Vol. 4, No. 2, Agustus 2024, Hal. 63-75

e-ISSN: 2809-0950

Jurnal Software Engineering and Information System (SEIS)

https://ejurnal.umri.ac.id/index.php/SEIS/index

AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 4.1 PADA TELKOM PENAJAM

Rezky Ramanda[1*)], Joy Nashar Utama Jaya[2)]

[1,2]Sistem Informasi, STMIK Borneo International Balikpapan

email: [1*]rezky_ramanda.20@stmik-borneo.ac.id, [2]joy.nashar@stmik-borneo.ac.id

**Corresponding Author*

Abstract

This research aims to evaluate and enhance data security at Plasa Telkom Penajam utilizing an information technology governance audit approach employing the COBIT 4.1 framework. data collection method in this research is interview, observation, and search for relevant documentation. Audit findings revealed several weaknesses in data security aspects at Plasa Telkom Penajam that require improvement. Auditing IT governance using the COBIT 4.1 framework will help Telkom Penajam to identify security gaps and implement effective controls to protect their sensitive data from internal and external threats. The results of this study are several aspects of data security that need to be improved in order to maintain the integrity and confidentiality of information managed by the company. It is hoped that this research can reduce the risk of data security threats, increase employee awareness and understanding of data security, and strengthen the company's information technology infrastructure.

Keywords: *Data security, Information technology governance audit, COBIT 4.1*

Abstrak

Penelitian ini bertujuan untuk mengevaluasi dan meningkatkan keamanan data di Plasa Telkom Penajam menggunakan pendekatan audit tata kelola teknologi informasi dengan memanfaatkan framework COBIT 4.1. metode pengumpulan data pada peneilitian ini wawancara, observasi, dan penelusuran dokumentasi yang relevan. Temuan audit mengungkapkan bahwa Plasa Telkom Penajam masih memiliki beberapa kelemahan dalam aspek keamanan data yang memerlukan perbaikan.Audit tata kelola TI dengan menggunakan framework COBIT 4.1 akan membantu Telkom Penajam untuk mengidentifikasi celah keamanan dan mengimplementasikan kontrol yang efektif untuk melindungi data sensitif mereka dari ancaman internal dan eksternal. Hasil dari penelitian ini beberapa aspek keamanan data yang perlu ditingkatkan demi menjaga integritas dan kerahasiaan informasi yang dikelola oleh perusahaan. Diharapkan penelitian ini dapat mengurangi risiko terhadap ancaman keamanan data, meningkatkan kesadaran dan pemahaman karyawan mengenai keamanan data, serta memperkuat infrastruktur teknologi informasi perusahaan.

Kata Kunci: *Keamanan data, Audit tata kelola teknologi informasi, COBIT 4.1*

PENDAHULUAN

Plasa Telkom Penajam, sebagai bagian integral dari PT Telkom Indonesia, memainkan peran penting dalam menyediakan layanan telekomunikasi dan informasi di Penajam, Kalimantan Timur. Sebagai unit bisnis yang bertanggung jawab atas segala aspek operasionalnya, Plasa Telkom Penajam mengandalkan teknologi informasi sebagai tulang punggung dalam menjalankan kegiatan bisnisnya. Dengan memanfaatkan teknologi informasi, Plasa Telkom Penajam dapat mempercepat dan meningkatkan efisiensi dalam berbagai proses bisnisnya (Saryoko et al. 2021).

Salah satu manfaat utama teknologi informasi bagi Plasa Telkom Penajam adalah dalam hal penjualan produk dan layanan. Melalui sistem yang terintegrasi, pelanggan dapat dengan mudah menjelajahi produk dan layanan yang ditawarkan serta melakukan transaksi secara online. Dengan adanya platform e-commerce, Plasa Telkom Penajam dapat menjangkau lebih banyak pelanggan tanpa terbatas oleh batas wilayah geografis, sehingga memperluas pangsa pasar dan meningkatkan pendapatan.

Tidak hanya itu, teknologi informasi juga berperan penting dalam pengelolaan pelanggan. Dengan basis data pelanggan yang terpusat dan terintegrasi, Plasa Telkom Penajam dapat melacak preferensi dan riwayat transaksi pelanggan dengan lebih baik. Hal ini memungkinkan Plasa Telkom Penajam untuk memberikan layanan yang lebih personal dan berkualitas tinggi kepada pelanggan, meningkatkan kepuasan pelanggan, dan membangun hubungan jangka panjang (Sinaga and Permana 2023).

Selain itu, pengelolaan keuangan merupakan aspek bisnis yang tidak bisa diabaikan. Plasa Telkom Penajam menggunakan teknologi informasi untuk mengotomatisasi proses akuntansi, pelaporan keuangan, dan pengelolaan kas. Dengan sistem yang terintegrasi, Plasa Telkom Penajam dapat memantau arus kas secara real-time, mengidentifikasi pola pengeluaran dan pemasukan, serta membuat keputusan keuangan yang lebih tepat waktu dan akurat (Muharom and Nugraha 2020).

Namun, meskipun teknologi informasi memberikan banyak manfaat bagi Plasa Telkom Penajam, tantangan dan risiko juga ada. Keamanan data dan privasi pelanggan menjadi prioritas utama, mengingat jumlah informasi sensitif yang disimpan dan diproses oleh Plasa Telkom Penajam. Oleh karena itu, Plasa Telkom Penajam harus terus meningkatkan sistem keamanan informasinya, termasuk penerapan enkripsi data, firewalls, dan pemantauan keamanan yang ketat (Andry and Riwanto 2019).

Tata kelola teknologi informasi yang baik menjadi hal yang sangat penting bagi Plasa Telkom Penajam guna memastikan keamanan data yang mereka kelola. Dalam era digital yang semakin maju, di mana data menjadi aset yang sangat berharga, perlunya perlindungan terhadap data menjadi krusial. Dengan tata kelola teknologi informasi yang baik, Plasa Telkom Penajam dapat memastikan bahwa data yang mereka miliki terlindungi dari berbagai ancaman yang mungkin terjadi (Sayekti et al. 2020).

Salah satu manfaat utama dari tata kelola teknologi informasi yang baik adalah kemampuannya untuk melindungi data dari kehilangan. Dengan adanya kebijakan dan prosedur yang ketat terkait dengan penyimpanan dan pemulihan data, Plasa Telkom Penajam dapat meminimalkan risiko kehilangan data akibat kegagalan sistem atau kejadian tak terduga lainnya. Backup data secara berkala dan penyimpanan data yang aman menjadi langkah-langkah penting dalam menjaga keberlangsungan operasional dan keamanan informasi (Andry and Sanjaya 2017).

Selain melindungi data dari kehilangan, tata kelola teknologi informasi yang baik juga membantu dalam melindungi data dari kerusakan. Dengan menerapkan kebijakan dan prosedur yang memastikan integritas data, Plasa Telkom Penajam dapat mengurangi risiko kerusakan data akibat serangan virus, kegagalan perangkat keras, atau bencana alam. Penggunaan teknologi canggih seperti sistem deteksi dan pencegahan malware serta redundansi perangkat keras menjadi bagian dari strategi untuk menjaga keandalan dan keutuhan data (Hambali 2021).

