Computer Based Information System Journal

ISSN (Print): 2337-8794 | E- ISSN : 2621-5292
web jurnal : http://ejournal.upbatam.ac.id/index.php/cbis

ANALISA PENERAPAN DISASTER RECOVERY PLAN PADA DATA CENTER PERUSAHAAN

Zulkarnain
Universitas Internasional Batam, Indonesia

INFORMASI ARTIKEL

Diterima Redaksi: 25 Juli 2022
Diterbitkan *Online*: 30 September 2022

KATA KUNCI

Disaster recovery plan; data center

KORESPONDENSI

E-mail: zulbtm@gmail.com

A B S T R A C T

Disaster recovery plan atau DRP merupakan sebuah perencanaan yang digunakan unutk menjalankan operasional dalam kondisi terjadi gangguan. Saat ini perusahaan tidak mempunyai gambaran tentang keberhasilan implementasi DRP. Dengan melakukan analisa implementasi disaster recovery plan pada data center perusahaan, maka peneliti akan mengetahui apakah implementasi DRP sudah dilakukan dengan benar, apabila terjadi bencana atau gangguan, perusahaan masih bisa menjalakan operasionalnya atau bisa juga mengembalikan system dengan waktu yang cepat. Penelitian ini menggunakan metode deskriptif kualitatif. Sumbar data diambil dari pengamatan langsung, melakukan pengecekan dokument serta melakukan wawancara. Hasil dari analisa dan pembahasan, penulis akan mengetahui tentang beberapa kegiatan atau proses DRP yang telah dilakukan dengan benar dan ada juga beberapa kegiatan atau proses yang harus menjadi fokus perbaikan.

I. Latar Belakang

Dukungan sarana teknologi IT sangat diperlukan untuk mendukung kegiatan perusahan. Perusahan berusaha untuk menjaga kelanjutan atau kesediaan sarana IT agar bisa digunakan setiap saat. Ada berapa gangguan yang mungkin timbul sehingga berdampak kepada ketersediaan sarana IT dan menghambat jalannya operasional perusahaan.

Dalam kesempatan ini peneliti melakukan penelitian pada sebuah perusahaan pabrik elektonik tentang analisa implementasi Disaster Recovery Plan (DRP) pada data center mereka. Program ini akan memberikan panduan kepada perusahaan bagaimana menjaga ketersediaan sarana teknologi IT khususnya ada di data center. Baik dalam aspek pencegahan maupun ketika terjadi maka perusahaan mengetahui apa yang harus dilakukan.

Penelitian menggunakan beberapa langkah dalam melakukan penelitian ini, seperti melakukan pengecekan dokumen yang berkaitan dengan program disaster recovery plan. Serta melakukan wawancara secara langsung ke tim data center perusahaan untuk mendapat gambaran dan informasi yang benar.

Disaster atau bencana adalah gangguan yang timbul disebabkan oleh bencana alam, kerusakan sumber listrik, kejahatan manusia dan hal – hal lainya yang berdampak tidak bisa beroperasinya

system dalam sebuah perusahaan dalam waktu tertentu. Durasi gangguan tersebut bisa mulai dari beberapa jam atau hari sehingga menimbulkan kerugian bagi perusahaan. Dampak kerusakannya juga bisa bervariasi, mulau dari kerusakan perangkat keras atau juga perangkat lunak.

Menurut laudon, disaster recovery plan merupakan sebuah rencana yang digunakan untuk menjalankan operasional bisnis dalam kondisi sistem teknologi informasi tidak dapat digunakan secara keseluruhan. Untuk mengatasi ini, diperlukan rencana yang terstruktur, agar ketika terjadi bencana, kita tahu apa yang harus dilakukan dan berusaha agar dampak dari bencana dapat diminimalisasikan.

Saat ini perusahaan tidak mempunyai gambaran apakah konsep implementasi a saat ini sudah dijalankan dengan baik, sehingga apabila terjadi disaster maka tim akan mengurangi dampaknya atau tim dengan cepat mengambil tindakan yang tepat.

Tujuan dari penelitian ini adalah untuk mengetahui implementasi disaster recovery plan ada data center perusahaan, apakah program yang dibuat sudah dijalankan dengan benar, sehingga ketika terjadi bencana, perusahaan masih bisa menjalakan operasonal pada saat itu atau minimal perusahaan dapat melakukan recovery dengan waktu yang cepat.

