Un informe revela la vulnerabilidad de las empresas argentinas ante ataques hackers

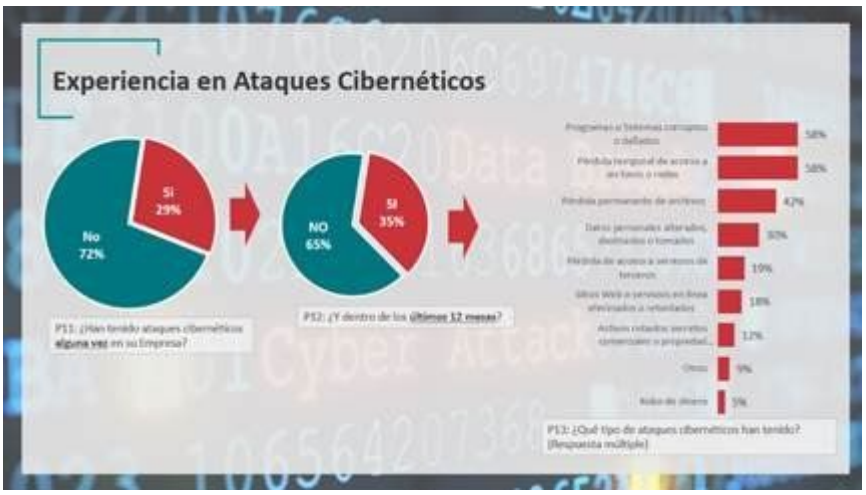
07/02/2020

El empleado recibió una videollamada de su jefe y realizó la transferencia bancaria tal cual le ordenó, hasta que unos minutos más tarde descubrió que su jefe nunca lo había llamado. El caso es verdadero y el ataque se valió de lo que se conoce como deep fake, videos que aprovechan la Inteligencia Artificial para simular escenas de envidiable realismo. **Los ciberataques se volvieron cada día más ingeniosos.**

Los hackers, creativos y organizados, no reconocen fronteras y están virando hacia una faceta más ambiciosa, en la que dejan de tener al usuario final como principal objetivo y centran su mayor poder de daño en las compañías. El problema golpea las puertas: **el 29% de las empresas argentinas admitió que fue víctima de ciberataques, un tercio de ellas durante el último año, sin embargo no es una de sus preocupaciones prioritarias.**

“Nos enfrentamos a un paradigma de seguridad más sofisticado. Es un adversario totalmente distinto, casi una industria con empresas bien financiadas, incluso hay gobiernos por detrás”, explicó **Ignacio Conti**, especialista en Ciberseguridad de **Microsoft** para Argentina y Chile, durante un encuentro con la prensa del que participó **Ámbito** para presentar un informe sobre el estado de prevención de las empresas en nuestro país realizado para la firma tecnológica

por la consultora **Ipsos**.

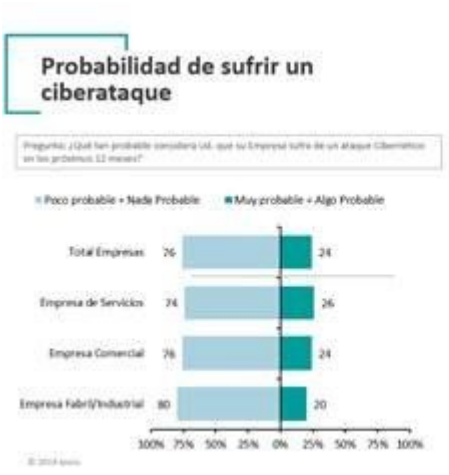


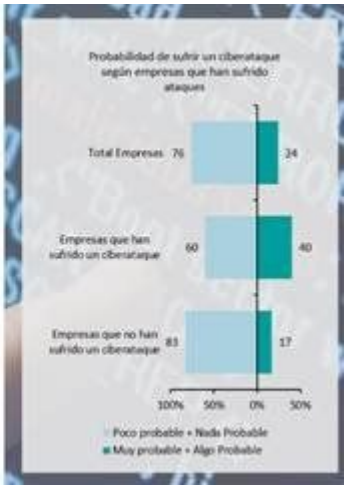
Las consecuencias del accionar de esos carteles hackers para las firmas son amargas: se calcula que cada ciberataque cuesta en el promedio global unos u$s3,9 millones. Y el futuro no es prometedor: la sangría total de dólares para 2022 se calcula en 8 billones. **“Hay que replantearse el tema de que la ciberseguridad es cara, porque el que mejor se proteja tendrá una ventaja y terminará ahorrando dinero”**, señaló Conti.

