Las cinco principales tendencias de ciberseguridad para este 2023

nexus aggity

A medida que han proliferado los ataques y han aumentado las posibles sanciones, la ciberseguridad se ha convertido en una prioridad en todos los niveles de la organización.

En los últimos años hemos visto cómo el tema de la ciberseguridad ha pasado del departamento de TI a la sala de juntas. A medida que han proliferado los ataques y han aumentado las posibles sanciones, tanto normativas como en términos de pérdida de confianza de los clientes, **se ha convertido en una prioridad en todos los niveles de la organización.**

A menudo pensamos en la ciberseguridad como una batalla continua entre hackers y delincuentes y expertos en seguridad, que se intensifica constantemente debido a los constantes avances tecnológicos. Este es el lado «glamuroso» del negocio que a veces vemos representado en programas de televisión y películas. Y en efecto, las amenazas provienen a veces de Estados extranjeros hostiles o de astutos cerebros criminales expertos en tecnología. Sin embargo, es probable que surjan amenazas debido a **redes mal protegidas** que dejan datos confidenciales expuestos accidentalmente o empleados desprevenidos o indiscretos que usan dispositivos no seguros mientras trabajan desde casa.

El cambio hacia una cultura de trabajo en casa y a distancia que comenzó durante la pandemia del Covid-19 y que ha persistido en muchas organizaciones, así como la propagación del internet de las cosas (IoT) en todos los ámbitos de la empresa y la sociedad, significa que nunca ha habido más oportunidades para que la seguridad laxa cause dolores de cabeza y gastos. Por ello, la ciberseguridad es una prioridad en la agenda de todo el mundo en 2023, así que a continuación veremos algunas de las **tendencias clave del próximo año:**

Internet de las cosas y seguridad en la nube

Cuantos más dispositivos conectamos entre sí y en red, más puertas y ventanas potenciales existen para que los atacantes puedan utilizar para entrar y acceder a nuestros datos. Y en 2023, según predicen los analistas de Gartner, habrá 43.000 millones de dispositivos conectados al IoT en el mundo.

Los dispositivos IoT –que van desde los dispositivos portátiles inteligentes hasta los electrodomésticos, los coches, los sistemas de alarma de los edificios y la maquinaria industrial– han demostrado ser a menudo un problema para los responsables de la ciberseguridad. Esto se debe a que, como a menudo no se utilizan directamente para almacenar datos sensibles, los fabricantes no siempre se han centrado en mantenerlos seguros con parches y actualizaciones de seguridad frecuentes. Esto ha cambiado recientemente, ya que se ha demostrado que incluso cuando no almacenan datos en sí mismos, los atacantes pueden encontrar a menudo formas de utilizarlos como puertas de entrada para acceder a otros dispositivos en red que sí podrían hacerlo. Hoy en día, por ejemplo, es menos probable encontrar un dispositivo que se envíe con una contraseña o un PIN por defecto que no requiera que el usuario establezca el suyo propio, como ocurría con

frecuencia en el pasado.
En 2023, deberían entrar en vigor una serie de iniciativas gubernamentales en todo el mundo diseñadas para aumentar la seguridad de los dispositivos conectados, así como de los sistemas en la nube y las redes que los unen. Esto incluye un sistema de etiquetado para los dispositivos IoT que se pondrá en marcha en los Estados Unidos para proporcionar a los consumidores información sobre las posibles amenazas a la seguridad que plantean los dispositivos que llevan a sus hogares.

La ciberseguridad desde el hogar se convierte en una prioridad para las empresas.

ciberseguridad para muchas organizaciones ha sido asegurar los millones de dispositivos en todo el mundo que se utilizan para el trabajo en casa y a distancia desde el comienzo de la pandemia. Antes de la pandemia, cuando todos trabajábamos en la oficina, era bastante sencillo para los agentes de seguridad, probablemente ubicados en los departamentos de TI, comprobar y actualizar regularmente los ordenadores portátiles y los teléfonos inteligentes de la empresa. Esto hacía que fuera relativamente sencillo asegurarse de que estaban libres de spyware y malware y de que ejecutaban las últimas versiones de software antivirus y otras medidas preventivas. En 2023, cuando los trabajadores son más propensos que nunca a utilizar dispositivos personales para conectarse de forma remota a las redes de trabajo, ha surgido un nuevo conjunto de desafíos.

