ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

INFRASTRUTTURE CRITICHE

E

REGOLAMENTI EUROPEI

Bruno Carbone
Responsabile Sicurezza Informatica ENAV S.p.A.
Lead-Auditor ISO/IEC 27001:2005
Roma 31 maggio 2007

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Agenda

1. Normativa Europea sulle Infrastrutture Critiche
2. AIIC *(Associazione Italiana Esperti Infrastrutture Critiche)*
3. ENAV S.p.A

Normativa Europea Infrastrutture Critiche

CONSIGLIO DELL'UNIONE EUROPEA

(Bruxelles, Dicember 18th, 2006)

La proposta di DIRETTIVA DEL CONSIGLIO, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la relativa protezione, trae le sue origini dai seguenti avvenimenti:

- Novembre 2005 - la Commissione adotta un libro verde relativo a un programma europeo per la protezione delle infrastrutture critiche (EPCIP), che presenta varie alternative relative all'elaborazione dell' EPCIP e della CIWIN

- Dicembre 2005 - il Consiglio "Giustizia e affari interni" (GAI) invitata la Commissione a presentare una proposta sull' EPCIP entro giugno 2006

Normativa Europea
Infrastrutture Critiche (2)

Tale proposta di direttiva espone le misure previste dalla Commissione ai fini dell'individuazione e della designazione delle infrastrutture critiche europee (ICE) e della valutazione della necessità di migliorarne la protezione

Articolo 1

Oggetto: la presente direttiva stabilisce una procedura di individuazione e designazione delle infrastrutture critiche europee, e un approccio comune per la valutazione della necessità di migliorarne la protezione.

Articolo 2

Definizioni: ai fini della presente direttiva si applicano le seguenti definizioni:

a) **Infrastruttura Critica** - strutture o parti di esse che sono essenziali per il mantenimento delle funzioni cruciali della società, tra cui la catena di approvvigionamento, la salute, la sicurezza e il benessere economico o sociale dei cittadini

b) **Infrastruttura Critica Europea** - infrastruttura critica la cui perturbazione o distribuzione avrebbe conseguenze significative su due o più Stati membri, o su uno Stato membro se l'infrastruttura critica è ubicata in un altro Stato membro. So no compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture

(segue)

Normativa Europea Infrastrutture Critiche (3)

c) **Gravità** - l'impatto della perturbazione o della distruzione di una particolare infrastruttura, con riferimento ai seguenti aspetti:

- Conseguenze per i cittadini (numero di persone colpite)
- Conseguenze economiche (entità delle perdite economiche e/o del deterioramento di prodotti o servizi)
- Conseguenze ambientali
- Conseguenze politiche
- Conseguenze psicologiche
- Conseguenze a livello di salute pubblica

d) **Punto Vulnerabile** - caratteristica o elemento della progettazione, della realizzazione o del funzionamento di un'infrastruttura critica che la espone a una minaccia di perturbazione o distruzione. Sino comprese le dipendenze in relazione ad altri tipi di infrastrutture

e) **Minaccia** - qualsiasi indicazione, circostanza o evento potenzialmente in grado di perturbare o distruggere un'infrastruttura critica o un suo elemento

f) **Rischio** - la possibilità di perdita, danno o lesione rispetto al valore attribuito all'infrastruttura dal suo proprietario/operatore e alle ripercussioni della perdita o dell'alterazione dell'infrastruttura, e la probabilità che una particolare minaccia sfrutti uno specifico punto vulnerabile

g) **Informazioni relative alla Protezione delle Infrastrutture Critiche** - fatti specifici relativi a un'infrastruttura critica che, se divulgati, potrebbero essere usati per pianificare ed eseguire azioni con danni certi e con conseguenze inaccettabili per tali strutture

Normativa Europea Infrastrutture Critiche (4)

