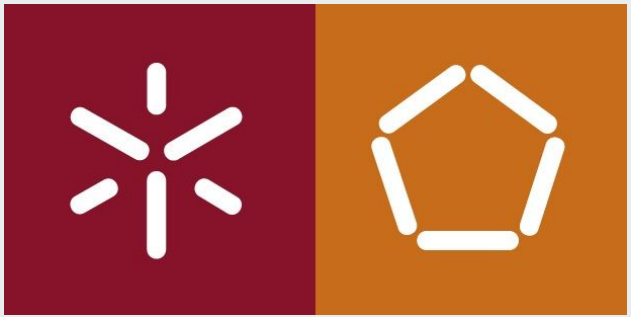
Apresentação Projeto 1
Engenharia de Segurança

Grupo 11

André Gonçalves - A80368

Nelson Sousa - A82053

Pedro Freitas - A80975



Índice

Introdução

Importância do Desenvolvimento de Software Seguro

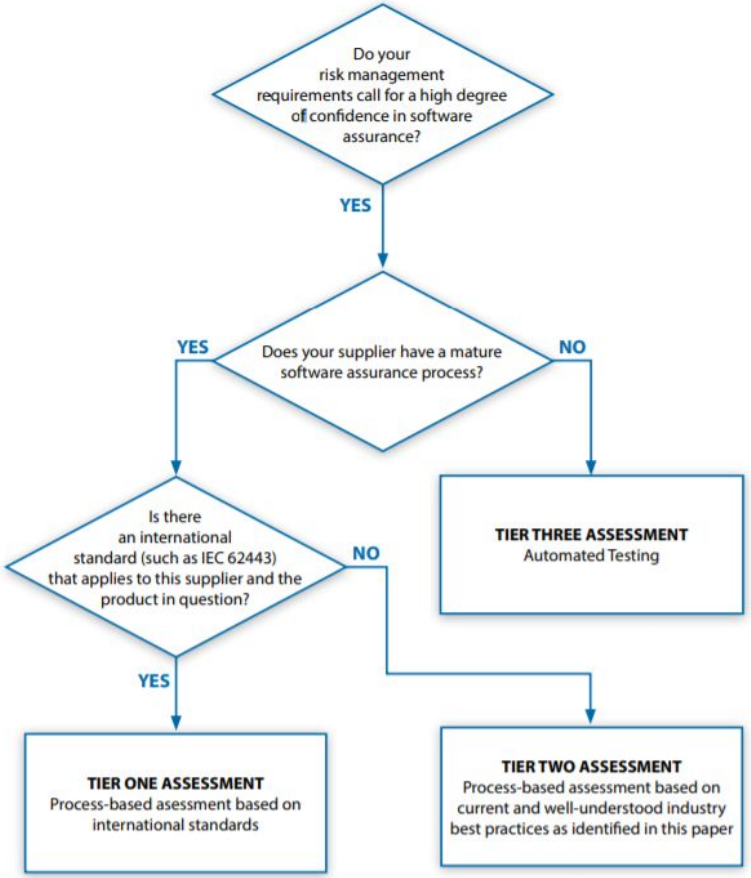
Software assurance engloba o desenvolvimento e implementação de métodos e procedimentos de forma a assegurar que o software funciona como o esperado enquanto atenua os riscos de vulnerabilidades e da existência de código malicioso que poderia prejudicar o utilizador final.

SAFECode

- A garantia de software não é alcançada por uma única prática, ferramenta ou lista de verificação; antes pelo contrário, é o resultado de um processo abrangente de engenharia de software seguro
- A diversidade de abordagens usadas pelas organizações que adquirem software e as desigualdades na adoção de práticas de garantia de software pelas organizações de desenvolvimento de TI tornou claro que precisamos de uma abordagem em camadas para avaliar a segurança dos softwares adquiridos com base na maturidade do fornecedor de tecnologia que desenvolve o software
- Os problemas atuais enfrentados por muitos clientes e fornecedores exigem uma solução imediata a curto prazo e que sejam amplamente aceites a médio / longo prazo pelos padrões internacionais abrangentes
- Os clientes podem exigir evidências para apoiar as reivindicações de um fornecedor
- Os clientes precisam de conhecer o processo de garantia, tanto na empresa quanto no produto para apoiar as suas necessidades de gerenciamento de riscos

Níveis de Abordagem

- Avaliação de Nível 1
- Avaliação de Nível 2
- Avaliação de Nível 3



Práticas de Construção de Software Seguro

- No que toca a este tópico, a SAFECode publicou *papers* com os fundamentos para a Prática de Construção de Software Seguro.

