N-economía Síntesis de documentos

FEBRERO 2015

AUTOR: ALICIA GONZALEZ

Nº 290

FICHA TÉCNICA

Título: 2014 State of Risk Report

Año: 2014

Fuente: Trustwave

Nº de páginas: 20

Acceso/coste: Gratuito

Localización: página web corporativa

CONCLUSIÓN PRINCIPAL

El año 2014 se considera el año del *data breach*. Sólo durante el último año se han producido en Estados Unidos 783 de estos ataques a la seguridad de las organizaciones y 229 en Europa de acuerdo con el instituto Identity Theft Resource Center y el Center for Media Data and Society, demostrando la enorme vulnerabilidad de las compañías, con cada vez más datos e información clave en la red.

Sin embargo, a pesar del número creciente de estos ataques, la ciberseguridad sigue siendo una asignatura pendiente en la mayoría de las empresas.

El informe señala que un 63% de las organizaciones no dispone de un método maduro de control y rastreo de información financiera, un 18% nunca testea la vulnerabilidad de su sistema, un 50% lo hace menos de una vez al trimestre y un 21% de las compañías no dispone de procedimientos de respuesta implementados.

Asimismo, este estudio funciona como una guía de seguridad que ofrece tips y sugerencias para mejorar la seguridad informática de las compañías.

AUTORÍA

El informe es elaborado por Trustwave, empresa presente en 96 países dedicada a la seguridad informática, protección de datos y lucha contra el cibercrimen .

Para su elaboración se compilaron 476 opiniones de profesionales del ámbito IT de 50 países. Los encuestados opinaron acerca de la susceptibilidad al riesgo que presentan sus empresas en los ámbitos de estrategia, gestión, procedimientos, mantenimiento de la seguridad y controles técnicos.

DESCRIPCIÓN Y CONTENIDO

La ciberseguridad es un área que se ha empezado a desarrollar de forma importante en los últimos años debido a la necesidad de las empresas de proteger sus datos clave (transacciones, cuentas bancarias, planes estratégicos, etc) ante la proliferación de malware que circula por la web, software utilizado por los atacantes externos con el objetivo de infiltrarse o dañar los dispositivos.

Tras evaluar la capacitación real que tienen las empresas para hacer frente a amenazas como el hacking y robo de datos, Trustwave pone a descubierto los puntos débiles más comunes en materia de seguridad. En base a estos resultados, asesora qué procedimientos o controles técnicos implementar y cómo responder eficientemente ante una amenaza a nuestra red interna.

Principalmente a través de fortalecer las siguientes áreas: la seguridad informática como objetivo corporativo, medidas para aumentar la protección de los datos y utilización de software y servicios de seguridad especializados.

ESTRUCTURA DEL INFORME

1) **Overview**
2) **Key findings**
3) **Methodology and scope**
4) **Major risk and Mitigation strategies**
5) **Management and Governance**
6) **Security Maintenance**
7) **Physical Security**
8) **Technical Controls**
9) **Conclusion**

OTRAS CONCLUSIONES

Realizar tests de forma regular

Implementar un programa que testeé la vulnerabilidad de los sistemas críticos de la empresa de forma periódica. Deberá incluir, entre otros: tests de penetración, escáneres de bases de datos y chequeos en la configuración.

Implantar cortafuegos y routers entre la red interna e Internet

Se trata de garantizar la protección de la red interna de la organización mediante barreras de seguridad que impidan la entrada de agentes externos.

Encriptar y monitorizar data

Los datos sensibles almacenados en sistemas aprobados tienen que someterse a un proceso de encriptación que los haga inaccesibles si no se introduce una determinada contraseña o si se conecta desde otro equipo. Además, para evitar la pérdida o filtración de datos se tiene que realizar un control y seguimiento de éstos.

Generar un compromiso que englobe a todos los niveles de la compañía en materia de seguridad

Crear una cultura de gestión del riesgo promovida y apoyada desde la presidencia de la compañía.

Todos los empleados deben ser conscientes de la importancia de los protocolos de seguridad y estar comprometidos en su mantenimiento. Asimismo, los contratos deben incluir acuerdos de confidencialidad que protejan los datos de la compañía.

Controlar el acceso de dispositivos al network de la empresa

Limitar el uso de dispositivos externos. La organización tiene que ser consciente de todos los dispositivos conectados a su red. Además de generar un sistema en el que cada empleado acceda a la red de acuerdo con los permisos que tenga, en relación a su puesto de trabajo o posición dentro de la empresa.