ELENCO DEI SETTORI DI INFRASTRUTTURE CRITICHE

- Produzione di petrolio e gas, raffinazione, trattamento,stoccaggio e distribuzione con oleodotti e gasdotti
- Produzione e trasmissione di energia elettrica
- Industria Nucleare: Produzione e stoccaggio/trattamento di sostanze nucleari
- Tecnologie dell'informazione e della comunicazione (ICT):
  - Sistemi di informazione e protezione delle reti
  - Sistemi di strumentazione, automazione e controllo (SCADA ecc.)
- Internet:
  - Fornitura di servizi di telecomunicazioni fisse
  - Fornitura di servizi di telecomunicazioni mobili
  - Radiocomunicazione e navigazione
  - Comunicazione via satellite
  - Diffusione radiotelevisiva
- Erogazione di acqua potabile
- Controllo della qualità dell'acqua
- Gestione e controllo della quantità d'acqua
- Alimenti: Approvvigionamento e sicurezza alimentare

(segue)

Normativa Europea Infrastrutture Critiche (5)

- Salute:
  - Cure mediche e ospedaliere
  - Medicine, sieri, vaccini e prodotti farmaceutici
  - Biolaboratori e bioagenti
- Finanze:
  - Infrastrutture e sistemi di pagamento e di compensazione e
  - regolamento di titoli
  - Mercati regolamentati
- Trasporti:
  - Trasporto su strada
  - Trasporto ferroviario
  - Trasporto aereo
  - Vie di navigazione interna
  - Trasporto oceanico e trasporto marittimo a corto raggio
- Industria Chimica:
  - Produzione e stoccaggio/trattamento di sostanze chimiche
  - Pipeline per sostanze pericolose (sostanze chimiche)
- Strutture di Ricerca

Statuto

L'Associazione senza fine di lucro **AIIC** nasce al fine di costruire e sostenere una cultura interdisciplinare per lo sviluppo di strategie, metodologie e tecnologie in grado di gestire correttamente tali infrastrutture specialmente in situazioni di crisi

Art. 2: l'Associazione è apolitica, non ha fini di lucro ed ha per scopo quello di promuovere e favorire in Italia le attività di ricerca, di formazione, di analisi, di sensibilizzazione, consulenziali ed operative nell'ambito delle infrastrutture critiche, della loro sicurezza e delle loro interdipendenze

AIIC
ASSOCIAZIONE ITALIANA ESPERTI IN INFRASTRUTTURE CRITICHE

Obiettivi

L'Associazione "AIIC", nell'ambito dei suoi fini, si propone di:

a) Promuovere la conoscenza e la divulgazione delle tematiche proprie delle infrastrutture critiche mediante riunioni e convegni, giornate di studio, tavole rotonde, conferenze, visite tecniche e scambio di informazioni fra gli specialisti

b) Promuovere la diffusione della informazione relativa alle tematiche delle infrastrutture critiche e della loro sicurezza mediante

- seminari
- manifestazioni
- giornate di studio

c) Promuovere la ricerca scientifica e tecnologica su tematiche di interesse per le infrastrutture critiche mediante accordi con Università, Enti di Ricerca ed ogni altro soggetto operante nell'ambito delle infrastrutture critiche nonché partecipando a bandi di finanziamento nazionali ed internazionali

d) Sviluppare attività di formazione avanzata, pre- e post-laurea e formazione permanente su tematiche connesse con le infrastrutture critiche

e) Collaborare con organizzazioni governative, scientifiche e tecniche nazionali ed internazionali operanti nei settori propri delle infrastrutture critiche

(segue)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Obiettivi (2)

f) Porsi quale soggetto di raccordo fra le diverse realtà industriali e di ricerca operanti o interessate alla tematica ed i decisori politici sia a livello nazionale che internazionale

g) Pubblicare newsletters, riviste, atti di riunione, monografie relative alle infrastrutture critiche e a tematiche ad esse connesse

h) Fornire attività consulenziali ad enti pubblici e ad operatori di infrastrutture critiche

Pubblicazioni

Protezione delle Infrastrutture Critiche Informatizzate

- Questa pubblicazione è stata realizzata da un GdL inusualmente sorto sulla base di una "spinta dal basso" da parte di soggetti attenti e coinvolti alla problematica presenti nei vari dicasteri ed enti.

