Analisis Keamanan Informasi Aplikasi HRIS Dengan Metode SQUARE Pada PT. XYZ

Information Security Analysis of HRIS Application With SQUARE Method at PT. XYZ

Yudhi Arta*[1], Muhammad Ilhan[2], Anggi Hanafiah[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau, Riau
e-mail: ***[1]yudhiarta@eng.uir.ac.id**, [2]m.ilhan@students.uir.ac.id, [3]anggihanafiah@eng.uir.ac.id

Abstrak

Keamanan dalam suatu sistem tentunya sangat dibutuhkan untuk menjaga integritas data penting yang tersimpan dalam sistem tersebut. Oleh sebab itu untuk menjaga integritas data ini bermula setelah sistem tersebut terkoneksi dengan jaringan internet. Integritas data tersebut digunakan oleh dua perspektif yaitu penyelenggara dan pengguna. Salah satu sistem yang digunakan oleh perspektif tersebut yaitu Human Resources Information System (HRIS) atau sistem penginputan data karyawan pada perusahaan PT. XYZ . Dalam penelitian ini menggunakan metode SQUARE untuk mencari celah keamanan system atau kelemahan dari system HRIS. Adanya masalah tersebut, dengan menggunakan metode SQUARE dapat mengetahui celah keamanan sistem dan melihat seberapa aman sistem terhadap serangan yang kemungkinan terjadi dan memberikan rekomendasi yang dapat mengatasi kelemahan sistem dengan melakukan pengujian dan melakukan beberapa observasi terhadap sistem. Hasil analisis yang telah di lakukan dengan menggunakan metode SQUARE, dapat memberikan rekomendasi terhadap kebutuhan keamanan sistem yang bertujuan untuk menjaga availibilitas dan kerahasiaan serta integritas sistem.

Kata kunci — Keamanan, SQUARE, HRIS

Abstract

Security in a system is certainly needed to maintain the integrity of important data stored in the system. Therefore, to maintain the integrity of this data begins after the system is connected to the internet network. The data integrity is used by two perspectives, namely the organizer and the user. One of the systems used by this perspective is the Human Resources Information System (HRIS) or employee data input system at the company PT. XYZ . In this study using the SQUARE method to find system security gaps or weaknesses in the HRIS system. The existence of these problems, using the SQUARE method can find system security gaps and see how safe the system is against attacks that may occur and provide recommendations that can overcome system weaknesses by testing and making some observations on the system. The results of the analysis that has been carried out using the SQUARE method, can provide recommendations for system security needs that aim to maintain availability and confidentiality as well as system integrity.

Keywords— Security, SQUARE, HRIS

1. PENDAHULUAN

Keamanan sebuah sistem tentunya sangat diperlukan untuk menjaga integritas data yang tersimpan dalam sebuah sistem maupun aplikasi. Tantangan untuk menjaga integritas data ini bermula setelah sistem terkoneksi dengan jaringan komputer yang terhubung ke internet ataupun *cloud computing* yang ada. Integritas data ini digunakan oleh dua perspektif yaitu penyelenggara dan pengguna. Salah satu sistem yang digunakan yaitu sistem *Human Resources Information System* (HRIS) atau sistem data karyawan pada perusahaan PT. XYZ.

Keamanan dalam sistem *Human Resources Information System* (HRIS) tentunya bersesuaian dengan informasi dasar yang harus dipenuhi suatu sistem keamanan dalam web *application*. Semisal pemalsuan data atau pencurian data yang dilakukan oleh orang luar ataupun karyawan untuk memasuki sistem yang ada. Hal ini bersesuaian dengan informasi keamanan CIA (*Confidentiality, Integrity and Availability*) dan authentification [1]–[6]. CIA (*Confidentiality, Integrity and Availability*) merupakan prinsip dasar keamanan informasi, Ketika ingin membangun sebuah sistem yang aman, maka CIA yang dijadikan sebagai acuan yang harus di capai dan di lindungi, misalnya akses bagi pengguna yang berperan sebagai admin harus berbeda dengan seorang user, oleh karena itu harus ada langkah pengamanan untuk hal tersebut, sehingga tidak ada pengguna yang dapat memalsukan informasi yang tersimpan pada sistem [6]–[8]. sedangkan *Authentication* merupakan tindakan mengkonfirmasi kebenaran suatu bagian dari sebuah data user yang telah tersimpan dan sistem yang terhubung ke jaringan internet, kemungkinan pencurian atau perusakan data akan semakin besar, karena pengguna yang berpotensi berbahaya akan dengan mudah memasuki sistem melalui jaringan internet [9]–[11].

