JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

IMPLEMENTASI PCI-DSS UNTUK KEAMANAN DATA KARTU PEMBAYARAN PADA PT DHARMA LAUTAN NUSANTARA

Fahrizal[1)], Ade Surya Budiman[2)], Muhammad Rifqi Anuar[3)]
[1]Sistem Informasi, FTI, Universitas Bina Sarana Informatika
[2,3]Teknologi Informasi, FTI, Universitas Bina Sarana Informatika

Correspondence author: Fahrizal, fahrizal.fzl@bsi.ac.id, Jakarta, Indonesia

Abstract

The quality of service provided by the company must be maintained including providing transaction facilities using a secure credit card so that it can provide the best to customers and aims to increase the sense of trust in the company in making payments using credit cards. The method used to improve information security and corporate networks is to implement network security in accordance with the Payment Card Industry Data Security Standard (PCI-DSS) standard. The method used in this study is to identify data and communications that are the focus of security in compliance with PCI DSS, reduce the scope of security by implementing network segmentation by determining the classification of devices, communication lines and people into three categories based on the presence or absence of a relationship to data. credit cards, namely Cardholder Data Environment (CDE), Shared Network and Corporate Local Area Network. (LAN) Then manage the data communication traffic between the three segments according to compliance with the PCI DSS standard.

Keywords: PCI-DSS, VLAN, ACL'S, AAA, network security

Abstrak

Kualitas pelayanan yang diberikan perusahaan harus tetap dijaga diantaranya memberikan fasilitas bertransaksi menggunakan kartu kredit yang aman sehingga dapat memberikan yang terbaik kepada pelanggan dan bertujuan untuk meningkatkan rasa kepercayaan kepada perusahaan dalam melakukan pembayaran menggunakan kartu kredit. Cara yang diterapkan untuk meningkatkan keamanan informasi serta jaringan perusahaan yaitu dengan mengimplementasikan keamanan jaringan sesuai dengan standar *Payment Card Industry Data Security Standard* (PCI-DSS). Metode yang digunakan dalam penelitian ini yaitu dengan mengidentifikasi data dan komunikasi yang menjadi fokus pengamanan dalam kepatuhan terhadap PCI DSS, memperkecil ruang lingkup pengamanan dengan mengimplementasikan segmentasi jaringan dengan cara menentukan penggolongan perangkat, jalur komunikasi dan orang kedalam tiga kategori berdasarkan ada atau tidaknya hubungan terhadap data kartu kredit yaitu *Cardholder Data Environment* (CDE), *Shared Network* dan *Corporate Local Area Network* (LAN). Kemudian mengatur lalu lintas komunikasi data antar ketiga segmen tersebut sesuai kepatuhan terhadap standar PCI DSS.

Kata Kunci: PCI-DSS, VLAN, ACL'S, AAA, keamanan jaringan

A. PENDAHULUAN

Kartu kredit merupakan salah satu alat pembayaran yang banyak digunakan karena kemudahan kenyamanan dan kecepatan yang ditawarkan pada setiap transaksinya. Berdasarkan data Bank Indonesia penggunaan kartu kredit periode September 2021 tercatat mengalami kenaikan sebesar 13,07%. Namun penggunaan kartu kredit memiliki risiko keamanan karena rentan terhadap pencurian data yang utamanya pencurian terhadap uang pemilik kartu kredit yang saat ini dikenal dengan istilah *carder*. *Carding* adalah bentuk kejahatan menggunakan nomor kartu kredit orang lain untuk dibelanjakan (*non face to face transaction*) tanpa sepengetahuan pemiliknya yang sah. Transaksi lazimnya dilakukan secara elektronik. Pelaku kejahatan kartu kredit atau *carder* memperoleh data kartu kredit dengan beberapa cara yaitu dengan rekayasa sosial atau *social engineering* yaitu dengan cara berpura-pura sebagai Bank penerbit kartu kredit *(acquirer*) menghubungi pemegang kartu melalui telepon, email dan sebagainya dengan alasan mengadakan undian atau memerintahkan nasabah untuk segera mengganti kartu kreditnya hingga nasabah tersebut percaya dan memberikan informasi data kartu kreditnya. Atau juga dengan menggunakan teknologi informasi yang rentan dilakukan oleh oknum yang memiliki akses ke komputer dan perangkat jaringan yang melakukan pencatatan *(create)*, pemprosesan *(process)*, penyimpan *(save)*, mentransmisikan (*transmit*) dan menerima (*receive)* yang dalam standar Payment Card Industry (PCI) Data Security Standard (DSS) perangkat-perangkat tersebut masuk dalam lingkup *Cardholder Data Environment* (CDE). Atau juga oknum yang memiliki akses ke perangkat yang dapat berkomunikasi tanpa pembatasan dan pencatatan (log) ke perangkat-perangkat CDE. Tindakan kejahatan tersebut dapat dilakukan oleh orang yang bekerja di perusahaan yang menerima pembayaran menggunakan kartu kredit yang oleh standar PCI DSS disebut *merchant.* Karena itulah PCI Security Standards Council's (SSC) yang terdiri atas *brand* American Express, Discover Financial Services, JCB International, MasterCard Worldwide, Visa Inc. dan Visa Europe mensyaratkan standar kepatuhan bagi setiap *acquirer*, *merchant* dan setiap organisasi baik itu besar maupun kecil yang menerima, mentransmisikan, atau menyimpan data pemegang kartu/ *Card Holder Data* (CHD) apapun yang termasuk dalam SSC, untuk mengimplementasikan standar yang disebut sebagai PCI DSS.

PT Dharma Lautan Nusantara sebagai *merchant* yang mengutamakan kualitas layanan terhadap pelanggan dengan cara mengimplementasikan PCI DSS untuk memberikan rasa aman ketika bertransaksi atau melakukan pembayaran menggunakan kartu kredit dengan melakukan pembenahan dari sisi jaringan komputer yang aman sesuai rekomendasi dari persyaratan / *requirement* PCI DSS. Dalam tulisan ini akan dibahas tentang *requirement* yang dipersyaratkan PCI DSS bagi merchant dalam menyediakan keamanan data dalam bertransaksi menggunakan kartu kredit. Dalam tulisan ini untuk membentuk sistem jaringan komputer yang *secure.*

Maksud dalam tulisan ini dapat dirumuskan sebagai berikut :

1. Bagaimana memperkecil ruang lingkup pengamanan data pada jaringan PT Dharma Lautan Nusantara.
2. Bagaimana meningkatkan keamanan lalu lintas data pada jaringan PT Dharma Lautan Nusantara.
3. Bagaimana mengimplementasikan keamanan data pada jaringan PT Dharma Lautan Nusantara sesuai dengan persyaratan standar PCI-DSS.

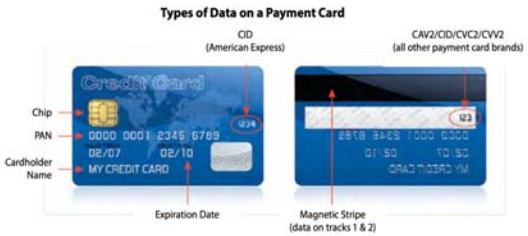
Penelitian ini memperoleh referensi dari standar PCI DSS dan beberapa publikasi dokumen dan jurnal yang terkait yaitu:

1. *PCI DSS Quick Reference Guide Understanding the Payment Card Industry*

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Data Security Standard version 3.2.1, yang diterbitkan oleh PCI SSC. Dalam publikasi tersebut dijelaskan tentang pengertian PCI DSS, Card Holder Data yang menjadi object data yang harus dilindungi seperti pada gambar 1 yaitu:

a. Informasi data yang terdapat pada Chip kartu
b. *Primary Account Number* (PAN)
c. Nama pemegang kartu
d. Tanggal berlaku kartu
e. *Credit Card Identification Code* (CID)
f. Informasi pada *magnetic stripe* dan
g. Tiga angka di belakang kartu (CAV2/CID/CVC2/CVV2)



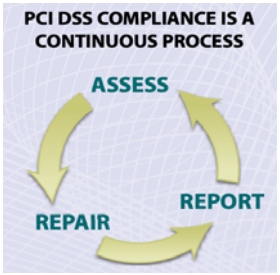
Gambar 1. *Cardholder Data* atau Tipe Data pada Kartu Pembayaran

Pada dokumentasi ini juga dijelaskan 12 *requirement* seperti pada table 1dibawah ini

Tabel 1. Requirement PCI-DSS

Goal	PCI DSS Requirement
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti- virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Pada dokementasi tersebut juga terdapat informasi framework yang digunakan oleh PCI DSS yang diperlihatkan pada gambar 2 di bawah ini.



Gambar 2 . Framework PCI DSS

2. Informasi suplemen yang diterbitkan oleh PCI SSC dengan judul *"Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation"*. Dalam publikasi ini dijelaskan tentang *requirement* dan rekomendasi dari PCI DSS untuk *merchant* dalam mengimplementasi standar keamanan data dengan mengidentifikasi data yang harus diamankan, memperkecil scope pengamanan dengan segmentasi jaringan dan mengatur alur komunikasi dari dan

ke segmen *CDE* yang menjadi fokus pengamanan.

