PERENCANAAN DAN TATA KELOLA MERESPON INSIDEN PADA KEAMANAN JARINGAN *SMART GRID*

Makalah Tugas Kuliah EL6115

Operasi Keamanan dan *Incident Handling*

Oleh
KHILDA AFIFAH
NIM: 23214316
(Program Studi Magister Teknik Elektro)

INSTITUT TEKNOLOGI BANDUNG
April 2016

ABSTARK

Smart grid merupakan suatu konsep pengelolaan energi listrik yang mampu mengkoordinasikan peran pembangkit listrik kecil berbahan bakar energi terbarukan secara optimal. Logika awal dari pengembangan teknologi *smart grid* adalah berusaha semksimal mungkin mengoptimalkan apapun yang tersedia di bumi ini. Keuntungan besar dengan hadirnya sistem *smart grid* diantaranya dapat meningkatkan efisiensi, ekonomis serta transparansi dalam konsumsi energi listrik, meningkatkan kehandalan dalam bidang tenaga listrik dan mengurangi efek rumah kaca karena emisi karbon sehingga mengoptimalkan pemanfaatan energi terbarukan. Di dalam *smart grid* terdapat 3 unsur teknologi yaitu teknologi tenaga listrik, informasi, dan telekomunikasi. Ketiga unsur tersebut saling terintegrasi yang memungkinkan adanya komunikasi 2 arah antara perusahaan penyedia tenaga listrik seperti PLN dengan konsumen. Transfer energi listrik dalam *smart grid* ini tidak seperti sistem konvensional yang hanya satu arah tetapi juga dapat dilakukan sebaliknya. Sistem jaringan yang berada pada *smart grid* ini berupa sistem SCADA dan WLAN/WiMax. Oleh karena itu perlunya sistem keamanan jaringan yang baik agar saat terjadinya serangan siber perangkat tidak mudah terserang. Selain itu diperlukan adanya penangan respon yang terstandar dan terstuktur apabila suatu saat terjadi sebuah insiden. Maka dari itu diperlukan badan standarisasi dan penelitian terhadap insiden jaringan untuk *smart grid*, salah satu badan dan standart tersebut yaitu IEC dan NIST. Serangan-serangan yang terjadi pada *smart grid* dapat berupa serangan virus maupun serangan pemalsuan data pada *smart meter* maka dari itu penanaman pentingnya data pada *smart grid* harus ditanamkan pada SDM yang bergerak di bidang tersebut. Saat terjadi sebuah insiden, respon yang harus dilakukan yaitu melakukan langkah-langkah sudah di rancang sebelumnya agar tidak terjadi insiden yang lebih besar. Maka dari itu dibutuhkan sebuah stuktur penanganan insiden dan melakukan pelatihan-pelatihan maupun simulasi apabila terjadinya insiden.

Kata Kunci: *smart grid*, insiden respon, sistem keamanan

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

A. Latar Belakang

Saat ini ketersediaan sumber energi listrik tidak cukup memenuhi kebutuhan masyarakat. Oleh karena itu sering terjadi pemadaman bergilir yang dijadikan solusi keterbatasan tersebut. Maka dari itu diperlukan suatu sistem yang dapat menghimpun energi listrik dari berbagai sumber mulai dari energi listrik skala besar seperti energi listrik dari batu bara maupun energi listrik skala kecil pada pedesaan yaitu energi listrik mikro hidro, panel surya maupun energei listrik tenaga angina. Solusi untuk menghimpun dan mengelola ketersediaan pasokan energi listrik yaitu sistem *smart grid*. *Smart grid* merupakan suatu konsep pengelolaan energi listrik yang mampu mengkoordinasikan peran pembangkit listrik kecil berbahan bakar energi terbarukan seperti energi listrik tenaga surya, angin, air, dan ombak secara optimal. Logika awal dari pengembangan teknologi *smart grid* adalah berusaha semaksimal mungkin mengoptimalkan apapun yang tersedia di bumi ini agar pembangkit sampai ke konsumen lebih efisien, ekonomis, transparasi, berkelanjutan dan distribusi yang aman. Keuntungan besar dengan hadirnya sistem *smart grid* diantaranya dapat meningkatkan efisiensi dalam konsumsi energi listrik, meningkatkan kehandalan dalam bidang tenaga listrik, mengurangi efek rumah kaca karena emisi karbon, dan mendukung kehadiran dari pemanfaatan energi terbarukan secara optimal.

Smart grid merupakan sistem dari sistem besar, menurut National Institut Standards and Technology (NIST) *smart grid* terdiri dari layer utama [1] yaitu (i) layer power dan energi, (ii) layer komunikasi dan (iii) layer komputerisasi. Layer (ii) dan (iii) memungkinkan adanya komunikasi layer power dan energi saling berkomunikasi timbal balik antara penyedia layanan dengan konsumen.

Selain itu pada sistem *smart grid* penghasil energi bukan hanya *utility* (PLN) tetapi juga konsumen dapat mendistribusikan energi listrik yang mereka hasilkan ke konsumen lain.