Penelitian ini bertujuan unntuk mengetahui celah ancaman dan menganalisa kebutuhan keamanan serta rekomendasi yang tepat demi menerapkan analisis keamanan pada aplikasi HRIS. Sebagai contoh pada tahun 2018 hingga 2019 sudah hampir 250 serangan yang dilakukan sehingga kinerja system terganggu. Pencegahan sudah dilakuakan dengan menandai IP dari mana saja dan dilakukan pengeblokan IP. Oleh karena itu diperlukan keamanan informasi yang tepat untuk memastikan keamanan sistem HRIS agar identifikasi keamanan dapat dilakukan. Salah satu langkah metode square yaitu *Identify Security Goals* yang melakuakan analisis tujuan dan persyaratan kemanan sebuah sistem. Analisis kebutuhan keamanan sistem dalam pengembangan sistem informasi berbasis open source dapat dilakaukan oleh metode SQUARE karena analisa kebutuhannya sangat detail sehingga rekomendasi bisa diberikan sejak tahap awal pengembangan sistem agar dapat dihasilkan sebuah sistem informasi yang aman.

2. METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah metodologi SQUARE yang terdiri dari sembilan langkah proses yang dikembangkan untuk membantu menganalisis kebutuhan keamanan sistem sebagai berikut [12], [13]:

Langkah 1. *Agree on Definitions* (Mendefinisikan kebutuhan Sistem)
Pada tahap ini melakukan pendeskripsian aplikasi HRIS yang akan di analisa dan mendefinisikan istilah keamanan informasi untuk aplikasi HRIS tersebut.

Langkah 2. *Identify Security Goals* (Mengidentifikasi tujuan keamanan)

Pada tahap kedua ini melakukan analisis tujuan dan persyaratan keamanan sistem yang di perlukan oleh perusahan PT. XYZ untuk menjaga keamanan secara menyeluruh terhadap ketersediaan (*availability*).

Langkah 3. *Develop Artifact* (Pengembangan Artefak)

Pada tahap ini akan menjelaskan arsitektur sistem HRIS yang sedang berjalan atau pun yang sedang di bangun yang berupa diagram arsitektur jaringan, diagram *usecase*, diagram *misusecase* dan pohon serangan.

Langkah 4. *Perform Risk Assesment* (Penilaian Risiko)
Pada tahap ini melakukan analisa penilaian risiko untuk mengidentifikasi ancaman terhadap sistem yang kemungkinan terjadi

Langkah 5. *Select Elicitation Technique* (Memilih Teknik Elisitasi)
Pada tahap kelima ini Memilih teknik elisitasi yang cocok untuk melakukan penanganan terhadap pekerjaan yang dilakukan dengan Pengumpulan data terkait kondisi sistem secara menyeluruh antara melalui metode observasi, *interiew*, atau analisa *use case*

Langkah 6. *Elicit Security Requirements* (Permintaaan persyaratan keamanan)
Pada tahap enam melakukan Elisitasi persyaratan keamanan untuk menyediakan solusi bagaimana melakukan elisitasi keamanan yang baik dan dari hasil observasi, analisa *use case* dan studi pustaka kemudian dibuat kedalam bentuk daftar kebutuhannya

Langkah 7. *Categorize Requirement* (Kategori Persyaratan)
Setelah persyaratan yang dihasilkan maka selanjutnya yaitu mengelompokan persyaratan keamanan yang dipilih, dalam hal ini menggabungkan langkah-langkah pengelompokan, penamaan, dan kategorisasi bersama-sama

Langkah 8. *Prioritize Requirements* (Prioritas Persyaratan)
Pada proses ini akan dilakukan persyaratan prioritas mengenai sistem keamanan di jaringan nirkabel dan LAN di jaringan sebuah instansi atau perusahaan berdasarkan kasus *Misusecases.* yang dibuat sebelumnya. Untuk memprioritaskan serangan yang membuat ancaman lebih berbahaya, maka ancaman ini akan dimasukan ke dalam sebuah tabel agar mudah dalam memproses dan menganalisanya kembali.

Langkah 9. *Requirement Inspection* (Penilaian Kebutuhan)
Membuat table penilaian dan pada metode ini bertanggung jawab kepada anggota tim inspeksi dan pengembangan log dengan arsitektur terperinci dan rekomendasi kebijakan untuk persyaratan penyebaran keamanan sistem berdasarkan tingkat prioritas *misuse case*

2.1. Pengumpulan Data

Dalam melakukan analisis keamanan Sistem menggunakan metodologi SQUARE maka harus menggunakan Sembilan Langkah untuk membantu proses menganalisis kebutuhan keamanan sistem. Pada hasil Penelitian ini, peneliti menggunakan 3 metode teknik pengumpulan data yang digunakan dalam penelitian sebagai berikut :

1. Melakukan pengambilan data dengan mencari berbagai sumber tertulis, baik berupa buku-buku, arsip, artikel, dan jurnal, atau dokumen-dokumen yang relevan.
2. Melakukan metode Observasi pengamatan langsung pada proses penggunaan aplikasi HRIS di PT. XYZ.
3. Melakukan metode wawancara untuk mendapatkan informasi dengan cara bertanya langsung kepada pemangku instansi yaitu karyawan di perusahan atau institusi sehingga data yang diperoleh bersifat objektif dan data dapat dipertanggung jawabkan

2.2. Konsep Teori

Security Quality Requirements Engineering (SQUARE) adalah merupakan sebuah model yang dikembangkan untuk memprediksi proses persyaratan. SQUARE merupakan langkah untuk mengkategorikan persyaratan keamanan yang utamakan pada sarana dan infrastruktur teknologi

informasi, banyak metode yang dapat dijelaskan dengan menggunakan metode SQUARE yaitu kaitannya dengan kasus penyalahgunaan dalam system [8].

