Procesos de seguridad

por Bruce Schneier

https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

Prevención

Limite los privilegios

No le de a ningún usuario más privilegios de los que necesita absolutamente para hacer su trabajo. Del mismo modo que no se le daría a un empleado cualquiera las llaves del despacho del director general, no le de la contraseña de los archivos del director general.

Proteja el eslabón más débil.

Dedique su presupuesto de seguridad a asegurar los mayores problemas y las mayores vulnerabilidades. Con demasiada frecuencia, las medidas de seguridad informática son como plantar una enorme estaca en el suelo y esperar que el enemigo corra directo hacia ella. *Intente construir una amplia empalizada.*

Utilice puntos de estrangulamiento.

Al canalizar a los usuarios a través de puntos de estrangulamiento (piense en cortafuegos), puede asegurar con más cuidado esos pocos puntos. Los sistemas que eluden estos puntos de estrangulamiento, como los módems de escritorio, dificultan mucho la seguridad.

Proporcione defensa en profundidad.

No confíe en soluciones únicas. Utilice varios productos de seguridad complementarios, para que el fallo de uno de ellos no suponga una inseguridad total. Esto podría significar un cortafuegos, un sistema de detección de intrusos y una autenticación fuerte en los servidores importantes.

Falla con seguridad

Diseñe sus redes de modo que, cuando fallen los productos, lo hagan de forma segura. Cuando falla un cajero automático, se apaga; no expulsa dinero por la ranura.

Aproveche la imprevisibilidad

Usted conoce su red; su atacante, no. Esta es su gran ventaja. Dificúltele el trabajo disfrazando las cosas, añadiendo *honey pots* y trampas explosivas, etcétera.

Aliste a los usuarios

La seguridad no puede funcionar si los usuarios no están de su lado. Los ataques de ingeniería social suelen ser los más dañinos de cualquier ataque, y solo pueden defenderse con la educación de los usuarios.

Adopte la simplicidad

Mantenga las cosas lo más sencillas posible. La seguridad es una cadena; el eslabón más débil la rompe. Simplicidad significa menos eslabones.

Detecciones y respuestas

Detecte los ataques

Vigile los productos de seguridad. Busque señales de ataque. Con demasiada frecuencia, las valiosas alertas de cortafuegos, servidores e incluso IDS simplemente se ignoran.

Responder a los atacantes

No basta con detectar los ataques. Es necesario cerrar las vulnerabilidades cuando los atacantes las encuentran, investigar los incidentes y perseguir a los atacantes. Tenemos que construir un mundo en el que los delincuentes sean tratados como tales.

Esté alerta

La seguridad requiere una vigilancia continua; no basta con leer un informe semanal. Infórmese de los nuevos ataques lo antes posible. Instale inmediatamente todos los parches y actualizaciones de seguridad.

Vigile a los vigilantes

Audite sus propios procesos. Con regularidad.

> La seguridad es un proceso, no un producto. Los productos proporcionan cierta protección, pero la única manera de hacer negocios eficazmente en un mundo inseguro es poner en marcha procesos que reconozcan la inseguridad inherente a los productos. El truco está en reducir el riesgo de exposición independientemente de los productos o parches.
>
> Traducción parcial del blog de Bruce Schneier publicado en el mes de abril de 2020

---

https://twitter.com/schneierblog/status/1722250129863004367