Sistem *smart grid* memiliki banyak keuntungan dalam proses memanfaatkan energi terbarukan dan penghematan daya, tetapi *smart* pula memiliki berbagai masalah salah satunya yaitu sistem keamanan dalam sistem jaringan *smart grid* harus memiliki sistem keamanan yang baik. Seperti sistem keamanan yang terjadi pada sistem *Supervisory Control and Data Acquisition* (SCADA) yang digunakan untuk mengelola, mengendalikan, dan memantau sistem *smart grid* ini yang berlokasi sangat jauh dari satu grid ke grid yang lain [2]. Sistem SCADA ini memiliki kerentanan karena dapat terjadi pencurian informasi tentang penggunaan listrik konsumen, ketersediaan listrik power plant, maupun pengontrolan yang akan dilakukan oleh sistem kontrol. Banyak konsumen dari Negara-negara yang sudah menerapkan sistem *smart grid* ini bermasalah terhadap persoalan privasi yang dimiliki konsumen lewat data yang didapat dari *Advanced Metering Infrastructure* (AMI) [3].

B. Tujuan dan Manfaat

Tujuan dari penulisan ini yaitu memaparkan insiden yang sering terjadi pada pengelolaan jaringan *smart grid* dan pemaparan bagaimana mengatasi insiden tersebut.

C. Metode Penulisan

Metode penulisan yang digunakan yaitu studi literatur untuk mencari dan melihat tentang insiden dan respon bagaimana insiden tersebut ditangani dalam permasalahan tata kelola jaringan *smart grid*. Sumber literatur berasal dari jurnal dan paper.

BAB II

TINJAUAN PUSTAKA

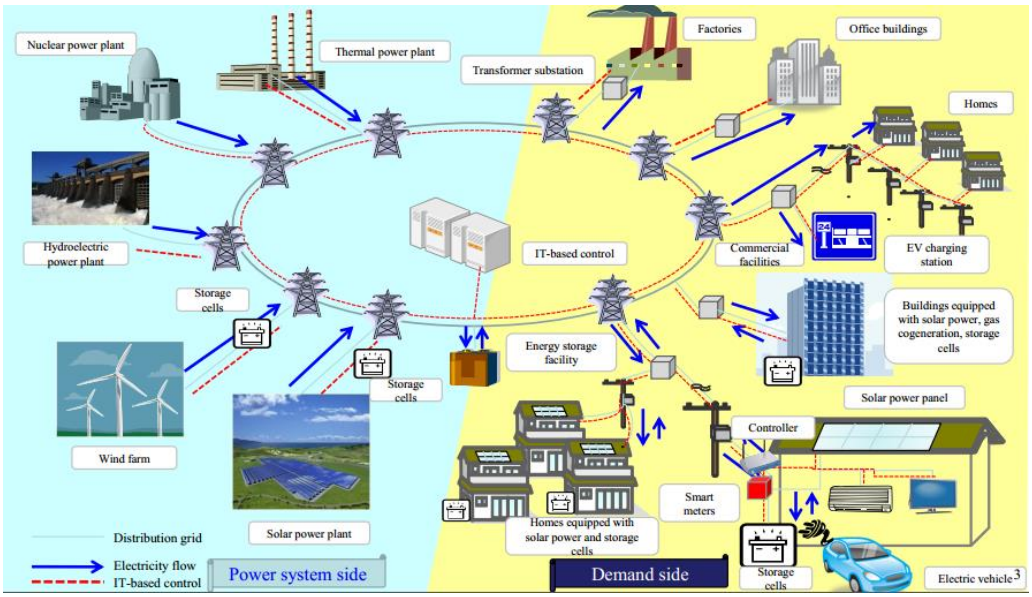
A. Pengertian *Smart Grid*

Seperti yang telah dijelaskan sebelumnya s*mart grid* adalah pengelolaan energi listrik dengan konsep terintegrasi dan mengurangi tergantungan terhadap sumber daya alam yang berasal dari fosil. Integrasi ini memungkinkan adanya komunikasi dan pertukaran informasi antara pembangkitan, distribusi dan konsumsi energi listrik untuk membuat keputusan yang lebih cerdas mengenai konsumsi energi dan produksi. Di dalam *smart grid* terdapat 3 unsur teknologi yaitu teknologi tenaga listrik, informasi, dan telekomunikasi. Ketiga unusur tersebut saling terintegrasi yang memungkinkan adanya komunikasi 2 arah antara perusahaan penyedia tenaga listrik seperti PLN dengan konsumen. Transfer energi listrik dalam *smart grid* ini tidak seperti sistem konvensional yang hanya satu arah tetapi juga dapat dilakukan sebaliknya. Apabila ternyata konsumen memiliki sumber energi listrik sendiri seperti panel surya yang dapat menghasilkan energi listrik dari cahaya matahari, maka saat energi listrik yang dihasilkan berlebih maka konsumen dapat mengirim energi listrik yang dihasilkan tersebut ke *grid* yang ada. Dari hal tersebut konsumen bukan hanya membayar tagihan listrik saja, tetapi juga dapat menghasilkan uang dari listrik yang dihasilkannya.

Saat ini di Indonesia penerapan *smart grid* sudah diuji coba melalui program pemerintah yaitu yaitu pilot projek sistem *smart grid* di Sumba Barat Daya, Nusa Tenggara Timur (NTT)[4]. Sistem *smart grid* sangat bagus untuk di terapkan di Indonesia karena kondisi geografis yang terdiri dari banyaknya pulau-pulau kecil yang membuat pemerintah kesulitan untuk mendistribusikan energi listrik, maka diharapkan dengan adanya *smart grid* pulau-pulau kecil dapat menghasilkan

energi listrik sendiri dengan sumber energi yang memanfaatkan kondisi alam daerah tersebut.

