Seguridad de la seguridad
un método empírico

I. Rossenbach
iro@cryptosec.org
Twitter @secucrypt

Buenos Aires, 03.11.2017

contexto

>= 128 bits !

pentest your apps !

2FA !

Patch, patch, patch !

…

contexto

objeto del estudio

> establecer un método para tomar decisiones fiables en el ámbito de la seguridad

> en particular en el dominio de la gestión de crisis o de incidentes mayores

definiciones

Seguridad?

> situación objetiva que se caracteriza por la existencia de riesgos, pero que están **dominados**

> la seguridad siempre es un **proceso**: involucra al individuo y a la organización, y nunca únicamente una metodología, un sistema, una técnica o un producto.

Qué fiabilidad?

En la mayoría de los casos, se apoyan sobre datos de leve fiabilidad:

> el asesoramiento de expertos

> de proveedores de soluciones

> la evaluación comparativa - la comparación con otras organizaciones similares (*benchmarking*)

decisiones de seguridad

¿cómo aumentar la fiabilidad de las decisiones?

¿cómo evaluar los riesgos?

¿cómo tomar decisiones acerca de los riesgos?

¿cómo reducir los riesgos de un sistema complejo a un costo razonable?

¿cómo decidir si se debe reducir o evitar los riesgos?

¿cómo organizar la reacción a la materialización de un riesgo?

modelizar la seguridad?

La imposibilidad o dificultad de establecer modelos deterministas para gestionar los riesgos tiene como consecuencia que esta actividad dependa mucho de las **decisiones humanas**

… la racionalidad del pensamiento humano y de los comportamientos colectivos es limitada y **no se puede modelizar**

Pero existe una importante cantidad de conocimiento acerca de:

> la psicología

> estudios sobre el *management* y las organizaciones

> estudio de casos de incidentes ataques, desastres y de la manera en que los humanos han reaccionado

problematica

Nos encontramos en una situación en la que tenemos que hacer frente a fenómenos **poco o nada modelizados**, usando nuestros cerebros y nuestras organizaciones cuyos funcionamientos son a menudo **erráticos**

una analogía fructífera

Open Web Application Security Project (OWASP) cuyo trabajo es de libre acceso, y cuya misión es construir y proponer recomendaciones, métodos y herramientas para mejorar la seguridad de las aplicaciones web

Ejemplo: Top 10 2013-A1-Injection

[…]

http://example.com/app/accountView?id=' or '1'='1

una analogía fructífera

OWASP no es el resultado de “buenas prácticas” o la opinión de expertos (como las normas ISO)

> análisis de cientos de miles de vulnerabilidades **efectivamente** descubiertas entre miles de clientes

Otro *framework* de seguridad similar:

CIS Critical Security Controls for Effective Cyber Defense (CIS CSC)

una analogía fructífera

OWASP y CIS CSC se materializan en *checklists*

El principio subyacente en ellas es que, dada la ausencia de modelos de seguridad deterministas, una clave para mejorar la seguridad de un sistema o de una aplicación es procurar que las vulnerabilidades **más peligrosas y comunes sean evitadas**

Una analogía fructífera

Por analogía, intentaremos establecer una lista de **errores comúnmente** cometidos en la toma de decisiones, y a continuación la confrontaremos al dominio de la toma de decisiones en situación de crisis

Ejemplo de problema de decisión en tiempos de crisis:

– dificultades de la jerarquía para distanciarse de las acciones técnicas, dificultades de los técnicos para despojarse de los reflejos diarios

Ejemplo de problema de decisión en tiempos de crisis:

– ocurre que se decida medidas técnicas que no tienen ninguna posibilidad de resolver los problemas (como reiniciar un servidor), sólo para que no se pueda criticar ulteriormente el hecho de no haberlo intentado

Ejemplo de problema de decisión en tiempos de crisis:

– a veces las células de crisis comenzaron a ordenar acciones precisas, en lugar de elegir entre las opciones propuestas por los técnicos y los expertos

problemas de decisión

Ejemplo de problema de decisión en tiempos de crisis:

– a menudo, las células de crisis en las que participan responsables de la organización, solicitan demasiado a los técnicos encargados de la resolución de la crisis. De esto resulta a menudo una tensión desfavorable en contra del trabajo eficiente

9 categorías de problemas en el estudio

riesgos humanos

Ejemplos de factores de riesgos humanos:

-Racionalidad limitada
-Sesgo de confirmación
-Órdenes contradictorias
-*Groupthink*
-Errores de razonamiento
-Soluciones preferidas
[…]

22 en el estudio

Racionalidad limitada: Los individuos y los grupos tienen **la intención de ser racionales**, pero debido a sus capacidades cognitivas limitadas, lo logran **parcialmente**. Para compensar esta debilidad, las organizaciones a menudo piensan racionalizar sus decisiones mediante el uso de números

Sesgo de confirmación: **Tendencia a favorecer la información y las ideas conocidas o aceptadas**, ignorando, rechazando o desvalorizando aquellos datos que **las contradicen**. Buscamos confirmar nuestras ideas, en lugar de cuestionarlas

Órdenes contradictorias: Ejemplos de estas directivas contradictorias: Por un lado aumentar el *reporting* y por el otro exigir autonomía

Groupthink: **Fenómeno de grupo mediante el cual el deseo de armonía y de conformidad** perturba o quita racionalidad a los procesos de decisión. Los miembros del grupo tratan de **minimizar los conflictos** y llegan rápidamente a decisiones por consenso sin un **análisis crítico de las alternativas**, y aislándose de las influencias externas.

