Artikel Arsitektur Aplikasi Security

MATAKULIAH. :Arsikterkturentreprise

KELAS. : C

Supangat M,kom,ITIL,COBIT

NAMA : JULIUS FERDINAND L

NBI 1461700234

PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS 17 AGUSTUS 1945 SURABAYA

Latar Belakang

Aplikasi mengenai informasi sangat berkembang pesat di dunia modern yang sangat berpengaruh pada kemajuan teknologi. Semakin banyak aplikasi yang berkembang banyak perusahan mendesain aplikasi yang bertujuan untuk mengaktualisakan proses bisnis dan mempermudah penggunaan untuk berjalannya bisnis pada perusahaan. Setiap aplikasi memiliki sistem security yang bertujuan agar tidak semua mendapatkan akses dari perusahan tersebut. Hal tersebut karena banyaknya kejahatan yang dialami oleh perusahaan salah satu contoh kejahatan yaitusiber,kejahatansibermerupakankejahatanyangpalingterpopulerditahun2019yaitukas us pembobolan perusahaan yang bernama “Cryptocurrency Binanceyang”. Persusahaan Cryptocurrency Binanceyang merupakan perusahaan penukaran dalam nidang mata uang kripto. Cryptocurrency Binanceyang merupakan perusahaan yang terkenal di dunia. Binance di rugikan olehhackeryangmembuatperusahaanCryptocurrencyBinanceyangmengalamikerugianse besar
7.00 Bitcoin dengan total senilai USD 41 juta (Rp 588 miliar). Penyadap atau hacker menggunakan berbagai jenis teknik serangan untuk melakukan aksinya. Seperti menyebarkan virus dan menggunakan serangan phishing dalam mendapatkan informasi keamanan yang dibutuhkannya. Dengan cara tersebut ternyata hacker bisa mengakses “hot wallet” milikBinance.

Mengenai arsitektur teknologi keamanan, IdM dan kebijakan diterapkan pada arsitektur yang bertujuan untuk mengatur semua kebijakan dan penegakan sumber daya melalui layanan yang diberikan, setiap perangkat jaringan keamanan akan memiliki kebijakan format, mungkin dalam bentuk XML yang dimasukan ke dalam konfigurasi sistem perangkat keamanan, oleh karena itu agen yang dapat diinstal pada perangkat teknologi seperti server, sistem penyimpanan, router dan switch untuk melengkapi konsep penerapan arsitektur teknologi keamanan, agen ini akan memeriksa apakah permintaan yang dikirim oleh pengguna dan aplikasi sesuai dengan kebijakanyangditetapkanolehpenggunayangditerapkan,darikecukupanidentitaspenggun adan aturan (peran) yang ditetapkan oleh mesin PDP Arsitektur teknologi yang dirancang, berdasarkan literatur yang dipelajari dan ana lisa dari keadaan perusahaan saat ini, berikut Tabel tersebut akan mewakili dan menjelaskan kapabilitas perusahaan setelah implementasi arsitektur teknologi keamanan, kapabilitaskapabilitas tersebut

nantinya harus bisa diuji dengan melibatkan kontrol yang terkait dengan layanan tersebut, untuk itu perlu disusun dan diuraikan deskripsikemampuan apasajayangbisadilakukanolehPMAyangmelakukanfungsiprovisioningdansecurityservices

yang melakukan layanan keamanan sesuai dengan penerapan Security Technology Architecture yang dirancang.

Maka dari itu artikel ini di tunjukan untuk mengetahui pentingnya keaman pada aplikasi keamananatauApplicationArchitectureSecurityagarperusahaantidakmengalamiyangnamanya kerugian yang diakibatkan olehhacker.

Tinjauan Pustaka

Tinjauan pustaka yang dilakukan pada karya ilmiah ini dihimpun melalui proses mencari beragam literasi, kemudiaan menelaah dan mengambil tulisan atau hasil melalui artikel jurnal ilmiah.Setelahitupenulisterlebihdahulumempelajaripenelitianterdahuludarijurnalilmiahguna memperkaya terkait topik yang digunakan. Karya ilmiah ini keamanan aplikasi yang banyak lakukan oleh penelitian sebelumnya. Berikut ini beberapa penelitian terdahulu sebagai referensi dalam memperkaya kajian padapenelitian:

