E-ISSN : 3025-1311
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 01, No. 12 2023, pp.21-30

PERANAN SISTEM DAN TEKNOLOGI INFORMASI PADA PROSES BISNIS INFORMASI (Keamanan Informasi Dalam Era Digital, Tantangan Dan Solusi Untuk Bisnis Organisasi)

Dewi Lestari,Muhammad Irwan Padli Nasution
Universitas Islam Negeri Sumatra Utara
E-mail: dewilestari020304@gmail.com,irwannst @uinsu.ac.id

ABSTRAC

In this paper, we investigate various aspects surrounding information security in the context of the digital era, and we also review the challenges faced along with relevant solutions for various business organizations. Amid the continuous development of the digital era, information systems have become a key element in carrying out business operations, communicating personally, and various aspects of daily life. Although information technology brings extraordinary changes, this rapid growth also brings serious problems related to security. Data protection concerns have the potential to have a major impact on companies, individuals and society in general. This article aims to understand how information security in the digital era is able to face current developments, especially in the realm of technology.
Keywords: *Technology, Information and Contemporary Development*

ABSTRAK

Dalam tulisan ini, kami menyelidiki berbagai aspek seputar keamanan informasi dalam konteks era digital, dan kami juga mengulas tantangan yang dihadapi bersama dengan solusi yang relevan bagi berbagai organisasi bisnis. Di tengah perkembangan terus-menerus dari era digital, sistem informasi telah menjadi elemen kunci dalam menjalankan operasi bisnis, berkomunikasi secara pribadi, dan berbagai aspek kehidupan sehari-hari. Meskipun teknologi informasi membawa perubahan luar biasa, pertumbuhan pesat ini juga membawa permasalahan serius terkait dengan keamanan. Kekhawatiran terhadap perlindungan data memiliki potensi dampak besar bagi perusahaan, individu, dan masyarakat secara umum. Tulisan ini bertujuan untuk memahami bagaimana keamanan informasi di era digital mampu menghadapi perkembangan zaman, terutama dalam ranah teknologi.
Kata Kunci: Teknologi, Informasi Dan Perkembangan Zaman

PENDAHULUAN

Kemajuan teknologi terus berlangsung dengan cepat. Di era digital saat ini, masyarakat secara luas telah mengadopsi gaya hidup yang sangat bergantung pada perangkat elektronik. Teknologi telah menjadi alat yang sangat penting dalam memenuhi berbagai kebutuhan manusia dan mendukung berbagai tugas dan pekerjaan. Perkembangan teknologi yang signifikan telah mengantarkan peradaban manusia ke dalam era digital. Era digital dimulai seiring dengan kemunculan internet digital, terutama dalam konteks teknologi informasi komputer. Media baru dalam era digital dicirikan oleh kemampuan untuk dikelola, terutama melalui jaringan atau Internet. Media massa telah beralih ke media baru atau internet sebagai respons terhadap perubahan budaya dalam penyampaian informasi. Teknologi digital memungkinkan masyarakat untuk menerima informasi dengan lebih cepat.Kemajuan teknologi digital saat ini telah membawa perubahan besar di seluruh dunia dan menghasilkan berbagai jenis teknologi digital yang semakin canggih. Ini telah memberikan kemudahan akses informasi dan fasilitas teknologi digital kepada berbagai kalangan. Namun, era digital juga menimbulkan ancaman terhadap privasi manusia. Data pribadi yang ada dalam komputer dapat memudahkan pelacakan aktivitas pengguna di internet, baik dalam hal kebiasaan penelusuran maupun aktivitas hiburan.

Menjaga keamanan informasi menjadi esensial bagi setiap organisasi. Kalangan industri telah lama menyadari perlunya perlindungan terhadap ancaman kriminal komputer, dan saat ini, pemerintah juga meningkatkan upaya keamanan sebagai bagian dari strategi melawan terorisme. Namun, ada sejumlah isu kunci yang harus diatasi dalam konteks keamanan, seperti menemukan keseimbangan antara keamanan dan ketersediaan serta menjaga hak pribadi. Sasaran utama dari usaha keamanan informasi adalah memastikan kerahasiaan, ketersediaan, dan integritas semua sumber daya informasi yang dimiliki oleh perusahaan. Manajemen keamanan informasi mencakup praktik-proaktif perlindungan yang sering disebut sebagai manajemen keamanan informasi,dan perencanaan operasional dalam menghadapi situasi darurat yang dikenal sebagai manajemen kontinuitas bisnis.