II. Kajian Literatur

Menurut Laudon (2014), Disaster Recovery Plan adalah proses menyusun rencana untuk pencegahan atau pemulihan layanan teknologi IT setelah terjadi gangguan. Disaster atau bencana adalah gangguan yang timbul disebabkan oleh bencana alam, kerusakan sumber listrik, kejahatan manusia dan hal – hal lainya yang berdampak tidak bisa beroperasinya system dalam sebuah perusahaan dalam waktu tertentu. Durasi gangguan tersebut bisa mulai dari beberapa jam atau hari sehingga menimbulkan kerugian bagi perusahaan. Dampak kerusakannya juga bisa bervariasi, mulau dari kerusakan perangkat keras atau juga perangkat lunak.

Menurut Susan Snedaker (2013), Banyak aspek yang dapat mencegah atau pemulihan bencana pada teknologi informasi, satu diantaranya adalah orang-orang yang bertugas melakukan perencanaan. Ada seseorang yang bertanggung jawab untuk area atau proses tertentu. Struktur organisasi dalam disaster recovery ini perlu dibuat agar ketika terjadi bencana, kita tahu siapa yang harus kita hubungi. Sehingga dapat memperlancar komunikasi dalam situasi bencana. Struktur ini harus terdokumentasi dengan baik dan dikomunikasikan ke seluruh karyawan. Bahkan nomor telpon yang dihubungi harus selalu diperbaharui.

Menurut Peter Gregory (2009), tentang gangguan disaster recovery plan. Diantara gangguan tersebut dari bencana alam, kegagalan teknologi, maupun dari kejahatan atau kelalaian manusia. Gangguan pertama bisa datang dari penyerangan siber. Yang dimaskud dengan serangan siber ini adalah serangan yang terjadi dalam dunia internet, baik itu untuk tujuan menyerang atau hal – hal lain yang berdampak pada kerusakan dari objek yang menjadi sasaran penyerangan. Bermacam-macam cara yang digunakan untuk melakukan penyerangan atau melakukan kerusakan seperti melalui malware, phishing, DoS dan masih banyak lagi model kejahatan lainnya.

Gangguan yang kedua adalah terjadinya power outage, yaitu tidak tersedianya listrik untuk menjalakan system IT atau data center di perusahaan. Kegagalan ini terjadi baik karena faktor alam maupun manusia. Dengan adanya disaster recovery plan diharapkan dapat mampu meminimalisir atau ketika terjadi dengan power outage, karyawan tahu apa yang harus dilakukan. Ketika terjadi gangguan bisa saja karyawan mengalami panik sehingga tidak mengambil tindakan yang tepat dan cepat.

Ganguan yang ketiga adalah bahaya kebakaran dan kebanjiran. Dalam jurnal yang ditulis Putra dan Aristana (2019), diperlukan sistem untuk melindungi data center dari bahaya kebakaran. Data center harus dilengkapi dengan alat pemadam kebakaran yang terawat dengan baik. Alat pemadam harus mudah diakses dan karyawan mengerti bagaimana menggunakannya, dan harus diperhatikan juga ancaman banjir, menempatkan ditempat yang lebih tinggi.

Gangguan yang ke empat adalah pencegahan terjadinya problem pada system dengan melakukan maintenance dan juga harus ada seseorang yang bertugas untuk melakukan perbaikan apabila terjadi gangggguan. Perlu adanya dukungan tenaga ahli untuk aplikasi atau system yang bersifat kritikal. Apabila terjadi

gangguan pada aplikasi kritikal, maka aplikasi tersebut tidak bisa digunakan.

Hal lain yang perlu diperhatikan adalah tentang backup dan restore data seperti yang terlihat dalam jurnal simulasi backup dan restore oleh Ilham Arnomo (2019) simulasi backup dan restore. Backup dan restore harus dilakukan setiap hari dan pada tempat yang berbeda. Apabila terjadi sesuatu yang fatal, maka minimal perusahaan masih mempunyai data backup dan bisa melakukan restore

III. Metodologi

Penelitian ini dilakukan di sebuah perusahaan pabrik elektronik yang berlokasi di kawasan industri Muka Kuning, Pulau Batam. Alasan pemilihan tempat ini adalah karena perusahaan tersebut sudah melakukan penerapan disaster recovery plan. Dan penulis ingin melakukan analisa, apakah penerapan disaster recovery sudah dilakukan dengan benar.