Tidak hanya itu, tata kelola teknologi informasi yang baik juga mampu melindungi data dari penyalahgunaan. Dengan menerapkan kebijakan akses yang ketat dan sistem autentikasi yang kuat, Plasa Telkom Penajam dapat memastikan bahwa hanya orang-orang yang berwenang yang memiliki akses ke data sensitif. Pemantauan aktif terhadap aktivitas pengguna juga menjadi bagian dari upaya untuk mendeteksi dan mencegah potensi penyalahgunaan data (Lesmono and Erca 2018).

Framework COBIT 4.1 telah terbukti menjadi alat yang sangat berguna dalam mengevaluasi tata

kelola teknologi informasi di berbagai organisasi. Dengan fokus pada lima domain utama, yaitu Plan and Organize, Acquire and Implement, Deliver and Support, serta Monitor and Evaluate, COBIT 4.1 memberikan panduan yang komprehensif untuk memastikan bahwa TI dapat diintegrasikan secara efektif dalam strategi bisnis organisasi. Domain pertama, Plan and Organize, menekankan pentingnya perencanaan yang matang dalam mengelola TI. Ini termasuk pengembangan strategi TI yang sejalan dengan tujuan bisnis organisasi serta penentuan struktur organisasi TI yang efektif. Selanjutnya, Acquire and Implement membahas proses pengadaan dan implementasi solusi TI yang sesuai dengan kebutuhan organisasi, termasuk pemilihan vendor, pengembangan aplikasi, dan manajemen perubahan. Domain ketiga, Deliver and Support, fokus pada penyediaan layanan TI yang berkualitas kepada pengguna akhir, termasuk dukungan teknis, manajemen kapasitas, dan manajemen keamanan informasi. Sementara itu, Monitor and Evaluate menekankan pentingnya pengawasan dan evaluasi berkelanjutan terhadap kinerja TI untuk memastikan bahwa sistem berjalan sesuai dengan yang diharapkan dan dapat memberikan nilai tambah bagi organisasi. Keseluruhan, COBIT 4.1 memberikan kerangka kerja yang holistik dan terstruktur untuk mengevaluasi dan meningkatkan tata kelola TI, membantu organisasi untuk mencapai tujuan bisnis mereka dengan lebih efisien dan efektif (Tomas and F. Andry 2020).

Tujuan utama dari penelitian ini adalah untuk melakukan audit terhadap tata kelola teknologi informasi di Plasa Telkom Penajam dengan menggunakan framework COBIT 4.1. Audit ini dilakukan dengan maksud untuk mengevaluasi seberapa efektif tata kelola teknologi informasi tersebut dalam mendukung pencapaian tujuan bisnis organisasi tersebut (Imami, Suprapto, and Mursityo 2019).

Dalam konteks penelitian ini, terdapat beberapa tujuan yang ingin dicapai, yaitu pertama, untuk mengetahui tingkat kematangan tata kelola teknologi informasi di Plasa Telkom Penajam. Hal ini penting untuk memahami sejauh mana organisasi telah menerapkan praktik-praktik terbaik dalam pengelolaan teknologi informasi, serta untuk mengidentifikasi area di mana perbaikan diperlukan.

Selanjutnya, tujuan penelitian ini adalah untuk mengidentifikasi risiko keamanan data yang dihadapi oleh Plasa Telkom Penajam. Dengan melakukan audit tata kelola teknologi informasi, peneliti akan dapat mengidentifikasi potensi risiko seperti kehilangan data, kerusakan data, dan penyalahgunaan data. Identifikasi ini merupakan langkah awal yang penting dalam mengembangkan strategi mitigasi risiko yang efektif (Tukino, Faqih Pratama Muthi, and Aditia Agustian 2021).

Terakhir, tujuan dari penelitian ini adalah untuk memberikan rekomendasi yang konkret dan praktis untuk meningkatkan keamanan data di Plasa Telkom Penajam. Rekomendasi ini akan didasarkan pada temuan dari audit tata kelola teknologi informasi dan bertujuan untuk membantu Plasa Telkom Penajam dalam mengimplementasikan perubahan yang diperlukan untuk memperkuat keamanan data mereka.

METODE PENELITIAN

Metodologi penelitian ini mengadopsi pendekatan audit tata kelola teknologi informasi dengan memanfaatkan framework COBIT 4.1 sebagai landasan utama. Audit tersebut dilakukan dengan tahapan pengumpulan informasi dan data melalui beberapa teknik, termasuk wawancara, observasi, dan penelusuran dokumentasi yang relevan.

Proses pengumpulan informasi dan data ini melibatkan berbagai aspek yang relevan dengan tata kelola teknologi informasi di Plasa Telkom Penajam. Pertama, peneliti mengumpulkan informasi terkait dengan kebijakan dan prosedur keamanan data yang telah diterapkan oleh organisasi. Hal ini mencakup evaluasi terhadap kebijakan pengamanan data yang telah ada serta prosedur-prosedur yang telah diimplementasikan untuk melindungi informasi sensitif dari berbagai risiko keamanan (Purwaningrum 2021).

Selanjutnya, penelitian ini juga memperhatikan infrastruktur teknologi informasi yang digunakan oleh Plasa Telkom Penajam. Ini melibatkan peninjauan terhadap perangkat keras dan perangkat lunak yang digunakan dalam operasional sehari-hari organisasi, serta evaluasi terhadap keandalan dan keamanan sistem tersebut.

Proses audit juga memerhatikan proses-proses keamanan data yang diimplementasikan oleh Plasa Telkom Penajam. Ini mencakup peninjauan terhadap langkah-langkah yang

diambil untuk mengamankan data selama proses pengumpulan, penyimpanan, pengolahan, dan penyebaran.

Selain itu, sumber daya manusia juga menjadi fokus dalam pengumpulan informasi dan data. Penelitian ini memperhatikan pengetahuan dan keterampilan personel yang terlibat dalam pengelolaan dan pengamanan teknologi informasi di Plasa Telkom Penajam, serta upaya-upaya yang dilakukan dalam meningkatkan kesadaran keamanan informasi di kalangan karyawan.

Setelah data terkumpul, langkah selanjutnya adalah menganalisisnya menggunakan framework COBIT 4.1. Framework ini digunakan sebagai panduan untuk mengevaluasi tingkat kematangan tata kelola teknologi informasi di Plasa Telkom Penajam. Dengan mengacu pada kriteria-kriteria yang ditetapkan dalam COBIT 4.1, peneliti dapat menilai sejauh mana organisasi telah mencapai tingkat kematangan yang diinginkan dalam pengelolaan dan pengamanan teknologi informasi.

HASIL DAN PEMBAHASAN

Hasil Audit

Kebijakan dan Prosedur Keamanan Data

Kebijakan dan prosedur keamanan data merupakan fondasi penting dalam menjaga keamanan dan integritas data, terutama dalam menghadapi berbagai ancaman seperti serangan siber, kesalahan manusia, dan bencana alam. Namun, ada kekhawatiran bahwa kebijakan dan prosedur yang ada belum mencakup semua aspek keamanan data, yang mengakibatkan ketidaklengkapannya dalam melindungi informasi sensitif yang dikelola oleh Plasa Telkom Penajam. Aspek-aspek penting dari keamanan data seperti keamanan fisik, keamanan jaringan, dan keamanan aplikasi harus diintegrasikan secara komprehensif dalam kebijakan dan prosedur yang ada.