Meskipun sistem keamanan informasi sering kali dibangun oleh para analis dan programmer, pengguna akhir sering kali meninggalkannya. Hal ini disebabkan oleh sistem yang cenderung difokuskan pada pembuatnya, sehingga pengguna akhir mengalami kesulitan dalam penggunaan yang efisien. Sistem juga mungkin kurang interaktif dan tidak memberikan kenyamanan bagi pengguna, Dalam situasi tertentu, sistem tersebut memiliki antarmuka yang sulit dimengerti dengan menu dan tata letak yang tidak selalu memperhatikan kebiasaan pengguna. Sistem terkadang memaksa pengguna untuk mengikuti prosedur baku, sehingga terasa kaku dan kurang fleksibel. Selain itu, keamanan sistem informasi yang dibangun juga tidak selalu dapat menjamin tingkat keamanan yang memadai.

Adapun tujuan saya memilih judul ini supaya bisa mengetahui keamanan informasi di era serba digital dapat menghadapi dan mampu mengikuti perkembangan zaman saat ini terutama dalam bidang teknologi. Semoga kedepannya perkembangan teknologi ini mampu membawa kemajuan yang besar bagi kita tanpa ada ancaman dari teknologi tersebut.

KAJIAN TEORI

Kemajuan teknologi terus bergerak dengan cepat. Di era digital saat ini, perangkat elektronik telah menjadi bagian yang tak terpisahkan dari kehidupan sehari-hari masyarakat. Teknologi memainkan peran sentral yang sangat penting dalam memenuhi berbagai kebutuhan manusia dan mendukung beragam tugas serta pekerjaan. Peran utama teknologi telah membawa peradaban manusia masuk ke dalam era digital, yang membawa sejumlah perubahan positif dan dampak menguntungkan yang dapat dieksplorasi sepenuhnya. Meskipun begitu, era digital juga membawa dampak negatif yang membawa tantangan baru bagi kehidupan manusia saat ini. Tantangan-tantangan dalam era digital memiliki dampak yang signifikan pada berbagai bidang, termasuk politik, ekonomi, budaya, masyarakat, pertahanan, keamanan, dan teknologi informasi nasional.

Di era digital yang terus berkembang pesat saat ini, sistem informasi telah menjadi elemen kunci dalam operasi bisnis, komunikasi pribadi, dan berbagai aspek kehidupan sehari-hari. Meskipun teknologi informasi telah membawa kemajuan yang sangat besar, pertumbuhan yang cepat ini juga membawa dampak serius dalam hal masalah keamanan. Tantangan menjaga keamanan data berpotensi menyebabkan kerugian besar bagi perusahaan, individu, dan masyarakat secara keseluruhan. Dalam konteks ini, kita akan menjelajahi isu-isu utama yang dihadapi dalam menjaga keamanan informasi selama era digitalisasi dan mengidentifikasi solusi terkini yang dapat digunakan untuk melindungi kerangka informasi dari berbagai ancaman.. Dalam konteks ini, berbagai tantangan keamanan informasi telah muncul dalam era digital ini Antara lain:

1) Tantangan Dalam Keamanan *Cybe*r

Perkembangan Teknologi: Perkembangan teknologi yang pesat memberikan tantangan baru dalam keamanan cyber. Semakin banyak perangkat yang terhubung ke internet, semakin banyak juga potensi celah keamanan yang bisa dieksploitasi oleh para penyerang. Selain itu, teknologi seperti kecerdasan buatan dan komputasi awan juga dapat digunakan oleh penyerang untuk melakukan serangan yang lebih canggih dan kompleks.

Serangan Berasal dari Berbagai Pihak: Serangan *cyber* tidak hanya dilakukan oleh individu atau kelompok tertentu, tetapi juga oleh negara-negara atau kelompok terorganisir. Serangan ini bisa berupa pencurian data, sabotase, atau bahkan serangan siber yang berpotensi menghancurkan infrastruktur kritis suatu negara. Tingkat

serangan yang semakin tinggi dan beragam meningkatkan kompleksitas dalam melindungi sistem dan data.

Kekurangan Tenaga Ahli Keamanan *Cyber*: Kekurangan tenaga ahli dalam bidang keamanan cyber menjadi masalah serius. Permintaan akan tenaga ahli keamanan *cyber* yang berkualitas melebihi pasokan. Hal ini menimbulkan celah dalam perlindungan dan menghambat kemampuan organisasi untuk merespons dan mencegah serangan cyber.

Sosial Teknik Serangan: Penyerang sering menggunakan teknik sosial dalam serangan mereka. Mereka memanfaatkan ketidaktahuan, kecerobohan, atau kecerdasan emosional sasaran untuk mendapatkan akses tidak sah atau informasi sensitif. Serangan phishing, spear phishing, atau social engineering menjadi metode populer yang digunakan oleh penyerang.

Kelemahan Sistem dan Aplikasi: Kelemahan dalam sistem operasi, perangkat lunak, atau aplikasi merupakan celah yang sering dimanfaatkan oleh penyerang. Kerentanan keamanan yang belum terdeteksi atau perangkat lunak yang tidak diperbarui secara teratur dapat menjadi titik masuk bagi serangan *cyber*.

Keberlanjutan Ancaman: Ancaman dalam keamanan cyber tidak pernah berhenti. Penyerang terus mengembangkan teknik dan metode baru untuk menghindari deteksi dan mengatasi upaya perlindungan. Ancaman yang berkembang dan berubah secara dinamis menuntut respons yang cepat dan adaptif dalam menjaga keamanan sistem dan data.

Adapun Solusi dalam Keamanan *Cyber* Antara lain:

- Kesadaran dan Pendidikan Pengguna
  Kesadaran akan ancaman keamanan cyber dan pendidikan pengguna tentang praktik keamanan yang baik sangat penting. Pengguna harus diberikan informasi dan pelatihan tentang penggunaan yang aman dari perangkat dan layanan digital, serta cara mengenali dan melaporkan serangan cyber
- Pemantauan dan Deteksi yang Kuat
  Teknologi pemantauan dan deteksi yang kuat harus digunakan untuk mendeteksi serangan cyber dengan cepat. Pemantauan lalu lintas jaringan, aktivitas pengguna, dan log sistem dapat membantu mengidentifikasi serangan secara dini dan mengambil tindakan yang tepat.
- Enkripsi dan Keamanan Data
  Data yang disimpan dan diproses harus dienkripsi dengan metode yang kuat. Enkripsi yang tepat pada tingkat file, jaringan, dan aplikasi dapat melindungi data dari akses yang tidak sah. Selain itu, praktik keamanan data seperti cadangan reguler dan pemulihan juga penting untuk melindungi data dari hilang atau kerusakan.
- Pembaruan dan Pemeliharaan Perangkat Lunak
  Memastikan sistem dan perangkat lunak selalu diperbarui dengan patch keamanan terbaru sangat penting. Pembaruan perangkat lunak rutin dan pemeliharaan yang baik dapat mengurangi risiko penyerangan yang memanfaatkan kelemahan yang diketahui.

- Kolaborasi dan Kerjasama

  Kerjasama antara organisasi, pemerintah, dan lembaga keamanan cyber adalah kunci dalam melawan serangan cyber. Berbagi informasi tentang ancaman dan serangan yang terdeteksi, serta mengembangkan praktik keamanan yang bersama-sama, dapat membantu memperkuat pertahanan dan respons terhadap serangan cyber.

  Tantangan dalam keamanan cyber terus berkembang seiring dengan perkembangan teknologi. Para penyerang terus mencari celah baru dan metode yang lebih canggih untuk melancarkan serangan. Oleh karena itu, penting untuk terus mengembangkan solusi keamanan cyber yang efektif.

  1) Internet of Things (IoT)

  Perkembangan Internet of Things (IoT) telah memperkenalkan berbagai perangkat terhubung yang meresap ke dalam berbagai aspek kehidupan sehari-hari. Namun, kemajuan teknologi ini juga telah menggarisbawahi masalah kerentanan dalam konteks IoT. Keamanan yang lemah pada perangkat IoT dapat membuka peluang bagi akses yang tidak sah ke jaringan dan data pribadi.