ISO 27001 adalah standar manajemen keamanan informasi yang digunakan oleh bisnis dan organisasi untuk menjaga keamanan informasi di seluruh dunia, ISO 27001 juga didefinisikan sebagai sistem manajemen keamanan informasi (ISMS), yang memberikan gambaran tentang apa yang perlu dilakukan lembaga untuk menilai, mengimplementasikan, dan memelihara keamanan informasi. ISO 27001 berfokus pada pengurangan risiko informasi yang penting bagi organisasi[14].

Human Resources Information System (HRIS) Adalah sistem untuk mengelola kegiatan personel menggunakan sistem yang dinetralisir. Ini termasuk data gaji, pembayaran, biodata karyawan, proses rekrutmen, kehadiran dan cuti, dan tinjauan kinerja karyawan[15][16].

3. HASIL DAN PEMBAHASAN

Hasil 1. *Agree on Definitions* (Mendefinisikan kebutuhan Sistem)

Ada beberapa ancaman keamanan dalam sistem HRIS, hal ini disebabkan oleh kerentanan yang dapat diperkenalkan oleh peretas untuk memalsukan data sehingga peretas dapat mengutak atik keamanan sistem HRIS. Dengan demikian, perlu analisis kebutuhan sistem keamanan yang dapat menjaga integritas sistem HRIS. Menentukan kondisi keamanan yang akan disepakati. Kondisi keamanannya adalah sebagai berikut: :

Beberapa definisi serangan pada sistem :

Tabel 1 Definisi serangan sistem

No.	Keterangan Definisi
1.	Serangan Injeksi SQL ini objek yang diserang berupa halaman web yang menggunakan *Structured Query Language* (SQL) untuk melakukan *query* dan memalsukan database
2.	Serangan Data *Sniffing*, pada serangan ini melakukan *sniffing* terhadap data yang ada dalam jaringan
3.	Serangan *Spoofing,* Penyerang ini untuk mendapatkan informasi yang disediakan atau mengambil *mac address*
4.	*Password Attack*, serangan untuk crack sebuah *password*
5.	*Denial of Service* (DoS), jenis serangan dengan cara menghabiskan sumber *(resource*) yang dimiliki oleh komputer tersebut sehingga komputer tersebut tidak dapat menjalankan fungsinya dengan benar
6.	Sistem HRIS tidak di lengkapi dengan keamanan yang berupa *Secure Socket Layer* (SSL). Tujuan utama pemasangan SSL adalah sebagai pengaman pertukaran data yang terjadi melalui jaringan internet. Sistem HRIS tidak di lengkapi dengan pengaman SSL dan dapat di buktikan pada gambar berikut

Gambar 1 URL Tanpa SSL

Pada gambar 1, dapat kita lihat pada portal system dari PT. XYZ tidak memiliki keamanan SSL ditandai dengan URL terdapat simbol gembok yang di silang merah yang artinya sertifikat SSL tidak Valid dan pada URL tidak terdapat HTTPS karena website yang memiliki sertifikat SSL.

Hasil 2. *Identify Security Goals* (Mengidentifikasi tujuan keamanan)

Hasil pada tahap kedua ini melakukan Analisis tujuan dan persyaratan keamanan sistem dengan menggunakan cara *interiew* yang di perlukan oleh perusahan PT. XYZ untuk memastikan keamanan secara menyeluruh terhadap ketersediaan (*availability*)

Tabel 2 Tujuan bisnis (*Business Goals*)

No.	Keterangan
1	Sistem HRIS di bangun untuk keperluan proses penyimpanan data karyawan dan identitas perusahaan
2	Sistem HRIS dapat melayani karyawan untuk melakukan penginputan data baru dan data pensiun serta informasi terkait masa jabatan
3	Sistem HRIS dapat menjaga privasi *user*. Dalam hal ini karyawan di awasi oleh admin sebagai pengelola sistem HRIS

Tabel 3 Tujuan keamanan (*Security Goals*)

