El Instituto de Auditores Internos frente al Coronavirus

Siete razones para no bajar la guardia en ciberseguridad

- **El cibercrimen se convierte en una de las mayores amenazas para empresas públicas y privadas**

21/04/2020.- La actual situación de crisis ha propiciado un crecimiento del cibercrimen en todas sus versiones, convirtiéndose en una amenaza aún mayor tanto para empresas privadas como públicas. El Instituto de Auditores Internos, consciente de los riesgos que supone, analiza las siete razones por las que no se debe bajar la guardia en ciberseguridad.

1. **La improvisación puede haber dejado puertas abiertas.** La rapidez con la que muchas compañías tuvieron que improvisar un sistema de teletrabajo puede haber dejado abiertos algunos resquicios para la ciberdelincuencia. En este sentido, es importante que las empresas, a través de Auditoría Interna, supervisen que todos los sistemas y protocolos de ciberseguridad se han implantado correctamente y no ha quedado fuera nada relevante. Además, es necesario recordar a los empleados la necesidad de ser más cautos y utilizar contraseñas robustas en toda la red, cambiándolas cada cierto tiempo.

2. **Incluir la ciberseguridad en el plan de continuidad** con el objetivo de dar solución a posibles situaciones que pudieran plantearse, como que los responsables de IT tengan realmente acceso a los equipos que trabajan en remoto para resolver cualquier incidencia; prever que puede haber bajas por enfermedad en el equipo de ciberseguridad cuyo reemplazo (interno o externo) debe tener el mismo acceso y herramientas; prever diferentes cauces de comunicación en estos equipos y no dejarlo solo en uno (email, por ejemplo) que pueda fallar e impida contactar con ellos en caso de emergencia; y, por último, tomar buena nota de las lecciones aprendidas para corregir los errores y que no vuelvan a producirse.

3. **Concienciar a la plantilla: toda conexión es un riesgo**. Los ciberdelincuentes van a utilizar todas las opciones para acceder a los sistemas de seguridad y a lo más valioso de las organizaciones, los datos. Por ello, se debe verificar su protección y la seguridad de las conexiones evitando aquellas plataformas o aplicaciones que no tengan total garantía. Ya se han dado casos de personas que han entrado en webinars para interrumpirlos o sistemas de videoconferencias que no garantizan la protección de datos.

4. **Cuidado con la suplantación de identidad**. La suplantación de identidad o phishing es una de las ciberamenazas que se están prodigando durante la pandemia para obtener credenciales del usuario y acceder a los sistemas de la empresa. Actualmente existen 24.000 dominios en Internet que contienen los términos: “coronavirus”, “corona-virus”, “covid19” y “covid-19”. La mitad se ha creado en marzo, algunos con fines legítimos y otros con objetivos cibercriminales. El phishing es un caso de ingeniería social para explotar la debilidad de las personas.

5. **El móvil, tan frágil como otros dispositivos**. Los dispositivos móviles son miniordenadores a través de los que se accede a la información personal y profesional. Son más vulnerables a las amenazas. Hay que encriptar e instalar cortafuegos. Las empresas deben comprobar que los móviles corporativos cuentan con robustos sistemas de seguridad y los empleados saber bien lo que no deben hacer con ellos.

6. **Contemplar la posibilidad de contar con un ciberseguro.** Hace tiempo que las compañías de seguros ofrecen pólizas para protegerse frente a los riesgos de ciberseguridad, tanto desde un punto de vista de prevención como de mitigación. Si la compañía dispone ya de uno, debe revisar la letra pequeña para ver si las pandemias son una excepción a la cobertura de la póliza o no. En caso de no disponer de un ciberseguro, quizá es el momento de planteárselo identificando primero las necesidades concretas de la compañía para comparar luego las ofertas del mercado analizando tanto el alcance como las obligaciones. Hay pólizas que no solo cubren el riesgo directo, sino también el de terceras partes (clientes, proveedores, etc.). Hay aseguradoras que incluso añaden otros servicios de valor adicionales como la evaluación previa de la seguridad y algunos servicios de gestión de crisis. Los expertos auguran un fuerte crecimiento de los ciberseguros en los próximos años.

7. **RGPD**. Si la compañía ha sufrido algún tipo de ciberincidente durante la crisis originada por el COVID-19, no se debe olvidar que siguen totalmente vigentes los estrictos protocolos de comunicación que puso en marcha el Reglamento General de Protección de Datos (RGPD). Y tampoco estos tiempos de pandemias eximen de las posibles sanciones en caso de brechas de seguridad que hayan afectado a la obligación de protección de datos.

Acerca del Instituto de Auditores Internos de España:

El Instituto de Auditores Internos de España es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.500 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

Para más información

Instituto de Auditores Internos
Gabriela González-Valdés
Fernando Fuentes Colado
91 593 23 45
www.auditoresinternos.es

Elcano Comunicación
Aurora Ochoa / Beatriz Colomer
aochoa@elcanomg.com / bcolomer@elcanomg.com
607477764 / 678474374
www.elcanomg.com

Síguenos en: