SYNACKTIV

Édition #2

Product Security

De l'ombre à la lumière

09/06/2021

Lumière sur notre Ninja

Tiphaine Romand-Latapie
Responsable du pôle Reverse Engineering

Expériences :

- Responsable de l'équipe d'évaluation (redteam) @ Airbus
- Responsable sécurité produit @ Orange
- Expert cryptographie @ gov

SYNACKTIV

Plan

- **Cyber Sécurité**
  - Perception vs Réalité
- **Erreurs les plus vues en sécurité produit**
- **Sécurité produit dans un monde parfait**
  - Un processus intégré de bout en bout

Plan

- **Cyber Sécurité**
  - Perception vs Réalité
- **Erreurs les plus vues en sécurité produit**
- **Sécurité produit dans un monde parfait**
  - Un processus intégré de bout en bout

Sécurité Produit

- Ce que le monde pense que nous faisons

- Ce que nous faisons vraiment

La cyber sécurité vue comme une fonction « support »

- **« Information management »**
  - Est une fonction de production :
    - Développe des outils (interne ou produit)
  - Offre des outils de production :
    - Déploie et maintient des outils pour les métiers
    - Offre des services de maintenance et de support à ses outils

- **Finance/Légal**
  - Conseillent :
    - Utilisent une connaissance technique spécifique (finance, loi) pour conseiller l'entreprise
    - Aident l'entreprise à prendre des décisions éclairées
    - Sont des fonctions support de management du risque

La cyber est souvent placée ici

La cyber devrait être ici

SYNACKTIV

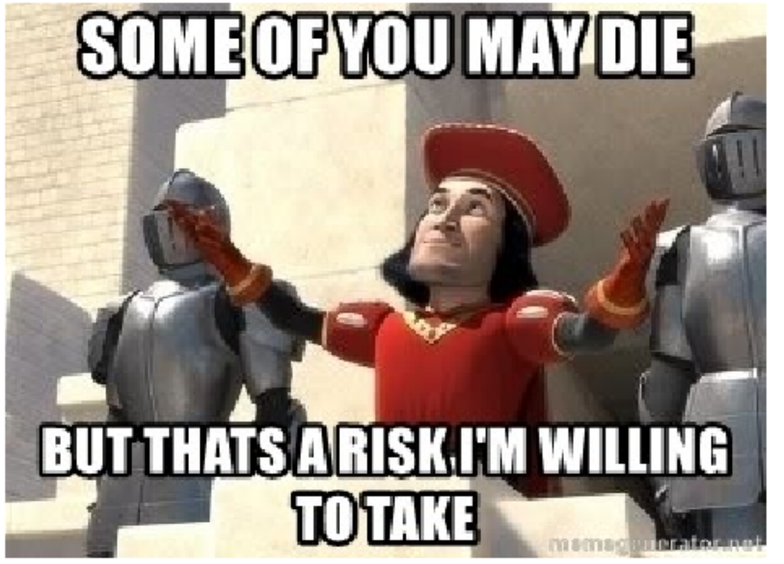
Plan

- **Cyber Sécurité**
  - Perception vs Réalité
- **Erreurs les plus vues en sécurité produit**
- **Sécurité produit dans un monde parfait**
  - Un processus intégré de bout en bout

Erreurs les plus vues en sécurité produit

- **Processus sécurité limité au pentest**
  - Ou au bug bounty ...

- **Chefs de projet acceptant les risques**
  - Qu'ils ne portent pas vraiment



Erreurs les plus vues en sécurité produit

- **L'ingénieur sécurité qui impose son point de vue**
  - Impose la solution technique
  - Décide seul si un risque doit être pris ou pas

- **Pas d'analyse de risque**

Erreurs les plus vues en sécurité produit

- **Sécurité vue comme une autre « fonctionnalité » du produit**
  - Équipe sécurité vue comme un sous-groupe de développeurs ou d'architectes
  - La fonctionnalité n'apporte pas de plus value visible pour le client final, est vue comme optionnelle

- **Pas de vision de bout en bout de la sécurité**

Erreurs les plus vues en sécurité produit

- **Équipes sécurité passives**
  - Attendant qu'on les appelle
  - Ce qui arrive (ou pas) deux jours avant la mise en prod...

