WORKSHOP GARR 2023

NET MAKERS

Sinergie in ambito cyber: *responsible disclosure* in Ateneo

Ilaria Comelli

Università di Parma

Chi siamo: UO Sicurezza IT

Ci occupiamo di sicurezza informatica attraverso attività di:

- monitoraggio del livello di sicurezza delle risorse elettroniche dell'Ateneo al fine di prevenire gli incidenti di sicurezza e di indagarne le cause
- indirizzo per le azioni di adeguamento alla normativa di settore
- stesura di politiche di sicurezza IT
- analisi del rischio e relativi piani di mitigazione e piani di continuità operativa
- valutazione degli aspetti di sicurezza su servizi, prodotti e tecnologie da adottare
- indirizzo e collaborazione in ambito formativo sui temi della sicurezza dei dati

Contesto universitario: punti di debolezza

eterogeneità delle risorse informatiche e dei soggetti che le usano

difficoltà nel definire e far rispettare regole stringenti di sicurezza ad alcune categorie di utenti

necessità di interagire e mettere in condizione di lavorare tanti soggetti esterni (ospiti, ***visiting professor***, studenti Erasmus, docenti a contratto, borsisti, assegnisti etc.)

risorse umane sempre più limitate (e sempre meno giovani...)

scarsa attrattività dei concorsi pubblici

Contesto universitario: punti di foza

- Pluralità di risorse
  - Docenti
  - Studenti
  - Risorse economiche
- Relazioni e rete
- Reputazione
- Interesse da parte di aziende e professionisti a costruire collaborazioni

Che fare?

Cercare sinergie!

Dialogo con i docenti di ambito cybersecurity

Docenti del corso di laurea di:

Ingegneria Informatica
Scienze Informatiche

Creazione di
un **indirizzo in cybersecurity**
per il corso magistrale di Scienze Informatiche

Sinergie con gli studenti

Tirocini
Tesi di Laurea (triennale e magistrale)

Sinergie con gli studenti

Formazione e supporto alla partecipazione a

CyberChallenge

Possibili future sinergie con gli studenti

Associazione studentesca
Spin-off
Borse di studio
Dottorati

Collaborazioni più significative

Simulazione di **phishing** per la formazione mirata del personale dell'azienda ospedaliera di Parma.

Sperimentazione di **Honeypot** a bassa, media e alta interazione.

Applicazione Web per l'installazione autonoma di un **agente Cloud Vulnerability Management**.

Ricerca di vulnerabilità su risorse informatiche dell'Ateneo.

Strumenti e procedure di rilevazione vulnerabilità sui **siti web**

Modalità di progettazione e realizzazione dei **Pen Test**

Confronto e sviluppo di piattaforme di **Cyber-range**

CyberChallange e **CTF** nazionali e internazionali.

Sperimentazione di Honeypot a bassa, media e alta interazione

Bassa interazione
Registra solo le scansioni di rete su porte TCP/UDP.

Media interazione
Viene esposta una shell emulata con funzionalità limitate.

Alta interazione
Funzione di proxy verso un sistema operativo completo (Linux o Windows).

Honeypot: caratteristiche della configurazione

12 VulnBox attive:
- 6 di sperimentazione (virtuali)
- 6 in produzione (fisiche);

diverse tecnologie Honeypot su ogni macchina

installazione e configurazione centralizzata delle VulnBox

raccolta dati centralizzata dalle VulnBox in sperimentazione.

Obiettivi futuri:

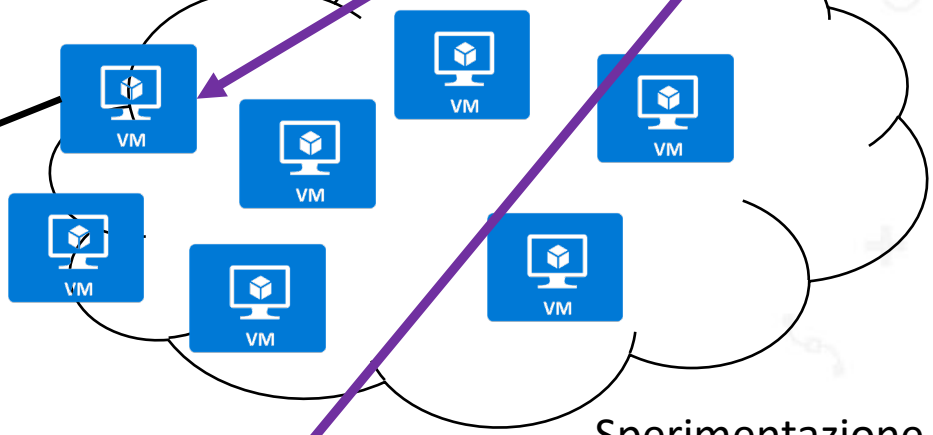
segnalazione e raccolta informazioni (IP, protocolli, etc.) delle risorse interne alla rete di Ateneo che contattano le VulnBox e cercano di sfruttarne le vulnerabilità presenti

VulnBox fisiche posizionate in punti strategici della rete di Ateneo.