  2) Risiko Komputasi Awan

  Tren penyimpanan data dan pelaksanaan komputasi di lingkungan awan semakin umum, namun hal ini juga membawa potensi kerentanan. Perusahaan harus memastikan bahwa penyedia layanan awan mereka memiliki mekanisme keamanan yang kuat.

  3) Ancaman Internal

  Ancaman yang berasal dari dalam organisasi, seperti perilaku tidak jujur atau kelalaian dari karyawan., dapat Ini merupakan sebuah tantangan besar bagi organisasi, terutama dalam hal potensi kebocoran data atau pelanggaran terhadap kebijakan keamanan.

  4) Kebijakan Privasi yang Ketat dan Regulasi

  Dengan munculnya regulasi privasi yang semakin ketat, seperti GDPR di Uni Eropa, organisasi harus terus memastikan bahwa mereka selalu mematuhi peraturan tersebut, atau menghadapi konsekuensi serius berupa sanksi.

METODE PENELITIAN

a) Dalam rangka penelitian ini, metode kualitatif diterapkan dengan tujuan untuk menghimpun data deskriptif, termasuk data yang diperoleh melalui wawancara dan dari berbagai sumber tertulis.
b) Teknik Pengumpulan Data

Dalam pengumpulan data Keamanan Informasi Dalam Era Digital, Tantangan Dan Solusi Untuk Bisnis Organisasi), dari hasil wawancara, observasi dan dokumentasi.

HASIL DAN PEMBAHASAN

A. Kebutuhan Organisasi akan Keamanan dan Pengendalian

Di zaman yang modern ini, semakin banyak organisasi menyadari betapa pentingnya menjaga keamanan semua aset mereka, baik yang berbasis virtual maupun fisik, terhadap berbagai ancaman, baik yang berasal dari internal maupun eksternal. Ketika

awal munculnya sistem komputer, perlindungan keamanannya masih sangat minim. Namun, situasinya berubah saat perang Vietnam, di mana beberapa instalasi komputer mengalami serangan dari pihak yang mencoba merusaknya. Pengalaman tersebut mendorong industri untuk memberikan prioritas yang lebih tinggi pada upaya keamanan yang bertujuan untuk mengurangi risiko kerusakan atau penghancuran, sambil memungkinkan organisasi untuk tetap menjalankan operasional mereka setelah mengalami gangguan.Pendekatan-pendekatan ini, yang pertama kali muncul di sektor industri, kemudian menjadi contoh dan diterapkan secara lebih luas. Ketika prinsip-prinsip perlindungan keamanan ini diadopsi dalam kerangka federal, dua isu utama yang perlu diperhatikan adalah seimbangnya antara keamanan dan hak-hak individu serta antara keamanan dan ketersediaan.

B.Ancaman Terhadap Keamanan Informasi

Ancaman terhadap keamanan informasi merujuk pada individu, Ancaman bisa timbul dari individu, entitas, atau situasi yang memiliki potensi untuk mengancam sumber daya informasi suatu perusahaan. Ancaman ini dapat berasal dari pihak internal atau eksternal organisasi, dan bisa bersifat sengaja atau tidak sengaja. Ancaman internal melibatkan tidak hanya karyawan perusahaan, melainkan juga pekerja kontrak, konsultan, kontraktor, bahkan mitra bisnis perusahaan tersebut. Ancaman internal ini, seringkali dianggap lebih serius dalam dampak potensialnya dibandingkan dengan ancaman eksternal, karena mereka memiliki pemahaman yang lebih mendalam tentang sistem tersebut. Ancaman eksternal, di sisi lain, dapat melibatkan perusahaan lain yang menghasilkan produk serupa atau pesaing dalam industri yang sama. Penting untuk diingat bahwa tidak semua ancaman berasal dari tindakan sengaja dengan niat jahat; beberapa di antaranya mungkin muncul karena kecelakaan yang disebabkan oleh individu, baik dari dalam maupun luar perusahaan.

C. Solusi Keamanan Data untuk Organisasi

Setiap entitas organisasi memiliki sejumlah informasi yang dianggap sensitif. Dalam usaha menjaga kerahasiaan informasi yang termasuk dalam kategori sensitif, seperti data pembayaran pelanggan, data karyawan, atau informasi strategi bisnis, langkah ini memiliki tingkat kepentingan yang sangat tinggi dalam melindungi data rahasia organisasi dan memastikan bahwa informasi tersebut tetap terlindungi dari akses publik. Dalam situasi ini,terdapat beberapa tindakan yang dapat diambil untuk menjaga keamanan informasi dalam sebuah organisasi.

