

JaCkHaCk^{Response}

RESOLVIENDO INTERROGANTES POST ATAQUE

La reacción natural de restaurar lo dañado, luego o durante un incidente, sin analizar lo que pasó, permite que muchas veces se vuelva a revivir el incidente.

En el 2007, un ISP en Perú informó que el 60% de los incidentes de sus clientes eran reincidentes.

Ello significa que las víctimas desestiman la oportunidad de mejorar sus defensas de seguridad al aprender la lección del incidente.

Descripción

JaCkHaCk-Response es un servicio de investigación de cómputo, orientada a descubrir quién, cómo y cuándo logró introducirse y dañar en los sistemas de información de una organización víctima.

Características y beneficios

- Sus ejecutivos sabrán contra qué, quién o quiénes se enfrentan.
- Luego del ataque, usted podrá escalar información científica y no subjetiva, para mejorar la toma de decisiones de sus ejecutivos.
- Aprenderá qué debe corregir para que el incidente no vuelva a acontecer.
- Descubrirá evidencias que el intruso o al mal manejo del incidente haya eliminado en la escena del crimen.
- Contará con la posibilidad de someter la evidencia a un procedimiento de salvaguarda y firma digital.

Ofrecimiento

Para que sus altos directivos cuenten con información precisa de los hechos detrás de un incidente de seguridad, JaCkSecurity ha desarrollado JaCkHaCk-Response, un servicio de análisis de intrusión en tiempo real, o *post mortem*.

JaCkSecurity logra éste cometido a través, de un estudio científico de los hechos detrás de un incidente, al arrojar la evidencia requerida para saber quién, cómo y cuándo lo hizo.

Nuestro compromiso

Suministrarle la ayuda para el manejo del incidente a fin de evitar arruinar la escena del crimen.

JaCkSecurity usa procedimientos competentes para el manejo de la evidencia

Los consultores de JaCkSecurity cuentan con experiencia en innumerables incidentes de seguridad y en la realización de servicios de análisis forense informático en Perú a redes y sistemas operativos Windows y Unix, con la posibilidad de extenderse a otros sistemas si así se requiere. Los procedimientos del manejo del incidente, que emplea JaCkSecurity, son competitivamente superiores para la preservación de evidencia forense.



Nuestros expertos comentan:

“La destrucción de evidencia tiene hasta tres diferentes orígenes:

- la inocente práctica de los responsables de TI, con el fin de restablecer los servicios,

- el mal intencionado acto de un empleado deshonesto o cómplice de un daño interno.

- y los criminales informáticos (a sueldo o por iniciativa propia), que no desean ser descubiertos.

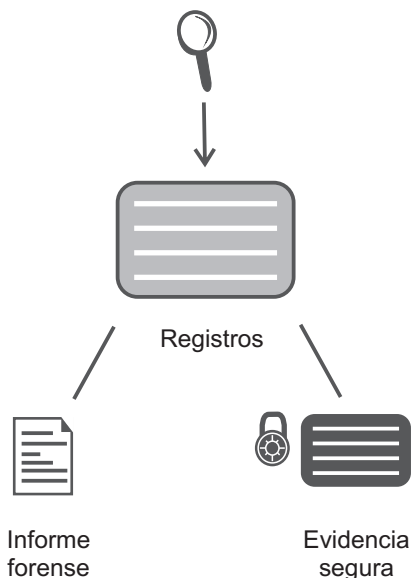
Sin embargo, aún ni la suspicacia será suficiente para señalar el origen real, si no se tiene una ayuda forense.

Nuestro servicio también es importante para medir la validez, daño e impacto de un incidente no concluyente, que está aconteciendo en su red”.

Especificaciones técnicas del servicio

JaCkHaCk-Response cubre los siguientes ámbitos: depende el caso.

- Análisis de intrusión en tiempo real
 - Incluye el manejo del incidente
 - Informe del incidente a discreción
- Análisis forense (informe *post mortem*)
 - Cronología del incidente
 - Quién(es) lo provocaron
 - Propósito
 - Debilidades aprovechadas
 - Posibilidad de metástasis
 - Recomendaciones técnicas
 - Sugerencias legales o civiles
 - Informe tipo técnico y ejecutivo



¿Por qué JaCkHaCk-Response?

JaCkHaCk-Response tiene dos momentos, durante y luego de un incidente. En el durante, es necesario descartar qué clase de evento o problema es el que se está experimentando, es decir, si es verdaderamente un incidente de seguridad o no, y de serlo, de qué tipo. En cambio, el luego, es para realizar tareas de restauración, sin dañar la evidencia, para analizar fuera de línea y determinar los hechos detrás.

Todo incidente de seguridad debe verse como una oportunidad de mejorar continua, tal y cómo lo son las no-conformidades en los sistemas ISO 9001, lo que ayudará a mejorar las defensas de sus sistemas.

JaCkHaCk-Response ayuda a descubrir aquellas evidencias que el intruso o al mal manejo del incidente haya eliminado en la escena del crimen.

Si el dinamismo de su negocio lo requiere, solicítenos asesoramiento para guiarles en la preparación de sistemas de recolección de evidencia de calidad ante futuros incidentes, de tal forma que pueda saber con rapidez los hechos. Vea la hoja técnica del servicio JaCkHaCk-Consulting en formulación de estrategias defensivas.