J-ICON, Vol. 11 No. 1, Maret 2023, pp. 1~6
DOI: 10.35508/jicon.v11i1.9139

KEAMANAN INFORMASI (*INFORMATION SECURITY*) PADA APLIKASI SISTEM INFORMASI MANAJEMEN KEPEGAWAIAN DENGAN *DEFENSE IN DEPTH*

Enggar Novianto[1], Erik Iman Heri Ujianto[2] dan Rianto[3]

[1,2,3] Magister Teknologi Informasi, Universitas Teknologi Yogyakarta, Jl Siliwangi, Yogyakarta, Indonesia
[1] Email: 6220211003.enggar@student.uty.ac.id
[2] Email: erik.iman@uty.ac.id
[3]Email: rianto@staff.uty.ac.id

ABSTRAK

Pesatnya perkembangan Teknologi Informasi (TI) telah menjadikan TI sebagai aspek terpenting untuk memenuhi kebutuhan organisasi. Keberadaan TI diyakini mampu memberikan solusi terkait proses bisnis organisasi, sehingga banyak organisasi menawarkan sumber dayanya untuk meningkatkan efisiensi dengan mengandalkan dukungan teknologi informasi. Keamanan sistem informasi adalah subsistem organisasi internal yang bertugas mengelola risiko yang terkait dengan sistem informasi terkomputerisasi. Keamanan sistem informasi adalah penerapan prinsip pengendalian internasional, yang khusus digunakan untuk memacu masalah dalam sistem informasi. Informasi penting mengarah pada struktur informasi yang dilindungi, lebih banyak informasi sekarang tersedia dari internet, sehingga manajemen informasi sekarang mencakup teknologi komputer dan jaringan. Tujuan keamanan informasi adalah untuk memperkuat operasi bisnis dan melindungi dari jatuhnya harga bisnis dengan meminimalkan risiko yang terkait dengan keamanan internal. Tujuan dari penelitian ini adalah untuk memahami keamanan informasi dalam penerapan Sistem Informasi Manajemen Kepegawaian (SIMPEG) di Universitas Sebelas Maret. Metode penelitian yang digunakan adalah penerapan *Defense In Depth* untuk menganalisis keamanan informasi, termasuk banyak lapisan keamanan untuk menjamin keamanan informasi. Hasil analisis deskriptif menjelaskan bahwa perancangan dan pengembangan SIMPEG memperhatikan prinsip dan aspek keamanan data dan informasi. Namun, kerentanan keamanan informasi dapat terjadi pada lapisan perlindungan *server*, lapisan perlindungan jaringan, dan lapisan perlindungan fisik.
Kata Kunci : Keamanan informasi, SIMPEG, *defense in depth*, sistem informasi

ABSTRACT

The rapid development of Information Technology (IT) has made IT the most important aspect to meet organizational needs. The existence of IT is believed to be able to provide solutions related to the organization's business processes, so that many organizations offer their resources to increase efficiency by relying on information technology support. Information system security is an internal organizational subsystem tasked with managing the risks associated with computerized information systems. Information system security is the application of international control principles, which are specifically used to trigger problems in information systems. Important information leads to protected information structures, more information is now available from the internet, so information management now includes computer and network technology. The goal of information security is to strengthen business operations and protect against falling business prices by minimizing the risks associated with internal security. The purpose of this study is to understand information security in the implementation of the Personnel Management Information System (SIMPEG) at Sebelas Maret University. The research method used is the application of Defense In Depth to analyze information security, including many layers of security to ensure information security. The results of the descriptive analysis explain that the design and development of SIMPEG pays attention to the principles and aspects of data and information security. However, information security vulnerabilities can occur at the server protection layer, network protection layer, and physical protection layer.
Keywords : Information security, SIMPEG, defense in depth, information system

1. PENDAHULUAN

Pesatnya perkembangan TI telah menjadikan TI sebagai aspek terpenting untuk memenuhi kebutuhan organisasi. Keberadaan TI diyakini mampu memberikan solusi terkait proses bisnis organisasi, sehingga banyak organisasi menawarkan sumber dayanya untuk meningkatkan efisien dengan mengandalkan dukungan teknologi informasi. Keamanan data secara ketat ditujukan untuk mencegah

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)

kebocoran rahasia pengguna dan data penting perusahaan, sesuai dengan aspek tujuan keamanan data penting organisasi, data kerahasiaan, integritas dan ketersediaan [1].

