

CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ



Dott. Ing. Alessandro Picchi

ESTAR – Ente per i Servizi tecnici ed Amministrativi Regionali della Toscana

Direttore Area Tecnologie Informatiche Toscana Sud Est

Direttore U. O. C. Reti e Sistemi Area Vasta Toscana Sud Est

CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ

- Rivoluzione industriale: decenni e secoli.
- Rivoluzione informatica: anni e decenni.
- Sicurezza informatica: utopia a cui tendere.
- Analisi del rischio: sempre aggiornata rispetto al modificarsi continuo degli attacchi?



CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ

- Termini ed acronimi sempre nuovi che riassumono concetti sempre più vasti ed interdipendenti.
- Concetti che si modificano, si moltiplicano, si ramificano ancor prima di averli pienamente approfonditi.



CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ

- Una continua rincorsa fra innovazione tecnologica, disponibilita' di dati, necessità di informazioni.
- Rincorsa fra chi i dati li raccoglie, chi li interpreta, chi cerca di appropriarsene, chi cerca di proteggerli da un uso non etico.



CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ

- Fare sicurezza informatica: comprendere quello che succede.
- Per comprendere quello che succede: imparare da quello che è successo.
- Per imparare: studiare approfonditamente quello che è successo.
- **L'essere umano non riesce a farlo.**



CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ

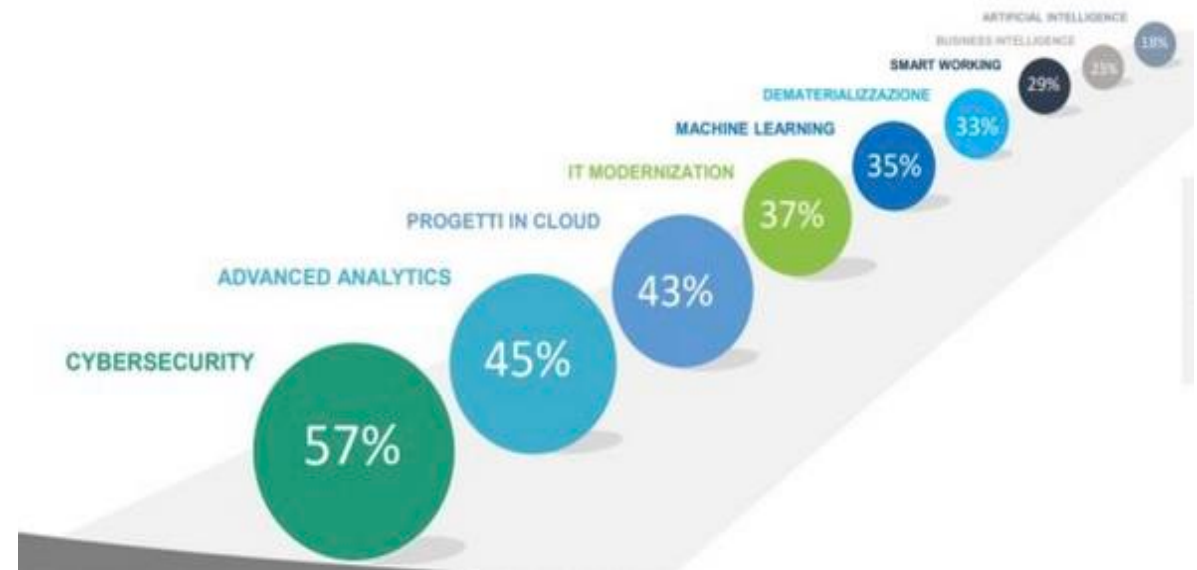
- AI: imparare da (vasto) pregresso per definire nuovi comportamenti.
- L'uso di AI negli attacchi informatici è ormai abitudine.
- Le imprese che usano AI devono attentamente valutare i rischi di sicurezza che lo stesso utilizzo introduce.



CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ

Un pacchetto di dati, durante i suoi “spostamenti”, viene trattato molte più volte per verificare che sia integro, non portatore di parassiti, che non per lo scopo principale oggetto dell’automazione informatica.

Gli investimenti in sicurezza informatica superano gli investimenti per il semplice trattamento dei dati.



CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ

- Immane complessità di gestione: solo per conoscere la normative bisognerebbe essere geni della memoria: quale esercizio, si legga (e memorizzi?...) il documento **“Linee di indirizzo percorso evolutivo sistemi medicali per telemonitoraggio”** di Age.Na.S. del maggio 2024, capitolo 5.



5. Quadro normativo

Questo capitolo fornisce una panoramica delle principali normative pertinenti, con particolare riferimento a quelle applicabili in ambito Telemedicina/FSE, privacy e sicurezza informatica. Le normative elencate offrono un contesto essenziale per guidare lo sviluppo, la produzione, l'acquisto e la gestione dei Sistemi Medicali in conformità con gli standard più elevati.

L'elenco delle normative di seguito predisposto non è esaustivo e deve essere interpretato nel contesto di un quadro normativo dinamico, soggetto a modifiche e aggiornamenti, incluso di Linee di indirizzo e raccomandazioni emanate periodicamente dagli enti preposti a livello nazionale ed europeo, tra cui il Garante per la Protezione dei Dati Personali, l'Agenzia per l'Italia Digitale (AGID), l'Agenzia per la Cybersecurity Nazionale (ACN), l'Autorità Nazionale Anticorruzione (ANAC) assicurando così una gestione dei dati conforme alle migliori pratiche e agli standard di sicurezza più aggiornati.

5.1 Sanità Digitale

Le normative e gli ulteriori riferimenti per la Telemedicina e il Fascicolo Sanitario Elettronico individuano il contesto, con particolare riferimento all'aspetto organizzativo, funzionale e tecnologico, all'interno del quale i Sistemi Medicali devono operare e cooperare rispetto alle finalità delle presenti Linee di indirizzo. Tra i principali riferimenti si annoverano quelli di seguito elencati.

- **Intesa Conferenza Stato-Regioni 20 febbraio 2014** "Telemedicina – linee di indirizzo nazionali".
- **Accordo Conferenza Stato-Regioni 17 dicembre 2020** "Indicazioni nazionali per l'erogazione di prestazioni di Telemedicina".
- **Decreto ministeriale del 29 aprile 2022** "Approvazione delle Linee di indirizzo organizzative contenenti il Modello digitale per l'attuazione dell'assistenza domiciliare".
- **Decreto ministeriale del 21 settembre 2022** "Approvazione delle Linee di indirizzo per i servizi di Telemedicina - Requisiti funzionali e livelli di servizio".
- **Decreto ministeriale del 30 settembre 2022** "Procedure di selezione delle soluzioni di Telemedicina e diffusione sul territorio nazionale, nonché i meccanismi di valutazione delle proposte di fabbisogno regionale per i servizi minimi di Telemedicina e l'adozione delle Linee di indirizzo per i servizi di Telemedicina".
- **Ministero della Salute – Dipartimento per la trasformazione digitale – AGENAS.** "Piattaforma di Telemedicina ed Ecosistema FSE Punti di contatto e raccordo tra i due progetti".
- **Decreto-legge n. 179 del 18 ottobre 2012** "Ulteriori misure urgenti per la crescita del Paese. Art. 12 - Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario".
- **Decreto del presidente del Consiglio dei ministri n. 178 del 29 settembre 2015.** "Regolamento in materia di fascicolo sanitario elettronico".
- **Decreto-legge n. 76 del 16 luglio 2020** "Misure urgenti per la semplificazione e l'innovazione digitale".
- **Decreto ministeriale 18 maggio 2022** "Integrazione dei dati essenziali che compongono i documenti del Fascicolo sanitario elettronico".
- **Decreto ministeriale del 20 maggio 2022.** "Adozione delle Linee di indirizzo per l'attuazione del Fascicolo Sanitario Elettronico".
- **Decreto del 7 settembre 2023.** "Fascicolo sanitario elettronico 2.0".

5.2 Privacy e protezione dei dati personali

Il documento Generale sulla Protezione dei Dati (GDPR) che stabilisce le basi per la raccolta, l'uso e la conservazione dei dati personali all'interno dell'UE, con particolare riferimento alla materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, modificato dal decreto legislativo 10 agosto 2018, n. 101.

informatica

Disciplinare la produzione, l'immissione sul mercato europeo e la gestione dei Sistemi Medicali, ed autorità hanno redatto diversi documenti in ambito sicurezza informatica. Tra i principali verranno quelli di seguito elencati.