Goals		Tujuan Keamanan
G-01	Kerahasiaan (*Confidentiality*)	Data admin, data pengguna, dan informasi pengguna harus dirahasiakan dari akses pengguna ilegal. Untuk mencegah pengguna ilegal mengetahui data autentikasi pengguna
G-02	Integritas Data (*Data Integrity*)	Data admin, data pengguna, dan informasi pengguna harus tetap otentik. Pengguna yang ingin terhubung dapat mengikuti semua prosedur di atas
G-03	Ketersediaan (*Availabilty*)	Semua data dan informasi harus tersedia dalam sistem, terutama jika data diperlukan dan akan digunakan oleh pengguna
G-04	Kontrol Akses (*Access Control*)	1. Hanya admin yang berwenang yang dapat melakukan penginputan data pada system 2. Adanya kontrol akses terhadap pengguna dan komponen sistem

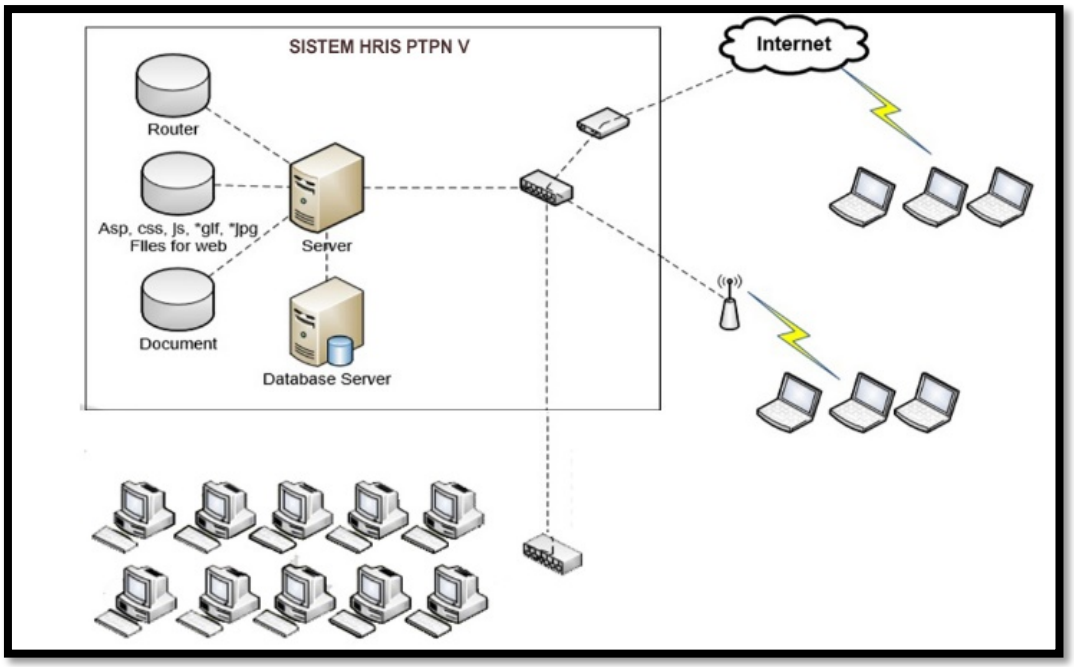
G-05	Penggunaan (*Aplication*)	1. Keamanan harus terkelola secara terstruktur dan terencana agar tidak menghambat proses bisnis 2. Menghindari resiko dari aktifitas yang merugikan sistem

Hasil 3. *Develop Artifact* (Pengembangan Artefak)

Pada tahap ini akan Menjelaskan secara detail arsitektur sistem HRIS yang sedang berjalan berupa :

a. Diagram Arsitektur

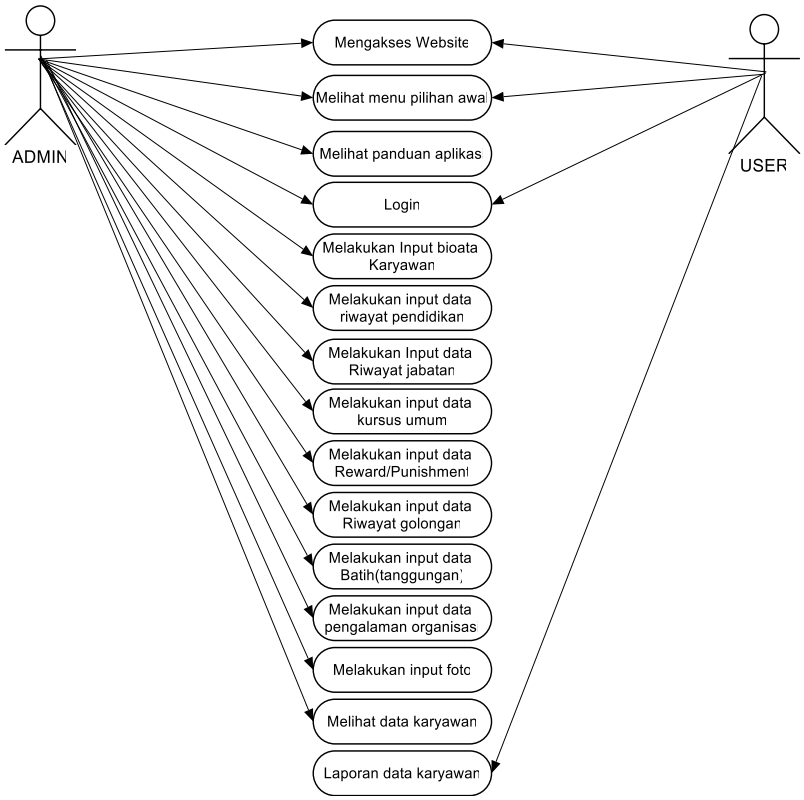
Pada perencanaan artefak ini berisi gambaran arsitektur sistem jaringan dan deskripsi kinerja sistem.



