yubico

Los requisitos de los ciberseguros suben el nivel de seguridad

El papel crítico de la MFA resistente al phishing para ofrecer la máxima seguridad

Evolución de los ciberseguros y aumento de las primas

En 1995, cuando se lanzó al mercado la primera póliza de ciberseguro, pocas personas aparte de los informáticos conocían el verdadero riesgo y las implicaciones económicas de un desastre digital. Eso es cosa del pasado. Desde entonces, los ataques se han vuelto más frecuentes, más sofisticados, más mediáticos y, en algunos casos, más devastadores. Es raro que pase un mes sin que un ataque importante acapare los titulares y redefina las expectativas en cuanto a ciberseguridad. Y debido al reciente auge del ransomware, los riesgos nunca han sido más altos: el cibercrimen generó pérdidas por valor de 6 billones de dólares solo en 2021, con un crecimiento interanual del 15 %.

No es de sorprender que el resultado haya sido una mayor demanda de ciberseguros. Pero al igual que las empresas se han esforzado por mantener sus equipos de TI a salvo de ataques en continua evolución, las empresas de seguros se han esforzado por asegurar de forma eficaz los riesgos cibernéticos. Algunos piensan que las posibles pérdidas son demasiado grandes y han dejado de ofrecer ciberseguros por completo. En muchos casos, aquellas que los mantienen han aumentado los precios de las primas entre un 150 % y un 300 %.

Las primas más altas compensan el riesgo para los proveedores de ciberseguros, pero no por mucho. Para que un ciberseguro sea un producto viable en un mundo en el que el riesgo cibernético está disparado, la probabilidad de que los ataques tengan éxito se debe reducir drásticamente. En 1995, cuando el mayor riesgo era un fallo del hardware, cualquier persona que tuviera una tarjeta de crédito podía obtener una póliza. Sin embargo, ahora las empresas deben demostrar que cumplen unos estándares de ciberseguridad mínimos y tomarse en serio la seguridad cibernética y la protección. Conseguir un seguro (a cualquier precio) depende de ello. Por lo tanto, cualquier empresa que quiera obtener o mantener un ciberseguro debe evaluar y posiblemente actualizar su propia estrategia de seguridad.

Una seguridad mínima ya no permite obtener la cobertura de un ciberseguro

Cada proveedor de seguros establece los requisitos de cobertura de sus ciberseguros, pero la amplia mayoría espera que los solicitantes de cobertura dispongan de controles de seguridad de correo electrónico, herramientas de detección y respuesta de puntos finales, protecciones antivirus de última generación y capacidades de copia de seguridad y recuperación, como mínimo. Sin embargo, por muy importantes que puedan ser estos, el sector de los ciberseguros considera que la autenticación de múltiples factores (MFA) es la defensa más importante. De hecho, puede que sea imposible obtener un ciberseguro sin MFA.

Estos nuevos y elevados requisitos de seguridad tienen perfecto sentido. Ningún otro control de seguridad reduce más el riesgo cibernético que la MFA, porque no solo mitiga el riesgo asociado a un panorama de ciberamenazas en evolución, sino que también minimiza los riesgos asociados con los comportamientos y errores de los usuarios. Sin ella, las cuentas privadas y los datos confidenciales son muy vulnerables a los ataques, independientemente del resto de protecciones que se apliquen. Al requerir capas adicionales de autenticación, las empresas pueden detener los ataques de phishing y ransomware, algo que resulta suficiente para disuadir a muchos hackers que buscan el camino de menos resistencia. Y para los pocos decididos que queden, atravesar dos o más capas de autenticación supone un obstáculo formidable.