1. Rancang Kebijakan Pengelolaan Data

Pemanfaatan sistem klasifikasi data yang bersifat hierarkis dapat membantu dalam memisahkan informasi dengan tingkat sensitivitas yang bervariasi. Setiap tingkat data akan dikenai langkah-langkah keamanan yang berbeda, di mana tingkat pertama merujuk pada data yang sangat sensitif, memiliki potensi risiko tinggi, dan memerlukan tingkat keamanan tertinggi serta pembatasan akses yang ketat sesuai dengan kebutuhan spesifik. Tingkat kedua melibatkan data yang cukup sensitif dengan risiko yang lebih rendah, sehingga memerlukan kontrol keamanan yang lebih ringan dan izin akses internal yang lebih luas. Tingkat ketiga mencakup data yang

tidak sensitif dan memiliki risiko minimal atau bahkan tidak ada risiko yang signifikan bagi organisasi, sehingga memerlukan tingkat keamanan minimal atau bahkan tanpa pembatasan akses.

2. Seleksi Perangkat Lunak yang Terpercaya

Kita harus memahami sepenuhnya betapa pentingnya memilih perangkat lunak yang direkomendasikan oleh para ahli keamanan informasi sesuai dengan standar keamanan yang berlaku. Terkadang, perangkat lunak yang digunakan oleh organisasi mungkin tidak selalu mematuhi praktik keamanan yang sangat ketat.yang dapat meningkatkan risiko akses yang tidak sah terhadap informasi yang bersifat sensitif. Masalah ini menjadi lebih serius terutama ketika perangkat lunak tersebut berhubungan dengan data pembayaran pelanggan melalui aplikasi akuntansi. Untuk mengatasi hal ini, organisasi dapat mengambil beberapa langkah dasar dalam pemilihan dan identifikasi perangkat lunak yang aman. Disarankan untuk menghindari mengandalkan layanan keamanan dan perangkat lunak anti-malware gratis, karena meskipun cocok untuk usaha kecil yang memerlukan perlindungan dasar, seringkali mereka tidak dapat memberikan tingkat keamanan yang mendalam. Sebaliknya, fokus pada solusi khusus yang, meskipun tidak selalu mahal, Dengan melakukan tindakan ini, tingkat perlindungan dapat meningkat secara nyata.

3. Peningkatan Keamanan Kata Sandi

Mengatasi permasalahan penggunaan kata sandi yang rentan merupakan praktek umum yang dapat ditingkatkan melalui pelatihan dan penerapan berbagai aplikasi pengelolaan kata sandi.

. Banyak insiden pencurian data sensitif terjadi karena kelalaian dalam mengikuti praktik dasar keamanan informasi.

4.Optimalisasi Penggunaan Komputer Pribadi

Penggunaan komputer pribadi merupakan elemen penting dalam kehidupan dan pekerjaan saat ini. Selain meningkatkan produktivitas dan mengontrol biaya, Penggunaan komputer pribadi juga memiliki peran penting dalam menjaga kerahasiaan data dan mencegah akses oleh pihak yang tidak berwenang. Menggunakan komputer pribadi merupakan tindakan yang cerdas untuk melindungi data yang bersifat rahasia dari akses dan penyimpanan yang tidak sah oleh pihak yang tidak memiliki izin.

5. Menerapkan Sistem Manajemen Keamanan Informasi sesuai dengan standar ISO/IEC 27001:2005 adalah pendekatan yang terstruktur dan diakui secara global dalam mengelola keamanan informasi. ISO/IEC 27001:2005 adalah dokumen sistem manajemen keamanan informasi yang memberikan panduan umum mengenai langkah-langkah yang perlu diambil oleh perusahaan atau organisasi untuk mengevaluasi, mengimplementasikan, dan memelihara keamanan informasi menerapkan, dan menjaga keamanan informasi mereka sesuai dengan praktik terbaik dalam bidang keamanan informasi.

