ANALISIS CELAH KEAMANAN DAN MEKANISME PENGAMANAN *SMART CITY* MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK DAN REFERENSI INFORMATIF ISO 27001:2013

TESIS

Oleh :

Taufik Hidayat

55418110005

PROGRAM MAGISTER TEKNIK ELEKTRO

PROGRAM PASCASARJANA

UNIVERSITAS MERCU BUANA

TAHUN 2020

ANALISIS CELAH KEAMANAN DAN MEKANISME PENGAMANAN *SMART CITY* MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK DAN REFERENSI INFORMATIF ISO 27001:2013

TESIS

Diajukan sebagai Salah Satu Syarat untuk Menyelesaikan

Program Pascasarjana Program Magister Teknik Elektro

Oleh :

Taufik Hidayat

55418110005

UNIVERSITAS MERCU BUANA

PROGRAM PASCASARJANA

PENGESAHAN TESIS

Judul	:	Analisis Celah Keamanan dan Mekanisme Pengamanan *Smart City* Menggunakan NIST Cybersecurity Framework dan Referensi Informatif ISO 27001:2013
Nama	:	Taufik Hidayat
NIM	:	55418110005
Program	:	Pascasarjana Program Magister Teknik Elektro
Konsentrasi	:	Security ICT
Tanggal	:	28 Agustus 2020

Mengesahkan,

Pembimbing

(Dr. Marza Ihsan Marzuki, MT)

Direktur Pascasarjana

(Prof. Dr. -Ing. Mudrik Alaydrus)

Ketua Program Studi

(Prof. Dr. Andi Adriansyah, M.Eng)

PERNYATAAN *SIMILARITY CHECK*

Saya yang bertanda tangan di bawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh:

Nama : Taufik Hidayat

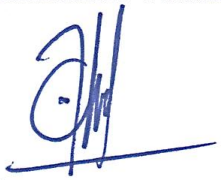
NIM : 55418110005

Program Studi : Magister Teknik Elektro

dengan judul "Analisis Celah Keamanan dan Mekanisme Pengamanan *Smart City* Menggunakan NIST Cybersecurity Framework dan Referensi Informatif ISO 27001:2013", telah dilakukan pengecekan similarity dengan sistem Turnitin pada tanggal 19 Agustus 2020, didapatkan nilai persentase sebesar 28 %.

Jakarta, 28 Agustus 2020

Administrator Turnitin



Arie Pangudi, A.Md

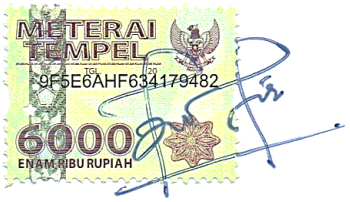
PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam Tesis ini :

Judul	: Analisis Celah Keamanan dan Mekanisme Pengamanan *Smart City* Menggunakan NIST Cybersecurity Framework dan Referensi Informatif ISO 27001:2013
Nama	: Taufik Hidayat
NIM	: 55418110005
Program	: Magister Teknik Elektro
Konsentrasi	: Security ICT
Tanggal	: 28 Agustus 2020

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Pembimbing yang telah ditetapkan dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana Nomor : 09-4/630/F-STT/VIII/2019. Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Bekasi, 28 Agustus 2020



Taufik Hidayat

KATA PENGANTAR

Puji syukur kehadirat Allah SWT., karena dengan berkah, rahmat, dan hidayah-Nya lah penulis dapat menyelesaikan tesis ini. Tak lupa pula shalawat dan salam penulis haturkan kepada baginda besar Rasulullah Muhammad SAW beserta keluarga, sahabat dan pengikut setianya hingga akhir zaman.

Tesis ini tidak mungkin dapat terselesaikan tanpa adanya bantuan dari banyak pihak, oleh sebab itu penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Kedua orang tua dan keluarga yang selalu mendukung, terutama kepada ibu dan bapak atas doanya, juga kepada istri yang selalu memotivasi penyelesaian studi S2.
2. Anak-anak tercinta, yang menjadi penyemangat dan penyejuk hati dengan tingkah laku kekanak-kanakannya sehingga memberikan energi ekstra untuk dapat menyelesaikan tesis ini.
3. Dr. Marza Ihsan Marzuki, MT, sebagai pembimbing tesis, karena berkat ilmu, arahan, dan bimbingannya, akhirnya penulis dapat menyelesaikan tesis dan beberapa jurnal pendukung lain.
4. Dr. Setiyo Budiyanto, MT, sebagai penelaah dan penguji tesis, atas arahan, saran, kritik dan masukannya yang membangun.
5. Segenap dosen pengajar di Magister Teknik Elektro UMB : Prof. Dr. -Ing. Mudrik Alaydrus sebagai Direktur Pascasarjana, Prof. Andi Adriansyah, M.Eng selaku Ketua Program Studi Magister Teknik Elektro, Dr. Iwan Krisnadi, MBA, Dr. Denny Setiawan, MT, Ir. Bambang Setiawan, MT, dan lainnya yang tidak bisa disebutkan satu persatu.
6. Miyono serta seluruh staf dan tim pendukung Program Magister Teknik Elektro UMB yang selalu siap membantu masalah administrasi.
7. Rekan-rekan MTEL 22 dan MTEL 23 yang tidak bisa disebutkan satu persatu, yang telah berjuang bersama untuk menyelesaikan studi ini, semoga selalu diberikan kesehatan dan keluangan waktu sehingga semua dapat lulus tepat pada waktunya.

