Gerenciamento de Vulnerabilidades

CI1007

André Grégio
gregio@inf.ufpr.br

DInf/UFPR

2 de abril de 2024

Terminologia

Bug

- Um problema de *software* que **pode existir** no código-fonte, **mas nunca ser executado**;
- Problemas no nível da implementação podem ser facilmente encontrados por ferramentas de revisão de código (ex.: RATS[1], Splint[2], FindBugs[3], FlawFinder[4]);
- Exemplo de *bug*: *buffer overflow*.

[1] `https://code.google.com/p/rough-auditing-tool-for-security/`
[2] `http://www.splint.org/`
[3] `findbugs.sourceforge.net`
[4] `http://www.dwheeler.com/flawfinder/`

Terminologia

Falha

- Problema de *software* em nível mais profundo do que um *bug*;

Terminologia

Falha

- Problema de *software* em nível mais profundo do que um *bug*;
- É instanciada no código, mas pode existir no projeto;

Terminologia

Falha

- Problema de *software* em nível mais profundo do que um *bug*;
- É instanciada no código, mas pode existir no projeto;
- Ex.: tratamento de erros que se propagam por várias funções ou módulos de um código, ataques de *cross-site scripting* (XSS), etc.

Terminologia

Vulnerabilidade

- Um *bug* ou falha explorável por atacantes;

Terminologia

Vulnerabilidade

- Um *bug* ou falha explorável por atacantes;
- Varia de:
  - erros na implementação local (uso da função `gets()` em C);

Terminologia

Vulnerabilidade

- Um *bug* ou falha explorável por atacantes;
- Varia de:
  - erros na implementação local (uso da função `gets()` em C);
  - erros na interface de interação entre processos (*Time of Check, Time of Use* - TOCTOU);

Terminologia

Vulnerabilidade

- Um *bug* ou falha explorável por atacantes;
- Varia de:
  - erros na implementação local (uso da função `gets()` em C);
  - erros na interface de interação entre processos (*Time of Check, Time of Use* - TOCTOU);
  - equívocos no nível do projeto (falhas não graciosas que levem a situações inseguras, por ex., servidor Web ao ser invadido permite a execução de comandos arbitrários com privilégio de administrador).

Terminologia

Vulnerabilidade

- Um *bug* ou falha explorável por atacantes;
- Varia de:
  - erros na implementação local (uso da função `gets()` em C);
  - erros na interface de interação entre processos (*Time of Check, Time of Use* - TOCTOU);
  - equívocos no nível do projeto (falhas não graciosas que levem a situações inseguras, por ex., servidor Web ao ser invadido permite a execução de comandos arbitrários com privilégio de administrador).
- Problema grave: *0-day exploits*!

Terminologia

Vulnerabilidades no Projeto

- Difíceis de encontrar, complexas para explorar, porém mais arriscadas para o programa cujo projeto é vulnerável $\rightarrow$ pode não ser possível aplicar um *patch*!

Terminologia

Vulnerabilidades no Projeto

- Difíceis de encontrar, complexas para explorar, porém mais arriscadas para o programa cujo projeto é vulnerável → pode não ser possível aplicar um *patch*!
- Incluem:
  - compartilhamento de objetos/recursos (ex.: regiões de memória);

Terminologia

Vulnerabilidades no Projeto

- Difíceis de encontrar, complexas para explorar, porém mais arriscadas para o programa cujo projeto é vulnerável → pode não ser possível aplicar um *patch*!
- Incluem:
  - compartilhamento de objetos/recursos (ex.: regiões de memória);
  - problemas de confiança/autenticação/autorização;

Terminologia

Vulnerabilidades no Projeto

- Difíceis de encontrar, complexas para explorar, porém mais arriscadas para o programa cujo projeto é vulnerável $\rightarrow$ pode não ser possível aplicar um *patch*!
- Incluem:
  - compartilhamento de objetos/recursos (ex.: regiões de memória);
  - problemas de confiança/autenticação/autorização;
  - propagação de exceções, etc.

Definição

Gerenciamento de Vulnerabilidades - *Vulnerability Assessment*

- Processo para identificar, quantificar e priorizar as vulnerabilidades em um sistema.

Definição

Gerenciamento de Vulnerabilidades - *Vulnerability Assessment*

- Processo para identificar, quantificar e priorizar as vulnerabilidades em um sistema.
- Realizados de acordo com alguns passos:
  1. Catalogação de bens e recursos em um sistema.
  2. Atribuição de ordem/valor/importância a cada recurso.
  3. Identificação de vulnerabilidades ou ameaças em potencial ao recurso.
  4. Mitigação ou eliminação das vulnerabilidades mais graves presentes nos recursos mais importantes.

