



ECONOMÍA Y EMPRESAS > PROTECCIÓN

Ante el aumento del teletrabajo, ¿cómo pueden mejorar la ciberseguridad las empresas?

Crece el trabajo remoto y también los ciberataques. Por eso, los expertos proponen algunas medidas que pueden tomar las empresas para cuidarse



Tiempo de lectura: 7'

14 de diciembre de 2020 a las 16:46

A+

A-

La abrupta transición hacia la transformación digital tomó a varias empresas desprevenidas y sin la contención de seguridad necesaria para tener a sus trabajadores de forma remota.

“En lo que llevamos de 2020, la incapacidad para facilitar el teletrabajo sin exponer información confidencial ha hecho que casi el 25 % de las empresas deban asumir costos inesperados para hacer frente a las brechas de la ciberseguridad y las infecciones de malware. Si las empresas no replantean sus enfoques en materia de seguridad, la ciberdelincuencia seguirá creciendo y se aprovechará de los trabajadores remotos para usarlos como puntos de entrada perfectos a los ecosistemas de TI de las empresas”, dice la periodista Aina Pou Rodríguez del sitio español CyberSecurity News, especializado en información sobre Ciberseguridad y Fintech.

Según Pou Rodríguez, “el auge previsto de nuevas tecnologías (como el 5G) en el próximo año probablemente hará aumentar la sofisticación de los ciberataques. Por consiguiente, es imprescindible que las empresas financieras (y todas las compañías que operan en sectores altamente regulados) adopten un enfoque proactivo respecto a la protección de los datos”.

El aumento de la adopción de la nube, así como del análisis de datos basado en Inteligencia Artificial y Machine Learning permite a las empresas ampliar sus negocios, pero también las puede dejar más vulnerables. Este aumento del uso de herramientas tecnológicas y de la conectividad de los usuarios es una tendencia que lejos está de desaparecer, por lo que es crucial tomar medidas para asegurar la confidencialidad y seguridad de los datos y de las interacciones en la red.

“Los ciberdelitos notificados al Centro de Quejas de Crímenes en Internet del FBI (IC3) prácticamente se han multiplicado por cuatro desde el comienzo de la pandemia”, resalta la periodista especializada.

Principales casos de ciberataques y cómo evitarlos

La empresa tecnológica uruguaya Isbel informó en un comunicado que “a medida que los casos de covid-19 crecían, se constató un aumento en ataques cibernéticos, en particular aquellos vinculados a la ingeniería social: una práctica que, en contraposición a otras que explotan directamente vulnerabilidades de los sistemas informáticos, utilizan la manipulación o engaño a los usuarios finales para que, sin saberlo, accedan a contenido malicioso o divulguen información confidencial”.

