**PROPOSAL SKRIPSI NON KELAS**

**STUDI ANALISIS LALU LINTAS JARINGAN UNTUK PENINGKATAN KEAMANAN SIBER**

**A STUDY OF NETWORK TRAFFIC ANALYSIS FOR CYBERSECURITY ENHANCEMENT**

**Topik**: Networking

2301855545 / Aryanto Bayu Setya Prawira / Computer Science / 085780000098



BINUS University

2024

Diperiksa oleh\*\*

<<tanda tangan>>

<<KdDosen-NmDosen>>

# DAFTAR ISI

[Daftar Isi i](#_Toc39496154)

[Bab 1. Pendahuluan 1](#_Toc39496155)

[Bab 2. Tinjauan Pustaka 5](#_Toc39496156)

[Bab 3. Metode Pelaksanaan 6](#_Toc39496157)

[Daftar Pustaka 7](#_Toc39496158)

# BAB 1. PENDAHULUAN

**1.1 Latar Belakang**

Di ruang lingkup digital yang saling berhubungan, ketergantungan pada infrastruktur jaringan telah menjadi hal yang umum, menekankan perlunya Langkah-langkah keamanan siber yang Tangguh. Seiring dengan kemajuan teknologi, begitu juga Tingkat kompleksitas dan keragaman ancaman siber. Pendekatan keamanan tradisional seringkali kurang efektif dalam mengidentifikasi dan mengatasi risiko-risiko baru secara proaktif. Hal ini menekankan pentingnya keamanan jaringan, di mana analisis lalu lintas jaringan menjadi strategi penting untuk memperkuat jalur digital.   
  
Permasalahan yang akan diangkat untuk diatasi pada penelitian ini adalah dimulai dengan berkembangnya ruang lingkup Ancaman Siber. Sifat dinamis dan terus-menerus berkembangnya ancaman siber merupakan tantangan besar. Penyerang terus menyesuaikan taktik, Teknik dan prosedur mereka (TTP), membuat Tindakan keamanan konvensional sulit mengikuti perkembangan ini. Karena hal tersebut dibutuhkan untuk dilakukan analisis mendalam terhadap tren ancaman siber terkini, menekankan perlunya Tindakan keamanan yang proaktif dan mampu beradaptasi dengan ancaman yang muncul. Kemudian permasalahan mengenai Tindakan keamanan tradisional yang kurang efektif. Tindakan keamanan tradisional, seperti system deteksi intrusi berbasis tanda tangan, mungkin tidak efektif melawan vector serangan baru dan canggih seperti eksploitasi zero-day. Dengan permasalahan itu, ada baiknya untuk mengevaluasi keterbatasan Tindakan keamanan tradisional dan mengusulkan integrasi teknologi lanjutan, seperti pembelajaran mesin, dalam analisis lalu lintas jaringan untuk deteksi ancaman yang lebih adaptif.   
  
Dengan pembahasan masalah berikut, ini adalah Solusi yang akan dibahas dalam penelitian ini, dimulai dengan peningkatan pemantauan ancaman dari dalam. Pemantauan ancaman ini berupa penerapan analisis perilaku pengguna yang komprehensif untuk mengidentifikasi penyimpangan dari aktivitas pengguna normal, dengan menandai potensi ancaman dari dalam. Kemudian adalah Solusi yang berupa mengadopsi Tindakan keamanan yang adaptif. Solusi ini mengusulkan adopsi Tindakan keamanan yang adaptif, yang dapat menyesuaikan diri secara dinamis dengan ancaman yang muncul, mengurangi ketergantungan pada konfigurasi keamanan statis. Rencana selanjutnya adalah untuk adanya Pendidikan dan pelatihan personal. Rencana ini bertujuan untuk mengembangkan program kesadaran keamanan siber untuk karyawan, guna mengurangi kemungkinan pelanggaran keamanan yang tidak disengaja dan meningkatkan postur keamanan keseluruhan organisasi.