Penulis menyadari bahwa karya tulis ini pasti tidak luput dari kesalahan dan kekurangan oleh karena itu saran dan masukan dari para pembaca adalah sangat diharapkan, sebagai bahan untuk memperbaiki kesalahan dan kekurangan yang ada. Akhir kata penulis berharap semoga tulisan ini bisa memberikan manfaat, sekecil apapun itu, bagi pembacanya, khususnya untuk diri penulis sendiri.

Bekasi, 28 Agustus 2020

Penulis

Taufik Hidayat

ABSTRAK

Infrastruktur sistem *smart city (fisik, informasi, Information and Communication Technology, dan services)* pemerintah kota/kabupaten di Indonesia yang dimaksimalkan untuk mensupport program *smart city* saat ini belum mengindikasikan *cybersecurity* menjadi bagian yang tidak terpisahkan dari *smart city*. Padahal konsep *smart city* dengan segala macam interkoneksi perangkat ICT, aplikasi, sistem, IoT, sensor, actuator, cloud platform, server dan *services* yang ada sangat rentan dan memiliki risiko terhadap ancaman dan serangan yang dapat membahayakan sistem secara keseluruhan. Data statistik pun menunjukan adanya peningkatan serangan *cybersecurity* yang signifikan setiap tahunnya terhadap semua layanan berbasis internet. Atas dasar hal tersebut di atas, penelitian ini dimaksudkan untuk mengamankan *smart city* dengan melakukan analisis terhadap risiko adanya celah keamanan pada *smart city* dan bagaimana mekanisme pengamanannya dengan pendekatan dari sisi *cybersecurity* dengan menggunakan NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) dan referensi informatif ISO 27001:2013. Penggunaan NIST CSF dan ISO 27001:2013 diharapkan membuat aktivitas *cybersecurity* menjadi lebih terarah dan terstruktur. Penelitian yang dilakukan menunjukkan adanya 72 buah celah keamanan pada s*mart city* yang berhasil teridentifikasi dan 76 buah mekanisme pengamanan yang sesuai sebagai langkah mitigasi risiko, ancaman dan serangan siber.

***Kata Kunci** : Smart City, Cybersecurity, ICT, IoT, Sensor*

ABSTRACT

Smart city system infrastructure (physical, information, Information and Communication Technology, and services) city / district government In Indonesia, which is maximized to support the smart city program, currently it has not indicated that cybersecurity is an integral part of a smart city. Even though the concept of a smart city with all kinds of interconnection of ICT devices, applications, systems, IoT, sensors, actuators, cloud platforms, servers and services is very vulnerable and has the risk of threats and attacks that can harm the system as a whole. Statistical data also shows a significant increase in cybersecurity attacks every year against all internet-based services. On the basis of the foregoing, this study is intended to secure the smart city by analyzing the risk of security gaps in the smart city and how the security mechanism uses a cybersecurity approach, using the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and informative references ISO 27001: 2013. It is hoped that the use of NIST CSF and ISO 27001: 2013 will make cybersecurity activities more targeted and structured. The research conducted shows that there are 72 security gaps in the smart city that have been identified and 76 security mechanisms that are suitable for mitigating risks, threats and cyber attacks.