Gerenciamento de Vulnerabilidades vs. Análise de Risco

Análise de Risco

- Objetivo é investigar os riscos associados a algum "objeto", seu projeto e operações.

Gerenciamento de Vulnerabilidades vs. Análise de Risco

Análise de Risco

- Objetivo é investigar os riscos associados a algum "objeto", seu projeto e operações.
- O foco é nas causas e consequências diretas para o objeto em questão.

Gerenciamento de Vulnerabilidades vs. Análise de Risco

Análise de Risco

- Objetivo é investigar os riscos associados a algum "objeto", seu projeto e operações.
- O foco é nas causas e consequências diretas para o objeto em questão.
- Ex.: Risco → vazamento de informações sensíveis;
  Possível causa → não implementação de políticas e controles;
  Consequência direta → perda de confidencialidade por exposição.

Gerenciamento de Vulnerabilidades vs. Análise de Risco

Análise de Risco

- Objetivo é investigar os riscos associados a algum "objeto", seu projeto e operações.
- O foco é nas causas e consequências diretas para o objeto em questão.
- Ex.: Risco $\rightarrow$ vazamento de informações sensíveis;
  Possível causa $\rightarrow$ não implementação de políticas e controles;
  Consequência direta $\rightarrow$ perda de confidencialidade por exposição.

Gerenciamento de Vulnerabilidades

- O foco é nas consequências para o "objeto" e nas consequências primárias e secundárias para o ambiente associado ao objeto em questão.

Gerenciamento de Vulnerabilidades vs. Análise de Risco

Análise de Risco

- Objetivo é investigar os riscos associados a algum "objeto", seu projeto e operações.
- O foco é nas causas e consequências diretas para o objeto em questão.
- Ex.: Risco $\rightarrow$ vazamento de informações sensíveis;
  Possível causa $\rightarrow$ não implementação de políticas e controles;
  Consequência direta $\rightarrow$ perda de confidencialidade por exposição.

Gerenciamento de Vulnerabilidades

- O foco é nas consequências para o "objeto" e nas consequências primárias e secundárias para o ambiente associado ao objeto em questão.
- Lida com as possibilidades de redução de tais consequências e de melhoria na capacidade de gerenciar incidentes futuros.

