Framework untuk menyusun Network Policy pada institusi Pendidikan

Mohammad Fal Sadikin

STMIK Amikom Yogyakarta

Abstrak

Untuk mencapai tujuan pengoptimalan jaringan komputer baik itu dari segi kinerjanya maupun dari segi keamanannya, network policy adalah salah satu bagian penting selain teknologi devices yang digunakan dan konfigurasi dari devices tersebut. Bahkan Teknologi devices yang baik dan konfigurasi yang baik pula, tidak akan optimal tanpa network policy yang sesuai. Saat ini banyak sistem jaringan komputer di institusi pendidikan belum optimal karena masalah network policy yang belum efektif dan efisien dalam menunjang kinerja suatu organisasi sebagai institusi pendidikan. Menyusun network policy di institusi pendidikan bukanlah pekerjaan sederhana, terlebih lagi user yang kompleks menyebabkan proses penyusunan menjadi semakin kompleks.

1. Pendahuluan

Salah satu masalah utama kinerja layanan dan keamanan jaringan komputer di suatu institusi pendidikan saat ini adalah tidak berfungsinya atau tidak tepatnya implementasi network policy sebagai salah satu bagian penting dalam system layanan jaringan komputer. Banyak pengelola jaringan komputer dan para user masih belum memperhatikan pentingnya network policy tertulis, bagaimana cara menyusunnya, mengelola, dan mengimplimentasikan dalam berbagai aplikasi layanan jaringan komputer. Oleh sebab itu, paper ini memfokuskan pada masalah network policy, bagaimana menyusunnya, mengimplementasi, serta mengelolanya secara efektif dan efisien, agar tujuan pengoptimalan kenerja dan keamanan dapat tercapai.

2. Tiga Kesalahan Utama Konsep Network Policy

1. Tujuan utama network policy adalah untuk mengamankan Jaringan Komputer, mengamankan jaringan pada dasarnya bukanlah tujuan utama dari network policy, yang menjadi tujuan utama adalah bagaimana mengamankan proses kegiatan yang

ada di dalam organisasi tersebut, agar dapat mendukung proses kegiatan menjadi lebih efektif dan efisien dengan menurangi resiko akibat kesalahan user, administrator, serta pihak-pihak yang terkait di dalamnya. Network policy menydiakan blueprint tentang apa yang harus diamankan, bagaimana cara mengamankannya untuk mendukung proses kegiatan atau misi yang ada di dalamnya dengan bantuan berbagai teknologi dan konfigurasi seperti Firewalls, intrusion detection systems (IDS), anti-virus (AV), backup and restore strategies, locked doors, and system administration checklists.

2. Network policy harus panjang, lengkap, dan kompleks. Pada kenyataannya, network policy yang efektif dan efisienlah yang bertahan lebih baik. Network policy yang kompleks biasanya tidak proporsional dan pada umumnya diabaikan. Network policy yang baik adalah kumpulan dokumen yang dipisahkan berdasarkan berdasarkan spesifikasi kebutuhan dan pada siapa ditujukan, pengelola, user, atau pihak ketiga. Dengan memisahkan tujuan policy-nya akan lebih mudah diserap oleh audience sesuai dengan tanggung jawabnya masing-masing.

3. Network policy harus 100% lengkap dan merupakan pekerjaan sekali jadi. Pada kenyataannya network policy adalah proses dan evaluasi berkelanjutan, bahkan dinamika dalam sebuah organisasi ikut menetukan perubahan dalam network policy, karena tentunya kebijakan baru akan sejalan dengan munculnya kelemahan dan ancaman baru dalan system jaringan. Oleh sebab itu network policy adalah pekerjaan yang tidak pernah akan berakhir.

3. Proses Penyusunan Network Policy

Tahap pertama dalam penusunan security policy adalah pembentukan *team*. Biasanya proses penulisan network policy adalah dengan pendekatan top-down process, meskipun ini bukan merupakan syarat mutlak karena pendekatan campuran antara top-down dan bottom-up memungkinkan untuk diterapkan. Teamwork yang dibentuk sebaiknya terdiri dari para personil yang erat kaitannya dengan aplikasi yang berjalan di atas jaringan tersebut, tidak hanya para personil yang paham akan aplikasi teknologi yang dipakai tetapi juga para personil yang mengerti betul seluk beluk bisnis proses di institusi tersebut, sehingga masing-masing personil memiliki kontribusi yang unik sesuai dengan latar belakang bidang yang dimilikinya untuk menghasilkan network policy yang efektif dan efisien.

3.1. Kerangka Network Policy

Pada bagian ini akan dibahas mengenai inti dalam penulisan network policy, setiap institusi tentunya akan menghasilkan policy yang berbeda-beda, namun policy tersebut pada dasarnya akan merujuk pada kerangka tertentu, antara lain sebagai berikut.

1. Seberapa sensitif informasi harus ditangani.
2. Bagaimana maintenance ID, Password, dan seluruh account data penting.
3. Bagaimana merespon potensi security incident dan percobaan gangguan sistem keamanan.
4. Bagaimana menggunakan workstation dan internet dengan cara yang benar.
5. Bagaimana manajemen email system.