Aspek-Aspek Keamanan Data

Keamanan data terdiri dari berbagai aspek, antara lain:

Keamanan fisik

Keamanan fisik adalah aspek penting dalam melindungi data dari akses fisik yang tidak sah, termasuk pencurian, sabotase, dan kerusakan. Dalam konteks perlindungan data, berbagai strategi dapat diterapkan untuk memastikan keamanan fisik yang optimal. Pertama, membangun pagar dan gerbang merupakan langkah awal yang efektif untuk membatasi akses ke area yang menyimpan data penting. Dengan membatasi akses fisik secara fisik, organisasi dapat mengendalikan siapa yang memiliki izin untuk mengakses ruang tersebut, mengurangi risiko dari pihak-pihak yang tidak berwenang untuk masuk ke area tersebut. Selain itu, memasang kamera pengawas juga merupakan solusi yang efektif dalam memantau area yang menyimpan data penting.

Kamera pengawas dapat memberikan pengawasan 24/7 terhadap area tersebut, sehingga memungkinkan deteksi dini terhadap kegiatan yang mencurigakan atau ancaman keamanan potensial. Dengan demikian, keberadaan kamera pengawas dapat memberikan tingkat keamanan tambahan dan memberikan bukti visual yang berguna dalam investigasi keamanan jika diperlukan. Selain itu, melakukan pemeriksaan keamanan secara berkala juga merupakan langkah yang krusial dalam memastikan keamanan fisik yang berkelanjutan. Pemeriksaan keamanan rutin dapat mencakup pengecekan terhadap semua titik masuk dan keluar, memastikan bahwa pintu dan jendela terkunci dengan baik, serta memverifikasi identitas setiap orang yang masuk ke area yang menyimpan data penting.

Dengan melakukan pemeriksaan secara berkala, organisasi dapat mengidentifikasi dan mengatasi potensi kerentanan keamanan fisik sebelum dapat dieksploitasi oleh pihak yang tidak berwenang. Selain itu, pemeriksaan keamanan berkala juga merupakan kesempatan untuk memastikan bahwa semua sistem keamanan fisik berfungsi dengan baik dan sesuai dengan standar keamanan yang ditetapkan. Dengan menerapkan langkah-langkah tersebut, organisasi dapat meningkatkan keamanan fisik data mereka dan mengurangi risiko terhadap ancaman yang mungkin timbul dari akses fisik yang tidak sah. Dengan demikian, keamanan fisik yang efektif menjadi bagian integral dari strategi perlindungan data secara menyeluruh, memastikan bahwa data sensitif dan kritis tetap aman dan terlindungi dari berbagai ancaman yang ada.

Keamanan jaringan

Keamanan jaringan menjadi aspek kunci dalam menjaga keamanan data dari akses yang tidak sah, seperti serangan siber dan penyadapan. Dalam konteks keamanan jaringan, terdapat beberapa langkah yang dapat diambil untuk memastikan bahwa data tetap terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang. Pertama, memasang firewall merupakan salah satu cara yang efektif untuk menghalangi akses jaringan yang tidak sah. Firewall bertindak sebagai penghalang pertama yang dapat mendeteksi dan mencegah akses dari luar yang mencurigakan atau berpotensi berbahaya. Dengan memasang firewall yang konfigurasi dengan benar, organisasi dapat memblokir lalu lintas yang tidak diinginkan dan memastikan bahwa hanya lalu lintas yang diizinkan yang dapat mengakses jaringan.

Selain itu, melakukan enkripsi data juga menjadi langkah penting dalam menjaga keamanan jaringan. Enkripsi data melibatkan proses mengubah data menjadi format yang tidak dapat dibaca secara langsung tanpa kunci enkripsi yang sesuai. Dengan menerapkan enkripsi data, informasi yang dikirim melalui jaringan akan menjadi lebih aman dari penyadapan atau perekaman oleh pihak yang tidak berwenang. Ini memastikan bahwa data sensitif tidak dapat diakses atau dimanipulasi oleh pihak yang tidak sah selama proses pengiriman atau penerimaan.

Selain itu, patch management juga menjadi faktor penting dalam menjaga keamanan jaringan. Patch management melibatkan penerapan pembaruan atau "patch" ke perangkat lunak dan sistem operasi yang digunakan dalam jaringan. Pembaruan ini biasanya dirilis oleh vendor perangkat lunak untuk memperbaiki kerentanan keamanan yang ditemukan dalam perangkat lunak mereka. Dengan menerapkan pembaruan secara teratur, organisasi dapat memastikan bahwa sistem dan perangkat lunak mereka tetap aman dari serangan yang mengambil keuntungan dari kerentanan yang ada.

Keamanan aplikasi

Keamanan aplikasi merupakan aspek penting dalam menjaga integritas dan kerahasiaan data dari akses yang tidak sah, baik dari serangan siber maupun kesalahan manusia yang mungkin terjadi. Dalam konteks keamanan aplikasi, beberapa langkah dapat diambil untuk memastikan bahwa data tetap terlindungi dengan baik. Pertama, melakukan validasi dan otentikasi pengguna sebelum mengakses aplikasi adalah langkah yang penting dalam mencegah akses yang tidak sah. Dengan memastikan bahwa pengguna harus melewati proses validasi dan otentikasi yang tepat sebelum diizinkan untuk mengakses aplikasi, organisasi dapat memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data sensitif yang disimpan di dalam aplikasi tersebut. Ini membantu mencegah akses yang tidak sah dan melindungi data dari penyalahgunaan.

Selanjutnya, melakukan enkripsi data yang tersimpan di dalam aplikasi juga merupakan langkah penting dalam menjaga keamanan aplikasi. Enkripsi data melibatkan proses mengubah data menjadi format yang tidak dapat dibaca secara langsung tanpa kunci enkripsi yang sesuai. Dengan menerapkan enkripsi pada data yang disimpan di dalam aplikasi, organisasi dapat memastikan bahwa data sensitif tetap aman bahkan jika terjadi pelanggaran keamanan atau akses yang tidak sah. Enkripsi memungkinkan data untuk tetap terlindungi bahkan jika data tersebut dicuri atau disusupi oleh pihak yang tidak berwenang.

Selain itu, melakukan audit aplikasi secara berkala juga merupakan langkah yang penting dalam menjaga keamanan aplikasi. Audit aplikasi melibatkan pemeriksaan dan evaluasi terhadap kode dan konfigurasi aplikasi untuk mendeteksi adanya celah keamanan atau kerentanan yang mungkin dieksploitasi oleh pihak yang tidak berwenang. Dengan melakukan audit secara berkala, organisasi dapat mengidentifikasi dan memperbaiki celah keamanan sebelum dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mengakses atau merusak data di dalam aplikasi.

