LITORALPRESS

Fecha: 22-07-2024
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Noticia general
Título: Cada vez más ejecutivos creen que su empresa puede sufrir una filtración de datos

Pág. : 3
Cm2: 607,8

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Expertos plantean que inversión en infraestructura no es suficiente, se debe capacitar a los trabajadores:

Cada vez más ejecutivos creen que su empresa puede sufrir una filtración de datos

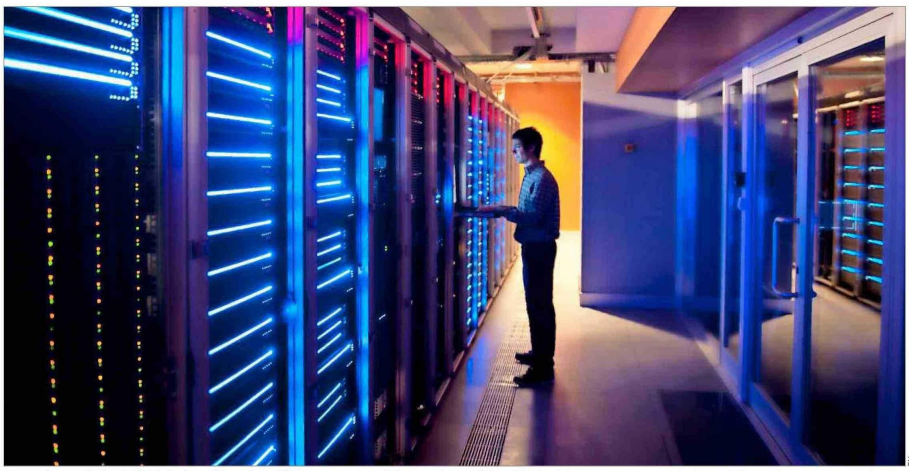
En Chile, la preocupación por la ciberseguridad en las compañías está asociada a la mayor regulación que se ha impuesto en este aspecto, además de la creciente digitalización.

CATALINA MUÑOZ-KAPPES

La ciberseguridad es cada vez una mayor prioridad para los altos ejecutivos. Incidentes como la falla en una plataforma de ciberseguridad que prestaba servicios a Microsoft resultó en cientos de vuelos cancelados a nivel mundial. En Chile, debido a las leyes que se han promulgado recientemente y que están prontas a publicarse, como la ley de delitos económicos —que incluyen los ilícitos informáticos—, la ley marco de ciberseguridad, y el proyecto de ley de protección de datos personales, la ciberseguridad se ha vuelto una de las principales preocupaciones al interior de las empresas.

Según una encuesta realizada por Forvis Mazars a 800 directivos en 30 países, el 40% de los ejecutivos cree que una filtración de datos podría ocurrir en su empresa en los próximos doce meses. Esta cifra representa un alza desde la versión anterior del sondeo, cuando el 32% estimaba que una filtración era probable. De la misma manera, el porcentaje de ejecutivos que afirmaba que no veía probable que ocurriese una filtración de datos disminuyó de 65% a 57%.

También ha habido una disminución en la confianza de los ejecutivos de que su información está completamente protegida. Si en 2022 el 68% tenía esta convicción, en la encuesta de 2024 el 62% asegura estar completamente protegido.



A nivel mundial, el 40% de los altos ejecutivos cree que podría ocurrir una filtración de datos en su empresa en los próximos doce meses, según una encuesta de Forvis Mazars.

"Mientas más digitalizamos, tenemos que entender que estamos expuestos a riesgos del ámbito de la seguridad en información. (En Chile), se genera esta preocupación porque hay una mayor percepción de riesgo", asevera Darío Rojas, director de Consultoría en Riesgo de Forvis Mazars. Este tema ha cobrado más relevancia en el último tiempo en Chile, ya que ahora una filtración de datos no sólo afectará la reputación de la compañía, sino que también puede traer asociadas sanciones, producto de las nuevas legislaciones.

Para Ricardo Seguel, director académico del Magíster en ciberseguridad UAI, la protección digital se está poniendo cada vez en un ámbito más importante para los directores y la alta gerencia, especialmente en las empresas que tienen un regulador que les exige fortalecer sus controles.

Infraestructura

Según Rojas, existen dos frentes en que las empresas deben hacer transformaciones para disminuir las posibilidades de tener un incidente de ciberseguridad: la infraestructura tecnológica y la capacitación de los trabajadores.

"Hay un tema técnico que tiene que ver con la infraestructura, en donde las compañías tienen que invertir en empresas dedicadas y que están acostumbradas a dar este servicio, como actualizar los sistema operativos, mantener activos los antivirus, hacer monitoreo de acceso, para disminuir la probabilidad de que se materialice uno de estos riesgos tecnológicos", dice Rojas. Este aspecto, entonces, solo depende de los recursos que destine una empresa a la ciberseguridad.

Debido a esta situación, Seguel ve una brecha entre las compañías reguladas y las no reguladas, ya que las firmas de menor tamaño no están obligadas a tener que invertir en ciberseguridad. "Todo lo que es el sector de empresas no reguladas, y ahí caen muchas empresas pymes, no hay control, por lo tanto, tampoco hay un mayor incentivo a invertir en ciberseguridad. Y ahí es donde se generan hoy día los mayores riesgos de exposición", dice Seguel.

CONFIANZA

Ha disminuido la confianza de los ejecutivos de que la información de las empresas está completamente protegida.

Factor humano

Sin embargo, el aspecto más importante y difícil de implementar es lograr un cambio cultural al interior de las empresas.

"El mayor problema de la seguridad de la información somos los usuarios, que tendemos a hacer cosas que ponen en riesgo la infraestructura. Al usar mi PC, está conectado a la red. Entonces cualquier cosa que haga puede afectar la red (de la empresa)", señala Rojas. Capacitar a los trabajadores requiere "mucho entrenamiento" acerca de cómo los ciberdelincuentes logran infiltrase en la red de las compañías.

Para Seguel, el problema de no tener una cultura de seguridad digital es algo que afecta a todas las organizaciones de manera transversal, ya sean reguladas o no reguladas, o del sector privado o público.