

BAB V

PENUTUP

5.1 Kesimpulan

Pada sistem keamanan jaringan ini menggunakan firewall Next Generation, karena firewall jenis ini lebih mumpuni dibandingkan dengan firewall lainnya serta mempunyai banyak fitur serta fungsi tambahan. *Firewall Next Generation* ini sendiri merupakan perangkat keamanan jaringan yang memantau lalu lintas jaringan masuk dari publik ke pribadi dan jaringan keluar dari pribadi ke publik dan memutuskan akan mengizinkan atau memblokir lalu lintas tertentu apakah sesuai dengan aturan keamanan yang ditentukan. Desain jaringan yang menggunakan *firewall* fisik Cisco yang terhubung dengan router serta router yang terhubung pada internet akan membantu menghalangi peretas atau sebagai tembok penghalang yang terpercaya. Dengan adanya *firewall NextGen* ini dapat membantu melindungi sistem jaringan pada sebuah perusahaan atau instansi sehingga tidak menyebabkan kebocoran data, tidak dapat diakses atau pemblokiran oleh *hacker* dan juga dapat menyebabkan kerugian besar pada sebuah perusahaan karena sistem jaringan suatu perusahaan merupakan suatu hal yang sangat penting.

Pada instansi yang kami tempati dalam pelaksanaan praktik kerja lapangan ini memiliki kelemahan pada sistem keamanan jaringan pada sistem monitoring keandalan pada Jembatan Suramadu, dikarenakan kami ingin mengetahui cara kerjanya terhadap Jembatan Suramadu. Kondisi demikian terbukti pada

pertengahan Bulan Juni 2021 sistem integrasi SMKS Suramadu mendapat serangan peretas melalui program ransomware. Serangan ransomware mengakibatkan seluruh file pada perangkat server terenkripsi dan tidak dapat diakses. Jika ingin membuka file yang telah dienkripsi maka harus dilakukan pembayaran sejumlah BitCoin ke rekening peretas. Oleh karena itu diperlukan perubahan sistem integrasi data untuk mengamankan sistem dari kejadian serupa.

Oleh karena *firewall NextGen* ini perlu diterapkan pada instansi tersebut agar sistem keamanan jaringannya lebih aman dan tidak ada lagi pembobolan yang menyebabkan kerugian besar pada instansi seperti kejadian sebelumnya. Hal ini tidak hanya diperlukan oleh instansi tersebut melainkan instansi atau perusahaan lainnya juga lebih baik memasang pengaman jaringan dengan *firewall NextGen* sebagai tameng utama dari sistem jaringan sebelum terjadi hal yang tidak diinginkan dan berdampak mengalami kerugian.

5.2 Saran

Sebaiknya sistem keamanan jaringan lebih diperhatikan lagi agar tidak terjadinya serangan oleh hacker seperti sebelumnya dengan memantau secara terus menerus dan mencatat kelemahan pada jaringan untuk kajian ulang dan peningkatan pada sistem keamanan jaringan. Karena pada saat ini jaringan merupakan hal penting dalam suatu perusahaan sehingga jika terjadi pembobolan maka data bisa saja bocor dan pekerjaan menjadi tertunda.

Kemudian juga diperlukan tenaga kerja yang dikhususkan untuk memantau keamanan jaringan pada instansi tersebut agar ada tindak lanjut jika terjadi

penyerangan. Karena jaringan ini harus dipantau oleh orang yang benar-benar memiliki keahlian pada bidang sistem keamanan jaringan dan bukan semua orang. Namun, keahlian saja tidak cukup melainkan juga perlu memilih orang yang jujur sehingga tidak ada kenakalan dalam pembocoran data perusahaan maupun data perseorangan.