B. Komponen dan Sistem Kerja *Smart Grid*



Gambar 1 Sistem Alur *Smart Grid* [5]

Seperti yang terlihat pada gambar 1 *smart grid* terdiri dari jaringan komunikasi, sensor canggih dan perlanatan kontrol yang berfungsi memantau jalannya sistem tersebut. Aliran daya yang diterima dan konsumsi daya yang digunakan akan di data dan kontrol secara *real time*, maka dari itu alairan daya tersebut perlu diatu agar didapatkan kinerja jaringan yang optimal dan efisien. Oleh karena itu, diperlukan pengaturan alat pada jaringan tersebut yang dapat memantau aliran komunikasi dan informasi dua arah antara power plant, base kontrol dan konsumen. Metode pengaturan pada sistem ini didapatkan berdasarkan data yang terkumpul pada base kontrol yang menerima data dari sensor yang memantau konsumsi energi secara real time, kondisi cuaca, status operasi, kondisi peralatan serta ketersediaan energi yang dihasilkan power plant maupun energi yang dimiliki oleh konsumen. Data tersebut yang selanjutnya akan digunakan untuk memprediksi kebutuhan energi dan energi yang akan di salurkan ke konsumen.

Selain itu data yang didapatpun akan dijadikan pengontrolan grid mana yang membutuhkan energi yang lebih banyak.

Pada *smart grid* apabila sumber energi listrik dari salah satu power plan tidak dapat mendistribusikan energi listrik, maka sumber energi listrik dapat dialihkan dan disitribusikan dari sumber lainnya.

Bagian-bagian *smart grid* [6] terdiri dari bagian *integrated communication system*, hardware yang modern, *modern control & instrumentation (I & C)* dan bagian *smart software.* Dibawah ini akan dijabarkan masing-masing bagian tersebut.

1. *integrated communication system*, pada komponen ini memungkinkan komunikasi terjadi dua arah antara base kontrol, konsumen dan power plant serta dapat terintegrasi secara penuh sehingga sistem ini dinamis dan inteaktif untuk pertukaran data dan daya secara real time. Sistem yang ada pada bagian ini yaitu *copper wiring*, fiber optic, *power line carrier*, teknologi wireless dan *broadband over power line technologies.*
2. Hardware yang Modern, pada bagian ini yaitu sistem hardware yang mendukung sistem *smart grid* harus menggunakan material yang baik, bahan superkonduktif yang baik, bagian-bagian pada power plan seperti inverter, turbin dan lain sebagainya untuk mendukung ketersediaan sumber energi. Selain itu bagian terpenting yaitu baterai yang digunakan yang dapat menyimpan energi listrik agar dapat digunakan dilain waktu.
3. *modern control & instrumentation (I & C)* , pada bagian ini terdiri dari algoritma untuk mengontrol sistem agar berjalan dengan baik dengan bekerja menganalisa, mendiagnosa dan memprediksi kebutuhan listrik dan ketersediaan listrik sesuai dengan kejadian yang secang terjadi. Contoh dari sistem ini yaitu penggunaan SCADA, sensor, digital relay dan *smart meter.*

4. *Smart Software*, pada bagian ini yaitu penggunaan software yang dapat bekerja secara real time, dinamis, cepat dan akurat agar konsumen nyaman dan mudah menggunankannya.

C. Smart Meter pada *Smart Grid*

Pada *smart grid*, smart meter bukan hanya difungsikan sebagai alat untuk mengukur penggunaan listrik konsumen per bulan saja tetapi difungsikan untuk melakukan jaringan monitoring penggunaan konsumsi listrik, alarm, pengumpulan dan pengolaan data yang akan dikirimkan ke base kontrol, otomasi pada jaringan dan lain sebagainya. Oleh karena itu sistem smart meter ini di fungsikan bukan hanya menerima data dari penggunaan konsumsi listrik tetapi dapat mengirim data [13], maka sistem keamanan yang terdapat pada smart meter ini harus terkelola dengan baik agar data yang dikirim dari konsumen ke base kontrol aman dan tidak dapat dicuri datanya oleh orang yang tidak berkepentingan.

Smart meter yang digunakan pada *smart grid* yaitu *Advanced Metering Infrastructure* (AMI) yaitu suatu keseluruhan infrastuktur dari smart meter yang mengelola jaringan komunikasi dua arah ke pusat pengedalian peralatan (base kontrol), dan semua aplikasi yang dapat melakukan pengmpulan dan pengiriman informasi tentang penggunaan energi secara real time. Jadi AMI ini dapat memanagemen dan mengontrol parameter kelistrikan dan perangkat-perangkat lainnya pada grid konsumen maupun power plan.

Perangkat yang digunakan pada AMI yaitu perangkat meter, sensor dan kontrol setra perangkat wireless yang memungkinkan komunikasi jarak jauh antara grid dan base kontrol.

