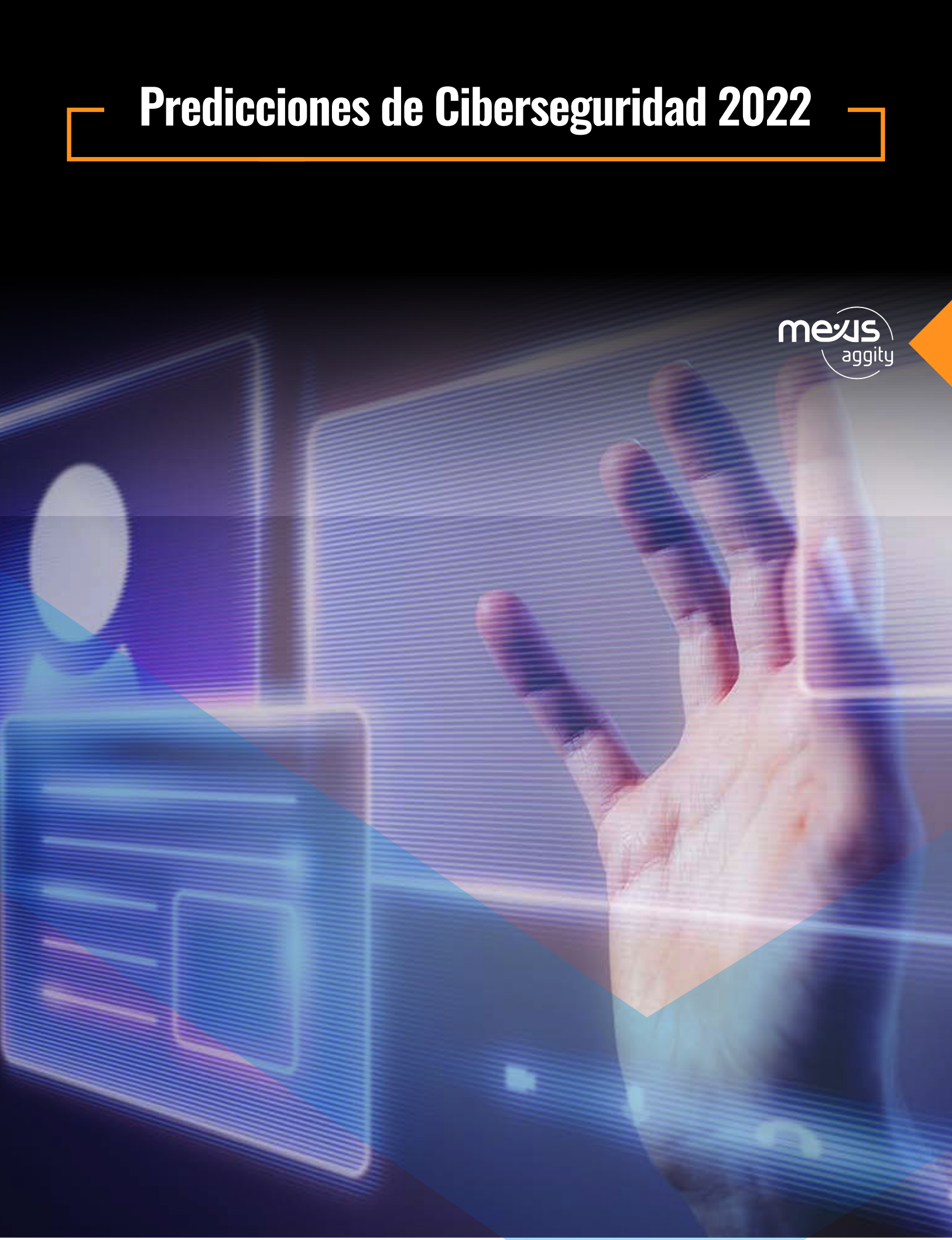
Predicciones de Ciberseguridad 2022



En las Predicciones de Ciberseguridad para 2022, WatchGuard Threat Lab hace un ejercicio relacionado con los principales titulares sobre seguridad que podríamos ver en 2022. A continuación, se explica cómo los hackers podrían dirigirse al espacio, cómo se explotarán las amenas a dispositivos móviles, qué pasará con los ciberseguros o Zero-Trust, y mucho más.

1.- Las amenazas a dispositivos móviles utilizadas por los Estados acaban en el submundo de la ciberdelincuencia.