Penelitian ini menjelaskan berbagai teknik untuk menguji keamanan aplikasi. Salah satu teknik pengujian yang digunakan adalah pengujian statis dan pengujian dinamis. Pengujian statis menggunakan sudut pandang kotak putih, sedangkan pengujian dinamis menggunakan sudut pandangkotakhitam.ProsespengujiankeamananDASTadalahprosespengujianaplikasidi mana perangkat lunak aplikasi dalam status Penyelidikan ini menjelaskan pengujian statis aplikasi Android,atauSAST.Padapenelitianini,pengujiandilakukandenganMobileSecurityFramework (MobSF) sebagai alat uji SAST. MobSF dipilih sebagai alat pengujian karena MobSF memiliki kemampuan untuk melakukan analisis statis dan dinamis dengan menampilkan analisis izin, melihat kode sumber aplikasi yang diuji, dan melihat file dan malware yang terdapat dalam kode sumber yang ada. Pengujian statis hanya berfokus pada analisis kode sumber, sehingga pengujian tidakdilakukansecaramenyeluruh.DASTmemilikikelebihansaatmengujiaplikasiyangterbukti sebagaiSAST.

Penelitian Kedua Dari hasil penelitian arsitektur teknologi keamanan dari hasil pembahasan penelitian arsitektur teknologi keamanan untuk PT “N” adalah studi tentang penyusunan arsitektur teknologi keamanan yang sesuai untuk enterprise. Karena tingkatkesulitan pengetahuan keamanan yang tinggi, PT "N" belum menerapkan teknologi keamanan berbasis kebijakan.3.MembangundanmerancangarsitekturteknologikeamananuntukPT“N”dengan

menggunakan framework Enterprise Security Architecture (ESA) dari Network Applications Consortium (NAC) yang kini telah tergabung dalam Open Group. Untuk meningkatkan kualitas desain teknologi keamanan yang memadai di PT "N", analisis yang cermat terhadap arsitektur TI perusahaan saat ini, penyusunan profil risiko perusahaan, kesimpulan pemeriksaan validasi pada analisiskesenjanganadalahdiperlukanuntukmelakukanpenilaianrisiko.Untukmemitigasiri siko keamanan TI, PT “N” dapat menyiapkan dan merancang arsitektur teknologi keamanan berdasarkan framework OpenGroup ESA yang melalui 4 (empat) fase penting, yaitu: kompilasi dan perancangan framework konseptual, pengembangan framework arsitektur konseptual ,desain arsitektur logis dan desain arsitekturfisik.

Menurut National Institute of Standards and Technology (NIST), Cloud computingadalah model komputer yang menawarkan kemudahan, kemudahan, dan akses sesuai permintaan untuk mengakses dan mengkonfigurasi sumber daya komputer (jaringan, server, penyimpanan,aplikasi, dan layanan). Mulai cepat tanpa banyak interaksi dengan penyedia layanan Jenis layanan cloud computingdibagimenjaditigajenis,yaituInfrastructureasaService(IaaS),PlatformasaServic e (PaaS) dan Software as a Service(SaaS).

Infrastruktur sebagai Layanan (IaaS): IaaS menyediakan penyimpanan atau sumber daya komputasiyangdapatdiaksessecaraonline.MisalnyaGoogleCloudStorage,MicrosoftWind ows Azure Storage dan Dropbox. Platform as a Service (PaaS): PaaS menawarkan platform kepada pelanggan untuk menjalankan aplikasi. Biasanya, PaaS menyediakan alat pengembangan perangkat lunak untuk membangun aplikasi di platform. Jenis aplikasi umum yang umumnya berjalan pada platform adalah script (seperti PHP, Python) atau bytecode (seperti C#).Contoh penyedia PaaS seperti Google App Engine atau Microsoft Azure. Software as a Service (SaaS): SaaS menawarkan akses penuh ke perangkat lunak atau aplikasi. Aplikasi ini adalah serveremail, klien email, atau editor dokumen. Layanan SaaS umumnya dapat diakses melaluibrowse

Perangkat teknologi informasi perusahaan berupa server menggunakan berbagai platform teknologi sistem operasi, seperti sistem operasi dengan Windows Server, HPUX, Redhat, dll, dalam kaitannya dengan teknologi database dengan berbagai sistem manajemen database seperti

Oracle, DB2, MySQL , SQL-Server dan lain-lain. Selain menggunakan teknologi modern untuk pengoperasian server secara real-time, beberapa server telah mengadopsi teknologi clustering (ketersediaantinggidanmirroring).Teknologiinibergunaagartidakmenghentikanoperasiserver karena server terkunci, yang dapat mencegah pengguna dan aplikasi mengaksesserver.

