Tata Kelola Insiden Respon pada Jaringan *Smart Grid*

Khilda Afifah/23214316
Mata Kuliah
Teknik Elektro
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

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 dalam konsumsi energy listrik, meningkatkan kehandalan dalam bidang tenaga listrik, mengurangi eefek rumah kaca karena emisi karbon, dan mendukung kehadiran dari pemanfaatan energi terbarukan secara optimal.

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 energy listrik dari cahaya matahari, maka saat energy listrik yang di hasilkan 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.

Persoalan yang perlu di garis bawahi dari *smart grid* yaitu tentang keamanan dari serangan *cyberattack* dan tata kelola saat terjadinya insiden tersebut karena sistem ini menggunakan sistem *network* untuk mengirimkan data. Dengan melihat standar keamanan dan tata kelola dari berbagai bidang pengetahuan dan solusi maka solusi-solusi keamanan terbaik yang sudah ada dapat dimanfaatkan untuk sistem keamanan dan tata kelola insiden pada komunikasi jaringan *smart grid* ini. Beberapa subsistem dari elemen keamanan dan tata kelola insiden respon 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.

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

Referensi :

[1] M. Erol-Kantarci and H. T. Mouftah, "Smart grid forensic science: Applications, challenges and open issues," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 68–74, Jan. 2013.

[2] M. Erol-Kantarci, B. Kantarci, and H. T. Mouftah, "Reliable Overlay Topology Design for the Smart Microgrid Network," *IEEE Network*, Special Issue on Communication Infrastructures for Smart Grid, vol. 25, no. 5, Sept./Oct. 2011, pp. 38–43.

[3] 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.

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

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

[6] T. Kilpatrick, J. Gonzalez, R. Chandia, M. Papa, and S. Shenoi, "Forensic analysis of SCADA systems and networks," *Int. J. Secur. Netw.*, vol. 3, no. 2, pp. 95–102, 2008.

[7] W. Wang, "Risk-aware Attacks and Catastrophic Cascading Failures in U.S. Power Grid," *Proc. IEEE GLOBECOM*, Houston, TX, Dec. 2011.

[8] Y. Yan ,"A Survey on Cyber Security for Smart Grid Communications," *IEEE Commun. Surveys & Tutorials*, vo. 14, no. 4, 2012.