Autenticación Multifactor

Las contraseñas fallaron, ¿qué hacemos ahora?

Protección de las Credenciales de Usuario en Pequeñas y Medianas Empresas

MFA

Las pérdidas de datos son frecuentes y las contraseñas inseguras son el motivo principal.

La seguridad de las contraseñas es uno de los problemas más importantes que tiene la seguridad de la información en la actualidad. De acuerdo con el Informe sobre Pérdida de Datos de Verizon 2017, el 81% de las pérdidas de datos tienen que ver con contraseñas inseguras o robadas. Para superar estos desafíos, muchas organizaciones están recurriendo a la tecnología de autenticación multifactor (MFA) con el fin de ofrecer un enfoque por niveles y mitigar el papel que juegan las contraseñas al otorgar acceso.

Pero lamentablemente, las soluciones tradicionales de MFA con frecuencia son difíciles de implementar y administrar para las pequeñas y medianas empresas. Para comprender mejor el estado actual de la seguridad de contraseñas y el uso de MFA, WatchGuard realizó una encuesta de propietarios de empresas y de responsables de toma de decisiones de TI en empresas que tienen entre 100 y 1.000 empleados en los Estados Unidos, el Reino Unido y Australia.
Este fue el resultado.

25% De acuerdo con la investigación de WatchGuard **el 25% de las pequeñas y medianas empresas** dicen haber **experimentado una pérdida** en los últimos **18 meses**.

De acuerdo con nuestra investigación, la vulnerabilidad de las contraseñas puede atribuirse en gran medida a prácticas de contraseñas inseguras, tanto dentro como fuera de la oficina:

47% El 47% de los empleados utiliza **contraseñas simples o inseguras**

31% El 31% utiliza contraseñas **de red** para **aplicaciones personales**

30% El 30% comparte **contraseñas**

Nombre de Usuario
****

40% El 40% hace clic en **correos electrónicos de suplantación de identidad, etc.**

36% El 36% utiliza **Wi-Fi inseguro**

El problema NO se resolverá con formación

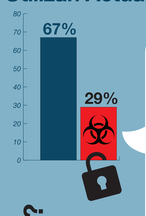
A pesar de que **el 80%** de las empresas afirman estar **ofreciendo formación sobre contraseñas** a sus empleados, **los problemas persisten**.

Las empresas buscan una mejor solución y el 84% señala que prefiere disponer de tecnología adecuada antes de depender en políticas de contraseñas.

La solución es la Autenticación Multifactor

La autenticación multifactor (MFA) es un método de verificación de inicio de sesión que agrega un nivel de seguridad más allá de un simple nombre de usuario y contraseña. Impide el acceso no autorizado que puede suceder como consecuencia de contraseñas perdidas o robadas, así como permite el fácil acceso de usuarios verificados a sus cuentas e información.

¿Cuántas Pequeñas y Medianas Empresas Utilizan Actualmente MFA?



67% de las empresas utilizan MFA PERO el 29% NO LO HACEN

Si bien es bueno notar que las empresas utilizan MFA, no todos los métodos de MFA están creados de la misma forma. Si las empresas no disponen de soluciones de MFA que utilicen métodos de seguridad avanzados, tienen posibilidades de correr un riesgo adicional. Se considera, por ejemplo, que los mensajes SMS constituyen un método inseguro de autenticación, ya que pueden ser falsificados o interceptados por el atacante. Además, los tokens de hardware plantean una amenaza debido a que pueden perderse o robarse, lo cual genera una falla de seguridad.

¿Por qué?

¿Por qué entonces no hay más pequeñas y medianas empresas que adopten las últimas tecnologías de MFA?

- El 61% piensa que la mayor parte de las soluciones están **diseñadas para empresas más grandes.**
- El 24% sostiene que **el mantenimiento y el soporte son difíciles**
- El 24% sostiene que **la implementación es difícil**
- El 24% sostiene que **es muy costoso**
- El 22% sostiene que **existe resistencia**
- **El 17% sostiene que SIMPLEMENTE NO NECESITA SOLUCIONES DE MFA**

No disponemos de MFA actualmente, ¡pero suena increíble!

Para aquellos que están interesados en comprarlo:

65% de los encuestados tiene en sus planes comprarlo en el futuro

83% de los encuestados está interesado en utilizar MFA

¿Tokens?
El 38% compraría tokens de escritorio
El 28%, tokens de hardware conectados
El 26%, tokens móviles
El 25%, SMS

54% de los encuestados preferiría servidores basados en la nube

Las contraseñas ya no son suficientes.
No permita que la contraseña insegura de un empleado comprometa los activos y la información de su empresa.
¡Compre AuthPoint hoy mismo!

WatchGuard AuthPoint
AuthPoint de WatchGuard proporciona autenticación multifactor (MFA) en una plataforma de nube fácil de usar. Debido a que está en la nube, no hay ningún hardware que implementar y el acceso se puede administrar desde cualquier lugar. La aplicación móvil permite que cada intento de inicio de sesión sea visible y sencillo para que los usuarios los aprueben o rechacen. AuthPoint también ofrece numerosas integraciones con terceros, incluidas conocidas aplicaciones en la nube, servicios web, VPN y redes.
Más información en www.watchguard.com/authpoint

WatchGuard