Según informó, a nivel de los usuarios finales la tendencia es una desaceleración de los virus y troyanos clásicos, al igual que de las maniobras para adueñarse del control de las computadoras, pero **lo que no deja de crecer es el pishing**, esos mails o mensajes de WhatsApp que simulan ser de nuestro banco o de una promoción atractiva y nos conducen a sitios insospechados y fraudulentos. **“Todavía hay mucha gente que hace click donde no debe”,** apuntó.

Los ataques tienen como fin adueñarse de la identidad digital de las víctimas, porque además del poder de cometer ilícitos cotizan alto en la Dark Web, esa parte de Internet que

funciona casi sin controles, donde una cuenta de correo electrónico puede valer entre 2 y 3 dólares y una ficha con datos bancarios o de la prepaga de salud unos u$s200.





Para **Sebastián Stranieri**, CEO de **VU Security**, firma especializada en prevención de fraude y protección de la identidad, el futuro es ir hacia la creación de una identidad única y descentralizada y que sea verificada con un historial del uso de cada dispositivo. **“Debe ser coherente y consistente, cuando se mide el comportamiento, dónde se lo usa, cuándo, de qué manera, esa será la fórmula”**.

El especialista consideró que “aunque parezca sorprendente, la Argentina está bastante avanzada, por ejemplo, se puede validar los datos con el DNI digital”.

Stranieri detalla que la IA en malas manos puede multiplicar el efecto nocivo, como hacer estadísticas y predecir cuál empleado es más vulnerable al ataque. Incluso hay un grupo que dice tener una base con 400 millones de rostros que puede jaquear los sitios de reconocimiento facial.

Las recomendaciones, las de siempre: actualizar los sistemas operativos de smartphones, computadoras notebooks y todos los dispositivos que estén conectados, cifrar los equipos, cambiar las claves periódicamente, no confiar en una sola password y, de una vez por todas, dejar de utilizar la bendita contraseña “1234”. Por último, cada tanto hacer un chequeo pormenorizado de todos los ítems del resumen bancario.

El año pasado la ofensiva logró vulnerar unas 3.000 millones de cuentas en el mundo, 44 millones de ellas coincidentes con usuarios de Microsoft. Un volumen de información gigantesco que hace necesario el uso de Inteligencia Artificial para poder procesarlo con eficiencia y velocidad. “La Nube” es otra gran aliada, porque las herramientas allí están siempre actualizadas y al alcance de la mano.

Lo que se percibió en los últimos tiempos es que los ataques están siendo cada vez más dirigidos a empresas que a usuarios finales, lo que debería llevar a las compañías a adoptar políticas de “confianza cero”, es decir, asumir que toda persona que ingresa al sistema intentará vulnerarlo,

desconfiando de todo y de todos, para obligar a los cibercriminales a contar con factores de autenticación adicionales para llegar a las partes más sensibles de la red. Pero poco de esto parece estar pasando en nuestro país.

Baja percepción de riesgo

“Las amenazas a la ciberseguridad no son una preocupación prioritaria para las empresas en Argentina. Existe una baja percepción de riesgo, derivado principalmente de la poca frecuencia con que se perciben en este tipo de incidentes. La mayoría de los entrevistados no considera a a nuestro país como un objetivo de ataques. Esta percepción genera un riesgo latente, ya que muchas compañías no están preocupadas de protegerse”, resumió **Brenda Lynch**, directora de Asuntos Públicos de **Ipsos**.

La encuesta relevó a 200 altos directivos de empresas grandes y pymes argentinas y multinacionales:

-El 29% admitió que sufrió un ataque cibernético en su empresa, con la pérdida de archivos, programas dañados y alteración o destrucción de datos personales como principales inconvenientes. Entre los afectados, las soluciones pasaron por comprar e instalar software de seguridad, capacitar al personal y contratar a un proveedor externo.

-El 51% de los entrevistados considera estar muy vulnerable a un ciberataque.

-Pero el 44% dijo que es una preocupación alta.

-Solo el 24% lo considera muy probable en el próximo año.

-Y apenas el 17% contrató a un especialista en ciberseguridad.

Los dos temas que más preocupan al empresariado son, en ese orden:

-La fuga de información de la empresa.

-Que peligre la continuidad del negocio.

Y son profundamente optimistas: pese al crecimiento de la ofensiva hacker mundial, solo el 39% cree que nuestro país está entre los objetivos de los ataques y **el 27% reconoció que, simplemente, no tomará ninguna medida para prevenirse.**

Fuente: Ámbito