MITA UE 2017/745 relativo ai dispositivi medici (MDR) che detta requisiti specifici di cybersecurity per i dispositivi medici (MDR) che detta requisiti specifici di cybersecurity. Il regolamento ha istituito un gruppo di coordinamento per la sicurezza dei dispositivi medici il quale, nel rilasciato il documento "Guidance on Cybersecurity for medical devices" il quale fornisce ai produttori una guida su come soddisfare i requisiti essenziali in ambito Cybersecurity e, in considerazione di ciò, ha suggerito diversi modi di fabbricazione, detta ulteriori considerazioni.

MITA UE 2017/746 che stabilisce le norme relative all'immissione sul mercato, la messa in commercio e la messa in servizio dei dispositivi medico-diagnostici in vitro (MDI) che stabilisce le norme relative all'immissione sul mercato, la messa in commercio e la messa in servizio dei dispositivi medico-diagnostici in vitro. Il regolamento è entrato in vigore il 17 gennaio 2023 e che dovrà essere recepita dagli stati membri entro il 17 ottobre 2024, che promuove l'adozione di misure per raggiungere un elevato livello di sicurezza e dei sistemi informativi in Europa, da estendere alle entità che operano in settori regolati dalla Direttiva NIS come quello legato ai dispositivi medici. Essa impone l'adozione di misure di cybersecurity anche nel settore sanitario quale "entità essenziale". Pertanto, il legislatore italiano adotti un atto legislativo utile a traghettare in considerazione gli aspetti cardine relativi alla cybersecurity, occorrente tenere in considerazione gli aspetti cardine relativi alla cybersecurity basati sull'analisi del rischio, la verifica della Supply Chain, i nuovi requisiti per la risposta agli incidenti (es. notifiche ad ACN e CSIRT Italia), il tracciamento di eventuali azioni svolte sull'ecosistema di strumenti tecnologici volti all'identificazione e tracciamento di eventi anomali.

indirizzo FDA (Food and Drug Administration) "Cybersecurity in Medical Devices: Quality System Requirements and Content of Premarket Submissions" finalizzate a fornire raccomandazioni in ambito cybersecurity per i dispositivi medici.

Il Garante del Sistema Medicale anche l'architettura delle componenti software e la sottostante deve essere adeguata all'installazione in-cloud, fino ad arrivare ad evoluzioni verso sistemi end-to-end e sistemi forniti in modalità SaaS, compatibilmente con le necessità di connessione e file componenti fisiche (dispositivi/strumenti) del Sistema Medicale. Per tale aspetto si segnalano i seguenti riferimenti.

AGID n. 2/2017 riguardante le misure minime di sicurezza ICT per le pubbliche amministrazioni, re per contrastare le minacce Cyber.

Page 11 di 31

CYBERSECURITY PROGETTO SSRT

Approfittando delle possibilità concretizzate dai finanziamenti PNRR, ESTAR ha ritenuto opportuno verificare se quanto già investito in sicurezza informatica nel SSRT potesse evolvere in maniera più organica e metodica verso un sistema vero e proprio dedicato alla sicurezza informatica della sanità Toscana.



CYBERSECURITY PROGETTO SSRT: ECOSISTEMA DI RIFERIMENTO

- Il Piano Nazionale di Ripresa e Resilienza (PNRR);
- Il Piano Triennale per l'Informatica nella PA (AGID) 2024-2026;
- DGRT 145/2023 che descrive “CSIRT Toscana”, con tutte le sue articolazioni e interazioni;
- SOC RT il cui perimetro è R.T. e quanto gestito direttamente da R.T. (rif. RT/Vannuccini);
- SOC SCT il cui perimetro è quanto gestito direttamente da SCT (rif. SCT/Chiota);
- Strumenti e servizi esplicitati nella scheda di progetto dove con SOC si intende SOC ESTAR, il cui perimetro è quanto gestito direttamente da ESTAR presso AA.SS. ed Enti SST e su e-Health presso SCT.



