Information Security Standards, Regulations, and Compliance

Agung Brastama Putra

Information Security Standart

- Keamanan informasi di dunia didasarkan pada standar keamanan.
- Standar-standar keamanan mengatur apa yang dianggap aman dan apa yang tidak.
- Selama mengelola lingkungan Anda, Anda pasti akan menemukan standar ini.
- Ini akan sangat bermanfaat bagi Anda jika Anda memahami standar ini, tahu siapa mengatur mereka, dan memahami mengapa mereka didirikan.

- Sebelum kita dapat membahas standar keamanan informasi, pertama kita harus pastikan bahwa anda tahu sedikit tentang organisasi yang menetapkan standar tersebut.
- Organisasi-organisasi yang umumnya menetapkan standar keamanan internasional di organisasi.
- Organisasi yang menetapkan standar keamanan informasi adalah ISO, IANA, NIST, dan IETF.

ISO

- ISO = the International Organization for Standardization.
- ISO adalah salah satu yang terbesar di seluruh dunia standar organisasi.
- ISO memiliki kantor di seluruh dunia, tetapi markas pusatnya adalah berlokasi di Jenewa, Swiss.
- ISO menetapkan standar untuk informasi keamanan, serta industri lainnya.
- situs Web-nya di www.iso.org.

NIST

- The NIST is the National Institute of Standards and Technology.
- Adalah badan pemerintah yang didirikan pada 1901.
- Badan ini bagian dari Amerika Serikat Departemen Perdagangan.
- NIST memiliki dua lokasi utama di Maryland dan Colorado.
- NIST menetapkan standar untuk semua bidang teknologi, bukan hanya teknologi informasi.
- situs Web-nya di www.nist.org.

IETF

- The IETF is the Internet Engineering Task Force.
- IETF adalah Masyarakat internasional yang menetapkan standar untuk Internet.
- IETF dibagi dalam beberapa entitas yang disebut kelompok kerja.
- Setiap kelompok kerja memiliki topik tertentu atau teknologi yang
  bertanggung jawab.
- Setiap kelompok juga memiliki piagam yang berbeda. kelompok itu
  juga memiliki direksi.
- IETF memiliki keanggotaan terbuka, sehingga siapapun dapat bergabung dan menghadiri pertemuan-pertemuan reguler.
- Situs Web-nya di www.ietf.org.

IANA

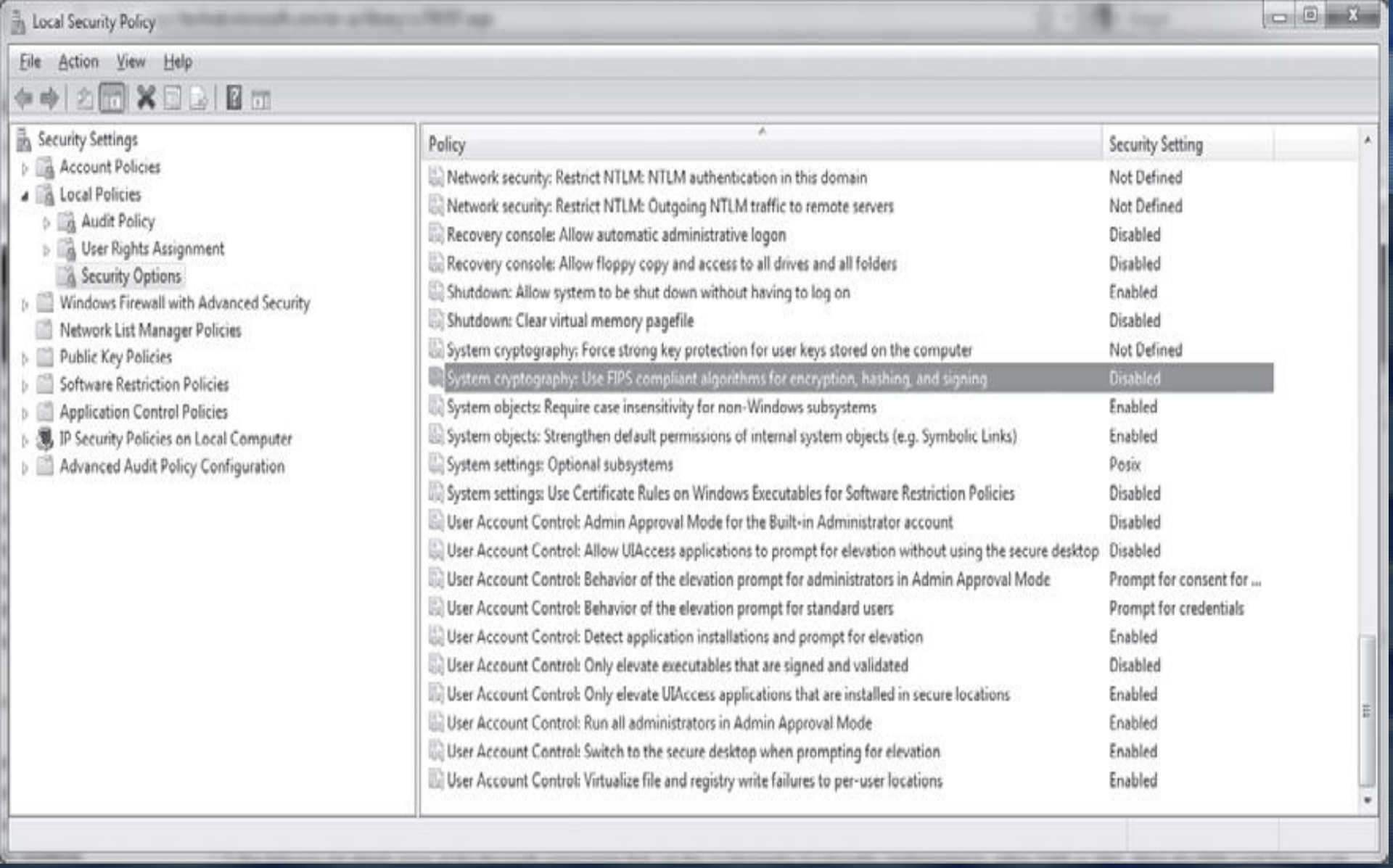
- The IANA is the Internet Assigned Numbers Authority.
- IANA bertanggung jawab untuk alokasi alamat IP.
- IANA akan mendelegasikan administrasi kelompok alamat IP untuk pendaftaran lebih kecil.
- IANA juga bertanggung jawab untuk peraturan DNS.
- IANA menangani operasi dari DNS akar domain (. Com, net,.Org, dan sebagainya).
- situs Web-nya di www. iana.org.