Keywords *: Smart City, Cybersecurity, ICT, IoT, Sensor*

DAFTAR ISI

JUDUL i
PENGESAHAN TESIS iii
PERNYATAAN *SIMILARITY CHECK* iv
PERNYATAAN v
KATA PENGANTAR vi
ABSTRAK viii
ABSTRACT ix
DAFTAR ISI x
DAFTAR TABEL xii
DAFTAR GAMBAR xiii
DAFTAR SINGKATAN xiv
BAB I PENDAHULUAN 1
1.1. Latar belakang 1
1.2. Rumusan masalah 4
1.3. Tujuan penelitian 5
1.4. Manfaat penelitian 5
1.5. Ruang lingkup 6
BAB II KAJIAN PUSTAKA 7
2.1. *Smart city* 7
2.2. *Security and challenges* pada *smart city* 9
2.3. *Cybersecurity* 13
2.4. *Cybersecurity risk management* pada *smart city* 13
2.4.1. NIST Framework *for Improving Critical Infrastructure Cybersecurity* 15
2.4.2. ISO 27001:2013 17
2.5. Penelitian Sejenis 18
BAB III METODOLOGI 22
3.1. Gambaran umum *smart city* 22
3.2. NIST CSF untuk mengamankan s*mart city* 27
BAB IV HASIL DAN ANALISIS 32

4.1. Tahapan implementasi NIST CSF 32
4.1.1. *Prioritize and scope* 32
4.1.2. *Orient* 36
4.1.3. *Create a current profile* 38
4.1.4. *Conduct risk assessment* 45
4.1.5. *Create a target profile* 46
4.1.6. *Determine, analyze and prioritize gaps* 47
4.1.7. *Implement action plan* 49
4.2. Analisis celah keamanan dan mekanisme pengamanan *smart city* 50
BAB V KESIMPULAN DAN SARAN 55
5.1. Kesimpulan 55
5.2. Saran 55
DAFTAR PUSTAKA 57
LAMPIRAN 60
Lampiran 1 Aset register kategori informasi 60
Lampiran 2 Aset register kategori SDM (personil) 61
Lampiran 3 Aset register kategori perangkat keras 62
Lampiran 4 Aset register kategori perangkat lunak 63
Lampiran 5 Aset register kategori layanan pihak ketiga dan aset tak berwujud 64
Lampiran 6 Risk register berbasis aset informasi 65
Lampiran 7 Risk register berbasis aset SDM (personil) 70
Lampiran 8 Risk register berbasis aset perangkat keras 72
Lampiran 9 Risk register berbasis aset perangkat lunak 74
Lampiran 10 Risk register berbasis aset layanan pihak ketiga 76
Lampiran 11 Risk register berbasis aset tak berwujud 77
Lampiran 12 Risk register berbasis aset informasi part 2 78
Lampiran 13 Risk register berbasis aset SDM (personil) part 2 81
Lampiran 14 Risk register berbasis aset perangkat keras part 2 82
Lampiran 15 Risk register berbasis aset perangkat lunak part 2 84
Lampiran 16 Risk register berbasis aset layanan pihak ketiga dan aset tak berwujud part 2 85

DAFTAR TABEL

Tabel 4.1.1.1 *Control objectives* dan *control* pada ISO 27001:2013 32
Tabel 4.1.1.2 Pemetaan 30 *Control Objectives ISO 27001:2013* menjadi 16 *Subcategory Framework Core NIST CSF* 34
Tabel 4.1.2.1 Kriteria penilaian kritikalitas aset 37
Tabel 4.1.3.2 Pemetaan 30 control objectives *smart city* terhadap 59 sub kategori NIST CSF 39
Tabel 4.1.4.1 Matriks penilaian risiko 45
Tabel 4.1.5.2 Sub kategori pada NIST CSF sebagai target profil *smart city* 46
Tabel 4.1.6.1 Hasil analisis gap 48
Tabel 4.1.6.2 Rencana aksi menuju level 3 49
Tabel 4.2.1 Celah keamanan dan mekanisme pengamanan *smart city* 50

DAFTAR GAMBAR

Gambar 1.1.1 Statistik isu *cybersecurity* tahun 2019.....3
Gambar 1.1.2 Penggunaan NIST CSF di AS 4
Gambar 2.5.1 Penelitian sejenis terkait *smart city* dan *cybersecurity* 18
Gambar 3.1.1 Cakupan domain pada *smart city* 24
Gambar 3.1.2 Arsitektur *smart city* 25
Gambar 3.1.3 Alur penelitian.....27
Gambar 3.2.1 Diagram alur penerapan *cybersecurity program*.....31
Grafik 4.1.3.1 Capaian sub kategori pada s*mart city* 38

DAFTAR SINGKATAN

ICT	: Information and Communication Technology
NIST	: National Institute of Standardization and Technology
ISO	: International Organization of Standardization
NIST CSF	: NIST Cybersecurity Framework
COBIT	: Control Objectives for Information and Related Technology
CSA	: Cybersecurity Agency of Singapore
IoT	: Internet of Things
OPD	: Organisasi Perangkat Daerah