Selainitu,sangatpentingbahwahampirsemuaperangkatservertidakmemilikiperangkat lunak keamanan seperti antivirus, antispam, dll., yang berarti bahwa banyak server tidak diinstal dengan antivirus, antispam, atau keamanan yang memadai. Software baik pada server berbasis platform. Windows serta yang berbasis platform Unix dan Linux. Untuk menjelaskan informasi tentang aset aplikasi dan perangkat keras yang digunakan, tabel berikut berisi informasi tentang perangkat server di bidang TI, yang merupakan hasil analisis dan pemrosesan dalam tabel ringkasan yang mewakili platform teknologi yang digunakan olehaplikasi.

Diagram arsitektur fisik lengkap harus menggambarkan zonasi keamanan TI dan semua perangkat jaringan di luar dan di dalam lingkungan TI jaringan, mewakili desain standar yang sesuai dengan arsitektur jaringan TI di perusahaan. Melalui proses panjang yang akhirnya dapat mengidentifikasi semua perangkat jaringan dan keamanan di perusahaan didasarkan pada nama host pada semua perangkat yang terhubung, nama host Nama host diidentifikasi menggunakan referensi dari data inventaris router, switch, firewall dll. , misalnya

jaringan, perangkat di kota Bandung di lingkungan pusat data perusahaan melalui perangkat komunikasi berikut: Dari sisi Bandung, pengguna terhubung ke perangkat router BDG01POPR1 / BDG01POPR2, perangkat ini melalui. terhubung ke router di Jakarta melalui jaringan POP pada perangkat router CIG01COREBDR1 / CIG01COREBDRF2 dan dirutekan melalui router CIG01POPR1 / CIG01POPR2 untuk mengakses jaringan internal di pusat data. Di luar jaringan POP antar kota terdapat jaringan fiber optic yang menghubungkan tower DEA (user area)dandatacenter,linktersebutterhubungdenganjaringanintifiberopticHuawei,jadidiagram jaringan ini juga menggambarkan sisi luar jaringan, yang terhubung dengan koneksi Internet, termasuk virtual private network (VPN) untuk fasilitas akses jarak jauh bagi karyawan dan pihak ketiga seperti penyedia afiliasi,dll.

Arsitektur aplikasi untuk mendukung sistem bisnis perusahaan merupakan aplikasi yang terintegrasi,hasilobservasilapangansecaramendalampadaareayangterkaitdenganproses bisnis utama terdiri dari beberapa jenis aplikasi ITBSS yang mendukung sistem bisnis perusahaanyaitu:

EAI, SAP, CRM, CCBS, ODS, Mediasi, Carmen, CLMandLD, Penyediaan, EDW, Interkoneksi, ECM, Penyelesaian IR, dan Middleware Pesan. Gunakan proses bisnis yang dijelaskan untuk menunjukkan bahwa aplikasi ini kompatibel dengan sistem bisnis perusahaan. mengintegrasikan dan berkomunikasi satu sama lain, baik melalui aplikasi EAI maupun langsung dari satu aplikasi ke aplikasi lainnya. EAI adalah aplikasi bisnis yang bertanggung jawab untuk melakukan proses permintaan dan respons untuk menghubungkan aplikasi terkait dengan proses bisnis utama perusahaan, seperti aplikasi CLMandLD, ECM, dan EDW. Aplikasi ini tidak hanya melayani pengguna internal seperti karyawan perusahaan dan aplikasinya, tetapi juga transaksi informasi dengan pengguna eksternal dan elemen jaringan (NORTHEAST).NE berada di sisi perangkat jaringan telekomunikasi, sebenarnya aplikasi ini terutama digunakan untuk memproses data dari NE.Di dalam penelitian ini, akan ada 4 serangan keamanan yang akan diteliti, di mana serangan tersebut akan menyebabkan kebocoran dan kehilangan data, Serangan-serangan keamanan tersebut diantaranya:

