MARSH

INSIGHTS | **MAYO 2020**

Ciberseguridad después de COVID-19: 10 formas de proteger su negocio y reenfocarse en la resiliencia

A raíz de la pandemia de COVID-19 y la implementación resultante de directivas de distanciamiento social, se han visto alterados los procesos comerciales y han surgido nuevas realidades económicas, por lo que las empresas deben revisar y abordar su infraestructura tecnológica y medidas de ciberseguridad.

Los rápidos cambios provocados por COVID-19, incluido el movimiento de una gran parte de la fuerza laboral al teletrabajo y la expansión del uso del comercio electrónico, han provocado que muchas compañías implementen nuevas capacidades de IT ad hoc. Algunas soluciones provisionales han pasado por alto los procesos normales de desarrollo, aprobación y despliegue, que a menudo han ampliado o violado las políticas de ciberseguridad existentes al mismo tiempo que la actividad de los malos actores ha aumentado a nivel mundial.

Preparándonos para el mundo post pandémico

A medida que disminuyen las medidas de distanciamiento social, y antes de una posible segunda ola de casos de coronavirus, las organizaciones deberán eliminar el riesgo de la empresa y adaptar las operaciones a una "nueva normalidad". Esto requerirá una evaluación exhaustiva de los cambios de IT y ciberseguridad impulsados durante la pandemia, algunos de los cuales se implementaron rápidamente durante la fase de respuesta, seguidos de ajustes estratégicos de arquitecturas empresariales, controles de ciberseguridad y procesos comerciales basados en el largo plazo.

Incluso durante los tiempos "normales", la política IT a menudo va a la zaga de la realidad en las empresas actuales. En el período de reconstrucción pandémica, la política y la documentación deberán ponerse al día. Es posible que sea necesario institucionalizar algunos cambios realizados para abordar la pandemia; otros pueden necesitar ser reemplazados por soluciones más seguras y permanentes. Todos los cambios deben verse a través de una lente de resiliencia, que conduzca a un futuro más ágil y seguro para las empresas.

A medida que las sociedades se recuperan de las posturas de lucha contra la pandemia, podemos anticipar algunas características del mundo empresarial posterior a COVID-19, que incluyen:

- Aumento e institucionalización del trabajo a distancia.
- Migración acelerada a infraestructura y aplicaciones en la nube.
- Crecimiento en la funcionalidad y uso de herramientas colaborativas en línea.
- Un aumento en el comercio electrónico.

- Superficies de ciberataques ampliadas debido al aumento del teletrabajo.
- Más atención a la resiliencia empresarial.

En el mundo post-COVID-19, destacamos 10 áreas que requerirán de especial atención.

1. Soluciones de teletrabajo

Anticipando un aumento permanente en el teletrabajo, las compañías deben considerar:

- Procurar suficiente ancho de banda bajo demanda para mover contenido, especialmente videoconferencia, a través y entre sitios geográficamente dispersos.
- Establecer la capacidad de VPN a través de la implementación de clientes VPN basados en IPsec (Internet Protocol Security) u otras soluciones de conectividad segura en las estaciones de trabajo de los empleados.
- Administrar la identidad y el acceso de una fuerza laboral remota que cumpla con los requisitos de seguridad corporativos y las necesidades de facilidad de uso de los empleados.
- Implementación de soluciones de administración de dispositivos móviles para abordar el uso de dispositivos móviles personales aprobados y emitidos por la empresa para fines comerciales. En coordinación, considere implementar políticas adecuadas para traer su propio dispositivo (BYOD), como las que se detallan a continuación.

- Examinar de cerca el uso empresarial del protocolo de escritorio remoto (RDP) basado en Internet, que permite el acceso remoto de los sistemas y servidores de Windows y es un objetivo atractivo para los piratas informáticos. Si su uso está justificado, las compañías deberían considerar permitir RDP solo con autenticación a nivel de red del punto final y parches rigurosos, incluida la vulnerabilidad BlueKeep en todas las máquinas con Windows.

2. Protección en el perímetro externo

Un aumento en las conexiones remotas puede aumentar la superficie de ciberataque de una empresa. Las organizaciones pueden proteger sus perímetros externos mediante:

- Implementación del control de acceso a la red (NAC) para autenticar y validar dispositivos y aplicar políticas de seguridad antes de permitirles conectarse a redes corporativas en la oficina o remotas.
- Bloquear las estaciones de trabajo de los usuarios y los ordenadores portátiles de la empresa con una configuración de seguridad definida, administrar la configuración de forma centralizada y no asignar privilegios administrativos a los usuarios finales.
- Implementación de capacidades de aislamiento y forense de punto final remoto que cumplan con los requisitos forenses de la cadena de custodia.
- Implementar capacidades que admitan la recopilación y el análisis de datos de puntos finales remotos para identificar actividades no autorizadas.

3. Servicios Cloud

Los servicios en la nube pueden ofrecer importantes eficiencias en costes, resistencia y posibles beneficios de seguridad sobre el almacenamiento de datos y las alternativas de alojamiento de aplicaciones. Pero estos beneficios requieren que los servicios en la nube se adopten y administren de manera meditada y estratégica. Las empresas deben considerar:

- Adoptar estrategias formales para el uso de servicios en la nube.
- Desarrollar inventarios completos del uso actual de la nube en la empresa y racionalizar el uso de múltiples servicios.

- Definir políticas de almacenamiento de datos que describan las condiciones requeridas para el uso de servicios en la nube, almacenamiento en centros de datos y almacenamiento local, particularmente para información confidencial.

Un agente de seguridad de acceso a la nube es un software local o basado en la nube que monitoriza la actividad de la nube y hace cumplir las políticas de seguridad. Puede ayudar a detectar y monitorizar el uso de la nube dentro de la empresa, aplicar políticas de ciberseguridad relacionadas, alertar a los administradores de un flujo de datos anómalos y proteger contra malware.

4. Herramientas de colaboración segura

Si bien el correo electrónico, las herramientas de productividad de la oficina y las videoconferencias han sido vitales durante la pandemia, las empresas pueden optar por innovar mediante la adopción y el uso de herramientas de colaboración segura adicionales. Las organizaciones deben explorar las capacidades emergentes, como la realidad aumentada / virtual o los chatbots para la entrega de contenido, que pueden mejorar sus operaciones.

5. Política de ciberseguridad

Actualice las políticas de ciberseguridad para abordar las capacidades, la arquitectura y los procesos de IT provocados por una pandemia. Las organizaciones deberían considerar realizar una evaluación de riesgos e identificar mecanismos de aplicación, como la autenticación multifactor, el inicio de sesión único y el cierre de sesión automático desde dispositivos desatendidos.

6. Política BYOD

Muchas organizaciones optaron por permitir que los empleados usen sus dispositivos personales, incluidos computadoras portátiles, teléfonos móviles y tabletas, para los negocios de la compañía durante la pandemia, a pesar de que algunos tenían prohibiciones antes de la emergencia. Las llamadas telefónicas comerciales se desviaron a teléfonos móviles personales, el correo electrónico se puso a disposición en dispositivos personales y se permitió a los empleados acceder a aplicaciones basadas en la nube desde dispositivos personales. Las organizaciones deben establecer una política, examinarla o reformarla, y documentar adecuadamente cualquier medida implementada durante la pandemia.

7. Plan de respuesta ante brechas de seguridad (CIBR)

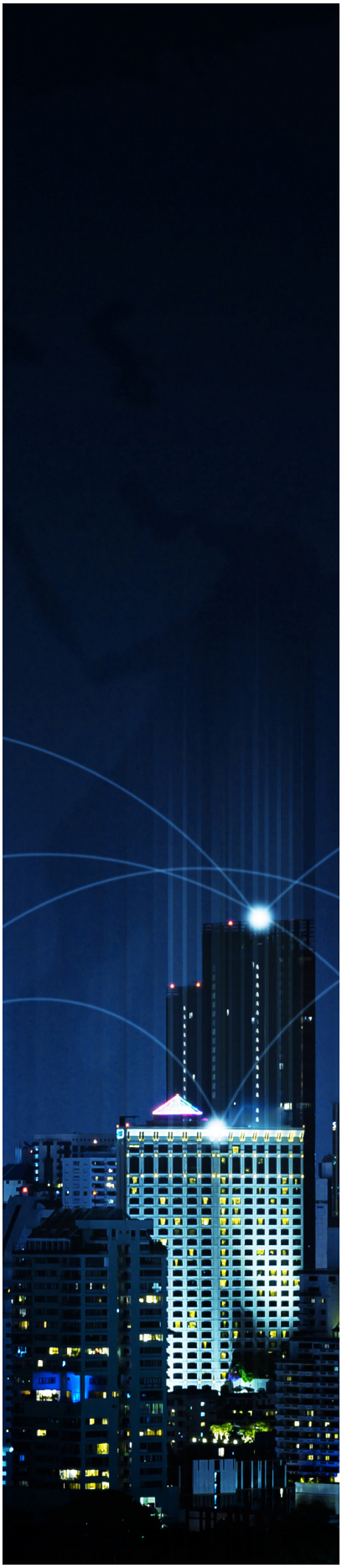
Las compañías con planes CIBR sólidos y actuales deberían considerar incorporar las lecciones de las operaciones de contingencia provocadas por la pandemia. Si no hubiera un plan CIBR preexistente, la necesidad de uno debería ser evidente. Las empresas pueden:

- Actualizar y mejorar los planes de recuperación de desastres y CIBR para abordar el contexto operativo actual.
- Coordinar y hacer referencia cruzada a los planes CIBR con recuperación ante desastres, continuidad del negocio y planes de gestión de crisis empresariales para crear conjuntos de documentos de planificación integral de crisis. Mantener estos documentos actualizados regularmente.