BAB III

PEMBAHASAN

A. Identifikasi Insiden pada *Smart Grid*

1. Sistem Keamanan Data pada *Smart Grid*

Serangan-serangan *cyber* yang mungkit terjadi pada *smart grid* yaitu serangan pada *smart grid kontrol* sistem, gangguan dan pemblokiran pada lalu lintas informasi jaringan *smart grid* , serta *smart grid* terinfeksi oleh malware [2]. Hal-hal tersebut dapat terjadi pada power plan, jaringan distribusi maupun base kontrol pada *smart grid.* Seperti yang sudah dipaparkan diatas data konsumen pada AMI dapat dicuri oleh peretas ataupun pengontrolan pada SCADA yang terdapat pada base kontrol di kontrol oleh peretas. Jadi keamanan yang terjadi harus dikelola dengan sebaik-baiknya agar tidak terjadi peretasan terhadap data ataupun pengontrolan terhadap sistem.

Apabila terjadi serangan pada *smart grid* maka dapat terjadi gangguan pada infrasuktur *smart grid* terkait dengan operasional pasokan energi dan menbuat akan membuat ketidak seimbangan kegiatan ekonomi dan bisnis, politik dan social.

Insiden-insiden yang dapat terjadi pada keamanan jaringan pengelolaan *smart grid* yaitu [2, 14] :

a. Informasi yang tidak benar dikirim ke base kontrol sistem *smart grid* seperti data palsu dari konsumen maupun dari power plan yang menyebabkan terjadinya tindakan yang salah pada sistem.
b. Software pada sistem *smart grid* terserang malware yang menyebabkan efek negative pada sistem.

c. Perubahan instruksi yang dilakukan peretas yang menyebabkan perubahan instruksi yang salah yang berakibat buruk pada sistem dalam skala kecil maupun dalam skala besar.
d. Masalah privasi konsumen misalnya dengan melihat data smart meter maka saat konsumen tidur atau di luar rumah dapat diketahui, hal tersebut dapat di manfaatkan oleh orang-orang nakal yang ingin mencuri rumah tersebut dengan melihat data smart meter.

Serangan-serangan siber yang terjadi pada dunia *smart grid* ini sangat banyak. Apalagi tujuan dari serangan siber yaitu untuk melemahkan keadaan suatu Negara. Dibawah ini akan dipaparkan serangan-serangan siber yang terjadi di dunia.

a. Serangan Virus Stuxnet [7, 15]

Serangan virus ini terdeteksi pda juli 2010 menyerang perangkat industry dengan software buatam Siemens dan perangkat OS Microsoft Windows. Virus ini di sebarkan melalui USB *flashdrive* dan menyerang perangkat kontrol pengawas pada SCADA yang menginfeksi PLC dengan cara mengubah aplikasi perangkat lunak dengan memprogram ulang perangkat tersebut dan menyembunyikan perubahan yang terjadi. Serangan yang terjadi di seluruh dunia 60% menyerang perangkat industry salah satunya pembangkit listrik tenaga nuklir di Iran. Pada tahun 2013 virus ini menyerang laptop-laptop yang berada pada stasiun luar angkasa internasional atau yang dikenal dengan ISS. Penyerangan virus ini berawal dari USB *flashdrive* yang dibawa oleh kosmonot Rusia yang menancapkan USB milik mereka ke laptop milik ISS.

Data dari Symnatec menunjukan data bahwa kasus-kasus yang terjadi yaitu Iran dengan 62.867 komputer yang terinfeksi, Indonesia dengan 13.336, India dengan 6.552, Amerika Serikat dengan 2913, Australia dengan 2.436, Inggris dengan 1.038, Malaysia dengann 1.013 dan Pakistan dengan 993. Perusahan antivirus Kaspersky menyimpulkan

bahwa serangan tersebut didukung oleh sebuah Negara dan telah diduga bahwa Negara tersebut adalah Israel dan Amerika Serikat. Hal tersebut didukung oleh pernyataan Edward Snowden pada tahun 2013 melalui media Jerman bahwa NSA dan Israel yang membuat virus tersebut.

b. Night Dragon [7]

Virus ini merupakan virus memiliki target penyerangan pada sector energi seperti minyak bumi, power dan perusahaan petrokimia. McAfee menyatakan bahwa Shell, Exxon Mobil dan BP telah terjangkit virus ini. Virus ini menyerang computer dengan sistem operasi MS Windows. Virus ini memiliki tujuan mendapatkan informasi sensitive tentang perusahaan seperti rincian keuangan, penawaran perusahaan dan lain sebagainya.

c. Serangan Virus pada Pembangkit Litrik [15]

Serangan virus *slammer worm* yang menyerang pembangkit listrik di Ohio yang menyebabkan pembangkit listrik tersebut harus berhenti beroperasi selama beberapa saat. Serangan virus yang terparah yaitu serangan virus yang terjadi pada pembangkit listrik tenaga nuklir di Georgia yang harus menghentikan operasinya selama 48 jam. Hal tersebut terjadi saat computer pengontrol merestart setelah proses update, setelah itu semua data kontroler mereset yang menyebabkan munculnya data bahwa terjadi penurunan pada penampungan air dingin pada radiator nuklir yang otomatis memerintahkan proses produksi berhenti.

2. Sistem Perancangan Jaringan pada *Smart Grid*

Serangan siber terhadap *smart grid* sangat berbeda dengan serangan siber terhadap media komunikasi lainnya, karena serangan siber terhadap *smart grid* bisa berdampak pada kelangsungan hidup banyak orang seperti matinya aliran listrik disuatu wilayah yang menyebabkan tidak berfungsinya peralatan yang membutuhkan energi listrik. Oleh karena itu sistem jaringan dan distribusi pada *smart grid* harus dirancang sedemikian rupa agar supply energi listrik tidak hanya dari satu sumber saja tetapi dari berbagai sumber.

