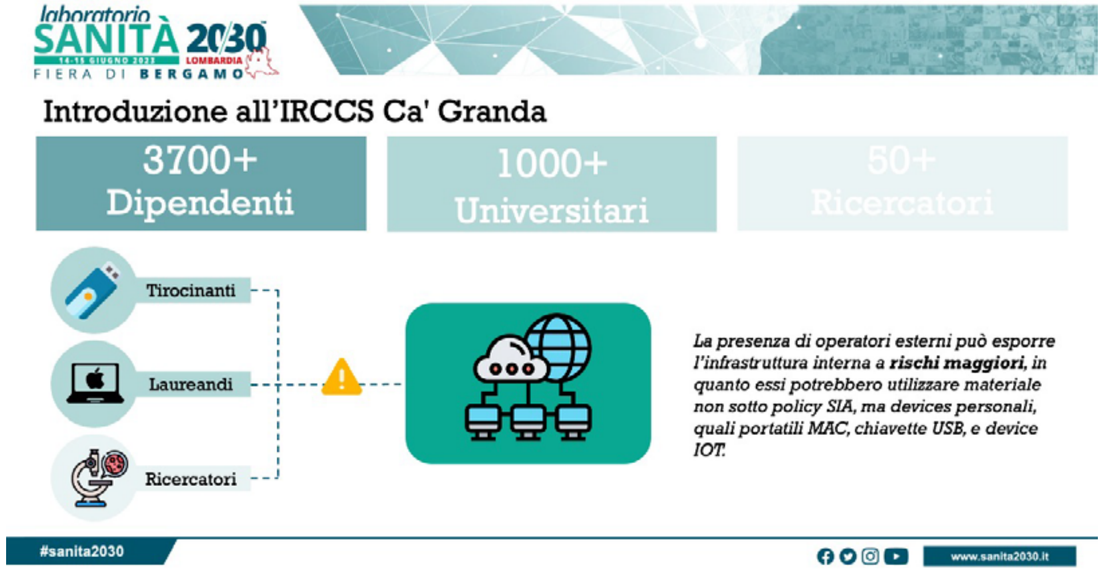
laboratorio SANITÀ 2030
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Policlinico di Milano Ospedale Maggiore
Fondazione IRCCS Ca' Granda

SC Sistemi Informativi: Dott. Fabrizio Pizzo

#sanita2030 www.sanita2030.it



Agiamo lungo 4 principali ambiti di sicurezza

Autenticazione a due fattori

MFA – Multi-Factor Authentication

PAM – Pugglable Authentication Modules

Sicurezza Dati

BaaS – Back-up as a Service

Sicurezza Server

Virtual Patching

Sicurezza Interna

NAC – Network Access Control

Sicurezza Autenticazione a due fattori *(in corso di implementazione)*

MULTI-FACTOR AUTHENTICATION

L'autenticazione del sistema VPN e di accesso alla casella elettronica saranno più sicuri, in quanto si dovranno inserire:

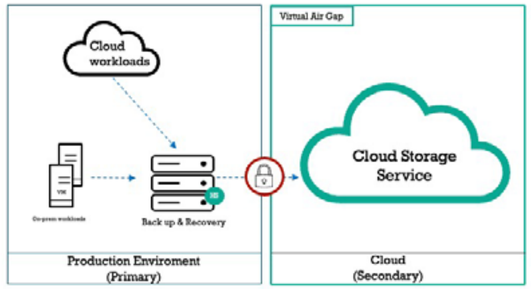
1. Il **PIN** o la **Password** (1° fattore) del proprio account
2. Il **codice numerico** (2°fattore) generato dall'app *FortiToken*

PIN/Password + Codice OTP da FortiToken

PRIVILAGE ACCESS MANAGER

Gli amministratori dei fornitori avranno accesso privilegiato su determinate macchine di produzione utilizzando la tecnologia PAM.

Sicurezza Dati



Ransomware Detection

- Monitoraggio e rilevazione di eventi anomali e predisposizione di una «Honey Pot», ovvero una «trappola» per dirottare il focus di un hacker verso macchine sacrificabili e studiarne il modus operandi di attacco.

Prevention

- Controllo restrittivo degli accessi e criptaggio per prevenire accessi non autorizzati

Recovery

- Backup su cloud isolato al di fuori della rete aziendale

Sicurezza Server

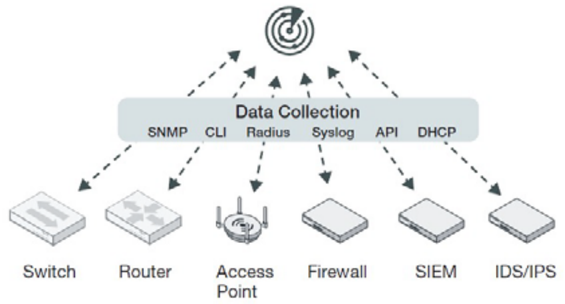
1. Vulnerability assessment
2. Identificazione criticità
3. **VIRTUAL PATCHING**
4. Remediation plan

Componente che, in caso di identificazione di una criticità in funzione di un Repository pubblico (CVE), inibisce il protocollo sotto attacco, in attesa di una nuova «patch» del fornitore.
Nel momento in cui non è possibile applicare alcun tipo di patch, il componente viene segmentato e messo in quarantena in una V-Lan sicura.

Sicurezza Interna

Implementazione del sistema NAC (Network Access Control).

Accesso sicuro ai nodi della rete da parte dei dispositivi

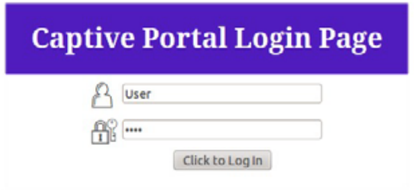


Sicurezza Interna

Il sistema NAC è fondamentale perché in grado di filtrare i contenuti malevoli all'interno dei device IoT che vengono collegati alla rete interna, difendendo da eventuali attacchi.

Captive Portal

Tra i moduli del NAC è previsto anche il Captive portale per l'autenticazione degli utenti Guest alla rete wireless aziendale.



Conclusioni

Le professionalità in ambito ICT richieste dalle nuove evoluzioni appena elencate, dimostrano la crescente necessità di queste figure all'interno delle Aziende Ospedaliere per permettere la governance delle strutture sanitarie.

Grazie per l'attenzione!

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Torna all'inizio