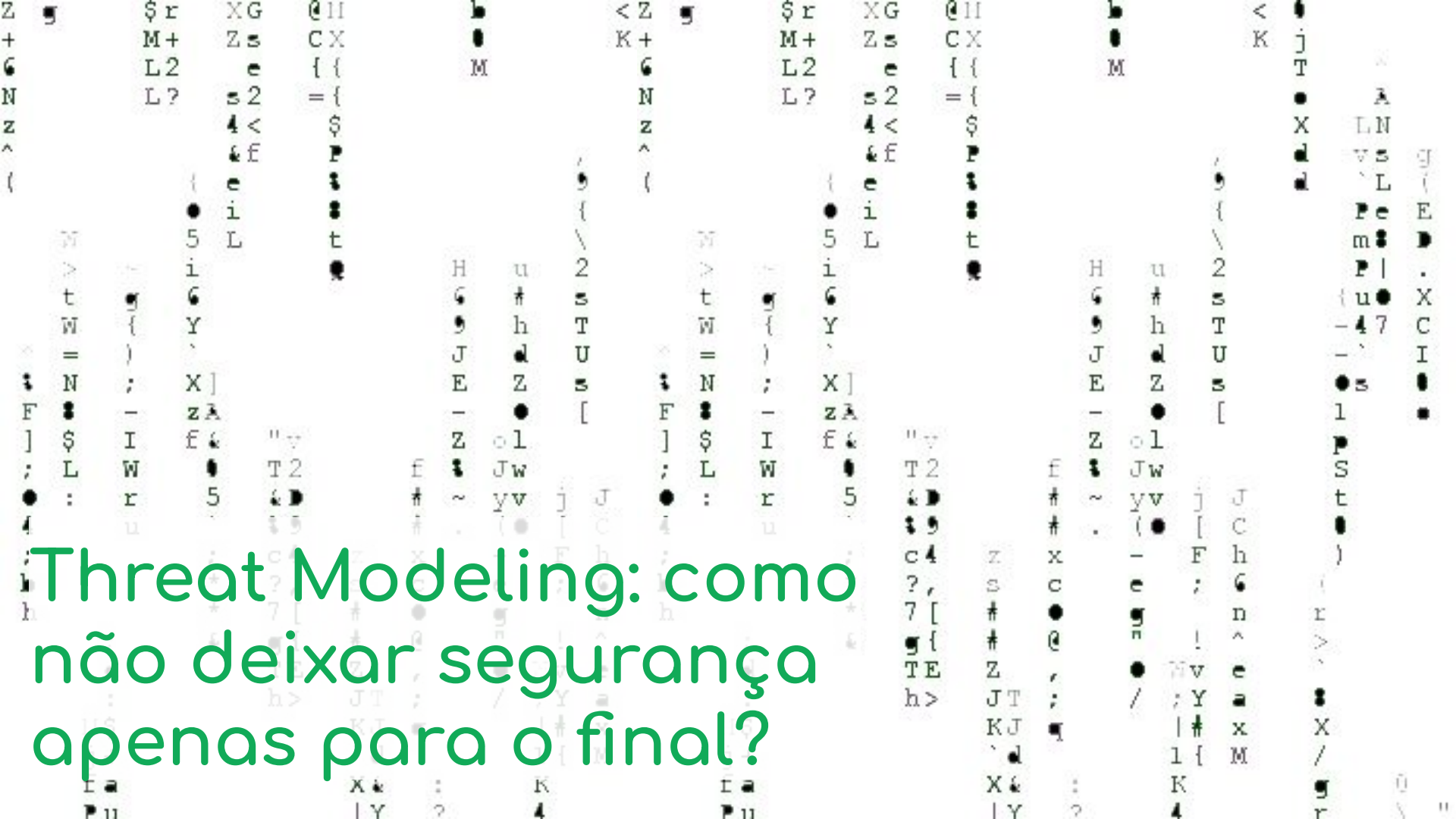
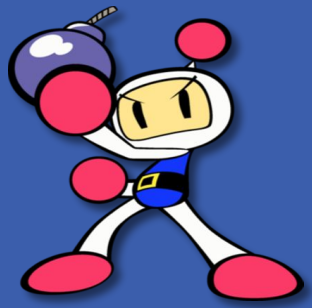


Threat Modeling: como não deixar segurança apenas para o final?

ThoughtWorks®

ThoughtWorks: Consultor Desenvolvedor
Made in: Salvador
Twitter: Ruanvictor_
Mais sobre: ruanvictor.dev

Ruan Victor

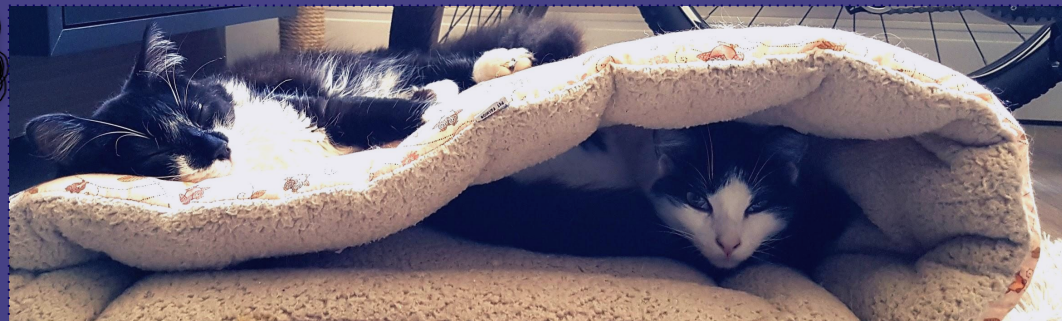


ThoughtWorks®

ThoughtWorks: Consultora Desenvolvedora
Made in: Brasília
Twitter: ThaiiBraga
Mais sobre: thaiane.github.io

Thaiane Braga

AFR@PYTHON



Por que falar disso?

REINO UNIDO

12/05/2017

Serviço Nacional de Saúde britânico alvo de um ciberataque esta sexta-feira

Os nossos jornalistas estão a acompanhar a notícia que será atualizada sempre que se justifique

Impacto

POR PAULA ZOGBI - EM NEGOCIOS / GRANDES-EMPRESAS - 03 ABR, 2018 13H53

Hackers roubam dados de cartão de crédito de 5 milhões de pessoas

Vítimas foram clientes das lojas Saks Fifth Avenue e Lord & Taylor, nos Estados Unidos

MUNDO

Ataque cibernético à escala global: Governos e multinacionais afetados

Ransomware WannaCry já infectou 200 mil computadores em 150 países

Um registro de domínio interrompeu acidentalmente uma (e apenas uma) das variantes do malware

REVISTA EXAME

Dados & Ideias — Na mira dos bandidos virtuais

29 mar 2018, 06h00

NEGÓCIOS

Risco de fraudes e vazamento de dados aumentou, diz pesquisa

25 mar 2018, 08h00

ATAQUES CIBERNÉTICOS ›

Vírus Petya é mais perigoso e mais sofisticado que WannaCry

Especialistas manifestam surpresa com últimos ataques, que não tentam roubar e vender informação

Norton Cybersecurity Insights Report
Global Comparisons

TOP FINDINGS	BRAZIL	GLOBAL (17 countries)
Amount consumers lost to cybercrime in the past year	**45 billion (BRL)**	$150 billion (USD)
Respondents who worry they will be a victim of online crime	**78%**	80%
Respondents who believe they're more likely to have their credit card details stolen while shopping online than their wallet	**60%**	62%
Consumers who feel completely in control over their online security	**20%**	15%
Consumers who would feel devastated if their personal financial information (bank and credit card details) was compromised	**85%**	81%
Respondents who think they're more likely to be bullied online than at school/work	Bullied Online. . . . . **57%** at School/Work **43%**	Bullied Online. . . . . 53% at School/Work 47%
Parents who worry their children will do something that makes the entire family vulnerable to online crime	**72%**	47%
Consumers who believe that dealing with the consequences of a stolen identity is more stressful than preparing for a presentation at work or sitting next to a screaming baby	Stolen Identity . . . . . **80%** Presentation at Work. . **47%** Screaming Baby. **69%**	Stolen Identity . . . . . 74% Presentation at Work. . 45% Screaming Baby. 54%