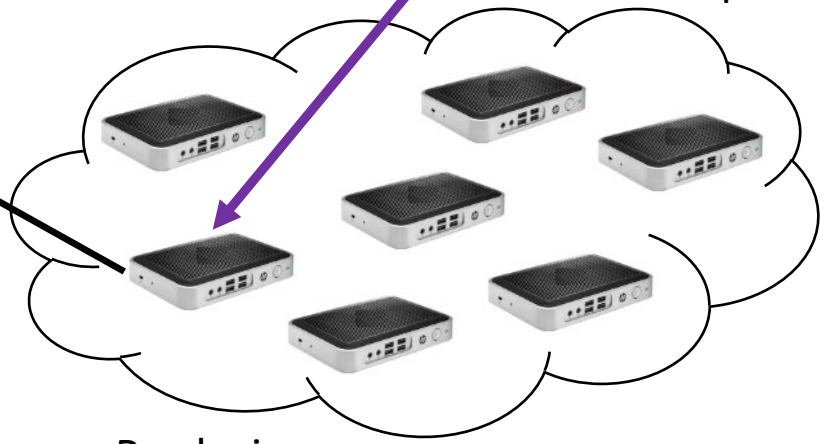
raccolta dati su sistemi in produzione

Honeypot: schema soluzione realizzata

Server
deploy e log



Sperimentazione



Produzione

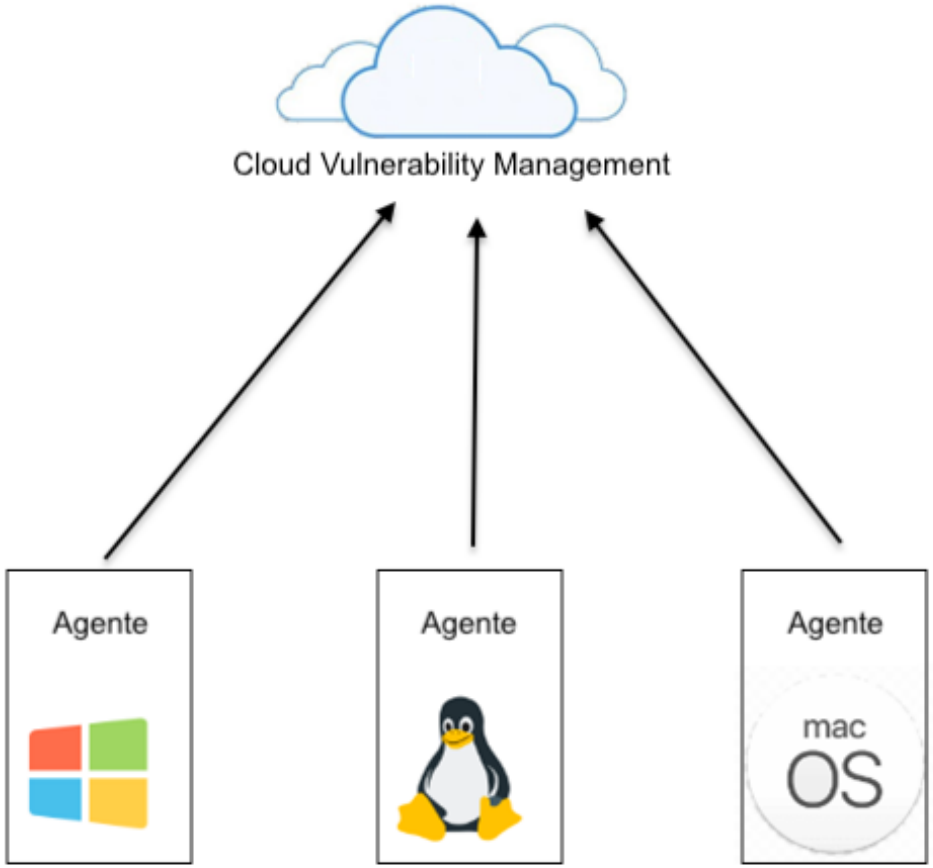
Applicazione Web per l'installazione autonoma di un agente Cloud Vulnerability Management

Prima del 2020 agent installato sulle PDL gestite dall'Area Sistemi Informativi (no PC personali, no PC ricerca).

