Cloud un nuovo perimetro di sicurezza

Rendere sicure le reti negli scenari cloud based

Nell'era moderna del cloud computing la tendenza è quella di spostare i propri workload nel cloud pubblico e di utilizzare scenari cloud ibridi. La sicurezza è spesso un elemento inibitore per l'utilizzo di ambienti cloud. Il perimetro di sicurezza non è più rappresentato dalla rete fisica on-premises, bensì dall'estensione verso il cloud pubblico. L'utilizzo di Azure per le proprie applicazioni e servizi consente di usufruire di un ampio set di funzionalità e strumenti di sicurezza integrati nella platform. In questo workshop sono presentate le security best practices in ambito network nel mondo Azure, le linee guida e gli accorgimenti utili per utilizzare al meglio le potenzialità presenti nella piattaforma. La protezione delle risorse in presenza di architetture ibride assume un'importanza strategica. Con Microsoft Azure Security Center è possibile monitorare lo stato di sicurezza delle risorse, attivare un'efficace protezione dalle minacce e certificare la compliance rispetto agli standard di sicurezza industriali.

Technology value

L'estensione della propria rete verso il cloud e l'erogazione di nuovi servizi attraverso il cloud introduce una nuova sfida per gli amministratori di rete e della sicurezza. Il workshop illustra come Microsoft Azure sia in grado di realizzare architetture di rete ibride e dotate di tutti i sistemi di sicurezza richiesti in questi contesti. Adottare soluzioni in grado di coniugare le moderne tecnologie di machine learning e big data, insieme all'esperienza maturata da grandi vendor del settore, per ottenere un approccio completo alla sicurezza delle applicazioni e dei sistemi. Il tutto per ambienti ospitati sia nel cloud pubblico che presso i data center locali. Con Azure Security Center è possibile verificare il proprio livello di sicurezza, usufruire delle raccomandazioni per elevare il proprio punteggio e proteggere i workload, diminuire il tempo di identificazione di nuove minacce di sicurezza e identificare, dare una priorità, rimediare il più velocemente possibile le vulnerabilità.

Business value

Il workshop presenta le soluzioni Microsoft Azure per la realizzazione di reti ibride e sicure, che consentano all'azienda di sfruttare le potenzialità del cloud allo scopo di continuare la propria evoluzione IT mantenendo e aumentando la propria competitività sul mercato. Per garantire la continuità operativa e di servizio di un IT è indispensabile prevenire, rilevare e rispondere alle minacce di sicurezza che interessano le risorse distrubuite su ambienti eterogenei. Con Azure Security Center è possibile verificare il proprio Security Posture, identificare le vulnerabilità e procedere alla loro risoluzione, rilevare nel minor tempo possibile nuove minacce e agire velocemente per contrastarle. È inoltre possibile certificare la compliance agli standard di sicurezza adottati dall'azienda.

Output

Materiale presentato ed elaborato durante il workshop.

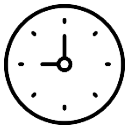
WORKSHOPS

Microsoft FastTrack Ready Partner

Area

Fabric

Durata



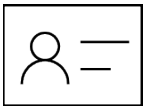
4h

PWS-18-28

Tecnologie coinvolte

Azure Networking, Azure Firewall, Application Gateway and Web application protection, Azure DDoS Protection, Azure Security Center, Azure Sentinel

A chi è rivolto



CSO, CTO, IT Pro

PROGEL SpA
Via Due Ponti, 2 - 40050, Argelato (BO)
Via Antonio Gramsci, 54/L 42124 Reggio Emilia
+39 051 66 39 411
info@progel.it

Gold Microsoft Partner

Microsoft