MONETARY AND CAPITAL MARKETS

Serie especial sobre la COVID-19

Las notas de la serie especial, preparadas por expertos del FMI, pretenden ayudar a los países miembros a abordar los efectos económicos de la COVID-19. Las opiniones expresadas en ellas son las de los autores y no representan necesariamente las del FMI, el Directorio Ejecutivo o la gerencia de la institución.

Ciberseguridad del teletrabajo durante la pandemia[1]

A consecuencia de la pandemia de COVID-19, han sido muchas las instituciones financieras y autoridades del sector financiero que han adoptado el teletrabajo, lo cual incluye el acceso remoto a sistemas y datos que puedan ser de importancia crítica en sus organizaciones. Debido a esta adopción generalizada del teletrabajo durante un período prolongado y a las vulnerabilidades asociadas a esta modalidad de trabajo, se espera un aumento considerable de los ciberataques. Por lo tanto, las instituciones financieras que aún no lo hayan hecho, deberían considerar la implantación de fuertes controles de seguridad para el acceso remoto a sus redes de trabajo. Del mismo modo, las autoridades financieras que aún no lo hayan hecho, deberían considerar emitir directrices de contenido técnico basadas en buenas prácticas internacionales.

I. POSIBLE AUMENTO DE LA VULNERABILIDAD

La mayoría de las instituciones financieras han estado usando infraestructuras de acceso remoto a la red desde hace tiempo; sin embargo, las capacidades instaladas pueden no haber sido las suficientes para permitir que la mayoría de sus empleados puedan trabajar simultáneamente con acceso remoto a la red, lo cual aumenta los posibles riesgos de seguridad. Los departamentos de informática han de estar sometidos a una actualizar de su capacidad permanente y rápidamente que permita cambiar o reemplazar sistemas existentes con poco tiempo para realizar pruebas de seguridad exhaustivas. Las vulnerabilidades en las infraestructuras y en los protocolos de acceso remoto pueden pasar inadvertidos y ser aprovechados durante ataques cibernéticos.

Está aumentando la implantación y uso de tecnologías en la nube para responder rápidamente a la necesidad de mayor capacidad. En un contexto de escasez de tiempo y de recursos, los riesgos de seguridad inherentes a la utilización de los servicios en la nube posiblemente no hayan sido debidamente evaluados y los controles existentes podrían no ser totalmente eficaces en los nuevos entornos. Este riesgo también está presente cuando se usan proveedores de servicios en la nube a los que se les ha considerado que ofrecen infraestructuras seguras, ya que los propios usuarios lo que siguen siendo responsables de

[1] Para más información, las autoridades nacionales pueden contactar a Nigel Jenkinson (njenkinson@IMF.org), Jefe de División, División de Supervisión y Regulación Financiera del Departamento de Mercados Monetarios y de Capital (MCMFR).

determinados aspectos de la seguridad en la nube (tales como configurar controles de acceso adecuados).

Los empleados que no estén familiarizados con el teletrabajo y estén bajo el estrés causado por la pandemia pueden ser objetivos fáciles de ataques de *phishing* y de ingeniería social. En las últimas semanas, ha habido un aumento de ciberataques que buscaban generar una respuesta aprovechando la sensibilización de la población a la información relacionada con la COVID-19. Por ejemplo, invitaciones a hacer clic en enlaces maliciosos y la descarga de ficheros adjuntos o aplicaciones infectadas por programas maliciosos.

Terminales (*endpoints*) inseguros y un sistema débil de autenticación para el acceso remoto a la red son dos de los elementos principales que aumentan el riesgo de ciberataques. Computadoras portátiles u otros dispositivos móviles que no tengan instalados los últimos parches de seguridad son ejemplos de terminales inseguros. En el contexto del acceso remoto a la red, se considera débil la autenticación que utilice contraseñas sin un segundo factor es deficiente. Por tanto, la aplicación de requisitos estrictos en materia de contraseñas es un tema importante que debe abordarse.

Funciones relacionadas con datos y sistemas críticos que normalmente no está permitido que se realicen fuera de las instalaciones físicas de las instituciones, por ejemplo, las operaciones de tesorería, puede que tengan que realizarse fuera de sus instalaciones durante la pandemia. Así, los controles existentes posiblemente no sean suficientes para proteger las funciones, los sistemas y datos de importancia crítica.

Es fundamental aplicar medidas técnicas y normativas centradas en la seguridad de la información para atenuar los riesgos de ciberseguridad que conlleva el acceso remoto. Pese a no referirse específicamente al acceso remoto, las políticas rigurosas de seguridad de la información (que incluye el control de acceso a los datos y políticas exhaustivas de registro detallado y seguimiento) refuerzan la seguridad del acceso remoto. Algunas instituciones financieras han tenido puntos débiles en la implementación de tales políticas y, por lo tanto, están más expuestas a sufrir ataques durante la pandemia.