1. Snooping Attack Snooping attack adalah suatu kondisi dimana penyerang akan melihat paket data mengalir ke dalam jaringan. Serangan snooping bersifat pasif, penyerang tidak akan mengubah paket data yang telah dilihatnya. Penyerang akan mengambil konten yang tersimpan di komputer pengguna, yang mengakibatkan hilangnyadata.
2. Serangan analisis lalu lintas Serangan analisis lalu lintas adalah serangan oleh penyerang yangmenganalisispergerakanlalulintasuntukmengekstrakinformasidaripolalalulintas. Dalam serangan ini, penyerang dapat melihat semua konten yang diminta oleh pengguna sehingga penyerang dapat menemukan konten yang tersedia di server. Jika konten itu berharga baginya, penyerang dapat memasuki server untuk mengambil kontentersebut.
3. Serangan Denial of Service (DOS) Serangan DoS adalah serangan yang bertujuan untuk membuat server atau situs web tidak dapat diakses oleh pengguna lain. Contoh serangan yang mungkin terjadi adalah membanjiri jaringan dengan paket sampah. Menerapkan serangan ini menyebabkan server penyedia cloud gagal sehingga dapat dengan mudah diakses olehpenyerang.
4. Man-In-The-Middle (MITM) Attack Si penyerang akan berada di tengah-tengah user dan server cloud yang sedang berkomunikasi untuk menginisiasi man-in-the-middle attack. Serangan ini adalah salah satu penyebab utama kebocoran data,

hal ini dikarenakan si penyerang dapat mengambil data yang mengalir antara user dan server penyediakonten

dalam cloud. User dan server tidak dapat mengetahui bahwa ada seseorang di tengah- tengah mereka yang sedang mengambil data-data tersebut.

Pada penelitian ini, teknik-teknik keamanan pada cloud computing dianalisis dan dibandingkan dalam hal kemampuan menangani ke-empat serangan-serangan keamanan di atas. Teknik-teknik keamanan yang akan diteliti mencakup teknik yang sudah diterapkan di cloud computing maupun teknik yang belum diterapkan. Beberapa konsep (Current Cloud Computing Network) sistem keamanan jaringan yang diterapkan pada cloud computing saat ini adalah:

a. VPN (Virtual Private Network) VPN adalah sebuah teknik yang digunakan untuk memastikan bahwa jaringan publik dapat mengakses jaringan privat, dalam kasus ini adalah jaringan cloud, secaraaman.

b. Kebijakan dan Konfigurasi Keamanan Pada Cloud Computing Penyedia layanan cloud computingdapatmenawarkanmekanisme-mekanismekeamananpadapelanggannya.Mekanisme keamanan ini dikonfigurasi berdasarkan permintaan pelanggan. Contoh mekanisme keamanan yang bisa diimplementasi pada cloud computing adalah autentikasi proses dan proses enkripsi-dekripsi.

c. Firewall Firewall adalah sebuah mekanisme yang berfungsi untuk memfilter paket-paket data atau user yang tidak sesuai dengan kebijakan penyedia cloud computing. Firewall dapat berupa software maupun hardware. Dengan melakukan pemfilteran tersebut, firewall dapat mencegah serangan dari dalam maupun dari luar jaringancloud.

Dari ketiga konsep sistem keamanan pada cloud computing diatas, ada juga beberapa sistem keamanan masa depan (Future Cloud Computing) yang sangat memungkinkan untuk di Implementasikan pada cloud computing, Sistem ini sering disebut NEBULA. NEBULA adalah sebuah arsitektur jaringan cloud masa depan yang bertujuan untuk meningkatkan keamanan dan fleksibilitas dari arsitektur jaringan cloud masa kini, salah satu upaya untuk meningkatkan keamanan pada NEBULA adalah mekanisme keamanan yang kuat telah ada di dalam-nya, sehingga apabila muncul serangan keamanan yang baru, maka mekanisme keamanan tersebut dapat beradaptasi secara fleksibel, diantaranya:

A. Onion routing Onion routing adalah teknik yang dapat menyembunyikan alamat IP dari pengguna. NEBULA dapat bekerja di jaringan Internet dan secara fleksibel menerapkan mekanismekeamanan,kemudianperuteanbawangdapatdiimplementasikandiNEBULA.
B. ProofofPath(PoP)lahirPoPadalahmekanismeuntukmemastikanbahwajaluryangakan dicakupolehpaketdatatelahdiautentikasi.Olehkarenaitu,paketmelaluijalurlegaluntuk menghindari paket banjir di NEBULA. Jaringan atau dikenal dengan packetflooding.
C. Proof of Consent (PoC) PoC adalah mekanisme untuk memastikan bahwa pengguna dan paket yang mengalir di NEBULA telah diautentikasi. Oleh karena itu tidak ada pengguna ilegal dalam NEBULA. Bahkan jika serangan terjadi dari dalam NEBULA, itu dikenali dan diperbaiki lebih cepat.d. Teknik kriptografi ICING ICING adalah sebuah teknik kriptografiyangberfungsiuntukmelakukanprosesenkripsidandekripsipadapaket-paket data yang mengalir di dalamNEBULA.