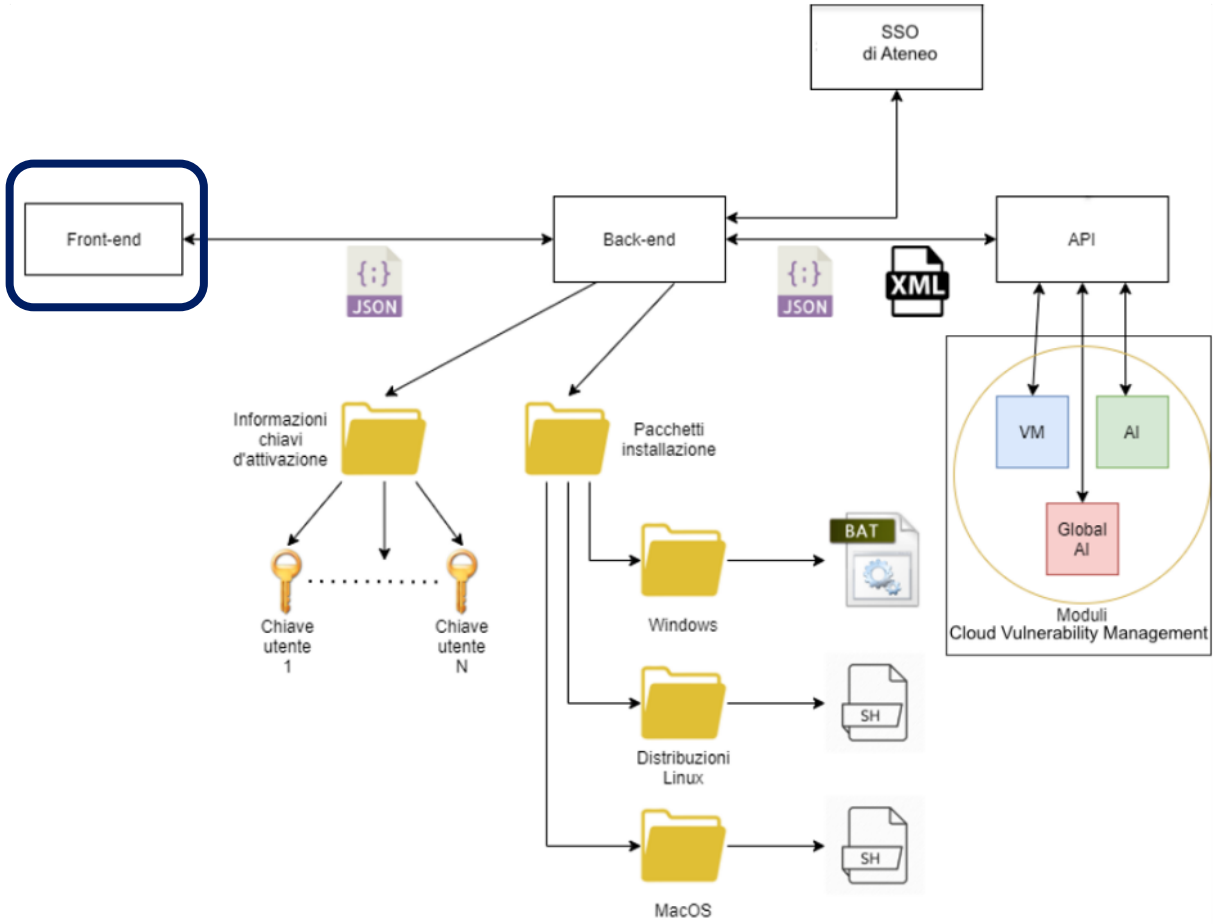
A inizio 2020 il perimetro della rete si vanifica. Tutti improvvisamente telelavorano e c'è la necessità di monitorare anche le PDL non gestite centralmente.

Viene sviluppata un'applicazione web che guida gli utenti nell'installazione autonoma dell'agent che si collega al Cloud Vulnerability Management.