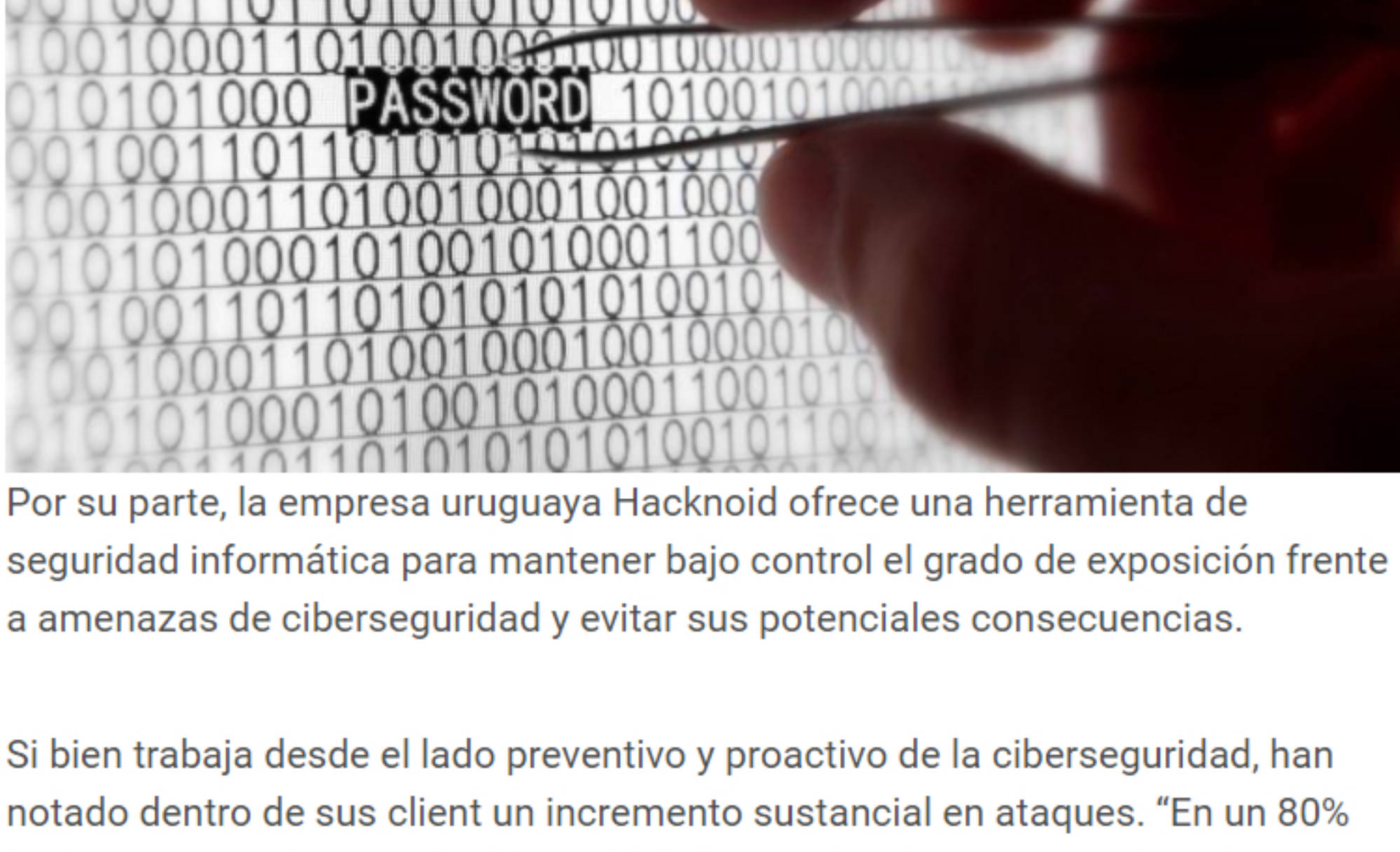
Señala que, según un reporte lanzado por la OEA y el BID, Uruguay es uno de los países que se encuentran mejor posicionado en ciberseguridad de Latinoamérica, gracias a que existe mucha conciencia sobre el tema, pero los ciberataques no son ajenos al país.

Los principales incidentes durante este año que detectó la división de Ciberseguridad de Isbel fueron la intervención de intrusos en videoconferencias; el robo de datos, tanto personales como de las empresas; el phishing o la estafa mediante la suplantación de identidad y los ataques a los dispositivos de IoT (Internet of Things), que en el caso de una empresa puede referir a sensores que miden la temperatura de las heladeras en un frigorífico o el controlador de los aires acondicionados de un data center. “Si un usuario no autorizado tuviera acceso a este sistema, podría alterar el funcionamiento previsto y esto tendría un fuerte impacto en la actividad empresarial”, explican desde Isbel.



“Muchas organizaciones no estaban preparadas a nivel de infraestructura ni de concientización sobre los riesgos que implica trabajar desde casa y se vieron forzadas a iniciar una transformación digital apresurada y poco planificada. Son muchos los riesgos que involucran al teletrabajo en estas condiciones, como la exposición de los usuarios a variados malware (programas maliciosos) o virus”, señalan desde Isbel. Esto sumado a la falta de concientización de los empleados, sirvió de campo fértil para los ciberdelincuentes al acecho de datos y a prácticas como el ataque de ransomware, “un tipo de malware en el que los atacantes cifran los datos de una computadora o sistema. Así, los datos permanecen inaccesibles para el propietario y luego los atacantes exigen una recompensa económica para devolverlos”.

Por otro lado, según una encuesta global de Open Text, las técnicas de phishing aumentaron un 34% desde el año pasado. La forma de captar a los usuarios para que hagan clic en un enlace o brinden información suele ser mediante noticias falsas, en su mayoría, vinculadas al



Por su parte, la empresa uruguaya Hacknoid ofrece una herramienta de seguridad informática para mantener bajo control el grado de exposición frente a amenazas de ciberseguridad y evitar sus potenciales consecuencias.