CYBERSECURITY PROGETTO SSRT: DELIBERA ESTAR n. 44/2024



DELIBERAZIONE DEL DIRETTORE GENERALE *

N° 44 del 06/02/2024

Oggetto: ADOZIONE QUARTA PARTE VI TRANCHE SCHEDE PROGETTO PNRR MISURA M6 C2 1.1.1. DIGITALIZZAZIONE DEA DI I E II LIVELLO	
Immediatamente eseguibile: SI	
Struttura proponente: DIRETTORE AMMINISTRATIVO	
Importo di Spesa: 0,00	
Proposta di delibera: 328	Del: 06/02/2024
Hash documento proposta formato .pdf (SHA256): 4f9294587c4eee0c42e297382eca5797bef4cd0a310e90b27af8e6069d48df56	

Vista le delibere ESTAR n. 46/, n. 4/8, n. 51/ del 2022 e n. 104, n. 133, n. 249, n. 2/0, n. 291, n. 360, n. 361, n. 363, n. 387, n. 388, n. 410 del 2023 e n. 5 del 2024 delle tranche di progetti PNRR ICT DEA I e II livello;

Vista la proposta di schede dei progetti finanziabili con il PNRR inviata da ESTAR alla Direzione Sanità, Welfare e Coesione Sociale della Regione Toscana relativa alla III tranche inviate in data 15/02/2023 (protocollo n. 9349 agli atti), con particolare riferimento alla scheda relativa alla Cyber Security;

Visti gli approfondimenti e le analisi del progetto svolte da Regione Toscana in collaborazione con ESTAR al fine di giungere a definirne i contenuti in linea con gli obiettivi di sistema definiti dalla Regione stessa;

Vista l' autorizzazione di Regione Toscana del 02/02/2024 (agli atti) con cui si prende atto dell'approvazione della scheda progetto:

SCHEDA	Oggetto	Importo Schede (IVA inclusa)
2174CYBER	Progetto di Cyber Security	17.543.295 €
TOTALE 4 PARTE VI TRANCHE DEA		17.543.295,00 €

Considerata la necessità di procedere all'approvazione della stessa al fine di avviare il progetto nonché il percorso di adesione alle convenzioni Consip vigenti tramite le procedure definite nei verbali del Gruppo di Coordinamento PNRR di ESTAR;

CYBERSECURITY PROGETTO SSRT: OBIETTIVO

- Acquisizione delle soluzioni (hardware, software, licenze e certificati) e dei servizi per il potenziamento dei sistemi IT in ambito di cybersecurity al fine di aumentare il livello complessivo di sicurezza informatica del SSRT;
- previsione attuale di crescita di 24 mesi;
- soluzioni corredate da servizi di assistenza e manutenzione dei brand produttori per 24 mesi, e da servizi di messa in esercizio, configurazione e tuning;



CYBERSECURITY PROGETTO SSRT: OBIETTIVO

- servizi di conduzione progetto necessari alla messa in opera e piena attività delle soluzioni sotto coordinamento del servizio SOC ESTAR (individuazione dei perimetri di competenza della conduzione operativa);
- servizio di formazione/addestramento per il personale tecnico ICT ESTAR con l'obiettivo di innalzare il livello di conoscenza sulla cybersecurity;
- attivazione della risorsa SOC ESTAR e definizione delle procedure operative che SOC ESTAR può garantire.



CYBERSECURITY PROGETTO SSRT: RIASSUNTO DEI SERVIZI IN OBIETTIVO

- Aggiornamento/attivazione firewall perimetrali presso I presidi sanitari considerati importanti;
- attivazione infrastruttura layer 3 che permetta di segmentare le reti sanitarie in vlan suddivise con attivazione di routing/filtering tra le vlan stesse via firewall;
- centralizzazione della gestione e del logging dei firewall;

CYBERSECURITY PROGETTO SSRT: RIASSUNTO DEI SERVIZI IN OBIETTIVO

- utilizzo in maniera diffusa e mirata di sonde per l'analisi del traffico di rete orizzontale;
- attivazione di server per l'analisi in sandbox di attività sospette;
- attivazione di sistemi di sicurezza dedicati alla protezione di aree che ospitano apparati con gestione informatica obsoleta/insufficiente;

