ANALISIS KEAMANAN WEBSITE PEMERINTAH KABUPATEN RAJA AMPAT MENGGUNAKAN METODE VULNERABILITY ASSESSMENT

FAHRIL YAU
31.1078
Program Studi Teknologi Rekayasa Informasi Pemerintahan Fakultas Manajemen Pemerintahan

email : fahrilyau81@gmail.com
Pembimbing Skripsi : Prof. Dr. Drs. Ismail Nurdin, M.Si

ABSTRACT

Problem Statement/Background (GAP): *Website security testing is crucial due to the increasing threats of cybercrime and the importance of information protection in governmental systems, including local government websites that contain a significant amount of personal data and public information. One of the regions in Indonesia that requires this is Raja Ampat Regency.* ***Purpose:*** *The main objectives of this research are to analyze the security level of the Raja Ampat Regency Government's website using the Vulnerability Assessment method, to evaluate the quality of human resource management (HRM) in the Information Technology (IT) sector that affects the website's security level, and to identify the efforts that have been made to enhance this security.* ***Method:*** *This research uses a mix of methods and a Vulnerability Assessment method approach. It involves automated testing through network security scans to identify vulnerabilities and potential threats. Data was collected from vulnerability evaluation reports and performance documents of relevant government agencies.* ***Results/Findings:*** *The study identified 19 vulnerabilities on the Raja Ampat Regency Government website that can affect the security of the data contained on the website. Some of these vulnerabilities include PII Disclosure, Absence of An-CSRF Tokens, Content Security Policy (CSP) Header Not Set, HTTP to HTTPS Insecure Transaction in Form Post, Missing An-clickjacking Header, Secure Pages Include Mixed Content, Strict-Transport-Security Header Not Set, Timestamp Disclosure - Unix, X-Content-Type-Options Header Missing, Charset Mismatch, Information Disclosure - Suspicious Comments, Modern Web Application, Re-examine Cache-control Directives, and User Controllable HTML Element Attribute (Potential XSS). Additionally, an evaluation of the quality of human resources in IT revealed that the lack of experts with higher education in information technology affects the effectiveness of website management and security.* ***Conclusion:*** *The main conclusion of this study is the need for greater attention to increasing the capacity and competence of human resources in the IT field as well as the implementation of more stringent and structured security policies to protect government information systems from cyber threats. The results of this research are expected to contribute to the improvement and development of information security systems in the local government environment.*

Keywords: *Cybercrime Threats; Quality of IT Personnel; Vulnerability Assessment; Website Security*

ABSTRAK

Latar Belakang (GAP): Pengujian keamanan website penting untuk dilakukan karena semakin meningkatnya ancaman kejahatan dunia maya dan pentingnya perlindungan informasi dalam sistem pemerintahan, termasuk pada website pemerintah daerah yang banyak memuat data pribadi dan informasi masyarakat. Salah satu daerah di Indonesia yang membutuhkan perhatian khusus dalam hal ini adalah Kabupaten Raja Ampat. **Tujuan:** Tujuan utama penelitian ini adalah untuk menganalisis tingkat keamanan website Pemerintah Kabupaten Raja Ampat menggunakan metode Vulnerability Assessment, mengevaluasi kualitas manajemen sumber daya manusia (SDM) di bidang Teknologi Informasi (TI) yang mempengaruhi tingkat keamanan website, dan mengidentifikasi upaya yang telah dilakukan untuk meningkatkan keamanan tersebut. **Metode:** Penelitian ini menggunakan pendekatan metode Mix Methods dan Vulnerability Assessment. Penelitian ini melibatkan pengujian otomatis melalui pemindaian keamanan jaringan untuk mengidentifikasi kerentanan dan potensi ancaman. Data dikumpulkan dari laporan evaluasi kerentanan dan dokumen kinerja instansi pemerintah terkait. **Hasil/Temuan:** Hasil penelitian menunjukkan terdapat 19 kerentanan pada website Pemerintah Kabupaten Raja Ampat yang dapat mempengaruhi keamanan data yang terdapat pada website. Beberapa kerentanan tersebut antara lain PII Disclosure, Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, HTTP to HTTPS Insecure Transaction in Form Post, Missing Anti-clickjacking Header, Secure Pages Include Mixed Content, Strict-Transport-Security Header Not Set, Timestamp Disclosure - Unix, X-Content-Type-Options Header Missing, Charset Mismatch, Information Disclosure - Suspicious Comments, Modern Web Application, Re-examine Cache-control Directives, dan User Controllable HTML Element Attribute (Potential XSS). Selain itu, evaluasi terhadap kualitas sumber daya manusia di bidang TI menunjukkan bahwa kurangnya tenaga ahli dengan pendidikan tinggi di bidang teknologi informasi mempengaruhi efektivitas pengelolaan dan keamanan situs web. **Kesimpulan:** Kesimpulan utama dari penelitian ini adalah perlunya perhatian yang lebih besar terhadap peningkatan kapasitas dan kompetensi sumber daya manusia di bidang TI serta penerapan kebijakan keamanan yang lebih ketat dan terstruktur untuk melindungi sistem informasi pemerintah dari ancaman siber. Hasil penelitian ini diharapkan dapat memberikan kontribusi terhadap perbaikan dan pengembangan sistem keamanan informasi di lingkungan pemerintah daerah.

Kata Kunci: Ancaman Kejahatan Dunia Maya, Kualitas SDM TI, Penilaian Kerentanan, Keamanan Website

I. PENDAHULUAN

1.1 Latar Belakang

Otonomi daerah memberikan peluang bagi daerah untuk mandiri dalam menjalankan tugas dan kewajibannya. Berdasarkan Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, urusan pemerintahan daerah terbagi menjadi tiga, salah satunya adalah urusan konkuren. Urusan ini menjadi dasar pelaksanaan otonomi daerah yang bertujuan untuk melindungi, melayani, memberdayakan, dan meningkatkan kesejahteraan masyarakat. Pemerintah daerah memiliki hak

untuk menetapkan kebijakan terkait urusan pemerintahan dengan tetap berpedoman pada ketetapan pemerintah pusat.

Undang-Undang Nomor 23 Tahun 2014 menyatakan bahwa kewajiban penyelenggaraan pelayanan publik oleh pemerintah daerah mencakup berbagai aspek seperti pelayanan, pengaduan, pengelolaan informasi, pengawasan, penyuluhan, dan konsultasi. Pelayanan publik yang efektif merupakan tolak ukur kinerja pemerintah yang paling nyata (Kurniawan, 2017). Teknologi informasi menawarkan kemudahan dalam membantu proses penyelenggaraan pemerintahan, terutama dalam hal pelayanan publik.

Teknologi Informasi dan Komunikasi (TIK) terdiri dari teknologi informasi dan teknologi komunikasi. Teknologi informasi mencakup semua hal terkait proses, penggunaan, modifikasi, dan manajemen informasi. Menurut Kamus Oxford (1995), teknologi informasi adalah penerapan perangkat elektronik, terutama komputer, untuk menyimpan, menganalisis, dan mendistribusikan berbagai jenis informasi. Rusman dkk. (2012) menyatakan bahwa teknologi informasi adalah serangkaian tahapan penanganan informasi yang meliputi penciptaan, pemeliharaan, seleksi, transmisi, penerimaan, penyimpanan, penelusuran, dan penggunaan informasi.

Teknologi informasi memiliki dampak besar di berbagai sektor kehidupan seperti perdagangan, ekonomi, dan politik. Penggunaan teknologi informasi memungkinkan masyarakat memenuhi tuntutannya dengan cepat melalui sistem yang terakses. Pengolahan data menjadi lebih cepat, akurat, efektif, dan efisien, menghasilkan informasi yang diperlukan.

Pada era milenium ketiga, lembaga pemerintah berbasis teknologi informasi berkembang pesat. Teknologi informasi digunakan untuk mengelola data dan menyediakan informasi yang akurat, tepat waktu, dan relevan. Informasi menjadi perekat yang menghubungkan komponen organisasi, sementara pengetahuan menentukan keefektifan organisasi pemerintah. Pemerintah perlu menyebarkan kebijakan dan informasi dengan cepat, salah satunya melalui pembuatan gateway website.

Website pemerintah daerah adalah alat komunikasi dan informasi yang penting. Informasi disampaikan melalui media elektronik yang disebarkan melalui internet. Pembuatan situs web pemerintah daerah memungkinkan masyarakat dan pemerintah untuk berbagi informasi, berkomunikasi, dan melakukan transaksi secara online. Ini menghasilkan manfaat seperti komunikasi yang lebih cepat, layanan pemerintah yang lebih efisien, dan akses informasi 24/7.

Namun, kemajuan teknologi ini tidak lepas dari penyalahgunaan. Tindakan peretasan, penipuan, dan kejahatan dunia maya sering terjadi, menargetkan individu, bisnis, perusahaan, dan organisasi pemerintah. Kejahatan dunia maya mencakup peretasan, pelanggaran hak cipta, pornografi anak, dan pencurian data pribadi. Oleh karena itu, keamanan sistem informasi sangat penting untuk mencegah dan mendeteksi penipuan di sistem berbasis informasi.

Pemerintah Kabupaten Raja Ampat adalah salah satu instansi yang memanfaatkan internet untuk mengelola data dan menyebarkan informasi kepada publik. Keamanan situs web pemerintah daerah sangat penting. Berdasarkan Laporan Kinerja Instansi Pemerintah (LKJIP) tahun 2022, terdapat tantangan dalam pengelolaan Manajemen Sumber Daya Manusia (MSDM) di sektor Teknologi Informasi (TI). Evaluasi kerentanan situs web dilakukan untuk mengidentifikasi dan menilai potensi ancaman. Salah satu studi kasus yang relevan adalah peretasan situs web Kejaksaan Agung Republik

Indonesia pada tahun 2021, yang menunjukkan bahwa bahkan situs web tingkat tinggi dapat rentan terhadap serangan.

1.2 Kesenjangan Masalah yang Diambil

Meskipun telah diakui bahwa penggunaan teknologi informasi (TI) dapat meningkatkan efektivitas dan efisiensi pelayanan publik oleh pemerintah daerah, masih terdapat kesenjangan dalam implementasi dan pemanfaatannya secara optimal. Salah satu kesenjangan yang mencolok adalah kurangnya sumber daya manusia (SDM) yang terampil dan kompeten dalam pengelolaan TI, terutama di wilayah-wilayah tertentu seperti Kabupaten Raja Ampat. Berdasarkan data dari Laporan Kinerja Instansi Pemerintah (LKJIP) tahun 2022, terlihat bahwa jumlah SDM dengan pendidikan tinggi yang relevan masih sangat minim. Hal ini mengindikasikan bahwa meskipun infrastruktur TI tersedia, kurangnya tenaga ahli yang dapat memanfaatkan teknologi tersebut menjadi penghambat utama dalam mencapai tujuan pelayanan publik yang optimal.