Si bien trabaja desde el lado preventivo y proactivo de la ciberseguridad, han notado dentro de sus client un incremento sustancial en ataques. “En un 80% de las empresas hemos tenido en distintos grados, se ha transformado de ciberseguridad. Según informes actuales del Harvard Business Review e IDC, el incremento, que venía ya siendo exponencial desde 2017, se ha transformado en una gráfica de *hockey stick* sorprendente, sobre todo debido a las brechas que se han abierto como consecuencia de una transformación digital forzosa en muchas organizaciones potenciada por la pandemia y por ende, por el teletrabajo”, explica Rosina Ordoqui, CEO de Hacknoid.

Uno de los elementos que las empresas deben tener en cuenta a la hora de implementar el teletrabajo es tener bajo control los dispositivos que se envían a los hogares, y que se conecten a la red corporativa de forma limitada y segura utilizando Redes Privadas Virtuales (VPN's), así como, “prestar especial atención a mantener el control de las actualizaciones de los sistemas, antivirus, firewalls y demás herramientas y softwares en cada punto remoto, que en esta nueva modalidad serán nuevos puntos de entrada de posibles vectores de ataque”, explica Ordoque.

Otro punto que destaca la CEO, es que la mayoría de los ataques ocurridos no vienen de grandes ingenierías de infiltración, sino de aprovecharse de vulnerabilidades “conocidas”.

¿Qué hacer para estar más preparados?

Los expertos en Ciberseguridad de Isbel recomiendan:

- Reforzar el estado de la seguridad informática en las organizaciones. Se debe poner especial atención en la adopción de políticas y procedimientos orientados a proteger los sistemas. Por ejemplo, es aconsejable realizar diagnósticos periódicos de seguridad, que permitan a los administradores comprender el estado actual de la ciberseguridad y ejecutar acciones correctivas. Otra práctica recomendable es incorporar sistemas de respaldo robustos para poder restaurar la información en caso de pérdida o robo.

- Se recomienda que los teletrabajadores utilicen soluciones de tipo VPN, es decir, una conexión segura entre la computadora del colaborador y la red de la empresa. Esto permite que los datos sean más difíciles de interpretar para cualquier intruso que esté interceptando la comunicación.

- Además, existen herramientas para restringir la navegación de los usuarios remotos, por ejemplo, prohibiendo aquellos sitios con mayores peligros potenciales. También es posible bloquear de forma automática el acceso a links sospechosos contenidos en los mails que llegan a la bandeja de entrada.

- Dado el aumento en ataques basados en ingeniería social, es fundamental una correcta y constante capacitación a los usuarios. También se recomienda analizar que las configuraciones de los servicios y sistemas que utilicen —y que estén expuestos a internet— sean acordes a las mejores prácticas y sean monitoreados de forma continua.

La CEO de Hacknoid recomienda

- Mejorar la ecuación entre automatización y recursos humanos comprometidos: utilizar herramientas que automaticen todo lo posible y los recursos técnicos capacitados centrarlos en los puntos estrictamente necesarios. Esto se debe fundamentalmente a que hoy por hoy, el recurso humano con conocimientos avanzados de seguridad es cada vez más escaso y por ende costoso.

- Enfocarnos en desarrollar un proceso práctico y cíclico: no podemos perder demasiado tiempo en laboratorios y análisis que no nos conduzcan a una rápida resolución de los problemas que se reportan como críticos. Es fundamental la agilidad para habilitar los procesos de negocio y su operación bajo un marco seguro.

- Intentar dar los pasos necesarios para una mirada proactiva. Posicionarnos en el “antes” de que ocurra y no solo en la reacción. Siempre es menos costosa la prevención que la reactivación, en caso de un incidente. Y ser conscientes de que tarde o temprano nos va a tocar.

- Adoptar marcos que ayuden a ordenar el proceso, aunque muchas veces debamos adaptarlos a las necesidades y recursos disponibles. Un marco siempre nos da un punto de partida y un orden para no perderse en el camino (Por ejemplo ISO 27.000; NIST, entre otros). No se trata de ser perfectos, pero si uno de los menos “fáciles” de ser atacados.

- Involucrar a más gente en el proceso y reordenar el rol del CISO/Oficial de seguridad o responsable de la materia en el organigrama. Según donde se ubique en la jerarquía y la independencia de su rol, se define la real importancia que la organización le está prestando a la materia y por ende los recursos y apoyo que se le prestará.

- Además, existen herramientas para restringir la navegación de los usuarios remotos, por ejemplo, prohibiendo aquellos sitios con mayores peligros potenciales. También es posible bloquear de forma automática el acceso a links sospechosos contenidos en los mails que llegan a la bandeja de entrada.