- **Prise de décision sécurité uniquement basée sur le "coût" de la sécurité**
  - Équipes sécurité en position défensive
  - Devant justifier chacune de leurs exigences
  - Les équipes sécurité oublient de parler argent

Plan

- **Cyber Sécurité**
  - Perception vs Réalité
- **Erreurs les plus vues en sécurité produit**
- **Sécurité produit dans un monde parfait**
  - Un processus intégré de bout en bout

Sécurité produit de bout en bout : dans un monde parfait

Intégrer la sécurité dans toutes les étapes du projet

Lancement projet → Brief Marketing → Cahier des charges → RFP → Dev. → QA → Prepa. lancement → Lancement → Vie du Produit

SYNACKTIV

Sécurité produit de bout en bout : dans un monde parfait

- **Avant le début du projet**
  - Identifier le porteur du risque métier (business)
    - Qui va en prison ? Quelle entité paiera les amendes/les compensations client ? Etc.
  - Définir un processus de prise de décision sécurité
    - Qui est autorisé à prendre quels risques ? Pour le projet ? Pour l'entreprise ?
    - Toutes les parties prenantes doivent être d'accord sur le processus
  - Définir la stratégie de l'accompagnement sécurité produit, la faire valider
  - Nommer un responsable Sécurité pour le projet/programme (Single point of contact) & définir leurs responsabilités dans la direction du projet

Un nouveau départ

- **« Brief Marketing »**
  - Faire une analyse de risque « business »
    - Risque image ?
    - Le client final attend-t-il une fonction sécurité ?
    - Il y a-t-il des obligations légales ou contractuelles ?
    - Etc.
  - Les risques doivent être priorisés par le porteur du risque

- **Cahiers des charges / Expression de besoin**
  - Les lire tous, c'est la première occasion d'éviter de futures situations problématiques
  - « Je viens de lire votre idée de fonctionnalité, avez-vous conscience des coût sécurité associés ? »
  - Faire une analyse de risques sécurité du projet : quelles sont les fonctionnalités produit risquées ? Il y a t'il des recommandations sécurité qui posent un risque projet (difficiles à développer, contraintes sur le développement etc.) ?

Les mains sous le capot

- **Exigences Sécurité**
  - Écrire un ensemble d'exigences (conseil : ce sont des exigences, pas des solutions techniques)
  - Soyez prêts à suivre la complétion de ces exigences tout au long du projet
  - Soyez prêts à lister et suivre toutes les exigences non remplies
  - Tracez le lien entre vos exigences et les risques business ou techniques de vos analyses de risques
- **RFP**
  - Doit contenir les exigences ou les expressions de besoin sécurité
  - L'équipe sécurité doit s'assurer que ses exigences ne sont pas en conflit avec les exigences projet (et préparer un dossier de décision le cas échéant)
  - Le fournisseur doit expliquer comment il compte remplir les exigences et s'engager à les remplir dans le contrat
  - La correction des problèmes de sécurité pendant le développement et la vie du produit devrait être au contrat !
  - N'oubliez pas la "clause de pentest/audit" au contrat

Qualité-Coût-Délai pour la Sécurité Produit

- **Planning Securité Demandé !**
  - Dès le début du projet, le planning global doit réserver du temps pour les activités sécurité (relecture des cahiers des charges, écritures des exigences, qualité, pentest etc.)
  - Paraît inutile mais:
    - “Normaliser” la sécurité dans le projet
    - Permet de montrer le travail effectué
    - Permet de se défendre contre l’argument « on est en retard à cause de la sécurité »

- **Tracer les coûts Securité**
  - Pour argumenter les dossiers de décision sécurité
  - Pour reconnaître et récompenser le travail des équipes (le temps passé en réunion est souvent oublié)
  - Permet l’amélioration continue du processus sécurité

Focus : Dossier de décision sécurité (1/2)

- **Quand une exigence sécurité pose problème :**
  - Elle est en conflit avec une autre exigence produit
  - Elle impact le processus QCD du projet
  - Autre
- **L'idée est de faire un dossier (slides, document etc.) préparé par les équipes sécurité et les équipes affectées**
- **Le dossier doit être présenté au bon niveau de management pour décision (dépendant des coûts et risques identifiés)**
  - Niveau maximal : porteur du risque
- **Devrait présenter 3 scenarios et les coûts et gains associés**
  - 1 scenario "sans sécurité": les gains **quantifiés** pour le produit ou le projet, coût ou impact légal/image en cas de réalisation du risque sécurité
  - 1 scenario "sécurité optimale": les coûts et risques **quantifiés** pour le produit ou le projet, les gains (ou protection contre les pertes) potentiels en cas de réalisation du risque sécurité
  - 1 scenario intermédiaire (quand c'est possible)
- **La plupart du temps: une solution est trouvée en préparant le dossier, et aucune décision n'est nécessaire… (WIN!)**

