Sistema Sanitario Regionale

L'organizzazione per la sicurezza informatica all'interno di una Azienda Sanitaria

Ing. Cinzia Spagno

ASUITS

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

SICUREZZA INFORMATICA – COS'È

SICUREZZA = NON AVERE DANNO

- FISICO SULLE PERSONE
- FISICO SULLE COSE
- NON FISICO ….

SICUREZZA INFORMATICA = ?

Sistema Sanitario Regionale

SICUREZZA INFORMATICA – COS'È

SICUREZZA INFORMATICA = SICUREZZA DEI DATI E DEI SISTEMI

SICUREZZA DEI DATI

- NON LI PERDO
- NON MI VENGONO RUBATI
- NON VENGONO MODIFICATI
- …

SICUREZZA DEI SISTEMI

- FUNZIONANO SEMPRE QUANDO SERVE

= SICUREZZA DELLE INFORMAZIONI

Sistema Sanitario Regionale

SICUREZZA INFORMATICA – COS'È

LA TERNA RID

RISERVATEZZA

INTEGRITÀ

DISPONIBILITÀ

CYBERSECURITY

LA SICUREZZA INFORMATICA SI OTTIENE CON LA TECNOLOGIA

BUSINESS CONTINUITY

DISSASTER RECOVERY

Sistema Sanitario Regionale

LE COMPONENTI TECNICHE

- Sicurezza fisica:
  - data center (locale tecnico principale per servizi accessori);
  - distribuzione (con locali tecnici dedicati);
  - client non sicurizzabili;
- Sicurezza logica infrastruttura di rete: parte attiva
- Sicurezza logica infrastruttura sistemistica
  - Server
  - Virtualizzazione
  - Storage
  - Client ‘’sicurizzabili‘’
- Sicurezza delle applicazioni
- Sicurezza dei dati (ultimo passo dopo i precedenti)

SICUREZZA INFORMATICA - PERCHÈ

- DERIVANTE DA OBBLIGHI
  - GDPR E PRIMA CODICE PRIVACY
  - CAD E AGID
  - E PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

O SOPRATTUTTO …

SANZIONI

Sistema Sanitario Regionale

OBBLIGHI da GDPR

Dall’entrata in vigore del Regolamento europeo in materia di protezione dei dati personali (GDPR) derivano gli obblighi di:

- ✓ Valutazione impatto privacy (DPIA) con metodi di analisi del rischio
- ✓ Accountability e Responsabilità del titolare nel garantire la sicurezza dei trattamenti

OBBLIGHI da CAD e da AgID

Dall'azione normativa del CAD (Codice dell'amministrazione digitale) e di AgID (Agenzia per l'Italia Digitale) derivano gli obblighi di:

- ✓ **elevare** la sicurezza informatica nelle pubbliche amministrazioni portandola alle Misure minime di sicurezza ICT dal 01/01/2018
- ✓ **attuare** il Piano Triennale per l'Informatica nella PA, ed in particolare:
  - **Garantire** adeguata *Business Continuity* per le applicazioni *Core Business* gestite (ovvero gran parte dei sistemi medicali)
  - **Remotizzare** le altre applicazioni (possibili) in *cloud* ottimizzando le risorse
  - **Implementare** un Sistema di Gestione della Sicurezza delle Informazioni (secondo le norme ISO 27000)

OBBLIGHI da perimetro di sicurezza nazionale cibernetica

Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi, dei servizi informatici, da cui dipende l'esercizio di una funzione essenziale dello Stato ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, e' istituito il perimetro di sicurezza nazionale cibernetica

OBBLIGHI da perimetro di sicurezza nazionale cibernetica

b) sono stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici … relative:

1) alle politiche di sicurezza, alla struttura organizzativa e alla gestione del rischio;

2) alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;

3) alla protezione fisica e logica e dei dati;

4) all'integrità delle reti e dei sistemi informativi;

5) alla gestione operativa, ivi compresa la continuità del servizio;

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

8) all'affidamento di forniture di beni, sistemi e servizi di information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale.

OBBLIGHI da perimetro di sicurezza nazionale cibernetica

Salvo che il fatto costituisca reato:

a) il mancato adempimento degli obblighi di predisposizione e di aggiornamento dell'elenco delle reti, dei sistemi informativi e dei servizi informatici è punito con la sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000;

b) il mancato adempimento dell'obbligo di notifica è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

c) l'inosservanza delle misure di sicurezza è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

…

e) l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e l'espletamento dei servizi informatici in violazione delle condizioni imposte è punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro

SICUREZZA INFORMATICA

- GLI OBBLIGHI NON SONO MERI ADEMPIMENTI MA RISULTATI COMPLESSI, SOSTANZIALI E DIMOSTRABILI
- SOLO L'OTTENIMENTO DI RISULTATI COMPLESSIVI PUÒ FARCI EVITARE LE SANZIONI
- MA
  - HA UN COSTO IN TERMINI DI BENI E SERVIZI
  - NON È SOLO TECNICA
  - SERVONO COMPETENZE