Maka dari itu sistem jaringan yang digunakan tidak menggunakan sistem jaringan bus dan ring tetapi mengunakan sistem lainnya yang apabila satu terputus maka tidak menyebabkan terhentinya aliran listrik.

B. Penanganan Insiden pada *Smart Grid*

1. Pencegahan Keamanan terhadap Serangan Siber

Sebelum menangani suatu insiden yang terjadi maka sebaiknya dilakukan pencegahan terlebih dahulu agar suatu insiden dapat dikurangi ataupun dihilangkan sama sekali. Dibawah ini merupakan beberapa solusi untuk mencegah suatu insiden pada sistem *smart grid.*

Suatu perusahaan InGuardians, Inc. menggunakan IPv6 pada teknologi terbaru untuk AMI. Perusahan tersebut menggunakan IPv6 untuk teknologi smart meter untuk *smart grid* maupun smart gas meter untuk distribusi penggunaan gas [8]. Dibawah ini merupakan kelebihan diterapkannya IPv6 pada komponen AMI.

a. IPv6 memiliki panjang alamat 128 bit yang memungkinkan pengalamatan lebih banyak yang sangat cocok digunakan untuk perlengkapan rumah tangga
b. Aspek keamanan dan kualitas layanan pada IPv6 sudah terintegrasi dengan baik
c. Desain pada IPv6 memungkinkan dukungan terhadap mobilitas komunikasi tanpa meutuskan komunikasi tanpa memutuskan komunikasi end-to-end
d. Dapat melakukan komunikasi peer to peer yang memudahkan komunikasi mesin ke mesin, manusia ke mesin dan sebaliknya.

Selain itu langkah-langkah yang teknis yang dilakukan untuk memperketat keamanan pada *smart grid* yaitu sebagai berikut [2].

a. Membatasi akses pada jaringan *smart grid* dengan mengidentifikasi semua koneksi yang berhubungan dengan sistem terutama koneksi terhadap sistem base kontrol, memutus koneksi yang tidak perlu

terhadap sistem jaringan *smart grid*. Solusi dalam tahap ini yang paling aman yaitu menggunakan zona demiliterisasi (DMZ) arsitektur jaringan dengan *firewall* agar lalu lintas data pada *smart grid* berjalan dengan baik dan aman.

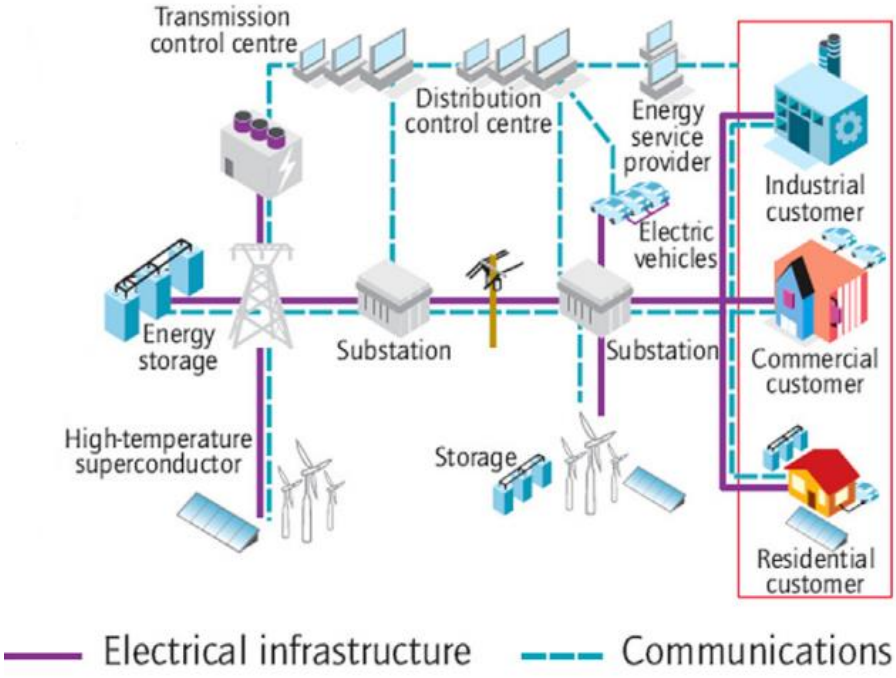
b. Membatasi akses fisik ke jaringan *smart grid* dan perangkat lainnya agar mempertegas jaringan base kontrol dengan menghapus atau menonaktifkan jaringan yang tidak perlu.
c. Melindungi komponen *smart grid* dari eksploitasi salah satunya ekploitasi malware
d. Mempertahankan fungsi kerja *smart grid* selama kondisi buruk sehingga apabila terjadi gangguan maka memiliki komponen cadangan.
e. Menerapkan sistem pematauan terhadap sistem selama 24 jam terkait terjadianya pemantauan insiden.
f. Membangun tim tanggap darurat untuk mengidentifikasi dan mengevaluasi scenario serangan dengan cara memperhatikan kelemahan dari keseluruhan jaringan.

