Check Point®
SOFTWARE TECHNOLOGIES LTD

GUÍA DE LA CIBER SEGURIDAD

10 PASOS HACIA UN NEGOCIO MÁS SEGURO

GUÍA DE LA CIBERSEGURIDAD

10 PASOS HACIA UN NEGOCIO MÁS SEGURO

TÓMESE EN SERIO EL ASUNTO DE LA SEGURIDAD

De la misma forma que hemos aprendido a desconectar las alarmas del coche, nos hemos vuelto insensibles a los titulares sobre ciberdelincuencia. A pesar de que los cibercriminales robaron más de 500 millones de identidades[1] solo en 2014. Según un artículo de Computer Weekly de diciembre de 2014[2], "La producción de malware continúa creciendo a escala industrial, con kits de exploit y servicios malware que ponen sofisticados métodos de ataque en manos de cibercriminales relativamente poco cualificados." Y desgraciadamente, ignorar este problema no hará que desaparezca.

Nos guste o no, las empresas tienen la carga añadida de tener que proteger la información con el mismo ímpetu y fuerza que los gobiernos protegen sus secretos. No importa si su empresa está dentro del negocio de la tecnología, banca, sanidad, fitness o comida rápida, si usted vende algo, lo más problable es que almacena información personal en su red.

Los activos de red requieren de la misma protección permanente que necesita un inventario físico o depósito bancario. Algunas compañías entienden exactamente cómo lograr esto, mientras que para otras la seguridad continúa siendo todo un misterio.

Comprender su exposición a las amenazas y lo que puede hacer al respecto no es solamente una gestión empresarial responsable — es algo de importancia vital para la supervivencia del negocio.

En las páginas siguientes encontrará 10 pasos que le ayudarán a llevar a su organización a estar más segura.

Queremos que su negocio crezca, que florezca y lo más importante de todo, que sea seguro.

> LA PRODUCCIÓN DE MALWARE CONTINÚA DESARROLLÁNDOSE A ESCALA INDUSTRIAL.

1 "Los funcionarios advierten sobre 500 millones de registros financieros hackeados", USA Today, Octubre de 2014
2 "Top 10 Cybercrime Stories of 2014", Computer Weekly, Diciembre de 2014

COMPRENDA LA NECESIDAD

Los riesgos y el acceso

El riesgo de la información es auténtico

La mayoría de la gente pensaba que los delitos cibernéticos eran algo que solo afectaba a las instituciones gubernamentales. Sin embargo, cada año que pasa la ciberdelincuencia se acerca más al rellano de nuestra puerta. En la mayoría de las ocasiones no somos conscientes de que existe una amenaza hasta que la sentimos en nuestras carnes.

En 2014, ataques a Target, Home Depot y Sony salieron ya en la prensa. Pero si no estuviera en la industria, es muy probable que no hubiera oído hablar sobre los miles de ataques a compañías grandes y pequeñas, de todos los sectores, y relativos a todo tipo de datos que se producen. Pese a que las 'vulneraciones más pequeñas' pueden verse como algo que no produce un impacto importante, cada una de ellas proporciona más información para que se perpetren más ataques posteriores, puesto que la mayoría de las personas realiza pequeñas modificaciones o ninguna a las contraseñas de sus distintas cuentas.

La regla del 1 y 3

El riesgo de seguridad en la información es una combinación de tres factores: activos, vulnerabilidades y amenazas (los activos quedan expuestos por las vulnerabilidades que pueden estar expuestas a las amenazas). Una vulneración se convierte en la semilla de muchas otras.

Estos tres factores han aumentado considerablemente en los últimos años. Aquí tenemos el motivo:

1. A medida que Internet se vuelve más ubicua, nuestra vida está aún más expuesta en la red, y damos por sentado que nuestra información y datos personales no están en riesgo. Mientras nos limitemos a acceder a sitios Web legítimos o conocidos y no facilitemos nuestras contraseñas estaremos a salvo ¿verdad? Error.
2. Cuanto más cómodos nos sintamos interactuando y haciendo negocios online, más huellas digitales dejaremos — y eso puede llevarnos a exponernos a más vulnerabilidades.
3. La ciberdelincuencia se ha convertido en una industria en sí misma. El volumen de amenazas ha alcanzado proporciones asombrosas, y continúa creciendo y evolucionando.

Un estudio de Rand[3] afirma que la ciberdelincuencia es en muchas situaciones más rentable que el tráfico de drogas, porque es más fácil de gestionar con pocas personas, tiene un riesgo de detección mucho menor, e incluso un riesgo menor de ser juzgado o acusado.

