SecureRDP – Sicurezza in Terminal Server

La procedura, esterna a WinOPUS ed indipendente da qualsiasi applicazione, va caricata sul server configurato per accettare connessioni RDP/Terminal Server e verifica che il nome del PC/dispositivo che tenta di collegarsi sia presente nell'elenco delle apparecchiature autorizzate. Se l'apparecchiatura che tenta il collegamento non è autorizzata, la procedura chiude immediatamente la connessione e scrive l'evento in un file di log, sempre nella cartella dell'applicazione. Contemporaneamente, l'intrusione viene notificata via e-mail ai destinatari configurati ed ha un contenuto simile a questo:

SecureRDP - Eseguito logoff forzato
ClientName : PC-MYPC
UserName : ADMINISTRATOR
ComputerName: SERVER
DomainName: MYDOMAIN
MacAddress : 9458A48BF6B1

Il software non ha interfaccia di amministrazione; ha un proprio setup che lo carica automaticamente nei servizi di Windows; funziona sia a 32 che a 64bit su qualsiasi sistema operativo Windows® ed è indipendente dalla lingua del sistema operativo delle apparecchiature/PC e dei server.

L'elenco delle apparecchiature/PC autorizzati è contenuto in un semplice file di testo che deve risiedere nella stessa cartella della procedura; il contenuto potrebbe essere simile a questo:

INTL-SERVER #Server internazionale
PC-LABOR01 #PC laboratorio
PC-LABOR02 #PC laboratorio
Z-SRV-03 #Server USA
Z-SRV-04 #Server EMEA
Z-SRV-05 #Server Italy
HP_UX #Unix Srv
[IMAC MRS LUCY]