Deloitte.

Cyber Consideraciones de Ciberseguridad en medio de una pandemia global

Consideraciones generales de ciberseguridad en medio de eventos extraordinarios

- Los procesos de negocio cambian y hay una mayor demanda hacia los servicios de acceso remoto y colaboración, lo que crea nuevos riesgos: **Se recomienda adaptar las políticas, procesos y controles de ciberseguridad al nuevo escenario de operación.**
- A medida que las organizaciones recomiendan que los empleados trabajen de forma remota, aumenta el uso de dispositivos móviles y el acceso remoto a los sistemas empresariales centrales: **Se recomienda fortalecer la gestión de acceso a la identidad organizacional y el monitoreo y correlación de eventos.**
- Las crisis, a menudo, reducen los niveles de alerta y protección de los usuarios finales y llevan a los ciberdelincuentes a aprovecharse de esta situación y operar bajo esquemas
- Maliciosos: **Se recomienda aumentar la conciencia ante el surgimiento de nuevas amenazas**
- Un mayor riesgo de fuga de datos confidenciales o privados debido a su exposición en entornos no seguros: **Se recomienda gestionar las conexiones remotas.**
- La transformación digital permite a las organizaciones desarrollar sistemas y medidas de seguridad para evitar la intrusión y el acceso a sistemas críticos: **Se recomienda contar con un plan de recuperación cibernética.**

Consideraciones de ciberseguridad dependientes de la situación de la compañía

1. Para las empresas que no han implementado soluciones de colaboración y acceso remoto y no tienen oficinas remotas a gran escala

• Evaluar el alcance y el modelo de colaboración empresarial remota en función del tamaño de la compañía y las características de la industria.

• Seleccionar herramientas de colaboración razonables adecuadas para escenarios comerciales específicos.

Para ello tener en cuenta:

- Las características de seguridad de la plataforma o el software de oficina remota.

- Las condiciones de propiedad de los datos y protección de la privacidad establecidos en el acuerdo de uso / cooperación - Las certificaciones de seguridad de la industria.

- Otras características relacionadas: portabilidad, disponibilidad, escalabilidad, entre otros.

• Clarificar el alcance del acceso a servicios de oficina por parte de terceros, definir los límites de integración con sistemas de terceros y fortalecer el control de acceso de seguridad a datos confidenciales.

• Mejorar el monitoreo de seguridad y la protección de los servicios y sistemas de información de la empresa, y, de ser necesario, reorganizar los roles de análisis y respuesta a ataques de ciberseguridad.

2. Para empresas con acceso remoto flexible y soluciones de colaboración ya implementadas

• Llevar a cabo actividades de concienciación y entrenamiento de seguridad de la información y ciberseguridad en aspectos relacionados con el modelo de colaboración remota de los empleados.

• Realizar un seguimiento oportuno de accesos sospechosos y situaciones anormales.

• Los departamentos de TI y seguridad deben ejecutar los planes de seguridad para oficinas remotas en escenarios especiales y repasar los procesos de respuesta de emergencia correspondientes.

• Centrar la atención en garantizar instalaciones de servicio que proporcionen acceso remoto y colaboración de forma segura, tales como: capacidad, disponibilidad y seguridad de los servicios VPN, seguridad de los servicios de correo electrónico y acceso a los datos almacenados en la red interna, entre otros.

• Revisar y de ser posible, mejorar, las medidas de protección de seguridad de los servicios e interfaces de acceso remoto (que incluyen, entre otros, autenticación multifactorial, la eliminación oportuna de privilegios de acceso remoto y el monitoreo sobre los servicios de acceso remoto) y los planes de emergencia correspondientes para mejorar la flexibilidad de los servicios de red.

• Fortalecer las capacidades de monitoreo y análisis de seguridad de toda la red de la empresa, prestando especial atención a los comportamientos de acceso privilegiado.

• Enfocar el monitoreo en el uso de datos confidenciales y en los servicios centrales que brindan acceso a estos datos (tales como el correo electrónico, plataformas de operaciones comerciales, entre otros).

• Dar prioridad a las soluciones de acceso y oficina remota aprobadas por la empresa, y tratar de evitar el uso temporal de software de terceros para compartir información confidencial.

• Realizar oportunamente copias de seguridad de los datos en la nube y proporcionar varias versiones de copias de seguridad históricas.

3. Otros escenarios de riesgo de seguridad para observar

Ciberseguridad en oficinas corporativas desatendidas:

• Reforzar las restricciones de acceso físico a las oficinas.

• Organizar el monitoreo de seguridad física en el sitio.

• Definir esquemas para responder de manera oportuna a condiciones anormales en el lugar.

• Establecer un sistema de servicio remoto para que el personal en servicio realice el monitoreo en tiempo real de la sala de computadoras, la red, los sistemas, las condiciones de operación de las aplicaciones, el uso de recursos.

• Apagar equipos innecesarios de red periférica y nodos en la oficina.

Protección de datos privados de los empleados:

• En respuesta a los requisitos de control de pandemia, las empresas deben controlar estrictamente el acceso, transmisión y uso de dichos datos en el proceso de estadísticas de información de salud y gestión de empleados para asegurar un alcance limitado de conocimiento.

• Establecer el nivel de protección de datos clínicos y médicos y evitar el uso de plataformas de terceros para su almacenamiento o transmisión.

Conclusión: Conforme mejore la pandemia y la rutina de trabajo vuelva gradualmente a la normalidad, las compañías tendrán que eliminar las excepciones, reglas especiales, planes temporales o entradas que se habilitaron durante la fase de oficina remota. Asimismo, deberán llevar a cabo un inventario y una actualización de las operaciones de seguridad de la red, establecer nuevamente las medidas adecuadas para la operación rutinaria y regresar a la gestión de la seguridad, bajo la filosofía de cero confianza.

En un contexto como el actual, será crucial que las estrategias cibernéticas estén alineadas a las funciones del negocio, las operaciones, la continuidad comercial / la resiliencia técnica y la gestión de crisis. Los planes de las organizaciones tendrán que contemplar métodos únicos que les permitan conocer los riesgos a los que su red puede estar expuesta, detectar amenazas avanzadas y descubrir brechas sistémicas en el proceso de respuesta ante posibles incidentes.