Abordar el problema

El crecimiento explosivo de las amenazas nos ha llevado a un nuevo nivel más elevado de sensibilización, y a tomar medidas y aplicar acciones para abordar el problema. Los gobiernos cada vez tienen más peso en esta materia, al igual que las fuerzas del orden. Es el momento de que las empresas intensifiquen sus esfuerzos proactivos en materia de seguridad.

Las empresas más conscientes de este riesgo — desde las más pequeñas a las más grandes, — están vislumbrando la necesidad de llevar el asunto de la seguridad al centro de atención. No se trata solo de proteger, se trata de habilitar.

Con los años, las empresas han empezado a reconocer la necesidad de tratar la ciberseguridad al mismo nivel que la seguridad física. Las violaciones o ataques físicos requieren mano de obra y proximidad; es más fácil hacer un inventario y hacer un seguimiento de las pérdidas. Un ciberdelincuente por el contrario, puede atacar desde el otro lado del mundo en cuestión de segundos. Puede llevar semanas descubrir qué han robado, por no mencionar lo difícil que será seguir la pista a los ladrones. Es más, la ciberdelincuencia produce un impacto mucho mayor en la cifra de resultados de la mayoría de compañías que el de los robos físicos.

Pese a que ahora la mayoría de ejecutivos califican el riesgo de la seguridad cibernética igual de alto que el de la seguridad física, no han estado sin embargo muy rápidos en llevar este asunto a las reuniones de sus consejos — no lo han hecho hasta que no se ha producido una violación de la seguridad. La nueva norma que hay que seguir es pensar en la seguridad de forma proactiva.

Cuando una empresa está en el negocio de manejar y gestionar datos personales, la apuesta es más alta y deben seguirse ciertas regulaciones legales. Hay que aplicar políticas de acceso y es necesario tomar determinadas precauciones. Los datos personales necesitan tratarse como información confidencial.

En el año 2014, el valor medio de una identidad estaba valorado en 188 dólares. Aunque eso pueda parecer poco, la información de identidades se almacena normalmente, y roba, en lotes de decenas de miles a millones de una vez. Todo esto suma al final unas pérdidas bastante significativas.

El acceso a la información sensible debería restringirse únicamente a aquellas que la necesitan. De esta forma puede seguir y supervisar cualquier violación de forma más eficiente. El resultado es que es más fácil gestionar las protecciones.

Asignar responsabilidades

La razón de que haya mucha gente que no está concienciada con el problema de la ciberdelincuencia es que no comprenden por completo las implicaciones que supone. La mayoría de la gente no valora que podría quedarse sin su trabajo si un ciberdelincuente robara los diseños de la empresa; o que robando la información de inicio de sesión de un juego online se podrían hackear las cuentas bancarias porque los ciberdelincuentes saben que los usuarios reúsan sus contraseñas en múltiples cuentas.

Divulgar que la protección de la información de la compañía es responsabilidad de todo el mundo no es suficiente. La gente necesita ser responsable a nivel individual y hacerle sentir que está involucrada en la seguridad de la compañía. Y la seguridad necesita ser una parte integrada y planificada de la infraestructura, no un añadido como resultado de una ocurrencia tardía.

Crear una cultura de la seguridad de la información requiere:

A. **Sumergirse en el concepto.** Prestar un cuidado especial a cómo quiere que opere su compañía y sus empleados. Luego crear una cultura que permita que esa visión se haga realidad, usando la seguridad como un habilitador.
B. **Preveer.** Conocer las regulaciones requeridas, las amenazas y vulnerabilidades. Pero no olvidarse de mirar con perspectiva al panorama general para asignar una política de seguridad que le ayude a conseguir eso — no solo ahora, sino más adelante.
C. **Cuidar los detalles.** Fortalezca la ejecutiva alrededor de la política de seguridad y póngala en marcha con responsabilidades claramente definidas.

Por encima de todo no complique las cosas en demasía. Cuando su política de seguridad es sencilla y clara, puede lograr una mayor tasa de éxito con la gente que se adhiere a su política.

3 Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar, Rand Corp, 2014

10 PASOS HACIA UN NEGOCIO MÁS SEGURO

USE LA SEGURIDAD PARA POTENCIAR LA INNOVACIÓN

1

La seguridad no tiene por qué ser el enemigo de la innovación. Un enfoque sólido de seguridad puede hacer mucho más que simplemente proteger la empresa frente a los ataques; también puede estimular la migración a tecnologías de base más completas que puedan impulsar su negocio. No debería subestimarse el valor de encontrar un equilibrio entre la evaluación del riesgo y los beneficios que las nuevas tecnologías podrían aportar a la empresa. Con frecuencia la innovación puede a la vez proteger y aumentar el rendimiento.