Gambar 2 Arsitektur HRIS

b. Diagram *Use Case*

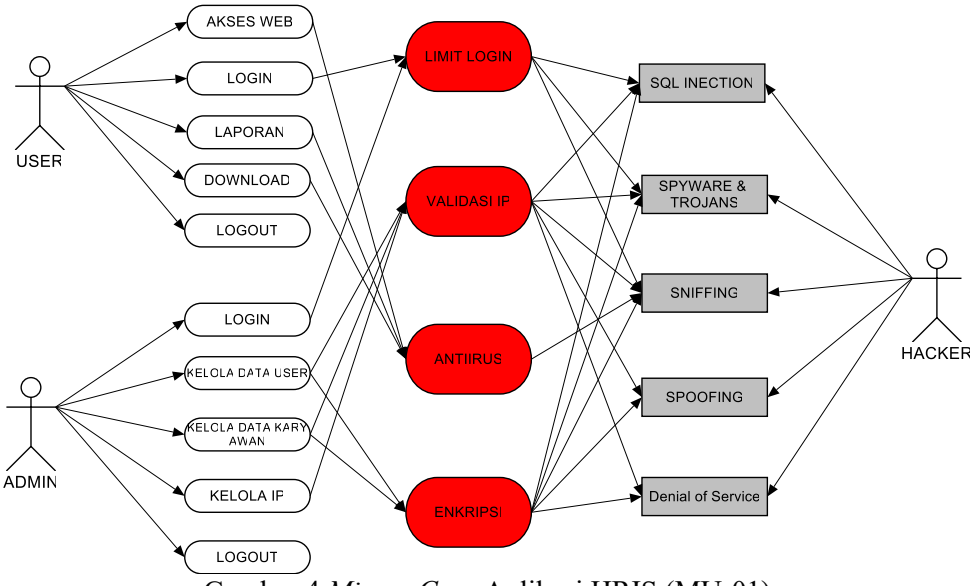
Use case merupakan skenario artefak untuk menanggapi tindakan yang terjadi dalam proses bisnis, menyediakan konteks bagi operasi, pemangku kepentingan, dan tim teknik untuk memahami interaksi komponen system. Tahapan dalam use case ini merupakan langkah – langkah yang dihadapi oleh setiap karyawan dalam mengakses system HRIS tersebut. Untuk session yang dilakukan oleh admin melingkupi keseluruhan dari kinerja sistem.



Gambar 3 *Use Case* Diagram Aplikasi HRIS

c. Diagram *Misuse Case*

Misuse cases merupakan Insiden penyalahgunaan termasuk serangkaian serangan yang terjadi pada sistem, sehingga pengguna ilegal mencoba masuk ke sistem menggunakan langkah atau metode illegal.