SICUREZZA INFORMATICA

- È NECESSARIO INVESTIRE RISORSE
  - PECUNIARIE
  - UMANE
    - ORE LAVORO
    - COMPETENZE
- E TRASFORMARE GLI OBBLIGHI IN OPPORTUNITÀ DI MIGLIORAMENTO PER MITIGARE IL COSTO OTTENENDO UN RAPPORTO FAVOREVOLE COSTO/BENEFICIO

Approccio per una sicurezza efficace e sostenibile

- La sicurezza è composta da una serie di azioni tecniche ed organizzative. Il livello di sicurezza raggiunto è uguale al livello più basso tra le diverse componenti.
- Va deciso quale è il livello raggiungere
- Va implementato in tutte le componenti
  - ✓ non ha nessun senso fare una componente molto sicura

- devo proteggere i dati dal punto di vista della terna RID
  - ✓ **Riservatezza**
  - ✓ **Integrità**
  - ✓ **Disponibiltà**

Approccio per una sicurezza efficace e sostenibile

- Uso di strumenti consolidati:
  - ✓ Domini Active Directory (AD) con le GPO
  - ✓ Certification Authority
  - ✓ Tool di asset inventory e software distribution
  - ✓ DHCP, RADIUS (NPS Ms), Firewall
  - ✓ piattaforme di endpoint protection, vulnerability assessment, data protection
  - ✓ …
- Prodotti ampiamente conosciuti nel panorama di mercato (esempi):
  - ✓ Cisco
  - ✓ Microsoft
  - ✓ Oracle
  - ✓ VmWare
  - ✓ ….
    - Ampia disponibilità consulenze specialistiche a prezzi ragionevoli

Approccio per una sicurezza efficace e sostenibile

- Modalità di implementazione basate su norme, standard, guide
  - ✓ ISO/IEC 38500:2015 Information technology - Governance of IT for the organization
  - ✓ COBIT Framework gestionale
  - ✓ ITIL Servizi
  - ✓ ISO 9001:2015 Quality management systems - Requirements
  - ✓ ISO/IEC 15504-ISO/IEC 33001:2015 Information technology - Process assessment - Concepts and terminology
  - ✓ ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements
  - ✓ ISO 22301:2012 Societal security - Business continuity management systems – Requirements
  - ✓ Center for Internet Security Critical Security Controls for Effective Cyber Defense – SANS20

Approccio per una sicurezza efficace e sostenibile

- Non inventiamo nulla MA definiamo un MODELLO tecnico coerente con quanto sopra, adeguato alla nostra realtà, da perseguire in tutte le azioni

- Non lo facciamo per abbattere il rischio cibernetico (AgID), il rischio privacy (GDPR), il rischio clinico, il rischio amministrativo, il rischio sul lavoro (D.Lgs. 81), il rischio …..
- MA
- Lo facciamo per abbattere con una unica visione AZIENDALE tutti i rischi con un approccio multidisciplinare che porta vantaggi su tutti i fronti e – complessivamente – costa meno

- NON SOLO COMPEONENTI TECNICHE

  - Procedure / protocolli / regolamenti / linee guida
  - Formazione
  - Controllo di applicazione (con responsabilità di risultato)

Le componenti tecniche

- Sicurezza fisica:
  - data center (locale tecnico principale per servizi accessori);
  - distribuzione (con locali tecnici dedicati);
  - client non sicurizzabili;
- Sicurezza logica infrastruttura di rete: parte attiva
- Sicurezza logica infrastruttura sistemistica
  - Server
  - Virtualizzazione
  - Storage
  - Client ‘’sicurizzabili‘’
- Sicurezza delle applicazioni
- Sicurezza dei dati (ultimo passo dopo i precedenti)

- Procedure / protocolli / regolamenti / linee guida
- Formazione
- Controllo di applicazione (con responsabilità di risultato)

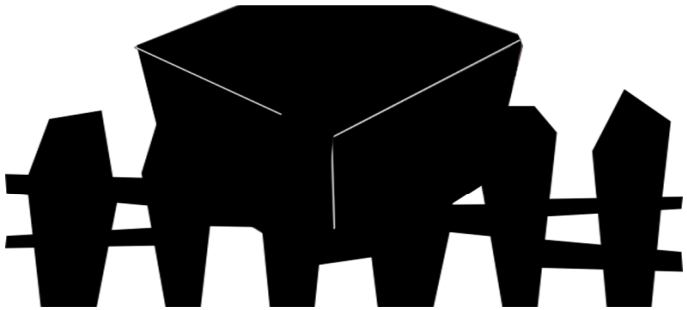
SICUREZZA FISICA

Riservatezza / Integrità / Disponibiltà

- ✓ Sistemi controllo accessi
- ✓ Videosorveglianza
- ✓ Ridondanza su doppia via separata del cablaggio verticale
- ✓ Ridondanza della alimentazione (generale, preferenziale, assoluta)
  - Doppio quadro
  - Doppia alimentazione
- ✓ Ridondanza sistema di raffreddamento e climatizzazione
- ✓ Sistemi antincendio
- ✓ Sistemi antiallagamento
- ✓ Sistemi di naming convention per prese, armadi distributori, apparati attivi
- ✓ Conoscenza anche dei percorsi: mappa
- ✓ Mai lasciare in locali aperti al pubblico armadi distributori (se non blindati)