Kebijakan dan Prosedur Keamanan Data yang Belum Dikomunikasikan Secara Efektif

Kebijakan dan prosedur keamanan data yang belum disampaikan secara efektif kepada seluruh pegawai dapat menjadi sumber ancaman serius terhadap keamanan data. Ketidaktahuan pegawai

mengenai kebijakan dan prosedur yang ada dapat membuka celah bagi pelanggaran keamanan yang tidak disengaja atau bahkan disengaja.

Komunikasi yang efektif mengenai kebijakan dan prosedur keamanan data merupakan langkah krusial dalam memastikan pemahaman yang tepat dan penerapan yang konsisten di seluruh organisasi. Salah satu cara untuk melakukan komunikasi yang efektif adalah dengan menerbitkan kebijakan dan prosedur keamanan data dalam format dokumen yang mudah dipahami oleh semua pegawai. Dokumen tersebut harus disusun dengan jelas dan rinci, serta menggunakan bahasa yang sederhana dan tidak terlalu teknis agar dapat dipahami oleh berbagai lapisan karyawan.

Selain itu, sosialisasi kebijakan dan prosedur keamanan data kepada seluruh pegawai juga merupakan langkah penting dalam memastikan kesadaran dan pemahaman yang merata di seluruh organisasi. Sosialisasi dapat dilakukan melalui pertemuan-pertemuan rutin, seminar, atau sesi pelatihan khusus yang diadakan oleh tim keamanan informasi. Dalam sosialisasi tersebut, penting untuk menjelaskan tujuan, pentingnya, serta konsekuensi dari kebijakan dan prosedur keamanan data yang ada.

Selain sosialisasi, pelatihan keamanan data secara berkala juga diperlukan untuk memastikan bahwa pegawai memiliki pengetahuan dan keterampilan yang diperlukan untuk melindungi data secara efektif. Pelatihan ini dapat mencakup topik-topik seperti pengenalan terhadap ancaman keamanan yang umum, praktik-praktik pengamanan yang disarankan, serta prosedur yang harus diikuti dalam menghadapi insiden keamanan. Dengan memberikan pelatihan yang berkualitas, organisasi dapat memperkuat budaya keamanan data di dalam perusahaannya.

Dalam rangka mengatasi masalah keamanan data yang disebabkan oleh kurangnya komunikasi yang efektif, organisasi perlu mengambil langkah-langkah proaktif untuk memastikan bahwa kebijakan dan prosedur keamanan data disampaikan dengan jelas dan tepat kepada seluruh pegawai. Hal ini membutuhkan upaya kolaboratif antara tim keamanan informasi, manajemen senior, dan departemen sumber daya manusia untuk menyusun strategi komunikasi yang efektif dan menyeluruh. Dengan demikian, organisasi dapat mengurangi risiko terhadap pelanggaran keamanan data dan membangun budaya keamanan yang kuat di seluruh perusahaan.

Infrastruktur Teknologi Informasi

Infrastruktur teknologi informasi (TI) merupakan fondasi penting untuk mendukung berbagai proses bisnis di organisasi. Infrastruktur TI yang aman dapat membantu melindungi data-data penting dari berbagai ancaman, seperti serangan siber, kesalahan manusia, dan bencana alam.

Penerapan firewall dan antivirus merupakan salah satu persyaratan dasar untuk keamanan infrastruktur TI. Firewall berfungsi untuk memblokir akses jaringan yang tidak sah, sedangkan antivirus berfungsi untuk melindungi sistem dari serangan malware.

Beberapa contoh celah keamanan yang dapat terjadi jika infrastruktur TI tidak memenuhi persyaratan keamanan data, antara lain:

Akses jaringan yang tidak sah

Akses jaringan yang tidak sah merupakan ancaman serius bagi keamanan sistem dan data suatu organisasi. Penyerang yang berhasil mendapatkan akses jaringan secara tidak sah dapat melakukan berbagai tindakan merugikan, seperti mencuri data sensitif, menyebarkan malware, atau merusak sistem secara keseluruhan. Dalam upaya melindungi jaringan mereka dari akses yang tidak sah, organisasi umumnya mengandalkan firewall sebagai lapisan pertahanan pertama.

Namun, firewall yang tidak dikonfigurasi dengan benar dapat menjadi celah keamanan yang signifikan yang dapat dimanfaatkan oleh penyerang. Sebagai contoh, jika konfigurasi firewall tidak memadai atau terlalu longgar, penyerang mungkin dapat dengan mudah menembus pertahanan jaringan dan masuk ke dalam sistem. Firewall yang terlalu longgar dapat membiarkan lalu lintas jaringan yang tidak sah masuk ke dalam jaringan internal, meningkatkan risiko serangan dan akses yang tidak diinginkan.

Selain itu, firewall yang tidak diperbarui secara teratur juga dapat menjadi masalah keamanan. Ancaman keamanan berubah dengan

cepat, dan sering kali firewall yang tidak diperbarui tidak dapat mengenali atau menghalangi serangan terbaru. Penyerang yang canggih dapat dengan mudah menemukan celah-celah dalam firewall yang tidak diperbarui dan menggunakan mereka sebagai pintu masuk untuk melakukan akses jaringan yang tidak sah.

Selain firewall yang tidak dikonfigurasi dengan benar atau tidak diperbarui secara teratur, serangan phishing juga dapat menjadi salah satu cara bagi penyerang untuk mendapatkan akses jaringan yang tidak sah. Dalam serangan phishing, penyerang menggunakan email palsu atau situs web yang meniru organisasi untuk mencuri informasi login atau kredensial pengguna. Setelah mendapatkan informasi tersebut, penyerang dapat menggunakan mereka untuk masuk ke dalam sistem atau jaringan secara tidak sah.

Dalam menghadapi ancaman akses jaringan yang tidak sah, organisasi harus mengambil langkah-langkah yang diperlukan untuk memperkuat pertahanan jaringan mereka. Hal ini mencakup pengaturan firewall dengan benar dan memastikan bahwa mereka terus diperbarui secara teratur untuk menghadapi ancaman yang berkembang. Selain itu, organisasi juga perlu meningkatkan kesadaran pengguna tentang serangan phishing dan memberikan pelatihan kepada karyawan untuk mengidentifikasi dan menghindari upaya phishing yang mencurigakan.

Serangan malware

Serangan malware merupakan ancaman serius bagi keamanan sistem dan data suatu organisasi. Malware, yang mencakup berbagai jenis seperti virus, trojan, dan ransomware, dapat menyebabkan berbagai kerugian seperti kerusakan data, kehilangan data, atau bahkan pencurian data sensitif. Dalam menghadapi ancaman malware, organisasi umumnya mengandalkan perangkat lunak antivirus sebagai pertahanan pertama.

Namun, antivirus yang tidak diperbarui dengan patch terbaru dapat menjadi celah keamanan yang signifikan yang dapat dimanfaatkan oleh malware untuk menginfeksi sistem. Ketika sebuah perangkat lunak antivirus tidak diperbarui secara teratur, ia mungkin tidak dapat mengenali atau menghalangi serangan malware terbaru. Ini memungkinkan malware untuk menyelinap masuk ke dalam sistem tanpa terdeteksi, mengakibatkan kerusakan atau kehilangan data yang signifikan.

