PROTEGIENDO EL TRABAJO REMOTO DE LAS PYME

Consejos básicos sobre la protección de datos: Autenticación simplificada

¿Por qué la autenticación en múltiples fases es imprescindible para el acceso remoto?

Las soluciones de autenticación en varias fases (MFA) requieren dos o más datos independientes para verificar la identidad de un usuario. La MFA es mucho más segura que la contraseña tradicional estática o la autenticación con un código PIN.

Más del 80% de las empresas almacenan información de identificación personal (PII) acerca de sus clientes así como de sus propios empleados.

Fuente: Datos recopilados de más de 27.000 participantes principalmente de la Unión Europea (UE) mediante el formulario de verificación de cumplimiento de normativas desde noviembre de 2017 a mayo de 2018

Mitigar el riesgo derivado del trabajo remoto

El cambio repentino hacia el trabajo desde el hogar como consecuencia de la pandemia COVID-19, ha resaltado la necesidad de proteger el acceso a los sistemas críticos de las empresas y los sistemas que procesan datos personales. El número exponencialmente mayor de intentos de acceso requiere el uso de medidas apropiadas que eviten el riesgo relacionado con el trabajo remoto. Al agregar un nivel adicional de autenticación, además del tradicional nombre de usuario y contraseña (que puede resultar comprometido con facilidad), **ESET Secure Authentication mejora significativamente la seguridad de la red de la empresa y los datos ingresados desde el exterior**.

Eliminar los malos hábitos de uso de contraseñas

El uso de contraseñas débiles pone en riesgo la seguridad IT significativamente. Además de utilizar contraseñas idénticas en distintos sitios Web y aplicaciones, los colaboradores muchas veces las comparten con amigos, familiares y colegas. Incluso cuando las empresas aplican políticas para el uso de contraseñas, los empleados siguen usando variantes de su contraseña anterior o incluso las escriben en notas adhesivas.

Evitar el robo de datos

Una de las formas más comunes en que los hackers pueden obtener acceso a sus datos es mediante la extracción de contraseñas o ataques dirigidos. Al incorporar una solución con MFA, es mucho más difícil que los hackers logren acceder a sus sistemas. Los **principales objetivos** del robo de datos siempre han sido **las organizaciones financieras, minoristas, de atención médica y del sector público**. Sin embargo, los hackers ahora también están atacando otros sectores.

Cumplir con las normativas

Varias reglamentaciones exigen el uso de la MFA y la mayoría (incluyendo GDPR e HIPAA) enfatiza la necesidad de fortalecer las prácticas de autenticación. **La autenticación en varias fases ya no es una solución opcional**. Las agencias reguladoras como ENISA recomiendan firmemente su uso a empresas que manejan tarjetas de crédito o gestionan transacciones financieras. Todas las organizaciones tienen que evaluar si están cumpliendo estas normativas.

Implementación de la autenticación en varias fases

ESET Secure Authentication ofrece una forma fácil de implementar la MFA en los sistemas comúnmente utilizados, tales como redes VPN, Escritorio remoto, Office 365, Outlook Web Access, inicio de sesión del sistema operativo y más.

El **80%** de los ataques de hackers se debe al uso de credenciales robadas o débiles.

Fuente: Informe de la Investigaciones de filtración de datos de Verizon 2017, 10º edición

FÁCIL PARA EL ADMINISTRADOR

- Configuración sencilla en pocos minutos
- No requiere la capacitación de los colaboradores
- Gestión remota completamente intuitiva
- Sin costos adicionales de infraestructura
- Admite numerosas VPN y servicios en la nube

FÁCIL PARA SUS USUARIOS

- No necesitan utilizar contraseñas cada vez más complejas
- Funciona con cualquier smartphone
- Solución de un solo toque, no necesita que se reescriba la contraseña
- No requiere tokens de hardware adicionales
- Extremadamente fácil de usar

Cómo usar ESET Secure Authentication en una cantidad cada vez mayor de dispositivos y entornos

LADO DEL CLIENTE

1

Proteja el acceso al **sistema operativo** de la estación de trabajo de los empleados

2

Proteja los datos corporativos almacenados con **aplicaciones y servicios en la nube**

GOOGLE APPS
OFFICE 365
DROPBOX
CONFLUENCE
Y MUCHOS MÁS

3

Asegúrese de que la **VPN** de la empresa solo permita la entrada de usuarios autenticados

BARRACUDA
CISCO ASA
CITRIX ACCESS GATEWAY
CHECK POINT SOFTWARE
CYBEROAM
F5 FIREPASS
FORTINET FORTIGATE
JUNIPER
PALO ALTO
Y MUCHOS MÁS

LADO DEL ADMINISTRADOR

4

Fortalezca el control del acceso para el **Protocolo de escritorio remoto (RDP)**

5

Utilice la MFA con **aplicaciones Web de Microsoft**

OUTLOOK WEB APP (OWA)
PANEL DE CONTROL DE EXCHANGE
SHAREPOINT
ACCESO WEB DE ESCRITORIO REMOTO
ACCESO WEB DE TERMINAL SERVICES

6

Integre la MFA con cualquier **proveedor de identidad** que admita SAML 2.0

OKTA
OPENAM
AZURE AD
AD FS
SHIBBOLETH

Proteja sus datos ahora, compre después. Obtenga su prueba gratuita con todas las funcionalidades.

ESET SECURE AUTHENTICATION