SICUREZZA LOGICA INFRA-STRUTTURA DI RETE

Il DM: irrisolvibilmente insicuro



In base ai criteri di gestione derivanti dalla direttiva dispositivi medici (CEE 2007/47), ma soprattutto alla situazione del mercato, spesso il dispositivo medico non è altro che una black box che deve accedere alla rete.
No antivirus, no aggiornamenti di sistema, no inclusione nel dominio aziendale, necessità di accesso a internet, al file server, all'assistenza remota etc.

Possiamo solo recintare il pericolo!

- Facile? Non tanto in sanità.
- Possiamo rottamare
  - ✓ la vecchia TC?
  - ✓ il pletismografo?
  - ✓ …
  - ✓ … la maggior parte dei DM e non medici datati ?
- Possiamo non dare connettività agli ospiti (es. Università)?
- Possiamo non far accedere dall'esterno (es. telemanutenzione)?
- COMUNQUE uno dei principi della sicurezza informatica è la RIDUZIONE DELLA SUPERFICIE DI ATTACCO

La rete IT medicale

Un’azienda sanitaria è costretta a gestire host molto insicuri ed accessi insicuri

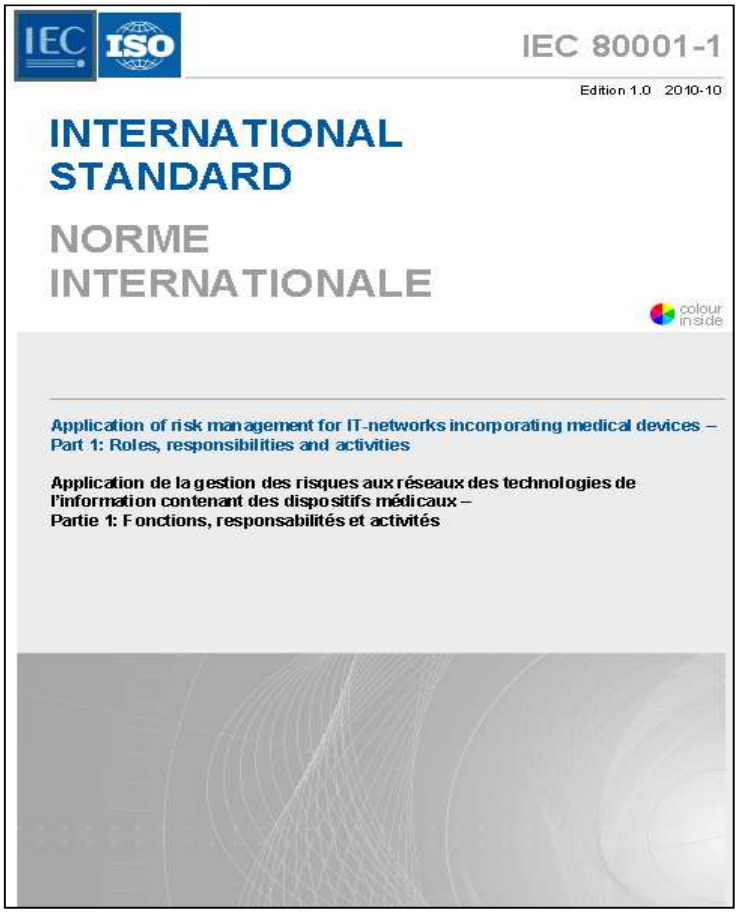
Inoltre in una azienda sanitaria la sicurezza informatica (security), non può prescindere da considerazioni in materia di safety … e viceversa.

Queste considerazioni sono state formalizzate per la prima volta a livello internazionale nella norma **IEC 80001-1:2010** “Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities”

Di fatto la rete di una azienda sanitaria è una

RETE IT MEDICALE

che è banalmente definita come una rete dati che comprende, tra gli host, dei DM … ma la gestione è molto più **complicata** della definizione



Un **IT medical network risk manager**

Deve considerare:

- che gli host insicuri sono fonte di infezione/attacco,
- che gli host insicuri sono oggetto di infezione/attacco,
- che non è possibile agire sugli host insicuri,

e nell'ottica della limitazione della superficie di attacco deve:

- **ISOLARLI**, ovvero impedire che possano fare traffico con host non appartenenti al loro gruppo
  - Limitare la visibilità solo a ciò che è necessario, ovvero **isolare** gli oggetti insicuri ed impedire la visibilità indiscriminata delle risorse
- **DISCIPLINARLI**, ovvero fare in modo che possano comunicare solo con il minimo indispensabile di host sicuri/insicuri e solo per la tipologia di traffico ritenuta lecita
  - Limitare le comunicazioni solo alle destinazioni necessarie, ovvero **disciplinare** il traffico ed impedire l'accesso indiscriminato alle risorse

ISOLAMENTO

E’ possibile confinare gli host in gruppi per mezzo di sottoreti definite sulla base di “criteri di compartimentazione verticale”:

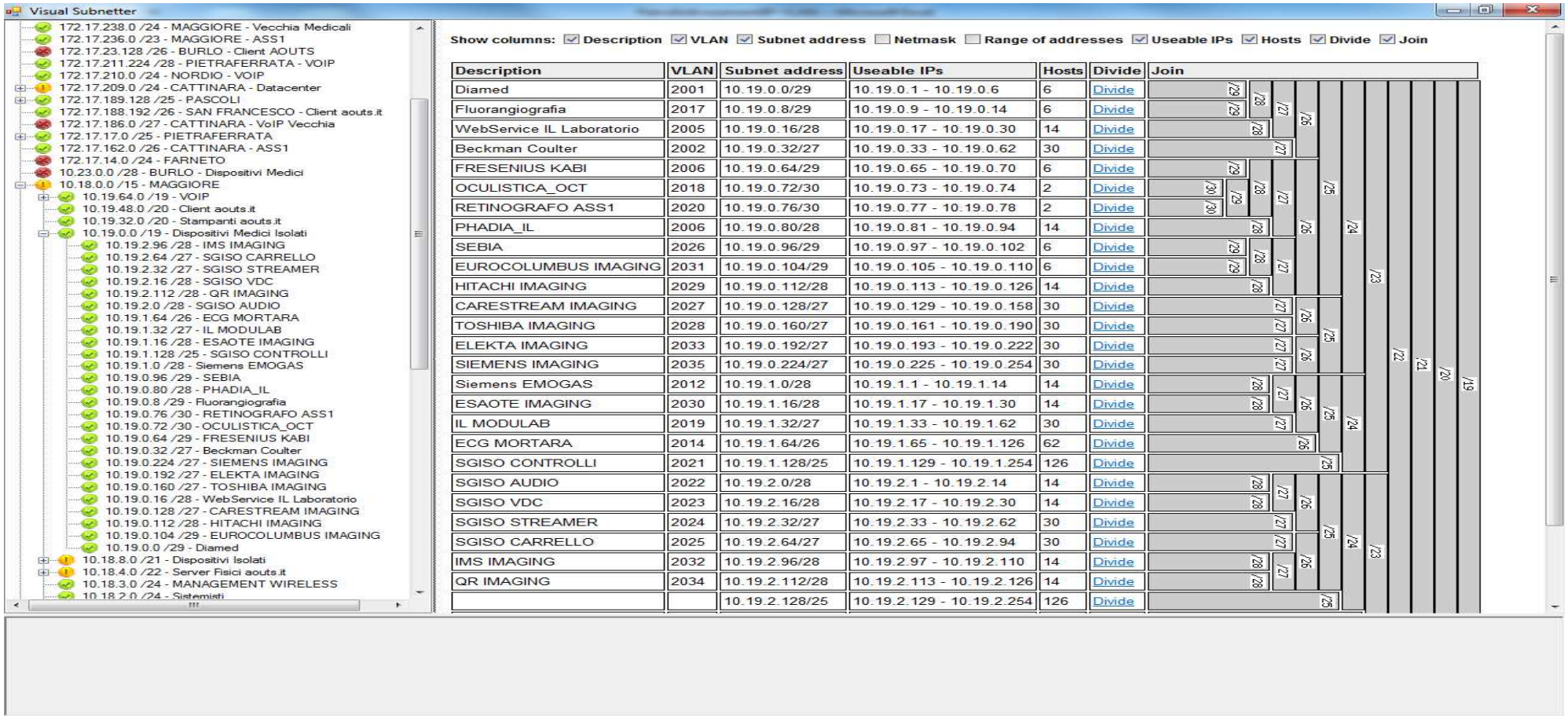
- **per ente/azienda**
- **per servizio**
- **per dominio di competenza**
- **per specifici problemi di sicurezza**

Se tali sottoreti sono definite a livello di centro stella, l’isolamento non è completamente garantito in quanto è sufficiente modifica l’IP dell’host per rendergli visibile una altra sottorete (ossia un altro gruppo di host).

Es - rete guest e rete aziendale

Per garantire la completa separazione è necessario operare non solo a livello 3 della pila ISO/OSI ma scendere al livello 2, ossia definire le VLAN (Virtual LAN) dedicate che di fatto sono anch’esse sottoreti ma strettamente correlate al mac address dell’host ed alla porta fisica dello switch.

