PROTECCIÓN DE MARCA
Reputación… ¿digital?

Antonio Villalón

Director de Seguridad

S2 Grupo

Índice

- Introducción: la reputación como activo crítico.
- Seguridad semántica.
- ¿Cómo protegernos?
  - Prevención.
  - Detección.
  - Respuesta.
- Reputación personal.
- Conclusiones.

Marca y reputación

- **Reputación:** Prestigio o estima en que son tenidos alguien o algo (de DRAE).
- **Reputación online**: reflejo del prestigio o estima de una persona o marca en Internet (de WikiPedia).
- La **marca** se puede generar a través de medios publicitarios, pero la reputación (digital o no) **no** depende en exclusiva de nosotros.
- Problema clásico: "¿qué dirán?".
- Problema actual: "¿qué dirán?"…en Internet.
  - $PA = (PC)^n$

Reputación: el problema actual

- Autoría.
  - ¿Quién puede opinar?
  - Anonimato.
- Alcance.
  - ¿A cuánta gente le llega el mensaje?
- Cantidad.
  - ¿Cuánta información existe?
- Calidad.
  - ¿Quién verifica que es cierto lo que se dice?

Reputación… ¿digital?

- Con frecuencia decimos que trabajamos por confianza.
  - Y buena parte de la confianza se basa en la reputación.
- Si alguien degrada mi reputación (digital o no), daña a la confianza de terceros en mí…
- …y garantizar nuestra reputación no siempre depende exclusivamente de nosotros.
  - *"No basta que la mujer del César sea honesta; también tiene que parecerlo."*
- ¿Qué hacer?
  - Ser honesto.
  - Parecerlo.
- ORM (*Online Reputation Management*).

La reputación como activo crítico

- **Activo:** Cualquier bien que tiene valor para la organización (ISO/IEC 13335-1:2004).
  - Soportes, funcionalidades, personas, software, hardware, suministros, ubicaciones, marca, **reputación**…

- Debo proteger mis activos de forma **correcta** y **completa**: Análisis y gestión de riesgos.
  - Amenazas, impactos, probabilidades…
  - *Risk appetite*.
  - Selección de controles.
  - Auditoría.
  - Bla, bla, bla…

Ataques a la reputación

- Bruce Schneier (a partir de estudios de Martin C. Libicki) diferenciaba hace años tres tipos de ataques: físicos, sintácticos y **semánticos**.
  - Yo no estoy de acuerdo, pero no soy Bruce Schneier ☹
- Consideremos ataques sintácticos y semánticos (tanto físicos como lógicos, organizativos…) a nuestra reputación.
  - Como a cualquier otro activo.
- Protección ante ataques **sintácticos**: todos la conocemos (o deberíamos).
  - Parches, cortafuegos, análisis de vulnerabilidades…
- Protección ante ataques semánticos: ¿y ahora qué?

Seguridad semántica

- Ataques semánticos: se focalizan en la forma en que nosotros, los humanos, damos significado a un contenido.
  - Atacan a la interpretación de la información.
- No es nada nuevo…
  - Leyendas urbanas, *hoaxes*…
- …pero con el uso masivo de Internet su impacto se puede multiplicar.
- Más difíciles de controlar que los ataques sintácticos… y muchas veces más dañinos.
  - *"Only amateurs attack machines; professionals target people".*

Bruce Schneier

Un ejemplo convergente

Situación: Ataque a unos grandes almacenes.

- Visión sintáctica:
  - DDoS, alteraciones de datos, etc.
  - Ataques relativamente complejos.
  - Probabilidad de éxito baja (creo).
- Visión semántica:
  - *El terrorista agradecido.*
  - Ataque simple.
  - Probabilidad de éxito alta (las personas somos así).

¿Cómo protegernos? PREVENCIÓN

- Bloqueo de fuentes.
  - Evito que la información indebida llegue al usuario.
- Valoración de fuentes.
  - Asocio a cada fuente un nivel de reputación para que el usuario juzgue la calidad de la información recibida.
- Canalización de fuentes.
  - Identifico exhaustivamente las fuentes de información válidas… y las controlo.
  - Caso particular de la valoración.
- Contrainformación.
  - Generación de contenidos, posicionamiento correcto, información positiva…
- FORMACIÓN E INFORMACIÓN.

Como siempre, la prevención es necesaria pero no suficiente.

¿Cómo protegernos? DETECCIÓN

- La **monitorización en tiempo real** es un aspecto clave para garantizar nuestra reputación en el tiempo.
- ¿Qué podemos monitorizar?
  - Análisis de contenidos sensibles (datos y metadatos).
  - Control de enlaces referenciados.
  - Abuso del correo electrónico corporativo.
  - Uso o abuso de material e imagen.
  - Información difamatoria.
  - Circulación de *hoaxes*, *phishings*...
  - Registros nocivos.
  - …
- Problema habitual: monitorización del contenido multimedia.
  - Aparte: velocidad del cambio, nuevos *sites*, etc.

¿Cómo protegernos? RESPUESTA

- Limitación.
  - Contraposición de información.
  - ¿Silencio?
- Neutralización.
  - Ataque a la reputación del atacante para degradar su credibilidad.
- Bloqueo.
  - Evito el acceso a información negativa.

Una buena prevención es básica para ofrecer una respuesta adecuada.

  - Generación de contenidos positivos, participación en foros, etc.

Reputación personal

- Hemos hablado de la reputación corporativa pero… ¿y la personal?
  - También es un "activo" para nosotros y nuestras organizaciones…
- Problema clásico: VIP.
- Problema actual: VIP + NIP.
- Contenido propio vs. Contenido impropio.
- ¿Qué dice la red de mí?
  - "Internet no olvida"
- Ciberdetectives, rastreo de redes, *CV screening*…
- Esta noche teclead en Google vuestro nombre…☺
  - …y si tenéis más tiempo, usad herramientas *ad hoc*, como Maltego.

Conclusiones

- Nuestra marca, imagen… en definitiva, nuestra reputación, puede ser objeto de ataques.
- Debo ser honesto… y parecerlo.
- Necesitamos por un lado garantizar la seguridad sintáctica de nuestros activos, incluyendo los reputacionales…
- …y por otro su seguridad semántica.
  - Más complicado: percepciones que en muchos casos no dependen de nosotros.
- ¿Estoy protegiendo adecuadamente mi reputación –o el resto de activos- desde ambos puntos de vista?

S2 GRUPO

ISACA®
Sistemas de información fiables y valiosos
Valencia Chapter

GRACIAS POR SU ATENCIÓN

ISACA® Serving IT Governance Professionals

IT Governance Institute®

COBIT®

CISA® Certified Information Systems Auditor™

CISM® Certified Information Security Manager®

CGEIT™ Certified in the Governance of Enterprise IT™