BAB V
PENUTUP

5,1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan hal-hal sebagai berikut:

Rancangan ini telah berhasil diimplementasikan dengan baik, bahwa berbagai alat dan teknologi yang digunakan dapat memastikan keamanan data dan mendeteksi ancaman dalam dunia *virtual* dan komputasi *cloud*.

Berbagai alat dan teknologi teknologi digunakan dalam perancangan ini untuk memastikan keamanan data dan mendeteksi ancaman dalam dunia *virtual* dan *cloud computing*. Pengguna dapan menjalankan berbagai sistem operasi secara bersamaan dengan *VMWare,* yang membantu untuk mengelola dan memantau berbagai aplikasi sistem.

1. Penguatan Keamanan Berkelanjutan: Tokopedia diharuskan untuk terus memperkuat infrastruktur keamanan mereka dengan mengadopsi teknologi-teknologi canggih seperti *IBM QRADAR SIEM* dan melakukan audit keamanan secara teratur
2. Penggunaan *VMWare* mempermudah pengelolaan para pengguna untuk menjalankan beberapa sistem, dan memungkinkan pengguna menjalankan beberapa sistem operasi secara bersamaan. Pengaturan memori untuk mengakses *IBM Qradar* berjalan dengan lancar dan efektif.
3. Perusahaan perlu terus meningkatkan kapasitas dan Rancangan ini berhasil menunjukan bahwa berbagai langkah dan teknologi dapat diterapkan untuk meningkatkan keamanan sistem dan mendeteksi ancaman. *Implementasi* yang berhasil ini menunjukan bahwa dengan alat dan teknik yang tepat, keamanan data dapat dijaga dengan baik.

PERPUSTAKAAN POLITEKNIK 'AISYIYAH PONTIANAK

5.2 Saran

Berikut adalah beberapa saran berdasarkan hasil penelitian ini, yang dapat memberikan implikasi bagi pengembangan ilmu pengetahuan dan penggunaan praktis di masa mendatang:

1. Meningkatkan Infrastruktur Keamanan:

a) Implementasi Teknologi *SIEM*: Tokopedia harus mempertimbangkan implementasi teknologi SIEM (*Security Information and Event Management*) seperti *IBM QRadar* untuk meningkatkan deteksi dan respons terhadap ancaman. *Qradar SIEM* dapat membantu dalam memonitor lalu lintas jaringan, mendeteksi *anomali*, dan memberikan *visibilitas* yang lebih baik tentang aktivitas jaringan.

b) Pembaruan Perangkat Lunak Berkala: Tokopedia harus memastikan semua perangkat lunak dan sistem mereka selalu diperbarui dengan patch keamanan terbaru untuk mengurangi risiko kerentanan yang dapat dieksploitasi oleh peretas.

2. Penelitian Lanjutan: Penelitian lanjutan memiliki kemampuan untuk mengeksplorasi lebih dalam penyebab kebocoran data, termasuk analisis lebih mendalam tentang teknologi keamanan yang dapat diterapkan untuk mengurangi ancaman terhadap keamanan digital.

PERPUSTAKAAN 1052A200001
POLITEKNIK 'AISYIYAH PONTIANAK

DAFTAR PUSTAKA

Chandra, K.D. (2019) 'Penerapan Business Continuity pada Bank Central Asia', *Bina Ekonomi: Majalah Ilmiah Fakultas Ekonomi Universitas Katolik Parahyangan,* 21(1), pp. 13–24.

Makarim, E. (2022) 'Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi', Fakultas Hukum Universitas Indonesia [Preprint]. Available at: https://law.ui.ac.id/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-oleh-edmon-makarim/.

Muhammad Fathur (2020) 'Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen (Tokopedia's Responsibility for the Leakage of Consumers Personal Data)', *Proceeding: Call for Paper 2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*, p. hlm. 43. Available at: http://jurnal.unissula.ac.id/index.php/PH/article/view/1476.

Roan, R.B. (2017, Agustus 17). 'Apa yang Dimaksud dengan Teori Manajemen Privasi Komunikasi (Communication Privacy Management - CPM)', *dictio*. Available at: https://www.dictio.id/t/apa-yang-dimaksud-dengan-teori-manajemen-privasi-komunikasi-communication-privacy-management-cpm/9011.

CNBC Indonesia (2020) 'Bocornya 91 Juta Data Akun Pengguna Tokopedia'. Available at: https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia.

IBM X-Force Exchange (n.d.) 'SSH Brute Force Attack'. Available at: https://exchange.xforce.ibmcloud.com/collection/SSH-Brute-Force-Honeypot-Live-56b3f3072e05dab76987bfcd3ba18fea.

IBM X-Force Exchange (n.d.) 'Telnet Brute Force'. Available at: https://exchange.xforce.ibmcloud.com/collection/Telnet-Brute-Force-e33ea5dd86257fdde0bfedffe3569604.

POLITEKNIK NEGERI PONTIANAK