ESEMPIO DI ISOLAMENTO



In funzione dell’omogeneità funzionale, del grado di sicurezza, del produttore e della visibilità esterna

DISCIPLINA

- In generale una VLAN potrebbe essere auto-sufficiente. Ma qualcosa potrebbe dover uscire /entrare

  es. TC in VLAN TC con le sue workstation deve poter archiviare in PACS, che ragionevolmente è in un'altra VLAN

  (con il consolidamento in generale tutti i servizi staranno in altre VLAN)

- Per fare questo è necessario introdurre strumenti che permettano la minima comunicazione necessaria e funzionale. Ossia è necessario definire delle ACL (Access Control List) che definiscono cosa è permesso e vietano tutto il resto.
- Sono liste di comandi a livello 3/4 della pila ISO/OSI che dettano al router le condizioni necessarie per far passare un pacchetto da una VLAN ad un'altra

AUTOMAZIONE

- L'IT medical network risk manager ha fatto il suo dovere … ma non riuscirà a gestire, perché tutto manuale.
- Serve l'AUTOMAZIONE

- ISOLAMENTO → automazione = Dynamic VLAN (e Dynanic IP)

- DISCIPLINA → automazione = Firewall

DYNAMIC VLAN

A ciascuna porta dello switch non è assegnata una VLAN fissa

Uno strumento esterno può quindi assegnare diverse VLAN alla stessa porta dello switch e relativo IP all'host che chiede il collegamento a seconda del gruppo a cui appartiene l'host che si deve collegare.

Tale gruppo è mappato in base a criteri:

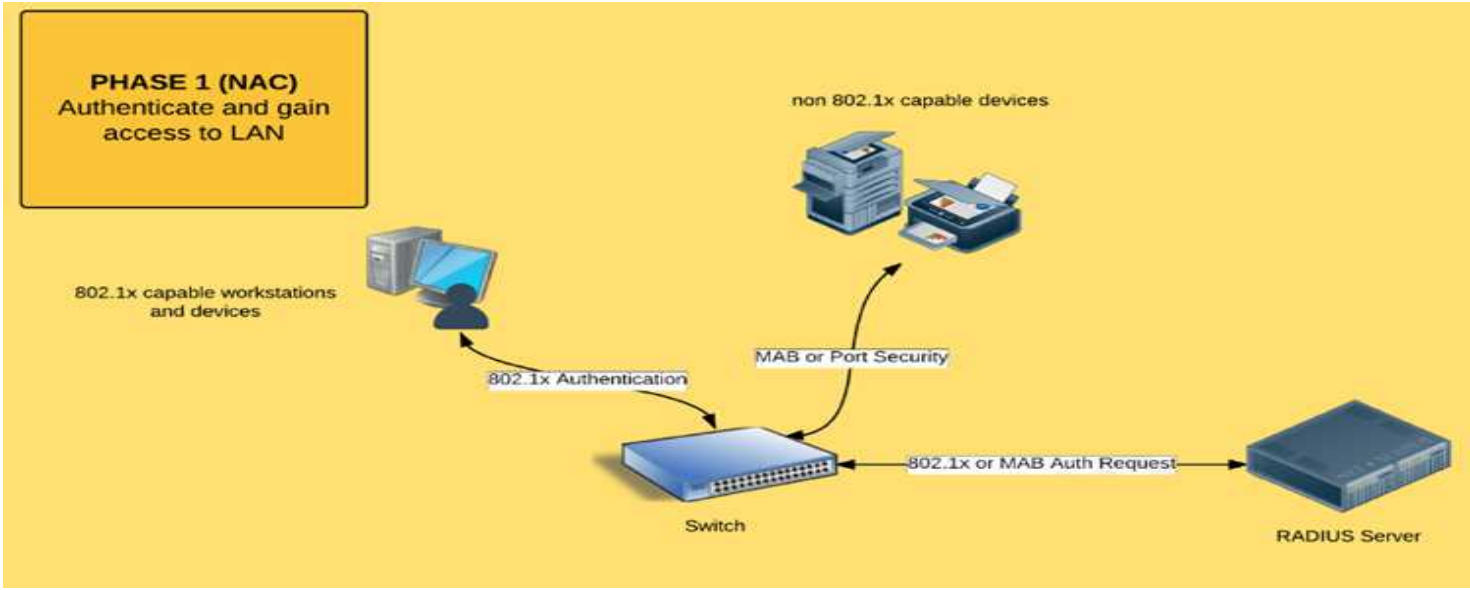
- ✓ di identificazione dell'host
  - Mac address
  - Login e passwd maggiore robustezza
  - Certificato
- ✓ di stato dell'host
  - presenza delle patch aggiornate
  - presenza dell'antivirus aggiornato
  - Versione di windows
  - …

Questo viene nominato NAC – Network Access Control

IEEE 802.1X

- Per la realizzazione di questo è sufficiente seguire quanto previsto dallo standard IEEE 802.1x
- Si poggia nel dettaglio su altri protocolli specifici di scambio messaggi
- In generali la realizzazione prevede:

- Switch in grado di supportare l'802.1x
- Server RADIUS che autentica: è un protocollo AAA (authentication, authorization, accounting)



Abbiamo ottenuto che per ciascun host il traffico di rete sia concesso:

- Prima dell'autenticazione solo traffico di autenticazione
- Dopo l'autenticazione, la porta va in stato di normale attività e l'host ha accesso alle risorse per la VLAN configurata

Il radius usa tabelle di criteri ma, nell'ambito dell'automazione può usare utilmente i servizi dell'infrastruttura di dominio AD

- Verifica le credenziali utilizzando generalmente un server di dominio **Active Directory**
- Collabora con il servizio DHCP
- Completa la risposta di autenticazione avvenuta con i parametri di configurazione necessari, tra cui la VLAN

AUTENTICAZIONE

- Nel caso di host in dominio, autenticazione effettuata mediante verifica **dell'account macchina o certificato associato**, la configurazione viene fatta con una regola sul gruppo di appartenenza della macchina
- Nel caso di host non in dominio ma con client 802.1x (es. telefoni VOIP) autenticazione con NU e PW memorizzati sul dispositivo
- Nel caso di host fuori dominio senza client 802.1x, l'autenticazione non può che essere effettuata per **MAC authentication**

- **Es. l'elettrocardiografo viene collegato ad una porta di rete permutata qualunque, si presenta per l'autenticazione, e gli viene assegnata in modo dinamico la VLAN degli elettrocardiografi che è definita come quella che può parlare solo con il server degli elettrocardiografi**

AUTOMAZIONE DELLA DISCIPLINA

- In una realtà complessa è impossibile garantire qualità di servizio gestendo manualmente le ACL, anche se portate tutte a livello di centro stella di presidio (comunque suggerito)

- È necessario quindi uno strumento (centralizzato) di facile utilizzo di disciplina del traffico tra diversi gruppi di host→ FIREWALL: nella moderna accezione firewall di segmentazione interna (Internal Segmentation Firewall – ISFW)
  - ✓ agevole implementazione di politiche di sicurezza su interfaccia grafica e moderne piattaforme di management
  - ✓ Possibilità di definire regole fino al livello applicativo (es. tra 2 VLAN è permesso solo il traffico HL7 o DICOM)

- Inoltre un ISFW garantisce la visibilità immediata e la reportistica del traffico e i relativi log

NEL CASO DI PIÙ AZIENDE

- Nei casi in cui vi siano più aziende (titolari) che insistono sulla stessa infrastruttura passiva va implementato un PROXI RADIUS (es. università)
- È necessaria comunque la fiducia che il RADIUS dell'altro titolare autentichi solo gli host sicuri sulla rete

SICUREZZA LOGICA INFRASTRUTTURA SISTEMISTICA

- Solo con la consapevolezza della infrastruttura sistemistica nel suo dettaglio si può garantire il livello di sicurezza definito

- È indispensabile quindi un INVENTARIO TECNICO
  - ✓ Hardware
  - ✓ Software

  Di tutti i dispositivi in rete ma anche dei cosiddetti «air gapped»

- Anche l'inventario va automatizzato, con gli strumenti:
  - ✓ CMDB (Configuration Management Data Base)
  - ✓ AAD (Automated Asset Discovery)
  - ✓ Software inventory / distribution

  <u>INTEGRATI TRA LORO</u>

CMDB

- Il Configuration Management Data Base CMDB traccia dati prettamente tecnici:
  - ✓ Tipo di hardware (client, server, stampante, etc)
  - ✓ Produttore hardware, modello e numero di serie
  - ✓ Risorse hardware quali CPU, RAM, disco
  - ✓ Sistema operativo e versione
  - ✓ Schede di rete
  - ✓ Hostname e indirizzo IP
  - ✓ Applicativi installati e versioni
- E dati informativi:
  - ✓ Funzione del sistema
  - ✓ Se il dispositivo è portatile e/o personale
  - ✓ Titolare responsabile della risorsa
  - ✓ Ufficio Associato
  - ✓ Ubicazione
- Per ogni oggetto denominato Configuration Item (CI), che viene definito da questi suoi attributi e dalle relazioni con gli altri CI
- Il CNDB storicizza ogni modifica di un attributo e/o di ogni relazione di ciascun CI

AAD

- L’Asset Automated Discovery AAD è indispensabile in una realtà di grandi dimensioni e complessa, per evitare di dover tenere l’allineamento dell’inventario a mano
- La piattaforma AAD scansiona in continuo gli spazi di indirizzamento e rileva i dati possibili
- Inoltre rileva asset ignoti o non autorizzati
- Rileva il sotto utilizzo

- NB – anche i dispositivi isolati dovrebbero essere raggiunti dalla piattaforma AAD