Perkembangan teknologi sudah sangat pesat, terutama pada internet yang dapat digunakan untuk komunikasi. Tidak hanya dapat digunakan pada perangkat besar seperti komputer atau laptop yang terhubung ke jaringan, tetapi bagian dari komunikasi tersebut kini dapat diakses oleh perangkat yang lebih ringkas, khususnya ponsel [2]. Kemajuan TI yang sangat pesat menjadikan TI sebagai aspek terpenting dalam pemenuhan kebutuhan organisasi. Pentignya TI dalam melakukan proses-proses bisnis tidak dapat terlepas dari aspek keamanaan informasi. Keamanan informasi mutlak diperhatikan untuk menghindari terjadinya kebocoran-kebocoran rahasia pengguna dan informasi penting sesuai aspek keamanan informasi [1]. Beberapa kejahatan dunia maya, termasuk kejahatan yang dilakukan oleh aktor jahat melalui jejaring sosial dan internet, serta di dunia maya yaitu *cybercrime* dapat membahayakan keamanan nasional sampai batas tertentu [3].

Sistem organisasi internal bertanggung jawab untuk mengidentifikasi risiko yang terkait dengan sistem informasi terkomputerisasi. Keamanan sistem informasi adalah penerapan prinsip pengendalian internasional, yang khusus digunakan untuk memacu masalah dalam sistem informasi. Perlindungan sistem informasi umumnya dikenal sebagai kontrol dan keamanan sistem informasi, didefinisikan sebagai perlindungan perangkat keras komputer dan proses dari instruksi yang disengaja atau tidak disengaja yang dapat menyebabkan modifikasi yang tidak sah, serta menghancurkan atau mencuri sumber daya sistem informasi [4]. Pengetahuan tentang kerentanan saja tidak membantu manajemen meningkatkan keamanan dari aplikasi. Melakukan penilaian risiko aplikasi, dengan mempertimbangkan berbagai faktor yang terkait dengan aplikasi, memberikan lebih banyak edukasi dan bertujuan untuk membuat aplikasi lebih aman [5].

Pentingnya data dalam perusahaan perlu dijaga dan dilindungi dari ancaman apapun. Ancaman dapat datang dari dalam organisasi, seperti kurangnya penilaian berkala terhadap sistem operasional atau tindakan pegawai yang tidak sesuai dengan aturan organisasi. Ancaman eksternal dapat berupa serangan sistem yang ditujukan untuk mengganggu operasi yang sedang berlangsung atau tindakan sabotase lainnya [6]. Informasi penting mengarah ke struktur untuk informasi yang dilindungi. Saat ini, informasi yang tersedia secara *online* semakin meningkat, yang mengarah pada kemajuan teknologi komputer dan jaringan serta informasi dan komunikasi. Tujuan keamanan informasi adalah untuk memperkuat operasi bisnis dan melindungi informasi keuangan dengan mengurangi risiko ancaman orang dalam [7].

Berdasarkan uraian di atas, maka tujuan dari penelitian ini adalah untuk mengetahui penerapan keamanan informasi pada pada penerapan Sistem Informasi Manajemen Kepegawaian (SIMPEG) di Universitas Sebelas Maret. Metode penelitian yang digunakan adalah penerapan model pertahanan mendalam untuk menganalisis keamanan informasi, termasuk banyak lapisan keamanan untuk menjamin keamanan informasi.

2. MATERI DAN METODE

Keamanan Informasi

Keamanan informasi adalah upaya untuk melindungi informasi sensitif terhadap ancaman yang berpotensi merugikan. Akibatnya semakin banyak informasi bisnis yang disebarluaskan, dikumpulkan, dan disimpan, risiko kehilangan, pencurian, atau penyalahgunaan data meningkat [8].