Penelitian ini menggunakan metode deskriptif kualitatif, yaitu dengan cara melihat gambaran secara lansung di perusahaan, melakukan wawancara serta pengecekan dokumen yang berhubungan dengan penelitian ini.

Sumber data primer didapat dari proses wawancara dan melihat secara lansung dokumentasi serta operasional yang ada di perusahaan.

Adapun langkah – langkah yang dilakukan dalam penelitian ini adalah sebagai berikut :

a) Melakukan observasi secara langsung kegiatan di perusahaan
b) Melakukan studi landasan teori
c) Melakukan wawancara secara langsung ke Tim IT yang menangani program ini.
d) Melakukan pengecekan dokumentasi yang ada pada perusahaan
e) Membuat rangkuman dan analisa data
f) Membuat kesimpulan

IV. Pembahasan

Berdasarkan hasil penelitian penulis tentang penerapan disaster recovery pada sebuah pabrik perakitan elektronik di kawasan industri batamindo. Penulis mengambil beberapa data yang berkaitan dengan penerapan disaster recovery. Data diambil melalui wawancara dan juga dokumentasi perusahaan. Berikut penulis jelaskan analisa dan pembahasan secara bertahap.

4.1 Data Contact Information

Penulis melakukan pengecekan tentang informasi yang dimiliki perusahaan berkaitan dengan dokumentasi orang – orang yang bisa dihubungi jika terjadi disaster. Ada beberapa target yang penulis ingin dapatkan seperti terlampir dalam tabel 1 dibawah ini.

Tabel 1 Contact Information

Fungsi	Tersedia Nomor yang bisa dihubungi	Apakah data update atau sudah usang
IT Service Desk	Tersedia	Updated
Polisi	Tersedia	Updated
Ambulance	Tersedia	Updated
Emergency Medical dan Dokter	Tersedia	Updated
Fire Brigade	Tersedia	Updated
Facility Management	Tersedia	Updated
Business Continuity Management	Tersedia	Tidak updated
IT Crisis Manager	Tersedia	Updated
PIC Network	Tersedia	Tidak Updated
PIC Server	Tersedia	Updated
PIC Client Service	Tersedia	Updated
Production	Tersedia	Tidak updated

Dari tabel contact information diatas, masih ditemukan data yang tidak diupdate. Tim DRP harus segera melakukan perbaikan contact information. Apabila terjadi bencana atau gangguan, akan menggangu proses informasi dan dapat berdampak lambatnya penanganan disaster.

4.2. Skenario Penyerangan siber

Disini penulis ingin mendapatkan informasi ketika terjadi penyerangan siber, karyawan dapat mengambil langkah yang tepat.

Tabel 2. Tentang Penyerangan siber

Fungsi	Jawaban	Perbaikan
Apakah ada proses yang mengatur terjadinya penyerangan siber	Ada, ada system yang digunakan untuk mendetect penyerangan siber	Dokumentai sudah ada, namun masih diperlukan sosialisasi lebih lagi
Apakah ada Crisis Team yang mengatur ketika terjadi disaster	Ada, Crisis team dari IT, FI dan Operation	Crisis team sudah ada dan berjalan, terutama ketika terjadi power outage, dimana IT infrastructure tidak bisa digunakan seluruhnya.
Apakah pernah dilakukan simulasi cyberattack tanpa sepengetahuan users	Ya pernah dilakukan dan masih ada user yang terjebak dengan simulasi tersebut	Perlu dilakukan sosialisai terkait dengan bahayanya cyberattack

4.3 Skenario Power Outage

Penulis melakukan wanwancara dengan tim Data Center terkait dengan langkah – langkah yang diambil ketika terjadi power outage.

Tabel 3. Skenario Power Outage

Fungsi	Jawaban	Perbaikan
Apakah ada tool yang dapat melakukan detection power outage	Ada, ketika terjadi power outage, ada local server yang mengirim sms atau dari global team akan memberikan informasi	Sudah cukup baik
Apakah pernah terjadi power outage yang berdampak pada tidak berfungsinya pelayanan IT	Pernah, Crisis manager langsung memberikan infromasi kepada seluruh stakeholder IT	Sudah cukup baik
Apakah komunikasi dilakukan oleh crisis manajemen team kepada respective admin atau user	Ya, Crisis manager akan melalukan sharing komunikasi ke seluruh stakholder	Sudah cukup baik
Apakah ada dual power source	Ada, data center menggunkan dua buah aliran listrik dari sumber yang berbeda	Sudah cukup baik
Apakah UPS saat ini sudah cukup	UPS berjalan dengan baik hanya daya tahan nya terbatas	Sudah cukup baik

4.4. Skenario Kebakaran dan kebanjiran

Penulis melakukan wanwancara dengan tim Data Center terkait dengan langkah – langkah yang diambil ketika terjadi kebakaran.