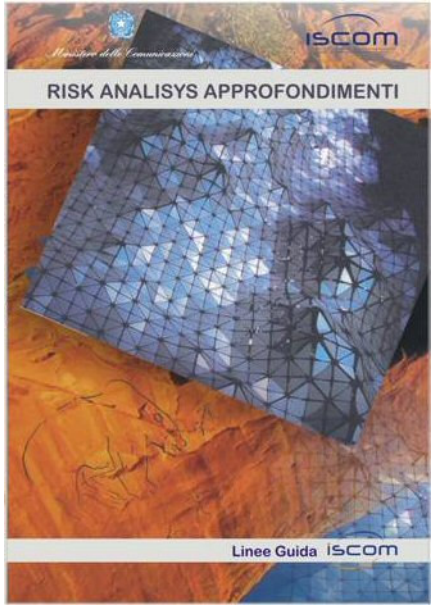
- E' la prima ad avere avuto come obiettivo quello di delinearla, evidenziandone gli aspetti di maggiore interesse e criticità per il sistema Paese.

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Pubblicazioni (2)

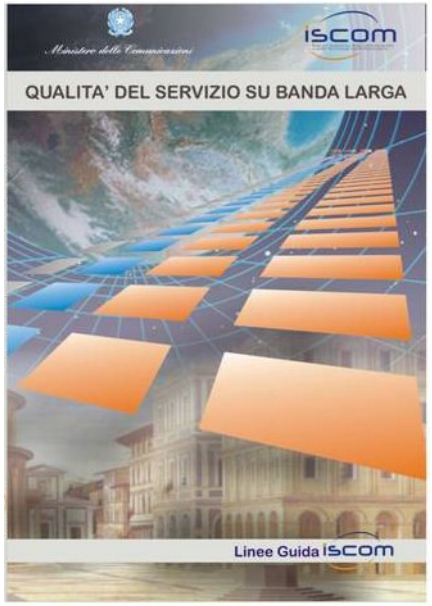
ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

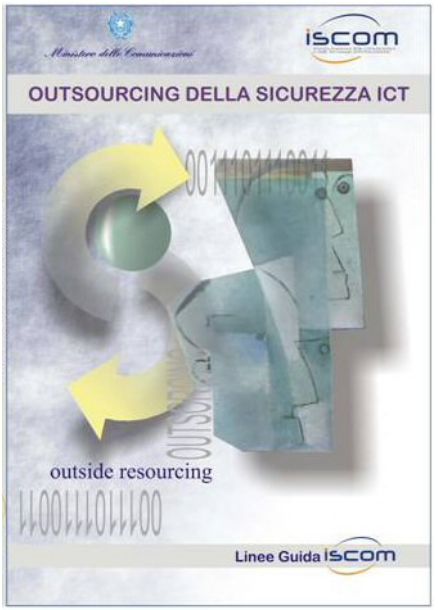
Pubblicazioni (3)



ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Pubblicazioni (4)





ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

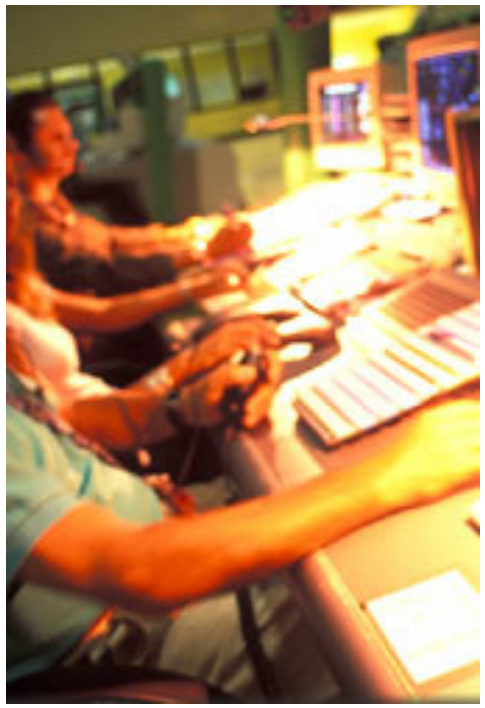
ENAV S.p.A.

