www.mexis.net

EL COSTO OCULTO DE LOS CIBERATAQUES:

CUANDO LA TECNOLOGÍA AMENAZA LA EXISTENCIA EMPRESARIAL

mexis aggity

Las consecuencias ante un incidente de ciberseguridad desde el punto de vista de reputación pocas veces son consideradas.

Los clientes pueden perder la confianza, los socios dudan en continuar trabajando con la empresa y la imagen pública puede verse afectada de una forma inmediata.

Las empresas y sus directivos saben que un ciberataque puede significar una pérdida de reputación y un gasto para poder regresar a la operación, pero pocas veces hablamos de todo lo que puede llegar a impactar. **¿puede una empresa cerrar operaciones definitivamente por un ciberataque?**

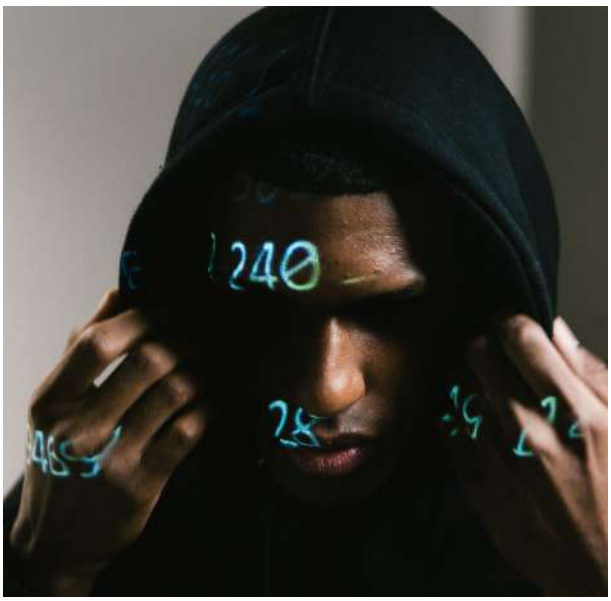
Las consecuencias ante un incidente de ciberseguridad desde el punto de vista de reputación pocas veces son consideradas. Los clientes pueden perder la confianza, los socios dudan en continuar trabajando con la empresa y la imagen pública puede verse afectada de una forma inmediata. Justo eso le pasó a Sony Pictures cuando se filtró información confidencial y se vio afectada su reputación.

Pero **¿qué pasa cuando el daño trasciende a un tema técnico?** Es importante entender que un ciberataque no es solo un tema técnico; es un desafío a toda la organización. El ataque de ransomware a la empresa Colonial Pipeline en 2021 detuvo no solo las operaciones de la red principal de oleoductos en los Estados Unidos, sino que también causó una crisis de suministro de combustibles a nivel nacional: la interrupción operativa y financiera fue inmediata y severa. **Un ataque como el descrito, evidencia cómo la infraestructura crítica de un país, administrada por una empresa, puede ser vulnerada afectando no solo el funcionamiento sino la economía y el bienestar de una parte del país.**

Uno de los ejemplos más impactantes de estas consecuencias ante un ciberataque es el caso de la cadena de supermercados sueca llamada Coop. **En 2021, esta empresa fue víctima de un ataque de ransomware que afectó a más de 350 organizaciones a nivel mundial.** El ataque se propagó por medio de un software de servicios de TI donde las empresas que usaban dicho software se vieron afectadas: Coop era un cliente final de ese software. **Como resultado, Coop tuvo que cerrar alrededor de 800 tiendas y requirieron alrededor de 300 personas para poder regresar a la operación reinstalando prácticamente toda la infraestructura.** Tardaron más de una semana en regresar a una operación limitada. Este ejemplo denota la interconexión y dependencia que las empresas tienen a su cadena de suministro y cómo un punto vulnerable puede generar un efecto dominó.

El impacto humano de los ciberataques pocas veces se considera, ya que esto también puede llegar a la pérdida de empleos, afectando la moral o generando un ambiente de desconfianza mientras se trata de regresar a la operación.

La empresa tecnológica Code Spaces se colocaba como una empresa prometedora que ofrecía servicios de gestión de código fuente. **En 2014, sufrió un ciberataque donde los atacantes lograron tener acceso a eliminar datos, copias de seguridad y configuraciones. A pesar de los esfuerzos para recuperar el control, el daño era irreversible.** En menos de 24 horas, Code Spaces tuvo que anunciar su cierre, demostrando que un solo ataque puede llevar a la extinción de una empresa. Este ejemplo demuestra no solo la importancia de prevenir, sino también de saber reaccionar correctamente y rápido: un plan de respuesta a incidentes y manejo de crisis.



Al final habrá gastos directos, indirectos y pérdidas ante un ciberataque que al final tendrán que ser registrados para reflejar el impacto financiero real de un incidente.

Los gastos directos, como los costos de recuperación de sistemas, el contratar a terceros que apoyen en la respuesta a incidentes, manejo de crisis, apoyo legal y especialistas en comunicación deberán ser considerados gastos operativos extraordinarios.

Por otro lado, habrá costos indirectos que incluyen la pérdida de ingresos por la interrupción, posibles demandas legales, compensaciones a clientes o usuarios afectados entre otros. Estos reflejan un impacto a largo plazo en la salud financiera de la empresa.

Al final se requiere que las empresas mantengan una **transparencia total en su contabilidad y reportes financieros post-ciberataque,** no solo para una gestión interna, sino también para mantener la confianza de inversores, accionistas y otras partes interesadas. Esto cobra relevancia cuando la empresa cotiza en bolsa.

El panorama actual de los ciberataques demuestra que estos incidentes son mucho más que un desafío técnico o una mera afectación a la reputación. Son una amenaza existencial que puede llevar a una empresa al borde del abismo. Por lo tanto, **es esencial que las organizaciones adopten medidas proactivas de ciberseguridad,** no solo para proteger su información y activos, sino para asegurar su supervivencia en el dinámico mundo digital de hoy.

Autor: Andrés Velázquez
Fuente de información: www.forbes.com.mx