El malware para móviles existe, sobre todo en la plataforma Android, pero todavía no ha alcanzado la misma magnitud que el malware tradicional para ordenadores de sobremesa. En parte, creemos que esto se debe a que los dispositivos móviles están diseñados con un mecanismo seguro (por ejemplo, el arranque seguro) desde el principio, lo que hace mucho más difícil crear amenazas "zero-touch" que no requieran la interacción de la víctima. Sin embargo, han existido vulnerabilidades remotas graves contra estos dispositivos, aunque son más difíciles de encontrar.

Mientras tanto, los dispositivos móviles representan un objetivo muy atractivo para los equipos de ciberseguridad de los Estados, tanto **por las capacidades de los dispositivos como por la información que contienen.** En consecuencia, los grupos que venden a organizaciones apoyadas por los Estados son los principales responsables de la financiación de gran parte de las sofisticadas amenazas y vulnerabilidades dirigidas a los dispositivos móviles, como el reciente programa espía para móviles Pegasus. Por desgracia, como en el caso de Stuxnet, cuando se filtran estas amenazas más sofisticadas, las organizaciones criminales aprenden de ellas y copian las técnicas de ataque.

El próximo año, preevemos un aumento de sofisticados ataques móviles por parte de los ciberdelincuentes.

2.- La noticia de que los hackers apuntan al espacio llega a los titulares.

Con el creciente interés de los gobiernos y del sector privado por la «carrera espacial» y la reciente investigación sobre ciberseguridad en las vulnerabilidades de los satélites, creemos que un **«hackeo en el espacio»** llegará a los titulares en 2022.

Recientemente, el hackeo de satélites ha ganado la atención de la comunidad de ciberseguridad entre los investigadores y en conferencias como DEF CON. Aunque los satélites pueden parecer fuera del alcance de la mayoría de las amenazas, los investigadores han descubierto que pueden comunicarse con ellos utilizando un equipo de unos 300 dólares. Además, es posible que los satélites más antiguos no se hayan centrado en los controles de seguridad modernos, confiando en la distancia y la oscuridad como defensa.

Mientras tanto, muchas empresas privadas han iniciado su carrera espacial, que aumentará en gran medida la superficie de ataque en órbita. Compañías como Starlink están lanzando miles de satélites. Entre estas dos tendencias, más el valor de los sistemas orbitales para los estados-nación, las economías y la sociedad, sospechamos que los gobiernos ya han comenzado discretamente sus campañas de ciberdefensa en el espacio. No nos sorprendamos si algún día vemos un hackeo relacionado con el espacio en los titulares.

3.- La propagación de SMSishing golpea a las plataformas de mensajería.

El phishing basado en mensajes de texto, conocido como SMSishing, ha aumentado de forma constante a lo largo de los años. Al igual que la ingeniería social del correo electrónico, comenzó con mensajes de señuelo no dirigidos que se enviaban como spam a grandes grupos de usuarios, pero últimamente ha evolucionado hacia textos más dirigidos que se hacen pasar por mensajes de alguien conocido, incluido quizás tu jefe.

Paralelamente, las plataformas de mensajes cortos de texto también han evolucionado.

Los usuarios, especialmente los profesionales, se han dado cuenta de la **inseguridad de los mensajes de texto SMS** sin cifrar gracias al NIST (Instituto Nacional de Estándares y Tecnología), a las diversas infracciones de las operadoras y al conocimiento de las **debilidades de los estándares de las operadoras,** como el Sistema de Señalización 7 (SS7). Esto ha hecho que muchos trasladen sus mensajes de texto empresariales a aplicaciones alternativas como WhatsApp, Facebook Messenger e incluso Teams o Slack.

Allá donde van los usuarios legítimos, los ciberdelincuentes los siguen. Como resultado, estamos empezando a ver un aumento en los informes de mensajes maliciosos tipo spear SMSishing a plataformas de mensajería como WhatsApp. ¿Has recibido un mensaje de WhatsApp de tu director general pidiéndote que le ayudes a crear una cuenta para un proyecto en el que está trabajando? Tal vez debas llamar o contactar con él a través de algún otro medio de comunicación para verificar que se trata realmente de esa persona.

En resumen, esperamos que los mensajes de phishing dirigidos a través de muchas plataformas de mensajería se dupliquen en 2022.

4.- La autenticación sin contraseña falla a largo plazo sin MFA.

Ya es oficial. Windows ha pasado a no tener contraseñas. Mientras celebramos el abandono de las contraseñas para la validación digital, también creemos que el enfoque actual de la autenticación de un solo factor para los inicios de sesión de Windows simplemente repite los errores del pasado. Windows 10 y 11 permitirán ahora configurar una autenticación completamente sin contraseña, utilizando opciones como Hello (la biometría de Microsoft), un token de hardware Fido o un correo electrónico con una contraseña de un solo uso (OTP).