3. *PCI DSS Compliance IT Checklist* yang diterbitkan oleh security matriks. berisi daftar 12 *requirement* PCI DSS yang harus dipenuhi oleh pengelola sistem Teknologi Informasi (TI).
4. Jurnal yang berjudul "Penyusunan Panduan Pengelolaan Keamanan Informasi Untuk Firewall Configuration Berdasarkan Kerangka Kerja PCI DSS v.3.1 dan COBIT 5" yang ditulis oleh Bagus Puji Santoso, Eva Hariyanti dan Eto Wuryanto. Dalam jurnal ini dibahas tentang bagaimana membuat panduan tata kelola keamanan informasi untuk konfigurasi firewall yang sesuai dengan kerangka kerja PCI DSS v.3.1 dan COBIT 5 dimana penyusunan panduan tersebut dilakukan dalam tiga tahap yaitu Tahap pertama adalah penyusunan prosedur pengelolaan keamanan informasi untuk firewall configuration yang terdiri dari tahap analisis pemetaan proses, tahap penyusunan prosedur dan tahap penentuan peran dan deskripsi kerja. Tahap kedua adalah tahap verifikasi panduan yang dilakukan melalui pemberian kuesioner penilaian. Tahap ketiga adalah tahap perbaikan panduan.
5. Buku *Cisco PCI Solution for Retail 2.0 Design and Implementation Guide* yang disusun oleh Christian Janoff dan Bart McGlothin yang berisi *guide*/ petunjuk untuk implementasi jaringan komputer menggunakan perangkat Cisco untuk solusi berbagai bisnis retail 2.0 untuk perusahaan kecil hingga besar.

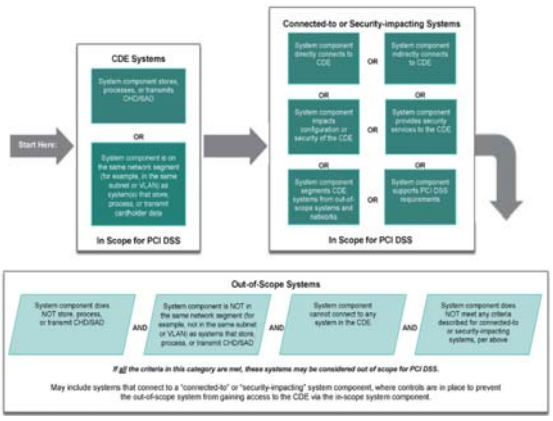
B. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini yaitu metode penelitian implementasi (*Implementation Research*) dengan sistem yang diimplementasi yaitu standar PCI DSS untuk menerapkan keamanan data. Ruang lingkup dari standar PCI DSS yaitu berlaku untuk semua komponen sistem yang disertakan atau terhubung ke lingkungan data pemegang kartu atau disebut dengan *Cardholder Data Environment* (CDE). Lingkungan data pemegang kartu (CDE) terdiri dari orang, proses, dan teknologi yang menyimpan, memproses, atau mengirimkan data pemegang kartu yang disebut sebagai *Cardholder Data* (CHD) atau juga termasuk data otentikasi yang bersifat sensitif yang disebut *Sensitive Authentication Data* (SAD).

Agar sesuai dengan framework standar PCI DSS penulis menggunakan tahapan proses sebagai berikut yaitu.

Assess

Mengidentifikasi semua lokasi data CHD/SAD, menginventarisasi asset TI dan proses bisnis untuk pemrosesan kartu pembayaran dan menganalisis kerentanan yang dapat mengekspos data pemegang kartu. Untuk mengidentifikasi berbagai perangkat yang termasuk dalam ruang lingkup standar digunakan diagram kategori scope pada gambar 3.



Gambar 3. Penentuan kategori dalam Ruang lingkup PCI DSS

Gambar 3 memperlihatkan bagaimana komponen sistem dapat dikategorikan menggunakan tiga pertanyaan dibawah ini :

1. Apakah terdapat data akun *Cardholder Data* (CHD) / *Sensitive Authentication Data* (SAD)) yang disimpan, diproses, atau dikirim pada komponen itu ?

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

2. Apakah terdapat konektivitas antara komponen tersebut dengan sistem dan *Cardholder Data Environment* (CDE) / SAD ?
3. Apakah komponen tersebut sistem dapat mempengaruhi keamanan pada *Cardholder Data Environment* (CDE) ?

Untuk identifikasi yang lebih lengkap dilakukan audit perangkat dengan menggunakan matriks tabel 2 dibawah ini.