Tinjauan Keamanan Informasi

Menurut [7] penilaian keamanan informasi dijelaskan sebagai berikut:

1. Pengamanan fisik, berfokus pada strategi untuk melindungi barang-barang fisik seperti aset fisik pemerintah atau organisasi, pegawai, pekerja dan tempat kerja dari ancaman bencana, bencana alam atau akses yang tidak sah.
2. Keamanan pribadi, terkait dengan keamanan fisik saat berinteraksi dengan organisasi dan orang, baik itu pemerintah maupun swasta.
3. Keamanan operasional, dengan fokus pada strategi operasional yang menjamin keamanan organisasi pemerintah atau swasta tanpa gangguan.
4. Keamanan komunikasi, mengamankan media teknologi komunikasi dan penggunaan peralatan teknologi komunikasi untuk mencapai tujuan organisasi.
5. Keamanan jaringan, yang menyangkut keamanan sumber data organisasi, jaringan dan isinya, dan kemampuan untuk menggunakan jaringan dan data untuk mengirimkan data dalam organisasi.

Aspek Keamanan Informasi

Menurut [9] aspek keamanan informasi harus dikontrol untuk melindungi informasi yang terkait dengan keamanan informasi, yaitu:

1. Kerahasiaan. Keamanan informasi dengan memastikan bahwa hanya individu yang berwenang yang dapat mengakses informasi dan informasi tersebut dijaga keamanannya.

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)

2. Integritas. Pemeriksaan untuk memastikan bahwa data tidak dibuang tanpa persetujuan dari pemilik setempat, otoritas, serta integritas data terjaga, dan metode pemrosesan untuk memastikan integritas tersebut.
3. Ketersediaan. Pastikan informasi tersedia saat dibutuhkan dan pengguna yang berwenang dapat mengakses informasi yang dibutuhkan.

Sistem Manajemen Informasi

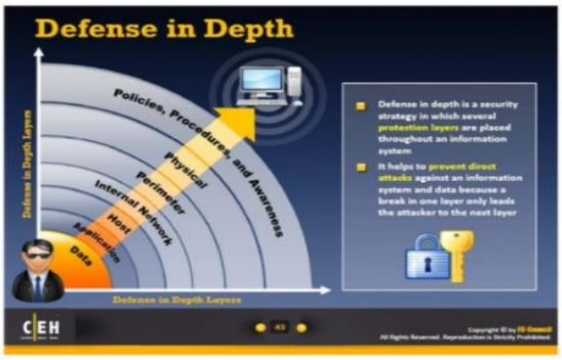
Untuk memastikan keamanan TI dan sistem komunikasi, organisasi harus menerapkan sistem manajemen informasi. Manajemen informasi untuk mengelola informasi sensitif terpisah dari prosedur kerja untuk menangani informasi sensitif dalam organisasi. Sistem manajemen informasi juga harus mengikuti standar nasional atau internasional yang berlaku sehingga kualitas keamanan yang diberikan tinggi dan masalah dapat diselesaikan [8].

Sistem Informasi

Sistem informasi dapat digunakan dalam berbagai proses organisasi, termasuk pengumpulan informasi, penyebaran, dan manajemen, untuk membantu organisasi mencapai tujuannya. Keamanan sistem informasi dapat digambarkan sebagai sistem operasional yang terdiri atas segala macam mekanisme yang tujuannya adalah untuk mencegah sistem dari berbagai ancaman yang berdampak buruk terhadap keamanan informasi dan keamanan sistem [3].

Defense In Depth

Defense In Depth adalah konsep keamanan dalam teknologi informasi yang mencakup beberapa tingkat lapisan untuk menjamin keamanan informasi. Gagasan di balik pendekatan *Defense In Depth* adalah menggunakan beberapa metode independen untuk melindungi sistem dari serangan tertentu. Tujuannya adalah untuk meningkatkan biaya dan upaya untuk menyerang sistem TI organisasi dengan mengidentifikasi serangan, merespon serangan, dan menyediakan lapisan perlindungan [10]. Pada metode *Defense In Depth* menggambarkan lapisan-lapisan dengan urutan lapisan terdalam sampai lapisan terluar dimulai dari lapisan perindungan data sampai lapisan kebijakan, prosedur dan kesadaran yang dapat dilihat pada gambar 1.