Kesenjangan lainnya adalah dalam hal keamanan sistem informasi. Penggunaan teknologi informasi yang luas membawa serta risiko kejahatan siber yang semakin meningkat, seperti peretasan, pencurian data, dan berbagai bentuk kejahatan dunia maya lainnya. Studi kasus peretasan situs web Kejaksaan Agung Republik Indonesia menunjukkan bahwa bahkan situs web pemerintah yang seharusnya memiliki tingkat keamanan tinggi pun dapat menjadi target serangan. Hal ini memperlihatkan adanya kesenjangan dalam penerapan langkah-langkah keamanan yang efektif dan berkelanjutan untuk melindungi data dan informasi publik dari ancaman siber. Evaluasi kerentanan dan tindakan pencegahan yang memadai belum diterapkan secara konsisten di seluruh instansi pemerintah daerah, termasuk di Kabupaten Raja Ampat.

Selain itu, kesenjangan dalam pemahaman dan kesadaran akan pentingnya teknologi informasi di kalangan aparatur pemerintah juga menjadi isu yang signifikan. Banyak aparatur pemerintah yang belum sepenuhnya memahami potensi dan manfaat dari penerapan teknologi informasi dalam meningkatkan pelayanan publik. Keterbatasan dalam pelatihan dan pengembangan kapasitas bagi aparatur pemerintah daerah mengakibatkan rendahnya tingkat adopsi teknologi baru dan inovatif. Untuk menjembatani kesenjangan ini, diperlukan upaya sistematis dalam memberikan pendidikan dan pelatihan yang sesuai bagi para aparatur pemerintah daerah agar mereka dapat memanfaatkan teknologi informasi secara optimal dalam menjalankan tugas dan fungsi mereka.

1.3 Penelitian Terdahulu

Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner - *Darojat E., Z. Sediyono E., Sembiring I.* (2022) Penelitian ini meneliti keamanan website e-government menggunakan metode NIST SP 800-115 dan OWASP. Kedua metode ini digunakan untuk menguji dan menilai parameter keamanan informasi pada dua situs web pemerintah, yakni semarangkab.go.id dan gunungtumpeng.id. Hasil penelitian menunjukkan persamaan dalam kategori ancaman dan jumlah kerentanan menggunakan dua alat

pemindai web, meskipun terdapat perbedaan dalam durasi dan kecepatan pemindaian (Darojat et al., 2022).

Analisis Pengujian Kerentanan Situs Pemerintahan XYZ dengan PTES - *Ningsih S. W.* (2021) Penelitian ini menganalisis keamanan situs web layanan terpadu pemerintah daerah XYZ menggunakan standar PTES. Beberapa alat seperti OWASP ZAP, Acunetix, dan Paros digunakan dalam pengujian. Hasilnya menunjukkan bahwa setiap alat mendeteksi kerentanan dengan tingkat risiko yang berbeda-beda, dengan OWASP ZAP menemukan risiko tinggi sebesar 10%, Acunetix sebesar 16,6%, dan Paros sebesar 20% (Ningsih, 2021).

Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating - *Ghozali B., Kusrini K., Sudarmawan S.* (2019) Penelitian ini menggunakan metode OWASP Risk Rating untuk mendeteksi kerentanan keamanan pada sistem informasi harga komoditas utama. Studi ini menunjukkan bahwa penerapan metode OWASP dapat memperkirakan risiko terhadap keberlangsungan bisnis dan mendeteksi kerentanan keamanan yang dapat digunakan untuk memperbaiki sistem (Ghozali et al., 2019).

Vulnerability Testing Analysis of XYZ Regional Government Site Using PTES - *Ningsih S. W., Almaarif A., Widjadjarto A.* (2021) Studi ini melakukan assessment dan penetration testing pada situs pemerintah daerah XYZ dengan standar PTES. Hasil penelitian menunjukkan bahwa berbagai alat mendeteksi jenis kerentanan dengan tingkat risiko yang bervariasi, dimana OWASP ZAP mendeteksi 10% risiko tinggi, Acunetix 16,6%, dan Paros 20% (Ningsih et al., 2021).

Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment - *Pendidikan J., Konseling D.* (2022) Penelitian ini menganalisis keamanan website Universitas Singaperbangsa Karawang menggunakan metode Vulnerability Assessment. Alat yang digunakan termasuk OWASP ZAP, Nmap, Nikto, dan Acunetix. Hasil penelitian menunjukkan adanya berbagai kerentanan yang dapat dieksploitasi dan memberikan rekomendasi untuk meningkatkan keamanan situs web tersebut (Akmal1 et al., 2022).

Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux - *FirdaPutri S., Kurniadi H.* (2023) Penelitian ini menggunakan metode penetration testing melalui Kali Linux untuk menganalisis keamanan website Pemerintah Kabupaten Kediri. Hasil penelitian menunjukkan adanya beberapa port terbuka yang dapat dieksploitasi oleh attacker untuk mengekspos data sensitif, dengan skor CVSS Base Score point 5.5 pada level medium (Firda et al., 2023).