Cuando se adoptan nuevas soluciones y dispositivos innovadores, la evaluación de riesgos de seguridad debería formar parte del proceso de investigación. Tome en consideración las medidas de seguridad adecuadas tan pronto como sea posible durante el periodo de adopción. Según estudia las necesidades del negocio, antes de levantar su infraestructura piense bien, qué quiere que haga, y de qué forma la seguridad puede impulsar sus objetivos.

Asegúrese de contar con un experto en seguridad en su planificación de TI, que se integre y no sea un simple añadido. Esto le dará el nivel de protección más profunda que necesita para liberar la innovación.

CONTINUACIÓN >

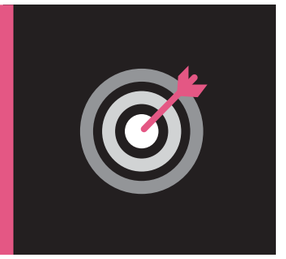
PRUEBE LOS LÍMITES

2

Un error que cometen muchas empresas es asumir que una vez que se han implementado medidas de seguridad el trabajo ya está hecho. En la actualidad esto no puede estar más lejos de la realidad. Las amenazas están cambiando y los ciberdelincuentes aprenden sobre la marcha, incrementando su nivel de sofisticación. Vigilar el panorama de amenazas, además de reforzar sus sistemas y políticas, es una cuestión de importancia vital.

La evaluación continua de la capacidad de recuperación de su empresa frente a las ciberamenazas ayuda a medir el progreso e idoneidad de las actividades de seguridad. Pruebe su infraestructura de forma periódica con auditorías de detección de intrusiones sobre el terreno. Considere trabajar con terceros para identificar vulnerabilidades. Asóciese con otros colegas del sector y manténgase al día de las nuevas amenazas.

CÉNTRESE



3

Con el volumen actual de amenazas, gestionar la seguridad de TI de su organización puede ser como arreglar constantemente fugas de agua en un barco. La clave es comprender la información o datos que resultan más críticos para mantener su negocio a flote.

Revise dónde es más vulnerable su organización en el caso de una violación de la seguridad y conviértalo en su principal prioridad. Considere cuestiones como la pérdida de información confidencial, la pérdida de reputación corporativa, y el incumplimiento de las normativas regulatorias. Luego céntrese en lo que puede hacer para minimizar el riesgo.

CONTINUACIÓN >

ESTÉ PREPARADO

4

Es un lema adoptado por los Boys Scouts (Siempre Listo) y debería aplicárselo cualquiera que esté a cargo de la securización de la integridad y operaciones de una empresa. No importa lo cuidadoso que uno sea, los incidentes de seguridad ocurrirán. En el entorno actual de amenazas y vulnerabilidades no debería preguntarse el "si", sino el "cuándo" seré víctima de un incidente con riesgo para la seguridad. El cómo gestione ese incidente, más que el incidente en sí mismo, puede representar un momento decisivo. No existe ni una sola compañía atacada en 2014 que esperara ser víctima antes de producirse el incidente. Las que contaban con un plan fueron las que se recuperaron más rápido y con un impacto menos negativo.

Haga que su negocio cuente con un plan de recuperación ante desastres (disaster recovery). Cuanto más grande y más compleja sea la organización, más tipos de incidentes habrá que tener en cuenta. Consulte con un tercer experto para comprender mejor y anticipar los posibles escenarios de amenazas. Identificarlos de forma anticipada reducirá significativamente los tiempos de respuesta en caso de una vulneración real de la seguridad.

Hágase cargo de su capacidad de respuesta y recuerde que la comunicación es la clave. Aquellos que hacen caso omiso de la importancia de esta regla acaban encontrándose desbordados por ayudas o atenciones no deseadas cuando la seguridad empieza a patinar.

Piense en un buen plan de comunicaciones en caso de un incidente de seguridad, con mensajes discretos e importantes para el personal interno, externo y las autoridades según sea necesario.

TENGA UNA VISIÓN GLOBAL

5

Cuando piense en su estrategia de seguridad, es importante considerar las amenazas y vulnerabilidades. Pero también es vital ver los factores que contribuyen y la imagen general de hacia dónde quiere llevar a su organización.