Tabel 2. kategori pelingkupan PCI-DSS

Sistem Tipe	Deskripsi	Ruang Lingkup dan Penerapan
CDE Sistem	1. Komponen system menyimpan, memproses atau mengirimkan CHD/SAD. Atau 2. Komponen system berada di segmen jaringan yang sama, misalnya dalam satu subnet atau dalam satu VLAN yang sama dengan system yang menyimpan, memproses dan mengirim CHD / SAD.	Sistem ini ● Berada dalam ruang lingkup untuk PCI DSS ● Harus dievaluasi terhadap semua persyaratan PCI DSS untuk menentukan penerapan setiap persyaratan.
Terhubung kepada dan/atau berdampak pada sistem keamanan	1. Komponen system yang berada pada jaringan yang berbeda (atau subnet atau VLAN), tetapi dapat terhubung ke atau mengakses CDE (misal melalui konektivitas jaringan internal) Atau 2. Komponen system yang dapat terhubung ke atau mengakses CDE melalui system lain – misalnya, melalui server lompat yang menyediakan akses ke CDE. Atau 3. Komponen sistem dapat mempengaruhi konfigurasi atau keamanan CDE, atau cara penanganan CHD / SAD -- misalnya, server pengalihan web atau server resolusi nama. Atau 4. Komponen sistem menyediakan layanan keamanan untuk CDE -- misalnya, pemfilteran lalu lintas jaringan, distribusi patch, atau manajemen otentikasi. Atau 5. Komponen system mendukung persyaratan PCI DSS seperti server waktu dan server penyimpanan log audit. Atau 6. Komponen sistem menyediakan segmentasi CDE dari sistem dan jaringan di luar cakupan -- misalnya, firewall yang dikonfigurasi untuk memblokir lalu lintas dari jaringan yang tidak terpercaya.	Sistem ini: ● Berada dalam ruang lingkup untuk PCI DSS. Meskipun koneksi terbatas pada port atau layanan tertentu pada sistem tertentu, sistem tersebut termasuk dalam cakupan untuk memverifikasi bahwa kontrol keamanan yang berlaku sudah diterapkan. ● Harus dievaluasi terhadap sebuah persyaratan PCI DSS untuk menentukan penerapan setiap persyaratan. ● Tidak boleh menyediakan jalur akses terhadap sistem CDE dan sistem di luar cakupan.
Diluar lingkup/*Out of Scope*	Komponen system yang tidak termasuk kategori A dan B	Sistem ini harus dipisahkan dari system CDE dan tidak boleh ada komunikasi dari dan ke CDE.

Repair

Memperbaiki kerentanan yang teridentifikasi, menghapus CHD/SAD yang

tidak perlu dengan aman, dan menerapkan proses bisnis yang aman. Jika salah satu atau lebih pernyataan pada tabel 1 diatas benar maka perangkat tersebut termasuk dalam ruang lingkup standar PCI DSS, dan wajib diterapkan sesuai dengan rekomendasi yang ada pada table 1 kolom ruang lingkup dan penerapan. Berdasarkan table 1, kategori perlingkupan PCI-DSS mencakup sistem yang terhubung ke dan yang berdampak pada keamanan. Kategori ini mengambil prioritas dan dievaluasi sebelum kategori sistem di luar cakupan dipertimbangkan. Untuk dipertimbangkan di luar ruang lingkup, sistem harus memenuhi semua kriteria kategori di luar cakupan dan tidak ada kriteria kategori yang lebih tinggi.

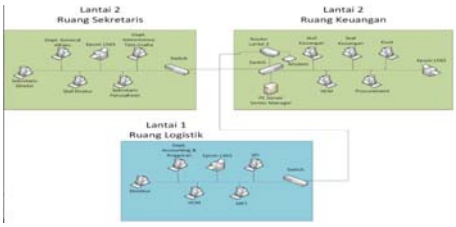
Report

Mendokumentasikan penilaian dan rincian perbaikan, dan mengirimkan laporan kepatuhan ke bank yang mengakuisisi dan merek kartu yang berbisnis dengan perusahaan. Pada tahap ini hanya dilakukan sampai mendokumentasikan penilaian, rincian perbaikan dan melakukan pengetesan konfigurasi jaringan, namun tidak mengirimkan laporan kepatuhan untuk sertifikasi PCI DSS.

C. HASIL DAN PEMBAHASAN

Kondisi Jaringan yang Ada (Existing Network)

Skema jaringan yang diperlihatkan pada gambar 4 merupakan skema jaringan yang disederhanakan dan alamat IP dari setiap perangkat juga tidak penulis perlihatkan untuk menjaga kerahasiaan perusahaan. Penggunaan alamat IP dalam penelitian ini tidak menggunakan alamat IP yang sebenarnya akan diimplementasikan karena bersifat rahasia dan untuk menjaga keamanan informasi perusahaan.



Gambar 4. Skema Jaringan Awal

Berdasarkan wawancara dari bagian departemen Teknologi Informasi dan pengamatan dari skema jaringan pada object penelitian, penggunaan alamat IP pada setiap perangkat masih menggunakan satu jaringan atau satu subnet saja, tidak ada pembatasan antara departemen atau antar lantai sehingga perlu perbaikan dari sisi disegmentasi jaringan dengan menerapkan virtual local area network (VLAN).

