Accesso remoto sicuro per collaboratori esterni e terze parti

Tutte le organizzazioni IT hanno la necessità di garantire un accesso ai propri sistemi a collaboratori esterni e in generale alle cosiddette terze parti, che includono consulenti, service provider, fornitori e partner. Quando queste risorse esterne all'azienda ottengono un **accesso privilegiato a sistemi critici**, la situazione diventa particolarmente delicata da gestire perché mette a rischio la sicurezza dell'organizzazione.

Dall'ultimo "Global Security Report", pubblicato da TrustWave, emerge che uno dei maggiori punti di vulerabilità è proprio collegato alla gestione di questi accessi, che spesso, per ragioni operative, vengono autorizzati addirittura in modalità 24x7.

Quello che viene mancare è una **gestione "sicura" degli accessi remoti** e soprattutto un processo di audit che consenta di tracciare tutte le attività realizzate attraverso di essi. Infatti, la maggior parte dei sistemi in commercio che abilitano la gestione degli accessi remoti di terze parti non offrono la possibilità di definire regole di sicurezza granulari o di garantire una tracciatura completa delle attività realizzate attraverso questi accessi.

Ci sono almento 5 azioni necessarie per rendere sicuri questa tipologia di accessi remoti, riducendo il conseguente stato di vulnerabilità:

1) **Consolidare gli strumenti di accesso remoto**, centralizzando tutti gli accessi su un unico strumento consolidato.

2) **Bloccare tutti gli accessi** che non passino attraverso lo strumento consolidato.

3) Eliminare le credenziali condivise, utilizzando **credenziali individuali** con una tecnica di "**strong authentication**".

4) Usare uno strumento che permetta di gestire **regole di accesso granulari**, per decidere chi accede, a cosa, e quando.

5) Usare uno strumento che consenta di fare un **audit completo** di tutte le operazioni effettuate da ogni account.

Come garantire un accesso remoto sicuro

Per affrontare e risolvere questo problema, il Gruppo Daman distribuisce in Italia **StarSupport**, una soluzione di supporto remoto particolarmente efficace, efficiente, sicura e che agisce nel pieno **rispetto della legislazione italiana sulla Privacy**.

Basata sulla tecnologia Bomgar, StarSupport è l'unica soluzione che consente di fornire a tutti i collaboratori esterni e alle terze parti, un **accesso remoto sicuro a tutti i sistemi e dispositivi in rete**. StarSupport indirizza tutti i principali requisiti della sicurezza IT nel pieno rispetto delle normative di settore, quali PCI, DSS e HIPAA. Tra questi requisiti citiamo le forme di autorizzazione granulare, la crittografia SSL, i report di Audit dettagliati.

Con StarSupport sarà possibile: **creare dei "modelli"** per semplificare la gestione dei permessi; definire **quali sistemi possono essere acceduti**, da chi, e quando; **tracciare le operazioni** effettuate da tutti gli account.

Attraverso la funzione **Embassy**, sarà possibile creare dei veri e propri "**passaporti**", con dedinizioni granulari, per consentire l'accesso alla propria rete a soggetti esterni all'organizzazione.

Con **Rep Invite**, sarà invece possibile **coinvolgere un collaboratore esterno** nelle attività dei team interni all'organizzazione, anche se il collaboratore esterno non ha mai usato StarSupport.

Con **Session Recording** verrà **tracciata ogni attività** effettuata attraverso una sessione di accesso remoto.

StarSupport consente di **monitorare tutte le sessioni di supporto remoto**, incluse quelle dei collaboratori esterni. Gli amministratori autorizzati potranno mantenere un pieno controllo su tutte le sessioni, attivando in ogni momento funzioni di gestione delle stesse.

Gruppo Daman

Le soluzioni BDNA sono distribuite in Italia dal **Gruppo Daman**. il quale seleziona prodotti innovativi e sofisticati mirati al mercato dell'ICT, per la successiva distribuzione sul territorio italiano.