Software inventory /distribution

- Analogamente anche la piattaforma di software inventory è indispensabile in una realtà di grandi dimensioni e complessa, per evitare di dover tenere l'allineamento dell'inventario a mano
- La piattaforma di software inventory scansiona in continuo gli spazi di indirizzamento e rileva i dati possibili
- Inoltre rileva i software (o le loro versioni) ignoti o non autorizzati

- NB – anche i dispositivi isolati dovrebbero essere raggiunti dalla piattaforma

- I software della WHITE list devono poi essere installati in modo standard (configurazioni sicure: clone, hardening) → piattaforma di software distribution

LOG MANAGEMENT, SIEM, VULNERABILITY ASSESSMENT, ANTIVIRUS

- Per rendere efficace per la sicurezza la consapevolezza data dall'inventario è necessario che ciascun asset invii ad una piattaforma centralizzata tutti i log (decisi)
- Vanno inoltre rilevate le vulnerabilità (sistema di vulnerability) assessment
- I sistemi vanno protetti dal malware

- Tutti i dati devono essere inviati ad una piattaforma di Security Information Event Management (SIEM) che, correttamente configurata con riguardo a:
  - ✓ modello di Rischio
  - ✓ allarmi e impostazione reportistica
  - ✓ regole di correlazione

    garantirà
  - ✓ servizi di Monitoraggio
  - ✓ Detection
  - ✓ Incident Management

SICUREZZA INFORMATICA - COME

QUINDI DOBBIAMO METTERE IN ATTO AZIONI TECNICHE DI ELEVATA SPECIALITÀ E COMPLESSITÀ

E DOCUMENTARE

E RENDERE L'ORGANIZZAZIONE «SICURA»

COMPERIAMO SERVIZI DALL'ESTERNO?

CONSIP – APPENA AGGIUDICATO CONTRATTO QUADRO

SYSTEM MANAGEMENT 2

Sistema Sanitario Regionale

SICUREZZA INFORMATICA - COME

- **Servizi di "System Management"** ovvero il complesso dei servizi e delle attività volti a garantire la piena operatività delle infrastrutture tecnologiche dei Centri Elaborazione Dati, a mantenerne la perfetta efficienza, a garantire agli utenti la disponibilità e le prestazioni delle applicazioni su di esse installate e l'integrità dei relativi dati nonché a fornire il supporto necessario per garantirne il costante allineamento con l'evoluzione tecnologica del mercato ICT.

consip MEF Ministero dell'Economia e delle Finanze

acquistinretepa

Sistema Sanitario Regionale

- **Sevizi base**
  - Conduzione operativa sistemi open (Windows, Linux, Unix):
    - con presidio on-site;
    - in modalità remota;
  - Conduzione operativa sistemi mainframe (presidio on-site).
- **Servizi opzionali**
  - Monitoraggio notturno/festivo sistemi open:
    - con presidio onsite;
    - o in modalità remota.
  - Supporto specialistico:
  - Reperibilità;
  - Interventi fuori orario.
- **Servizi accessori**
  - Gestione infrastrutture non standard;
  - Manutenzione hardware;
  - Supporto ambienti client.

SICUREZZA INFORMATICA - COME

ESTERNALIZZAZIONE (SYSTEM MANAGEMENT): LA PANCEA?

- COSA CI PUÒ DARE?
  - COMPETENZE TECNICHE SPECIFICHE (ESPERIENZA SU GRANDI DATA CENTER, SU MOLTE TECNOLOGIE, SULLE ISO, …)
    - → ADATTABILI ALLA SANITA?
    - → ADATTABILI ALLA NOSTRA ORGANIZZAZIONE?
  - ON SITE PER L'ATTUAZIONE
    - → REPERIBILI CON IL DOVUTO SKILL?

Sistema Sanitario Regionale

SICUREZZA INFORMATICA - COME

ESTERNALIZZAZIONE (SYSTEM MANAGEMENT): LA PANCEA?

- COSA CI PUÒ DARE?
  - FLESSIBILITÀ
  - SGRAVIO DI RESPONSABILITÀ
- L'ONERE DI GESTIONE DEL CONTRATTO E LA RESPONSABILITÀ DI RUP E DEC – E LE LORO COMPETENZE
- L'ONERE DI AFFIANCAMENTO (IT, IC, PROVV, …)
- COSTI ELEVATI
- FREQUENZA DI RINNOVO CONTRATTUALE

SICUREZZA INFORMATICA - COME

INTERNA?