Agenti e Cloud Vulnerability Management



Cloud agent VM: schema della soluzione realizzata

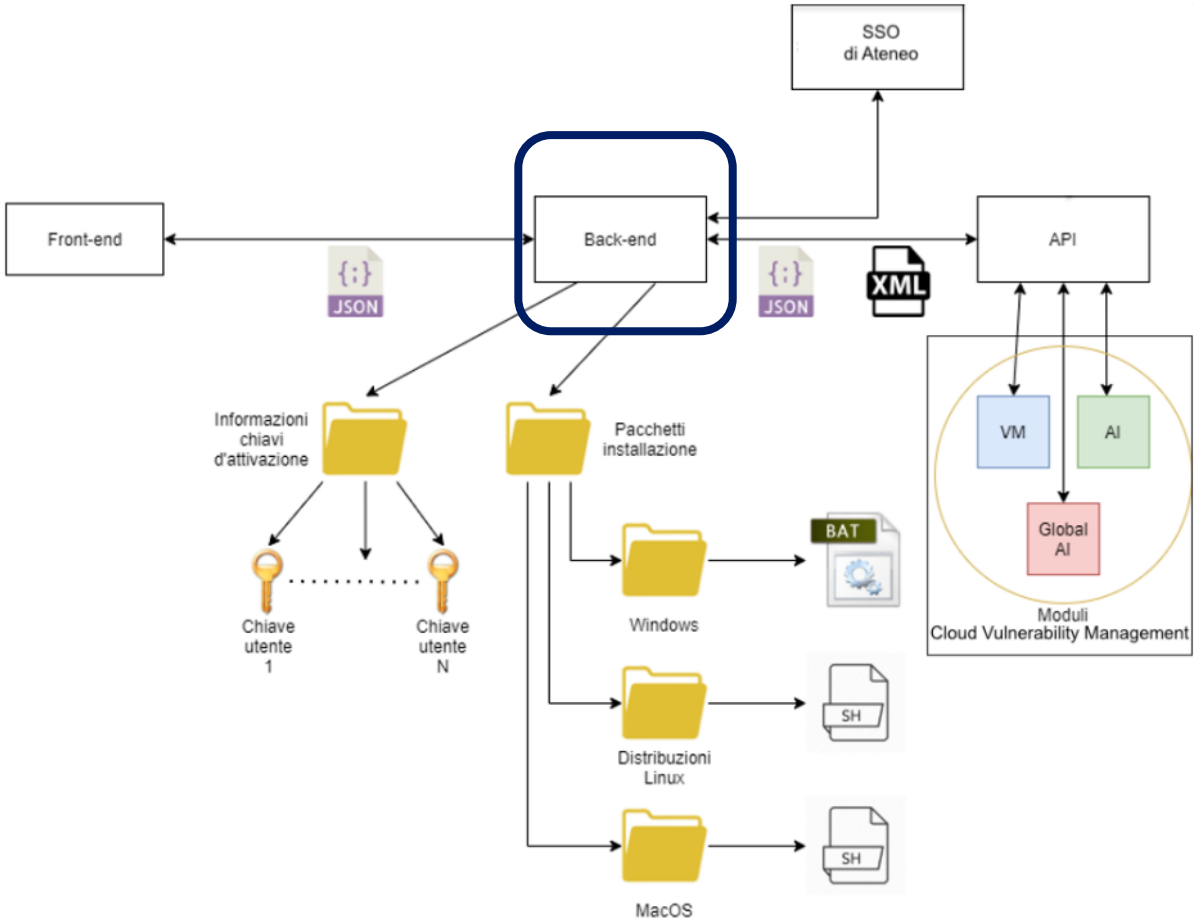


Lato front-end

Interfaccia mostrata all'utente per interagire con l'**applicazione web**.

Accessibile dopo aver effettuato la procedura di **autenticazione** mediante il **server SSO** di Ateneo.

Cloud agent VM: schema della soluzione realizzata



Lato back-end

Contiene la **logica** per gestire le informazioni relative alle **chiavi d'attivazione** di ogni utente,

fornisce gli **installer** degli agenti suddivisi per sistema operativo e restituisce al lato **front-end** le informazioni ottenute dalle **API**.

Ricerca di vulnerabilità su risorse informatiche dell'Ateneo.

Attraverso CyberChallenge gli studenti sviluppano tanti tipi di competenze di ambito cybersecurity, in particolare nel campo della ricerca di vulnerabilità software.

Abbiamo cercato di indirizzare le loro capacità in modo che potessero confrontarsi con scenari reali, in particolare trovando vulnerabilità su risorse informatiche dell'Ateneo (sempre in modo responsabile).

Sono state trovate diverse vulnerabilità, quella che vi presenteranno è probabilmente la più significativa perché si tratta di uno zero-day.

Grazie per l'attenzione

sicurezza.it@unipr.it

Con il contributo di:

Raffaele Cicchese
Giuseppe Tamborino