Évaluer la solidité de son SI : pratiques et valeur ajoutée

Si l'objectif d'en faire l'inventaire exhaustif est louable, il n'en reste pas moins difficile à atteindre dès que le SI devient complexe. Pour limiter les possibles conséquences graves des vulnérabilités, différents outils ont été développés pour les identifier tels que la veille, les techniques de scan, les tests d'intrusion, le Bug Bounty, les Red Team, les audits techniques, etc.

Au-delà de ça, il est intéressant de se poser la question de la posture à tenir face aux vulnérabilités : une fois qu'un chercheur a connaissance de vulnérabilités, comment communique-t-il auprès des organismes concernés, par exemple à travers une politique de full disclosure ?

Connaître ses vulnérabilités pour mieux se protéger : RETEX d'un hébergeur cloud

Le recours à des opérateurs de services cloud pose des problèmes spécifiques pour la sécurité des systèmes d'information :

- Le **nombre** de serveurs et d'équipements à protéger ;
- La très grande **diversité des technologies** à maîtriser et sécuriser ;
- L'**empilement de couches** matérielles et applicatives interdépendantes ;
- La **forte exposition** du système d'information dans la mesure où il est directement accessible sur les réseaux via des portails, API, machines virtuelles, etc ;
- Les **responsabilités partagées** entre le client et le fournisseur d'infrastructures ;
- La **mutualisation d'environnements multi-clients** répondant à des objectifs différents ;
- L'**interruption quasi-impossible** des services cloud garantissant une forte disponibilité dans le Service Level Agreement (SLA).

Dans ces conditions, un système d'information tributaire des services cloud est fortement exposé aux attaques et les opérations pour limiter les vulnérabilités sont complexes à organiser.

Pour Olivier Perrault, RSSI chez Orange Cloud for Business, la solution réside dans la mise en place d'une organisation interne robuste reposant sur :

- La **veille** sur les vulnérabilités en focalisant les moyens d'analyse selon la stratégie retenue et en utilisant des outils d'agrégation évitant de devoir se fier uniquement au buzz ;
- Le déploiement d'une **ingénierie** pour analyser et valider des scripts et guides d'implémentation, requalifier la criticité des vulnérabilités et fournir des environnements durcis. Cette étape est coûteuse car elle nécessite d'avoir du personnel qualifié et des environnements de test à disposition. Elle permet cependant de réduire les risques opérationnels et de ne pas se fonder uniquement sur les seuls guides des éditeurs ;
- Le **scan des vulnérabilités** sur l'ensemble du parc informatique permettant d'avoir une vue d'ensemble du niveau de risque et d'orienter la stratégie de patch globale. Cette méthode permet d'identifier les systèmes effectivement vulnérables sans réaliser un inventaire parfait ;

- Les **tests d'intrusion** pour toute nouvelle application afin de ne pas se limiter aux seuls outils automatiques. Cette politique impose de disposer d'une équipe de pentesters, d'anticiper l'étape du test dans les calendriers de production et de travailler en collaboration avec les développeurs pour identifier les mauvaises pratiques ;
- Le **scan automatique** de toutes les applications adapté pour les releases mineures et s'intégrant aux pratiques devops.

En conclusion, Olivier Perrault précise que l'exigence d'exhaustivité dans l'évaluation des vulnérabilités demande un effort important et une expertise des technologies et de la sécurité en interne. Cela renforce la confiance dans le système d'information, la réactivité face aux attentes des clients et l'autonomie dans le déploiement des stratégies d'assurance qui permet d'éviter des crises graves de sécurité.

Le Bug Bounty aujourd'hui et demain

Pour Clément Domingo, aka SaxX, pentester le jour chez Sopra Steria et chasseur de bug bounties la nuit, les programmes de bug bounty incitent les hackeurs éthiques à signaler les vulnérabilités qu'ils ont identifiées aux organisations concernées contre une rémunération.

Réputés efficaces et peu coûteux pour identifier les vulnérabilités d'un système d'information, les programmes Bug Bounty ont connu leurs prémisses en 1994 lorsque Netscape a promis une rémunération à toute personne qui lui remonterait une faille de sécurité.
En 2007, la fondation Mozilla a sollicité les hackeurs pour identifier des failles de sécurité dans son navigateur Firefox. Entre 2010 et 2012, ce fut au tour des GAFA de lancer des programmes Bug Bounty contre récompense en interne.
Enfin, le Département de la Défense des États-Unis a décidé d'ouvrir au public son programme Bug Bounty en 2016, ce qui fait état d'une évolution des mentalités sur ce sujet.

L'expérience de chasseur de Clément Domingo lui a permis de constater que les mœurs deviennent de plus en plus favorables au Bug Bounty : le recours à ces solutions par les entreprises est croissant et les compétitions entre hackeurs se multiplient. Il regrette cependant que les événements organisés ne soient pas plus nombreux pour asseoir cette nouvelle pratique et encourage au partage d'informations plutôt qu'au maintien de la culture du secret.

