ANALISIS KEAMANAN JARINGAN STMIK AMIKOM YOGYAKARTA BERDASARKAN ISO/IEC 27001:2005 STANDAR A.11.4.4

(Studi Kasus: Innovation Center STMIK Amikom Yogyakarta)

SKRIPSI

disusun oleh

Nur Hariawan Bulu

10.11.4019

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013

ANALISIS KEAMANAN JARINGAN STMIK AMIKOM YOGYAKARTA BERDASARKAN ISO/IEC 27001:2005 STANDAR A.11.4.4

(Studi Kasus: Innovation Center STMIK Amikom Yogyakarta)

SKRIPSI

untuk memenuhi sebagai persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Nur Hariawan Bulu

10.11.4019

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013

PERSETUJUAN

SKRIPSI

ANALISIS KEAMANAN JARINGAN STMIK AMIKOM YOGYAKARTA BERDASARKAN ISO/IEC 27001:2005 STANDAR A.11.4.4

(Studi Kasus: Innovation Center STMIK Amikom Yogyakarta)

yang dipersiapkan dan disusun oleh

Nur Hariawan Bulu

10.11.4019

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 1 Mei 2013

Dosen Pembimbing,

Andi Sunyoto, M.Kom
NIK. 190302052

PENGESAHAN

SKRIPSI

ANALISIS KEAMANAN JARINGAN STMIK AMIKOM YOGYAKARTA BERDASARKAN ISO/IEC 27001:2005 STANDAR A.11.4.4

(Studi Kasus: Innovation Center STMIK Amikom Yogyakarta)

yang dipersiapkan dan disusun oleh

Nur Hariawan Bulu

10.11.4019

telah dipertahankan di depan Dewan Penguji
pada tanggal 11 Juli 2013

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Sudarmawan, M.T **NIK. 190302035**	
Andi Sunyoto, M.Kom **NIK. 190302052**	
Tonny Hidayat, M.Kom **NIK. 190302182**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 13 Juli 2013

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 13 Juli 2013

Nur Hariawan Bulu
NIM. 10.11.4019

KATA PENGANTAR

Dengan memanjatkan puji syukur kepada Allah SWT atas limpahan rahmat, taufik serta hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan tepat pada waktunya yang berjudul "Analisis Keamanan Jaringan STMIK Amikom Yogyakarta Berdasarkan ISO/IEC 27001:2005 Standar A.11.4.4".

Skripsi ini ditulis guna memperoleh gelar Sarjana jurusan Teknik Informatika, STMIK Amikom Yogyakarta.

Selesainya penyusunan skripsi ini berkat bantuan dari berbagai pihak, oleh karena itu, penulis sampaikan terima kasih kepada yang terhormat:

1. Bapak Andi Sunyoto, M.Kom, selaku dosen pembimbing yang dengan sabar terus-menerus membimbing penulis dalam menyelesaikan penulisan skripsi ini. Beliau mengajarkan metode penulisan yang sangat baik dan memberikan arahan yang membangun.
2. Bapak Rachmad Agung Sukmawan, selaku manajer perangkat keras dan infrastruktur Innovation Center STMIK Amikom Yogyakarta memberikan penulis data-data dan informasi yang penulis perlukan demi penyelesaian penulisan skripsi ini.
3. Bapak Ir. Abas Ali Pangera, selaku dosen komunikasi data yang pertama kali mengajarkan tentang konsep jaringan atau Cisco kepada penulis.
4. Dosen-dosen STMIK Amikom Yogyakarta yang telah memberi ilmu dan pengetahuan.

5. Keluarga, Bapak, Ibu, Kakak dan Adik yang selalu memberi dukungan.
6. Pihak-pihak lainnya yang tidak sempat penulis sebutkan, yang selalu membantu dalam memberi semangat dan dorongan.