ENAV è la Società italiana per l'Assistenza e il Controllo del Traffico Aereo. Il suo obiettivo è gestire lo spazio aereo con sicurezza, puntualità e continuità operativa, al passo con i ritmi di crescita del settore aeronautico e garantendo ai voli che ogni giorno solcano i nostri cieli la possibilità di coesistere in massima sicurezza seguendo armonici flussi di traffico.

Servizi

Attualmente ENAV fornisce i servizi per la navigazione aerea di terminale in 38 aeroporti italiani e servizi di rotta dai quattro Centri di Controllo d'Area di Roma, Milano, Padova e Brindisi.

- Controllo e assistenza del traffico aereo, integrati nel sistema aeronautico europeo
- Servizio informazioni aeronautiche
- Gestione puntuale e sicura (H24x7) di 5200 voli al giorno, 2.000.000 ogni anno, grazie a sofisticate e aggiornate tecnologie ed a un personale altamente qualificato di 3500 dipendenti di cui 2400 direttamente impegnati nell'assistenza al volo



ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Approccio Metodologico

ENAV, in qualità di fornitore nazionale per il controllo del traffico aereo italiano ha manifestato la volontà affrontare le problematiche legate alla *Security* nella sua globalità dotandosi di specifiche strutture volte a migliorare il controllo ed il governo della stessa

Soluzioni:

- Possibilità di differenziare l'approccio
- Approccio essenziale (basato su soluzioni tecnologiche)
- Approccio metodologico

ENAV ha scelto l'approccio metodologico

- Stabilendo le esigenze di sicurezza
- Trasformandole in requisiti
- Implementando soluzioni di sicurezza
- Verificando la rispondenza tra requisiti e soluzioni
- Garantendo la conformità con i requisiti legali e normativi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Analisi del Rischio

La metodologia di analisi del rischio attuata da ENAV S.p.A. è volta all'identificazione dei seguenti fattori fondamentali:

- Minaccia
- Vulnerabilità
- Impatto

E focalizzata su ciascuna specifica area di valutazione

Individuazione delle metodologie specifiche per ciascuna di esse

Attività:

1. Valutazione dell'impatto sui beni critici di ENAV
2. Identificazione della Minaccia
3. Valutazione ed Analisi delle Vulnerabilità
4. Attività di Penetration Testing
   - Attività di exploiting manuale delle Vulnerabilità
   - Valutazione del grado di esposizione al Rischio
5. Identificazione le contromisure da porre in atto *(Risk Treatment)*

Standard internazionali utilizzati

- **CobiT 4:** COBIT è l'acronimo di "Control Objectives for Information and related Technology". E' un framework, sviluppato da ISACA (Information Systems Audit and Control Association) e da ITGI (Information Technology Governance Institute)
- **ISO 17799:2005 – 27001:2005:** La BS 7799:2 -Information Security Management System (ISMS)- è stata la principale norma di riferimento per l'applicazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)
- **SSE-CMM (ISO 21827):** Questo standard, divenuto ISO nel Giugno del 2001 ed il cui titolo completo è "Systems Security Engineering Capability Maturity Model", è stato concepito come supporto ai processi di security engineering delle organizzazioni
- **ITIL:** L'ITIL, Information Technology Infrastructure Library, nasce, alla fine degli anni '80, come un insieme di direttive, ad uso e consumo della Pubblica Amministrazione Britannica, finalizzato alla gestione ottimale dei servizi IT
- **ISO/IEC 13335 :** Information Technology - Guidelines for the Management of IT Security

Criteri di valuazione

- **TCSEC** *(Trusted Computer System Evaluation Criteria – Orange Book)*
- **ITSEC** *(Information technology Security Evaluation Criteria)*
- **CC** *(Common Criteria – ISO/IEC 15408)*