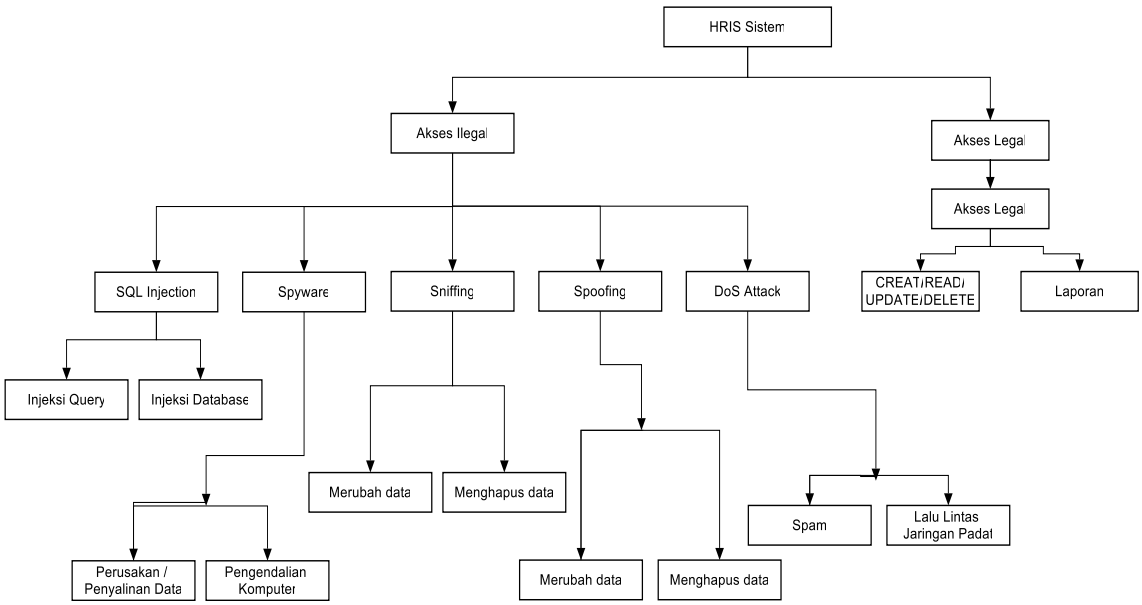


Gambar 4 *Misuse Case* Aplikasi HRIS (MU-01)

d. Attack Tree

Pohon serangan merupakan tindakan formal yang menggambarkan ancaman keamanan terhadap sistem dengan jenis serangan yang dapat terjadi dan diimplementasikan. Pohon serangan yang terjadi dalam proses sistem HRIS diantaranya:

- Pohon serangan SQL Injection (MC-01)
- Pohon serangan Spyware and Trojans (MC-02)
- Pohon serangan Sniffing (MC-03)
- Pohon serangan Spoofing (MC-04)
- Pohon serangan Denial of Service (MC-05)



Gambar 5 *Attack Tree* Sistem HRIS

Hasil 4. *Perform Risk Assesment* (Penilaian Risiko)

Pada tahap ini melakukan analisa Penilaian risiko secara kualitatif dan bertahap untuk mengidentifikasi ancaman terhadap sistem yang kemungkinan terjadi dan ini adalah hasil dari penilaian risiko dengan melakukan metode *interview*.

Tabel 4 Penilaian risiko

No	Kategori Ancaman	Kondisi	Dampak	Kategori
1	SQL *Injection*	Melakukan acak login pada menu *login* klien	Kehilangan data pengguna dan *password* pengguna yang legal	*Medium*
2	Data *Sniffing*	Melakukan pengintipan lalulintas jaringan	Penyerang dapat melihat dengan jelas dan mengetahui aktifitas data di sistem.	*Low*
3	*Mac Address Spooffing*	Mengambil IP *Address* yang ada di dalam jaringan untuk di palsukan	Penyerang dapat mengambil informasi yang tersedia pada pengguna legal	*High*

4	*Trojans*	Melakukan perusakan, pencurian aktifitas sebuah komputer	Dapat melihat aktivitas admin, mengendalikan komputer serta dapat mencurri data *user*	*Low*
5	*Denial of Services*	Mengirim data dalam jumlah banyak terhadap *server* agar *server* mengalami kerusakan.	Membuat jaringan menjadi padat sehingga komputer tidak menanggapi permintaan layanan	*Medium*

Hasil 5. *Select Elicitation Technique* (Memilih teknik elisitasi)

Pemilihan Teknik elisitasi yang dilakukan penulis yaitu dengan cara *interview*, sumber tertulis dan observasi. Karena metode elisitasi ini sangat efisien karena langsung mengetahui dari instansi apa saja yang perlu dipecahkan dan mengenali batasan-batasan sistem dan mengenali siapa saja pemangku kepentingan untuk tujuan sebuah sistem.

Hasil 6. *Elicit Security Requirements* (Permintaaan persyaratan keamanan)
Untuk melakukan elisitasi persyaratan keamanan, maka perlu melakukan elisitasi keamanan yang baik dari hasil *interview*, sumber tertulis dan observasi, dan kemudian dibentuk dalam daftar kebutuhannya. Berikut adalah hasil dari persyaratan keamanan.
R : *Requierements*

Tabel 5 Persyaratan keamanan

R-01	Kebutuhan untuk memverifikasi di *gateway* dengan hanya membatasi komputer dengan resolusi alamat IP tertentu yang terdaftar di komputer *server* sehingga tidak dapat memalsukan data
R-02	Persyaratan untuk kontrol akses berbasis peran yang mengontrol elemen sistem (data, fungsi, dll.), Pengguna dapat berkomunikasi dengan sistem. Karakter yang ditentukan hanya memperbolehkan huruf a - z, A - atau angka 0 - 9 dan melarang karakter unik atau simbol
R-03	Diperlukan untuk rencana kerja ketersediaan sistem. Setiap pengguna diharuskan menggunakan nama pengguna dan kata sandi kombinasi, seperti angka, huruf besar, atau huruf kecil
R-04	Sistem ini diperlukan bagi personel keamanan yang ditunjuk untuk memantau status dan penggunaan, termasuk peralatan keamanan
R-05	Petugas yang ditunjuk diperlukan untuk memantau sumber daya sistem dan penggunaannya secara teratur
R-06	Sistem diperlukan untuk komunikasi jaringan yang dilindungi dari informasi yang tidak sah, enkripsi, dan metode lainnya. Enkripsi sangat membutuhkan penyebaran, seperti otentikasi *login*. Karena untuk mencegah peretas membobol sistem agar tidak mengetahui akses *login*
R-07	Memerlukan izin proses penting untuk mencegah perangkat di gunakan secara ilegal
R-08	Lindungi perangkat dari kerusakan, pencurian, atau penggantian perangkat yang tidak dikenal, kecuali bencana alam
R-09	Implementasi komponen keamanan virus perangkat lunak yang dirancang untuk keamanan perangkat lunak yang lebih baik, seperti antivirus