Security Standards and Certifications

FIPS

- FIPS dikembangkan oleh pemerintah federal AS melalui NIST.
- FIPS lebih banyak dikenal adalah FIPS seri 140.
- FIPS 140 berfokus pada kriptografi.
- FIPS 140 menetapkan standar untuk perangkat keras kriptografi perangkat lunak dan modul.
- Kriptografi adalah bertanggung jawab menyediakan serifikat untuk mereka agar algoritma kriptografi mereka mendapatkan sertifikat dengan standar FIPS 140.

- Lingkungan tertentu memerlukan penggunaan FIPS 140-bersertifikat algoritma. Jika hal ini terjadi, maka Anda harus memastikan bahwa algoritma yang digunakan di lingkungan anda juga mematuhi standar ini.
- Anda harus memeriksa dengan vendor perangkat lunak anda untuk memastikan bahwa aplikasi yang digunakan mematuhi standar FIPS 140.
- Selain itu, Sistem Microsoft memungkinkan Anda untuk membatasi penggunaan kriptografi hanya menggunakan algoritma standar FIPS 140.
- Anda dapat menggunakan Local Security Policy pada aplikasi Sistem Windows 7 untuk memaksa penggunaan FIPS 140 algoritma compliant.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Network security: Restrict NTLM: NTLM authentication in this domain
Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers
Not Defined
Recovery console: Allow automatic administrative logon
Disabled
Recovery console: Allow floppy copy and access to all drives and all folders
Disabled
Shutdown: Allow system to be shut down without having to log on
Enabled
Shutdown: Clear virtual memory pagefile
Disabled
System cryptography: Force strong key protection for user keys stored on the computer
Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
Disabled
System objects: Require case insensitivity for non-Windows subsystems
Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
Enabled
System settings: Optional subsystems
Posix
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies
Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator account
Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for standard users
Prompt for credentials
User Account Control: Detect application installations and prompt for elevation
Enabled
User Account Control: Only elevate executables that are signed and validated
Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations
Enabled
User Account Control: Run all administrators in Admin Approval Mode
Enabled
User Account Control: Switch to the secure desktop when prompting for elevation
Enabled
User Account Control: Virtualize file and registry write failures to per-user locations
Enabled

Kriteria Umum (Common Criteria) dan EAL

- Common Criteria adalah standar internasional untuk informasi keamanan sertifikasi.
- Karena Common Criteria adalah standar internasional dan bukan hanya standar di AS,
- di banyak organisasi lingkungan yang sesuai Kriteria umum adalah menggantikan kebutuhan compliant FIPS 140.