- Qual o objetivo?
  - Auxiliar as indústrias com as melhores práticas de construção de Software para garantir que este seria seguro.
  - Fornecer um conjunto de critérios comuns entre os clientes e as empresas que fornecem os Softwares, globalizando assim os procedimentos recomendados.

Práticas de Construção de Software Seguro

- Nesses *papers* são sugeridas formas do cliente tirar partido de algumas questões que podem ser feitas às entidades que lhes fornecem o serviço, para perceber se de facto a segurança foi tida em conta.
- São também apresentadas várias práticas de construção de software seguro:
  - Threat Modeling
  - Least Privilege
  - Sandbox
  - Minimizar funções de buffer
  - Usar bibliotecas XSS (Anti-Cross Site Scripting)
  - Eliminar a Criptografia Fraca
  - entre outras...

Entidades Reguladoras de Segurança do produto

- O que são?
  - Empresas com um processo de garantia de segurança de Software com um elevado grau de maturidade.
  - Possuem uma estrutura de regulação robusta que supervisionam todo o processo de garantia de segurança.

- Quanto à estrutura....
  - A empresa garante que tanto o processo de construção de software como o processo de supervisão estão bem explícitos e que são compreendidos por toda a organização.

Entidades Reguladoras de Segurança do produto

- O que fazem estas entidades?
  - Garantem que a equipa de desenvolvimento de software tem elementos com treinos e aptidões de segurança
  - Garantem que existem métodos que garantem que os requisitos de segurança são amplamente compreendidos
  - Garantem que os responsáveis de gestão de segurança do produto, da organização, analisam e assinam a qualidade de segurança do produto
  - Garantem que existe um planeamento adequado para identificar e registar passos e decisões para solucionar quaisquer descobertas não mitigadas, para ser usada no futuro.

Entidades Reguladoras de Segurança do produto

- A entidade deve
  - Adotar uma avaliação apropriada a quaisquer riscos identificados como parte do processo de desenvolvimento e como parte de atividades realizadas durante o ciclo de produção

- Porém não é esperado que a entidade reguladora corrija todos os defeitos de segurança!
- … Eles devem ter uma abordagem baseada na análise de risco desses mesmos defeitos!

Resposta a Vulnerabilidade

- Apesar de todos os cuidados com a construção segura de software temos de ter consciência que poderão existir vulnerabilidades!
  - Má análise da equipa de desenvolvimento
  - Aparecimento de novas técnicas e tecnologias de ataque
- Como tal é necessário cuidados adicionais para garantir:
  - Que qualquer utilizador possa reportar vulnerabilidades que o produto possua à empresa que o desenvolveu
  - Que a empresa de desenvolvimento de software consiga comunicar aos clientes vulnerabilidades encontradas
  - O uso de ID's no formato CVE para listar vulnerabilidades na NVD

Métodos de avaliação de segurança de software

- Usando a framework da SAFECode existem três métodos distintos para a avaliação de segurança do produto:
  - Transparência da documentação do processo:
    - Documentar o método de desenvolvimento de software.
    - Muitas entidades documentam abertamente todo o seu processo em páginas *web* focadas em segurança por meio de *white papers* ou posts em blogs públicos.
    - Toda a documentação deve ser detalhada mostrando as práticas usadas e o contexto dessa utilização
  - Partilha sob NDA (Non Disclosure Agreement):
    - Quando a documentação não pode ser pública (por opção ou indisponibilidade) o fornecedor deverá comunicar via NDA com o cliente para lhe fornecer essa documentação
    - Isto demonstra confiança na relação *cliente-fornecedor*.
  - Validação por terceiros:
    - No caso desta validação por terceiros ser um requisito, a avaliação é feita por outra entidade que se deverá seguir por todos métodos de segurança definidos.