Gambar 1. *Defense in Depth* [10].

1. Lapisan 1: Perlindungan Data
   Data adalah penjumlahan daya termahal di banyak bisnis. Setiap kali data tidak akurat atau tidak tersedia, maka hal itu dapat mempengaruhi kinerja organisasi. Data dapat dilindungi dengan *file* dan daftar akses direktori (ACL), enkripsi, dan kebijakan pencadangan.
2. Lapisan 2: Perlindungan Aplikasi
   Lapisan keamanan aplikasi mengontrol akses ke informasi rahasia seperti *server web*, situs *web* perdagangan elektronik, dan layanan suara. Melalui otentifikasi, otorisasi, dan kebijakan kata sandi, sebuah aplikasi dapat dianalisis.
3. Lapisan 3: Perlindungan *Server*
   Komputer yang meluncurkan klien dan *server* dikenal sebagai *host*.
4. Lapisan 4: Perlindungan Jaringan
   Segmen jaringan terdiri dari dua atau lebih perangkat yang berkomunikasi melalui kantong fisik yang sama. Jaringan area lokal virtual dijelaskan dalam segmen kalimat (VLAN). Saat menggunakan domain, tidak ada hak administratif lokal yang diberikan untuk mencegah instalasi atau penghapusan program yang tidak dimaksudkan.
5. Lapisan 5: Pertahanan Perimeter
   Koneksi antara jaringan internal dan eksternal untuk menyediakan lapisan keamanan tambahan. Setiap layanan yang ditawarkan kepada pengguna sistem jaringan eksternal dapat ditemukan di sistem jaringan yang mendasarinya.

6. Lapisan 6: Perlindungan Fisik
   Sambungan fisik ke komputer memungkinkan data dienkripsi dengan kata sandi. *Server* dikelola dalam lingkunganaman yang hanya dapat diakes oleh pergawai tertentu.
7. Lapisan 7: Kebijakan, Prosedur dan Kesadaran
   Aturan mendasar untuk mengembangkan strategi manajemen untuk semua jenis organisasi. Prosedur dan laporan keamanan tertulis dengan jelas.

Metode Pengumpulan data

1. Observasi, berlangsung dalam bentuk pengamatan langsung pada lokasi objek kajian dan mengumpulkan informasi dan data sebanyak-banyaknya tentang masalah yang diteliti.
2. Kajian literatur ini dilakukan dengan mencari beberapa sumber keilmuan yang meliputi ulasan atau dokumen yang berkaitan dengan pokok bahasan yang diteliti. Oleh karena itu, informasi yang diperoleh dari kajian pustaka ini menjadi acuan untuk membuat tulisan ini.

3. HASIL DAN PEMBAHASAN

Hasil analisis keamanan informasi dengan metode *Defense In Depth* sebagai bagian dari implementasi dari sistem SIMPEG di Universitas Sebelas Maret yaitu:

1. Lapisan 1: Perlindungan Data
   Keamanan data dalam SIMPEG dipastikan dengan memberikan kontrol akses dimana pengguna diberikan izin tertentu untuk mengakses sistem atau informasi. Administrator SIMPEG mengamankan informasi dengan menetapkan hak akses terhadap informasi yang dapat diakses oleh operator dan non operator. Operator diberikan akses untuk memperbarui, mengunggah dan mengubah data pada SIMPEG dan harus mendapatkan persetujuan dari operator lain di setiap unit kerja, sedangkan pengguna yang non operator hanya dapat mengakses informasi dan data, tetapi tidak dapat memperbarui dan menggunggah dokumen ke SIMPEG. Data dan informasi SIMPEG hanya dapat diakses secara internal oleh seluruh pegawai Universitas yaitu Tenaga Pendidik dan Tenaga Kependidikan. Data yang dikelola oleh SIMPEG meliputi data kepegawaian meliputi kepangkatan, jabatan fungsional, jabatan struktural, pendidikan, pelatihan, SKP, dan data lainnya. Pengguna SIMPEG dibedakan menjadi:
   a. Pimpinan Universitas (Rektor, Wakil Rektor, Kepala Biro, Dekan, Wakil Dekan, Koordinator Bagian Tata Usaha) dapat melihat data tentang semua staf serta rekapitulasi data untuk pengambilan keputusan.
   b. Pengguna biasa, yaitu seluruh staf tenaga pendidik dan tenaga kependidikan dimana dapat melihat data pribadi masing-masing sekaligus dapat mengirimkan koreksi kepada operator SIMPEG apabila terjadi kesalahan data. Pengguna biasa juga dapat mengunduh file kepegawaian secara *online* yang sebelumnya sudah diunggah oleh operator SIMPEG.
2. Lapisan 2: Perlindungan Aplikasi
   Pada level perlindungan aplikasi, aplikasi SIMPEG terjamin dan terlindungi karena pegawai harus membuat akun terlebih dahulu sebelum dapat masuk ke dalam aplikasi SIMPEG dengan cara mengaktifkan menggunakan SSO (*single sign on*) dan memasukkan kode verifikasi google yang tersedia pada form aktivasi. Pengamanan informasi aplikasi SIMPEG umumnya menggunakan langkah-langkah pengamanan sesuai standar. Pengguna internal yang tidak memiliki NIP/NIK tidak dapat mengakses aplikasi SIMPEG.
3. Lapisan 3: Perlindungan *Server*
   Sistem yang awalanya terdiri dari 1 *server* dengan database terpusat, sekarang dikembangkan menjadi 2 *server* yang mana 1 *server* dipergunakan sebagai *database server* dan FTP *server* (menggunakan OS Ubuntu, DB MySQL, ProFTPD) sedangkan *server* yang lain kami persiapkan untuk web service server untuk menangani kebutuhan sistem eksternal (OS CentOS, DB MySQL, *Apache Web Server*).
4. Lapisan 4: Perlindungan Jaringan
   Jalur komunikasi yang digunakan dalam SIMPEG menggunakan keamanan jaringan berbasis Linux dan NOC (*Network Operation Center*), sehingga penelurusan gangguan dan keamanan jaringan menjadi lebih mudah karena NOC diawasi bersama oleh admin NOC, admin UPT TIK maupun pengelola. Proses pengamanan jaringan jaringan masih dapat menyebabkan celah kebocoran keamanan sistem informasi. Proses pengaman jaringan yang digunakan pada SIMPEG terbatas pada penggunaan yang membuat lemahnya pengamanan fisik jaringan menimbulkan kerentanan keamanan informasi.

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)

5. Lapisan 5: Perlindungan Perimeter
   Implementasi keamanan perimeter diimplementasikan menggunakan *router* mikrotik, tetapi terbatas pada konfirgurasi standar saja, seperti mengubah kata sandi dan tidak ada upaya yang dilakukan untuk mengoptimalkan penggunaan *server proxy* untuk perlindungan perimeter.
6. Lapisan 6: Perlindungan Fisik
   Upaya untuk membatasi akses fisik ke *server* adalah dengan menempatkannya di ruangan khusus dan akses terbatas untuk sistem administrator dan *server* administrator. *Server* berada di UPT TIK yang aman, tidak banjir, ruangan ber-AC dan di jaga oleh satpam di depan Gedung UPT TIK.
7. Lapisan 7: Kebijakan, Prosedur dan Kesadaran
   Sumber daya manusia lemah dalam mengoptimalkan keamanan informasi. Upaya yang dilakukan untuk mengoptimalkan keamanan informasi, misalnya dalam kaitannya dengan sumber daya manusia yaitu dengan memberlakukan peraturan pimpinan universitas, serta memberikan pelatihan antara lain pelatihan *web service*, peningkatan keamanan, keamanan jaringan dan kemanan *database*.