Berdasarkan wawancara dan dokumen prosedur perusahaan didapatkan proses bisnis yang berhubungan dengan Cardholder Data secara langsung yang ada di perusahaan terdapat pada bagian kasir, komputer kasir yang berada di lantai II ruang keuangan berfungsi sebagai tempat pembayaran para pelanggan dan pegawai. Alat pembayaran yang digunakan merupakan mesin *Electronic Data Capture* (EDC) yang berfungsi untuk pembayaran transaksi non tunai, baik dengan kartu kredit maupun kartu debit. Komputer kasir juga terhubung dengan server yang menyediakan sistem *Point of Sales* (POS) yang bertujuan untuk meningkatkan keamanan data sekaligus mengurangi risiko kehilangan data pada kasir walaupun hanya merecord data nama pelanggan dan transaksi yang dilakukan. Berdasarkan hal tersebut dapat disimpulkan mesin EDC yang ada di kasir termasuk dalam lingkup *Cardholder Data Environment* (CDE) karena terdapat kegiatan memproses dan mengirimkan Cardholder data (CHD) yang dapat memproses, memyimpan, dan mengirimkan data pemegang kartu atau data otentikasi pembayaran yang sensitif.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Secara fungsi proses bisnis dan keterlibatan setiap perangkat dengan CHD dan SAD diperlihatkan pada table 3 berikut.

Tabel 3 Tabel Kategori Perangkat Existing

No	Nama Komputer	Keterlibatan dengan CHD	Keterangan berdasar Tabel 1
1	Departement accounting dan anggaran	Tidak ada	Kategori C
2	Direktur	Tidak ada	Kategori C
3	Human Capital Management (HCM)	Tidak ada	Kategori C
4	MKT	Tidak ada	Kategori C
5	SPI	Tidak ada	Kategori C
6	Sekretaris Direksi	Tidak ada	Kategori C
7	Departemen General Affairs	Tidak ada	Kategori C
8	Staff Direksi	Tidak ada	Kategori C
9	Sekretaris Perusahaan	Tidak ada	Kategori C
10	Departemen Administrasi Tata Usaha	Tidak ada	Kategori C
11	Staff Keuangan 1	Ada	kategori A2
12	Staff Keuangan 2	Ada	kategori A2
13	Kasir	Ada	kategori A1
14	PC Server Senior Manager	Ada	kategori A2
15	HCM	Tidak ada	Kategori C
16	Procurement	Tidak ada	Kategori C
17	Router	Ada	kategori A1
18	Modem	Ada	kategori A1
19	Switch Lantai 1	Tidak ada	Kategori C
20	Switch Lantai 2	Ada	ketegori A1
21	Komputer Tim IT	Ada	kategori B

Berdasarkan wawancara dari tim IT didapatkan kesesuaian sistem jaringan komputer saat ini dengan 12 *requirement* yaitu:

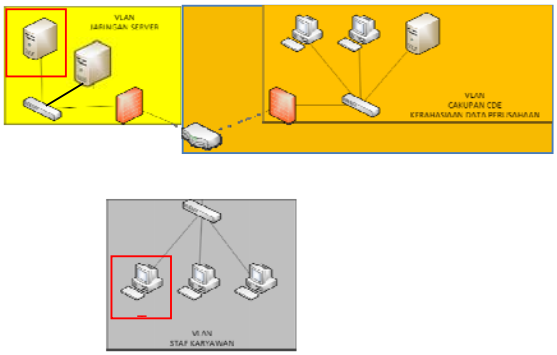
1. Telah terdapat sistem *firewall* pada setiap diperangkat komputer dan router, sehingga hanya karyawan yang diberi izin yang dapat mengakses setiap komputer masing-masing. Hal ini sesuai dengan *requirement* 1 dan 8 PCI DSS.
2. Setiap perangkat yang ada telah diterapkan password yang harus dirubah secara berkala. Hal ini sesuai dengan *requirement* ke 2, 6 dan 12 PCI DSS.
3. Transaksi yang langsung menggunakan kartu hanya dilakukan pada mesin EDC tang telah memiliki fasiltas *Point to Point Encryption*. Hal ini sesuai dengan *requirement* PCI DSS nomer 3 dan 4.
4. Telah terdapat *software antivirus* pada setiap komputer dan diupdate secara berkala. Hal ini sesuai dengan *requirement* PCI DSS nomer 5
5. *Swipe* kartu pembayaran hanya dilakukan 1 kali yaitu pada mesin EDC. Hal ini sesuai dengan *requirement* PCI DSS nomer 7
6. Pada object penelitian telah terdapat pembatasan secara fisik ke perangkat jaringan. Hal ini sesuai dengan *requirement* PCI DSS nomer 9
7. Pada aplikasi perusahaan yang menghubungkan komputer yang terindikasi sebagai CDE dengan server yang tidak terindikasi sebagai CDE telah menerapkan komunikasi yang terenkripsi. Hal ini sesuai dengan *requirement* PCI DSS nomer 4

Berdasarkan infrastruktur yang ada dan proses bisnis perusahaan yang berhubungan dengan CHD/SAD dan sepatuhan terhadap standar PCI DSS didapatkan prioritas gap sebagai berikut.

1. Tidak adanya pemisahan atau segmentasi jaringan terhadap perangkat yang termasuk dalam CDE firewall hanya menahan kemungkinan serangan dari luar perusahaan. Hal ini belum sesuai dengan requirement PCI DSS nomer 1 dan 3,
2. Tidak adanya pembatasan akses komunikasi antar perangkat terutama akses dari dan ke perangkat CDE. Hal ini belum sesuai dengan requirement PCI DSS nomer 1 dan 3,
3. Tidak adanya sistem pencatatan akses/log yang dibuat dari perangkat komputer tim IT ke system CDE. Hal ini

belum sesuai dengan requirement PCI DSS nomer 1 dan 3,

Untuk memperkecil ruang lingkup keamanan data CHD/SAD sekaligus memperkecil area CDE maka diterapkan segmentasi jaringan dengan membagi jaringan menjadi tiga segmen dengan sistem *subnetting* jaringan.



Gambar 5. Skema Jaringan Usulan

Dalam skema jaringan usulan selain membagi jaringan menjadi 3 kelompok subnet yaitu

1. Area CDE
   Area ini terdiri atas perangkat komputer dan jaringan yang terindikasi berhubungan dengan CHD dan SDA yang tidak dapat dilakukan eliminasi karena kebutuhan pada proses bisnis perusahaan. Setiap komputer pada area ini memiliki sistem autentikasi yang ketat, penggunaannya hanya berhubungan dengan *Point of Sales* dan diaudit secara berkala.
2. Area jaringan Server (*Shared*)
   Area ini terdiri atas komputer server-server perusahaan yang salah satunya terkoneksi dengan server PoS yang berada di Area CDE. Area ini juga dikenal sebagai area *De Military Zone* (DMZ) karena diakses juga oleh Area Staff Karyawan yang merupakan diluar Scope PCI DSS.
3. Area Staff Karyawan (Corporate LAN)
   Pada Area ini berisi berbagai perangkat yang telah terindikasi tidak berhubungan dengan system CDE kecuali komputer khusus untuk keperluan *remote maintenance* ke dalam sistem CDE via server *Authentication, Authorization, Accounting* (AAA) yang disediakan untuk tim IT.

Konfigurasi pada Switch

Pada switch diterapkan 3 VLAN yang akan diisi dengan ketiga jaringan subnet pada penjelasan sebelumnya. Pada switch juga menerapkan port security dengan mengidentifikasi setiap MAC address yang terhubung terutama pada port VLAN terutama untuk jaringan CDE dan jaringan server(Shared).

```
Switch CDE
Switch>en
Switch#
Switch(vlan)#vlan 10 name CDE
VLAN 10 added:
Name: CDE
Switch(vlan)#vlan 20 name Shared
VLAN 20 added:
Name: Shared
Switch(vlan)#vlan 30 name corp
VLAN 30 added:
Name: corp
Switch(vlan)#ex
Switch#conf t
Switch(config)#int range fa0/1-3
Switch(config-if-range)#switchport mode
access
Switch(config-if-range)#switchport access
vlan 10
Switch(config-if-range)#int range fa0/4-22
Switch(config-if-range)#switchport mode
access
Switch(config-if-range)#switchport access
vlan 30
Switch(config-if-range)#int range fa0/23-24
Switch(config-if-range)#switchport mode
access
Switch(config-if-range)#switchport access
vlan 20
Switch(config-if-range)#int range gig0/0-1
```

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

```
interface range not validated - command
rejected
Switch(config)#int gig0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 0060.3E81.EAC7
Found duplicate mac-address
0060.3e81.eac7.
Switch(config-if)#switch port-security
violation protect
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 0090.2BAD.39A8
Switch(config-if)#switch port-security
violation protect
Switch(config-if)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 00D0.D344.8D67
Switch(config-if)#switch port-security
violation protect
Switch(config-if)#

Switch(config)#int fa0/23
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 0005.5E4D.1E3A
Switch(config-if)#switch port-security
violation protect
Switch(config-if)#int fa0/24
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 0001.9739.0209
Switch(config-if)#switch port-security
violation protect
```