La primera prioridad para cualquiera que busque un ciberseguro es implementar la MFA en toda la organización. Y aunque la solución que se percibe como más rápida, barata y fácil, como la autenticación por SMS o móvil, puede parecer suficiente, los proveedores de seguros podrían verlo de forma diferente. Quieren ofrecer cobertura a las empresas que son más inmunes a los ataques, especialmente porque los proveedores son cada vez más reacios a los riesgos. Por lo tanto, la elección correcta de una MFA es aquella que ofrezca la mejor protección, ahora y en el futuro. Cualquier otra cosa solo aumentaría el riesgo para la empresa y para el proveedor de seguros, por lo que esa opción será cada vez menos aceptable para obtener y mantener un ciberseguro.

La MFA resistente al phishing es ahora más crítica que nunca

Siempre es más seguro usar múltiples factores de autenticación que uno solo. Dicho esto, algunas formas de MFA son mucho menos seguras que otras. Por ejemplo, los productos de MFA que envían una contraseña de un solo uso (OTP) al teléfono o la dirección de correo electrónico, aunque son más seguros que el uso exclusivo de contraseñas, siguen siendo vulnerables a los ataques de phishing. Lo único que tiene que hacer un hacker es convencer a una persona para que se autentique en un sitio falso que parece idéntico al sitio real, con lo que el hacker obtiene las credenciales de usuario y los códigos de MFA. Y una vez que los tiene, puede autenticarse fácilmente y continuar con su ataque disfrazado de usuario autorizado, lo que puede retrasar la detección hasta que sea demasiado tarde y tener repercusiones enormes.

La MFA resistente al phishing funciona de forma diferente. En lugar de autenticar a los usuarios en función de “algo que saben”, como una OTP, los autentica en función de “algo que tienen”, como una llave de seguridad que conectan al puerto

USB de su dispositivo. Es casi imposible robar a distancia los secretos de una llave de seguridad basada en hardware, en comparación con la facilidad con la que se pueden interceptar los códigos por SMS y otros métodos mediante ataques remotos y de intermediario, como demuestran muchos incidentes que aparecen en las noticias. Como resultado, la MFA resistente al phishing real es un enfoque extremadamente difícil de franquear, por lo que las empresas y sus proveedores de ciberseguros pueden estar tranquilos sabiendo que solo los usuarios adecuados tendrán acceso a los recursos confidenciales.

Todos los organismos federales tuvieron que adoptar forzosamente MFA resistente al phishing y es cada vez un requisito más habitual entre los organismos estatales y locales, además de en el sector privado. Y para que sean totalmente resistentes al phishing, se urge a estas organizaciones a que adopten la MFA basada en los protocolos FIDO/WebAuthn o Smart Card/PIV. Cualquier otra cosa no es resistente al phishing y está por debajo del estándar aceptable para las organizaciones conscientes de la seguridad. Las empresas que adoptan este enfoque de la seguridad moderno tienen un riesgo mucho menor de que un ciberataque tenga éxito. Por lo tanto, no solo son las candidatas más atractivas para obtener la cobertura de un ciberseguro con primas posiblemente más bajas, sino que también son las más seguras frente a daños financieros, legales y a la reputación, que ninguna cobertura podría remediar.

YubiKeys: MFA resistente al phishing que le sitúa en una buena posición para los nuevos requisitos de los ciberseguros

Yubico lleva más de una década como líder e innovador en el campo de la autenticación robusta. Nuestro producto, la YubiKey, es considerado como la mejor solución por muchos expertos en seguridad y proveedores de ciberseguros.

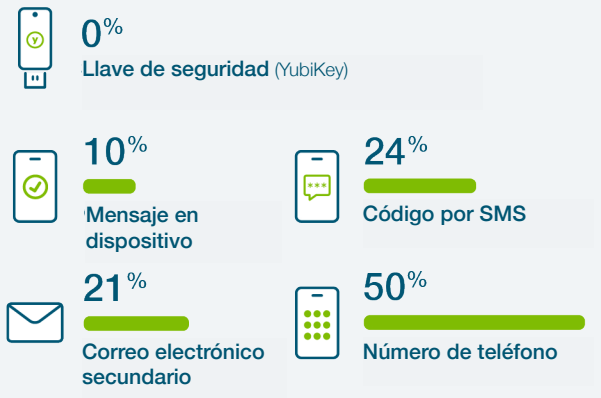
> El papel de Yubico en el sector es único; las soluciones que Yubico ofrece actualmente son la próxima generación de seguridad de identidad. El resto del mundo necesita seguir la estela de Yubico y no al contrario.
>
> **Steve Brasen** | director de investigación | Enterprise Management Associates

