Paolo Masala - Intervista al Forum ICT Security 2018

Author : Redazione

Date : 13 novembre 2018

Paolo Masala

Partendo dalle esperienze fatte sul mercato durante le attività di vulnerability assessment, abbiamo compreso quanto utile possano essere strumenti che collezionano informazioni puntuali sulle debolezze della infrastruttura e correlandole con le caratteristiche dei servizi digitali erogati, possano dare una visibilità dei livelli di rischio per singola risorsa o per l'intera infrastruttura. La piena conoscenza delle proprie vulnerabilità è la base per decidere come proteggersi. Abbiamo quindi sviluppato una nuova soluzione software Sentinet3 Security Analyzer che attraverso discovery automatiche rileva le vulnerabilità presenti ed evidenzia ai vari livelli funzionali, gli indici di rischio e le attività necessarie per la mitigazione. Indispensabile per programmare le azioni di remediation e di adeguamento continuo della strategia di difesa. Molto utile per le organizzazione che, sensibili alle tematica di sicurezza, vogliono implementare processi automatici ed Audit continuativi per tenere costantemente il rischio sotto controllo.

Con il Security Analyzer è possibile gestire i rischi associati alle vulnerabilità intrinseche della infrastruttura ed alla superficie di attacco. In realtà il fattore umano è ancora molto importante. Negli ambienti Enterprise dove siamo presenti con la nostra piattaforma di monitoraggio Sentinet3, vediamo che la maggior parte degli eventi che creano problemi o criticità nelle infrastrutture IT, dipendono da errori umani. Quindi per una gestione globale dei rischi di sicurezza è fondamentale creare una opportuna cultura sulla sicurezza informatica a tutti i livelli. Per questo tramite la nostra struttura di formazione ed i nostri docenti eroghiamo corsi specialistici per gli addetti alla gestione della sicurezza, ma anche percorsi di sensibilizzazione su tutti gli utenti finali affinché ci sia una consapevolezza dei potenziali rischi che affliggono gli end point; Pc , ma oggi anche tablet e smartphone.

Il ventaglio dei temi caldi è molto ampio ed argomentato bene dai vari soggetti istituzionali che rilasciano studi specifici in merito. Da parte nostra rileviamo che oltre all'innalzamento della qualità delle tecniche di attacco da parte del cybercrime da cui bisogna difendersi in modo sempre più puntuale, i moderni trend evolutivi che impongono l'adozione di nuove tecnologie come il cloud, i container con interi datacenter guidati da logiche software defined, impongono una rivisitazione delle strategia di difesa. La flessibilità richiesta dal business, di gestione on demand delle risorse deve essere sempre accompagnata da processi gestionali che mantengono alti gli standard di sicurezza informatica. Da qui la necessità di strumenti automatici ed intelligenti che aiutano l'uomo ad implementare un approccio proattivo piuttosto che reattivo. La minima distrazione può costare cara sia in termini economici che di reputazione aziendale.

Domande:

1. Quale messaggio/esperienza condividete qui al Forum per i partecipanti all'evento?
2. Quindi con questa soluzione è possibile avere sotto controllo tutti i fattori di rischio?
3. Quali sono secondo voi le sfide più importanti per il prossimo futuro nel disegnare le strategia di difesa?

Vai all'evento Forum ICT Security 2018