Gerenciamento de Vulnerabilidades vs. Análise de Risco

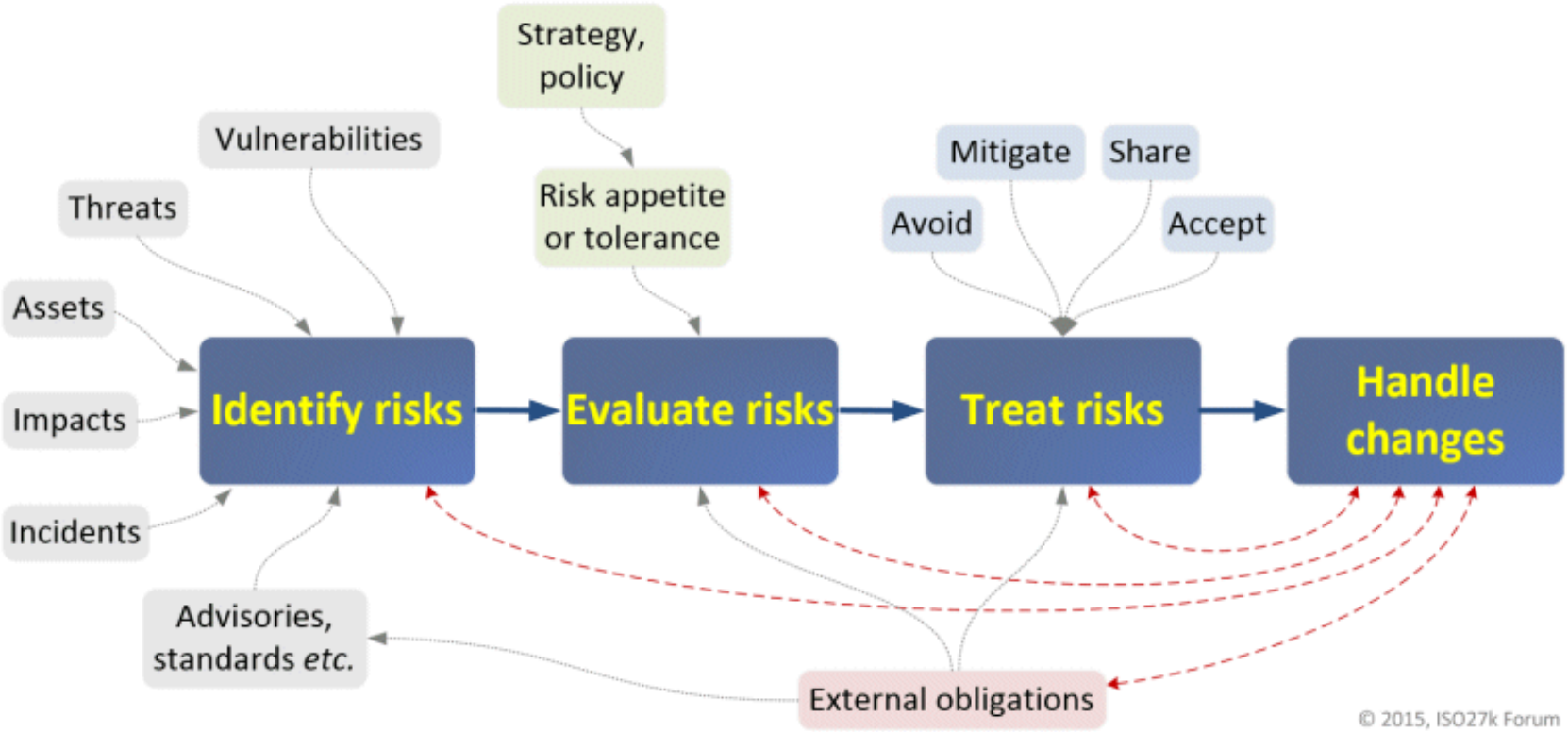
Análise de Risco

- Objetivo é investigar os riscos associados a algum "objeto", seu projeto e operações.
- O foco é nas causas e consequências diretas para o objeto em questão.
- Ex.: Risco → vazamento de informações sensíveis;
  Possível causa → não implementação de políticas e controles;
  Consequência direta → perda de confidencialidade por exposição.

Gerenciamento de Vulnerabilidades

- O foco é nas consequências para o "objeto" e nas consequências primárias e secundárias para o ambiente associado ao objeto em questão.
- Lida com as possibilidades de redução de tais consequências e de melhoria na capacidade de gerenciar incidentes futuros.
- Ex.: Servidor de documentos interno mal configurado permite acesso externo não autenticado devido a falta de atualização do SO/aplicação.

Ciclo do Gerenciamento de Riscos



Fonte: `http://www.iso27001security.com/html/risk_mgmt.html`

Conformidade

Padrões

- ISO 27001:
  - Padrão para gerenciamento da informação "genérico", isto é, não orientado a tecnologias ou fabricantes.
- ISO 27002:
  - Melhores práticas recomendadas para selecionar e implementar um sistema de gerenciamento da segurança da informação efetivo.
- ISO 27005:
  - Guia para gerenciamento de risco (levantamento, tratamento e mitigação).

Conformidade

Justificativa

- Estabelecimento de conjunto de processos:
  - Implantação de **Governança de TI**.
- Criação e aplicação de políticas de segurança:
  - Uso aceitável;
  - Senhas;
  - Acesso físico (auxilia no gerenciamento de riscos);
  - Acesso à rede (auxilia na implementação do *firewall*);
  - Manutenção da segurança de sistemas (auxilia no gerenciamento das vulnerabilidades).
- Revisão/validação de processos:
  - Engenharia social, varredura e enumeração, *pentesting* (requer apenas uma brecha!).

Sobre Segurança e Processos

O que é segurança?

- Processo para prevenção e detecção de violações ou uso não autorizado de um recurso computacional[1].
- Escopo inclui redes e dispositivos (incluindo disp. móveis), sistemas de informação e programas/aplicações.

[1] Adaptado de: `https://www.us-cert.gov/Home-Network-Security`

Sobre Segurança e Processos

O que é segurança?

- Processo para prevenção e detecção de violações ou uso não autorizado de um recurso computacional[1].
- Escopo inclui redes e dispositivos (incluindo disp. móveis), sistemas de informação e programas/aplicações.

[1] Adaptado de: `https://www.us-cert.gov/Home-Network-Security`

Segurança é um processo, não um produto!

– Bruce Schneier

Contato

E-mail

- gregio@inf.ufpr.br