Over 1 Billion Consumers* Have Ever Been the Victim of a Cyber Crime; More Than 800 Million in the Last Year Alone

Global 16 Country Total: 1.2 billion ever 867.2 million in the last year

*In 16 countries

On Average, Past Year Cyber Crime Victims Spent 6 Hours Resolving Issues and Nearly 2 in 5 Were Impacted Financially*

Globally, those who experienced cyber crime in the past year spent an average of

6* hours resolving it

**Average has been trimmed to remove outliers*

Almost **1 in 3** needed a week or more to resolve the issue

Report losses or theft due to cyber crime*

Includes money lost or stolen, money that was stolen and returned, and money used to resolve the issue or repair/replace impacted device(s)

Como geralmente ocorre nos projetos?

Expectativa

!(Priorização de negócio)

Equipe separada

!(Responsabilidade compartilhada)

!(Fomentação de conhecimento de SI)

!(Conhecimento de SI aplicado no contexto)

Realidade

Segurança preventiva
!=
Apagar fogo


VAMOS FALAR DE COISA BOA!
VAMOS FALAR SOBRE COMO MINIMIZAR ISSO

Threat Modeling: modelagem de ameaças

Modelagem de Ameaças é...

... um **processo** pelo qual **ameaças potenciais**, como vulnerabilidades estruturais, podem ser **identificadas, enumeradas e priorizadas** - tudo do ponto de vista de um **invasor hipotético**. - Wikipedia

... trabalha para **identificar, comunicar** e **entender ameaças e mitigações** dentro do contexto de proteção de algo de valor.
- *OWASP*

Quem participa?

PESSOAS DESENVOLVEDORAS

- Visão técnica da aplicação
- Incentiva desenvolvimento seguro
- Fortalece conhecimento de vulnerabilidades
- Busca soluções técnicas e automatizadas

TIMES SEC, OPS, QA e outros

- Responsabilidade compartilhada
- Quebrar silos
- Visões diferentes
- Visão unificada das ameaças e mitigações

PESSOAS DA ÁREA DE NEGÓCIO

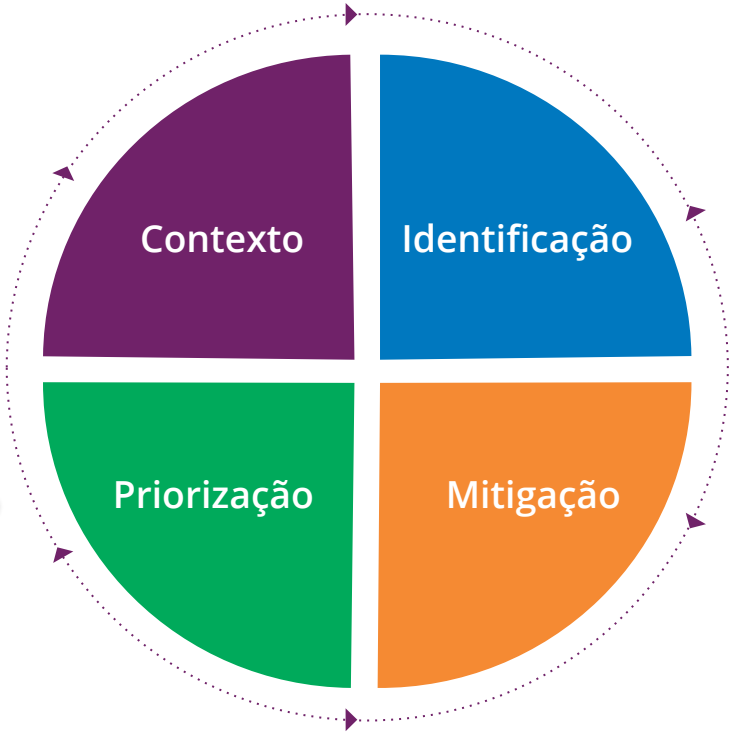
- Contexto do negócio
- Priorização do backlog
- Identificação dos riscos
- Melhora contínua do projeto

CLIENTES

- Transparência
- Fortalece a confiança
- Apoio na priorização
- Responsabilidade e riscos compartilhados

4 Questões

1 - O que estamos construindo?



