Título No a la intrusión: Diez “tips” a cumplir para conservar segura su información

Tipo de Producto Parte de Prensa

Autores Pirola, Alejandro Martin

Código del Proyecto y Título del Proyecto

A15S24 - Gestión de la ciberseguridad. Acceso no autorizado a sistemas informáticos

Responsable del Proyecto

Bertizzolo, Maria Eugenia Leila

Línea

Nuevas tecnologías y Derecho

Área Temática

Derecho

Fecha

2016

INSOD
Instituto de Ciencias Sociales y Disciplinas Proyectuales

UADE FUNDACIÓN UADE

No a la intrusión: Diez "tips" a cumplir para conservar segura su información.

Alejandro Martin Pirola (Inf. en Informática de Fundacion UADE)

Casi a diario las noticias nos cuentan sobre organizaciones que han sido víctimas de lo comúnmente llamado *hackeo.* Este parece un mal de la era tecnología, imposible de flanquear y superar. Esto no es así, como tampoco es correcto pensarlo en términos de última tecnología. Lo importante es el factor humano organizacional y la información a proteger. En este sentido, compartimos diez consejos a tener en cuenta sin importar si ud tiene un gran negocio o un modesto emprendimiento.

1. Planificar: es imposible pensar en una estrategia sin saber cuál es nuestro objetivo. Necesitamos pensar cual es la información a proteger, cual es la mejor alternativa para esa información. que recursos se necesitan para llevar a cabo la tarea, cuanto tiempo nos va a llevar cumplimentar esta tarea, quien o quienes serán los responsables y, por último, como, en cuanto tiempo y quien va a ser el encargado de auditar los resultados.
2. Enseñar: Es importante invertir en formación de las personas que están dentro de nuestra organización. Muchas veces se detectan intrusiones informáticas productos del error humano. Este no es voluntario y no significa un descompromiso de las personas que componen nuestra organización. Es saludable pensar en términos de darle a quienes integran nuestra organización capacitación sobre prevención. La responsabilidad no es solo del área de tecnología sino de todos y cada uno de los que integran nuestra organización.
3. Priorizar: Es relacionado al factor humano también. El cambio culturar en post de la seguridad de la información refuerza el mensaje de la importancia que tienen estos datos para las organizaciones. El liderazgo y la revalorización de recursos (tanto técnicos como financieros) van a contribuir a la creación de esta cultura. El compromiso de los directivos, la inversión en recursos y tiempo en el tema, son visibles para el resto. Es necesario crear la aversión a la perdida y daños de nuestra información.
4. Monitorear: Muchas empresas sufren intrusiones durante días, semanas, meses y años antes de advertir el hecho. Es importante tener en cuenta que la seguridad no es algo que se decide una vez y se mantiene por siempre. Si bien hay herramientas tecnológicas que ayudan en la tarea es necesario un monitoreo y análisis continuo de los datos que estas herramientas nos brinden. No siempre hay recursos para tener especialistas en seguridad informática en nuestra organización pero es importante que al menos pidamos ayuda externa en este punto.
5. Gestionar: no solo actuamos pensando en disminuir la probabilidad de que ocurra una intrusión sino también en disminuir los potenciales daños que esta genere. Mantener copias de seguridad de la información ayuda pero no siempre es suficiente. Debe establecer una política de gestión relacionado a este punto. No solo es hacer la copia de la información sino también herramientas para validad el contenido de nuestras copias y como se va a llevar adelante la restauración de la misma. Asimismo, si este proceso se realiza a través de un servicio en línea (o los hoy denominados en "la nube"), asegurarse la

política que ellos mantengan al respecto. Como regla general considere: el material de resguardo debe tener al menos el mismo sistema de seguridad que el material original. Para más claridad pregúntese lo siguiente: ¿qué datos son los que se guardan como copia de seguridad? ¿cada cuánto se realiza esta tarea? ¿en quién recae esta responsabilidad? ¿Quiénes tienen acceso a estas copias? ¿Dónde, cómo y en que entorno se almacena esta información? ¿Si necesito esta información, como se hace la restauración de los datos?

6. Actualizar: tenemos que tener en claro dos aspectos sobre este punto. Por un lado, la actualización de las herramientas informáticas relacionadas a la seguridad y a los propios sistemas que se utilizan. Muchas veces la intrusión se da por fallas en los programas que ya han sido detectadas y que existen parches o actualizaciones para ellas. Este factor se mitiga actualizando, con versiones oficiales, los programas que se utilizan en los dispositivos de nuestra organización. El otro factor, relacionado a las personas, tiene que ver con la actualización de sus accesos al sistema. Es importante establecer reglas periódicas de cambio de contraseñas y, si existen, validad otros medios de autenticación que requieran algo más que una contraseña. Dependiendo el grado de acceso que la persona tenga a la información, suponiendo que esta esté segmentada, puede ser útil requerir otros niveles de seguridad como pines, token (hoy muy de moda), etc.
7. Preparar: tenemos que entender que la información no está segura, que siempre hay riesgos de intrusión y que hace necesario establecer qué hacer cuando algún hecho no deseado pase. La lógica seria: me preparo para lo peor y busco el menor riesgo. Nuevamente tenemos que tener en cuenta dos aspectos. Armar un plan para actuar de manera coordinada y rápida en las acciones que tomemos. No podemos pensar que vamos a hacer cuando ya haya pasado. Se pueden establecer grados de vulnerabilidad y sobre ellos diferentes medidas de acción. Es importante que haya un plan organizado previamente. Además, tener un plan, ejecutarlo de manera rápida y eficiente es vital cuando hablamos de operatividad de la organización. ¿Qué queremos evitar? Falta de acceso de la información producto de la intrusión, la imposibilidad de reanudar tareas y la pérdida de tiempo por falta de operatividad.
8. Cooperar: Luego del mal rato que pasamos por la intrusión es necesario tomar medidas que muchas veces implican involucrar al Estado. Es importante determinar ante qué tipo de intrusión, como y cuando se va a realizar una denuncia al respecto a las fuerzas de seguridad. Determinar qué tipo de incidentes se denuncia y quien tiene a su cargo hacerlo muchas veces se vincula al cumplimiento de normas jurídicas. Por ejemplo, aspectos relacionados a la protección de datos personales sensibles.
9. Actuar: Casi tan importante como prevenir es saber curar y es vital para nuestra imagen. Aquí confiamos en la gente de comunicación. Gestionar una respuesta tanto a nuestras personas internas sino también a la población en general. En muchos casos, sobre todo en empresas de tecnología, los hechos de intrusión se perciben como pérdida de calidad en la marca. En otros casos, se percibe como un hecho bochornoso o como un caso para que la prensa pueda informar.
10. Evaluar: Si llego a este paso no es necesario frustrarse sino entender la realidad actual y tratar de mejorar. Existen modelos de autoevaluación para instituciones sencillos que ud

puede realizar para comprender en qué estado se encuentra hoy su organización. Vislumbre el incidente como una oportunidad de mejora, como un momento de inflexión para cambiar el rumbo de su política de seguridad.

Tenga presente que existen muchas reglas, documentos y guías en materia de seguridad informática. Hay mucho escrito y dicho en materia de buenas prácticas. Es un terreno complicado pero necesario de atravesar. Antes de decidir que tecnología queremos necesita conocer y determinar qué es lo que quiere proteger.