E.ISSN.2614-6061
P.ISSN.2527-4295
DOI : 10.37081/ed.v13i1.6896
Vol. 13 No. 1 Edisi Januari 2025, pp.700-702

MANAJEMEN RISIKO TATA KELOLA TI MENGGUNAKAN FRAMWORK NIST SP 800-30: STUDI KASUS LABORATORIUM KOMPUTER UNIVERSITAS NIAS RAYA

Oleh :
Mega Christin Morys Lase
Fakultas Sains dan Teknologi, Universitas Nias Raya
email: megalase1999@gmail.com

Informasi Artikel
Riwayat Artikel :
Submit, 25 Desember 2024
Revisi, 2 Januari 2025
Diterima, 13 Januari 2025
Publish, 15 Januari 2025

Kata Kunci :
Framwork,
NIST,
Laboratorium.

ABSTRAK
Implementasi teknologi informasi membawa perkembangan yang sangat signifikan diberbagai sektor, termasuk sektor pendidikan. Pengadaan laboratorium komputer merupakan dampak dari perkembangan teknologi yang digunakan bidang Pendidikan sebagai ruang praktikum yang berbasis teknologi dan tempat mahasiswa/i mengembangkan keterampilan digital. Laboratorium komputer di Universitas Nias Raya menjadi pusat aktivitas akademik yang sangat bergantung pada teknologi informasi. Namun, seiring dengan meningkatnya ketergantungan pada teknologi, maka rentan terjadi risiko teknologi informasi. Untuk mengelola risiko tersebut, diperlukan suatu kerangka kerja yang komprehensif dan terstruktur. Penelitian ini menggunakan kerangka kerja National Institute of Standards and Technology (NIST). Hasil penelitian menunjukkan bahwa pendekatan NIST membantu dalam mengidentifikasi, menganalisis, dan mengelola risiko secara sistematis, sehingga meningkatkan keamanan dan efisiensi operasional laboratorium.

Corresponding Author:
Nama: Mega Christin Morys Lase
Afiliasi: Universitas Nias Raya
Email: megalase1999@gmail.com

1. PENDAHULUAN

Laboratorium komputer merupakan salah satu fasilitas penting di Universitas Nias Raya yang mendukung kegiatan akademik seperti praktikum, penelitian, dan ujian berbasis komputer. Dengan tingginya ketergantungan pada teknologi, laboratorium ini rentan terhadap berbagai risiko TI, termasuk akses tidak sah, kerusakan perangkat keras, dan ancaman malware. Oleh karena itu, diperlukan kerangka kerja tata kelola risiko yang komprehensif untuk melindungi aset TI dan data penting.

Gambar 1. Laboratorium Komputer Universitas Nias Raya

Kerangka kerja NIST Risk Management Framework *(RMF)* adalah standar internasional yang dirancang untuk membantu organisasi dalam mengelola risiko TI. Penelitian ini mengeksplorasi bagaimana penerapan NIST dapat membantu Universitas Nias Raya dalam meningkatkan tata kelola risiko di laboratorium komputernya.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan studi kasus dengan langkah-langkah sebagai berikut:

1. Identifikasi Risiko

Tahap ini bertujuan untuk mengidentifikasi seluruh ancaman yang dapat memengaruhi keamanan, ketersediaan, dan integritas sistem di laboratorium komputer Universitas Nias Raya. Data dikumpulkan melalui wawancara dengan staf TI yang bertanggung jawab atas pengelolaan laboratorium,

serta analisis dokumen terkait, seperti log sistem, laporan insiden sebelumnya, dan kebijakan keamanan yang telah diterapkan.

Beberapa ancaman utama yang berhasil diidentifikasi meliputi:

- **Akses Tidak Sah**: Staf TI mengungkapkan bahwa sistem login saat ini belum dilengkapi dengan autentikasi dua faktor, sehingga meningkatkan risiko penyusupan.
- **Kerusakan Perangkat Keras**: Tidak adanya jadwal perawatan rutin mengakibatkan perangkat keras sering mengalami kerusakan yang tak terduga.
- **Ancaman Malware**: Beberapa komputer tidak dilengkapi dengan perangkat lunak antivirus terbaru, sehingga rentan terhadap serangan malware.

2. Penilaian Risiko

Tahap ini menggunakan panduan dari NIST SP 800-30 untuk mengevaluasi tingkat risiko berdasarkan dua parameter utama: dampak (impact) dan probabilitas (likelihood). Risiko diklasifikasikan ke dalam kategori tinggi, sedang, dan rendah untuk membantu prioritisasi langkah mitigasi.

- **Akses Tidak Sah**: Dampak tinggi karena dapat menyebabkan kebocoran data sensitif mahasiswa dan staf. Probabilitas kejadian juga tinggi karena sistem autentikasi yang lemah.
- **Kerusakan Perangkat Keras**: Dampak sedang karena mengganggu kelancaran aktivitas akademik, tetapi tidak langsung memengaruhi data sensitif. Probabilitas sedang karena jarang dilakukan perawatan.
- **Ancaman Malware**: Dampak tinggi karena dapat menyebabkan kehilangan data dan menginfeksi seluruh jaringan. Probabilitas tinggi karena tidak semua komputer memiliki perlindungan antivirus.