Beberapa pendekatan dasar antara lain sebagai berikut.

1. Mengidentifikasi apa yang perlu diamankan.
2. Pihak-pihak mana yang akan dilindungi.
3. Mendefinisikan apa saja potensi resiko terhadap seluruh aset informasi.
4. Pertimbangan pemonitoran untuk evaluasi.

Daftar kategori yang harus diamankan.

1. Hardware: seluruh server, workstation, personal komputer, removable media (CD, floppy, flashdisk, dan seterusnya.), jalur komunikasi, dan seterusnya.
2. Software: identifikasi seluruh potensi penggunaan software, jenis ancaman, dan cara menanggulanginya.
3. User: penggolongan user berdasarkan prioritas, siapa saja yang boleh dan tidak boleh terhadap akses informasi tertentu.

Kerangka Network Policy.

1. Computer Acceptable Use, yakni dokumen yang bersifat umum yang mencakup seluruh penggunaan komputer oleh user, termasuk server dan aplikasi yang berjalan di atas jaringan tersebut.

2. Password, yakni deskripsi tentang persyaratan dalam penggunaan password untuk keamanan komputer dan aplikasinya, bagaimana cara pemilihan password yang tepat, dan bagaimana password policy tersebut di implementasikan.

3. Email, Policy yang mengatur mengenai penggunaan email, mencakup seluruh persyaratan untuk mengoptimalkan email system yang ada.

4. Web, yakni policy yang mengatur tentang spesifikasi web browser yang boleh digunakan, bagaimana cara meng implementasikanya, bagaimana konfigurasinya, dan segala policy yang mengatur tentang pembatasan akses pada situs-situs tertentu.

5. Mobile Computing and Portable Storage, yakni deskripsi tentang persyaratan penggunaan mobile computing dan portable storage, bagaimana mensupport device tersebut dan spesifikasi device yang diijinkan untuk digunakan dalam system network.

6. Remote access, yakni deskripsi tentang persyaratan penggunaan remote access, siapa saja yang boleh menggunakan, spesifik lokasi, dan segala persyaratan keamanan.

7. Internet, yakni deskripsi tentang konfigurasi gateway, apa saja yang dibolehkan masuk dan keluar gateway, dan mengapa?

8. Wireless, yakni policy yang mengatur megenai wireless system, konfigurasi, persyaratan penggunaan, maintenance, pengamanan, dan kondisi penggunaan.

9. Servers, statement dari institusi mengenai standart penggunaan server, tujuan dari spesifik server tertentu, enabled/disabled services.

10. Incident Response Plan, tentunya policy tidak akan pernah lengkap tanpa Incident Response Plan policy, deskripsi tentang apa yang harus dilakukan ketika keamanan jaringan mengalami kegagalan, siapa yang bertanggung jawab, bagaimana penanggulangannya, dan siapa yang memiliki kekuasaan penuh dalam proses ini.

3.2. Tujuan Network Policy

Untuk lebih mengoptimalkan network policy yang dibuat, maka perlu diketahui apasajakah factor-faktor yang harus dipenuhi, ditujukan pada siapa, dan cakupan wilayah kerjanya.

1. The institution name, apakah network policy berlaku untuk seluruh bagian dari institusi, hanya fakultas tertentu saja, jurusan tertentu saja, atau bahkan hanya untuk bagian tertentu dari jurusan tertentu.

2. The purpose of the policy, apa tujuan dari network policy, untuk apa? Dan apa yang diharapkan dari dari penyususnan network policy? Missal, untuk tujuan keamanan, atau untuk pengoptimalan kinerja.

3. The individuals or organizations responsible for the policy, siapa yang bertanggung jawab untuk keseluruhan keamanan jaringan, IT Departement atau Sistem Informasi Departement.

3.3. Peraturan dalam Network Policy

1. Penalties for breaking policy, detail tentang hukuman atau sanksi bagi para pelanggar network policy, mulai dari peringatan hingga pemecatan.

2. Who enforces the policy, seluruh manajemen dan user harus memiliki tanggung jawab yang spesifik pada peraturan yang ada di network policy.

3. How to request policy changes, detail tentang bagaimana proses perubahan network policy, bagaimana cara mengubahnya, siapa yang merevisi, dan parameter apa yang dipakai untuk merevisi network policy.

4. How often your policies must be reviewed, seberapa sering network policy dievaluasi?

3.4. Contoh Network Policy di Institusi Pendidikan.

The Acceptable use policy

1. Pegawai, dosen, mahasiswa D3, S1, dan pasca sarjana diberi fasilitas email dengan domain masing – masing.
2. Account mahasiswa dan dosen bersifat seterusnya tetapi kapasitasnya dibatasi sesuai dengan kebijakan Jurusan/Fakultas. Untuk account pegawai bersifat sementara selama masih bekerja.
3. Mahasiswa yang melanjutkan studi ke jenjang yang lebih tinggi mendapatkan email baru sesuai dengan jenjang studinya.