- Dado el aumento en ataques basados en ingeniería social, es fundamental una correcta y constante capacitación a los usuarios. También se recomienda analizar que las configuraciones de los servicios y sistemas que utilicen —y que estén expuestos a internet— sean acordes a las mejores prácticas y sean monitoreados de forma continua.

- Adoptar marcos que ayuden a ordenar el proceso, aunque muchas veces debamos adaptarlos a las necesidades y recursos disponibles. Un marco siempre nos da un punto de partida y un orden para no perderse en el camino (Por ejemplo ISO 27.000; NIST, entre otros). No se trata de ser perfectos, pero si uno de los menos “fáciles” de ser atacados.

- Involucrar a más gente en el proceso y reordenar el rol del CISO/Oficial de seguridad o responsable de la materia en el organigrama. Según donde se ubique en la jerarquía y la independencia de su rol, se define la real importancia que la organización le está prestando a la materia y por ende los recursos y apoyo que se le prestará.

- Además, existen herramientas para restringir la navegación de los usuarios remotos, por ejemplo, prohibiendo aquellos sitios con mayores peligros potenciales. También es posible bloquear de forma automática el acceso a links sospechosos contenidos en los mails que llegan a la bandeja de entrada.

- Dado el aumento en ataques basados en ingeniería social, es fundamental una correcta y constante capacitación a los usuarios. También se recomienda analizar que las configuraciones de los servicios y sistemas que utilicen —y que estén expuestos a internet— sean acordes a las mejores prácticas y sean monitoreados de forma continua.

- Adoptar marcos que ayuden a ordenar el proceso, aunque muchas veces debamos adaptarlos a las necesidades y recursos disponibles. Un marco siempre nos da un punto de partida y un orden para no perderse en el camino (Por ejemplo ISO 27.000; NIST, entre otros). No se trata de ser perfectos, pero si uno de los menos “fáciles” de ser atacados.

- Involucrar a más gente en el proceso y reordenar el rol del CISO/Oficial de seguridad o responsable de la materia en el organigrama. Según donde se ubique en la jerarquía y la independencia de su rol, se define la real importancia que la organización le está prestando a la materia y por ende los recursos y apoyo que se le prestará.

- Además, existen herramientas para restringir la navegación de los usuarios remotos, por ejemplo, prohibiendo aquellos sitios con mayores peligros potenciales. También es posible bloquear de forma automática el acceso a links sospechosos contenidos en los mails que llegan a la bandeja de entrada.

- Dado el aumento en ataques basados en ingeniería social, es fundamental una correcta y constante capacitación a los usuarios. También se recomienda analizar que las configuraciones de los servicios y sistemas que utilicen —y que estén expuestos a internet— sean acordes a las mejores prácticas y sean monitoreados de forma continua.

- Adoptar marcos que ayuden a ordenar el proceso, aunque muchas veces debamos adaptarlos a las necesidades y recursos disponibles. Un marco siempre nos da un punto de partida y un orden para no perderse en el camino (Por ejemplo ISO 27.000; NIST, entre otros). No se trata de ser perfectos, pero si uno de los menos “fáciles” de ser atacados.

Comentarios

0 comentarios

Ordenar por Más recientes

Agregar un comentario...

Plugin de comentarios de Facebook

Editar



El Observador



Member

Punta del Este: ¿ciudad resort para vivir o segunda vivienda?

INVERSIONES

"Van a venir conscientes de que somos más caros": la espera de una llegada "masiva" de argentinos

CIBERSEGURIDAD

BCU advierte por llamadas telefónicas que solicitan datos sobre tarjetas de débito y crédito



ÚLTIMAS NOTICIAS

09:19 MERCADOS

La economía digital, un enorme desafío para los reguladores

09:17 EMERGENCIA SANITARIA

Murió por covid-19 el cardiólogo Enrique Soto

08:41 CONGRESO DE INTENDENTES

Intendente de Rivera propone ajustar patente a valores de 2015 por pandemia

08:40 BBC NEWS MUNDO

Elecciones en Estados Unidos: las declaraciones de Joe Biden después de que el Colegio Electoral confirmara su victoria

08:14 BBC NEWS MUNDO

Coronavirus: por qué incluso después de ponerte la vacuna contra la covid-19 deberás seguir usando mascarilla

06:29 BBC NEWS MUNDO

Piotr Cywiński, el historiador polaco que se ofrece a pasar un mes en prisión en Nigeria a cambio de que liberen a un niño preso por blasfemia