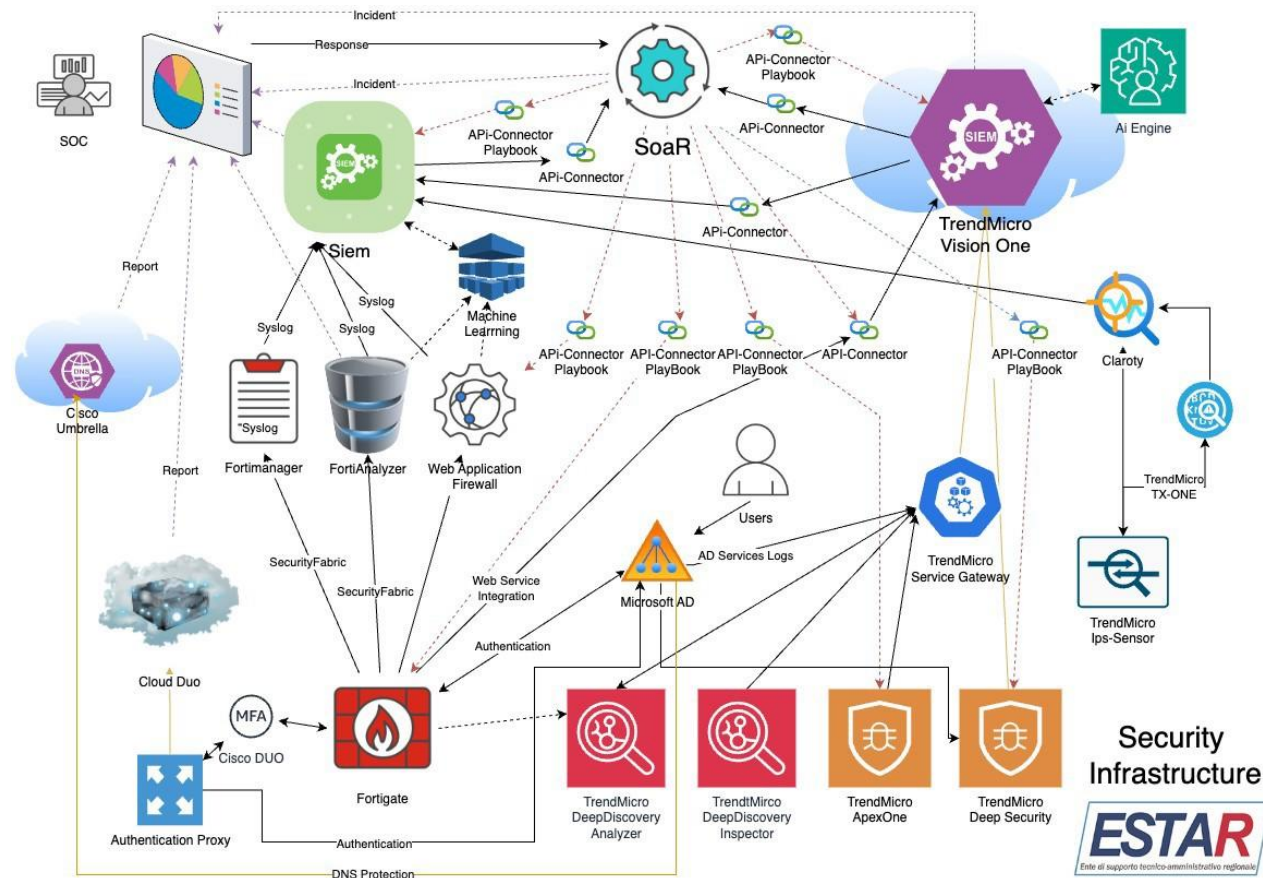
CYBERSECURITY PROGETTO SSRT: RIASSUNTO DEI SERVIZI IN OBIETTIVO

- attivazione protezione dei traffici delle arce che ospitano server;
- attivazione dell'utilizzo di dual factor authentication per l'accesso alle risorse di rete dall'esterno della rete stessa;
- attivazione dell'analisi dei traffici DNS;
- attivazione di una piattaforma di gestione dei certificati digitali;

CYBERSECURITY PROGETTO SSRT: RIASSUNTO DEI SERVIZI IN OBIETTIVO

- attivazione di risorse risorse Web Application Firewall;
- evoluzione di conoscenze, esperienze, infrastrutture per consentire la pianificazione e la messa in opera di sistemi centralizzati di visibilità, analisi e controllo tramite apposite piattaforme SIEM/SOAR;
- attivazione di supporto specialistico di secondo livello.

CYBERSECURITY PROGETTO SSRT: LA COMPLESSITÀ



CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ RIFLESSIONI

- È possibile correre a queste velocità?
- È possibile rimanere professionisti validi all'interno di questo vortice?
- Quali sono gli strumenti minimi per rispondere?





Forum Risk Management

obiettivo sanità salute

26-29 NOVEMBRE 2024
AREZZO FIERE E CONGRESSI

19

CYBERSECURITY ED AI: SFIDE AD ALTA VELOCITÀ RIFLESSIONI

