Terbit *online* pada laman web jurnal : http://journal.unbara.ac.id/index.php/INTECH

INFORMATIKA DAN TEKNOLOGI (INTECH)

ISSN (Online) : 2722-7367

SYSTEMATIC LITERATURE REVIEW: PERMASALAHAN *RANSOMWARE* PADA APLIKASI BERBASIS *CLOUD*

Zidnii Ilma Rimbarawa [1], Elis Kholisoh [2] , Zahwa Putri Rahmayani [3]

[1]Universitas Negeri Jakarta, Jl. R.Mangun Muka Raya No.11, RW.14, Rawamangun, Kec. Pulo Gadung, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta 13220, Indonesia

[1]zidnii.rimbarawa@gmail.com, [2]semangatelis@gmail.com, [3]zahwaputrir@gmail.com

INFORMASI ARTIKEL

Diterima Redaksi: 20 Agustus 2021

Revisi Akhir: 30 Oktober 2021

Diterbitkan *Online*: 30 November 2021

KATA KUNCI

Ransomware, Cloud Application, Database, Systematic Literature Review

ABSTRACT

Ransomware has created questions on the security aspects of a cloud architcture, especially with cloud services being adopted by more enterprises. Ransomware encrypts data and makes it inaccessible. Victims are given instructions to pay the attacker a fee in exchange for having their data accessible again. Ransomware has organizations and is increasingly targeting applications running on databases. To prevent this problem, this study uses the Systematic Literature Review method to provide information about ransomware problems in cloud-based applications, as well as ransomware prevention in cloud-based applications and its challenges including the differences in effectiveness for each type of ransomware and the strategies that do not apply to server-side attacks. The research review shows that backup and recovery is a key defense strategy against ransomware. Ransomware protection, applications, and databases require the right strategy, including reliable recovery. This research is useful to ensure that the cloud-based is protected from ransomware attacks.

1. PENDAHULUAN

Ransomware merupakan salah satu bentuk *malware* yang mencegah akses ke perangkat yang bertujuan untuk menuntut uang tebusan untuk data yang telah dicuri atau dibatasi (enkripsi). *Ransomware* oleh *cyber criminal* menjadi semakin populer selama beberapa tahun terakhir dalam memonetisasi aktivitas *malicious* dengan perkiraan kerusakan total lebih dari 5 miliar USD pada tahun 2017 dan diperkirakan mencapai 11,5 miliar pada tahun 2019 [1][2]. *Ransomware* telah memakan banyak korban yang meluas hingga sektor kesehatan. Pada tahun 2017, *ransomware* Wannacry menyerang dan memutuskan akses beberapa *database* pasien pada computer di Rumah Sakit Dharmais dan Rumah Sakit Harapan Kita di Jakarta. Hal ini membuat rumah sakit terpaksa membayar uang tebusan kepada penyerang [3]. Pengembang *ransomware* telah memperluas domainnya, *ransomware* umumnya ditemukan di komputer pribadi, sementara pada tahun 2017 terjadi peningkatan serangan *ransomware* yang ditujukan untuk *database* [1]. Tulisan ini bertujuan untuk melakukan studi literatur terhadap masalah *ransomware* pada aplikasi berbasis *cloud*, serta melakukan penelitian terhadap pencegahan *ransomware* pada aplikasi berbasis *cloud* dan tantangannya.

2. TINJAUAN PUSTAKA

Systematic Literature Review merupakan istilah yang digunakan pada metodologi penelitian untuk mengumpulkan serta mengevaluasi penelitian yang terkait pada topik tertentu [4]. SLR menjadi metode standar untuk mendapatkan jawaban dengan melakukan tinjauan pustaka berdasarkan studi terkait sebelumnya. SLR dilakukan untuk berbagai tujuan, di antaranya untuk merangkum penelitian sebelumnya, mengidentifikasi informasi yang berguna pada penelitian yang tersedia dalam bidang topik, mengkaji pertanyaan penelitian yang relevan, dan menghasilkan laporan penelitian yang koheren [5]. SLR juga sering dibutuhkan untuk penentuan agenda riset serta bagian dari disertasi atau tesis [6]. Dalam melakukan kajian, pemahaman suatu penelitian secara komprehensif merupakan salah satu syarat yang harus dipenuhi oleh peneliti. SLR merupakan metode yang berkaitan dengan pertanyaan yang harus dijawab oleh peneliti. Hal tersebut dilakukan secara realistis dengan mengidentifikasi, menyeleksi, dan menilai literatur penelitian yang relevan [7].

