9 modi

in cui gli utenti con privilegi introducono rischi di sicurezza

Gli utenti che non sono amministratori IT, ma dispongono comunque di diritti di amministratore, possono aumentare i rischi di sicurezza e i costi di gestione, nonché ostacolare la compliance. Ecco cosa possono fare per minare la sicurezza, e cosa potete fare voi per impedirlo.

1 Installare app non autorizzate che veicolano malware

Impedite che gli utenti con diritti di amministratore possano disattivare il controllo degli account, usare app non autorizzate o modificare involontariamente le impostazioni di sistema.

2 Disattivare servizi importanti, come l'antivirus

Microsoft Management Console (MMC) consente agli utenti di caricare snap-in che possono controllare i servizi. Impedite agli utenti con diritti di amministratore di accedere a MMC.

3 Bypassare restrizioni basate su interfaccia grafica

Limitate l'esecuzione di comandi o script sui sistemi operativi.

4 Disinstallare agent e software di protezione

Impedite agli utenti con privilegi di disinstallare i software di protezione di terze parti.

5 Aggirare i criteri di protezione della gestione centrale

Impedite agli utenti con privilegi di accedere al registro di Windows, e di modificare le configurazioni.

6 Disabilitare o modificare le impostazioni del firewall

Evitate la diffusione di malware in rete, impedendo la disattivazione dei firewall.

7 Modificare il comportamento delle applicazioni tramite data e ora errate

Impedite agli utenti di cambiare le impostazioni di data e ora, per tutelare l'integrità di applicazioni e marche temporali, indispensabile per gli audit o la risoluzione di problemi.

8 Interrompere i software di protezione

Aggiungete la possibilità di controllare le interruzioni dei processi, per ridurre i rischi di sicurezza.

9 Elevare le applicazioni che possono introdurre malware

Limitate alcune applicazioni in modo che possano essere eseguite solo con privilegi standard.

Grazie alle capacità di Application Control disponibili in Ivanti® Security Controls, potete impostare subito alcune limitazioni semplici ma efficaci, per ridurre i rischi e migliorare lo stato di compliance. Potrete anche porre fine agli interventi derivanti dalla modifica involontaria di impostazioni che dovrebbero essere gestite solo da un amministratore.

SCARICA IL WHITE PAPER