**1.2 Rumusan Masalah**

1. Apa yang membuat Tindakan keamanan yang ada kurang efektif?

2. Bagaimana perkembangan ruang lingkup ancaman siber yang ada sekarang?

**1.3 Ruang Lingkup**

Untuk penelitian ini, dengan topik utama untuk pengembangan keamanan spesifik dalam analisis lalu lintas. Penelitian ini ingin bekerja untuk skala nasional dan lebih kepada individual dan industry kecil. Penelitian ini akan memusatkan pada kondisi saat ini berdasarkan dari data dan bahan yang sudah pernah diteliti sebelumnya.

**1.4 Tujuan dan Manfaat**

**1.4.1 Tujuan Penelitian**

Tujuan penelitian ini adalah dimulai dengan meningkatkan kesadaran terhadap bahaya ancaman cyber. Kemudian adanya pelatihan interaktif mengenai ancaman cyber yang dapat membuat karyawan lebih terbiasa dengan ancaman skala kecil. Ada pula monitoring dan evaluasi untuk dapat memantau kemajuan dan mengukur Tingkat kesadaran keamanan cyber dari waktu ke waktu.

**1.4.2 Manfaat Penelitian**

Manfaat penelitian ini yang utama adalah untuk meningkatkan keamanan bisnis kecil tersebut, dengan meningkatkan pemahaman dan kesadaran karyawan terhadap potensi ancaman. Selanjutnya pengurangan resiko serangan cyber, dengan identifikasi dan mengatasi atau membuat pencegahan terhadap serangan cyber yang umum. Ada pula manfaat untuk reputasi bisnis, dengan menjaga dan meningkatkan kesadaran keamanan cyber maka dapat memajukan reputasi bisnis terhadap keamanan data dan informasi pelanggan.

**1.5 Metodologi**

**1.5.1 Metode Pengumpulan Data**

Pada penelitian ini metode pengumpulan data yang akan digunakan adalah lebih banyak kepada studi kasus dan analisis dokumen. Studi kasus yang berupa pemahaman mendalam tentang tantangan yang bisnis kecil hadapi dalam meningkatkan kesadaran keamanan cyber. Lalu analisis dokumen adalah untuk meninjau kebijakan keamanan yang sudah ada, catatan insiden keamanan atau laporan keamanan internal untuk mendapatkan pemahaman tentang situasi saat ini.

**1.5.2 Metode Perancangan Solusi**

Metode perancangannya akan dibagi menjadi beberapa tahap, dimulai dengan:

1. Analisis Kebutuhan  
   Pada bagian ini akan ditentukan kebutuhan utama bisnis kecil terkait kesadaran keamanan cyber melalui hasil studi kasus dan kuesioner.
2. Penentuan Fitur Aplikasi  
   Selanjutnya adalah mengidentifikasi fitur utama yang diperlukan dalam aplikasi, berdasarkan analisis kebutuhan. Yang dapat termasuk dalam fitur aplikasi ini adalah modul pelatihan, pelacakan kemajuan, notifikasi keamanan dan alat evaluasi resiko.
3. Perancangan Interface Pengguna  
   Kemudian adalah pembuatan interface yang ramah untuk pengguna dan dapat diakses, memastikan bahwa informasi keamanan disajikan dengan cara yang mudah dipahami.
4. Pengembangan Aplikasi  
   Setelah pembuatan interface maka aplikasi akan dikembangkan sesuai kebutuhan dan dilakukan pengujian berkala.
5. Uji Coba dan Evaluasi  
   Selanjutnya adalah uji coba aplikasi dengan pemilik bisnis kecil dan mengumpulkan umpan balik mereka. Setelahnya adalah evaluasi efektivitas aplikasi dalam meningkatkan kesadaran keamanan.

# BAB 2. TINJAUAN PUSTAKA

* 1. **Teori yang berkaitan dengan penelitian**

**1.1.1 Kesadaran Keamanan**

Teori ini mencakup aspek-aspek psikologis dan social dari kesadaran keamanan, membantu dalam memahami bagaimana individu dan kelompok pegawai bisnis kecil dapat membentuk pemahaman tentang ancaman cyber.

**1.1.2 Technology Acceptance Model**

TAM membahas factor-faktor yang memengaruhi penerimaan teknologi. Dalam konteks ini, ini dapat membantu menjelaskan bagaimana pemilik bisnis dan karyawan menerima dan mengadopsi Solusi keamanan cyber.

**1.1.3 User Behavior Theory**

Melibatkan pemahaman tentang perilaku individu terkait dengan keamanan cyber, seperti kepatuhan terhadap kebijakan keamanan, Tindakan preventif, dan respons terhadap ancaman.

**1.1.4 Teori Pembelajaran**

Pembelajaran dalam konteks kesadaran keamanan dapat mencakup pendekatan yang efektif untuk menyampaikan informasi keamanan kepada karyawan dan pemilik bisnis.

**1.1.5 Teori Perilaku Organisasi**

Melibatkan pemahaman tentang bagaimana budaya dan struktur organisasi dapat memengaruhi sikap dan perilaku terkait dengan keamanan cyber.

**1.1.6 User Engagement Theory**

Teori ini dapat membantu memahami cara meningkatkan keterlibatan pengguna**.**

* 1. **State of the Art**

Pada penelitian ini, terdapat penelitian terdahulu yang dapat membantu pengembangan dari penelitian ini. Beberapa penelitian terdahulu tersebut akan dijadikan sebagai referensi dan dapat dijadikan sebagai sumber daya untuk membantu penelitian yang dilakukan. Kemudian dari adanya paper penelitian-penelitian sebelumnya, dapat dipaparkan adanya persamaan dan perbedaan yang berkaitan dengan judul penelitian. Berikut adalah paper yang diambil yang akan berhubungan dengan judul penelitian ini:

|  |  |
| --- | --- |
| Jurnal Penelitian | |
| Penulis | Septian Reri Winarto, Rahadin Bisma |
| Tahun | 2021 |
| Jurnal | JINACS: Volume 03 Nomor 01 |
| Metode Penelitian | Metode yang digunakan adalah metode analisis data dengan bantuan sumber paper terdahulu |
| Judul Penelitian | Studi Literatur: Analisis Persepsi UMKM di Indonesia Terhadap *Cyber Security* Menggunakan Model *Protection Motivation Theory* (PMT) |
| Hasil | Hasil yang ditemukan adalah adanya beberapa hubungan aspek-aspek Cyber Security yang memengaruhi penggunaan teknologi |
| Hal yang berkaitan dengan penelitian | Dengan mengetahui aspek-aspek ini, penelitian dapat lebih difokuskan untuk mengembangkan Solusi yang berkaitan dengan aspek-aspek Cyber Security tersebut. |

# BAB 3. METODE PELAKSANAAN

**3.1 Kerangka Berpikir**

**3.1.1 Requirements**

Digunakan sumber pengetahuan dan kebutuhan terhadap Network Security yang akan dipelajari dan perlu untuk disebarkan pada software yang akan dibuat

**3.1.2 Data Analysis**

**3.1.3 Prototype**

**3.1.4 Prototype Evaluation**

**3.2 Analisis Masalah**

**3.2.1 Deskripsi singkat mengenai tempat penelitian**

**3.2.2 Analisis kebutuhan *user***

**3.2.3 Topologi**

**3.2.4 Observasi yang dilakukan**

**3.2.5 Identifikasi Masalah**

**3.2.6 Usulan Pemecahan Masalah**

**3.3 Perancangan**

**3.3.1 Rancangan topologi jaringan**

**3.3.2 Rancangan distribusi IP**

**3.3.3 Rancangan yang berkaitan dengan skripsi**

# DAFTAR PUSTAKA

Marelli M. The SolarWinds hack: Lessons for international humanitarian organizations. *International Review of the Red Cross*. 2022;104(919):1267-1284. doi:10.1017/S1816383122000194