Vantaggi nell'uso degli Standard

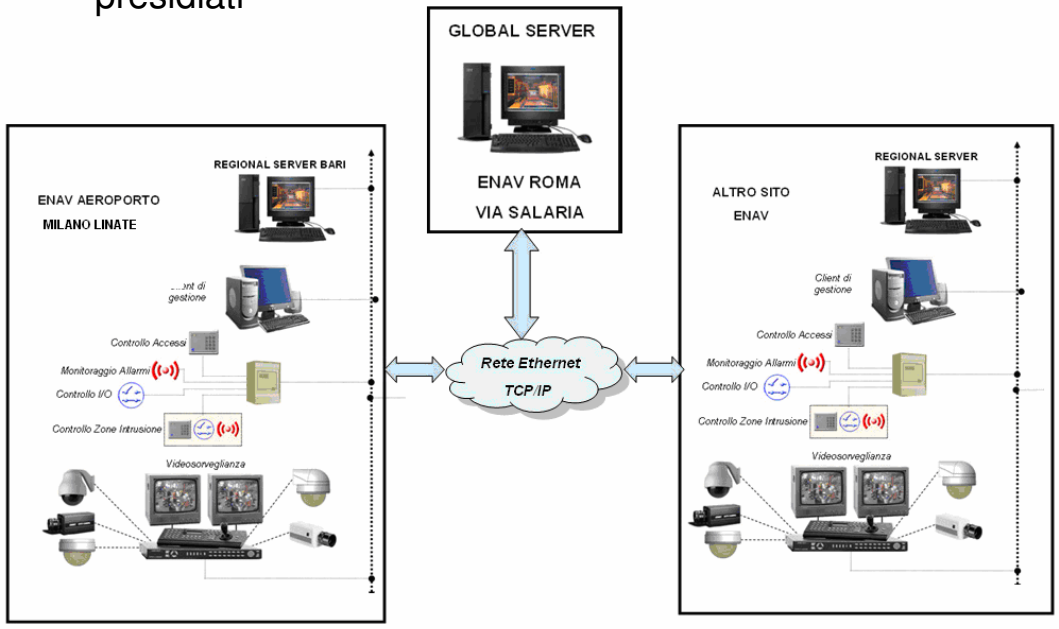
L'utilizzo di Standard internazionali di sicurezza consentono di raggiungere elevati livelli di *safety & security* ed allo stesso tempo permettono di usufruire di svariati vantaggi:

- Certificazione (ISO/IEC:27001/9001 ecc.)
- Conformità rispetto a requisiti legali e normativi (es.196/2003)
- Standardizzazione delle procedure
- Facilità di implementazione
- Facilità di monitoraggio e manutenzione

Sicurezza Fisica

Le azioni svolte da Enav S.p.A. in materia di sicurezza fisica hanno avuto come focus principale i seguenti ambiti:

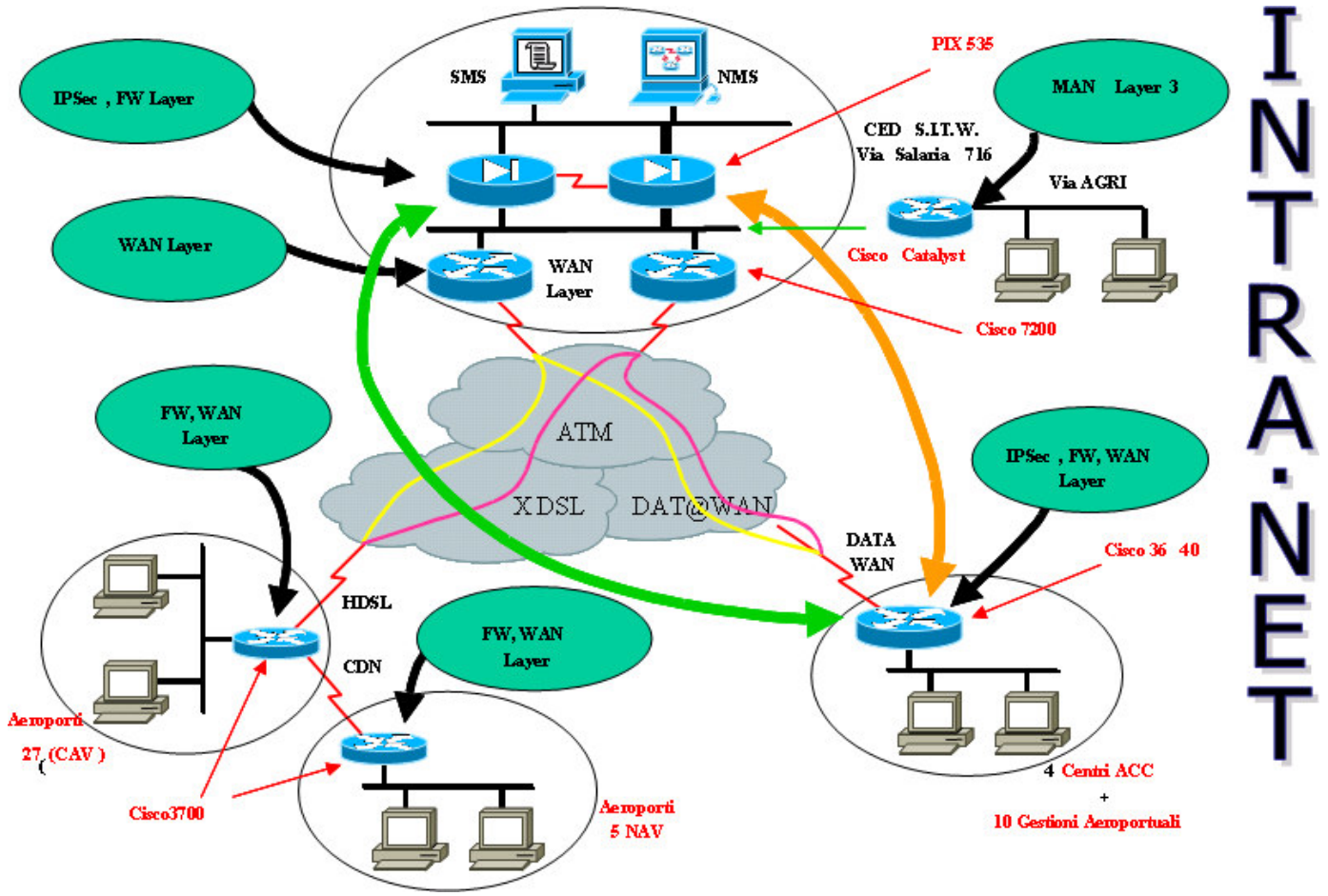
- Vigilanza h24 sui principali Siti
- Sistemi antintrusione mediante videosorveglianza antiscavalcamento e recinzioni
- Ronde
- Interventi su segnalazione di infrazioni con sistemi di radiosorveglianza in siti non presidiati



Nel prossimo futuro, realizzazione di un piano nazionale per il controllo accessi basato su smart-card e controlli biometrici

