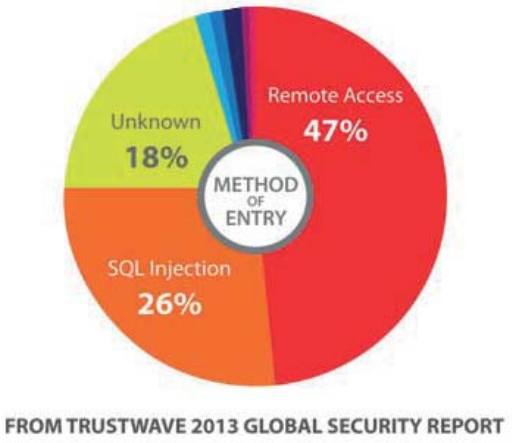
L'assistenza remota sicura nell'era del mobile computing

Le aziende hanno sempre più bisogno di servizi di assistenza efficaci, in grado di attivarsi prontamente sui device remoti e garantendo una rapida soluzione ai tanti problemi che possono minare l'efficienza dei servizi di business. Per questo i centri di supporto si sono nel tempo dotati di strumenti in grado di connettersi alle stazioni degli utenti finali.

La maggior parte di questi strumenti presenta però problematiche di Sicurezza e di salvaguardia della Privacy.

Dall'ultimo "Global Security Report", pubblicato da TrustWave, risulta evidente che il punto di vulnerabilità da cui originano il numero più consistente (47%) di attacchi da parte di hacker è rappresentato proprio dai sistemi di "accesso remoto", i quali spesso non posseggono alcuni requisiti fondamentali a salvaguardia della sicurezza aziendale. Da un'analoga ricerca di Verizon, questa percentuale risulta ancora più alta.



FROM TRUSTWAVE 2013 GLOBAL SECURITY REPORT

Questo tipo di vulnerabilità, sistematicamente ignorata dalla maggior parte delle organizzazioni, risulta particolarmente pericolosa, perché attraverso questi sistemi di tele-assistenza **è possibile accedere ad informazioni sensibili presenti nel dispositivo remoto senza lasciare alcuna "traccia"**, e quindi l'operazione può essere ripetuta più volte senza che nessuno si renda conto della violazione.

In Italia inoltre esiste una legislazione particolarmente restrittiva soprattutto per ciò che concerne le **normative sulla Privacy**, e la sistematica violazione di queste normative che si verifica durante l'erogazione di questi servizi di assistenza remota, espone l'azienda a dei concreti rischi di carattere penale.

Il quadro viene ulteriormente aggravato dal fatto che oggi molti di questi servizi di tele-assistenza, vengono esternalizzati e quindi di fatto **erogati da entità esterne all'organizzazione**, a cui viene "aperta una porta" molto ampia sul patrimonio informativo aziendale, "una porta" dalla quale possono uscire informazioni di particolare valore.

Come uscire dallo stato di Vulnerabilità garantendo un Supporto 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 garantire un supporto remoto efficace, sicuro ed integrato senza la necessità di installare preventivamente alcun software sulle postazioni remote.

StarSupport è l'unica soluzione che è stata sviluppata per aderire pienamente ai **criteri di massima sicurezza** e alle normative sulla Privacy. Sotto questo profilo, StarSupport possiede un **livello di certificazione specifica** (FIPS 140-2), che riguarda i requisti di sicurezza per l'utilizzo della crittografia. Inoltre, la soluzione StarSupport è stata specificatamente personalizzata per aderire alla **legislazione sulla Privacy vigente in Italia**, che risulta particolarmente restrittiva.

StarSupport si caratterizza inoltre per la sua **architettura centralizzata e basata su appliance**, che consente di mantenere i dati sensibili sempre all'interno del firewall aziendale e quindi in area protetta.

Il sistema di autenticazione è integrato con i principali sistemi di **Identity Management**, e include più di 50 controlli che consentono di definire in modo granulare "**chi accede a cosa**". Inoltre, tutte le operazioni di assistenza remota vengono archiviate e video-registrate per successivi controlli e attività di tipo "forense".

Sotto il profilo della sicurezza Starsupport presenta alcune caratteristiche peculiari: disponibilità di una **Chat sicura** tra operatore e postazione di lavoro; **Log dettagliato** di tutte le operazioni svolte dagli operatori sulle stazioni remote; creazione di un **file video criptato** per documentare ogni singola sessione; **cifratura di tutte le comunicazioni** tra operatore e postazione di lavoro; **utilizzo di porte conosciute** ed in genere già aperte sui firewall; **profilazione granulare** dei diritti di accesso e delle funzionalità consentite.

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.