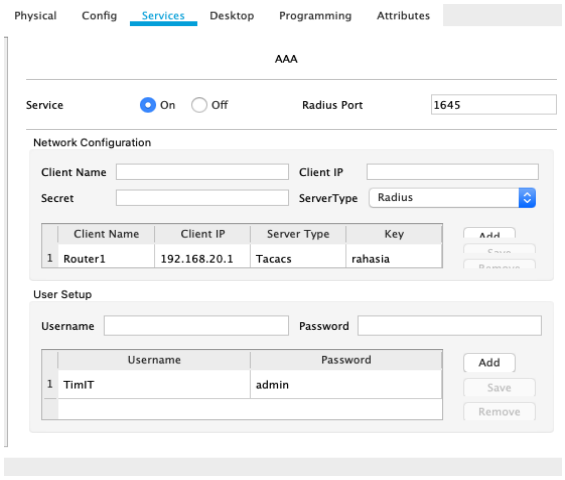
Konfigurasi Router

```
Router#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)#int gig0/0
Router(config-if)#no sh
Router(config-if)#ip add 192.168.10.1
255.255.255.0
Router(config-if)#int gig0/1
Router(config-if)#no sh
Router(config-if)#ip add 192.168.20.1
255.255.255.0
Router(config-if)#int gig0/2
Router(config-if)#no sh
Router(config-if)#ip add 192.168.30.1
255.255.255.0
Router(config-if)#exit
```

Konfigurasi ACL's

```
Router(config)#access-list 1 deny
192.168.30.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#int gig0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#ex
Router(config)#access-list 2 deny
192.168.10.0 0.0.0.255
Router(config)#access-list 2 permit any
Router(config)#int gig0/2
Router(config-if)#ip access-group 2 out
Router(config-if)#ex
```

Konfigurasi server AAA dengan TACACS+



Gambar 6. Konfigurasi TACACS+ di Server AAA

Konfigurasi pada Router

```
Router1#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Router1(config)#aaa new-model
Router1(config)#aaa authentication login
default local
Router1(config)#username admin password
admin
Router1(config)#username timIT password
admin
Router1(config)#aaa authentication login
AAA-SERVER group tacacs+ local
Router1(config)#line console 0
Router1(config-line)#login authentication
AAA-SERVER
Router1(config-line)#exit
Router1(config)#tacacs-server host
192.168.20.2
Router1(config)#tacacs key rahasia
Router1(config)#ex
Router1#
%SYS-5-CONFIG_I: Configured from
console by console
Router1#debug aaa authentication
AAA Authentication debugging is on
Router1#exit
```

Pengujian Jaringan

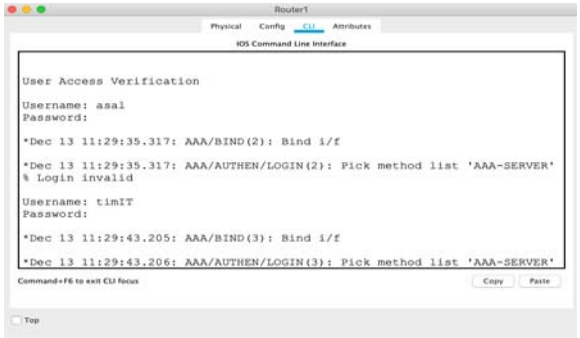
Pengujian jaringan dilakukan dengan menggunakan simulasi packet tracer yang mempresentasikan lingkungan jaringan yang telah diusulkan.

1. Pengujian port security
   Pada pengujian ini dilakukan penggantian port yang terhubung dengan komputer CDE dengan komputer yang mac addressnya tidak terdaftar di switch di jaringan CDE. hasilnya komputer yang mac addressnya tidak terdaftar tersebut tidak dapat ping ke jaringan walaupun ip addressnya disamakan dengan Ip address di network CDE.
2. Pengujian ACLS
   Pengujian dilakukan dengan test ping dari komputer yang terhubung ke corporate LAN ke jaringan CDE dan sebaliknya. Hasil pengujian didapatkan tidak ada paket ping yang Kembali atau request timed out. dan dicek ke router dengan perintah show access-list

```
Router1#show access-list
Standard IP access list 1
10 deny 192.168.30.0 0.0.0.255 (5
match(es))
20 permit any (2 match(es))
Standard IP access list 2
10 deny 192.168.10.0 0.0.0.255 (2
match(es))
20 permit any (1 match(es))
```

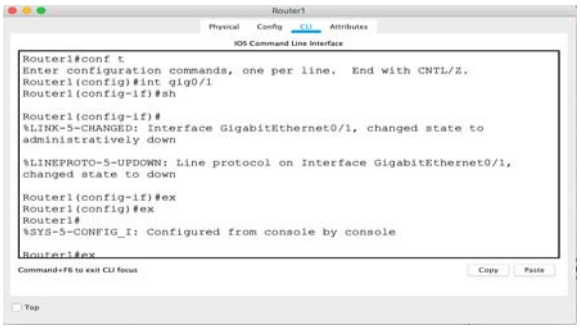
   Artinya router berhasil menahan koneksi dari CDE ke corporate LAN dan sebaliknya. Sedangkan koneksi ke jaringan server/ shared network bisa dilakukan.
3. Pengujian TACACS+
   Pengujian akses ke router dengan konfigurasi TACACS+ seperti lampiran gambar di bawah ini