ANALISIS PENGUJIAN PENETRASI PADA LAYANAN HOSTING MENGGUNAKAN METODE BLACK BOX (Studi kasus: Blogspot, Wordpress dan Shared Hosting) - *Bimandaru A., Alamsyah A., Nugroho A.* (2023) Penelitian ini menganalisis keamanan layanan hosting menggunakan metode Black Box. Dengan menggunakan sampel dari Blogspot, Wordpress, dan Shared Hosting, studi ini menemukan bahwa jenis kerentanan yang sering terjadi adalah XSS, CSRF Tokens, dan Clickjacking. Penelitian ini bertujuan membantu pemerintah desa dalam memilih layanan hosting yang aman (Bimandaru et al., 2023).

ANALISIS KEAMANAN WEBSITE DINAS PERHUBUNGAN PROVINSI JAWA TIMUR MENGGUNAKAN METODE OCTAVE ALLEGRO DAN FMEA - *Ayu Setia H., Safitri*

E. M., Wibowo C. P. (2023) Penelitian ini menggunakan metode OCTAVE Allegro dan FMEA untuk menganalisis keamanan website Dinas Perhubungan Provinsi Jawa Timur. Studi ini menekankan pentingnya adaptasi teknologi untuk memastikan kualitas penyampaian informasi kepada masyarakat dan menunjukkan bahwa analisis risiko dan mitigasi yang tepat dapat meningkatkan keamanan informasi (Ayu Setia et al., 2023).

Pengujian Keamanan Website Universitas A Menggunakan OWASP ZAP dan Burp Suite - (Aryanti et al., 2021) Penelitian ini menguji keamanan website Universitas A menggunakan alat OWASP ZAP dan Burp Suite. Hasil pengujian menunjukkan adanya beberapa kerentanan dengan tingkat risiko tinggi, seperti SQL Injection dan XSS. Rekomendasi diberikan untuk meningkatkan kebijakan keamanan dan implementasi teknis.

Evaluasi Keamanan Website Pemerintah Kota B dengan Metode Penetration Testing dan Risk Assessment - (Carkiman et al., 2021) Studi ini mengevaluasi keamanan website Pemerintah Kota B menggunakan metode penetration testing dan risk assessment. Hasil penelitian menunjukkan bahwa meskipun ada beberapa kebijakan keamanan yang sudah diterapkan, masih terdapat kerentanan yang signifikan. Rekomendasi diberikan untuk memperbaiki kebijakan dan prosedur keamanan

1.4 Pernyataan Kebaruan Ilmiah

Pernyataan kebaruan ilmiah ini menyoroti pentingnya analisis keamanan terbaru terkait website pemerintah, khususnya di Kabupaten Raja Ampat, menggunakan metode Vulnerability Assessment (VA). Penelitian ini menjadi signifikan karena Kabupaten Raja Ampat, sebagai destinasi wisata internasional yang terkenal, memiliki kebutuhan akan infrastruktur digital yang aman dan andal untuk mendukung layanan publik dan promosi pariwisata. Metode VA digunakan untuk mengidentifikasi dan mengevaluasi kerentanan keamanan yang mungkin ada pada website pemerintah ini, dengan fokus pada OWASP sebagai kerangka kerja yang umum digunakan untuk menilai dan mengelola risiko keamanan aplikasi web.

Penelitian ini menawarkan kontribusi berharga dalam konteks keamanan informasi pemerintah daerah di Indonesia, khususnya dalam konteks Kabupaten Raja Ampat yang unik dengan tantangan infrastruktur dan lingkungan yang khas. Dengan menerapkan metode VA, penelitian ini tidak hanya mengevaluasi keamanan website dari aspek teknis, tetapi juga memberikan pandangan mendalam tentang bagaimana kerentanan ini dapat mengancam integritas dan ketersediaan layanan publik yang disediakan melalui platform digital pemerintah.

Selain itu, penelitian ini memberikan wawasan baru tentang adaptasi dan penerapan metode keamanan canggih dalam konteks administrasi publik lokal di Indonesia. Dengan fokus pada penerapan VA pada website pemerintah Kabupaten Raja Ampat, penelitian ini diharapkan dapat memberikan rekomendasi praktis bagi pengembang dan administrator sistem untuk memperbaiki keamanan, meningkatkan ketahanan terhadap serangan siber, dan mengoptimalkan kinerja serta keandalan layanan e-government di tingkat lokal.

1.5 Tujuan

Tujuan utama dari penelitian ini adalah untuk mengevaluasi dan menganalisis pelaksanaan reformasi birokrasi di Badan Pengembangan Sumber Daya Manusia Daerah (BPSDMD) Provinsi Sumatera Selatan. Secara lebih spesifik, penelitian ini bertujuan untuk mengidentifikasi dan memahami proses reformasi yang telah dilakukan, serta mengevaluasi sejauh mana reformasi tersebut telah berjalan sesuai dengan harapan dan standar yang ditetapkan. Dengan demikian, penelitian ini diharapkan dapat memberikan gambaran yang komprehensif mengenai keberhasilan dan kekurangan dalam pelaksanaan reformasi birokrasi di BPSDMD Provinsi Sumatera Selatan.

Selain itu, penelitian ini juga bertujuan untuk mengidentifikasi faktor-faktor yang mendukung dan menghambat pelaksanaan reformasi birokrasi di BPSDMD Provinsi Sumatera Selatan. Dalam hal ini, peneliti akan menganalisis berbagai elemen yang berperan dalam proses reformasi, baik yang bersifat internal maupun eksternal. Faktor-faktor pendukung seperti kebijakan yang efektif, dukungan dari pimpinan, dan ketersediaan sumber daya yang memadai akan diidentifikasi dan dianalisis. Sebaliknya, peneliti juga akan mencari tahu hambatan-hambatan yang menghalangi pelaksanaan reformasi, seperti resistensi terhadap perubahan, keterbatasan anggaran, dan kurangnya kompetensi pegawai.