Tabel 4. Tentang kebakaran dan kebanjiran

Fungsi	Jawaban	Perbaikan
Apakah tersedia tabung pemadam kebakaran di Data Center	Ada, tersedia tabung pemadam kebakaran	Sudah cukup baik
Apakah ada pengecekan regular tabung pemadam kebakakaran	Ada, ada kartu yang digunakan untuk melakukan jadwal pengecekan	Sudah cukup baik
Apakah ada alat pemadam lain selain tabung kebakaran	Ada, perusahaan menggunakan FM200 Fire Suppression, jika terjadi deteksi kebakaran, maka sistem akan mengambil langkah cepat dalam waktu 10 detik	Sudah cukup baik
Apakah data center berada dalam area yang aman dari banjir	Ya, ruangan menggunakan raised floor dan lebih tinggi dari lantai utama, serta adanya irigasi yang baik diperusahaan	Sudah cukup baik

4.5 Skenario kerusakan aplikasi kritikal

Penulis melakukan wanwancara dengan tim Data Center terkait dengan langkah – langkah yang diambil ketika terjadi kerusakan aplikasi kiritikal.

Tabel 5. Tentang kerusakan aplikasi kritikal

Fungsi	Jawaban	Perbaikan
Apakah ada tool yang digunakan untuk mendeteksi ketersediaan aplikasi kritikal ?	Ada, perusahaan menggunakan tool khusus untuk melakukan monitor aplikasi kritikal tersebut	Sudah cukup baik
Apakah ada jadwal on call service bagi team IT ketika terjadi kerusakaan aplikasi	Ada, Tim IT menyiapkan anggota untuk menerima panggilan telpon ketika terjadi kerusakan pada aplikasi kritikal, aplikasi kritikal harus diselesaikan dalam waktu 2 jam. Apabila dalam waktu 2 jam tidak bisa diselesaikan maka Crisis Manager akan melalukan komunikasi	Sudah cukup baik
Apakah ada emergency Team ketika terjadi kerusakan	Crisis Manager akan melakukan komunikasi ke stake holder yang terlibat ketika terjadi kerusakan	Sudah cukup baik

4.6. Backup dan Restore

Penulis melakukan wanwancara dengan team Data Center terkait dengan backup dan restore.

Tabel 6. Tentang backup dan restore

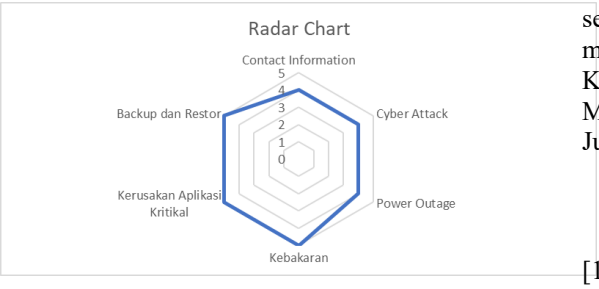
Fungsi	Jawaban	Perbaikan
Apakah ada tools yang digunakan untuk melakukan backup dan restore	Ada, perusahaan menggunakan tool khusus untuk melakukan backup (druva)	Sudah cukup baik
Apakah hasil backup bisa dilihat	Ya, hasil backup bisa dilihat	Sudah cukup baik
Apakah pernah dilakukan percobaan restore	Ya, percobaan melakukan restore data berhasil	Sudah cukup baik
Apakah backup dilakukan setiap hari	Ya, backup dilalukan setiap hari	Sudah cukup baik
Apakah hasil backup disimpan ditempat yang berbeda	Ya, backup ditempatkan di beberapa tempat	Sudah cukup baik

4.7. Rangkuman dari Hasil Wawancara

Berdasarkan hasil wawancara dan anlisa dokumen, berikut penulis rangkum dalam Radar chart.