II. RECOMENDACIONES

Las autoridades e instituciones financieras que aún no lo hayan hecho, deben implementar con rapidez y eficacia buenas prácticas y normas técnicas internacionales sobre la materia para que el teletrabajo sea seguro. Si bien algunas normas técnicas vigentes abordan específicamente los controles del teletrabajo (por ejemplo, NIST 800-46 Rev 2 o BSI IT- Grundschutz Compendium), otras describen controles genéricos que son pertinentes para el teletrabajo (tales como COBIT 2019[2], o la serie ISO 27000). Entre los temas clave a los que las instituciones financieras deben dar prioridad se incluyen los siguientes: i) una robusta autenticación de usuarios y dispositivos[3], y métodos sólidos de encriptación; ii) dispositivos seguros de acceso a la red; y iii) monitoreo de la seguridad en las redes.

Los servicios de acceso remoto a la red y los perfiles de usuario deben activarse únicamente cuando sea necesario. Cuando no hay una necesidad operativa, el acceso remoto a la red debe inhabilitarse para reducir la superficie de ataque.

[2] Por ejemplo: controles BAI09.02, DSS05.02, DSS05.03 y DSS05.06

[3] Para la autenticación de usuarios se recomienda especialmente usar dos factores. Deben autenticarse los dispositivos en ambos extremos de la conexión, por ejemplo, usando certificados digitales.

La utilización de la nube debe basarse en evaluaciones detalladas de riesgos. De acuerdo con estas evaluaciones de riesgo, que han de tener en cuenta la naturaleza crítica de los sistemas y datos que se transfieren a la nube, es preciso implementar mecanismos eficaces de control de seguridad que utilicen todas las instalaciones en la nube para respaldar esos mecanismos (tales como los controles de acceso a los equipos, la gestión de identidad y acceso, y el inicio de sesión y seguimiento).

Las teleconferencias deben realizarse en plataformas aprobadas que permitan evitar accesos no autorizados. Dado que se transmite y comparte una cantidad mucho mayor de información confidencial a través de los servicios de teleconferencia, resulta fundamental realizar una evaluación de vulnerabilidades antes de su uso a gran escala para garantizar una seguridad adecuada de la información. Además, se deben usar medios técnicos y de procedimiento para autenticar a los participantes en teleconferencias, por ejemplo, usando números de identificación personal (PIN) y verificando que quienes participan efectivamente hayan sido invitados.

Es preciso realizar campañas adicionales de sensibilización sobre ciberseguridad entre los empleados. Dado que la solidez del sistema lo determina su eslabón más débil, todos los empleados deben entender el mayor nivel de amenaza derivada del *phishing* y de las campañas en redes sociales durante la pandemia. Se debe dar rápido apoyo a los usuarios a través de centros de soporte técnico en caso de sospecha de incidentes de seguridad.

Deben implementarse fuertes controles en las configuraciones en ambos extremos de la conexión remota para evitar una posible utilización maliciosa. Por ejemplo, los empleados no deben tener derechos de administración sobre computadoras portátiles que sean propiedad de la empresa[4]; deben establecerse configuraciones de seguridad más estrictas y soluciones de seguridad actualizadas para los terminales (*endpoints*); los parámetros de seguridad de conexión deben configurarse de conformidad con buenas prácticas y mantenerse cerrados, y debe controlarse rigurosamente la infraestructura corporativa de acceso remoto a la red. Es una buena práctica realizar análisis de seguridad de los dispositivos que establezcan una conexión remota, y el acceso remoto a la red solo debe habilitarse para dispositivos que cumplan con las condiciones para ello.

Las instituciones financieras deben implantar controles adicionales de seguridad para aquellas funciones críticas que en condiciones normales no estaría permitido que se realizasen a distancia. Por ejemplo, los usuarios que realizan tales actividades solo deberían poder conectarse usando dispositivos que sean propiedad y estén controlados por la institución financiera y totalmente protegidos y configurados con un alto nivel de seguridad; por otra parte, no se debe permitir guardar datos sensibles en dispositivos locales[5].

Los supervisores deben reforzar el mensaje de que el teletrabajo aumenta el riesgo de ciberseguridad, el cual debe enfrentarse con fuertes controles. Se recomienda que las autoridades emitan directrices adicionales que describan el riesgo, así como hacer referencia a las directrices pertinentes que ya existan, y aporten información más detallada en caso necesario, por ejemplo de manera similar a esta nota[6].Los supervisores deben ser conscientes que de no existir previamente directrices pertinentes y si las prácticas de gestión del riesgo de ciberseguridad en las instituciones financieras no son lo suficientemente maduras, es

[4] Se recomienda firmemente que, en el caso de computadoras personales que no puedan ser controladas adecuadamente por la empresa, por ejemplo, en un contexto en el que los empleados usan sus propios dispositivos, los empleados trabajen con cuentas de usuario sin privilegios.

[5] El uso obligatorio de servidores de escritorio remoto debidamente configurados o servidores de salto son ejemplos de formas para restringir eficazmente el almacenamiento local de datos.

[6] Véase un análisis más amplio de las prácticas de supervisión recomendadas en el documento del FMI titulado “Cybersecurity Risk Supervision”. Puede acceder al documento en https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238.

posible que varios controles clave o no existan o sean ineficaces, lo cual hará difícil mejorar la situación en las circunstancias actuales. En este caso, se puede tratar de compensar en parte esta carencia fortaleciendo los controles de la dirección y la supervisión de las actividades de los empleados y realizando campañas de sensibilización.