RECOMENDACIONES DE CIBERSEGURIDAD DURANTE LA PANDEMIA DE COVID-19

BDO

RECOMENDACIONES DE CIBERSEGURIDAD DURANTE LA PANDEMIA DE COVID-19

A nivel mundial, las diferentes industrias han visto un fuerte aumento en los ataques cibernéticos desde que el gobierno chino reveló la propagación del coronavirus o COVID-19 dentro de China e internacionalmente.

Los ataques cibernéticos se centraron, particularmente, en los sistemas de salud y atención médica mediante el uso de 'spear phishing' y 'ransomware', ataques de suplantación de identidad que comprometen el correo electrónico comercial, ataques cibernéticos a la cadena de suministro centrados en aquellas operaciones de fabricación relocalizadas fuera de China y ciberataques de 'denegación de servicio' (DDoS) en las industrias de energía, hotelería y viajes.

Con la difusión de COVID-19 en el resto del mundo, aumentarán las demandas de los servicios de soporte TI en casi todas las industrias, ya que los empleados, estudiantes, docentes universitarios y otros en todo el mundo están trabajando o estudiando de forma remota desde sus hogares para reducir la propagación del virus.

Como resultado, los grupos de ciberataques estatales y los grupos de ciberataques criminales, están aprovechando al máximo para atacar las vulnerabilidades cibernéticas en industrias seleccionadas, especialmente aquellas más afectadas por la crisis actual.

Si se toma en cuenta que, según los últimos estudios de Gartner, el 40% o más de las vulnerabilidades cibernéticas están directamente relacionadas con el comportamiento de los empleados, es vital que las organizaciones se centren más en sus empleados a través de la conciencia de seguridad cibernética, educación, capacitación y uso de simulaciones para crear un firewall humano más fuerte para proteger sus activos digitales vitales.

Después de todo, según los últimos hallazgos de IBM Security, el costo promedio de una violación de datos cibernéticos ahora es de $8.2M.

De seguido ofrecemos **cinco recomendaciones** principales de ciberseguridad para reducir la probabilidad de un ciberataque o una violación de datos significativa, así como para mitigar los impactos financieros y de reputación asociados a ataques de esa naturaleza:

Adaptado por Javier León de *'Top Cybersecurity Recommendations Amid Covid-19'*, BDO USA, Marzo 2020.

FOMENTAR LA CULTURA ORGANIZACIONAL DE CIBERSEGURIDAD:

Asegúrese que el equipo gerencial promueva y respalde de manera consistente durante la crisis a todos los empleados que practiquen políticas, procesos y procedimientos de ciberseguridad efectivos. Para ello, existen múltiples recursos en internet que permiten de forma rápida y barata reforzar esa cultura. Los mensajes, banners y comunicados oficiales constantes de la organización en ese sentido, se hacen indispensables en momentos de crisis.

IMPLEMENTAR 'QUIZES' DE CIBERSEGURIDAD:

Una de las mejores formas de mantener al personal alerta es evaluar a los miembros de la organización sobre su conocimiento del tema durante el manejo de la crisis, estos quizes pueden incluir:

- Medidas de protección del correo electrónico.
- Medidas de prevención en el uso de dispositivos externos que se utilizan en los equipos de la organización.
- Mecanismos de comunicación de dudas o alertas de eventuales riesgos.
- Revisión de la comprensión de los términos técnicos asociados al tema.

En ese sentido, aplicaciones como Survey Monkey tienen formatos de quizes predeterminados que pueden aplicarse fácilmente y de forma gratuita a organizaciones de todo tamaño.

ESTABLECER UN PLAN RÁPIDO DE RESPUESTA A INCIDENTES DE CIBERATAQUE:

La cabeza de TI de la organización junto con la alta gerencia, deben establecer el plan de respuesta en caso de ciberataque durante el tiempo de crisis. Deben además desarrollar un manual corto ('one pager') para que los colaboradores sepan perfectamente que hacer en caso de un ciberataque.

REALIZAR MONITOREO, DETECCIÓN Y RESPUESTA (MDR) 24 X 7 X 365:

Las implicaciones que esto puede tener en el personal y en el funcionamiento de la organización deben ser explicadas en detalle por cada gerente a su equipo y mitigadas hasta donde sea posible.

REVISAR LOS PLANES EXISTENTES:

Las implicaciones que esto puede tener en el personal y en el funcionamiento de la organización deben ser explicadas en detalle por cada gerente a su equipo y mitigadas hasta donde sea posible.

Adaptado por Javier León de *'Top Cybersecurity Recommendations Amid Covid-19'*, BDO USA, Marzo 2020.

ADAPTADO POR:
Javier León
Socio Director de Consultoría
jleon@bdo.cr

Oficentro Ejecutivo La Sabana
Edificio 6, 5to Piso
San José, Costa Rica
Tel.: +506 2231 7060

Paseo Colón
Torre Mercedes, Piso 8
San José, Costa Rica
Tel.: +506 2248 0808

www.bdo.cr
www.bdo.global