Penulis melakukan konversi ke dalam nilai melihat hasil wawancara secara keseluruhan sebagai berikut.

a) Nilai 1 adalah tidak ada prosedur
b) Nilai 2 adalah sudah tersedia prosedur dan belum dijalankan semuanya
c) Nilai 3 adalah sudah tersedia prosedur dan baru mulai dijalankan secara minor
d) Nilai 4 adalah sudah tersedia prosedur namun belum dijalankan secara sempurna dan perlu perbaikan secara minor
e) Nilai 5 adalah sudah tersedia prosedure dan dijalankan secara sempurna tanpa perbaikan



Gambar 1. Radar Chart

Setelah melakukan analisa dokumentasi, wawancara serta melakukan pengolahan data, maka penulis membuat kesimpulan dan saran sebagai berikut. Dari radar chart diatas, kita bisa melihat bahwa adanya kegiatan atau proses yang harus diperbaiki dan juga ada yang harus dipertahankan.

V. Kesimpulan

Setelah melakukan analisa dokumentasi, wawancara serta melakukan pengolahan data, maka penulis membuat kesimpulan dan saran sebagai berikut.

Perusahaan memahami pentingnya penerapan disaster recovery untuk mengambil tindakan penting ketika terjadi gangguan. Ada beberapa kegiatan atau proses yang telah dilakukan perusahaan dengan benar seperti kegiatan pencegahan bahaya kebakaran, kerusakan aplikasi kritikal dan menjalankan fungsi backup dan restore.

Diperlukan beberapa kegiatan atau proses perbaikan terkait dengan penanganan penyerangan siber, power outage dan juga data orang yang bisa dihubungi.

Demikian penelitian dibuat, semoga dapat bermanfaat bagi perusahaan tempat penulis melakukan penelitian maupun bermanfaat juga pada perusahaan lainnya. Dan peneliti menerima masukan dengan senang hati untuk penyempurnaan penelitian k edepan agar lebih berdaya guna.

Terima kasih kepada seluruh stakeholder Universitas Internasional Batam atas dukungan yang diberikan dalam menyelesaikan penelitian ini.

Ucapan Terima Kasih

Silahkan ucapkan terimakasih kepada pihak yang membantu dalam penelitian.

Kami mengucapkan terima kasih yang sebesar – besarnya atas dukungan dari segenap manajemen Universitas Internasional Batam, Kaprodi dan Kajur Sistem Informasi UIB, Manajemen SIM LPPM UIB serta Manajemen Jurnal CBIS dari Universitas Putra Batam.

Daftar Pustaka

[1] I. Maita and S. Akmal, "ANALISIS TATA KELOLA TEKNOLOGI INFORMASI DENGAN BEST PRACTICE ITIL V3," *Jurnal Rekayasa dan Manajemen Sistem Informasi,* vol. 2, no. 1, p. 1, 2016.

[2] L. W. Michael Wallace, The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, US: AMACOM, 2010.

[3] P. J. Peter Gregory, IT Disaster Recovery Plan, US: For Dummies, 2007.

[4] S. Snedaker, Business Continuity and Disaster Recovery Planning for IT Professionals, US: Syngress, 2013.

[5] K. H. George Haddow, Disaster Communications in a Changing Media World, US: Butterworth-Heinemann, 2013.

[6] I. G. N. A. Pawana, "PERANCANGAN SERVER DENGAN MENGGUNAKAN VIRTUALISASI, LOAD BALANCER, FAILOVER DAN DATABASE REPLICATION (STUDI KASUS : IKIP PGRI BALI)," *Univesitas Telkom,* p. a, 2016.

[7] M. Muhaemin, "MENGEMBANGKAN BUSINES CONTINUITY PLANNING (BCP) DENGAN PENDEKATAN KUANTITATIF STUDI KASUS : SIAK-DITJEN ADMINDUK KEMENDAGRI," *JUST IT,* p. 1, 2018.

[8] I. A. W. H. N. P. Adi Supriyanto, "Penyusunan Disaster Recovery Plan (DRP) berdasarkan Framework NIST SP 800-34 (Studi Kasus: Departemen Teknologi Informasi PT Pupuk Kalimantan Timur)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* p. 1, 2019.

[9] L. Nurtanzila, "PENERAPAN DISASTER RECOVERY AND CONTINGENCY PLANNING PADA PERLINDUNGAN ARSIP VITAL DI BPN DIY," *Diplomatika, UGM,* p. 1, 2018.