik Indonesia.
7. Purwaningtyas, Ratri (2010). Tantangan dan Etika Teknologi Informasi. Depok : Universitas Gunadarma.

8. Kementerian Komunikasi dan Informatika RI (2011). Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Jakarta : Kementrian Komunikasi dan Informatika Republik Indonesia.
9. Samy, G.N., Rabiah Ahmad., Zuraini Ismail (2009). Threats to Health Information Security: *Fifth International Conference on Information Assurance and Security*. Malaysia : Universiti Teknologi Malaysia.
10. Samy, G.N., Rabiah Ahmad., Zuraini Ismail (2012). An Integrated Approach in Risk Management Process for Identifying Information Security Threats using Medical Research Design. Malaysia : Universiti Teknologi Malaysia.