Hasil 7. *Categorize Requirements* (Mengkategorikan Persyaratan)
Setelah persyaratan yang dihasilkan maka selanjutnya yaitu mengelompokan persyaratan keamanan yang dipilih, dalam hal ini menggabungkan langkah-langkah pengelompokan, penamaan, dan kategorisasi bersama-sama. Berikut tabel pengkategoriannya :

Tabel 6 Kategori persyaratan

A. KERAHASIAAN	B. AKSES KONTROL
Admin yang mengakses internet melalui LAN dan *wireless* harus terjaga keamanannya agar data rahasia tidak diketahui oleh pengguna yang tidak sah atau illegal	1. Hanya user yang terdaftar saja yang dapat melakukan akses pada kontrol sistem. 2. Adanya pengaturan akses kontrol terhadap keamanan jaringan
C.INTEGRITAS DATA	D.PENGELOLAAN
Setting secara rutin terhadap data *user*, akses kontrol agar tidak dapat di serang pengguna ilegal	Adanya proses manajemen hak akses yang dapat dipertanggung jawabkan atas kebenaran data yang ada
E.PENGGUNAAN	F.AUTHENTIFIKASI
1. Penerapan manajemen terhadap Sistem keamanan agar dapat di Kelola dan tidak mengganggu aktifitas sistem 2. Melakukan Authentikasi terhadap akses user yang harus selalu tersedia 3. Menghilangkan risiko terhadap aktifitas yang dapat merusak sistem	Melakukan authentikasi dengan baik dan sesuai dengan prosedur ketentuan

Hasil 8. *Prioritize Requirements* (Prioritas Persyaratan)
Proses ini memprioritaskan pemilihan persyaratan keamanan untuk jaringan nirkabel dan LAN pada jaringan di PT. XYZ berdasarkan penyalahgunaan yang dibuat sebelumnya. Untuk memprioritaskan serangan yang membuat ancaman lebih berbahaya, tabel prioritas ancaman diharapkan dapat mengatasi masalah ini.

Tabel 7 Prioritas keamanan

Tujuan	***Confidentiality , Integrity* dan *Availability***
Kebutuhan	- Keamanan sistem *login* dan *server* - Keamanan pada alamat IP - *Database* yang terjaga kerahasiaannya
Kategori	- *Unauthorized Attack* - *Access Control* - *Privacy* - *Authentication*
Rekomendasi	- Pemasangan *firewall* pada *server* - Penggunaan tanda tangan digital untuk sistem *login* - *Patching* pada sistem apikasi - Pemasangan Anti virus - Menerapkan enkripsi pada *system database* - Perubahan *password* admin secara rutin - Installasi SSL pada *cPanel*

Tabel 8 Kategori prioritas

Requirements	*Missusecase*	Prioritas
Penerapan *Password* Enkripsi	MU-01	*MEDIUM*
Menerapkan Anti Virus	MU-01	*LOW*
Pemasangan *Firewall* pada *Server*	MU-01	*HIGH*
Menerapkan Enkripsi dan Authentifikasi	MU-01	*HIGH*
Instalasi SSL pada *cPanel*	MU-01	*HIGH*

Hasil 9. *Requirement Inspection* (Penilaian Kebutuhan)
Membuat tabel penilaian dan dalam metode ini memberikan tanggung jawab kepada anggota tim inspeksi dan mengembangkan log dengan tinjauan rekomendasi masalah terperinci untuk arsitektur dan persyaratan kebijakan implementasi keamanan sistem berdasarkan tingkat prioritas penyalahgunaan.

Tabel 9 Penilaian kebutuhan

Goal(s)	Melindungi akases jaringan komputer serta data yang terdapat didalamnya dari serangan pihak lain
Requerement(s)	Sistem harus memenuhi ketentuan : • Sistem harus dapat melindungi dirinya sendiri dari virus dengan menggunakan perangkat lunak pendeteksi virus dengan data yang terupdate • Sistem harus dapat mendeteksi Ketika serangan seperti *SQL Injection dan* DoS Ketika itu terjadi sistem harus memberi admin atau melalui notifikasi sehingga dapat langsung di cegah • Sistem harus menggunakan Teknologi *Firewall* • Sistem harus memiliki enkripsi data yang baik • Sistem harus di pasangkan SSL
Category	*Unauthorize Attack, Access Control, Privacy, Authentication, Encryption*
Missuse Case	MU-01
Implementation	Fitur yang telah di implementasi dalam sistem: • *Virus Detection* dengan menggunakan *Software* Antivirus • *Encode/Decode* algoritma • Pengamanan pada *Web Server* • Pembenahan pada Konfigurasi *Firewall* • Penerapan ACL pada jaringan • *Double Autentication* pada setiap aktifitas