Seguridad moderna: El tiempo y los amplios estudios han demostrado que las YubiKeys detienen el phishing y otras estrategias de apropiación de cuentas al instante. Las YubiKeys admiten varios protocolos de autenticación en una sola llave de seguridad, tanto los protocolos de autenticación heredados, como OTP, como los protocolos de seguridad modernos que ofrecen resistencia al phishing real, como FIDO U2F y FIDO2/WebAuthn, además de Smart Card/PIV. Al ofrecer compatibilidad con varios protocolos, las YubiKeys mejoran la estrategia de seguridad de las organizaciones, sin importar en qué parte de su proceso de autenticación se encuentren, y en una variedad de infraestructuras locales heredadas e infraestructuras de nube modernas.

Experiencia del usuario rápida y fácil: La sencillez de las YubiKeys es otro diferenciador clave. Las YubiKeys no requieren la instalación de software de cliente y no necesitan baterías o una conexión móvil. Los usuarios solo tienen que conectarla a un puerto USB y tocar el botón o "tocar y listo" mediante NFC para una autenticación segura. Las funciones de autoservicio de usuarios permiten a las organizaciones capacitar de forma rápida y fácil a los usuarios para que consigan su YubiKey sin demasiada implicación del equipo de TI o la necesidad de ir a la oficina. La MFA resistente al phishing se puede configurar en cuestión de minutos y la YubiKey funciona fácilmente en portátiles, tabletas y smartphones, e incluso como tarjeta inteligente dependiendo de las necesidades y políticas de la empresa para acceder a determinados sistemas.

Reduzca los riesgos financieros, legales y para la reputación: Se prevé que el coste del cibercrimen en el mundo sea de 10,5 billones de dólares en 2025, a pesar de que las empresas están invirtiendo cientos de miles de millones de dólares para reforzar sus estrategias de ciberseguridad. Las YubiKeys ofrecen los mayores niveles de defensa contra phishing, son llaves de seguridad de hardware diseñadas para proteger a su empresa y a sus usuarios eludiendo los riesgos de ataques.

Riesgo de robo de cuentas



Investigación de Google, NYU y UCSD basada en 350 000 intentos reales de secuestro. Los resultados mostrados se corresponden con ataques dirigidos.

Resumen:

Una vulneración de la ciberseguridad puede tener implicaciones catastróficas para la organización afectada. Esto se traduce en tiempo de inactividad y oportunidades perdidas, y afecta de manera importante también a los proveedores de ciberseguros. Manténgase protegido y prepárese para contar con la mejor estrategia considerando un enfoque de MFA capaz de afrontar las amenazas actuales, además de estar preparado para gestionar en el futuro las amenazas cada vez más sofisticadas. Las YubiKeys protegen una amplia variedad de entornos y ofrecen la comodidad necesaria para ayudar a los empleados que en la actualidad trabajan en persona, a distancia o de forma híbrida. Además ofrece un enfoque de MFA resistente al phishing coherente y robusto para los métodos modernos con los que trabajan las organizaciones y sus usuarios.

Contacto
yubi.co/contacto

Leer más
yubi.co/yk5-es

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) es la inventora de la YubiKey, el estándar de referencia para la autenticación de múltiples factores (MFA) resistente al phishing, y creadora y colaboradora de los estándares de autenticación abiertos FIDO. La empresa es pionera en ofrecer seguridad de autenticación de passkey basada en hardware a clientes de más de 160 países. Si desea obtener más información visite: www.yubico.com.