Tujuan akhir dari penelitian ini adalah untuk merumuskan strategi dan rekomendasi untuk mengatasi hambatan-hambatan yang dihadapi dalam pelaksanaan reformasi birokrasi di BPSDMD Provinsi Sumatera Selatan. Dengan memahami secara mendalam faktor-faktor penghambat dan pendukung, peneliti akan dapat menyusun langkah-langkah praktis dan strategis untuk memperbaiki dan mempercepat proses reformasi birokrasi. Rekomendasi ini diharapkan dapat digunakan oleh pemerintah daerah dan lembaga terkait lainnya untuk meningkatkan efisiensi, efektivitas, dan kualitas pelayanan publik di Provinsi Sumatera Selatan.

II. METODE

Penelitian ini menggunakan pendekatan campuran (mixed methods) yang dikenal sebagai metode ketiga setelah penelitian kuantitatif dan kualitatif. Pendekatan ini memungkinkan peneliti untuk menggabungkan berbagai pendekatan dalam pengumpulan dan analisis data, daripada membatasi diri pada satu metode saja. Dalam penelitian ini, penulis memilih desain campuran sequential eksplanatori (explanatory sequential mixed methods) (Sari sasi gendro, 2022).

Operasionalisasi konsep dalam penelitian ini mengacu pada rumusan masalah yang diuraikan dalam tiga masalah utama, yang kemudian dijabarkan menjadi dua tema penelitian. Tabel operasionalisasi konsep menunjukkan dimensi dan indikator yang digunakan untuk menganalisis keamanan website Pemerintah Kabupaten Raja Ampat menggunakan Metode Vulnerability Assessment (Sujarwoto, 2023).

Data dalam penelitian ini dikumpulkan dari berbagai sumber, termasuk dokumen, informan manusia, dan lokasi penelitian. Penggunaan purposive sampling untuk informan dan accidental sampling untuk masyarakat bertujuan memperoleh data yang mendalam dan representatif sesuai dengan tujuan penelitian (Murdiyanto, 2020).

Instrumen penelitian yang digunakan meliputi aplikasi OWASP ZAP untuk pengujian keamanan website secara kuantitatif dan wawancara serta dokumentasi untuk mendalami kualitas sumber daya manusia yang mempengaruhi keamanan website secara kualitatif. Teknik pengumpulan data meliputi observasi langsung dan dokumentasi proses pengecekan keamanan website (Sugiyono, 2013).

Analisis data dilakukan menggunakan Model Convergent Parallel Mixed, di mana data dari metode kuantitatif dan kualitatif diintegrasikan untuk memberikan pemahaman menyeluruh tentang keamanan website Pemerintah Kabupaten Raja Ampat. Teknik analisis melibatkan analisis vulnerability assessment dan teori manajemen sumber daya manusia untuk mendapatkan wawasan yang komprehensif (Dr.Sudaryono, 2018).

III. HASIL DAN PEMBAHASAN

3.1 Kinerja Sumber Daya Manusia IT di Dinas Komunikasi dan Informatika Kabupaten Raja Ampat

Faktor Penentu Kinerja SDM IT: Kinerja sumber daya manusia IT sangat dipengaruhi oleh pengetahuan, keterampilan, dan sikap individu yang terlibat dalam pengelolaan dan pengembangan teknologi informasi. Pengetahuan mencakup pemahaman mendalam tentang konsep dan teknologi yang digunakan, serta aplikasi praktisnya dalam konteks pekerjaan. Keterampilan teknis seperti pengembangan aplikasi dan manajemen sistem, serta keterampilan non-teknis seperti manajemen proyek dan komunikasi, juga sangat diperlukan. Sikap individu, seperti motivasi tinggi, keterbukaan terhadap perubahan, dan kemauan untuk terus belajar, memainkan peran penting dalam meningkatkan produktivitas dan inovasi dalam penggunaan teknologi informasi.

Implementasi Peraturan dan Teori Kinerja SDM: Dalam konteks Dinas Komunikasi dan Informatika Kabupaten Raja Ampat, implementasi pengembangan kinerja SDM IT terkait dengan Peraturan Pemerintah Nomor 30 Tahun 2019 tentang Penilaian Kinerja Pegawai Negeri Sipil. Teori kinerja SDM yang diperkenalkan oleh Sedarmayan (2017) membagi indikator kinerja menjadi pengetahuan, keterampilan, dan perilaku. Hasil wawancara menunjukkan bahwa karyawan di dinas ini memiliki pengetahuan yang kuat tentang infrastruktur jaringan dan pengelolaan sistem, namun masih perlu peningkatan dalam pemahaman tentang pengembangan aplikasi, analisis data, serta teknologi terbaru seperti kecerdasan buatan (AI) dan cloud computing.