Selain itu, serangan malware juga dapat dimulai dari sumber yang tidak terduga seperti lampiran email atau situs web yang terinfeksi. Penyerang sering menggunakan teknik sosial rekayasa untuk menipu pengguna agar mengklik pada lampiran atau tautan yang terinfeksi, yang kemudian dapat mengunduh dan menginfeksi sistem dengan malware. Dalam beberapa kasus, pengguna mungkin tidak menyadari bahwa mereka telah mengunduh malware sampai sudah terlambat dan kerusakan telah terjadi.

Selain antivirus yang tidak diperbarui, kelemahan dalam sistem operasi atau perangkat lunak juga dapat menjadi sasaran empuk bagi serangan malware. Jika sistem atau perangkat lunak tidak diperbarui dengan patch keamanan terbaru, mereka mungkin rentan terhadap serangan yang menggunakan kerentanan yang ada untuk menginfeksi sistem dengan malware. Oleh karena itu, penting untuk memastikan bahwa semua sistem dan perangkat lunak diorganisasi diperbarui secara teratur dengan patch terbaru untuk mengurangi risiko serangan malware.

Dalam menghadapi ancaman serangan malware, organisasi harus mengambil langkah-langkah proaktif untuk memperkuat pertahanan mereka. Ini termasuk memastikan bahwa antivirus dan perangkat lunak keamanan lainnya diperbarui secara teratur dengan patch terbaru, serta melaksanakan pelatihan keamanan yang menyeluruh untuk meningkatkan kesadaran pengguna tentang serangan malware dan cara menghindarinya. Selain itu, organisasi juga harus mempertimbangkan penggunaan teknologi keamanan tambahan seperti firewall yang kuat dan deteksi ancaman lanjutan untuk memberikan lapisan perlindungan tambahan terhadap serangan malware.

Kerusakan system

Kerusakan sistem merupakan ancaman serius bagi keberlangsungan layanan teknologi informasi (TI) suatu organisasi. Jenis kerusakan sistem yang umum meliputi serangan denial-of-service (DoS) dan serangan distributed denial-of-service (DDoS), yang memiliki potensi untuk mengganggu atau bahkan menghentikan layanan

TI secara keseluruhan. Dalam serangan DoS atau DDoS, penyerang mencoba untuk mengalirkan lalu lintas yang sangat besar ke server atau jaringan dengan tujuan membuatnya tidak responsif terhadap permintaan pengguna yang sah. Akibatnya, layanan TI menjadi tidak dapat diakses bagi pengguna yang sah, yang dapat menyebabkan kerugian finansial, reputasi, dan produktivitas bagi organisasi.

Sistem yang tidak memiliki perlindungan yang memadai dapat menjadi sasaran empuk bagi serangan kerusakan sistem. Salah satu contoh adalah ketika sebuah server tidak dilindungi oleh solusi keamanan yang kuat, seperti firewall atau sistem deteksi intrusi, yang dapat mengidentifikasi dan menghalangi lalu lintas mencurigakan. Tanpa perlindungan yang memadai, server tersebut dapat dengan mudah menjadi target bagi serangan DoS atau DDoS, yang dapat mengakibatkan penurunan kinerja atau bahkan kerusakan total pada sistem tersebut.

Selain serangan DoS dan DDoS, serangan lain seperti serangan malware atau hacking juga dapat menyebabkan kerusakan sistem yang serius. Sebagai contoh, serangan ransomware dapat mengenkripsi data yang penting bagi organisasi, menyebabkan gangguan serius pada operasi dan menyebabkan kerugian finansial yang signifikan. Di sisi lain, serangan hacking yang berhasil memanfaatkan celah keamanan dalam sistem dapat menyebabkan pencurian data sensitif atau merusak integritas data, mengakibatkan kerugian reputasi dan legal yang besar bagi organisasi.

Untuk melindungi sistem dari kerusakan yang disebabkan oleh serangan seperti DoS, DDoS, malware, atau hacking, organisasi perlu mengambil langkah-langkah yang proaktif dalam memperkuat pertahanan mereka. Salah satu langkah yang penting adalah mengimplementasikan solusi keamanan yang memadai, seperti firewall, sistem deteksi intrusi, dan perangkat lunak antivirus yang diperbarui secara teratur. Solusi keamanan ini dapat membantu mengidentifikasi dan menghalangi serangan sebelum mereka dapat menyebabkan kerusakan yang signifikan pada sistem.

Selain itu, organisasi juga perlu mengadopsi praktik-praktik terbaik dalam manajemen keamanan informasi, seperti melakukan pembaruan sistem dan perangkat lunak secara teratur, memberlakukan kebijakan keamanan yang ketat, dan melaksanakan pelatihan keamanan bagi karyawan. Dengan menggabungkan teknologi keamanan yang efektif dengan budaya keamanan yang kuat, organisasi dapat meminimalkan risiko kerusakan sistem dan melindungi data dan layanan mereka dari serangan yang merusak. Dengan demikian, investasi dalam keamanan sistem menjadi kunci untuk menjaga kelangsungan operasi dan reputasi organisasi di era digital yang penuh dengan ancaman cyber.

Pencurian data

Pencurian data merupakan ancaman serius bagi keamanan informasi suatu organisasi. Data yang dicuri memiliki potensi untuk menyebabkan kerugian finansial yang signifikan dan merusak reputasi perusahaan. Informasi sensitif yang jatuh ke tangan yang salah dapat digunakan untuk berbagai tujuan yang merugikan, seperti melakukan penipuan, penyalahgunaan identitas, atau bahkan blackmail terhadap organisasi atau individu yang terkait. Oleh karena itu, melindungi data dari pencurian menjadi prioritas utama bagi setiap organisasi.

Sistem yang tidak memiliki enkripsi data yang memadai merupakan sasaran empuk bagi serangan pencurian data. Enkripsi data adalah proses mengubah data menjadi format yang tidak dapat dibaca atau dimengerti tanpa memiliki kunci enkripsi yang sesuai. Jika data tidak dienkripsi dengan benar, penyerang dapat dengan mudah mencuri informasi sensitif yang disimpan dalam database atau sistem informasi organisasi. Hal ini terutama berlaku jika data disimpan dalam format teks biasa tanpa perlindungan tambahan, memudahkan penyerang untuk mencuri dan memanfaatkannya untuk kepentingan mereka sendiri.

Selain kurangnya enkripsi data, celah keamanan lain dalam sistem juga dapat dimanfaatkan oleh penyerang untuk melakukan pencurian data. Salah satu contoh adalah ketika sistem tidak diperbarui secara teratur dengan patch keamanan terbaru. Celah keamanan yang ada dalam sistem yang tidak diperbarui dapat dimanfaatkan oleh penyerang untuk memasuki jaringan dan mencuri data dengan mudah. Oleh karena itu, penting bagi organisasi untuk memastikan bahwa sistem mereka terus

diperbarui dengan patch keamanan terbaru untuk mengurangi risiko pencurian data.