2. Melakukan Assesment Kegiatan Assesment berupa observasi yang penulis lakukan meliputi kegiatan pemanfaatan informasi sehari-hari oleh unsur administrasi kampus, melakukan wawancara dan melakukan asesmen sebagai bagian dari proses audit berdasarkan manajemen investasi teknologi informasi dan juga harapan ideal padapandanganmu.

3. Fase A: Visi arsitektur Menentukan kesepakatan posisi tentang pentingnya EA untuk pencapaiantujuanorganisasi,yangdirumuskandalambentukstrategidariruanglingkuparsitektur yang akandikembangkan.

4. Fase B: Arsitektur Bisnis Pada fase ini, mengembangkan tujuan dan deskripsi arsitektur bisnis organisasi saat ini, kemudian mengembangkan arsitektur yang ada berdasarkan hasil analisis kondisi saatini.

5. Fase C: Arsitektur sistem informasi Pada fase ini, penekanannya adalah pada berfungsinya arsitektur sisteminformasi

Fase A: Visi arsitektur Kegiatan yang dilakukan pada fase ini adalah menentukan kesepakatan pemahaman untuk menjadi bagian dari pemangku kepentingan untuk

mencapai tujuan organisasi dan menentukan ruang lingkup arsitektur yang akan dibangun dengan diagram rantai nilai, dan mengonsepkan solusi bisnis berdasarkan sistem informasi berdasarkan kondisi saat ini dalam bentuk dari sebuah diagram.

Phase B: Business Architecture Pada tahap ini menggambarkan arsitektur organisasi saat ini dan mengembangkannya dengan menyusun strateginya agar dapat mencapai tujuan bisnis yang telah ditetapkan, dalam bentuk diagram.

Phase C: Information System Architecture Dalam fase ini melibatkan dua arsitektur, yaitu arsitektur data dan arsitektur aplikasi, dengan berfokus pada identifikasi dan definisi aplikasi dan data yang mendukung arsitektur bisnis.

- ArsitekturDataMemetakanhubunganentitasdanfungsibisnisdalamorganisasi(business functionmatrix)
- Arsitektur Aplikasi Melakukan proses revisi pada konsep solusi bisnis (pada gambar 7) dan membuat model referensi teknis standar TOGAF yang mengacu pada diagramkonsep solusi bisnis.

PhaseD:TechnologyArchitectureMembangunarsitekturteknologiyangdiinginkan,dimulaidari penentuan jenis kandidat teknologi yang diperlukan, baik berupa perangkatlunak

Kesimpulan dan Saran

Dari hasil pembahasan yang telah dilakukan, maka dapat disimpulkan bahwa:

1) Konsep sistem keamanan yang telah terimplementasikan saat ini (Current Cloud Computing Network) belum cukup untuk mengatasi seluruh serangan keamanan yang telah diteliti, hal ini dikarenakan tidak fleksibelnya jaringan cloud computing untuk mengaplikasikan mekanisme keamanan.

2) Konsep sistem keamanan pada NEBULA (Future Cloud Computing) diantaranya: PoC, PoP, dan ICING jauh lebih baik dalam hal mengatasi beberapa serangan yang telah diteliti, yakni Snooping attack, DoS attack dan man-in-the-niddle attack. Konsep sistem keamanan ini sangat memungkinkan menggunakan pemakaian onion routing yang dapat diimplementasikan dengan cepat pada nebula untuk mengatasi serangan Trafficanalysis.

3) Dibalik kelebihan teknologi cloud computing, privacy data merupakan hal penting dalam sebuahorganisasiterutamapenggunaCloudComputingyangharusmemperhatikanaspekproteksi datayangdisediakanolehprovider.tidakmenutupkemungkinandatayangtersimpandalamcloud computing merupakan data penting dan rahasia yang tidak semua orang bisa mengaksesnya. Jika provider mengalami down, data organisasi terancam hilang, tidak dapat diakses, atau dapat direcovery namun tidak utuh, Hal tersebut tentu saja dapat merugikan pihak user. Dari hasil pembahasan, penulis menyimpulkan bahwa user sangat perlu bersifat selektif untuk memilih atau menentukan provider penyedia layanan Cloud Computing. Langkah terbaik yakni menentukan Provider penyedia Layanan sesuai pemetaan standard keamanan yang perlu diperhatikan oleh penyedia cloudcomputing.