Tantangan dalam Latar Belakang Pendidikan: Tantangan utama yang dihadapi adalah terkait dengan latar belakang pendidikan para ASN di Dinas Komunikasi dan Informatika. Sebagian besar karyawan tidak berasal dari latar belakang pendidikan sistem komputer, yang merupakan aset kritis dalam mengelola teknologi informasi yang kompleks. Meskipun upaya terus dilakukan untuk meningkatkan kualitas tenaga kerja melalui pelatihan dan kursus, keterbatasan dalam jumlah ASN yang ahli di bidang teknologi informasi masih menjadi kendala dalam memenuhi tuntutan teknis yang semakin kompleks.

Upaya Meningkatkan Kinerja dan Pelayanan: Meskipun demikian, Dinas Komunikasi dan Informatika Kabupaten Raja Ampat terus berkomitmen untuk meningkatkan kualitas layanan dan keamanan website pemerintah melalui langkah-langkah seperti audit keamanan berkala, pengembangan kebijakan keamanan informasi, serta pelatihan bagi personel terkait. Kolaborasi internal dan eksternal juga menjadi strategi untuk mengoptimalkan penggunaan sumber daya manusia yang ada, meskipun tantangan dalam pengembangan teknologi terus dihadapi.

3.2 Keamanan Website

Dalam penelitian ini, dilakukan analisis keamanan menggunakan metode Vulnerability Assessment terhadap website resmi Pemerintah Kabupaten Raja Ampat dengan memanfaatkan aplikasi OWASP ZAP. Hasil pengujian menunjukkan adanya 19 kerentanan keamanan yang berhasil diidentifikasi, mulai dari tingkat rendah hingga tinggi. Beberapa kerentanan mencakup ketidakhadiran Anti-CSRF Tokens, ketidaksetelan Content Security Policy (CSP) Header, hingga potensi kebocoran informasi sensitif melalui Big Redirect Detected. Untuk mengatasi hal ini, langkah-langkah perbaikan seperti pembaruan perangkat lunak, konfigurasi ulang server, dan penerapan kontrol keamanan direkomendasikan. Hal ini diharapkan dapat meningkatkan keamanan website dan mendorong penerapan kebijakan keamanan informasi yang lebih efektif.

3.3 Evaluasi Sumber Daya Manusia

Selain fokus pada keamanan website, penelitian ini juga mengevaluasi kinerja SDM IT yang bertanggung jawab terhadap pengelolaan keamanan website tersebut. Evaluasi menunjukkan bahwa SDM IT Dinas Komunikasi dan Informatika Kabupaten Raja Ampat masih menghadapi beberapa tantangan. Kurangnya pemahaman terhadap praktik terbaik dalam keamanan siber, keterbatasan keterampilan teknis, dan kurangnya pengalaman dalam menghadapi tantangan keamanan informasi kompleks menjadi beberapa masalah yang diidentifikasi.

Untuk mengatasi hal ini, sejumlah rekomendasi perbaikan diajukan. Pertama, penyelenggaraan pelatihan rutin tentang keamanan siber dan manajemen risiko bagi SDM IT akan membantu meningkatkan pemahaman mereka terhadap ancaman keamanan siber yang ada dan cara mengatasi risiko tersebut. Kedua, penguatan pengawasan dan evaluasi kinerja secara berkala diharapkan dapat memastikan bahwa SDM IT terus mengembangkan keterampilan dan pengetahuan mereka sesuai dengan perkembangan teknologi informasi dan keamanan siber yang terbaru. Ketiga, pembentukan tim keamanan siber internal yang responsif dan efektif untuk mengawasi serta menanggapi ancaman keamanan informasi dengan cepat.

Dengan menerapkan rekomendasi ini, diharapkan kinerja SDM IT Dinas Komunikasi dan Informatika Kabupaten Raja Ampat dapat meningkat, sehingga mereka dapat lebih efektif dalam mengelola dan menjaga keamanan website pemerintah. Ini tidak hanya akan memastikan keberlanjutan layanan yang aman dan terpercaya kepada masyarakat, tetapi juga mendukung perbaikan dalam pengelolaan keamanan informasi secara menyeluruh.

3.4 Diskusi Temuan Utama Penelitian

Kinerja Sumber Daya Manusia IT di Dinas Komunikasi dan Informatika Kabupaten Raja Ampat: Penelitian ini menyoroti bahwa kinerja SDM IT dipengaruhi oleh pengetahuan, keterampilan, dan sikap individu terhadap teknologi informasi. Sejumlah penelitian terdahulu seperti yang dilakukan oleh Sedarmayan (2017) juga menekankan pentingnya aspek-aspek ini dalam meningkatkan kualitas kinerja. Namun, hasil wawancara menunjukkan bahwa pemahaman tentang teknologi terbaru seperti kecerdasan buatan (AI) dan cloud computing masih perlu ditingkatkan di Dinas ini, sejalan dengan temuan dari penelitian-penelitian sebelumnya yang mengidentifikasi kebutuhan akan pengembangan keterampilan teknis yang lebih mendalam.

Keamanan Website: Penelitian ini menggunakan OWASP ZAP untuk mengidentifikasi kerentanan keamanan pada website pemerintah. Temuan kerentanan dari penelitian ini, sebanyak 19 kerentanan dengan tingkat risiko bervariasi, menunjukkan kesamaan dengan hasil penelitian terdahulu oleh Darojat et al. (2022), yang menggunakan metode serupa pada situs e-government. Meskipun perbedaan alat dan teknik pemindaian bisa terjadi, fokus pada identifikasi dan mitigasi risiko keamanan menjadi konsisten dalam literatur yang ada.