Selain memastikan keamanan sistem secara keseluruhan, organisasi juga perlu mengadopsi kebijakan dan prosedur yang ketat dalam manajemen akses data. Ini termasuk memberikan akses data hanya kepada individu yang membutuhkannya untuk melaksanakan tugas pekerjaan mereka, serta memantau dan membatasi aktivitas akses data yang mencurigakan. Dengan menerapkan kontrol akses yang ketat, organisasi dapat mengurangi risiko pencurian data oleh insider atau oleh pihak luar yang telah mendapatkan akses yang tidak sah.

Selain itu, pelatihan keamanan yang menyeluruh bagi karyawan juga merupakan langkah yang penting dalam melindungi data dari pencurian. Karyawan perlu diberikan pemahaman yang mendalam tentang risiko pencurian data dan langkah-langkah yang dapat mereka ambil untuk melindungi informasi sensitif. Dengan meningkatkan kesadaran karyawan tentang pentingnya keamanan data dan tindakan yang dapat mereka ambil untuk melindunginya, organisasi dapat mengurangi risiko pencurian data yang disebabkan oleh kesalahan manusia atau tindakan yang tidak disengaja.

Proses-proses keamanan data

Proses-proses keamanan data yang belum terintegrasi dengan baik merupakan salah satu masalah serius dalam menjaga keamanan informasi suatu organisasi. Ketika proses-proses keamanan data tidak terintegrasi secara menyeluruh, hal ini dapat menyebabkan celah keamanan yang signifikan yang dapat dimanfaatkan oleh penyerang untuk melakukan akses yang tidak sah atau pencurian data. Misalnya, ketika sistem keamanan data tidak terhubung dengan baik dengan sistem manajemen akses pengguna, maka pengguna yang tidak berwenang mungkin tetap memiliki akses yang tidak diinginkan ke data sensitif, meningkatkan risiko pencurian atau penyalahgunaan data.

Kurangnya integrasi antara proses-proses keamanan data juga dapat menyebabkan redundansi atau tumpang tindih dalam kontrol keamanan. Misalnya, jika organisasi memiliki beberapa sistem yang mengelola hak akses pengguna secara terpisah tanpa sinkronisasi yang tepat, hal ini dapat menyebabkan kesulitan dalam mengelola dan memantau akses pengguna secara konsisten. Akibatnya, ada risiko bahwa pengguna yang seharusnya tidak memiliki akses ke data tertentu dapat secara tidak sengaja atau sengaja memperoleh akses yang tidak sah, meningkatkan risiko kebocoran data atau penyalahgunaan informasi.

Selain kurangnya integrasi, evaluasi terhadap efektivitas proses-proses keamanan data juga merupakan hal yang penting namun sering diabaikan. Tanpa evaluasi yang teratur, organisasi mungkin tidak menyadari kelemahan atau celah dalam sistem keamanan mereka, meninggalkan mereka rentan terhadap serangan atau pencurian data. Evaluasi terhadap efektivitas proses keamanan data memungkinkan organisasi untuk mengidentifikasi area-area yang memerlukan perbaikan atau peningkatan, serta menilai kinerja kontrol keamanan yang ada dalam melindungi data sensitif.

Selain itu, evaluasi terhadap efektivitas proses-proses keamanan data juga dapat membantu organisasi untuk mengukur sejauh mana kebijakan dan prosedur keamanan yang ada telah diikuti dan diterapkan dengan benar oleh karyawan. Ini dapat membantu dalam menemukan potensi pelanggaran keamanan atau kesenjangan dalam kepatuhan yang perlu segera ditangani. Tanpa evaluasi yang teratur, organisasi mungkin tidak menyadari ketidakpatuhan atau ketidakefektifan dalam penerapan kebijakan keamanan mereka, meninggalkan mereka rentan terhadap risiko keamanan yang tidak terdeteksi.

Untuk mengatasi masalah ini, organisasi perlu meningkatkan integrasi antara proses-proses keamanan data mereka dan melakukan evaluasi teratur terhadap efektivitas mereka. Ini dapat melibatkan mengadopsi solusi teknologi yang memungkinkan integrasi yang lebih baik antara sistem keamanan yang berbeda, serta melaksanakan audit keamanan rutin untuk mengevaluasi kepatuhan dan efektivitas kontrol keamanan yang ada. Dengan melakukan langkah-langkah ini, organisasi dapat meningkatkan keamanan data mereka dan mengurangi risiko terhadap serangan atau pencurian data yang merugikan.

Sumber Daya Manusia

Sumber daya manusia merupakan faktor penting dalam menjaga keamanan data suatu organisasi. Namun, masalah sering terjadi ketika sumber daya manusia tidak memiliki pemahaman yang cukup mengenai keamanan data. Tanpa pemahaman yang memadai, karyawan mungkin tidak menyadari praktik-praktik keamanan yang penting atau bahkan tidak menyadari risiko yang terkait dengan tindakan mereka dalam pengelolaan data. Hal ini dapat meningkatkan risiko kebocoran data atau pelanggaran keamanan lainnya yang disebabkan oleh tindakan yang tidak disengaja atau kurangnya kesadaran akan keamanan informasi.

Salah satu langkah yang penting untuk mengatasi masalah ini adalah memberikan pelatihan keamanan data secara berkala kepada karyawan. Pelatihan keamanan data dapat membantu meningkatkan pemahaman karyawan tentang ancaman keamanan yang ada, serta memberikan mereka pengetahuan dan keterampilan yang diperlukan untuk mengidentifikasi dan mengatasi risiko keamanan. Ini termasuk memahami praktik-praktik terbaik dalam pengelolaan kata sandi, keamanan email, dan penggunaan perangkat lunak keamanan. Dengan memberikan pelatihan keamanan data secara berkala, organisasi dapat meningkatkan kesadaran karyawan tentang pentingnya keamanan informasi dan membantu mengurangi risiko keamanan yang disebabkan oleh kesalahan manusia.

Selain kurangnya pemahaman dan pelatihan, kesadaran karyawan tentang keamanan data juga penting untuk dipertimbangkan. Tanpa kesadaran yang cukup, karyawan mungkin tidak menyadari pentingnya melindungi data sensitif atau mungkin tidak menganggap serius ancaman keamanan yang ada. Ini dapat mengakibatkan praktik-praktik yang tidak aman, seperti menggunakan kata sandi yang lemah atau berbagi informasi sensitif melalui email tanpa enkripsi. Oleh karena itu, penting bagi organisasi untuk meningkatkan kesadaran karyawan tentang keamanan data melalui berbagai cara, termasuk menyediakan sumber daya pendidikan dan mengkomunikasikan kebijakan keamanan dengan jelas kepada karyawan.

Selain memberikan pelatihan dan meningkatkan kesadaran, organisasi juga perlu memastikan bahwa kebijakan dan prosedur keamanan data mereka mudah dipahami dan diterapkan oleh karyawan. Kebijakan yang rumit atau tidak jelas dapat menyebabkan kebingungan dan kesalahan dalam penerapan, meningkatkan risiko keamanan yang tidak perlu. Oleh karena itu, penting bagi organisasi untuk menyediakan panduan yang jelas dan mudah diakses tentang kebijakan dan prosedur keamanan data mereka, serta memberikan dukungan dan bimbingan kepada karyawan dalam memahami dan mengikuti kebijakan tersebut.