Conectarse a las redes con dispositivos no seguros puede llevar a los empleados a ser víctimas involuntarias de ataques de phishing, en los que los atacantes engañan a los usuarios para que divulguen sus contraseñas. Con un mayor número de personas empleadas a distancia, es cada vez más probable que nos encontremos trabajando en equipos en los que no nos conocemos tan bien y corremos el riesgo de caer en estafas de suplantación de identidad. También permite los ataques de ransomware, en los que se inyecta software en las redes que borra datos valiosos a menos que los usuarios paguen un rescate a los atacantes. El riesgo de esto también aumenta en situaciones de trabajo a distancia, donde es más probable que los dispositivos queden desatendidos.

Los atacantes internacionales patrocinados por el Estado se dirigen tanto a las empresas como a los gobiernos.

Los estados-nación participan con frecuencia en el ciberespionaje y el sabotaje en un intento de socavar gobiernos hostiles o competidores o de acceder a secretos. Sin embargo, hoy en día, es cada vez más probable que las empresas y las organizaciones no gubernamentales (ONG) se encuentren en el punto de mira de los agentes estatales.

Desde el ataque del ransomware WannaCry de 2017, que se cree que fue perpetrado por hackersafiliados al gobierno de Corea del Norte, se han producido cientos de miles de ataques a servidores de todo el mundo que las agencias de seguridad creen que pueden ser rastreados hasta gobiernos extranjeros.

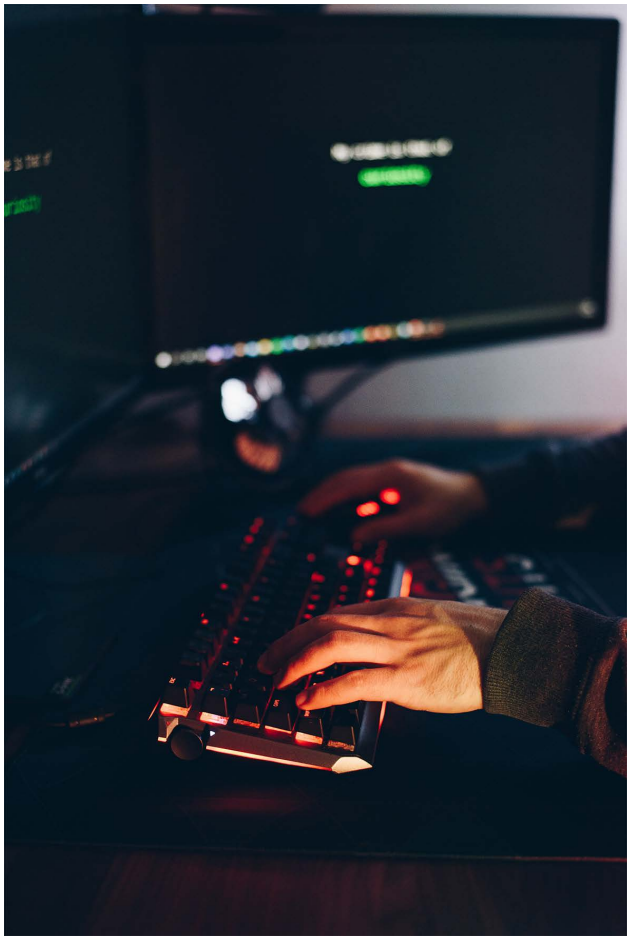
En 2023, más de setenta países van a celebrar elecciones gubernamentales, acontecimientos que suelen ser objeto de ataques por parte de intereses extranjeros hostiles. Además de la piratería informática y los ciberataques a las infraestructuras, estos ataques adoptarán la forma de **campañas de desinformación en las redes sociales.** A menudo se trata de influir en los resultados a favor de los partidos políticos cuyas victorias beneficiarían al gobierno del Estado hostil. Y la guerra cibernética seguirá siendo, sin duda, un elemento clave en los conflictos armados, y un analista ha dicho sobre la guerra entre Rusia y Ucrania que «lo digital es una parte tan importante de esta guerra como los combates sobre el terreno».