- Common Criteria menyediakan satu set rinci persyaratan untuk Sertifikasi.
- Sertifikasi Common Criteria diperoleh oleh vendor hardware dan software.
- Sertifikasi Common Criteria dilakukan untuk produk tertentu atau lingkungan tertentu dengan konfigurasi spesifik.
- Produk atau lingkungan yang disertifikasi disebut the Target of Evaluation (TOE).
- Sertifikasi TOE membutuhkan tiga komponen: Proteksi profil, Target Keamanan, dan Persyaratan Keamanan Fungsional.

- The Protection Profile adalah dokumen yang merinci secara aman implementasi perangkat atau jenis perangkat.
- beberapa produsen menggunakan Proteksi profil sebagai referensi ketika membuat jenis tertentu dari perangkat. Juga, Proteksi profil dapat memberi umpan balik ke Target Keamanan digunakan untuk sertifikasi.

- The Security Target adalah rincian konfigurasi keamanan TOE.
- Target Keamanan merupakan konfigurasi yang tepat untuk sertifikat.
- Vendor umumnya membuat The Security Target tersedia untuk pelanggan mereka.
- Dengan cara ini, pelanggan dapat mengkonfigurasi dengan cara yang mencerminkan konfigurasi Sertifikat.

- *Security Functional Requirements* adalah menyediakan fungsi sertifikat untuk produk.
- Common Criteria memiliki daftar fungsi standar yang dapat untuk produk.
- Fungsi-fungsi yang Anda inginkan termasuk dalam evaluasi harus terdaftar.
- Selama proses evaluasi Common Criteria, Anda juga harus menentukan tingkat jaminan. tingkat jaminan disebut Jaminan Evaluasi Level (EAL).
- EAL adalah indikator seberapa ketat pengujian tersebut. Ada tujuh tingkat EAL mungkin.
- 7 EAL adalah yang paling ketat.
- anda akses di situs http://www.commoncriteriaportal.org/

Regulations and Compliance

- sertifikasi peraturan dan kepatuhan yang berbeda dapat mempengaruhi lingkungan Anda.
- Beberapa peraturan mempengaruhi perusahaan di industri tertentu.
- Sangat penting bahwa Anda memahami peraturan dan sertifikasi kepatuhan mempengaruhi organisasi Anda.
- Aturan-aturan dan peraturan dapat secara dramatis mempengaruhi konfigurasi lingkungan Anda.

PCI DSS

- PCI DSS is the Payment Card Industry Data Security Standard.
- PCI DSS standar didirikan oleh Dewan Kartu Pembayaran Standar Keamanan Industri.
- Standar PCI DSS mengatur sistem yang menyimpan dan memproses informasi kartu kredit.
- Tujuan adalah untuk membantu mencegah penipuan kartu kredit dan / atau pencurian.

- Standar PCI DSS memiliki 12 persyaratan yang dikelompokkan ke dalam enam Kategori

Build and maintain a secure network

- Menginstal dan memelihara sebuah konfigurasi firewall untuk melindungi Data pemegang kartu
- Jangan gunakan vendor- default disediakan untuk password sistem dan parameter keamanan lainnya

Protect cardholder data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open public networks

Maintain a vulnerability management program

- Use and regularly update antivirus software or programs
- Develop and maintain secure systems and applications

Implement strong access control measures

- Membatasi akses ke data pemegang kartu
- Menetapkan ID yang unik untuk setiap orang dengan akses komputer.
- Membatasi akses fisik ke data pemegang kartu

Regularly monitor and test networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an information security policy

- Maintain a policy that addresses information security for employees and contractors

Keuntungan

- Sertifikat TI dapat meningkatkan kredibilitas seorang profesional TI di mata pemberi kerja.

Jenis Sertifikat

- Sertifikasi akademik (sebetulnya tidak tepat disebut sertifikasi) yang memberiakn gelar, Sarjana, Master dll
- Sertifikasi profesi. Yaitu suatu sertifikasi yang diberikan berdasarkan keahlian tertentu unutk profesi tertentu.

Sertifikasi profesional pada dasarnya memiliki 3 model, yaitu :

- Dikembangkan oleh Profesional Society, sebagai contoh British Computer Society (BCS), Australian Computer Soicety (ACS), South East Asian Regional Computer Confederation (SEARCC) etc

- Dikeluarkan oleh Komunitas suatu profesi, sebagai contoh Linux Profesional, SAGE (System Administration Guild), CISA(IS Auditing) [http://www.isaca.org/]

- Dikeluarkan oleh vendor sebagai contoh MCSE (by Microsoft), CCNA (Cisco), CNE (Netware), RHCE (Red Hat) etc. Biasanya skill yang dibutuhkan untuk memperoleh sertifikat ini sangat spesifik dan sangat berorientasi pada suatu produk dari vendor tersebut.