Ransomware mengunci sistem atau data dan mencegah korban untuk mengaksesnya kecuali sampai tebusan dibayarkan kepada penyerang. Penggunaan internet yang meluas memberikan platform untuk pertumbuhan *ransomware*. Keberadaan layanan *cloud*, *big data*, dan internet membuat studi tentang serangan *ransomware* diperlukan [8]. *Cloud computing* didefinisikan sebagai kumpulan sumber daya teknologi informasi yang menyediakan sumber daya di antara banyak pengguna, tersedia melalui internet, dan disediakan oleh layanan perusahaan [9]. Dalam hal ancaman terhadap *cloud*, salah satu ancaman utama adalah pembajakan akun menggunakan curian kredensial yang dapat digunakan oleh penyerang untuk mengakses, menumbangkan, memanipulasi, dan menghapus informasi atau data sensitif dari akun [10]. Analisa terhadap kesesuaian judul dan abstrak dengan kata kunci dan domain terkait teknologi informasi dilakukan untuk mencapai hasil. Kesimpulan ditarik berdasarkan tulisan yang ditelaah dari penelitian dan tulisan yang ada.

3. METODE PENELITIAN

Tahapan dari *Systematic Literature Review* (SLR) pada penelitian ini mengacu pada penelitian yang dilakukan oleh Entot Suhartono (2017)[11], yaitu:

3.1 *3.1. Perumusan Masalah*

Untuk mencapai tujuan penelitian, terdapat 3 rumusan masalah. Rumusan masalah membantu untuk mengumpulkan informasi yang dibutuhkan. Studi tentang serangan *ransomware* diperlukan untuk memberikan solusi bagi pengguna komputer, pelayanan *cloud*, dan internet untuk melindungi data mereka dari *cyber criminal*.
Berikut adalah pertanyaan-pertanyaan yang dapat membantu memecahkan masalah:

1. Bagaimana *ransomware* menjadi masalah untuk aplikasi berbasis *cloud*?
2. Bagimana pencegahan *ransomware* pada aplikasi berbasis *cloud*?
3. Apa tantangan dalam pencegahan *ransomware* pada aplikasi berbasis *cloud*?

3.2 *3.2. Pengumpulan Data*

Data collection adalah tahap di mana data-data untuk penelitian dikumpulkan [6]. Tujuan studi literatur pada penelitian ini adalah untuk memahami topik riset *ransomware* pada aplikasi berbasis *cloud*. Penelitian yang akan diteliti diambil dari beberapa literatur yang diterbitkan di Google Scholar, IEEE, SpringerLink, ResearchGate, dan IECE dari tahun 2015 sampai tahun 2021 berjenis jurnal atau konferensi. Literatur yang dicari berbahasa Indonesia dan bahasa Inggris. Kata kunci yang digunakan adalah "*cloud ransomware*", "*cloud application*", "*database ransomware*", dan "*cloud vulnerability*".

3.3 *3.2. Analisa dan Evaluasi Data*

Dari prosedur di atas, artikel yang ditemukan berjumlah 13. Dari jumlah tersebut, 4 mengatasi masalah *ransomware* pada aplikasi berbasis *cloud*, 2 mengatasi pencegahan *ransomware* pada aplikasi berbasis *cloud*, dan 2 mengatasi tantangan dalam pencegahan *ransomware* pada aplikasi berbasis *cloud*. Artikel yang tersisa dikeluarkan dari tinjauan ini karena tidak dapat digunakan untuk memenuhi tiga pertanyaan penelitian. Berikut adalah kutipan pembatasan sumber referensi pertanyaan penelitian:

Fokus	Media Pencari	Sumber
Masalah *Ransomware* Pada Aplikasi Berbasis *Cloud*	Google Scholar, IEICE, ResearchGate, IEEE	(Yun, Hur, Shin, & Koo, 2017); (Iffländer, et al., 2019); (Hagen, Dmitrienko, Iffländer, Jobst, & Samuel, 2018); (Bhattacharya & Kumar, 2017)
Pencegahan *Ransomware* Pada Aplikasi Berbasis *Cloud*	IECE, IEEE	(Yun, Hur, Shin, & Koo, 2017); (Bhattacharya & Kumar, 2017)
Tantangan pencegahan *Ransomware* Pada Aplikasi Berbasis *Cloud*	SpringerLink, IEEE	(Lee, Moon, & Park, 2017); (Hagen, Dmitrienko, Iffländer, Jobst, & Samuel, 2018)

4. HASIL DAN PEMBAHASAN

Berdasarkan tinjauan literatur, maka hasil yang diperoleh untuk menjawab tiga pertanyaan penelitian akan dibahas pada di bagian ini.