Focus : Dossier de décision sécurité (2/2)

- **Trop souvent, les équipes de sécurité essaient de convaincre via un “scenario catastrophe” imaginaire**
  - Peut être utile pour illustrer une discussion, mais pas suffisant pour prendre une décision stratégique
- **La finance et le légal sont vos amis**
  - Et même la communication ou les équipes « branding » !
  - Ils vous aideront à qualifier et quantifier vos risques (ils vous trouveront même de nouveaux scenarios catastrophe)
  - Quand les conséquences potentielles d’une attaque sont écrites par ces entités, votre impact en tant qu’équipe sécurité est démultiplié (ce n’est plus “ces paranos de la sécurité”)

Phase de développement

- **Spécifications techniques**
  - Laissez les différentes équipes projets (ou le fournisseur) offrir des solutions techniques de réalisation de vos exigences (évitez au maximum d'imposer une solution technique)
  - Aidez les à comprendre vos exigences et à trouver des solutions
  - Préparez une analyse de sécurité et un dossier de décision si il y a un écart entre l'exigence et la solution
  - Tracez et documentez toutes les écarts ou non conformités à vos exigences et les risques associés
- **Qualité**
  - Le suivi de qualité des fonctions de sécurité doit faire partie du processus qualité global
  - Identifiez ce qui peut être suivi en Qualité de ce qui doit être évalué en évaluation/pentest
  - Les équipes sécurité doivent aider les équipes Qualité à noter la criticité des défauts
  - Un pentest seul n'est PAS un processus qualité

Pendant toute la durée du projet

- **Suivre et mettre à jour le tableau de risques “macro”**
  - Objectif : reporting au porteur du risque et entités impliquées
  - Permet de lever des alertes au plus tôt
- **Suivre et documenter les risques résiduels:**
  - Description
  - Quels sont les impacts (business ou techniques) en cas de réalisation du risque
  - Statut : Contre-mesure déjà planifiée dans une future mise-à-jour ? Contre mesure organisationnelle ? Le risque est accepté ? Si oui par qui ?
  - Objectif: Livrer la liste aux équipes sécurité de production pour qu’elles aient toutes les information leur permettant de gérer un incident de sécurité ou un changement de contexte de déploiement

Le lancement approche

- **Maintenant vous pouvez faire un pentest :D**
  - Décidez ce qui doit être évalué par pentest et ce qui nécessite une analyse approfondie
  - Scopez le test! Vérification de suivi de bonne pratique ? Scenario critique ? Etc.
  - En cas de résultat négatif non basique → analyse de risque
  - Dossier de décision en cas de faille critique difficile à corriger
  - Plan de correction (après lancement si nécessaire)
- **Si ce n'est pas déjà fait, embarquez les équipes sécurité responsables de la production**
  - Présentez et expliquez le statut des risques résiduels et le plan de correction prévu
  - Vérifiez que tout ce dont ils auront besoin est documenté
- **Rencontre avec le porteur du risque**
  - Il/Elle doit accepter les risques résiduels au lancement !
  - Présentez le plan de correction

Lancement

- **Gardez une équipe mixte (projet/production) pour quelques semaines/mois**
  - Pour suivre le plan de correction
  - Pour aider le transfert de connaissances
- **Faire un post-mortem (debriefing, retex etc.) du processus sécurité pendant ce projet**
  - Et partagez le :)
- **Les équipes sécurité de « production »**
  - Gèrent le suivi de vulnérabilités
  - Suivent le déploiement des correctifs
  - Conseillent les métiers si le contexte de déploiement à changé « on décider de connecter le produit en 4G »

Conclusion / à retenir

- Normalisez la sécurité dans le projet !
- La fonction « sécurité » est plus proche des fonctions « légal » et « finance » que de la fonction « développement »
- Le plus tôt est le mieux

Questions ?

Merci pour votre attention

SYNACKTIV

https://www.linkedin.com/company/synacktiv
https://twitter.com/synacktiv
Nos publications sur : https://synacktiv.com