Pembahasan

Temuan Audit

Temuan audit merupakan hasil yang sangat penting dalam mengevaluasi efektivitas tata kelola teknologi informasi, termasuk keamanan data, dalam suatu organisasi. Dalam konteks Plasa Telkom Penajam, temuan audit menunjukkan bahwa masih ada beberapa aspek keamanan data yang perlu ditingkatkan. Sebagaimana yang terungkap dari audit, kekurangan atau celah dalam sistem keamanan data dapat menjadi ancaman serius bagi integritas dan kerahasiaan informasi yang dikelola oleh Plasa Telkom Penajam.

Salah satu temuan audit yang mungkin ditemukan adalah kurangnya kebijakan dan prosedur keamanan data yang komprehensif. Kebijakan dan prosedur yang tidak memadai atau belum diterapkan dengan baik dapat meninggalkan celah dalam perlindungan data, meningkatkan risiko kebocoran atau pencurian informasi. Dalam hal ini, audit dapat membantu mengidentifikasi kekurangan dalam kebijakan dan prosedur yang ada, serta memberikan rekomendasi untuk meningkatkannya agar lebih sesuai dengan kebutuhan dan tantangan keamanan yang dihadapi oleh Plasa Telkom Penajam.

Selain itu, temuan audit juga dapat mencakup evaluasi terhadap kontrol keamanan yang ada. Dalam beberapa kasus, kontrol keamanan yang seharusnya efektif mungkin tidak berfungsi dengan baik atau tidak diterapkan secara konsisten. Contohnya, mungkin ada kesenjangan dalam manajemen hak akses pengguna, yang memungkinkan pengguna tidak berwenang untuk mengakses informasi sensitif. Atau, sistem deteksi intrusi mungkin tidak diatur untuk mengidentifikasi serangan yang lebih baru atau lebih canggih. Dengan mengidentifikasi

kelemahan dalam kontrol keamanan yang ada, audit dapat membantu Plasa Telkom Penajam untuk mengambil tindakan yang tepat untuk memperbaiki atau memperkuat kontrol tersebut guna meningkatkan perlindungan data mereka.

Selain itu, temuan audit juga dapat menyoroti kekurangan dalam kesadaran dan keterampilan keamanan karyawan. Karyawan yang tidak memahami pentingnya keamanan data atau tidak memiliki pengetahuan yang memadai tentang praktik-praktik keamanan yang tepat dapat menjadi faktor risiko yang signifikan. Misalnya, karyawan mungkin tidak mematuhi kebijakan password yang kuat atau mungkin tidak waspada terhadap potensi serangan phishing atau malware. Dalam hal ini, audit dapat merekomendasikan program pelatihan keamanan tambahan atau inisiatif kesadaran untuk meningkatkan pemahaman dan keterampilan keamanan karyawan.

Dengan menganalisis temuan audit dan mengambil tindakan yang tepat berdasarkan rekomendasi audit, Plasa Telkom Penajam dapat meningkatkan keamanan data mereka secara signifikan. Ini termasuk mengembangkan dan menerapkan kebijakan dan prosedur keamanan yang lebih kuat, memperkuat kontrol keamanan yang ada, dan meningkatkan kesadaran dan keterampilan keamanan karyawan melalui pelatihan dan program kesadaran. Dengan demikian, audit tidak hanya menjadi alat untuk mengidentifikasi masalah, tetapi juga sebagai langkah awal untuk meningkatkan perlindungan data secara keseluruhan dan mengurangi risiko keamanan yang mungkin dihadapi oleh Plasa Telkom Penajam.

Aspek Keamanan Data Yang Perlu Ditingkatkan

Kebijakan dan prosedur keamanan data memegang peran krusial dalam melindungi integritas, kerahasiaan, dan ketersediaan informasi yang dimiliki oleh suatu organisasi. Namun, temuan audit menunjukkan bahwa Plasa Telkom Penajam masih memiliki beberapa kekurangan dalam aspek keamanan data mereka. Salah satu permasalahan utama yang diidentifikasi adalah bahwa kebijakan dan prosedur keamanan data yang ada belum mencakup semua aspek keamanan data yang diperlukan.

Sebuah kebijakan dan prosedur keamanan data yang baik harus merangkul seluruh spektrum keamanan data, termasuk keamanan fisik, keamanan jaringan, dan keamanan aplikasi. Keamanan fisik mencakup langkah-langkah perlindungan terhadap akses fisik yang tidak sah, seperti pencurian, sabotase, atau kerusakan perangkat keras yang dapat menyebabkan kehilangan data. Keamanan jaringan mencakup perlindungan terhadap akses jaringan yang tidak sah, seperti serangan siber dan penyadapan. Terakhir, keamanan aplikasi mencakup perlindungan terhadap akses aplikasi yang tidak sah, seperti serangan siber dan kesalahan manusia dalam penggunaan aplikasi.

Ketidakcakupan semua aspek keamanan data dalam kebijakan dan prosedur Plasa Telkom Penajam dapat memberikan celah bagi potensi risiko keamanan yang tidak terdeteksi. Misalnya, jika kebijakan hanya fokus pada keamanan jaringan tanpa memperhatikan aspek keamanan fisik, maka ancaman pencurian fisik atau kerusakan perangkat keras mungkin tidak tercakup dengan baik. Oleh karena itu, penting untuk memperbarui kebijakan dan prosedur keamanan data agar mencakup seluruh aspek keamanan data yang relevan dengan operasi organisasi.

Infrastruktur teknologi informasi yang tidak memenuhi persyaratan keamanan data merupakan tantangan serius yang perlu diatasi. Infrastruktur yang aman adalah pondasi utama dalam melindungi data dari berbagai ancaman, termasuk serangan siber, kesalahan manusia, dan bencana alam. Temuan audit menunjukkan bahwa Plasa Telkom Penajam perlu melakukan evaluasi mendalam terhadap keamanan infrastruktur teknologi informasinya. Kelemahan dalam infrastruktur dapat menciptakan celah yang memungkinkan penyerang mengakses dan mencuri data secara tidak sah. Oleh karena itu, diperlukan investasi dan perbaikan pada infrastruktur untuk memastikan keamanan data yang optimal.

Selain itu, temuan audit menyoroti bahwa proses-proses keamanan data di Plasa Telkom Penajam belum terintegrasi dengan baik. Integrasi yang efektif antara proses-proses keamanan data dapat memberikan perlindungan yang lebih solid terhadap ancaman. Sebagai contoh, integrasi antara manajemen hak akses pengguna dengan

sistem deteksi intrusi dapat memberikan keamanan lebih baik terhadap akses tidak sah atau aktivitas mencurigakan. Oleh karena itu, diperlukan upaya untuk meningkatkan integrasi antarproses keamanan data agar saling melengkapi dan memperkuat satu sama lain.

