Analisi Comparativa sulla Sicurezza delle Infrastrutture di Rete Aziendali

Facoltà di Ingegneria dell'informazione, informatica e statistica
Corso di Laurea in Informatica

SAPIENZA
UNIVERSITÀ DI ROMA

Candidato: Mattia Giordano
Matricola: 1884283
Relatore: Prof. Alessandro Checco
Anno Accademico**:** 2024/2025

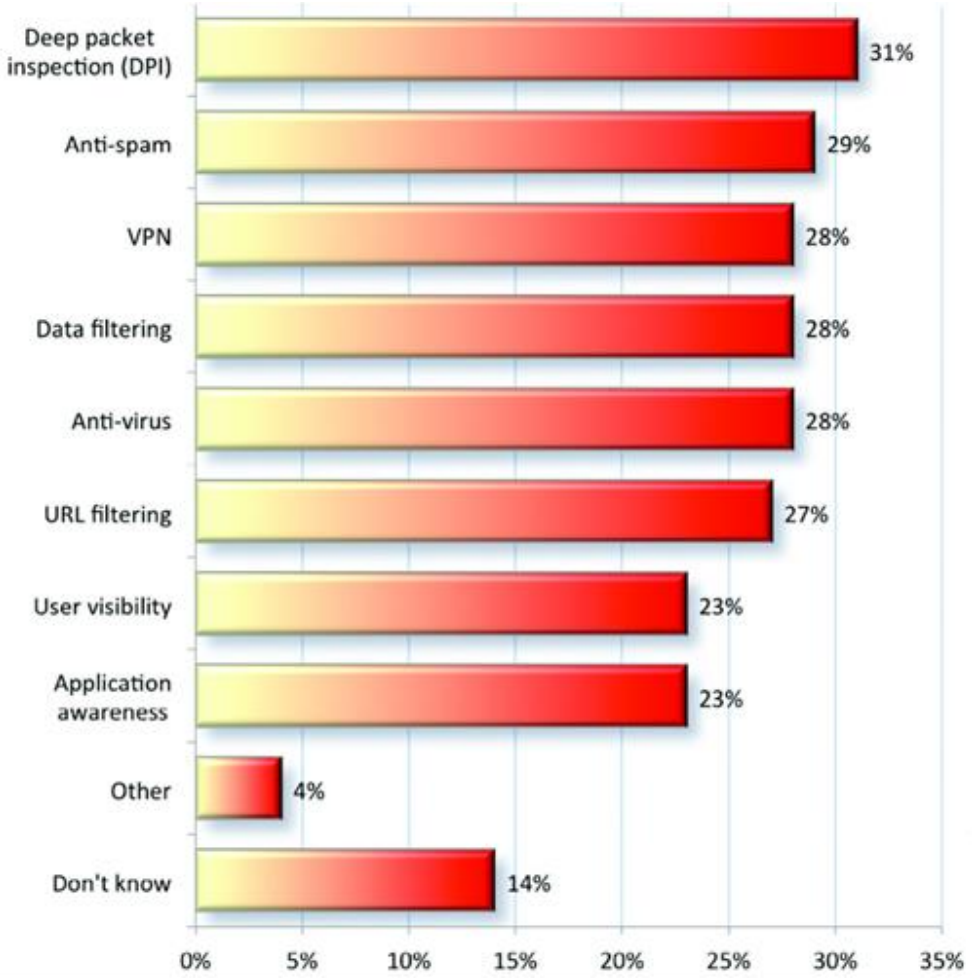
Introduzione e Analisi del Problema

- Ruolo centrale delle reti nella società di oggi.
- Coinvolgimento di enti **governativi**.
- La **negligenza**, i ransomware e il caso **Colonial Pipeline**.

Strumenti e fonti come IEEE Xplore, NIST, CISA, NIST NVD, NSA, Google Scholar e **sondaggi** all'interno di aziende italiane, sono stati il centro della **metodologia** utilizzata.

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

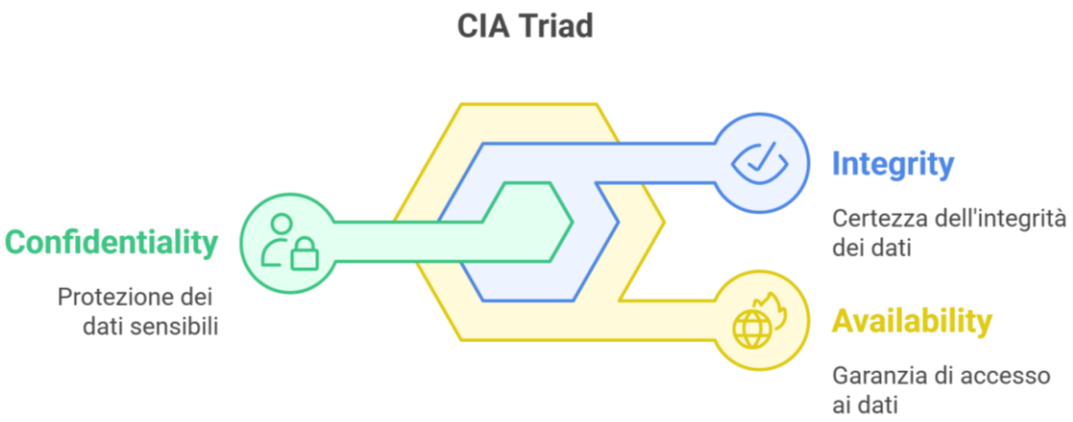
Contrasto tra Sicurezza e Performance



Principi di base per una Progettazione Sicura delle Reti

Nella raccolta di informazioni per la ricerca, è emerso da subito l'importanza di stabilire in primis i **requisiti** e gli **obiettivi** che si vogliono raggiungere dalla propria rete in base al **tipo di utilizzo** che se ne farà.

