LLYC

ÁREA DE ESPECIALIDAD ISSUES

Nota técnica

Ciberriesgos y Covid-19, la tormenta perfecta

Madrid
16 de abril de 2020

Uno de los efectos de la pandemia Covid-19 es el incremento de los ciberataques debido al confinamiento y a depender de las redes para comunicarnos: mucha gente está trabajando desde casa y se incrementa la búsqueda de información, las transacciones online. Los ciberdelincuentes aprovechan el **aumento de vulnerabilidades para ciberatacar en dos grandes frentes**: contra los sistemas de las compañías y contra empleados y ciudadanía para acceder a sus dispositivos.

RIESGOS CIBERNÉTICOS: EL MAYOR PELIGRO PARA LAS COMPAÑÍAS

Los ciberdelincuentes utilizan la crisis del coronavirus para hacerse pasar por organismos oficiales y empresas y **conseguir datos confidenciales**, modalidad de ciberdelincuencia denominada *phishing*, o para acceder a los sistemas e insertar **programas informáticos maliciosos** (*malware*) o para **secuestrar datos y pedir rescate** económico y chantajear con filtrar información confidencial si no se paga, una técnica conocida como *ransomware.*

Las **ciberestafas** con el señuelo Covid-19 se han multiplicado, y son millones los correos enviados con la finalidad de infectar el ordenador y acceder a las claves e información. Un *phishing* cada vez más sofisticado al personalizarse el email que enlaza al virus. "**No, los ciberdelincuentes no están en cuarentena**", como señala un eslogan de concienciación del Instituto Nacional de Ciberseguridad (Incibe).

Antes de estallar esta crisis, los riesgos cibernéticos ya eran clasificados como **el mayor peligro para las empresas a nivel mundial** (Barómetro Allianz Riesgos 2020) y el Informe Global de Riesgos 2020 del Foro Económico Mundial, advierte que entre los diez principales riesgos figuran los ciberataques a compañías y estructuras críticas y el robo de datos y dinero.

¿PODEMOS PREVENIRLOS?

Dada la dependencia básica de los sistemas centrales a los que se accede de forma remota, **las compañías van a vivir un aumento continuo de los intentos de extorsión**: la tendencia es sufrir ataques cada vez **más frecuentes, silenciosos, inteligentes, sofisticados** y con un alto coste económico.

El nuevo contexto de ataques y amenazas ciber es **complejo,** no descansa ya que es 24/7 y obliga a las organizaciones a prepararse con un cambio de cultura: no es un tema solo técnico, del CISO o equipos de

IT, **implica a toda la organización** empezando por la alta dirección.

Su abordaje debe ser multidisciplinar y con capacidad para poder ser gestionado en tiempo real. En un mundo que está más conectado que nunca las compañías deben **prepararse para el peor ciber escenario** de riesgo con un **enfoque más holístico, proactivo y preventivo** del riesgo cibernético desde el inicio, que involucre la participación total de la empresa y todo su ecosistema de producción y trabajo.

La mejor protección para hacer frente a este desafío es trabajar desde tres ámbitos de manera paralela: la formación a los empleados, la inversión tecnología y la planificación estratégica.

Formación a empleados:

Existe una falta de educación o concienciación de muchos empleados en términos de ciberseguridad que se magnifica en las actuales circunstancias por el Covid-19. **Un 60% de los ciberataques tienen su origen en descuidos y brechas abiertas por los propios empleados**, según datos del Centro Criptológico Nacional CCN-CERT. Sin embargo, tres de cada cuatro usuarios no están preparados para hacer frente a la ciberdelincuencia y a los riesgos que entrañan las nuevas tecnologías.

Una compañía es tan fuerte como lo es su eslabón más débil y **el empleado es la parte de la cadena más vulnerable a la ciberseguridad.** Para minimizar su riesgo como vector de entrada hay que impulsar facilitar su formación, información y colaboración digital.

- **Disponer de canales** internos de comunicación corporativa que faciliten la formación y preparación de los empleados
- Dar proactivamente **instrucciones sencillas y útiles** en materia de ciberseguridad, por ejemplo, con sencillos vídeos, dinámicas de gamificación, webinars o formación en línea.
- Intensificar la **frecuencia** de la información para asegurar la toma de medidas preventivas. En especial en lo que respecta a no abrir los correos sospechosos y sólo descargar aplicaciones de instituciones y organismos acreditados.
- **Alertar de posibles riesgos** comunicados por organismos oficiales de ciberseguridad o Policía, como, por ejemplo, de los riesgos de seguridad al usar Zoom para videoconferencias por posible espionaje.

Planificación estratégica:

Cuanto mayor es el riesgo se deben tomar medidas para proteger la empresa y a sus empleados, en especial, para que el teletrabajo masivo no suponga una brecha de seguridad en la compañía.