Semoga penyusunan skripsi ini dapat bermanfaat bagi pembaca, perusahaan, organisasi, dan lain sebagainya. Akhir kata, bila terdapat kesalahan dalam penyusunan skripsi, penulis minta maaf karena sesungguhnya kesempurnaan hanya milik-Nya, oleh karena itu penulis sangat mengharapkan kritik dan saran yang membangun

.

Yogyakarta, 9 Juli 2013

Nur Hariawan Bulu

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Informasi maupun data di era informasi seperti saat ini sudah menjadi hal yang sangat berharga. Bahkan kita bisa katakan sangat fital sehingga kerusakan ataupun kebocoran terhadap informasi suatu organisasi dapat mengakibatkan organisasi tersebut berhenti atau tutup. Dikarenakan begitu berharganya suatu informasi atau data maka tidaklah heran jika kemudian bermunculan beberapa pihak yang tidak bertanggung jawab dimana pihak tersebut berusaha mencuri maupun merusak dan mengubah data atau informasi dari sistem komputer yang dimiliki oleh suatu organisasi tertentu, apakah itu untuk kesenangan individual atau sekelompok orang, oleh karena itu dibutuhkan keamanan sistem informasi yang terjamin bahwa sistem kita aman.

Penelitian kali ini akan dilakukan di salah satu perguruan tinggi di Yogyakarta, yaitu STMIK Amikom Yogyakarta. Penelitian ini akan dilakukan dengan berdasarkan pada standar internasional ISO/IEC 27001:2005. Di dalam ISO/IEC 27001:2005 terdapat 11 domain. Penelitian ini akan lebih khusus tentang di salah satu domain, standar A.11.4.4, yaitu *remote diagnostic and configuration port security*. Terdapat dua jenis serangan, dari luar ataupun dari dalam jaringan. Diketahui bahwa serangan dari dalam lebih berbahaya dan sering terjadi daripada serangan dari luar, oleh karena itu disini akan dilakukan analisis pada salah satu jaringan dari dalam, yaitu diagnosa pengendalian jarak jauh dan konfigurasi *port security*.

Setelah penelitian dijalankan, maka didapatkanlah bahwa terdapat dua celah yang belum diimplementasikan oleh STMIK Amikom Yogyakarta, yaitu pencegahan serangan *brute force* pada layanan protokol SSH dan implementasi teknologi *port security* pada perangkat jaringan switch Cisco. Diharapkan, dengan adanya penelitian ini, perusahaan atau organisasi dapat menggunakannya demi pengamanan perangkat jaringan yang digunakan dalam sistem jaringan.

Kata Kunci: Informasi, Keamanan, Sistem Manajemen, Standarisasi, Perangkat Jaringan.

ABSTRACT

Information and data in the information age as it's been a very valuable thing. In fact we can say it is very vital that damage or leakage of the information an organization can lead the organization to stop or closed. Due to the preciousness of the information or data then it is no wonder if then popping some irresponsible parties where the party is trying to steal and destroy and alter data or information from a computer system owned by a particular organization, whether it's for fun individual or group of people, therefore needed information system security is assured that our systems secure.

This research will be conducted in one of the universities in Yogyakarta, STMIK Amikom Yogyakarta. This research will be carried out with international standards based on ISO/IEC 27001:2005. There are eleven domains in ISO/IEC 27001:2005.This study will more specifically about in one domain, A.11.4.4 standards, the remote diagnostic and configuration port security. There are two types of attack, from outside or from within the network. It is known that an attack from within is more dangerous and common than attacks from outside, therefore the analysis here will be done inside of networks, the remote control diagnostics and port security configuration.

After research conducted, then it was found that there were two gaps has not been implemented by STMIK Amikom Yogyakarta, namely the prevention of brute force attacks on SSH protocol and implementation of treatment technologies network device port security on Cisco switches. Hopefully this research, enterprise or organization can use for peacekeeping network devices used in network systems.

Keywords: *Information, Security, System Management, Standardization, Network Devices.*