Pada masalah yang serangan terhadap virus Stuxnet dan Night Dragon, rata-rata virus tersebut menyerang computer yang berbasis windows maka untuk mencegahnya adalah menggunakan computer berbasis sistem operasi Linux atau Mac. Walaupun interface dari kedua OS tersebut kurang familiar tetapi pencegahan tersebut lebih baik. Sistem pencegahan dengan mengganti sistem operasi sudah pernah dilakukan pada computer yang berada pada *International Space Station* yang pernah terjangkit oleh virus Stuxnet.

Dengan melihat standar keamanan dari berbagai bidang pengetahuan maka solusi keamanan terbaik yaitu menggunakan sistem keamanan yang sudah diterapkan dapat dimanfaatkan untuk sistem keamanan dan tata kelola insiden pada komunikasi jaringan *smart grid* ini. Beberapa solusi sistem keamanan dari beberapa subsistem pada *smart grid* yaitu subsistem SCADA,

mekanisme standar keamanan dari SCADA sudah dikelola dengan baik seperti standar DNP3, GOOSE, IEC 61850, dan IEC 60870-5A. Komponen keamanan subsistem kedua dari sistem standar keamanan pada jaringan *wireless* seperti untuk WLAN dan WiMax yang menggunakan standar seperti 802.11i dan 802.16e. Subsistem keamanan ketiga yaitu solusi keamanan untuk *smart grid* dengan penggunaan standar keamanan menggunakan teknologi *public key infrastructure* (PKI). Aplikasi dari PKI ini berguna untuk otentifikasi, otorisasi dan privasi teknologi yang dapat memberikan solusi efisiensi harga dan koperhensif [16].

2. Solusi Sistem Perancangan Jaringan pada *Smart Grid*



Gambar 2 Rancangan Stuktur Komponen pada Sistem *Smart Grid* [9]

Sistem perancangan untuk stuktur *smart grid* dapat dilihat pada gambar 2. Pada gambar 2 dapat terlihat bahwa harus ada *energy storage* yang berfungsi untuk menyimpan energi yang dihasilkan oleh power plant darimana saja. Jadi apabila salah satu power plant tidak menghasilkan energi listrik maka energi yang sebelumnya di simpan pada *storage* dapat di distribusikan ke konsumen. pusat pengpntrolan pada sistem ini pun memiliki tiga bagian yaitu

pusat kontrol untuk transmisi yang berfungsi untuk mengatur pengontrolan dan pendataan pada power plant dan jaringannya, pusat kontrol distribusi yang berfungsi mengatur arah distribusi dan data yang diterima dari konsumen dan yang terahir yaitu pusat kontrol untuk penyedia layanan energi yang berfungsi melihat mendata kapasitas listrik pada *energy storage* yang kemudian akan memberikan keputusan pendistribusian energi listrik.

3. Solusi terjadi Gangguan pada Sistem Distribusi

Pada dasarnya sistem pada *smart grid* sudah memiliki kemampuan mendeteksi, mengantisipasi dan merespon terhadap masalah yang terjadi pada sistem jaringannya, karena sensor-sensor pada *smart grid* mengirim data, kondisi maupun keadaan lainnya secara real time ke base kontrol [10]. Oleh karena itu, apabila terjadi gangguan distribusi pada suatu wilayah maka secara cepat base kontrol akan memback up keadaan tersebut agar tidak terjadi ganguan pada wilayah lainnya ataupun wilayah distribusi yang terganggu mendapatkan supply distribusi pengganti. Misalnya pada suatu wilayah mendapatkan pasokan listrik dari power plan yang berasal dari panel surya tetapi terjadi gangguan distribusi listrik dari panel surya ke wilayah tersebut, dengan adanya *smart grid* gangguan tersebut dapat diatasi dengan penggantian distribusi listrik dari power plan lain yang memiliki cadangan listrik berlebih. Maka dari itu pengiriman data dan pengontrolan secara real time ini dapat memudahkan konsumen dan *utility* dalam ketersediaan energi listrik yang memadai.

4. Respon Insiden dalam Sistem *Smart Grid*

Pada sebuah pengamatan terhadap perusahaan pengeboran minyak di Norwegia, insiden yang terjadi pada perusahaan tersebut mayoritas tidak berbahaya karena hanya menyebabkan gangguan kecil dan mengurangi efisensi saja [10]. Insiden yang lebih berbahaya yang dapat menonaktifkan peralatan teknis seperti sensor, komputer dan koneksi jaringan, yang mengganggu kelangsungan produksi tidak pernah terjadi atau tidak di laporkan ke khalayak umum. Yang termasuk insiden parah dalam katergori

ini yaitu saat insiden dapat menyebabkan kerusakan pada rantai ekosisem perusahaan, di mana hasil akhirnya mungkin kerugian ekonomi yang besar, kerusakan lingkungan dan hilangnya nyawa. Penanganan insiden yang efektif dapat meminimalkan konsekuensi terjadinya sebuah insiden dan dengan demikian menjamin kelangsungan bisnis.