2 - O que estamos fazendo errado?

4 - Quando faremos?

3 - O que faremos sobre isso?

Contexto

Esta etapa é destinada ao **entendimento** da aplicação ou solução, qual o ser **valor para o negócio** do cliente e qual o **aspecto de segurança mais importante.**

- Entender a função da aplicação, o fluxo dos dados na aplicação, as informações manipuladas
- Use diagramas (arquitetura, sequência, componentes e/ou desenhos)
- Dica: definir tema principal e *time-box*

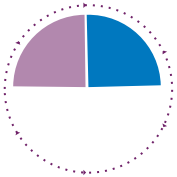
✓ Confidencialidade
✓ Integridade
✓ Disponibilidade
✓ Autenticidade
✓ Não repúdio

Identificação

Esta etapa é destinada a entender aquilo que pode acontecer de ruim com a app, quem pode causar isso e como pode causar isso.

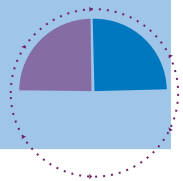
- Discuta com o time e liste os principais atores que podem nos atacar.

- Após identificar os possíveis atacantes discuta com o time e identifique de que forma elas podem concretizar os cenários definidos como nossos objetivos.
    - Top 10 OWASP
    - STRIDE



Identificação

Ameaça	Propriedade Violada	Definição
Spoofing	Autenticação	Representando algo ou outra pessoa
Tampering	Integridade	Modificando dados ou código
Repudiation	Não repúdio	Alegando não ter realizado uma ação.
Information Disclosure	Confidencialidade	Expondo informações para alguém que não tem autorização para ver
Denial of Service	Disponibilidade	Negar serviços ao usuário
Elevation of Privilege	Autorização	Obtenha capacidades de realizar ações sem a devida autorização



Mitigação

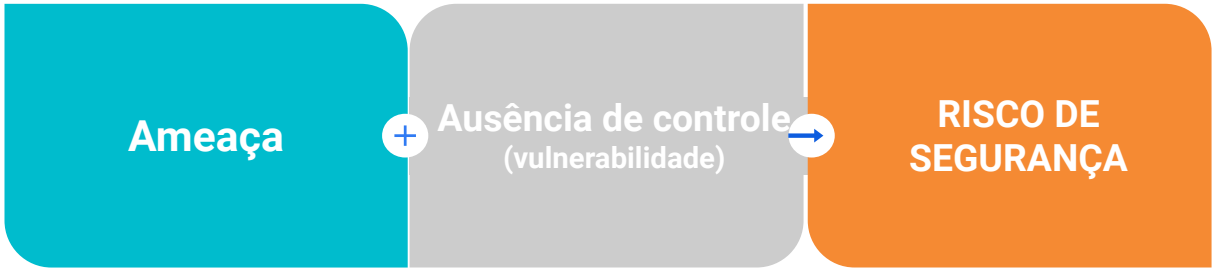
Etapa destinada a identificarmos quais são **os controles que já possuímos** e quais são **os controles que precisamos implementar**

- Para cada vulnerabilidade realizar a pergunta:

"***Temos algum controle que impeça isso de acontecer?***"

- **Se sim, retirar** item com referência do controle.
- **Se não, manter** o item no diagrama.

Mitigação



Ameaça	Vulnerabilidade	Risco
Interceptação de comunicação entre APIs	Ausência de criptografia ou canal seguro (HTTPS)	Vazamento de dados pessoais

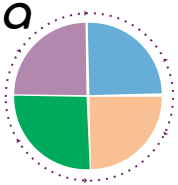
Priorização

Esta etapa é destinada a identificar os **riscos**, **probabilidade** e **impacto** de cada associados às ameaças encontradas. Com isso, priorizá-las.