- Difesa in Profondità
- Minimo Privilegio
- Separazione dei Ruoli
- Sicurezza by Default
- Modularità
- Fail Safe
- Isolamento



Gestione e Manutenzione delle Reti

- Sviluppo di vari **framework** di sicurezza negli anni
- Importanza delle **policy** e dell’organizzazione **interna**
- **Monitoring** della rete e sistemi dedicati alla prevenzione

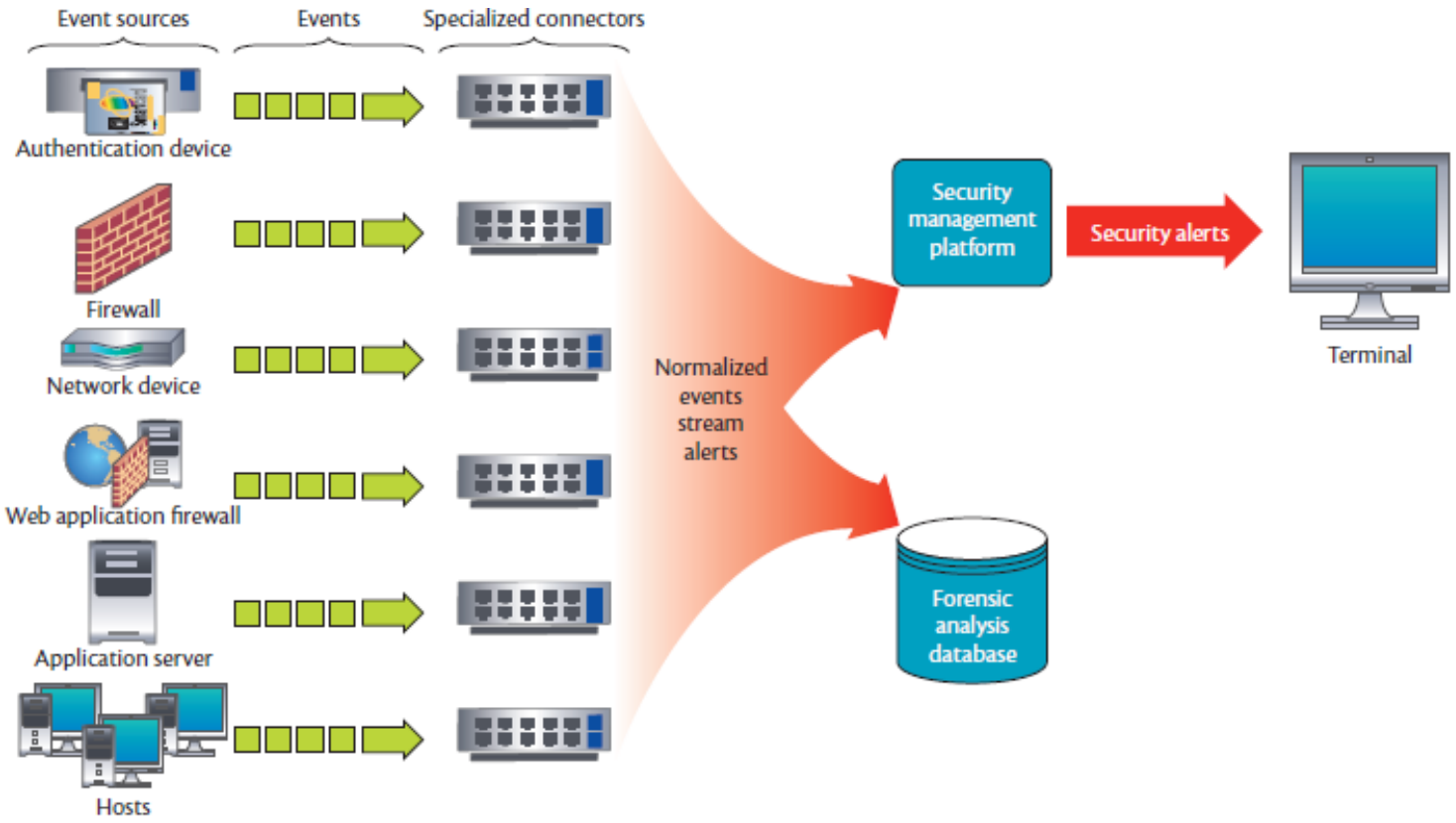
Il Monitoraggio per la Gestione della Rete

Una gestione ottimale della rete è ottenuta grazie a tecniche di monitoring Come l'**active** monitoring, il **passive** monitoring o l'**SNMP** monitoring.