Sebuah skema untuk menanggapi insiden keamanan harus maju dan perusahaan perlu melatih untuk memastikan bahwa skema respon terhadap insiden akan bekerja dalam kasus insiden yang sebenarnya. Misalnya sebuah skema perlu dirancang untuk menentukan bagaimana hal-hal yang dilakukan apabila terjadi sebuah insiden dan bagaimana penanganan untuk melaporkan insiden tersebut, siapa yang bertanggung jawab atas tindakan tersebut, bagaimana pengalaman dari insiden tersebut menjadi bahan cerminan untuk mencegah terjadinya insiden serupa. Banyak perusahaan-perusahaan yang tidak melaporkan dan membagi pengalaman mereka tentang bagaimana suatu insiden terjadi dan bagaimana insiden tersebut diatasi. Oleh karena itu perlunya dibentuk badan khusus yang mengorganisir semua perusahaan yang bergerak dibidang yang sama untuk berkumpul dan membagi pengalaman mereka, maka dari itu sudah dibentuk badan-badan tersebut yaitu National Institute of Standards and Technology Interagency Report (NISTIR). NISTIR merupakan badan khusus yang bergerak dalam bidang keamanan dan manajemen resiko dari keamanan jaringan. NIST dibentuk untuk koordinasi penelitian di bidang *smart grid* yang bertugas melaporkan pekerjaan mereka secara berkala dan memberikan solusi-solusi tentang resiko yang akan dihadapi dan bagaimana melakukan pencegahan dan penangan terjadinya insiden pada *smart grid* [13]. Seperti contohnya NISTIR Draf 7628 [1, 10] tentang pedoman keamanan siber pada *smart grid* dengan judul *Smart Grid Cyber Security Strategy and Requirements*, sedangkan sistem *Incident Response Management* (IRMA) dalam bidang jaringan SCADA dijelaskan oeh ISO/IEC TR 18044 dan NIST 800-61.

Beberapa langkah yang dilakukan untuk persiapan menghadapi sebuah insiden, saat terjadi insiden dan sesudah dilakukannya penanganan insiden tersebut adalah sebagai berikut [1, 10, 11, 12].

a. Persiapan untuk Menghadapi Insiden

Dari persiapan ini diharapkan para karyawan memiliki persiapan dan siap apabila sewaktu-waktu terjadi sebuah insiden. Dibawah ini merupakan hal-hal yang perlu dilakukan dalam persiapan dalam menghadapi terjadinya sebuah insiden.

1) Menentukan kemungkinan apa saja yang akan mendapatkan sebuah insiden, aset apa saja yang paling krusial dan perlu ditangani terlebih dulu apabila terjadi insiden dan pengelompokan sector karyawan yang akan diberikan laporan apabila terjadi insiden
2) Sebelum terjadinya insiden sebaiknya melakukan persiapan dokumentasi perihal rutinitas, konfigurasi dan sistem dari berbagai bidang. Hal tersebut dapat digunakan sewaktu-waktu terjadi insiden seseorang yang bertanggung jawab dibidang tersebut berhalangan hadir.
3) Membuat skema siapa saja yang bertangguang jawab apabila terjadinya sebuah insiden. Hal tersebut dilakukan untuk skema pelaporan apabila terjadi insiden agar skema pergerakan terjadinya insiden sistematis dan tidak beraturan yang menyebabkan keadaan semakin kacau.
4) Menciptakan kesadaran SDM tentang pentingnya keamanan informasi dan pelatihan untuk meningkatkan kemampuan mendeteksi insiden dan reaksi saat terjadinya insiden.
5) Selalu memonitoring segala aspek untuk mengetahui efisiensi dan kualitas. Apabila efisiensi dan kualitas menurun maka lihat aspek yang mempengaruhinya. Hal tersebut mungkin saja sudah terjadi insiden kecil yang tidak dapat terdeteksi dengan baik

b. Mendeteksi dan Menghadapi Insiden

Apabila sudah terjadi sebuah insiden maka hal yang sebaiknya dilakukan adalah sebagai berikut.

1) Deteksi sebuah insiden dapat diketahui secara kebetulan bahwa disuatu bidang terjadi insiden atau dengan pendeteksian rutin seperti scanner virus pada computer. Langkah utama apabila insiden telah di deteksi yaitu memberikan peringatan kepada karyawan lain dan mencari siapa yang harus bertanggung jawab untuk menangani insiden tersebut.
2) Menilai tingkat keparahan dari insiden tersebut apakah insiden tersebut mempengaruhi terhadap produksi ataupun keselamatan dan menambah personil tambahan jika diperlukan untuk menangani insiden tersebut.
3) Memutus dan mengisolasi aliran yang terkena insiden agar insiden tersebut tidak menyebar ke bidang lainnya, sebisa mungkin memback up bidang yang terkena insiden tersebut agar tidak mengurangi kerugian yang lebih banyak, serta pendokumentasian dan pelaporan telah terjadi insiden dengan mencantumkan masalah yang telah terjadi dan bagaimana menanganinya. Dokumentasi tersebut sangan berguna jika terjadi insiden di lain hari ataupun untuk dianalisa lebih lanjut tentang insiden yang telah terjadi dan di evaluasi agar tidak terulang dikemudian hari.
4) Merancang komunikasi untuk menginformasikan tentang insiden tersebut dan memilih individu yang sebaiknya dihubungi.
5) Memulihkan seperti keadaan normal, memastikan bahwa keadaan telah aman dan mengembalikan bidang yang terkena insiden ke jaringan sebelumnya agar sistem bekerja normal kembali.
6) Hal yang terakhir yang dilakukan apabila keadaan sudah berjalan normal adalah mengeksploitasi insiden tersebut dan

mengingkatkan keamanan agar tidak terjadi insiden lain di lain waktu.

c. Pembelajaran dari Insiden dan Bagaimana Mengatasinya

Hal yang perlu dilakukan untuk meningkatkan kesiapan jika suatu hari terjadi insiden dan mengatasinya dengan sistematis adalah dengan simulasi terjadinya insiden. Simulasi dilakukan untuk mengetahui pergerakan-pergerakan apa yang seharusnya penting untuk dilakukan dan yang tidak harus dilakukan agar semua SDM tidak kaget jika terjadi sebuah insiden besar yang dapat merusak sistem.