4. KESIMPULAN DAN SARAN

Kesimpulan

Untuk menjaga kerahasiaan informasi, pada implementasi SIMPEG menerapkan hak akses terbatas sesuai dengan hak dan kewenangan masing-masing pegawai. Prosedur pengamanan akun SIMPEG milik masing-masing pegawai dilakukan dengan cara menggunakan kata sandi dari masing-masing pegawai yang sudah diaktivasi melalui SSO (*single sign on*) dan dapat diganti secara berkala pada masing-masing akun pengguna untuk mencegah terjadinya celah kemanan informasi dari akun pengguna biasa dan operator. Terdapat kerentanan *Information Security* yang berada pada lapisan perlindungan *server*, perlindungan jaringan dan lapisan perlindungan fisik, sedangkan lapisan yang sudah aman berada pada lapisan perlindungan data, aplikasi, perimeter, serta kebijakan, prosedur dan kesadaran.

Saran

Meningkatkan perlindungan *server*, perlindungan jaringan, dan lapisan perlindungan fisik dengan memberikan kebijakan dan prosedur serta pelatihan terkait dengan mengelola *server* dan jaringan kepada pengelola atau pegawai yang bertugas serta meningkatkan pengamanan fisik dengan memberikan autentikasi atau *password* yang tidak mudah diketahui oleh pihak yang tidak berwenang.

DAFTAR PUSTAKA

[1] L. M. M. Matin, A. Arini, and L. K. Wardhani, "Analisis Keamanan Informasi Data Center Menggunakan COBIT 5," *Jurnal Teknik Informatika,* vol. 10, no. 2, pp. 119-128, 2017, doi : https://doi.org/10.15408/jti.v10i2.7026.

[2] M. Hayati, and D. Fata, "Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising," *Djtechno : Journal of Information Technology Research,* vol. 2, no. 1, pp. 21-28, 2021, doi : https://doi.org/10.46576/djtechno.v2i1.1252.

[3] I. A. Dianta, and E. Zusrony, "Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking," *INTENSIF : Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 3, no. 1, pp. 1-9, 2019, doi : https://doi.org/10.29407/intensif.v3i1.12125.

[4] E. M. Safitri, A. S. Larasati, and S. R. Hari, "Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0 : Studi Literatur," *JIFTI - Jurnal Ilmiah Teknologi Informasi dan Robotika,* vol. 2, no. 1, pp. 12-16, 2020, doi : https://doi.org/10.33005/jifti.v2i1.25.

[5] A. Elanda, and R. L. Buana, "Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security Project (OWASP) Versi 4 : Systematic Review," *CSS (Journal of Computer Engineering System and Science),* vol. 5, no. 2, pp. 185-191, 2020, doi : https://doi.org/10.24114/cess.v5i2.17149.

[6] Zulkarnain, "Analisis Implementasi Keamanan Sistem Informasi Pada Perusahaan Perakitan Elektronik," *Journal of Information System and Technology*, vol. 1, no. 1, pp. 1-4, 2020 .

[7] A. P. Galih, "Keamanan Informasi (Information Security) Pada Aplikasi Perpustaakn iPUSNAS," *Al Maktabah Jurnal Kajian Ilmu dan Perpustakaan,* vol. 5, no. 1, pp. 9-17, 2020, doi : http://dx.doi.org/10.29300/mkt.v5i1.3086.

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)

[8] T. E. Wijatmoko, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Kementerian Hukum Dan HAM DIY," *CyberSecurity dan Forensik Digital*, vol. 3, no. 1, pp. 1-6, 2020, doi : https://doi.org/10.14421/csecurity.2020.3.1.1951.

[9] M. B. Yel, and M. K. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *Jurnal Informatika Kaputama (JIK)*, vol. 6, no. 1, pp. 92-101, 2022, doi : https://doi.org/10.1234/jik.v6i1.768.

[10] F. Novianto, "Evaluasi Keamanan Informasi E-Government Menggunakan Model Defense In Depth," *CyberSecurity dan Forensik Digital*, vol. 3, no. 1, pp. 14-19, 2020, doi : https://doi.org/10.14421/csecurity.2020.3.1.1962.

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)