TRANSFORMACIÓN DIGITAL: COMIENCE CON LA CIBERSEGURIDAD EN MENTE

Con demasiada frecuencia, las empresas se mueven hacia la transformación digital sin un enfoque estratégico o proactivo para la ciberseguridad y la privacidad de los datos. Como resultado de la pandemia de COVID-19, ha habido un aumento dramático, repentino e inesperado de personas que trabajan, aprenden, enseñan y consultan desde casa. Esta transición en gran parte no planificada del acceso remoto a la red de la oficina y de la escuela en el hogar ha creado algunos desafíos de capacidad, operativos y de ciberseguridad únicos. Muchas organizaciones que realizan transformaciones digitales han obtenido ganancias en la productividad digital, a través de una mayor velocidad y acceso a los datos, un análisis de datos más rápido y ahorros de costos de almacenamiento de datos relacionados, especialmente cuando se incluye el almacenamiento de datos basado en la nube. Sin embargo, cada vez más, estas mismas organizaciones se han enfrentado a ciberataques costosos en forma de ataques de spear-phishing diseñados socialmente, compromisos de correo electrónico empresarial (BEC) o ataques de suplantación de identidad, y / o ataques de ransomware, porque no comenzaron de manera adecuada o proactiva su transformación digital teniendo en cuenta la ciberseguridad.

Con frecuencia, organizaciones de todos los tamaños y de todas las industrias consideran que la ciberseguridad es una ocurrencia tardía. Sin embargo, estas organizaciones están aprendiendo que esto conduce a lecciones costosas sobre el fraude cibernético y / o violaciones de datos. En 2019, los daños globales estimados por el fraude cibernético y las violaciones de datos excedieron los USD 4 billones, según Gartner Group. Por el contrario, la ciberseguridad debería estar a la vanguardia de la planificación empresarial estratégica para todos los proyectos digitales. IBM Security informó que el costo promedio de una violación de datos cibernéticos ahora supera los USD 8.2 millones.

A medida que tanto el nivel de sofisticación como el número de ciberataques aumentan cada año, se ha vuelto dolorosamente evidente que los beneficios de la información digital, que incluyen: velocidad, fácil acceso a los datos, análisis rápido de datos, visualización de datos y ahorros de costos relacionados, pueden ser completamente perdidos o robados como resultado de daños. Los daños pueden provenir de muchas formas, tales como: ataques cibernéticos, fraude cibernético, violaciones de datos cibernéticos, demandas judiciales relacionadas con ciberseguridad por negligencia en seguridad cibernética, sanciones regulatorias federales y / o estatales por fallas en el cumplimiento de la privacidad de datos / seguridad cibernética e impactos negativos en la reputación de la organización debido a una seguridad de la información inadecuada. Además, el panorama regulatorio global de ciberseguridad y privacidad de datos es cada vez más complejo. Esto deja la puerta abierta a posibles demandas colectivas masivas por violaciones de datos cibernéticos que revelen información de identificación personal de los consumidores, como la nueva Ley de Privacidad del Consumidor de California (CCPA) promulgada en enero de 2020. La CCPA establece claramente que una organización no puede garantizar la privacidad de los datos sin "seguridad razonable".

BDO DIGITAL

COMIENCE CON LA CIBERSEGURIDAD EN MENTE

Entonces, ¿qué significa exactamente comenzar un proyecto digital o transformación digital de una organización con la ciberseguridad en mente? En pocas palabras, significa comenzar toda la planificación de proyectos digitales haciendo las preguntas correctas relacionadas con la ciberseguridad por adelantado, incluidas las siguientes:

20 Preguntas Clave de Ciberseguridad a Considerar:

1. Este proyecto y / o la organización requerirán acceso a alguno de los siguientes tipos de datos o información:
   - Información de identificación personal (PII) de empleados, socios o consumidores Información de salud protegida (PHI)
   - Información de la tarjeta de pago (PCI)
   - Propiedad Intelectual (PI)
   - Información no clasificada controlada (CUI)
   - Información de defensa cubierta (CDI)
   - Información clasificada (CI)
   - Información confidencial de la empresa (CSI)
2. ¿Quién necesitará acceder a los datos del proyecto y la organización?
3. ¿Cómo se controlará el acceso a la información, internamente y con proveedores / subcontratistas / clientes?
4. ¿Dónde se almacenará la información del proyecto y la organización y cómo se protegerá?
5. ¿Quién desarrollará y administrará el plan de gobierno de la información de la organización, el plan de seguridad del sistema de información y el plan de respaldo o resiliencia de datos?
6. ¿Cuenta la organización con las personas y los recursos adecuados para liderar eficazmente la planificación e implementación estratégica de ciberseguridad y privacidad de datos?
7. What project and organization data segmentation or compartmentalization (i.e. zero trust data architecture) is needed to protect the information?
8. ¿Qué segmentación o compartimentación de datos de proyectos y organizaciones (es decir, arquitectura de datos de confianza cero) se necesita para proteger la información?
9. ¿Es necesario que el proyecto o los datos de la organización cumplan con uno o más requisitos contractuales o reglamentarios de privacidad de datos o ciberseguridad específicos de la industria? Si es así, ¿qué requisitos específicos (es decir, el Procedimiento especial 800-171 del Instituto Nacional de Estándares y Tecnología [NIST], ISO 27001, Estándar de seguridad de datos de la industria de tarjetas de pago [DSS], Departamento de Servicios Financieros de Nueva York [NYDFS] Ciberseguridad, Ley de Portabilidad y Responsabilidad del Seguro Médico [HIPAA] Ciberseguridad, HITRUST - Marco de Seguridad Común [CSF], la nueva certificación del modelo de madurez de ciberseguridad del Departamento de Defensa de EE. UU. [DOD] [CMMC], el Reglamento general de protección de datos de la Unión Europea [GDPR] y / o la Ley de privacidad del consumidor de California [CCPA], etc.)
10. ¿Qué vulnerabilidades de ciberseguridad existen actualmente dentro del sistema de correo electrónico, la red / sistema de información, las aplicaciones de software y los terminales de las organizaciones?
11. ¿La organización realiza actualmente monitoreo de datos 24/7/365, detección de intrusiones cibernéticas y respuesta a incidentes cibernéticos para toda la información? Si no es así, ¿estos servicios son proporcionados por un proveedor de servicios de seguridad administrada (MSSP) altamente calificado?
12. La organización ha desarrollado, documentado, implementado y probado políticas, planes y procedimientos de ciberseguridad efectivos para la información del proyecto, incluyendo:
    - Plan de Respuesta a Incidentes (IRP)
    - Plan de Continuidad del Negocio (BCP)
    - Plan de Recuperación ante Desastres (DRP)