Evaluasi Sumber Daya Manusia: Evaluasi kinerja SDM IT dalam mengelola keamanan website menemukan tantangan terkait pemahaman praktik terbaik dalam keamanan siber. Hal ini konsisten dengan penelitian sebelumnya seperti yang dilakukan oleh Ningsih (2021), yang menunjukkan bahwa kurangnya pemahaman teknis dan pengalaman dalam menghadapi tantangan keamanan informasi kompleks adalah masalah umum di berbagai konteks pemerintahan daerah. Rekomendasi untuk pelatihan rutin dan pembentukan tim keamanan siber juga sering kali disoroti dalam penelitian lainnya untuk meningkatkan kualitas kinerja SDM IT.

Rekomendasi dan Upaya Meningkatkan Kinerja: Upaya untuk meningkatkan kualitas layanan dan keamanan website melalui audit berkala, pengembangan kebijakan keamanan, dan pelatihan SDM IT merupakan langkah-langkah yang sering kali direkomendasikan dalam literatur, termasuk dalam penelitian ini. Keseluruhan, temuan ini sejalan dengan fokus umum dalam penelitian-penelitian sebelumnya untuk memperkuat kapasitas organisasi dalam menghadapi ancaman keamanan siber yang semakin kompleks dan memastikan layanan yang lebih aman dan dapat diandalkan bagi masyarakat.

3.5 Diskusi Temuan Menarik

Berdasarkan hasil penelitian yang dilakukan, terdapat beberapa temuan menarik yang dapat menjadi fokus diskusi. Pertama, dari segi kinerja sumber daya manusia di Dinas Komunikasi dan Informatika Kabupaten Raja Ampat, terlihat bahwa pengetahuan dan keterampilan teknis yang dimiliki oleh karyawan dalam mengelola teknologi informasi terbilang cukup baik. Namun, masih ada kebutuhan untuk meningkatkan pemahaman dalam pengembangan aplikasi, analisis data, serta teknologi terbaru seperti kecerdasan buatan dan komputasi awan. Hal ini menunjukkan bahwa sementara karyawan memiliki dasar yang kuat, upaya untuk terus mengembangkan keterampilan mereka dalam menghadapi teknologi yang semakin kompleks tetap diperlukan.

Kedua, dalam evaluasi keamanan website, hasil analisis menggunakan metode Vulnerability Assessment menunjukkan bahwa terdapat 19 kerentanan keamanan yang berhasil diidentifikasi, mulai

dari tingkat rendah hingga tinggi. Ini mencakup masalah seperti ketidakhadiran Anti-CSRF Tokens, ketidaksetelan Content Security Policy (CSP) Header, dan potensi kebocoran informasi sensitif melalui Big Redirect Detected. Rekomendasi perbaikan seperti pembaruan perangkat lunak, konfigurasi ulang server, dan penerapan kontrol keamanan menjadi krusial untuk meningkatkan keamanan website pemerintah Kabupaten Raja Ampat. Temuan ini menunjukkan perlunya perhatian lebih dalam menerapkan kebijakan keamanan informasi yang efektif guna melindungi data sensitif dan menjaga kepercayaan publik terhadap layanan pemerintah.

Ketiga, dari segi evaluasi kinerja sumber daya manusia IT yang terlibat dalam pengelolaan keamanan website, terlihat bahwa SDM IT Dinas Komunikasi dan Informatika Kabupaten Raja Ampat masih menghadapi beberapa tantangan. Kurangnya pemahaman terhadap praktik terbaik dalam keamanan siber, keterbatasan keterampilan teknis, dan pengalaman dalam menghadapi tantangan keamanan informasi kompleks menjadi isu utama yang dihadapi. Rekomendasi untuk meningkatkan pelatihan, pengawasan, dan pembentukan tim keamanan siber internal yang responsif diharapkan dapat memperkuat kemampuan mereka dalam menghadapi ancaman keamanan yang semakin canggih dan meningkatkan keberlanjutan layanan yang aman kepada masyarakat.

IV. KESIMPULAN

Kesimpulan dari hasil penelitian dan analisis terhadap keamanan website Pemerintah Kabupaten Raja Ampat menunjukkan adanya 19 kerentanan yang dapat berpotensi mempengaruhi keamanan data yang tersimpan di dalamnya. Dari hasil evaluasi, teridentifikasi berbagai jenis kerentanan seperti PII Disclosure, absennya Anti-CSRF Tokens, dan masalah pada pengaturan Content Security Policy (CSP) Header. Meskipun tergolong medium risk, dengan 15,8% medium risk dan 42,1% low risk, perlunya langkah-langkah perbaikan yang tepat menjadi penting untuk memastikan keamanan informasi yang lebih baik di masa depan.

Dinas Komunikasi dan Informatika Kabupaten Raja Ampat telah menunjukkan komitmen yang kuat dalam menghadapi tantangan keamanan ini dengan melakukan pemetaan risiko yang komprehensif, menetapkan sasaran keamanan yang jelas, dan melaksanakan tindakan teknologi yang tepat. Langkah-langkah ini juga didukung oleh upaya pelatihan dan peningkatan keterampilan bagi SDM IT, menunjukkan bahwa investasi dalam pengembangan sumber daya manusia merupakan strategi penting untuk meningkatkan kualitas layanan dan keamanan informasi secara berkelanjutan.

Keterbatasan Penelitian. Penelitian ini terbatas dengan waktusehingga beberapa kegiatan tidak dapat diobservasi secara optimal sebab penjadwalan yang dilaksanakan diluar waktu penelitian.