4. KESIMPULAN

Dari hasil penelitian ini, peneliti dapat menyimpulkan bahwa :

1. metode SQUARE sangat berguna untuk menganalisis dan membuat rekomendasi kebutuhan keamanan sistem yang bertujuan untuk meningkatkan ketersediaan, kontinuitas dan integritas Sistem Informasi HRIS PT. XYZ.
2. Metode SQUARE ini memungkinkan untuk mengetahui bahwa bagian kerentanan yang dapat dimasukkan oleh pengguna jahat dan dapat digunakan sebagai perencanaan saat membangun sistem dan infrastruktur dan tidak menutup kemungkinan adanya kegagalan dalam proses Analisa terutama pada bagian implementasi.

5. SARAN

Adapun saran dari hasil penelitian ini adalah :

1. Penggunaan metode SQUARE, baiknya dilakukan oleh tim, agar pada saat uji dan analisis mendapatkan hasil yang lebih rinci terhadap sistem *Human Resources Information System* (HRIS) PT. XYZ.
2. Hasil dari metode SQUARE ini, ada baiknya dibandingkan dengan hasil metode yang lain yang berhubungan dengan keamanan sebuah sistem.

DAFTAR PUSTAKA

[1] I. A. Sumra, H. Bin Hasbullah, and J. Bin AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey," in *Vehicular Ad-Hoc Networks for Smart Cities*, Springer, 2015, pp. 51–61.

[2] A. Tchernykh, U. Schwiegelsohn, E. Talbi, and M. Babenko, "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability," *J. Comput. Sci.*, vol. 36, p. 100581, 2019.

[3] M. Aminzade, "Confidentiality, integrity and availability–finding a balanced IT framework," *Netw. Secur.*, vol. 2018, no. 5, pp. 9–11, 2018.

[4] M. Kumar, J. Meena, R. Singh, and M. Vardhan, "Data outsourcing: A threat to confidentiality, integrity, and availability," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 1496–1501.

[5] T. Gřivna and J. Drápal, "Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic," *Digit. Investig.*, vol. 28, pp. 1–13, 2019.

[6] Y. Arta, A. Syukur, and R. Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik," *IT J. Res. Dev.*, vol. 3, no. 1, pp. 94–104, 2018.

[7] S. Martsanto and G. Nabihi, "Metode Square Pada Aplikasi Remittance," vol. 2, no. 1, pp. 39–44, 2016.

[8] Y. H. Akbar, "Evaluasi Keamanan Jaringan Wireless Hotspot Menggunakan Metode Square (Studi Kasus Warnet Medianet Sumedang)," *Infoman's J. Ilmu-ilmu Manaj. dan Inform.*, vol. 9, no. 2, pp. 75–90, 2015.

[9] L. Yin, B. Fang, Y. Guo, Z. Sun, and Z. Tian, "Hierarchically defining Internet of Things security: From CIA to CACA," *Int. J. Distrib. Sens. Networks*, vol. 16, no. 1, p. 1550147719899374, 2020.

[10] W. A. Conklin, "IT vs. OT security: A time to consider a change in CIA to include resilienc," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 2642–2647.

[11] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. networks*, vol. 169, p. 107094, 2020.

[12] H. Suhaemi, A. Sunarto, D. Murtiningsih, D. Napitupulu, and R. Rahim, "Implementation of Square Methods in Analyzing the Security of an Application System," in *ICASI 2019: Proceedings of The 2nd International Conference On Advance And Scientific Innovation, ICASI 2019, 18 July, Banda Aceh, Indonesia*, 2019, p. 390.

[13] S. Bhattacharya and M. Nandi, "A note on the chi-square method: A tool for proving cryptographic security," *Cryptogr. Commun.*, vol. 10, no. 5, pp. 935–957, 2018.

[14] S. T. A. Ramadhani, R. Hartanto, and E. Nugroho, "Manajemen Risiko Keamanan

Informasi Dengan Menggunakan Metode Octave Allegro Dan Kontrol Iso 27001 Pada Instansi Pelayanan Penyelenggara Publik," *Pros. SEMNASTEK 2018*, vol. 1, no. 1, 2018.

[15] S. N. Ambo and M. Ghufron, "Rancang Bangun Aplikasi Human Resource Information System (HRIS) Menggunakan Metode Model View Controller (MVC)," *Pros. Semnastek*, 2015.

[16] A. Hanafiah and R. Wandri, "Implementasi Load Balancing Dengan Algoritma Penjadwalan Weighted Round Robin Dalam Mengatasi Beban Webserver," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 226–233, 2021.