Ataques Cibernéticos en el Sector Universitario

Los sistemas informáticos de las instituciones académicas están más conectados, son más eficientes y fiables que nunca, mejorando todo desde la inscripción de estudiantes, informes, hasta las funciones administrativas como recursos humanos y finanzas. Si bien esto ha hecho avanzar drásticamente al sector, dicha conectividad también tiene sus inconvenientes. Los atacantes cibernéticos son una gran amenaza para el sector educativo, e indicios recientes muestran que las universidades son cada vez más atacadas por delincuentes cibernéticos, ya que los consideran como objetivos fáciles, mal equipados para hacer frente a incidentes cibernéticos.

¿Estamos realmente en riesgo?

Los datos recopilados para inscribir a los estudiantes se consideran "información de identificación personal" (IIP) y están formalmente protegidos por regulación. Las regulaciones internacionales y locales han vuelto mucho más estricto el procesamiento de datos personales.

Esto tiene implicaciones importantes para las universidades que procesan grandes cantidades de datos personales, pero a menudo carecen de los recursos de seguridad y cumplimiento para hacer frente a los riesgos de manera efectiva.

Si bien las implicaciones de las violaciones de datos son reales (y muy costosas, desde una perspectiva financiera como de reputación), existen enormes amenazas de un ataque cibernético más "tradicional". Eventos como la instalación de ransomware para cifrar archivos, el acceso no autorizado y robo de información de identificación personal valiosa, interrupción de los servicios o el hackeo de cámaras de CCTV dentro del campus, son una realidad hoy en día.

Las universidades son cada vez más objetivo de los atacantes cibernéticos, ya que fungen como proveedores del sector empresarial en forma de innovación, economía, investigación y desarrollo. Esta propiedad intelectual tiene valor elevado. Debido a la naturaleza pública y orientada hacia el exterior del sector académico y la facilidad con la que los académicos colaboran a través de redes privadas más pequeñas, esta propiedad intelectual es particularmente vulnerable. Estas redes privadas suelen ser más susceptibles al acceso no autorizado e incidentes cibernéticos.

Un informe de septiembre de 2019 del Centro Nacional de Seguridad Cibernética reveló el espionaje financiado por el estado dirigido a la investigación de alto valor de las universidades. El informe hizo referencia a los ataques de phishing y malware, y sus efectos inmediatos y disruptivos, pero llamó la atención específicamente sobre una amenaza a largo plazo de los estados nacionales que buscan robar investigación para obtener ganancias estratégicas.

Entre los daños más previsibles destacan al valor de la investigación, especialmente en temas STEM (Science, Technology, Engineering and Mathematics), una caída en la inversión del sector público o privado en las universidades afectadas y daños a la "ventaja de conocimiento".

Caso de estudio

Una brecha demasiado lejos

En junio de 2017, la Universidad de East Anglia (EAU) sufrió una vergonzosa violación de datos cuando envió inadvertidamente datos personales relacionados con 191 estudiantes universitarios a casi 300 personas. La hoja de cálculo distribuida contenía problemas de salud de los estudiantes, duelos y problemas personales.

A pesar de que la universidad aseguró que había endurecido sus procedimientos como resultado del incidente, cinco meses después, los datos personales sobre un miembro del personal se enviaron por error a cientos de estudiantes de posgrado y, en octubre del año pasado, se supo que un profesor de la UEA envió accidentalmente datos privados sobre la tesis de maestría fallida de un alumno a cientos de estudiantes.

Tras una investigación de la Oficina del Comisionado de Información sobre el incidente de junio de 2017, los Emiratos Árabes Unidos tuvieron que pagar más de £140,000 en compensación a los estudiantes afectados.

Lecciones aprendidas

La Universidad de Maastrict recibió un ataque cibernético a través de un malware en diciembre de 2019. El malware cifró los datos de Windows en 267 de los servidores de la universidad, comprometiendo simultáneamente una serie de copias de seguridad del sistema. La interrupción puso en peligro el acceso al trabajo y notas del curso, ocasionando presión en los estudiantes para acceder a la información y prepararse para los exámenes.

Se establecieron protocolos de gestión de crisis que ayudaron a la pronta reanudación de los servicios del sistema para los estudiantes y el personal. La universidad fue transparente en el informe de los eventos acontecidos y cómo la institución respondió ante ellos.

Lo que se hizo evidente a partir del análisis de la Universidad de Maastrict fue la necesidad de abordar los aspectos técnicos y humanos del riesgo cibernético, opinando que las instituciones de educación superior “no están exentas de dichas vulnerabilidades”.

La universidad mencionó la alta probabilidad de un incidente cibernético dada la gran apertura pública de las instituciones educativas, así como la prevalencia de dispositivos digitales, pueden comprometer la seguridad de la universidad, dando como resultado mayor exposición al riesgo.

Seguro específico CYBER

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética para el sector universitario. Es vital salvaguardar el sistema de cualquier proveedor académico para permitir proteger sus actividades, estudiantes, reputación e ingresos.

Reconocer las vulnerabilidades particulares en todo el sector académico es fundamental. En Lockton, trabajamos para un número significativo de instituciones educativas, desde primarias, secundarias y educación superior hasta administradores educativos y proveedores de e-learning. Esto nos da una excelente exposición a los hábitos de compra cibernética y las exposiciones que enfrenta el sector educativo.

Es importante mencionar que muchas pólizas tradicionales no responderán a una violación cibernética. Una cobertura afirmativa bajo una póliza de cyber independiente será vital.

Una póliza de cyber está diseñada para responder a los siguientes eventos, que no necesariamente serían cubiertos por pólizas más tradicionales:

a. Violación de datos de un ataque cibernético.
b. Pérdida financiera e impactos reputacionales tanto a la compañía como a los altos directivos por la falla de un sistema informático debido a un ataque malicioso.
c. Defensa regulatoria, multas y sanciones civiles como resultado de una violación de la seguridad (asegurable por ley).
d. Costos de respuesta a la violación.
e. Solicitud de rescate (ransom) tras un ataque a los sistemas informáticos.

Un ataque cibernético puede tener ramificaciones de gran alcance para el sector universitario. Comprender estos riesgos y mitigarlos de manera proactiva es clave. Nuestro equipo de expertos en riesgos cibernéticos trabajará para crear una solución personalizada que proteja y asegure su negocio exactamente donde lo necesite, y garantice que los riesgos cibernéticos se integren en su proceso de gestión de riesgos.

La seguridad de los datos de sus clientes está en sus manos. Coloque la seguridad de su negocio en las nuestras.

Para mayor información:

Ricardo Millán
Head ProFin México
ricardo.millan@lockton.com

Moisés García
ProFin México
moises.garciab@lockton.com