- COSTI BASSI
- FACILITÀ DI MOVIMENTO NELLA ORGANIZZAZIONE
- POCA FLESSIBILITÀ MA STABILITÀ

- ALTA RESPONSABILITÀ
- DIFFICILE REPERIMENTO (POSTO FISSO, STIMOLI TECNICI, …)

- RESISTENZA AL CAMBIAMENTO DELLA ORGANIZZAZIONE

SICUREZZA INFORMATICA - PROPOSTA

DEFINIZIONE DI UN MODELLO DI SICUREZZA AZIENDALE

- TECNICO
- ORGANIZZATIVO

CONOSCIUTO IN OBIETTIVI E MODI DA TUTTA LA DIREZIONE AZIENDALE E SOSTENUTO

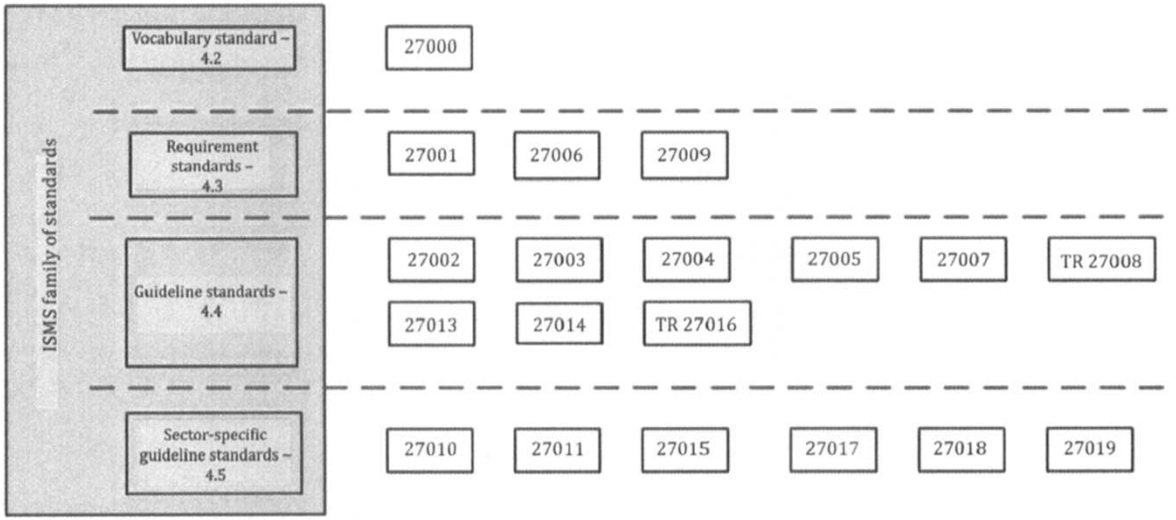
Sistema Sanitario Regionale

SICUREZZA INFORMATICA - PROPOSTA

CHE COMPRENDA

-PIANI DI ADEGUAMENTO E CONTEMPORANEA INNOVAZIONE FINO AL PUNTO DI CONVERGENZA A 5 ANNI

-AVVIAMENTO DI UN SISTEMA DI GESTIONE SICURA DELLE INFORMAZIONI SECONDO LE ISO 27000



Sistema Sanitario Regionale

SICUREZZA INFORMATICA - PROPOSTA

- KNOW HOW INTERNO ELEVATO
- ESTERNALIZZAZIONE
  - DEI PICCHI TECNOLOGICI
  - DELLA GESTIONE DOCUMENTALE
  - DI QUANTO SI È IN GRADO DI GOVERNARE
  - DELLE RISORSE UMANE REPERIBILI ON SITE E DA REMOTO
  - CONDUZIONE (MA NON LE SCELTE)
  - INNOVAZIONE (MA NON LE SCELTE)
- AGGIUNTA DI FUNZIONI AD HOC IN ORGANIGRAMMA

PROPOSTA

- Definizione di una funzione che operi per la gestione sicura delle informazioni secondo quanto standardizzato come “Sistema di Gestione della Sicurezza Informazioni” dalla famiglia di norme ISO 27000, e di supporto alla qualità documentata dei processi di mitigazione dei rischi e di tutte le attività.

- Definizione di una funzione dedicata alla conduzione tecnica della infrastruttura IT in house ed in cloud, ed alla erogazione dei servizi IT afferenti, a garanzia della sicurezza e della continuità dei servizi *core business e di supporto*.

PROPOSTA

Una organizzazione trasversale e capace di rispondere in maniera sinergica sui diversi argomenti, snella ed efficace, che garantisca uniformità di risposta agli obblighi dei diversi ambiti senza sovrapposizioni, e che nel contempo trasformi in opportunità di miglioramento – inteso come efficacia ed efficienza ed economicità – le nuove attività.

OPPORTUNITÀ

- Realizzare un atlante completo di processi e percorsi a disposizione per
  - migliorare i processi ed i percorsi razionalizzandoli in ottica di efficacia, efficienza ed economicità
  - definire indicatori di processo e misurarli
  - semplificare il turn over grazie alla documentazione
- Uniformare ed accrescere i livelli di sicurezza
- Migliorare le scelte di innovazione tecnologica

Sistema Sanitario Regionale

SIAMO PRONTI PER IL CAMBIAMENTO?

IRCCS materno infantile Burlo Garofolo
Regione Friuli Venezia Giulia
BURLO

ASUITS