4. Username email ditentukan sendiri oleh user, sedangkan password diberikan oleh admin. password tersebut harus segera diganti untuk menghindari penyalahgunaan account email.
5. User yang melaporkan lupa password ke admin wajib mengganti password-nya.
6. Username dan password proxy sama dengan username dan password email. Password proxy dapat di ubah, tetapi username tidak bisa diubah – ubah.
7. Semua user yang menggunakan internal workstation wajib men-setting password protected screen saver.
8. Semua user yang akan meninggalkan komputer atau workstation dalam waktu lebih dari 3 menit dan dengan jarak lebih dari pandangan untuk melihat komputernya wajib menjalankan lock screen / logout user.
9. Komputer menggunakan OS linux yang terpusat di server dengan account proxy sebagai autentikasi.
10. Komputer lab tidak diijinkan meng-install software selain yang berkepentingan (asisten dosen lab dan admin)
11. Tidak ada user yang diijinkan untuk meng-copy file system operasi (contoh : file SAM, etc/passwd) yang ada di workstation kecuali admin.

User Account Policy

1. Semua user dilarang untuk membagikan account milik sendiri ke orang lain (termasuk keluarga, sahabat karib, dll).
2. Semua user dilarang menggunakan account milik orang lain.
3. Account user hanya dapat digunakan sekali pada waktu yang bersamaan (menggunakan kabel atau wireless)
4. Tamu yang akan memakai koneksi internet diberi nama user “guest” dengan password yang selalu berbeda tiap hari. Password guest diberikan oleh admin.

Remote Access Policy

1. Admin dapat menggunakan fasilitas VPN untuk akses server – server yang ada.
2. Pegawai dapat menggunakan fasilitas VPN untuk akses Sistem Informasi Pegawai (SIP).
3. Tidak boleh menggunakan modem dan access point portable sendiri.
4. Semua user yang akan menggunakan remote access wajib menggunakan software yang dapat meningkatkan keamanan (contoh : antivirus, trojan horse scanning, dll).

Information Protection Policy

1. Semua Civitas Akademika Teknik Elektro yang memiliki kertas dokumen, CD, DVD, Flash disk dan media penyimpanan lainnya dan tidak terpakai atau rusak wajib menghancurkan sebelum dibuang.
2. Level akses data disesuaikan dengan status kepegawaian yang dimiliki.
3. Level akses data untuk pegawai baru atau pegawai yang naik / turun jabatan akan diberi tahu oleh pimpinannya.

Network Connection Policy

1. Semua perbaikan komputer server harus dapat dilakukan 1 x 24 jam.
2. Installasi network hardware wajib diawasi oleh admin.
3. Jika ditemukan ada user yang tidak terdaftar dalam jaringan akan langsung di matikan access-nya.
4. Autentikasi wifi menggunakan WEP
5. Seting VLAN untuk dosen, karyawan, mahasiswa.

The Strategic partner policy

1. Dosen luar yang menggunakan video conference wajib menggunakan fasilitas VPN.
2. Jaringan Inherent hanya bersifat read only.

The Privileged Access Policy

1. Admin hanya dapat dipecat oleh pimpinan Fakultas.
2. Admin berhak membuat user account baru sesuai dengan kebutuhan Fakultas/Jurusan.
3. Admin diijinkan untuk menggunakan network scanning tools.
4. Admin tidak diijinkan untuk mengakses secara remote komputer – komputer selain komputer lab.
5. Admin dilarang keras untuk melihat password milik user lain kecuali adanya laporan tentang lupa password yang sifatnya tertulis dan ditanda tangani oleh ketua jurusan masing-masing bagi mahasiswa dan bagi pegawai ditanda tangani oleh kepala bagian pegawai.

The Password Policy

1. Panjang password user minimal 8 karakter dengan perpaduan antara huruf kapital, huruf kecil, angka, dan karakter khusus (!@#$%^&*()_+|).
2. Disarankan semua user mengganti password-nya dalam 1 bulan
3. Password yang menggunakan 1 karakter dengan panjang 8 digit atau lebih akan tetap kena pinalti
4. User yang mengganti password-nya akan dicatat dalam file log server.

Internet Policy

1. Semua user dapat mengakses internet.
2. Setiap user memiliki batasan bandwidth untuk akses internet pada jam kerja (8.00-16.00). Selebihnya bebas.
3. Semua user dilarang mengakases website porno atau website underground.

4. Kesimpulan

Penyusunan network policy adalah pekerjaan berkesinambungan dan tidak akan pernah menjadi 100% kompleks, oleh sebab itu dibutuhkan evaluasi secara periodik sesuai dengan kebijakan manajeman, serta pemonitoran rutin untuk mencegah pelanggaran terhadap network policy tersebut.

Daftar Pustaka

Dancho Danchev. Building and Implementing a Successful Information Security Policy.WindowSecurity.Com. 2003.

Frederick M. Avolio and Steve Fallin. Producing Your Network Security Policy. Watchguard.com. July 2007.

URL : http://www.sans.org/rr/policy

URL : http://www.secinf.net/policy_and_standards/

URL : http://directory.google.com/Top/Computers/Security/Policy/