Errores de razonamiento: Si A, entonces B. B. Entonces A (malware DNS 8.8.8.8)

Ilusión de causalidad, donde sólo hay correlación

Soluciones preferidas

Ciertas opciones son preferidas por los individuos u organizaciones. Se trata de aquéllas que son o parecen: – **Obvias**, de “sentido común” (entendido como la expresión de la ideología dominante); – **Irresistibles**, a causa del *hubris*, o porque son soluciones dominantes o prometen beneficios o éxitos excepcionales; – **Prácticas**, es decir, que evitan considerar otras; – **Disponibles**, validadas o experimentadas por otros; – **Fáciles de justificar**.

transformación en preguntas

Racionalidad limitada

¿Estamos dispuestos y preparados para decidir sin contar con todas las informaciones (lo que equivale a asumir que las decisiones no serán del todo racionales)?

transformación en preguntas

Órdenes contradictorias

Durante la gestión de la crisis, ¿hay pedidos u órdenes contradictorios (por ejemplo, exigir que los técnicos propongan soluciones y que a la vez tengan en cuenta las instrucciones técnicas de la jerarquía)?

transformación en preguntas

Soluciones preferidas

¿Hay opciones para salir de la crisis que se consideran preferentemente porque parecen “obvias”, “irresistibles”, “prácticas”, “disponibles” o “fácilmente justificables”?

¿Hay decisiones técnicas que sólo se deciden por miedo a que se critique posteriormente el no haberlas tomado?

transformación en preguntas

Groupthink

¿Ha surgido un consenso rápidamente?

¿Existieron alternativas viables descartadas demasiado rápido?

¿Es el grupo muy homogéneo (funciones, experiencia, personalidad)?

¿La jerarquía o el líder expresan una fuerte preferencia hacia ciertas opciones?

ejemplo de aplicación

La pregunta:

¿La jerarquía o el líder expresan una fuerte preferencia hacia ciertas opciones?

[*groupthink*]

Puede revelar un problema de dificultad de la jerarquía para distanciarse de las acciones técnicas

ejemplo de aplicación

La pregunta:

¿hay pedidos u órdenes contradictorios (por ejemplo, exigir que los técnicos propongan soluciones y que a la vez tengan en cuenta las instrucciones técnicas de la jerarquía)?

[órdenes contradictorias]

Puede revelar el problema de una célula de crisis en las que participan responsables de la organización, solicitan demasiado a los técnicos encargados de la resolución de la crisis

ejemplo de aplicación

La pregunta:

¿Hay decisiones técnicas que sólo se deciden por miedo a que se critique posteriormente el no haberlas tomado?

[soluciones preferidas]

Puede revelar el problema de medidas técnicas que no tienen ninguna posibilidad de resolver los problemas (como reiniciar un servidor)

conclusión

El ejercicio de confrontación de los problemas observados con las preguntas identificadas sugiere cierta relevancia

Sin embargo, este cuestionario no puede pretender ser exhaustivo

Como las metodologías OWASP o CIS CSC mencionadas anteriormente, hay que considerarlo como un tamiz

conclusión

A su vez, y al igual que los métodos citados, la presente metodología irá aumentando su eficacia al ser **pulida por la confrontación con la realidad**

Practicarla permitirá afinar preguntas, descartar otras o añadir categorías importantes de riesgos humanos

conclusión

Una profundización del método deberá detallar los aspectos **temporales**:

> ¿cómo determinar el momento adecuado para tomar una decisión de seguridad?

> ¿cómo evitar que las precauciones tomadas – para evitar malas decisiones – no terminen retrasando demasiado el proceso de decisión?

y desarrollar una **herramienta** para facilitar el uso de la metodología

conclusión

El principal interés del método es **plantear preguntas**. Incentivar a la reflexión. Alentar dudas. Incumbe a aquéllos que lo utilizan la responsabilidad de **imaginar respuestas** apropiadas a su propio contexto

Así planteado, este método no es una herramienta de ayuda a la toma de buenas decisiones de seguridad, sino más bien una **herramienta de ayuda para no tomar malas decisiones**

Gracias!

Preguntas?

I. Rossenbach
iro@cryptosec.org
Twitter @secucrypt