

Aproximaciones a la gestión de vulnerabilidades

Javier Zubieta Moreno

Business Development Manager

jzubieta@unitronics.es

“Que resuelven los problemas de negocio de nuestros Clientes”



Introducción a las vulnerabilidades

- Por vulnerabilidad entendemos una **debilidad conocida** en un componente de TI cuyo aprovechamiento de manera intencionada **puede reportar beneficios económicos** a un atacante o **pérdidas económicas** a la organización que lo sufre
- Las vulnerabilidades se **publican** en medios de difusión masiva donde se exponen los síntomas de la **existencia** de la vulnerabilidad así como la manera de **remediarla**
- Muchos de los problemas serios de seguridad de las organizaciones se deben a vulnerabilidades **conocidas de antemano** así como su remedio
- En el 2007 se reportaron oficialmente **7.236** vulnerabilidades y **39.490** en los últimos 12 años (fuente US-CERT, junio 2008)



Ejemplo de anuncio de vulnerabilidades

CCN-CERT
Equipo de Respuesta ante Incidentes de Seguridad Informática del CCN

Boletines de Vulnerabilidades

Desbordamiento de búfer en AIX uucp

Clasificación de la vulnerabilidad

Propiedad	Valor
Riesgo	Alto
Nivel de Confianza	Oficial
Impacto	Compromiso Root
Dificultad	Experto
Requerimientos del atacante	Acceso remoto con cuenta

Información sobre el sistema

Propiedad	Valor
Plataforma afectada	UNIX
Software afectado	AIX 5.2 AIX 5.3

Descripción

Se ha encontrado una vulnerabilidad del tipo desbordamiento de búfer en el comando uucp. La vulnerabilidad reside en un error no especificado.

Un atacante local podría ejecutar código arbitrario con privilegios de root.

Solución

Actualización de software

IBM (3851)
AIX 5.2.0 - APAR IY97215
AIX 5.3.0 - APAR IY95852
<http://www.ibm.com/servers/eserver/support/unixservers/aixfixes.html>

Logo: **FIRST** Improving Security Together MEMBER

Logo: **Listed by TRUSTED Introducer The European CSIRT Directory**

Por qué es importante para Banca y Seguros

- **Porque es un sector fuertemente regulado y en materia de seguridad no solo hay que ser bueno sino también parecerlo**
 - PCI-DSS lo exige
- **Porque las consecuencias de un aprovechamiento de una vulnerabilidad pueden ser peores que en otros sectores (pérdida de imagen, cuando no es de dinero)**
- **Porque el sector financiero siempre ha estado a la cabeza en inversiones e implantaciones en materia de seguridad**
- **Y, en general, porque más vale prevenir que curar, ¿verdad?**



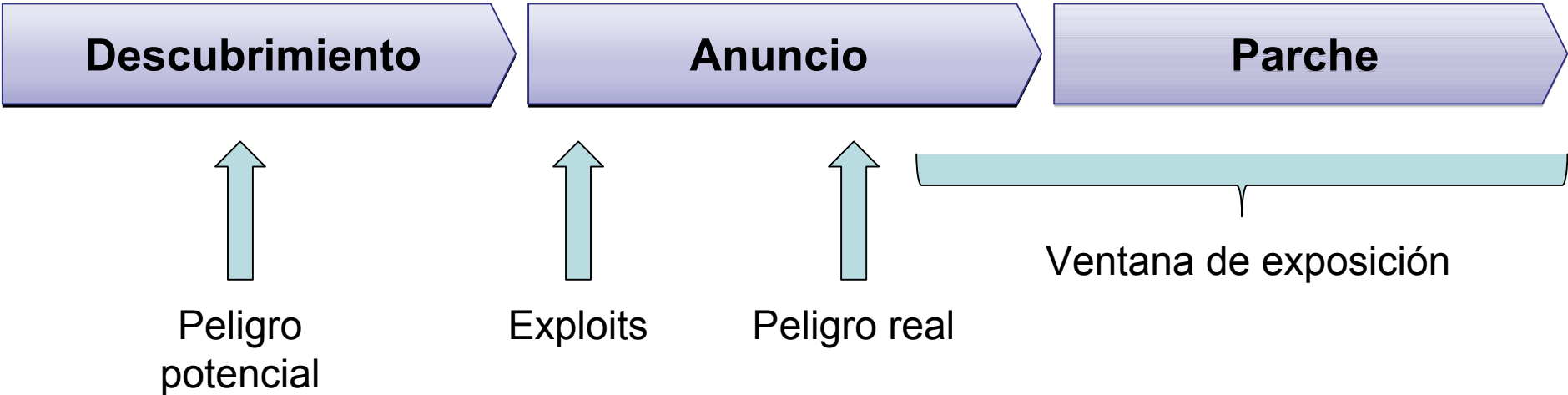
Gestión de vulnerabilidades

El correcto **tratamiento** de una vulnerabilidad de seguridad a lo largo de su ciclo de vida pudiendo, así:

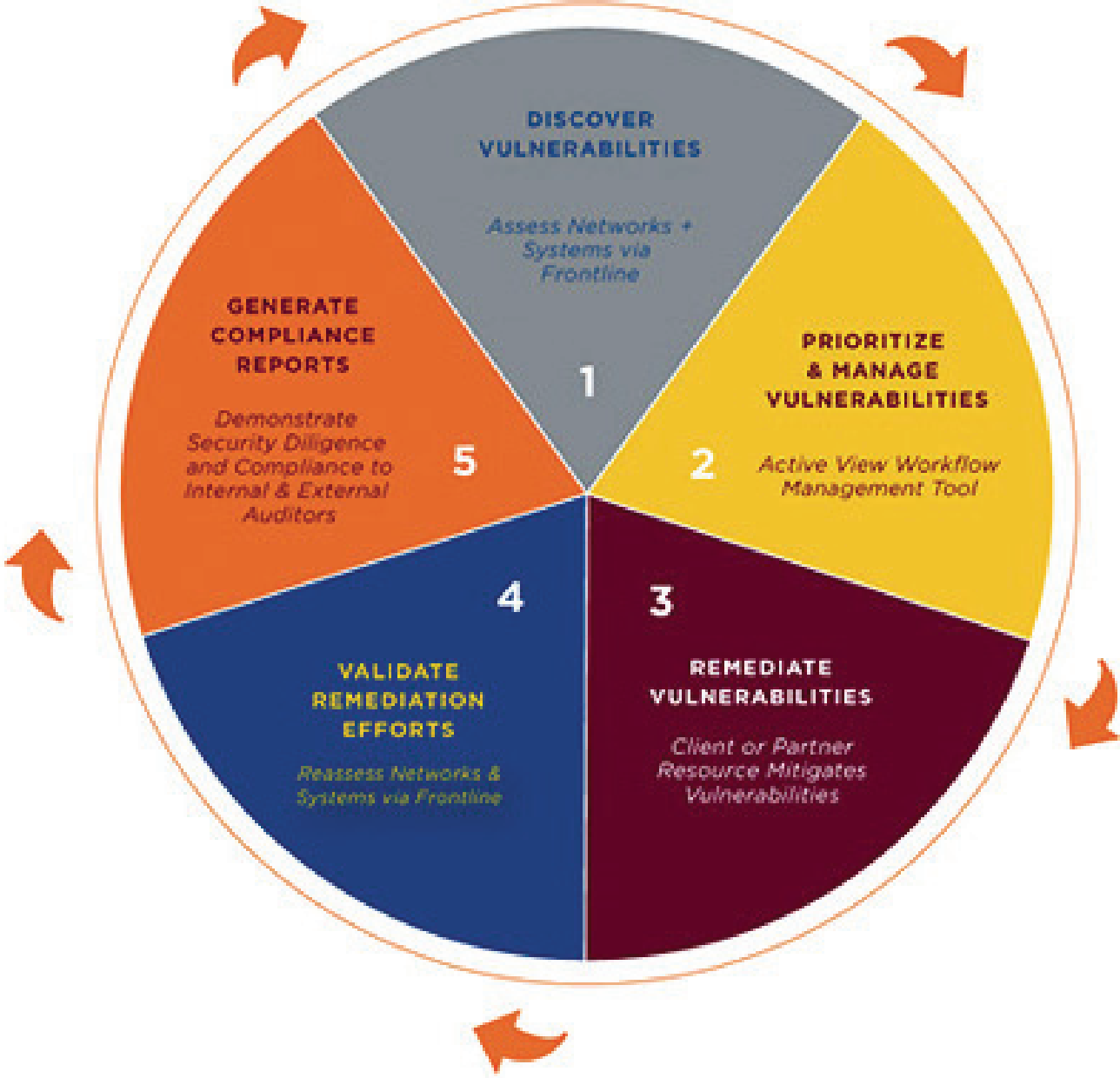
1. **Minimizar el nivel de riesgo** de la organización **reduciendo** al máximo la ventana de exposición a vulnerabilidades
2. Evitar pérdidas económicas derivadas de una incidencia potencial de la cual **se sabe su resolución de antemano**
3. Elevar la eficiencia y la eficacia de la gestión operativa de la seguridad en su conjunto, predominando las actividades **preventivas** sobre las **reactivas**
4. Tener una **visión** más nítida sobre la actividad real de seguridad en la organización y complementar las estadísticas e informes corporativos al respecto



Ciclo de vida de una vulnerabilidad



Gestión completa de vulnerabilidades



Opciones para abordarlo

Consultoría hacking ético

- Análisis exhaustivo, basado en conocimiento del consultor
- Se planifica
- Sus resultados constituyen un plan de acción de mejora global

Servicio gestionado

- Análisis rápidos y dirigidos, basado en servicio
- Se puede disparar en cualquier momento
- Sus resultados pueden alimentar un servicio de gestión operativa



Pros y Contras

Consultoría hacking ético

- El análisis es muy completo, aunque se alarga en el tiempo
- Tiene entidad propia, pero puede convertirse en un “ente aislado”
- Sus resultados se pueden presentar a un auditor, aunque el plan de mejora se puede quedar en el olvido

Servicio gestionado

- El análisis es rápido pero no exhaustivo
- No es necesario planificarlo pero debería formar parte de un servicio más general
- Sus resultados pueden alimentar otros servicios, pero pueden tener bastante carga técnica

En general, son dos aproximaciones muy diferentes y se recomienda inicialmente hacer una consultoría y darle continuidad con el servicio gestionado

www.unitronics.es