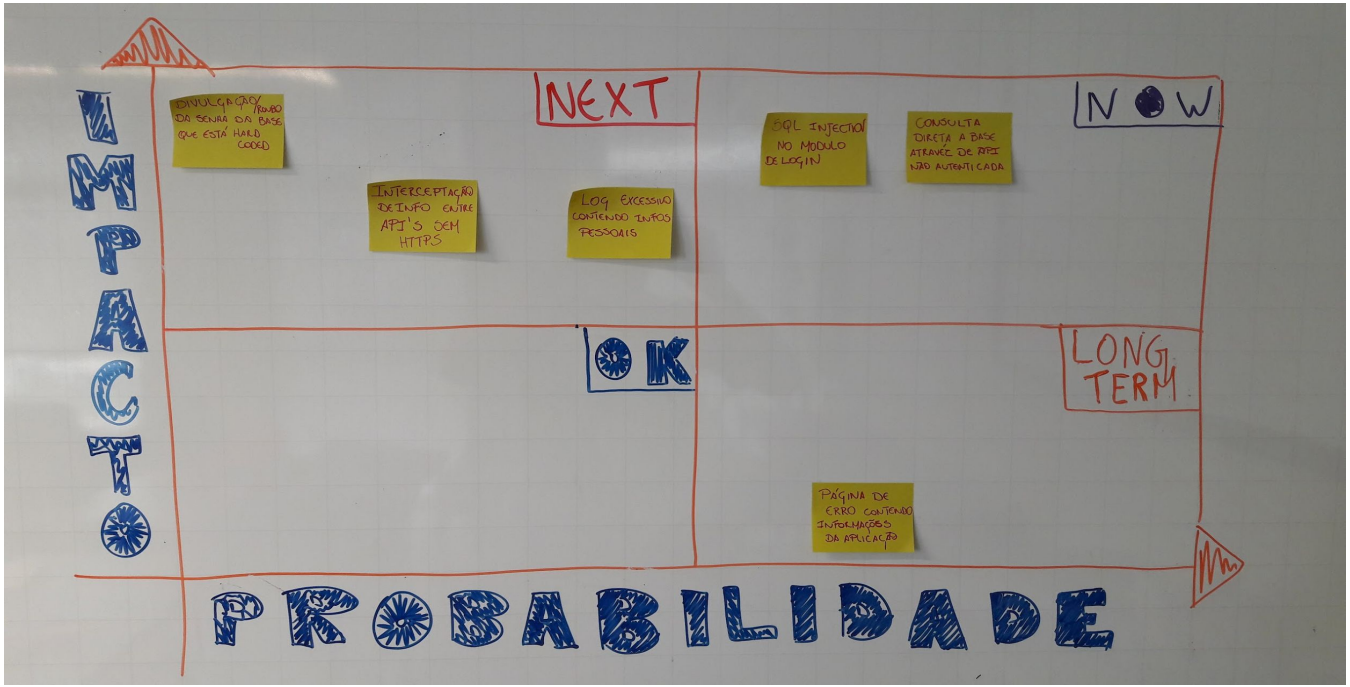
- Desenhe um matriz de **Impacto** *versus* **Probabilidade**.
- Defina para cada item qual é quadrante que ele está. Por exemplo: **alto** *impacto*, **baixa** *probabilidade*.
- Derive e priorize tarefas no backlog de acordo com o risco de cada uma.

RISCO = PROBABILIDADE de ocorrência

x IMPACTO do dano causado



Priorização



Experiências E Aprendizados

Leia mais sobre em...

- OWASP Threat Modeling
- Norton LifeLock Cyber Safety Insights Report Global
- ThoughtWorks Threat Modeling
- Dipping Your Toes Into Threat Modeling
- Secure Design with Threat Modelling
- Mapa de segurança
- Lean Model Security and Security Practices
- Sensible Security Conversations

Nos ache aqui :)
Até mais

github/thaiane
thaianebraga
thaianefbraga@gmail.com
ThaiiBraga
thaiane.github.io

github/ruandev
ruanvictor
ruan@ruanvictor.dev
Ruanvictor_
ruanvictor.dev