Clément Domingo conseille à toute organisation qui souhaiterait lancer un programme Bug Bounty de définir précisément son périmètre, de décider si le programme doit être intégré à une plateforme ou managé en interne et s'il doit être public ou privé. Il lui semble opportun de commencer par un programme privé de façon à vérifier si l'équipe interne a les capacités de trier les vulnérabilités soumises et de les corriger. Une grille de rémunération doit également être accessible afin de motiver les chercheurs et de leur préciser s'ils seront récompensés au moment où la vulnérabilité est trouvée, acceptée ou résolue.

En tant que chasseur, Clément Domingo encourage les hackeurs à tester leurs compétences sur les plateformes Bug Bounty en se montrant persévérant car les échecs sont nombreux. Il souligne qu'un chercheur doit rester humble même s'il est talentueux et cultiver de bonnes relations avec le manager du programme Bug Bounty afin de mieux orienter ses recherches. Il lui semble enfin primordial de retranscrire les vulnérabilités identifiées de façon claire afin que l'équipe interne

puisse les évaluer facilement et récompenser les chercheurs en conséquence.

Sur le modèle du site Cyberexcuse, Clément Domingo narre enfin quelques cas concrets de vulnérabilités qu'il a été en mesure d'exploiter afin d'acheter des produits gratuitement sur une e-boutique à l'aide d'un proxy, de cartographier tous les sites d'une entreprise grâce aux adresses IP recueillies lors d'une attaque SSRF, de récupérer tous les fichiers d'une base de données suite à une injection SQL avancée ou de prendre la main sur un système après avoir intercepté des mots de passe basiques de type admin.

La divulgation des vulnérabilités pour fédérer

La coopération est au cœur de la divulgation des vulnérabilités pour Guillaume Vassault-Houlière, CEO de YesWeHack. Il rappelle qu'elle est définie dans la norme ISO/CEI 29147 comme « *un processus par lequel les fournisseurs et les personnes qui découvrent des vulnérabilités peuvent travailler en collaboration pour trouver des solutions qui réduisent les risques associés à une vulnérabilité.* »

La norme ISO/CEI 30111 précise quant à elle la procédure qui permet de coordonner les différents acteurs intervenant dans l'identification et la résolution d'une vulnérabilité, à savoir :

- Le chercheur qui identifie la vulnérabilité ;
- Le rapporteur qui avise le fournisseur de son existence ;
- Le fournisseur qui créé ou entretient le produit vulnérable ;
- L'administrateur système qui déploie des mesures correctives ;
- Le coordinateur qui fédère la communauté.

Le concept de remontée coordonnée de vulnérabilité (CVD) a émergé pour réduire au minimum le risque en veillant à ce que les vulnérabilités identifiées soient prises en compte. Pour cela, il est nécessaire que suffisamment d'informations soient fournies aux entreprises pour évaluer la criticité des vulnérabilités de leurs systèmes.

La CVD repose sur la croyance aux bonnes actions de bons samaritains, le respect de la déontologie et la stimulation de la coopération grâce aux récompenses des hackeurs sous forme de rémunérations, goodies ou inscription au Hall of Fame. Cette méthode favorise l'apprentissage en s'inspirant de la boucle OODA, ce qui permet d'éviter de trouver des vulnérabilités par hasard.

L'Europe est en avance dans l'adoption de la CVD même si les discussions sont toujours en cours.

La création de canaux de confiance est primordiale pour cadrer le processus de remontée des vulnérabilités et éviter que les chercheurs soient assimilés à des hackeurs malveillants. Diverses méthodologies existent, parmi lesquelles :

- La **Responsible Disclosure Policy** qui précise les modalités de communication des vulnérabilités par mails cryptés en PGP, le délai de réponse de trois mois et le système de récompense pour les vulnérabilités qui n'ont pas déjà été rendues publiques en fonction de leur sévérité évaluée par le CERT ;
- **Security.txt** qui permet de transmettre des vulnérabilités en renseignant différents champs dans un draft RFC (contact, encryption, acknowledgements, policy, hiring…) ;
- Les **programmes Bug Bounty** assimilés à de la crowd security dans la mesure où ils font

appel à une communauté pour identifier des vulnérabilités sans contrainte de temps et contre rémunération ;
- L'**article 47 de la loi pour une République numérique (2016)** qui cadre les règles de soumission des vulnérabilités en légitimant l'absence de poursuites pénales pour les personnes de bonne foi tout en garantissant leur confidentialité ;
- **Zerodisclo.com** qui permet de transmettre les vulnérabilités via un système décentralisé reposant sur la blockchain.

RETEX d'une plateforme web

Confronté à un incident en décembre 2016, Dailymotion a déclenché un programme Bug Bounty privé afin d'identifier la vulnérabilité en cause. Malgré des remontées intéressantes, le programme a été mis en pause en l'état en sortie de crise car cet outil n'a pas permis de répondre à l'objectif ciblé et que l'équipe interne n'avait pas assez de ressources pour traiter toutes les soumissions dans un délai raisonnable.