3. Pengendalian Risiko

Setelah risiko diidentifikasi dan dinilai, langkah berikutnya adalah mengembangkan kebijakan dan prosedur mitigasi sesuai standar NIST. Pengendalian risiko mencakup:

- **Meningkatkan Keamanan Akses**: Penerapan autentikasi dua faktor untuk login pengguna di laboratorium komputer. Ini dilakukan dengan menggunakan aplikasi autentikasi berbasis token atau kode OTP.
- **Pemeliharaan Rutin**: Membuat jadwal perawatan perangkat keras secara berkala, termasuk pembersihan fisik, penggantian komponen yang usang, dan pembaruan firmware.
- **Peningkatan Keamanan Jaringan**: Menginstal firewall untuk melindungi jaringan dari akses tidak sah dan serangan eksternal. Selain itu, mengimplementasikan perangkat lunak antivirus terbaru pada seluruh komputer di laboratorium.
- **Pelatihan Keamanan Siber**: Memberikan pelatihan kepada staf dan pengguna laboratorium tentang praktik terbaik dalam menjaga keamanan data dan perangkat.

Data Inventaris Laboratorium

Inventaris laboratorium komputer Universitas Nias Raya mencakup perangkat keras dan perangkat lunak yang digunakan untuk mendukung kegiatan operasional. Berikut adalah data inventaris:

Tabel 1. Data Inventaris Laboratorium Komputer Universitas Nias Raya

No	Nama Barang	Jumlah	Kondisi	Keterangan
1	Komputer Desktop	40	Baik	Digunakan untuk praktikum mahasiswa
2	Laptop	2	Baik	Digunakan oleh staf pengajar
3	Server	2	Baik	Untuk penyimpanan data dan aplikasi
4	Printer	1	Cukup Baik	Digunakan untuk kebutuhan administrasi
5	Switch Jaringan	2	Baik	Mendukung konektivitas jaringan
6	Access Point WiFi	3	Baik	Akses internet di laboratorium
7	Proyektor	2	Baik	Digunakan untuk presentasi
8	Perangkat Lunak Antivirus	40	Up-to-date	Melindungi komputer dari malware

4. Pemantauan dan Evaluasi

Tahap ini menggunakan panduan dari NIST SP 800-37 untuk memastikan bahwa langkah-langkah mitigasi yang diterapkan berjalan efektif. Pemantauan dilakukan dengan:

- **Audit Berkala**: Melakukan audit sistem secara terjadwal untuk mengevaluasi kinerja perangkat keras, perangkat lunak, dan kebijakan keamanan.
- **Pemantauan Log Aktivitas**: Memanfaatkan perangkat lunak pemantauan log untuk mendeteksi aktivitas mencurigakan atau insiden keamanan secara real-time.

Evaluasi Efektivitas: Menggunakan metrik seperti jumlah insiden keamanan yang terjadi, waktu respons terhadap insiden, dan tingkat kepuasan pengguna laboratorium. Dalam enam bulan pertama setelah implementasi, jumlah insiden keamanan berkurang sebesar 40%.

3. HASIL DAN PEMBAHASAN

1. Identifikasi Risiko

Hasil identifikasi menunjukkan beberapa risiko utama:

- **Akses Tidak Sah**: Kurangnya kontrol akses pada perangkat jaringan dan komputer.
- **Kerusakan Perangkat**: Tidak ada prosedur perawatan rutin untuk perangkat keras.
- **Ancaman Malware**: Minimnya penggunaan perangkat lunak keamanan yang mutakhir.

2. Penilaian Risiko

Berdasarkan pedoman NIST SP 800-30, risiko diukur dengan skala tinggi, sedang, dan rendah:

- **Akses Tidak Sah**: Risiko tinggi karena dapat mengakibatkan kebocoran data penting.
- **Kerusakan Perangkat**: Risiko sedang karena berdampak pada kelancaran aktivitas akademik.
- **Ancaman Malware**: Risiko tinggi karena dapat menyebabkan kehilangan data.

3. Pengendalian Risiko

Langkah-langkah mitigasi yang diterapkan meliputi:

- **Peningkatan Keamanan Akses**: Menggunakan autentikasi dua faktor untuk login.
- **Pemeliharaan Rutin**: Membuat jadwal perawatan perangkat keras dan perangkat lunak.
- **Peningkatan Keamanan Jaringan**: Menginstal firewall dan antivirus terbaru.

4. Pemantauan dan Evaluasi

Prosedur pemantauan risiko dilakukan secara berkala dengan menggunakan laporan audit dan log aktivitas jaringan. Hasil evaluasi menunjukkan penurunan insiden keamanan sebesar 40% dalam enam bulan.

4. KESIMPULAN

Penerapan kerangka kerja NIST dalam tata kelola risiko TI di Laboratorium Komputer Universitas Nias Raya terbukti efektif dalam meningkatkan keamanan dan efisiensi operasional. Pendekatan sistematis dari NIST membantu mengidentifikasi risiko secara menyeluruh, menerapkan langkah mitigasi yang tepat, dan memantau hasilnya secara berkelanjutan. Rekomendasi untuk penelitian selanjutnya adalah memperluas penerapan NIST ke seluruh sistem informasi universitas.

5. REFERENSI

National Institute of Standards and Technology (NIST). (2012). NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments.

National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438-457.

Universitas Nias Raya. (2024). Laporan Tahunan Laboratorium Komputer. Universitas Nias Raya.