Saran

Berdasarkanhasilpenelitiandankesimpulanyangtelahdijelaskanpadabagiansebelumnya. Maka, saran peneliti dapat disajikan sebagaiberikut:

1. Untuk akademisi, diharapkan penelitian ini dapat memberikan sumbangsih pengetahuan terkait Perusahaan mengenai Aplikasi keamanan, sehingga penelitian ini dapat memberikan suatu pandangan dan pertimbangan baru di masa mendatang. Penelitian ini tentunyamemilikibanyakkekurangan,olehsebabitudiharapkanbagipenulisankaryail muah berikutnya dapat menggunakan sudut pandang yang berbeda untuk menyempurnakannya.Penulisberikutnyadapatmenggunakananalisisresepsiatauanalisis lain agar penelitian lebih komprehensif.
2. UntukPerusahaanterutamapadaperusahaanyangmemilikibisnisbesarsebaiknyabe kerja sama memberikan keaman untuk perusahaan dan memberikan kesempatan kepada paraIT untuk mengembangkan aplikasi guna menjaga keamanan bisnis. Selain itu, harapannya semoga pemilik perusahaan memiliki beberapa pertimbangan yang bermanfaat bagibisnis dalamperusahaan
3. UntukPerusahaansebaiknyamempertimbangkanresikodankonsekuensiuntukkea manan Perusahaan. Para pemilik Usaha harus mempertimbangkan aplikasi yang menunjang agar sistem berjalan sesuai dengan harapan. Apabila sudah sesuai maka harus di perhatikan lebih lagi dan mengikuti perkembanganzaman.

Daftar Pustaka

Perancangan Security Technology Architecture PT. “N” Menggunakan Kerangka Kerja Enterprise Security Architecture Sriwisnu Noloadi Program Studi Magister Sistem Informasi Fakultas Pascasarjana Universitas Komputer Indonesia

PENGUJIAN CELAH KEAMANAN APLIKASI BERBASIS WEB MENGGUNAKAN TEKNIK PENETRATION TESTING DAN DAST (DYNAMIC APPLICATION SECURITY TESTING) Bagus Wicaksono1, Rr. Yuliana Rachmawati Kusumaningsih2, Catur Iswahyudi3 1, 2, 3 Jurusan Informatika, FTI, IST AKPRIND

ARTIKEL PUBLIKASI MAXIMUM SECURITY PRISON DESIGN Pendekatan Pada Humanis desain dan Eko Arsitektur Universitas Muhammadiyah Surakarta Disusun Oleh: Rizqi Azhar Al Habib

HomeSecurityMenggunakanArduinoBerbasisInternetOfThings.FazrolRozi1*,Hidra Amnur1, Fitriani1, Primawati2 1Jurusan Teknologi Informasi, Politeknik Negeri Padang 2Fakultas Teknik, Universitas NegeriPadang

Analisis Sistem Keamanan Pada Cloud Computing Menggunakan Metode Attack-Centric (Security System Analysis of Cloud Computing Using Attack-Centric Method) Aditya Dwi P.W. 1*, E.I.H. Ujianto 2 1

Rashid, F.Y. The dirty dozen: 12 cloud security threats, 2016. [Online]. Available: https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-securitythreats.html

PERENCANAAN PENINGKATAN KEMATANGAN TEKNOLOGI INFORMASI MENGGUNAKAN ACMM DAN TOGAF PADA POLITEKNIK XYZ Agus Hermanto1) , Fridy Mandita2) , Supangat3)

Septiadi, B. E., Kusnanto, G., & Supangat, S. (2019). Analisis Tingkat Kematangan Dan Perancangan Peningkatan Layanan Sistem Informasi Rektorat Universitas 17 Agustus 1945 Surabaya (Studi Kasus : Badan Sistem Informasi Universitas 17 Agustus 1945 Surabaya). *Konvergensi*, *15*(1). https://doi.org/10.30996/konv.v15i1.2831

SCREENSHOT PLAGARISME