Asociarse con proveedores de servicios de seguridad

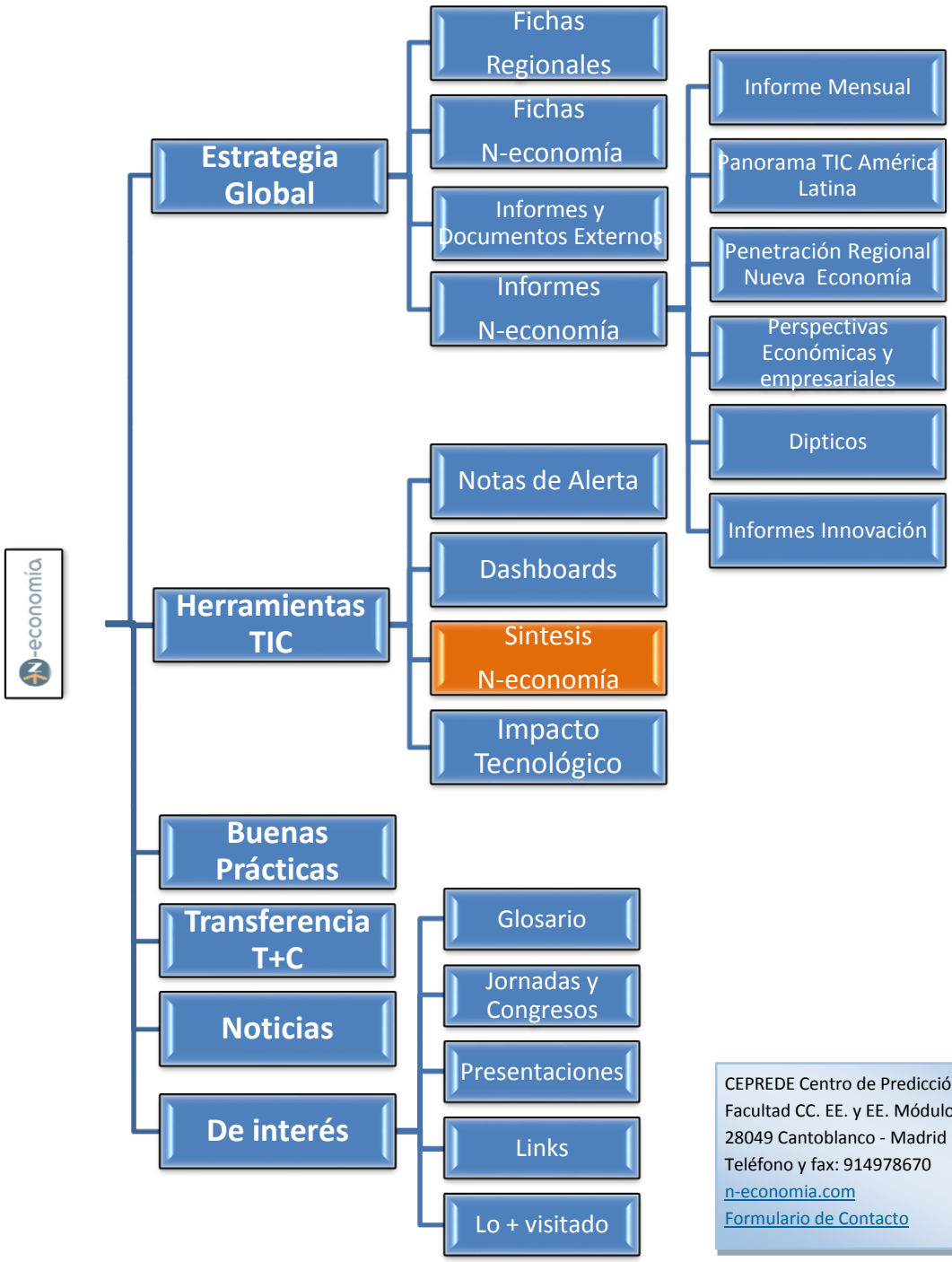
Si no se dispone de recursos o presupuesto suficiente para desarrollar habilidades informáticas internas, contratar los servicios de profesionales permite garantizarse de unos niveles de seguridad adecuados que mejoren la protección de la información con el apoyo de sistemas tecnológicos que generen análisis de control y prevención en tiempo real.

Diseñar protocolos de respuesta y reporte de incidencias

Cuando se produce una brecha en el sistema, una rápida respuesta puede ahorrar a la compañía grandes costes. La capacidad de actuar rápidamente es clave en la minimización del daño.

El reporte de incidentes permite mantener una base de incidencias actualizada con el fin de identificar indicadores de peligro en el sistema.

Consulta el resto de nuestro productos N-economía y siguenos en las redes sociales:



CEPREDE Centro de Predicción Económica
Facultad CC. EE. y EE. Módulo E-XIV UAM
28049 Cantoblanco - Madrid
Teléfono y fax: 914978670
n-economia.com
Formulario de Contacto

Entidades colaboradoras

N-economía es una iniciativa promovida por: