TUGAS

KEAMANAN JARINGAN

“STANDAR-STANDAR MENDESAIN NOC & SOC”

Nama : Mega Putri Rahmawati Darta

Kelas : D4 LJ IT B

NRP : 3122640038

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Infrastruktur jaringan dan aset teknologi informasi lainnya saat ini sudah sangat penting bagi keberlangsungan operasional perusahaan. Dalam suatu bisnis atau lembaga, Network Operation Center (NOC, pusat operasi jaringan) dan Security Operation Center (SOC, pusat operasi keamanan) bertugas untuk memastikan jaringan dan aset IT lainnya berfungsi lancar tanpa halangan. NOC adalah suatu tempat pengelola jaringan yang berfungsi untuk mengawasi, memantau, dan memelihara jaringan komunikasi perusahaan. NOC bisa dikelola sendiri oleh perusahaan tersebut atau bisa diserahkan ke pihak ketiga. Sedangkan SOC secara singkat bisa didefinisikan sebagai pusat komando untuk tim profesional keamanan siber yang memantau, mendeteksi, dan membantu melindungi organisasi dari serangan siber. Bila kita lihat lebih lanjut, baik NOC maupun SOC memiliki banyak persamaan. NOC dan SOC bertugas memantau dan mengawasi lalu lintas jaringan perusahaan. Keduanya juga bekerja untuk mengenali, memeriksa, dan membantu mengatasi masalah yang mungkin terjadi di jaringan dan aset IT. Perbedaan Network Operation Center dan Security Operation Center NOC (Network Operation Center) pada umumnya memiliki kewajiban mengoperasikan dan memelihara infrastruktur jaringan. NOC akan mengambil tindakan bila terjadi insiden yang mengganggu performa jaringan. Idealnya, NOC akan memastikan bahwa jaringan komunikasi tetap bisa berjalan setiap saat. Sementara itu seperti namanya, SOC lebih berorientasi terhadap insiden keamanan. Fokusnya adalah untuk dapat memberikan tanggapan cepat suatu ancaman siber. Deteksi dini suatu insiden akan memungkinkan tim keamanan siber untuk dapat segera mengambil tindakan yang diperlukan, baik untuk menangkal maupun memulihkan kerugian yang terjadi.

1.2 Rumusan Masalah

1. Apakah perbedaan dari NOC dan SOC?
2. Apakah manfaat dari NOC dan SOC dalam infrastruktur jaringan?
3. Bagaimana standar-standar dalam mendesain NOC dan SOC?

1.3 Tujuan

1. Untuk mengetahui perbedaan dari NOC dan SOC.
2. Untuk mengetahui bagaimana manfaat NOC dan SOC dalam infrastruktur jaringan.
3. Untuk mengetahui bagaimana standar-standar dalam mendesain NOC dan SOC.

BAB 2

PEMBAHASAN

2.1 Perbedaan NOC dan SOC

NOC dan SOC bekerja secara terintegrasi untuk memastikan jaringan yang aman, andal, dan terlindungi. Fokus utama NOC adalah menjaga ketersediaan, performa, dan keandalan jaringan. NOC bertanggung jawab untuk memantau dan mengelola infrastruktur jaringan, memecahkan masalah jaringan, merespons peristiwa jaringan, dan menjalankan tugas operasional sehari-hari terkait dengan jaringan. SOC adalah keamanan informasi dan deteksi ancaman. SOC bertanggung jawab untuk memantau keamanan sistem dan jaringan, mendeteksi serangan atau insiden keamanan, merespons dan mengatasi kejadian keamanan, serta menjalankan kegiatan analisis dan investigasi terkait kejadian keamanan.

Tujuan utama NOC adalah menjaga ketersediaan dan kinerja jaringan agar tetap optimal. NOC berfokus pada pengelolaan dan pemeliharaan infrastruktur jaringan, peningkatan kinerja, dan memastikan keseluruhan jaringan berfungsi dengan baik. Tujuan utama SOC adalah menjaga keamanan sistem dan data dari serangan atau ancaman. SOC berfokus pada pemantauan dan perlindungan terhadap serangan keamanan, deteksi dini terhadap aktivitas mencurigakan, dan menangani kejadian keamanan secara efektif untuk mencegah atau meminimalkan dampaknya.

Tanggung jawab NOC meliputi pemantauan jaringan, pemecahan masalah jaringan, manajemen perubahan, manajemen kapasitas, manajemen insiden jaringan, dan pemeliharaan infrastruktur jaringan. Tanggung jawab SOC meliputi pemantauan keamanan, deteksi ancaman dan serangan, analisis kejadian keamanan, respons terhadap insiden keamanan, manajemen kejadian, manajemen ancaman, dan peningkatan keamanan.

Tugas NOC cenderung lebih operasional dan berfokus pada pemecahan masalah teknis terkait jaringan, pemantauan performa, penjadwalan perawatan rutin, dan pemulihan jika terjadi gangguan. Tugas SOC lebih berorientasi pada pemantauan keamanan, analisis ancaman, investigasi insiden, tanggapan dan penanganan kejadian keamanan, serta pemantauan proaktif untuk mencegah serangan keamanan.