Según el informe de Servicios de Seguridad 2014 de IBM[4], más del 95% de los incidentes investigados indicaron el error humano como factor contribuyente. Mientras algunos errores provenían de una mala configuración de los sistemas y una gestión deficiente en la actualización de parches, el informe también revelaba la pérdida de portátiles o dispositivos móviles, la divulgación de información regulada (confidencial) a través de direcciones de correo electrónico incorrectas, o la apertura de adjuntos/URLs infectados como los cinco incidentes de infección principales.

En definitiva, la seguridad es un problema de todo el mundo dentro de la organización. Los negocios más preparados saben que la política de seguridad tiene que derivarse o surgir de objetivos estratégicos, objetivos de negocio y políticas corporativas; y asignarse a procedimientos y requerimientos, medidas de rendimiento, y por supuesto, gente de todos los niveles dentro de la organización.

Si quiere un bosque saludable debe cuidar el ecosistema que lo rodea.

Formar a la gente sobre cómo puede minimizarse el riesgo y cómo una seguridad sólida puede hacer avanzar el negocio en vez de entorpecerlo.

4 Informe IBM Security Services 2014 Cyber Security Intelligence Index

CONTINUACIÓN >

HAGA MÁS DE LO NECESARIO

6

El cumplimiento de seguridad está, entre otras cosas, dentro de la larga lista de leyes y normativas a las que deben atenerse las empresas. Desgraciadamente, muchos creen que cumpliendo los requisitos que regulan la privacidad, finanzas y protección del consumidor, ya están cubiertos. Pero este tipo de pensamiento puede sesgar el alcance y efectividad de una buena estrategia de seguridad. El cumplimiento de estos requisitos habitualmente se centra en amenazas específicas, que lo hacen menos completo de lo que una estrategia de seguridad podría o debería ser. Dado que estas normativas no garantizan una red segura, no debería constituir los fundamentos de su política. Teniendo esto en mente queda claro que hay que hacer más de lo necesario. Cree una política sóida de seguridad que salvaguarde la información y apoye procedimientos de respuesta y mitigación. Luego construya el cumplimiento en base a ella.

HÁGALO OFICIAL

7

Hacer oficiales las políticas corporativas de seguridad de la información y compartirlas en toda la compañía, puede proporcionar muchos beneficios interesantes:

- Crea un estándar a lo largo de toda la empresa como referencia para todos los empleados, que se convierten en integrantes de la cultura de seguridad.
- Más gente se involucra y compromete en proteger los activos de información vitales; y
- Su exposición al riesgo se hace más manejable.

Cuando cuenta con una gran población que le ayuda a implementar la política de seguridad, su aplicación y cumplimiento se hace más eficiente. Por ejemplo, de media existe un oficial de policía por cada 600 residentes en las ciudades con poblaciones por encima de los 50.000 habitantes. Cuando el público general se compromete a cumplir con la ley, los ciudadanos obedecen las reglas.

Esto funciona de igual forma en los negocios. Involucre a sus empleados en mejorar su estrategia de seguridad de la información educándoles en la forma en la que pueden ayudar. Cree políticas de seguridad que los empleados puedan comprender y ayuden a fortalecer.

CONTINUACIÓN >

OBTENGA APOYOS

8

Los objetivos globales producen el mayor impacto cuando vienen de más arriba. Y la protección de la información de su organización debe ser un objetivo global. Para muchos directivos, la seguridad de la información no está en lo más alto de la lista de prioridades; hay que ponerla ahí arriba.

Las brechas producidas durante los pasados cinco años en prácticamente todos los sectores proporcionan mucha información sobre los potenciales riesgos de no hacer de la seguridad una prioridad fundamental. Encuentre ejemplos de empresas similares a la suya y comunique los riesgos potenciales a la directiva. Si todavía no se han sumado a esta iniciativa, proporcionar estos datos debería ayudarles a decidirse. Asegurar los recursos necesarios, en términos de presupuesto y personas, es muy importante para la protección de la compañía. La firma ejecutiva de una política de seguridad demuestra un apoyo activo.

Ayude a todo el mundo, desde arriba hasta abajo, a comprender la importancia de mitigar los riesgos informáticos para proteger la propiedad intelectual. Esto solo salvaguarda el corazón de la compañía y ayuda a mantener la ventaja competitiva.

Dado que todos conocemos que las cifras y los datos importan más que las palabras, establezca un sistema de medida que le permita informar de forma periódica sobre sus progresos en cuanto la seguridad de la información. Además, asegure que comparte métricas con la alta dirección una vez al año.