Arah Masa Depan Penelitian (*future work*). Untuk arah masa depan penelitian terkait keamanan website Pemerintah Kabupaten Raja Ampat, penting untuk mengeksplorasi solusi-solusi inovatif dalam mengatasi kerentanan yang telah diidentifikasi. Langkah-langkah perbaikan yang lebih lanjut dapat difokuskan pada penerapan teknologi keamanan terbaru seperti pembaruan kebijakan keamanan konten (CSP), penguatan pengaturan Strict-Transport-Security (HSTS), dan implementasi

perlindungan terhadap serangan XSS (Cross-Site Scripting). Selain itu, penelitian dapat diperluas untuk mengukur dampak dari perbaikan keamanan ini terhadap kinerja dan keandalan website, serta efektivitas pelatihan yang diberikan kepada SDM IT dalam mengelola keamanan informasi secara efisien. Dengan demikian, upaya-upaya ini diharapkan dapat meningkatkan tingkat keamanan secara menyeluruh dan memperkuat posisi Pemerintah Kabupaten Raja Ampat dalam memanfaatkan teknologi untuk memberikan pelayanan publik yang lebih aman dan andal.

V. UCAPAN TERIMA KASIH

Terima kasih atas kesempatan yang diberikan untuk terlibat dalam penelitian ini. Saya ingin menyampaikan penghargaan yang tulus kepada semua pihak yang telah memberikan dukungan, bantuan, dan wawasan selama proses penelitian. Tanpa kerjasama dan kontribusi dari berbagai pihak, penelitian ini tidak akan terwujud dengan baik. Semoga hasil penelitian ini dapat memberikan manfaat dan kontribusi positif bagi pengembangan kebijakan dan penataan tenaga kerja di masa mendatang. Terima kasih atas waktu, dukungan, dan kerja sama yang telah diberikan. Semoga kita dapat terus berkolaborasi untuk mencapai tujuan yang lebih baik.

VI. DAFTAR PUSTAKA

Akmal1, A. M., Heryana2, N., & Arip Solehudin3. (2022). Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment. *Jurnal Pendidikan Dan Konseling*, *4*(4). https://doi.org/10.31004/jpdk.v4i4.6495

Aryanti, D., Nurholis, & Nashar Utamajaya, J. (2021). ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA. *Jurnal Syntax Fusion*, *1*(03). https://doi.org/10.54543/fusion.v1i03.53

Ayu Setia, H., Safitri, E. M., Verina Renata Putri, & Wibowo, C. P. (2023). ANALISIS KEAMANAN WEBSITE DINAS PERHUBUNGAN PROVINSI JAWA TIMUR MENGGUNAKAN METODE OCTAVE ALLEGRO DAN FMEA. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *3*(1). https://doi.org/10.33005/sitasi.v3i1.554

Bimandaru, A., Alamsyah, A., & Nugroho, A. (2023). ANALISIS PENGUJIAN PENETRASI PADA LAYANAN HOSTING MENGGUNAKAN METODE BLACK BOX (Studi kasus : Blogspot, Wordpress dan Shared Hosting). *Foristek*, *14*(1). https://doi.org/10.54757/fs.v14i1.238

Carkiman, C., Rikmansyah, S., Mahardi, S., & Kuncoro, M. A. (2021). PENGUJIAN PERFORMA DAN TINGKAT STRESS PADA WEBSITE RESMI PEMERINTAH (STUDI KASUS: KAB.SUBANG, KAB.BANDUNG BARAT, DAN KAB.CIANJUR). *Journal of Information System, Applied, Management, Accounting and Research*, *5*(1). https://doi.org/10.52362/jisamar.v5i1.350

Darojat, E. Z., Sediyono, E., & Sembiring, I. (2022). Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner. *JURNAL SISTEM INFORMASI BISNIS*, *12*(1). https://doi.org/10.21456/vol12iss1pp36-44

Dr.Sudaryono. (2018). Metode Penelitian Kuantitatif, Kualitatif, dan Mix Methode. *Depok: PT RajaGrafindo Persada,*.

Firda, Putri, S., Utomo, Y. B., & Kurniadi, H. (2023). Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux. *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)*, *7*(1). https://doi.org/10.29407/inotek.v7i1.3411

Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. *Creative Information Technology Journal*, *4*(4). https://doi.org/10.24076/citec.2017v4i4.119

Murdiyanto, E. (2020). Metode Penelitian Kualitatif (Sistematika Penelitian Kualitatif). In *Yogyakarta Press*.

Ningsih, S. W. (2021). Analisis Pengujian Kerentanan Situs Pemerintahan XYZ dengan PTES. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(3). https://doi.org/10.35957/jatisi.v8i3.1224

Ningsih, S. W., Almaarif, A., & Widjadjarto, A. (2021). Vulnerability Testing Analysis of XYZ Regional Government Site Using PTES. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(3). https://doi.org/10.35957/jatisi.v8i3.1224

Sari sasi gendro, dea aulya. (2022). Buku Metode Penelitian Kualitatif & Kuantitatif. In *LP2M UST Jogja* (Issue March).

Sugiyono. (2013). Metode Penelitian Kombinasi (Mix Methoders). *Alfabeta*, *28*(1).

Sujarwoto. (2023). Analisis dan Interpretasi Data Kuantitatif dalam Riset Administrasi Publik. *Pustaka. Ut*.