Sementara Security Operations Center berfokus pada pemantauan, pendeteksian, dan analisis kesehatan keamanan organisasi 24/7/365, tujuan utama NOC, atau pusat operasi jaringan , adalah untuk memastikan bahwa kinerja dan kecepatan jaringan secara normal dan bahwa waktu henti terbatas. Insinyur dan analis Security Operations Center mencari ancaman siber dan upaya serangan, dan merespons sebelum data atau sistem organisasi disusupi. Personil NOC mencari masalah apa pun yang dapat memperlambat kecepatan jaringan atau menyebabkan waktu henti. Keduanya secara proaktif memantau secara real-time, dengan tujuan mencegah masalah sebelum pelanggan atau karyawan terpengaruh, dan mencari cara untuk melakukan perbaikan terus-menerus sehingga masalah serupa tidak muncul lagi. SOC dan NOC harus berkolaborasi untuk bekerja melalui insiden besar dan menyelesaikan situasi krisis, dan dalam beberapa kasus fungsi SOC akan ditempatkan di dalam NOC. NOC dapat mendeteksi dan merespons beberapa ancaman keamanan, khususnya yang berkaitan dengan

kinerja jaringan, jika tim dilatih dengan benar dan mencari ancaman tersebut. SOC biasa tidak akan memiliki kemampuan untuk mendeteksi dan menanggapi masalah kinerja jaringan tanpa berinvestasi pada alat dan keahlian yang berbeda.

2.2 Manfaat NOC dan SOC dalam Infrastruktur Jaringan

Berikut merupakan manfaat dari NOC dan SOC :

1. Manfaat NOC
   - Identifikasi masalah jaringan lebih cepat. Karena NOC memantau situasi jaringan setiap saat, NOC dapat menemukan masalah dan mengatasinya tanpa harus menunggu keluhan dari pengguna.
   - Downtime minimal. Semakin banyak bisnis yang membutuhkan infrastruktur jaringan yang berfungsi setiap saat. Berkat pemantauan staf NOC, masalah yang mungkin menyebabkan downtime dapat diidentifikasi dengan segera dan tidak mengganggu operasi bisnis.
   - Menjaga keberlangsungan bisnis. Karena NOC bertanggung jawab atas backup dan disaster recovery, perusahaan yang memiliki NOC dapat menjamin keberlangsungan bisnis bila terjadi masalah kehilangan data karena berbagai alasan.

2. Manfaat SOC
   - Perlindungan terus-menerus dari ancaman siber. SOC melakukan pemantauan setiap saat terhadap semua kejadian secara real-time dengan bantuan SIEM (security information and event management)
   - Respons keamanan yang lebih cepat. Pemantauan setiap saat memungkinkan deteksi dini dan tanggapan lebih dini dari pengelola sistem.
   - Menekan kerugian. Secara umum, respons yang lebih cepat terhadap suatu insiden akan menekan kerugian yang mungkin muncul.
   - Idealnya, suatu perusahaan atau institusi memiliki baik NOC maupun SOC. Pada kenyataannya, ini belum tentu dapat dilakukan sendiri. Kendalanya mungkin anggaran, karena baik NOC dan SOC menuntut investasi teknologi yang tidak sedikit. Selain itu perusahaan yang ingin membangun NOC dan SOC sendiri harus merekrut tenaga profesional untuk kedua pusat operasi tersebut.

2.3 Standar-standar dalam mendesain NOC dan SOC

Dalam merancang Network Operations Center (NOC) dan Security Operations Center (SOC), ada beberapa standar dan praktik terkait yang dapat diikuti. Berikut adalah beberapa standar umum yang dapat digunakan dalam merancang NOC dan SOC:

1. ITIL (Information Technology Infrastructure Library): ITIL adalah kerangka kerja yang menyediakan pedoman terkait manajemen layanan TI. Ini termasuk proses dan praktik terkait NOC, seperti manajemen peristiwa, manajemen masalah, manajemen perubahan, dan manajemen pengetahuan.
2. ISO/IEC 20000: Standar ini memberikan kerangka kerja untuk manajemen layanan TI yang efektif. ISO/IEC 20000 memberikan pedoman terkait desain, operasi, dan peningkatan NOC dan SOC.

3. ISO/IEC 27001: Standar ini berkaitan dengan keamanan informasi dan menyediakan pedoman terkait manajemen keamanan informasi dalam organisasi. Dalam merancang SOC, kepatuhan terhadap ISO/IEC 27001 sangat penting.
4. NIST SP 800-61: Ini adalah panduan dari National Institute of Standards and Technology (NIST) yang memberikan kerangka kerja untuk respons insiden keamanan. Panduan ini dapat digunakan untuk merancang dan mengoperasikan SOC yang efektif.
5. SANS Institute: SANS Institute adalah organisasi yang menyediakan pelatihan dan sertifikasi dalam bidang keamanan informasi. Mereka memiliki sejumlah standar dan praktik terkait SOC yang dapat menjadi acuan dalam merancang SOC yang kuat.

BAB 3

PENUTUP

3.1 Kesimpulan

Dalam suatu bisnis atau lembaga, Network Operation Center (NOC, pusat operasi jaringan) dan Security Operation Center (SOC, pusat operasi keamanan) bertugas untuk memastikan jaringan dan aset IT lainnya berfungsi lancar tanpa halangan. SOC dapat membantu mengambil tindakan pencegahan, membatasi kerusakan akibat peretasan, dan menilai rantai pembunuhan dunia maya jika memang terjadi. Anggota tim Security Operations Center membantu organisasi mengidentifikasi penyebab utama serangan siber. Ketika seorang analis SOC melakukan ini, mereka dikatakan terlibat dalam analisis akar penyebab. SOC bekerja untuk mencari tahu dengan tepat kapan, bagaimana, dan bahkan mengapa serangan berhasil. Untuk tujuan ini, analis SOC meninjau bukti serangan. Bukti semacam itu disebut indikator serangan. Jika serangan berhasil, analis SOC kemudian akan mempelajari indikator kompromi untuk membantu organisasi merespons dengan tepat, serta membuat perubahan sehingga serangan serupa tidak terjadi di masa mendatang.