Tidak kalah pentingnya, temuan audit menyoroti bahwa sumber daya manusia Plasa Telkom Penajam belum memiliki pemahaman yang cukup mengenai keamanan data. Pemahaman yang kurang dapat menjadi faktor risiko utama, karena kesalahan manusia sering kali menjadi penyebab utama insiden keamanan. Penting untuk memberikan pelatihan keamanan data secara berkala kepada karyawan agar mereka dapat memahami praktik-praktik keamanan yang benar dan mengidentifikasi potensi risiko keamanan. Kesadaran karyawan tentang pentingnya keamanan data juga harus ditingkatkan melalui kampanye kesadaran dan edukasi yang terarah.

Dalam rangka mengatasi temuan audit ini, Plasa Telkom Penajam perlu mengambil langkah-langkah perbaikan yang terencana dan komprehensif. Ini mencakup pembaruan kebijakan dan prosedur keamanan data, investasi dalam perbaikan infrastruktur teknologi informasi, peningkatan integrasi antarproses keamanan data, dan penyelenggaraan program pelatihan keamanan data yang efektif. Dengan melakukan perubahan ini, Plasa Telkom Penajam dapat meningkatkan keamanan data mereka secara menyeluruh dan mengurangi risiko terhadap potensi ancaman keamanan di masa depan.

KESIMPULAN

Berdasarkan hasil penelitian di Plasa Telkom Penajam, dapat disimpulkan bahwa masih ada beberapa aspek keamanan data yang perlu ditingkatkan demi menjaga integritas dan kerahasiaan informasi yang dikelola oleh perusahaan.

Temuan ini menunjukkan bahwa ada potensi ancaman terhadap keamanan data yang dapat membahayakan operasi dan reputasi perusahaan. Ini berarti bahwa masih ada celah dalam perlindungan data, yang dapat meningkatkan risiko kebocoran atau pencurian informasi penting.

Selain itu, infrastruktur teknologi informasi yang belum memenuhi standar keamanan dapat menjadi celah bagi penyerang untuk mengakses dan mencuri data. Oleh karena itu, disarankan untuk meningkatkan kesadaran dan pemahaman karyawan tentang pentingnya keamanan data melalui pelatihan dan sosialisasi yang teratur.

Terakhir, penting untuk memberikan pelatihan keamanan data yang komprehensif kepada semua karyawan, serta melakukan evaluasi terhadap efektivitas proses-proses keamanan secara berkala.

Dengan menerapkan langkah-langkah perbaikan ini, Plasa Telkom Penajam dapat meningkatkan keamanan data mereka secara keseluruhan, mengurangi risiko terhadap potensi ancaman keamanan di masa depan, dan menjaga kepercayaan pelanggan serta pemangku kepentingan lainnya.

UCAPAN TERIMAKASIH

Ucapan terima kasih diberikan kepada seluruh keluarga, teman-teman, dosen dan seluruh civitas akademika STMIK Borneo International Balikpapan serta rekan-rekan seperjuangan yang telah memberikan dukungan moril dan materi terselenggaranya penelitian ini.

DAFTAR PUSTAKA

Andry, Johanes Fernandes, and Rengga Eko Riwanto. 2019. “Audit TI Pada PT Sinar Aceh Menggunakan Framework Cobit 4.1.” JBASE - Journal of Business and Audit Information Systems 2 (1). https://doi.org/10.30813/.v2i1.1498.

Andry, Johanes Fernandes, and Bobby Sanjaya. 2017. “AUDIT TATA KELOLA TI PADA PT. PORTO INDONESIA SEJAHTERA MENGGUNAKAN COBIT PADA DOMAIN PO.” Jurnal Ilmiah Teknologi Infomasi Terapan 3 (3). https://doi.org/10.33197/jitter.vol3.iss3.2017.136.

Hambali, Hambali. 2021. “PENERAPAN DOMAIN MONITOR AND EVALUATE FRAMEWORK COBIT 4.1 DALAM PELAKSANAAN AUDIT SISTEM INFORMASI.” JOURNAL OF SCIENCE AND SOCIAL RESEARCH 4 (2). https://doi.org/10.54314/jssr.v4i2.608.

Imami, Liliandara Wahyu, Suprapto, and Yusi Tyroni Mursityo. 2019. “Audit Tata Kelola Teknologi Informasi Pada Dinas Komunikasi Dan Informatika (DISKOMINFO) Kota Bandar Lampung Menggunakan Kerangka Kerja COBIT 4.1 Domain Plan and Organise Dan Acquire and

Implement." *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer* 2 (9).

Lesmono, Ibnu Dwi, and Denny Erca. 2018. "Tata Kelola Teknologi Informasi Dengan Metode COBIT 4.1 (Studi Kasus : PT.IMI)." Jurnal Kajian Ilmiah 18 (1). https://doi.org/10.31599/jki.v18i1.198.

Muharom, Ikhsan, and Darya Setia Nugraha Nugraha. 2020. "Audit Tata Kelola Teknologi Informasi Dan Proses Investasi Sistem Penerimaan Peserta Didik Baru (SPPDB) Dengan Pendekatan Framework COBIT 4.1 (Studi Kasus …." … Accounting Literacy Journal 1 (1).

Purwaningrum, Oktania. 2021. "STUDI LITERATUR : FRAMEWORK COBIT 5 PADA TATA KELOLA TEKNOLOGI INFORMASI." SCAN - Jurnal Teknologi Informasi Dan Komunikasi 16 (2). https://doi.org/10.33005/scan.v16i2.2598.

Saryoko, Andi, Agus Junaidi, Sopiyan Dalis, and Fitrayuda Rivaldy. 2021. "Tata Kelola Sistem Informasi PT. Maspion Menggunakan Framework Cobit 4.1 Domain Acquire And Implement." Paradigma - Jurnal Komputer Dan Informatika 23 (2). https://doi.org/10.31294/p.v23i2.11419.

Sayekti, Widya, Juliana Ermawati, Renny Sari Dewi, and Penulis Korespondensi. 2020. "Audit Tata Kelola Teknologi Informasi Pada Pengukuran Kinerja Dan Kapasitas Bandwidth Berdasarkan Cobit 4.1." Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK) 7 (1).

Sinaga, Rizwansyah, and Iman Permana. 2023. "AUDIT SISTEM INFORMASI TERHADAP PT ENSEVAL MENGGUNAKAN COBIT 4.1 DOMAIN ACQUIRE IMPLEMENTATION." Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi) 7 (1). https://doi.org/10.30998/semnasristek.v7i1.6236.

Tomas, Jordi, and Johanes F. Andry. 2020. "Audit Tata Kelola Teknologi Informasi Pada PT. EMD Menggunakan COBIT 4.1 Dan BSC." KALBISCIENTIA Jurnal Sains Dan Teknologi 6 (2). https://doi.org/10.53008/kalbiscientia.v6i2.47.

Tukino, Faqih Pratama Muthi, and Aditia Agustian. 2021. "ANALISIS PENERAPAN TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 4.1 PADA PEMINJAMAN BUKU PERPUSTAKAAN 'STUDI KASUS PERPUSTAKAAN KABUPATEN KARAWANG.'" BUANA ILMU 5 (2). https://doi.org/10.36805/bi.v5i2.1812