4.1 4.1. Masalah *Ransomware* pada Aplikasi Berbasis *Cloud*

Ransomware telah menjadi populer di kalangan *cyber criminal*. *Ransomware* adalah jenis *malware* yang mengunci komputer hingga pemilik melakukan pembayaran untuk mendapatkan kembali akses ke komputer. Ancaman *ransomware* baru dianggap sebagai tren *malware* yang paling terkenal setelah serangan ditargetkan pada tahun 2013. *Ransomware* Cryptolocker sendiri menginfeksi sekitar 250.000 komputer secara global dalam 100 hari pertama [12]. Meskipun awalnya menargetkan platform PC (klien), *ransomware* baru-baru ini membuat lompatan ke *database* sisi server. Dimulai pada bulan Januari 2017 dengan serangan puluhan ribu server MongoDB yang disebut MongoDB Apocalypse, diikuti oleh gelombang kedua yang menargetkan sever MySQL, dan serangan lainnya yang menargetkan berbagai jenis DB seperti ElasticSearch, Cassandra, Hadoop, dan CouchDB [2][1].

Cloud computing yang muncul sebagai kemajuan teknologi terbaru membawa berbagai ancaman keamanan data di *cloud*. Terlebih beberapa perusahaan keamanan IT terkenal menyebut tahun 2016 sebagai "Tahun *ransomware*". Ancaman terhadap *cloud* meningkatkan pertanyaan tentang aspek penting keamanan penting pada *cloud,* terutama dengan banyaknya perusahaan yang mengadopsi jasa *cloud*. Hingga akhir 2016, sejumlah ancaman terhadap *cloud* keamanan telah diidentifikasi secara luas yaitu, pembajakan data, kerentanan *backup*, pelanggaran integritas keamanan data, dan masalah keamanan jaringan yang merupakan pilar dasar arsitektur *cloud* [10].

4.2 4.2. Pencegahan *Ransomware* pada Aplikasi Berbasis *Cloud*

Jika komputer terinfeksi *ransomware* seperti CryptoLocker, *file* di penyimpanan lokal akan ditahan dengan *ransom* atau tebusan dan salinan di penyimpanan *cloud* akan ditimpa ketika komputer disinkronkan dengan sistem penyimpanan *cloud* [12]. Langkah terbaik untuk meningkatkan sistem pertahanan terhadap *ransomware* adalah untuk membuat dan melindungi sistem *backup* karena *ransomware* mengenkripsi *file* dan merusak sistem *backup*. Enkripsi dan penghapusan file *backup* akan menjadi proses yang memakan waktu untuk serangan *ransomware* dalam jumlah besar. Deteksi dari awal dapat mencegah kerusakan seluruh sistem [13]. Deteksi dapat mencakup IDS dengan tanda tangan terbaru, filter email yang dapat mendeteksi dan menyaring berbahaya dan email phishing. *Ransomware* biasanya dijalankan dari dua lokasi, yaitu *folder* %appdata% dan %temp%. Memeriksa lokasi ini adalah salah satu cara untuk mendeteksi eksekusi *ransomware* sebelum enkripsi dimulai. Jika *ransomware* terdeteksi, aktivitas jaringan harus dinonaktifkan sehingga file dalam jaringan tidak dapat dienkripsi. Tindakan setelah deteksi dan penahanan adalah mengganti sistem. Mengganti sistem lebih disarankan daripada membersihkan sistem karena deteksi apakah ada file sisa tersembunyi yang dapat menginfeksi kembali sangat sulit. Untuk mencapai pemulihan efisien, *backup* harus memiliki versi diaktifkan sehingga *backup* yang berfungsi dengan baik dapat dipulihkan. Penyelidikan forensik penuh untuk *phishing mail*, *web* berbahaya, tautan berbahaya atau *web* berbasis toolkit dapat membantu mengembangkan mekanisme deteksi dan pencegahan yang lebih baik untuk serangan pada sistem *cloud* di masa depan[10].

4.3 4.3. Tantangan Pencegahan *Ransomware* pada Aplikasi Berbasis *Cloud*

Metode pencegahan, salinan *backup*, file halaman web, pemeriksaan keamanan situs, dan berbagi manajemen folder berbeda dalam keefektifannya untuk setiap jenis serangan *ransomware*. Pencegahan terhadap *ransomware* akan sulit kecuali salinan *backup* dari fitur perlindungan sistem di CryptoLocker dihapus sebelum operasi kemudian dipisahkan secara fisik [14]. Selain kemajuan dalam keamanan sistem, beberapa strategi untuk mendeteksi *ransomware* ada, tetapi tidak berlaku untuk serangan sisi server. Sebagian besar perangkat lunak komersial anti-*malware* menggunakan deteksi berbasis tanda tangan dari biner berbahaya. Namun, pendekatan ini tidak efektif terhadap *ransomware* yang menargetkan *database* karena penyerang terhubung ke *database* dari jarak jauh dan mengeksekusi kueri berbahaya untuk menghapus tabel *database* dan menyisipkan pesan *ransom*[1].