Querrá identificar los indicadores de seguridad claves y poner en una gráfica la efectividad de las medidas de seguridad tomadas. Esto ofrece una información muy valiosa para la optimización continua de su política de seguridad, además de para las inversiones futuras en seguridad.

ESTABLEZCA MEDIDAS

9

Gestionar la seguridad de la información de una forma efectiva y eficiente requiere herramientas, formación y métodos de medida. Y dado que los empleados algunas veces ven la aplicación como algo negativo, también requiere una buena comunicación interna. Es vital asegurar que los métodos, técnicas de medida e iniciativas de seguridad se comparten y explican. Permita que sus equipos conozcan las últimas amenazas y la inversión que está haciendo la compañía para proporcionar una protección general.

Forme al personal para ayudarles a entender que tienen responsabilidades y cuál es su papel a la hora de ayudar a protegerse de las amenazas. Un tema importante en el que hay que detenerse es en el de la ingeniería social, dado su predominio en el panorama actual.

Con independencia del tamaño de su empresa, haga que sus empleados completen un cuestionario sobre su política de seguridad para reforzar su importancia.

Para las grandes compañías, tómese el tiempo y piense en identificar a personas específicas que sean los administradores de su política de seguridad de la información. Deberían asignarse diferentes responsabilidades para cada persona, junto con una clara comprensión de cómo se entrecruzan dichas responsabilidades. Documente y comparta la información con todo el mundo para que toda la gente involucrada lo sepa.

No olvide ir más allá de sus paredes para compartir la información con otros de su sector. Esto puede constituir una red de incalculable valor a la hora de identificar las mejores prácticas y advertir un ataque inminente.

CONTINUACIÓN >

NO BAJE LA GUARDIA

10

En algunas empresas la gestión de la seguridad se externaliza debido a la falta de personal o conocimientos. Con frecuencia, servicios como el backup, restauración, cifrado, y protección de datos pueden resultar atractivos para las pequeñas empresas. Pero la externalización presenta sus propios riesgos.

Las empresas externas que no protegen de forma adecuada la información o los sistemas de información pueden suponer una grave responsabilidad para las operaciones del negocio, reputación y valor de la marca.

Aquí tiene algunas directrices que siempre debe tener en mente:

1. Requiera a sus proveedores de servicios o suministradores que sigan sus políticas de seguridad de la información.
2. Asegúrese de que se respeten y definan acuerdos de nivel de servicio (SLAs) que incluyan puntos específicos acerca de métricas de disponibilidad del sistema y restauración. Haga auditorías periódicas para asegurar que su proveedor de servicios cumple el SLA. Compruebe sus registros de actividad para analizar y evaluar las amenazas.
3. Tenga en mente que cuando se trata de servicios cloud, existen políticas de seguridad de la información especiales. Si trabaja con un proveedor de servicios para almacenar, procesar o administrar datos en una red, familiarícese con sus políticas y consulte que cubren.

Bien sean proveedores de servicios de TI, proveedores cloud o una empresa externa subcontratada, si tienen acceso a, o gestionan cualquier información crítica para las operaciones de su empresa, asegúrese de que usted comprende sus políticas de seguridad y sus garantías.

CONVIERTA LA SEGURIDAD EN UN HABILITADOR

Dado que los datos son la piedra angular de los negocios, los líderes de hoy no se pueden permitir ignorar la cuestión de la seguridad Sin unas políticas adecuadas, tanto los clientes como la compañía misma están en riesgo. Comprendiendo las amenazas y vulnerabilidades potenciales, creando un plan robusto que se alinee con su negocio, y asegurando que las protecciones se integran en su infraestructura de TI, puede convertir la seguridad en un habilitador, más que en un deshabilitador.

De un paso proactivo para garantizar que su organización está segura. Realice un SECURITY CHECKUP de CHECK POINT, una evaluación gratuita que puede descubrir riesgos potenciales en su red:

http://www.checkpoint.com/campaigns/securitycheckup/index.html

Check Point®
SOFTWARE TECHNOLOGIES LTD

WE SECURE THE FUTURE

Para obtener más información sobre cómo asegurar su organización, visite:
www.checkpoint.com

CONTACTE CON NOSOTROS

Oficinas centrales | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
Oficinas centrales en EE.UU. | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com
Oficinas centrales en España | C/ Vía de las Dos Castillas, 33. Edificio Ática 6, Pta.3ª. Oficina D-1 | 28223 Pozuelo de Alarcón - España | Tel: +34 91 799 27 14

2015 de enero