La inteligencia artificial (IA) desempeña un papel cada vez más destacado en la ciberseguridad.

Como el número de intentos de ciberataque ha crecido rápidamente, cada vez es más difícil para los expertos en ciberseguridad humana reaccionar ante todos ellos y predecir dónde se producirán los próximos ataques más peligrosos. Aquí es donde entra en juego la IA. Los algoritmos de aprendizaje automático pueden examinar la enorme cantidad de datos que se mueven por las redes en tiempo real de forma mucho más eficaz de lo que podrían hacerlo los humanos y aprender a reconocer patrones que indiquen una amenaza. Según IBM, las empresas que utilizan la IA y la automatización para detectar y responder a las violaciones de datos **ahorran una media de tres millones de dólares en comparación con las que no lo hacen.**

Desgraciadamente, gracias a la creciente disponibilidad de la IA, los hackers y los delincuentes también son cada vez más hábiles en su uso. Los algoritmos de IA se utilizan para identificar sistemas con una seguridad débil o que probablemente contengan datos valiosos entre los millones de ordenadores y redes conectados a Internet. También se puede utilizar para crear un gran número de correos electrónicos de phishing personalizados, diseñados para engañar a los receptores para que divulguen información sensible, y cada vez son más buenos para evadir los sistemas automatizados de defensa del correo electrónico diseñados para filtrar este tipo de correos. La IA se ha utilizado incluso para **«clonar»** artificialmente la voz de altos ejecutivos y luego **autorizar fraudulentamente las transacciones.**

Por ello, el uso de la IA en la ciberseguridad se conoce a veces como una «carrera armamentística», ya que los hackers y los agentes de seguridad compiten para asegurarse de que los algoritmos más nuevos y sofisticados están trabajando de su lado y no para la oposición. Se ha predicho que para 2030 el mercado de productos de ciberseguridad con IA tendrá un valor cercano a los 139.000 millones de dólares, lo que supone un **aumento de casi diez veces el valor del mercado de 2021.**



Construir una cultura consciente de la seguridad.

Tal vez el paso más importante que se puede dar en cualquier organización es asegurarse de que está trabajando para iniciar y fomentar una cultura de concienciación en torno a las cuestiones de ciberseguridad. Hoy en día, ya no es suficiente que los empresarios o los empleados se limiten a pensar que la ciberseguridad es una cuestión de la que debe ocuparse el departamento de TI. De hecho, desarrollar una conciencia de las amenazas y tomar precauciones básicas para garantizar la seguridad debería ser una parte fundamental de la descripción del trabajo de todos en 2023.

Los ataques de phishing se basan en métodos de **«ingeniería social»** para engañar a los usuarios para que divulguen información valiosa o instalen malware en sus dispositivos. No es necesario tener conocimientos técnicos para aprender a ser consciente de este tipo de ataques y tomar las precauciones básicas para evitar ser víctima. Del mismo modo, los conocimientos básicos de seguridad, como el uso seguro de las contraseñas y la comprensión de la autenticación de dos factores (2FA), deberían enseñarse de forma generalizada y actualizarse continuamente. Tomar este tipo de precauciones básicas para fomentar una cultura de concienciación sobre la **ciberseguridad debería ser un elemento central de la estrategia empresarial** de las organizaciones que quieran asegurarse de que están preparadas y son resistentes en los próximos doce meses.

Autor: BERNARD MARR

Fuente de información: www.forbes