5. KESIMPULAN DAN SARAN

Mengingat ancaman *ransomware* yang berkembang pesat, mengikuti praktik keamanan merupakan garis pertahanan pertama yang penting dalam memerangi *ransomware*. *Backup* merupakan bagian penting dari infrastruktur keamanan. *Backup* dan pemulihan yang baik memungkinkan pemulihan sebagian atau seluruh database dari titik waktu tertentu. Tim infrastruktur organisasi juga harus mengubah pengaturan *default* yang dapat membuat *database* rentan terhadap serangan dan memastikan bahwa otentikasi dan kontrol akses dikelola sejalan dengan kebijakan perusahaan. Penelitian ini menyarankan penggunaan *backup* sebagai pertahanan untuk desktop, laptop, dan *file* yang sangat rentan terhadap *ransomware.* Hal yang sama pada *database*, terutama karena penyerang mulai menargetkan *database*. Pengubahan pengaturan *default* yang dapat membuat *database* rentan terhadap serangan, serta pemastian otentikasi dan kontrol akses dikelola dengan baik penting dalam pertahanan terhadap *ransomware*.

6. DAFTAR PUSTAKA

[1] C. Hagen, A. Dmitrienko, L. Iffländer, M. Jobst, and S. Kounev, "Efficient and effective ransomware detection in databases," *Annu. Comput. Secur. Appl. Conf.(ACSAC)*, no. April 2019, 2018.

[2] L. Iffländer, A. Dmitrienko, C. Hagen, M. Jobst, and S. Kounev, "Hands Off my Database: Ransomware Detection in Databases through Dynamic Analysis of Query Sequences," 2019.

[3] F. Kwarto and M. Angsito, "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan," *J. Akunt. Bisnis*, vol. 11, no. 2, pp. 99–110, 2018.

[4] I. Dan, T. Intech, I. Sulistiani, E. Mufida, P. M. Yasser, and L. Alamsyah, "Systematic Literature Review : Bankruptcy Prediction Menggunakan Teknik Machine Learning dan Deep Learning," vol. 2, no. 1, pp. 13–18, 2021.

[5] F. Rozi, "Systematic Literature Review pada Analisis Prediktif dengan IoT: Tren Riset, Metode, dan Arsitektur," *J. Sist. Cerdas*, vol. 3, no. 1, pp. 43–53, 2020.

[6] E. Triandini, S. Jayanatha, A. Indrawan, G. Werla Putra, and B. Iswara, "Metode Systematic Literature Review untuk Identifikasi Platform dan Metode Pengembangan Sistem Informasi di Indonesia," *Indones. J. Inf. Syst.*, vol. 1, no. 2, p. 63, 2019.

[7] I. Larasati, A. N. Yusril, and P. Al Zukri, "Systematic Literature Review Analisis Metode Agile Dalam Pengembangan Aplikasi Mobile," *Sistemasi*, vol. 10, no. 2, p. 369, 2021.

[8] R. S. Sajjan and V. R. Ghorpade, "Ransomware attacks: Radical menace for cloud computing," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018-January, no. May 2005, pp. 1640–1646, 2018.

[9] A. Murray, G. Begna, E. Nwafor, J. Blackstone, and W. Patterson, "Cloud Service Security & application vulnerability," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2015-June, no. June, 2015.

[10] S. Bhattacharya and C. R. S. Kumar, "Ransomware: The CryptoVirus subverting cloud security," *2017 Int. Conf. Algorithms, Methodol. Model. Appl. Emerg. Technol. ICAMMAET 2017*, vol. 2017-January, pp. 1–6, 2017.

[11] E. Suhartono, "Systematic Literatur Review (SLR): Metode , Manfaat , Dan Tantangan Learning Analytics Dengan Metode Data Mining di Dunia Pendidikan Tinggi," *J. Ilm. INFOKAM*, vol. 13, no. 1, pp. 73–86, 2017.

[12] J. Yun, J. Hur, Y. Shin, and D. Koo, "CLDSafe: An efficient file backup system in cloud storage against ransomware," *IEICE Trans. Inf. Syst.*, vol. E100D, no. 9, pp. 2228–2231, 2017.

[13] A. Rahman and A. Qosim, "SISTEM CERDAS PENGELOMPOKAN MAHASISWA BERDASARKAN PREDIKSI PERFORMA BELAJAR DENGAN METODE CASE BASED REASONING," *J. Edik Inform. J. Edik Inform.*, vol. 8, no. 1, pp. 13–25, 2021.

[14] J. K. Lee, S. Y. Moon, and J. H. Park, "CloudRPS: a cloud analysis based enhanced ransomware prevention system," *J. Supercomput.*, vol. 73, no. 7, pp. 3065–3084, 2017.