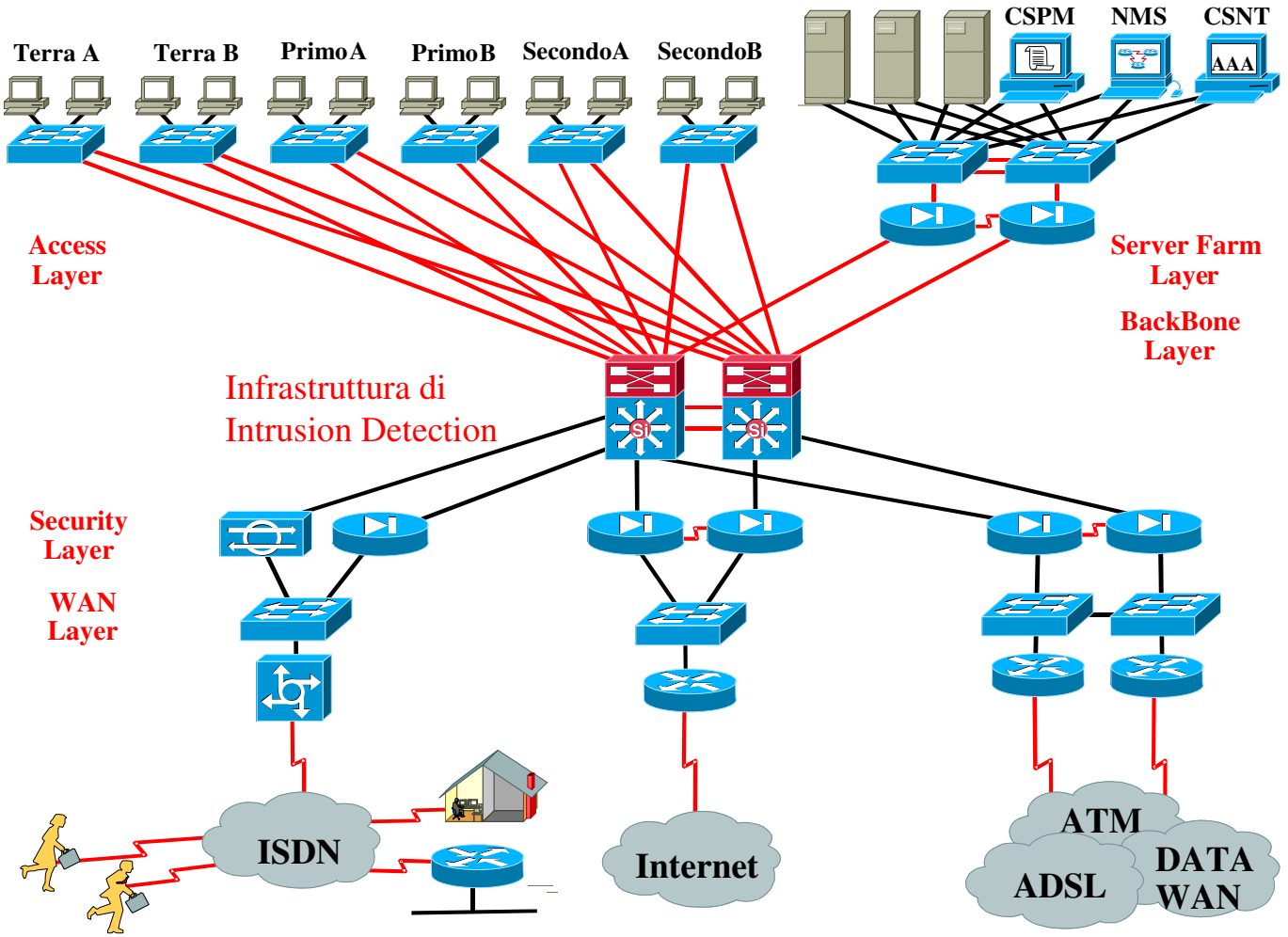
Architettura di Rete

La Rete WAN IP Corporate: Intranet/Internet ENAV



Il Progetto pilota : LAN 10 Giga/Bit Sede Centrale

(Sarà realizzata entro i primi mesi del 2004 - successivamente 2005 anche presso ACC)



Sicurezza Logica

Le azioni svolte da Enav S.p.A. in materia di sicurezza logica hanno avuto come focus principale i seguenti ambiti:

- Utilizzo PKI per l'autenticazione degli utenti e dei sistemi IT
- Profilazione utenti
  - Strumenti di Single sign-on
- Sistemi di Intrusion Detection
- Sistemi di firewalling per la protezione perimetrale
- Sistemi di videosorveglianza per la protezione fisica

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Sicurezza Organizzativa

Il carattere interdisciplinare delle tematiche correlate con la gestione della sicurezza, che richiede il concorso sinergico di varie competenze specialistiche, congiuntamente alla trasversalità organizzativa dei processi di gestione, impongono un approccio metodologico strutturato, che trova il suo fondamento nelle attività di sicurezza organizzativa. Tali attività perseguono lo scopo primario di stabilire gli indirizzamenti strategici per il Sistema di Gestione della Sicurezza, definiti sulla base di una analisi ponderata dei seguenti fattori, peculiari di qualsiasi Organizzazione:

- Normativa:
  - Codice in Materia di Protezione dei Dati Personali
  - Normativa interna all'organizzazione
- Formazione:
  - Piano di Formazione di base (sicurezza) suddivisa per ruoli e responsabilità
  - Piano periodico di aggiornamento
  - Piano di sensibilizzazione del personale
- Servizi Internet:
  - Condizioni di utilizzo di Internet
  - Politiche di utilizzo corretto dei servizi
  - Politiche sull'utilizzo di internet e posta elettronica

System Security Management

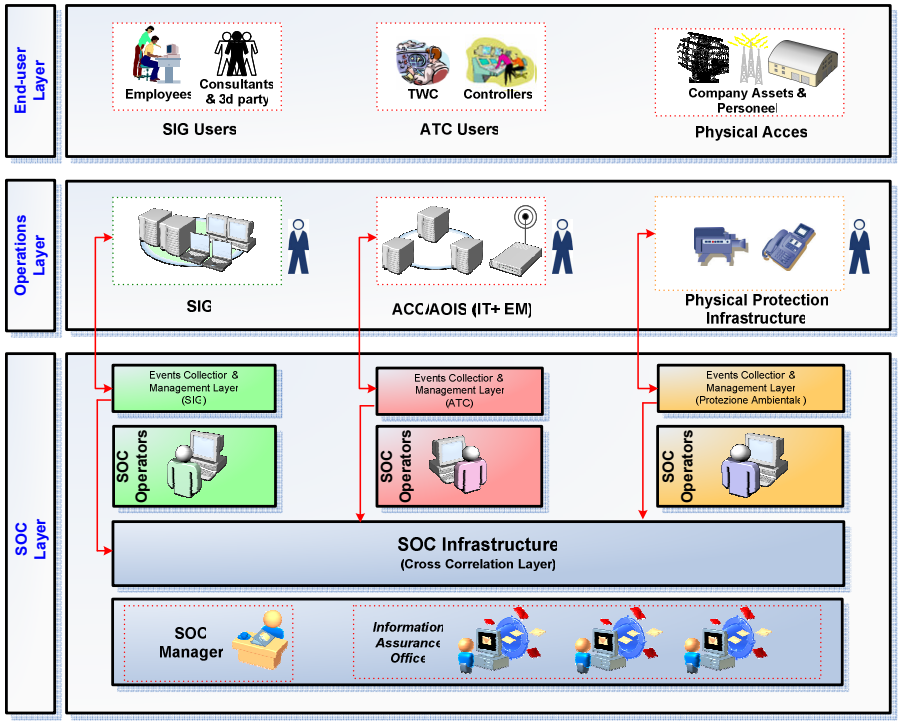
Stato Attuale

Adempimento delle attività volte a determinare preventivamente il grado di efficacia, efficienza e robustezza delle infrastrutture tecnologiche di sicurezza e delle procedure operative, rilevandone le eventuali inadeguatezze e fornendo le indicazioni necessarie alla stesura dei piani correttivi di intervento volti al miglioramento continuo ENAV si avvale di verifiche periodiche sulle attività svolte sui sistemi e sull'applicazione delle politiche di sicurezza.

Stato a Tendere

Definizione ed implementazione di un Security Operation Center (SOC) con l'obiettivo di:

- ***Controllare in maniera proattiva*** l'infrastruttura di sicurezza, soprattutto attraverso l'attività di monitoraggio e supervisione dei dispositivi che forniscono protezione all'organizzazione
- ***Prevenire e gestire*** efficacemente gli incidenti di sicurezza
- ***Contribuire al governo ed alla gestione della sicurezza*** in azienda, fornendo servizi, competenze e dati specifici relativi all'andamento ed al comportamento dei sistemi di sicurezza



DOMANDE?

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Grazie per l'attenzione

Bruno Carbone
Responsabile Sicurezza Informatica ENAV S.p.A.
Lead-Auditor ISO/IEC 27001:2005