6. Mencadangkan data secara berkala sangat disarankan sebagai tindakan untuk menjaga keamanan data. Disarankan agar perusahaan memiliki dua salinan

cadangan: satu dapat disimpan di layanan penyimpanan awan seperti Dropbox atau Google Drive, sementara yang lainnya bisa disimpan di server tambahan atau perangkat penyimpanan yang dapat dengan mudah dipindahkan jika ukuran data tidak terlalu besar.

7. Langkah melakukan pencadangan data merupakan usaha yang sangat penting dalam menjaga keamanan data. Kendala-kendala seperti pemadaman listrik yang tiba-tiba atau kehilangan koneksi internet seringkali dapat mengakibatkan kehilangan tugas dan informasi yang memiliki tingkat kepentingan yang sangat tinggi.

Meskipun teknologi komputer telah mengalami perkembangan, situasi semacam ini masih sering terjadi. Oleh karena itu, direkomendasikan untuk secara berkala mencadangkan data sebagai langkah pencegahan terhadap kehilangan informasi. Disarankan juga untuk membuat salinan data yang dapat disimpan di perangkat flash disk atau hardisk.

KESIMPULAN

Dalam usaha untuk menjaga perlengkapan komputer dan non-komputer, fasilitas, data, serta informasi dari penyalahgunaan, prinsip Keamanan Informasi menjadi kunci. Prinsip Keamanan Informasi memiliki satu tujuan utama, yaitu menjaga kerahasiaan, ketersediaan, dan integritas informasi. Pada saat ini, kesadaran organisasi tentang pentingnya menjaga semua aset mereka, termasuk yang bersifat virtual maupun fisik, dari berbagai ancaman, entah itu berasal dari internal atau eksternal organisasi, semakin meningkat. Konsep Keamanan Sistem digunakan untuk menggambarkan langkah-langkah perlindungan perlengkapan komputer dan non-komputer, fasilitas, data, dan informasi dari penggunaan yang tidak sah oleh pihak yang tidak berwenang. Upaya menjaga keamanan sumber daya informasi dikenal sebagai Manajemen Keamanan Informasi (Information Security Management - ISM), sementara langkah-langkah untuk memastikan kelangsungan operasional perusahaan dan sumber daya informasinya setelah terjadinya bencana dikenal sebagai Manajemen Keberlanjutan Bisnis (Business Continuity Management - BCM). Konsep Manajemen Risiko digunakan untuk menjelaskan pendekatan yang membandingkan tingkat keamanan sumber daya informasi perusahaan dengan risiko yang mungkin dihadapi. Ancaman terhadap keamanan sistem informasi dapat datang dari berbagai pihak, termasuk individu, organisasi, mekanisme, atau peristiwa yang berpotensi membahayakan sumber daya informasi perusahaan, baik dari dalam maupun luar organisasi. Risiko Keamanan Informasi bisa diartikan sebagai hasil yang tidak diinginkan akibat pelanggaran keamanan informasi oleh ancaman keamanan informasi. Semua risiko ini melibatkan tindakan yang melanggar hukum. Berbagai langkah pengendalian, termasuk pengendalian teknis, kriptografis, fisik, formal, dan informal, digunakan untuk mengatasi ancaman dan risiko keamanan informasi.

DAFTAR PUSTAKA

Putra, Y. M. (2018). Keamanan Informasi. Modul Kuliah Sistem Informasi Manajemen. Jakarta: FEB-Universitas

Mercu Buana Purwanto, Eko (2014). Keamanan Informasi [Online] tersedia di https://bpptik.kominfo.go.id/2014/03/24/404/keamanan-informasi/ [diakses pada 17 November 2019]

Retnowardhani, Astari (2017). Keamanan Informasi [Online] tersedia di https://mmsi.binus.ac.id/2017/11/17/keamanan-informasi/ [diakses pada 17 November 2019]

Zaidun, Achmad (2013). Keamanan Informasi [Online] tersedia di http://achmadzaidun.blogspot.com/2013/12/keamanan-informasi.html [diakses pada 17 November 2019]

Grace (2014). Keamanan Informasi [Online] tersedia di http://kumpulanmakalahsim.blogspot.com/2014/05/keamanan-informasi.html [diakses pada 17 November 2019]

Anggraini, Magy (2013). Sistem Informasi Manajemen Keamanan Informasi [Online] tersedia di http://megyanggraini.blogspot.com/2013/07/sistem-informasi-manajemen-keamanan.html [diakses pada 17 November 2019]