8. Cadenas de suministros y Gestión de terceros

La pandemia puede haber llevado a sus socios de la cadena de suministro y a otros terceros a transformar sus modelos comerciales. Las empresas deben considerar:

- Revisar los acuerdos de terceros, incluidos los acuerdos de nivel de servicio con proveedores de IT, para garantizar que cumplan con los requisitos actuales y tengan disposiciones de responsabilidad aceptables.



- Realizar auditorías de ciberseguridad y establecer requisitos de auditoría continuos para todos los terceros con acceso autorizado a las redes, sistemas o datos de la empresa.

9. Protección y recuperación financiera de un ciberataque

Los cambios en su infraestructura de IT, desde nuevos activos físicos hasta medidas de ciberseguridad, deben tenerse en cuenta en su perfil de ciberriesgo, con ajustes realizados a las coberturas de seguros según sea necesario. Como el riesgo no es únicamente un riesgo de operaciones o tecnología, es fundamental gestionar tanto la infraestructura IT como las exposiciones financieras de la organización. Se debe considerar el ciberseguro, que puede proporcionar un respaldo financiero crítico y rentable a raíz de un ciberataque durante una pandemia u otra crisis social y económica importante. Las empresas deberían:

- Revisar la cobertura de seguro existente, incluida la identificación de posibles brechas.
- Examine cómo los nuevos desafíos de ciberseguridad encajan en la estrategia de transferencia de riesgo ciber de la organización.
- Tenga en cuenta los posibles cambios en los términos y condiciones de cobertura en la renovación a medida que las aseguradoras evalúan las pérdidas y los cambios en los patrones de reclamo después de la pandemia.

10. Operaciones Ciber

El entorno operativo posterior a la pandemia será diferente. Las empresas deben considerar:

- Supervisar la recopilación y el análisis central de alertas de ciberseguridad y registros de auditoría para detectar y responder a actividades sospechosas / maliciosas.
- Revisar y actualizar los perfiles de VPN y las reglas de firewall para que los empleados reciban los privilegios apropiados que dependen de los roles.
- Implementar o actualizar procesos para obtener la aprobación de los propietarios de datos y sistemas para el aprovisionamiento y desaprovisionamiento de VPN remotas y otras cuentas asociadas con aplicaciones comerciales críticas.
- Deshabilitar el túnel dividido para los perfiles de VPN para evitar que los empleados remotos accedan a Internet directamente desde sus computadoras portátiles personales al mismo tiempo que acceden a los sistemas de información corporativos.
- Crear un mecanismo simple para marcar y reenviar correos electrónicos sospechosos para análisis técnico.
- Aprovisionamiento de soluciones de acceso seguro con capacidad suficiente para el mayor número de usuarios remotos y protección de seguridad en puntos finales.
- Aplicar actualizaciones de software a los dispositivos informáticos emitidos por la empresa de los trabajadores remotos.
- Habilitación de la autenticación multifactor para VPN y sistemas de información crítica.
- Aumentar la capacidad de la mesa de ayuda de TI y las horas de operación para manejar los mayores requisitos de servicio de una fuerza de trabajo remota.

Un nuevo enfoque en la resiliencia

Las capacidades actuales de IT y redes han permitido las estrategias que han mantenido a flote a muchas empresas durante la pandemia. La crisis actual, sin embargo, ha puesto de relieve la necesidad de prepararse para una seria interrupción del negocio. Una encuesta reciente encontró que más de una quinta parte de las organizaciones han comprado nuevas soluciones o servicios de seguridad para responder a su nueva realidad.

La pandemia ha hecho visible la necesidad de resiliencia empresarial en términos claros y convincentes. El período de recuperación y preparación posterior a la pandemia presenta la oportunidad para que las empresas se reconstruyan a una nueva normalidad, con la resiliencia empresarial como un objetivo generalizado.

Las organizaciones deberían considerar combinar nuevas inversiones en ciberseguridad con una cobertura de seguro ciber mejorada para reducir el riesgo retenido, optimizar el gasto en relación con la protección y conservar los recursos.

Para obtener más información e información sobre pandemias, visite nuestro Coronavirus Risk Hub en marsh.com, comuníquese con su representante de Marsh o comuníquese con:

NELIA ARGAZ
Business Resilience & Cybersecurity Consulting practice leader
South West Europe & Turkey
Marsh Risk Consulting
nelia.argaz@marsh.com
+34 672 426 740

MARC CHAMIZO GILABERT
Senior Consultant
CyberSecurity & Business Resilience Senior Consultant
Marsh Risk Consulting
marc.chamizo@marsh.com
+34 935 035 723 | +34 673 17 50 72

www.marsh.es

 twitter.com/MarshGlobal

 linkedin.com/company/marsh-spain

 facebook.com/MarshGlobal

 youtube.com/user/TheMarshChannel