Gambar 7. Login Router dengan otentikasi yang benar

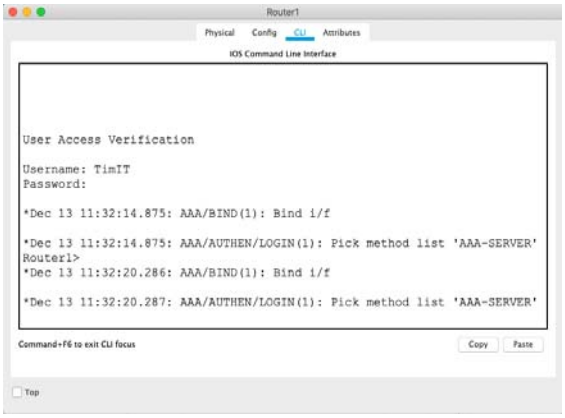


JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Gambar 8 Login Router dengan otentikasi yang salah

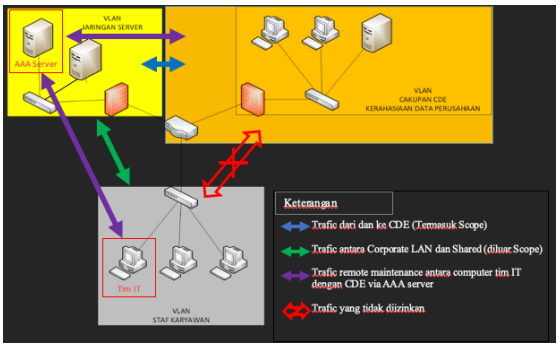


Gambar 9 mematikan koneksi ke AAA server



Gambar 10 login router ketika koneksi ke AAA server terputus

Dengan begitu untuk konfigurasi router, Tim IT wajib terverifikasi melalui AAA server. Gambar 11 berikut merupakan skematik diagram komunikasi hasil tes konfigurasi dan telah sesuai dengan dokumen PCI DSS *Scouping* and *Network Segmentation*.



Gambar 11. Skema hasil tes komunikasi antar jaringan

D. PENUTUP

Berdasarkan hasil penelitian dan pengujian Implementasi Keamanan Jaringan Berdasarkan Standar PCI-DSS yang telah dilakukan, maka dapat diambil kesimpulan yaitu :

1. Menerapkan Access Control List (ACL) untuk mengontrol setiap client yang ingin berinteraksi dengan client lain yang sangat dijaga kerahasiaan datanya.
2. Menerapkan segmentasi jaringan VLAN dan port security untuk memperkecil cakupan jaringan.
3. Menerapkan TACACS+ dapat digunakan untuk menyediakan remote maintenance yang terauthentikasi dan aman.
4. Dengan menerapkan keamanan jaringan berstandar PCI-DSS dapat mengurangi risiko pelanggaran keamanan data dalam bertransaksi menggunakan kartu pembayaran.

Saran untuk penelitian lanjut yaitu perlu diadakan penelitian untuk penetration testing berdasarkan standar PCI-DSS untuk lebih mengetahui tingkat keamanan jaringannya. Pada penelitian ini juga belum sampai pada tingkat pelaporan/ report untuk mendapatkan pengakuan dan sertifikat dari PCI SSC bahwa perusahaan telah menerapkan standar kepatuhan PCI DSS.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada PT Dharma Lautan Nusantara yang telah memberi kesempatan untuk melakukan penelitian.

E. DAFTAR PUSTAKA

Checklists, I. T. (2019). *PCI DSS COMPLIANCE REQUIREMENT 01*.

Dihni, vika A. (2021). Nilai Transaksi Kartu Kredit Naik 13,07% pada Agustus 2021.

Databoks.Katadata.Co.Id, *September*, 2021.

Janoff, C., Architect, V. S., Ise, C. M. O., & Systems, C. (2011). *Cisco PCI Solution for Retail 2 . 0 Design and Implementation Guide*.

Panjaitan, L. T. (2017). Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang- Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008. *Jurnal Telekomunikasi Dan Komputer*, *3*(1), 1. https://doi.org/10.22441/incomtech.v3i1.1111

PCI Security Standards Council. (2017). *Information Supplement : Guidance for PCI DSS Scoping and Network Segmentation*. *December*, 26.

PCI SSC. (2018). PCI DSS Quick Reference Guide 3.2.1. *PCI Security Standard Documents*, 1–40. *https://www.pcisecuritystandards.org/security_standards/documents.php*

Santoso, B. P., Hariyanti, E., & Wuryanto, E. (2016). Penyusunan Panduan Pengelolaan Keamanan Informasi Untuk Firewall Configuration Berdasarkan Kerangka Kerja PCI DSS v.3.1 dan COBIT 5. *Journal of Information Systems Engineering and Business Intelligence*, *2*(2), 67. Available at: *https://doi.org/10.20473/jisebi.2.2.67-73*