13. ¿Qué actores de ciberamenazas (grupos de ciberataques de estado-nación, grupos de ciberataques delictivos organizados y / o hackavists) estarían más interesados en la información relacionada con este proyecto, la organización, el liderazgo y la cadena de suministro?
14. ¿Qué vectores de amenazas cibernéticas probablemente explotarían los atacantes dentro de la organización para obtener acceso a información valiosa?
15. ¿Qué tan susceptibles son los empleados de la organización, de arriba a abajo, a los ataques cibernéticos de spear-phishing y los ataques de compromiso de correo electrónico empresarial (BEC) de ingeniería social?
16. ¿Actualmente la organización subcontrata los servicios de Tecnología de la Información (TI) a un proveedor de servicios administrados (MSP) o subcontrata la ciberseguridad a un proveedor de servicios de seguridad administrada (MSSP)? ¿Está satisfecha la Junta Directiva de la organización con los servicios de ciberseguridad o TI subcontratados?
17. ¿Recientemente realizó la organización una simulación de ataque cibernético o un ejercicio de mesa con la junta directiva? ¿Cuándo se realizó?
18. ¿Qué porcentaje del presupuesto anual de TI de la organización se gasta en ciberseguridad?
19. ¿Tiene la organización una cobertura adecuada de seguro de responsabilidad cibernética?
20. ¿Qué tan efectivo es el programa de capacitación y educación en ciberseguridad de la organización?

Las veinte preguntas clave de ciberseguridad a considerar son solo un punto de partida para una discusión más profunda sobre el desarrollo e implementación de un programa de ciberseguridad estratégico, proactivo e integral. Las respuestas de una organización a las preguntas mencionadas anteriormente ciertamente ayudarán a pintar una imagen de su nivel actual de ciberdefensa, posibles amenazas cibernéticas y vulnerabilidades cibernéticas conocidas, lo que ayudará a los expertos en ciberseguridad a construir una hoja de ruta personalizada para mejorar la ciberseguridad y la privacidad de los datos..

RESUMEN

Demasiadas organizaciones cometen errores críticos al embarcarse en una transformación digital a gran escala para su organización. Muchos no logran desarrollar un programa de ciberseguridad estratégico, proactivo y basado en amenazas y no invierten lo suficiente en los siguientes cinco elementos clave de la ciberseguridad.:

- Brindar educación / capacitación en ciberseguridad para todos los miembros de la organización de arriba hacia abajo.
- Contratar a las personas adecuadas para liderar la planificación e implementación estratégica de ciberseguridad y privacidad de datos de la organización desde el principio.
- Involucrar a empresas independientes para realizar pruebas de diagnóstico periódicas de seguridad cibernética, que incluyen: escaneo de vulnerabilidades informáticas, pruebas de penetración, evaluaciones de ataques cibernéticos del sistema de correo electrónico, campañas de spear-phishing y análisis de la web oscura para comprender las vulnerabilidades y amenazas cibernéticas de la organización.
- Garantizar la supervisión continua de la información las 24 horas del día, los 365 días del año, la detección de intrusiones y los servicios de respuesta rápida a incidentes cibernéticos, ya sea internamente o mediante proveedores de servicios de seguridad gestionados (MSSP) subcontratados.
- Implementar y probar planes y procedimientos adecuados de resiliencia de la información a través de planes de respuesta a incidentes cibernéticos, planes de continuidad del negocio cibernético y planes de recuperación ante desastres.

La clave del éxito es comenzar todos los proyectos de transformación digital teniendo en cuenta la ciberseguridad. Al interactuar con expertos en ciberseguridad desde el inicio de un proyecto o una nueva empresa comercial, una organización puede hacer las preguntas correctas y luego desarrollar un programa de ciberseguridad proactivo y basado en amenazas. Recuerde, en la era digital, una organización solo puede lograr la integridad de la información y la privacidad de los datos a través de una ciberseguridad efectiva.

CONTACTO:

GREGORY GARRETT
Head of US &
International Cybersecurity
703-893-0600
ggarrett@bdo.com