Aunque elogiamos a Microsoft por dar este audaz paso, creemos que todos los mecanismos de autenticación de factor único son una elección equivocada y repiten los errores de las contraseñas de antaño. La biometría no es una píldora mágica imposible de derrotar: de hecho, los investigadores y atacantes han vencido repetidamente a varios mecanismos biométricos. Sin duda, **la tecnología está mejorando, pero las técnicas de ataque también evolucionan** (especialmente en un mundo de redes sociales, fotogrametría e impresión 3D). En general, los tokens de hardware también son una opción fuerte de factor único, pero la brecha de RSA demostró que tampoco son invencibles. Y, francamente, los correos electrónicos de texto sin cifrar con una OTP son simplemente una mala idea.

La única solución robusta para la validación de la identidad digital es la autenticación multifactor (MFA). En nuestra opinión, Microsoft (y otros) podrían haber resuelto realmente este problema haciendo que MFA fuera obligatoria y fácil en Windows. Se puede seguir utilizando Hello como un factor de autenticación, pero las organizaciones deberían obligar a los usuarios a emparejarlo con otro, como una aprobación push a su teléfono móvil que se envía a través de un canal cifrado (sin texto o correo electrónico claro).

Nuestra predicción es que la autenticación sin contraseña de Windows despegará en 2022, pero esperamos que los hackers y los investigadores encuentren formas de eludirla, demostrando que no hemos aprendido de las lecciones del pasado.

5.- Las empresas aumentan los ciberseguros a pesar de que los costes se disparan.

Desde el éxito astronómico del ransomware a partir de 2013, las aseguradoras de ciberseguridad se han dado cuenta de que los costes del pago para cubrir a los clientes contra estas amenazas han aumentado drásticamente. De hecho, según un informe de S&P Global, **el ratio de siniestralidad de las ciberaseguradoras aumentó** por tercer año consecutivo en 2020 en 25 puntos, es decir, más del 72%. Esto hizo que las primas de las pólizas de ciberseguro independientes aumentaran un 28,6% en 2020, hasta alcanzar los 1.620 millones de dólares. Como resultado, han aumentado mucho los requisitos de ciberseguridad para los clientes. No solo ha aumentado el precio del seguro, sino que las aseguradoras ahora escanean y auditan activamente la seguridad de los clientes antes de ofrecer una cobertura relacionada con ciberseguridad.

En 2022, si no tienes las protecciones adecuadas, incluida la autenticación multifactor (MFA) en el acceso remoto, puede que no consigas un seguro de ciberseguridad al precio que te gustaría, o que no lo obtengas. Al igual que otras regulaciones y normas de cumplimiento, este nuevo enfoque de las aseguradoras en la seguridad y la auditoría impulsará un nuevo planteamiento por parte de las empresas para mejorar las defensas en 2022.

6.- Y lo llamaremos Zero Trust.

A la mayoría de los profesionales de seguridad se les ha inculcado el principio del mínimo privilegio desde el principio de sus carreras. Dar a los usuarios el nivel mínimo de acceso necesario para realizar sus funciones de trabajo es, en su mayor parte, una buena práctica indiscutible. Lamentablemente, las mejores prácticas no se traducen directamente en una amplia adopción, y menos en toda su extensión. En los últimos años, o décadas en realidad, hemos visto la facilidad con la que los atacantes pueden moverse lateralmente y elevar su nivel de acceso mientras explotan organizaciones que no han seguido los principios básicos de seguridad.

Recientemente, una arquitectura de seguridad de la información «moderna» ha crecido en popularidad bajo el nombre de Zero Trust. Un enfoque Zero Trust en la seguridad se reduce básicamente a **«asumir la brecha».** En otras palabras, asumir que un atacante ya ha puesto en peligro uno de tus activos o usuarios, y **diseñar tu red y las protecciones de seguridad de forma que se limite su capacidad de moverse lateralmente hacia sistemas más críticos.**

Verás términos como «microsegmentación» y asserted identity en los debates sobre Zero Trust. Pero cualquiera que lleve el tiempo suficiente reconocerá que esta

arquitectura se basa en los principios de seguridad existentes desde hace mucho tiempo, como la verificación de identidades sólidas y la idea del mínimo privilegio.

Esto no quiere decir que la arquitectura Zero Trust sea una palabra de moda o innecesaria. Al contrario, es exactamente lo que las organizaciones deberían haber estado haciendo desde los orígenes de las redes. Predecimos que, en 2022, la mayoría de las organizaciones promulgarán finalmente algunos de los conceptos de seguridad más antiguos en todas sus redes, y lo llamarán **Zero Trust.**

Fuente de información: revistacloudcomputing.com