9 formas

en que los usuarios con privilegios provocan riesgos de seguridad

Cuidado con los usuarios finales no formados como administradores de sistemas informáticos pero que cuentan con derechos de administrador completos de dichos sistemas. Estas son algunas de las formas en que aumentan los riesgos de seguridad y los costes de gestión y complican el cumplimiento de normativas y lo que puede hacer para resolverlo.

1 Instalan aplicaciones no autorizadas que introducen malware

Evite que los administradores desactiven el Control de cuentas de usuario y evite aplicaciones no autorizadas o cambios accidentales de ajustes del sistema.

2 Desactivan servicios críticos como los antivirus

La Microsoft Management Console (MMC) permite a los usuarios cargar complementos capaces de controlar servicios. Haga que la MMC sea inaccesible a usuarios finales con privilegios de administrador.

3 Sobrescriben restricciones basadas en la interfaz gráfica de usuario

Limite la ejecución de comandos en sistemas operativos.

4 Desinstalan agentes y software de protección

Evite que los usuarios con privilegios desinstalen software de protección de terceros.

5 Evitan las políticas de protección de la administración central

Excluya el acceso privilegiado al registro de Windows. Evite que los usuarios cambien ajustes de configuración.

6 Desactivan o cambian ajustes del cortafuegos de los nodos finales

Defiéndase contra la expansión por la red de software malicioso al evitar la desactivación.

7 Cambian el comportamiento de aplicaciones mediante el uso de fechas y horas incorrectas

Bloquee los cambios de fecha y hora para proteger la integridad de las aplicaciones y las marcas de hora para auditorías o resolución de problemas.

8 Eliminan software de protección

Añada el control de terminación de procesos para reducir los riesgos de seguridad.

9 Elevan aplicaciones que pueden introducir malware

Limite ciertas aplicaciones para que solo se ejecuten con privilegios estándar.

Con las características de control de aplicaciones en Ivanti® Security Controls puede crear limitaciones sencillas inmediatamente para reducir su riesgo, aumentar el cumplimiento corporativo y detener la creación de tickets de TI innecesarios por personas que cambian ajustes administrativos involuntariamente.

DESCARGUE EL INFORME