Un altro strumento fondamentale è quello del **Security Information and Event Management**

- Traffico sintetico o reale
- Accuratezza
- QoS
- Valutazione delle performance
- Funzionalità di IDS/IPS
- Analisi del traffico
- Costi
- Utilizzo di agenti o sensori
- Servizio di alerting
- Tradeoff corretto

Funzionamento Superficiale di un SIEM



Analisi di un Caso Reale – Poste Italiane

Nella nostra ricerca abbiamo approfondito il caso reale del monitoraggio della rete all'interno del gruppo di **Poste Italiane**.

- Protezione per tutti gli endpoint
- Integrazione con **MITRE ATT&CK**
- Protezione da **phishing** nelle email
- Integrazione con Microsoft **Sentinel**

Patch Management

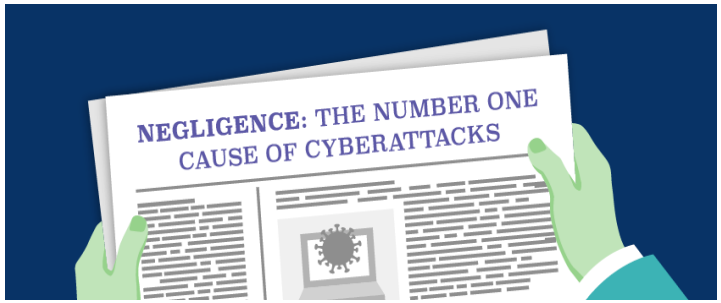
Dato il forte sviluppo della tecnologia è importante manutenere l'hardware e il software che viene venduto o utilizzato.

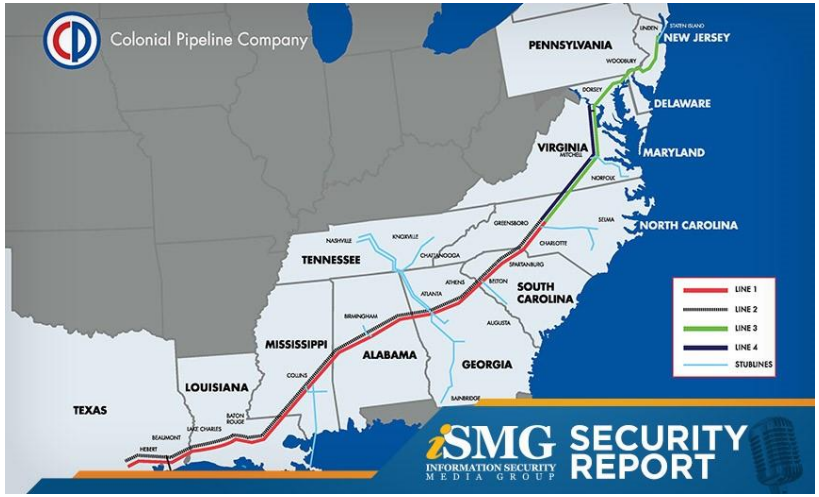
Questo aspetto è sempre stato molto trascurato negli anni, ma ha portato diverse volte ad eventi critici, come nel caso del **ransomware** WannaCry.

L'applicazione di una patch richiede anche del **testing**, in particolare se riguarda apparecchiature critiche, lasciando vulnerabile l'**ambiente** di **produzione** per un periodo di tempo.

Il caso Colonial Pipeline – Esempio Reale

- Società di distribuzione di prodotti petroliferi americana
- Cattiva igiene delle **password**
- Implementazione di **MFA**





- Vulnerabilità **SMB** di Windows
- Blocco dovuto a impossibilità di fatturazione dei clienti

Automated Context-aware Vulnerability Risk Management - ACVRM

- Nato per alleggerire il carico per il personale IT
- **Automatizzazione** dell'applicazione delle patch
- Tasso di rischio accettato
- Framework con patch **pesate** e **prioritizzate**
- Riduce al minimo l'intervento umano
- Storico prioritizzazione e pesi ottiene maggior successo

Nuove Tecnologie

- Tendenza all'adozione di architetture **Zero Trust come visto per i BYOD**
- Integrazione di soluzioni di **Machine Learning** e **AI** nel networking

Limiti

- Il costo è spesso un limite per le PMI
- Open Source
- Costi accessibili permettono di non trascurare la sicurezza

Riflessioni Personali

La ricerca è nata dalla **curiosità** su come rendere **più sicure** le **reti**, parte integrante della nostra vita. Ha fatto emergere un senso di **responsabilità**, mostrando l'impatto delle negligenze sulla società.

Inizialmente, **l'obiettivo** era creare un **framework** di sicurezza **universale**, ma si è rivelato **troppo ambizioso**. Di conseguenza, l'attenzione si è spostata sulla definizione di linee guida e strumenti utili per la cybersecurity nel networking

SAPIENZA
UNIVERSITÀ DI ROMA

Grazie per l'attenzione