Le programme initial a par la suite été réactivé en systématisant le tri des tickets, en réévaluant la sévérité des failles de sécurité et en vérifiant leur remédiation.

Un nouveau programme Bug Bounty privé intégré à un plan d'assurance sécurité a été lancé lors de la refonte complète du site Dailymotion. En formalisant les objectifs, le règlement et les rémunérations, le programme a permis d'obtenir des soumissions de qualité contribuant à l'amélioration du site de manière agile et de retarder la réalisation d'un audit technique exhaustif à un stade de développement plus avancé. Le Bug Bounty s'est dès lors inscrit dans une véritable démarche de gouvernance globale.

Quentin Berdugo, Chief Information Security Officer de Dailymotion, explique que l'ouverture du programme Bug Bounty au public a nécessité de clarifier le périmètre, les attentes et les rémunérations dans le règlement, d'anticiper la charge de travail pour les équipes internes et d'accompagner le lancement du projet par un plan de communication.
Lorsque le programme est arrivé à maturité les équipes ont choisi de diversifier les communautés de chercheurs, de les orienter sur des périmètres spécifiques et de les motiver grâce à des rémunérations au forfait les incitant à se familiariser avec les couches profondes de l'application.

Le Bug Bounty est un outil supplémentaire à la disposition du RSSI qui complète mais ne remplace pas les approches existantes. Il se caractérise par :

- Une structure de coûts difficilement prévisible qui peut néanmoins se révéler rentable et efficace dans la mesure où seuls les résultats sont rémunérés ;
- Le soutien nécessaire par une équipe interne qualifiée afin d'évaluer la pertinence des soumissions et de pouvoir corriger les vulnérabilités rapidement ;
- L'orientabilité limitée des recherches malgré la possibilité de définir des périmètres ciblés ;
- L'inadaptabilité de cette méthode pour scanner des domaines particulièrement sensibles ou qui nécessiteraient des connaissances métier approfondies ;
- L'efficacité du dispositif attirant une multiplicité de talents aux approches très pragmatiques.

Le devoir de transparence envers la communauté des chercheurs est essentiel afin de respecter le travail effectué. À cette fin, il est conseillé :

- D'établir un règlement complet et intelligible qui explicite les attentes et les interdits ;
- De faire preuve de réactivité dans le traitement des soumissions, la correction des failles et le versement des primes.
- D'expliquer la logique qui préside à l'évaluation de la sévérité des vulnérabilités en encourageant par exemple les chercheurs à apporter la preuve de l'impact des failles de sécurité sur les applications métier.

Les bonnes pratiques imposent en revanche de considérer les chercheurs comme des intrus en déclenchant par exemple les procédures de vérification des journaux ou de rotation des secrets dès qu'ils sont repérés afin de garantir la sécurité.
Si une organisation n'a pas les moyens de déployer un programme Bug Bounty, il est recommandé au minimum de définir une politique de divulgation, de la publier dans un security.txt et de disposer d'une adresse security@ dédiée au recueil des soumissions.

Quelles méthodes sont les plus efficaces pour identifier les vulnérabilités d'un SI ?

Jean-Marc Cerles explique que Veolia privilégie les tests d'intrusion répétés au Bug Bounty car ils représentent une charge de travail moindre et peuvent être déployés sur un périmètre restreint. Être capable de mesurer le niveau de risque et de diffuser des alertes lui semble cependant essentiel pour que le travail des équipes informatiques soit mieux compris et reconnu par la direction.

Adrien Petit expose la stratégie d'Inquest Risk spécialisé dans les attaques Red Team. La cartographie de l'ensemble du périmètre permet d'identifier les failles techniques et humaines qui vont faciliter l'introduction dans un SI.

Pour Laurent Beaussart de Vinci Autoroutes, il est préférable que les équipes internes ne soient pas informées d'une attaque Red Team afin que l'exercice soit le plus transparent possible. Il faut de plus fixer des objectifs tangibles aux Red Team comme l'interception de numéros de cartes bancaires et leur laisser le champ libre pour avoir recours à tous les vecteurs : intrusion physique, spams, etc.

Pour Henri Favreau de Bouygues Telecom, le debriefing entre la Red Team et la Blue Team doit être approfondi pour mettre en œuvre un plan de remédiation efficace.

Jean-Marc Grémy, Président du CLUSIF, s'interroge sur la nécessité d'évaluer la sécurité au moment du développement logiciel. Nicolas Andreu de Coface est favorable à l'intégration de tests continus et Laurent Beaussart de Vinci Autoroutes prône en faveur de l'adoption d'une grille d'analyse imposant la réalisation de tests suivant le type d'applications développées.

Laurent Beaussart de Vinci Autoroutes doute que l'intelligence artificielle (IA) puisse faciliter la détection des vulnérabilités à priori et non plus à postériori.
En effet, ce n'est pour lui pas tant l'automatisation des recherches que la meilleure compréhension des ressorts de la crédulité des gens qui améliorera le niveau de sécurité. Or cette dimension psychologique n'est à ce jour pas prise en charge par l'IA.