.

BAB IV

KESIMPULAN

Smart grid merupakan suatu konsep pengelolaan energi listrik yang mampu mengkoordinasikan peran pembangkit listrik kecil berbahan bakar energi terbarukan seperti energi listrik tenaga surya, angin, air, dan ombak secara optimal. Menurut NIST layer pada *smart grid* yaitu layer power dan energi, layer komunikasi dan layer komputerisasi. Layer komunikasi dan komputerisasi memungkinkan adanya komunikasi layer power dan energi saling berkomunikasi timbal balik antara penyedia layanan dengan konsumen. Persoalan yang perlu di garis bawahi dari *smart grid* yaitu tentang keamanan dari serangan *cyberattack* dan tata kelola bagaimana respon saat terjadinya insiden karena sistem ini menggunakan sistem *network* untuk mengirimkan dan menerima data.

Serangan-serangan pada sistem *smart grid* harus diwaspadai karena sudah terjadi peristiwa terjadinya serangan yang menyebabkan produksi pada pembangkit listrik berhenti selama beberapa hari. Maka dari itu diperlukan pengamanan dan pencegahan yang baik terhadap virus maupun serangan siber agar insden tersebut tidak terjadi. Apabila terjadi insiden maka harus melakukan urutan-urutan yang terstuktur terhadap penanganan insiden tersebut. Penanganan tersebut berupa persiapan sebelum terjadinya insiden berupa pelatihan dan membuat skema-skema saat terjadinya insiden, kemudian mendeteksi dan menangani insiden, dan yang terakhir tahapan pemulihan keadaan semula bagian yang terkena insiden dan pendokumentasian bagaimana sebab insiden tersebut terjadi dan cara penanganannya.

DAFTAR PUSTAKA

[1] NIST, "Guidelines for Smart Grid Cyber Security," *NISTIR 7628*, Sept 2010.

[2] A. B. Setiawan, A. Syamsudin, and Y. Rosmansyah, "Peningkatan Keamanan *Supervisory Control and Data Acquisition* (Scada) pada *Smart Grid* Sebagai Infrastruktur Kritis (Studi Kasus Pada Sistem Scada Ketenagalistrikan)," *Jurnal e-indonesia initiatives*, http://eii-forum.or.id/repositori

[3] M. A. Iskandar, F. Armansyah, A. Prastawa, and H. Hilal," Studi Disain Smart Micro Grid di Apartemen Taman Rasuna," *repositori.bppt.go.id*..

[4] D. A. Susanto and B. B. Louhenapessy, "Ketersediaan Standar dalam Mendukung Penerapan Sistem Smart Grid di Indonesia," *Jurnal Standardisasi*, vol. 6, no. 2, pp. 147-158, July 2014.

[5] Takashi Hamasaka, "Japan's New Roadmap to International Smart grid Standards and Collaborations with other Countries", http://www.teriin.org/events/EnergyForum/S1a4_METI_Yamamoto.pdf.

[6] S. Javadi and S. Javadi, "Steps to Smart Grid Realization," *Proc. Of the 4th WSEAS international Conference on Computer Engineering and Applications, Cambridge, USA*, pp. 223-228, Jan. 2010.

[7] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Cyber security challenges in smart grids," *Proc. ISGT Europe'11*, pp. 1-8, Dec. 2011.

[8] J. Sawyer and D. C. Weber, "Advanced Metering Infrastructure Security," *InGuardians, Inc*, 2012.

[9] I Colak, S. Sagiroglu, C. Covrig, "A survey on the critical issues in smart grid technologies". *Elsevieer Jurnal Renew Sustain Energy* Rev ;54, pp. 396–405, 2016.

[10] M. Gilje Jaatun, E. Albrechtsen, M. Line, I. Tøndel, O. H. Longva, "A framework for incident response management in the petroleum industry," *Intl. Journal of Critical Infrastructure Protection 2 (2009) pp. 26-37*, Feb. 2009.

[11] NIST, "Smart Grid Cyber Security Strategy and Requirements," *NISTIR 7628*, Sept 2009.

[12] A. R. Metke and R. L. Ekl., "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1(1), pp.99–107, June 2010.

[13] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - the new and improved power grid: A survey," *IEEE Commun. Surveys Tutorials*, vol. 14, no. 4, 2012.

[14] K. Kaur and N. Kumar, “Smart Grid with Cloud Computing : Architecture, Security Issues and Defense Mechanism,” *International Conference on Industrial and Information Systems (ICIIS)*, vol. 9, pp. 1-6, 2014.

[15] Y. Yang, T. Littler, S. Sezer and H. F. Wang, “Impact of Cyber-Security Issues on Smart Grid,” *Innovative Smart Grid Technologies (ISGT Europe), IEEE PES International Conference and Exhibition*, vol. 2, pp. 1-7, Dec. 2011.

[16] M. Erol-Kantarci, B. Kantarci, and H. T. Mouftah, “Reliable Overlay Topology Design for the Smart Microgrid Network,” *IEEE Network*, Special Issue