- Definir e instalar una **Política de seguridad en Teletrabajo** y un plan de acción para comunicarla.
- Revisar las **buenas prácticas de seguridad cibernética,** ¿Tienen todos los empleados, los subcontratistas y los terceros las necesarias instrucciones y orientaciones claras sobre cómo realizar su trabajo de forma segura?
- Es el momento de valorar adoptar un mínimo **Plan de Ciber Contingencia** donde se identifiquen los principales escenarios para la compañía y cómo

se va actuar contemplando la afectación a todos los grupos de interés y su impacto reputacional.

- Anticiparse con **soluciones digitales** que posibilitan la máxima eficacia y el mínimo tiempo en alertas, notificaciones y seguimiento. Máxime cuando este tipo de ciber crisis rápidamente trascienden al público.

- Preparar **canales alternativos de comunicación,** ya que hay casos donde el ciberataque implica no poder acceder a los dispositivos habituales, quedando sin vías para contactar de manera interna o externa.

Inversión tecnológica:

Las compañías habituadas al teletrabajo con trabajadores en remoto tienen según sus flujos de trabajo instalados sistemas de seguridad, servicios de herramientas en la nube (*cloud computing*), facilitan **conexiones VPN mediante redes privadas locales, actualizan los dispositivos y mantienen los equipos con adecuadas medidas de seguridad.**

Sin embargo, aquellas no habituadas se encuentran ahora sin las medidas suficientes, y necesitan empezar por la correcta protección antimalware en los equipos y protocolos de accesos con autentificación.

- Entre los consejos básicos que pueden reducir el riego de acceder a información corporativa figura tener una contraseña resistente en todos los dispositivos y modificarla con frecuencia.

- Asegurar que todos los empleados hayan firmado un documento de funciones y obligaciones en cuanto a la protección de datos.

- Habilitar un **sistema Cloud corporativo** de gestión documental para evitar los trabajadores utilicen almacenamiento privado de documentos corporativos.

- Recordar que los **sistemas** corporativos y la información son **confidenciales,** que terceros no pueden tener acceso y que los miembros de una familia se consideran externos.

- Si es necesario acceder a sistemas de la compañía habilitar los accesos con sistemas con conexiones seguras o VPNs.

- Que tengan un antivirus instalado y actualizado, y que dispongan de **contraseñas seguras** y no compartirlas.

- **Actualizar** los dispositivos, y eliminar información temporal que se haya podido almacenar en las carpetas de descarga, papelera de reciclaje, mis documentos, cookies, historial y no guardar contraseña en el dispositivo.

QUÉ HACER ANTE UN CIBERATAQUE

Llegado el momento, las compañías deben ser capaces de **responder de manera rápida, coherente, coordinada y responsable** ante crisis por ciberdelincuencia. Si se es víctima de un ciberataque el abordaje es multidisciplinar donde **la comunicación se integre** desde el primer momento en la gestión junto a los equipos de IT y Legal.

LLYC

Una vez evaluada por parte de los expertos técnicos la situación, la estrategia de comunicación está al servicio de la óptima gestión y las empresas liderarla al ser hechos que pueden agravarse por una mala actuación interna, o si no se reacciona **con diligencia, responsabilidad y transparencia**.

Por ello, se necesita establecer con la mayor celeridad todo el posible impacto del ciberataque en la actividad de la empresa, desde el **plano financiero al impacto reputacional, así como en los diferentes stakeholders**.

- Fijar el escenario del riesgo al que nos enfrentamos con sus factores agravantes y cómo proceder con cada uno de los grupos de interés.
- Revisar si las plataformas mediante las cuales la compañía puede comunicarse siguen estando operativas y seguras.
- Preparar los mensajes de la compañía para transmitir confianza fijando la narrativa de lo ocurrido y Q&A.
- Si el tipo de ciberataque implica una brecha o fuga seguridad en los datos, debe asumirse el **cumplimiento en materia de notificación y comunicación que marca la Ley**.
    - Obligación de notificación en el plazo de 72h a la autoridad de control, sobre las consecuencias y circunstancias, así como a los usuarios afectados.
    - Obligación de comunicación pública de lo ocurrido, no solo a los afectados, si se desconoce a cuántos afectan la ciberincidencia o fuga de seguridad de los datos.

La conclusión es que la ciberseguridad tradicional basada en un enfoque reactivo ante las amenazas y solo desde un ámbito tecnológico es ineficiente y las grandes organizaciones necesitan ir más allá. Aunque no existe el riesgo cero, y especialmente en lo que a ciberdelincuencia se refiere, prevenir y concienciar dentro de la compañía frente a estos ciberriesgos es posiblemente la mejor forma de evitarlos.

Se autoriza la difusión y reproducción del material contenido en esta Nota técnica para fines comerciales o no comerciales, citando en todo caso la fuente de los materiales utilizados.

Luis González
Director Senior Área Issues
LLYC Madrid
lgonzalez@llorenteycuenca.com

Daniel Fernández Trejo
Director Senior Área global Tecnología
LLYC Madrid
dfernandez@llorenteyucuenca.com

Natalia Sara
Gerente Crisis y Riesgos
LLYC Madrid
nsara@llorenteycuenca.com