ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité » n°70
Lundi 13 Mai 2024

Bug Bounty et Tests d'Intrusions

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 1 Cybersécurité et E-santé – Université Paris Cité

SOMMAIRE

Introduction

La session du "Lundi de la Cybersécurité" du 13 mai 2024 a été orchestrée par le Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks, qui ont réussi à réunir des esprits éminents du domaine de la cybersécurité pour une journée de discussions profondes et de partages d'expériences. Cette édition a été marquée par la présence notable de Nicolas Kalmanovitz, dont l'intervention principale a porté sur les avancées récentes et les défis persistants dans la sécurité offensive ,le Bug Bounty et les PenTests.

Cette conférence a également été l'occasion, durant le « quart d'heure accordé aux Associations » de découvrir des initiatives innovantes telles que la plateforme "Kids Can Hack", présentée par Sara Sellos. Cette plateforme vise à initier les enfants à la cybersécurité à travers des jeux de hacking éthique, illustrant l'engagement de la communauté à éduquer les plus jeunes aux bonnes pratiques du numérique dès leur plus jeune âge.

L'événement s'est concentré sur les implications des technologies émergentes pour la sécurité des systèmes d'information, soulignant les stratégies nécessaires pour renforcer les défenses contre une gamme toujours plus sophistiquée d'attaques cybernétiques. Le format en ligne a permis une large participation, facilitant un échange riche et diversifié entre experts de différents horizons, renforçant ainsi le dialogue nécessaire pour anticiper et répondre aux défis complexes de notre ère numérique.

I. Présentation de l’intervenant

Le rôle central de Nicolas Kalmanovitz dans cette conférence sur le Bug Bounty et les tests d’intrusions mérite une attention particulière. En tant qu'intervenant principal, Nicolas a apporté une expertise profonde acquise au fil d'une carrière distinguée dans le domaine de la sécurité des systèmes d'Information. Actuellement, il occupe une position de leader au sein de l'entreprise Yogosha, où il a la charge de l'innovation et du développement de solutions de cybersécurité avancées.

Nicolas est reconnu pour son approche pragmatique et son engagement envers les méthodologies de sécurité offensives. Ses travaux et projets sont centrés sur l'identification proactive des vulnérabilités et la mise en œuvre de stratégies défensives robustes qui sont essentielles pour protéger les infrastructures critiques contre les cyberattaques de plus en plus sophistiquées. Sa vision pour la cybersécurité s'étend également à la formation et au mentorat de la prochaine génération de professionnels de la sécurité, soulignant l'importance de la sensibilisation et de l'éducation continue dans ce domaine en évolution rapide.

L'intervention de Nicolas Kalmanovitz lors de cette session a été cruciale pour comprendre les tendances actuelles et futures en matière de cybersécurité, notamment en ce qui concerne les défis posés par les technologies émergentes et les meilleures pratiques pour y répondre efficacement. Son expertise et son expérience ont enrichi les discussions, offrant des perspectives précieuses sur la manière de naviguer dans le paysage complexe de la cybersécurité moderne.

II. Thèmes principaux et points forts

La conférence sur la cybersécurité du 13 mai 2024 a abordé une multitude de thèmes essentiels qui ont mis en lumière les enjeux et les innovations dans le domaine de la sécurité des systèmes d'information. Ces discussions ont permis de dégager plusieurs points forts qui méritent d'être soulignés pour leur pertinence et leur impact sur l'avenir de la cybersécurité.

Les discussions ont débuté par un état des lieux des défis actuels en matière de cybersécurité, notamment la manière dont les entreprises et les gouvernements peuvent répondre aux menaces croissantes de cyberattaques. L'accent a été mis sur la nécessité de développer des stratégies de défense plus robustes et adaptatives face à des adversaires qui évoluent constamment.

Nicolas Kalmanovitz a approfondi le sujet de la sécurité offensive, expliquant les dernières techniques et méthodologies utilisées pour anticiper et neutraliser les cyberattaques avant qu'elles ne causent des dommages. Cette approche proactive de la cybersécurité a été présentée comme un élément crucial pour renforcer la résilience des systèmes informatiques.

Un point saillant de la conférence a été l'importance de l'éducation et de la sensibilisation à la cybersécurité dès le plus jeune âge. Sara Sellos a partagé son expérience avec la plateforme "Kids Can Hack", qui vise à initier les enfants à la cybersécurité par le jeu. Cette initiative a été largement saluée pour son approche innovante et son potentiel à créer une génération plus consciente et préparée aux défis numériques.

Les participants ont également exploré comment les technologies émergentes, telles que l'intelligence artificielle et l'apprentissage automatique, transforment le paysage de la cybersécurité. Les discussions ont couvert les opportunités et les risques associés à ces technologies, mettant en évidence la nécessité d'une régulation et d'une éthique renforcées dans leur déploiement.

La conférence a souligné l'importance de la collaboration entre les secteurs public et privé pour combattre efficacement les cybermenaces. L'échange d'informations et les partenariats stratégiques entre les entreprises, les institutions académiques, et les gouvernements ont été identifiés comme des facteurs clés pour améliorer la sécurité globale du cyberspace.

III. Test de sécurité offensive

Nicolas Kalmanovitz a mis en lumière la nécessité d'adopter des approches offensives pour renforcer la cybersécurité des organisations. Dirigeant les opérations chez Yogosha, une plateforme de cybersécurité offensive, Nicolas a souligné que la sécurité traditionnelle ne suffit plus à contrecarrer les menaces actuelles, de plus en plus sophistiquées et fréquentes.

Le concept de Test de Sécurité Offensive (Offensive Security Testing) vise à tester activement les défenses d'un système en simulant les actions d'un adversaire. Cette méthode inclut diverses pratiques telles que le Pentest en tant que Service (PTaaS), les programmes de Bug Bounty, le Red Teaming, et plus encore. L'objectif est d'identifier et de remédier aux vulnérabilités avant qu'elles ne soient exploitées par des attaquants réels.

PenTest as a Service (PTaaS) :

PTaaS est une approche externalisée où les tests d'intrusion sont gérés via une plateforme en ligne, permettant aux utilisateurs de programmer et de réaliser des tests de sécurité à leur convenance, que ce soit sur demande ou de manière continue. Cette méthode offre des évaluations détaillées des risques, des interactions directes avec les pentesters et des recommandations de remédiation. Les tests peuvent être réalisés en mode Black Box, simulant une attaque externe sans connaissances préalables du système, en mode Grey Box avec des informations de haut niveau, ou en mode White Box où des informations détaillées sont fournies aux chercheurs pour une évaluation approfondie.

Bug Bounty :

Le Bug Bounty est une méthode qui implique l'utilisation d'une communauté de hackers éthiques pour tester la sécurité des actifs numériques. Les organisations offrent des récompenses monétaires pour chaque vulnérabilité validement identifiée. Les programmes peuvent être publics, ouverts à tous les chercheurs, ou privés, limités à des chercheurs invités en fonction de leurs compétences spécifiques. Cette approche permet une grande flexibilité et continuité dans la détection des vulnérabilités critiques.

Testing Offensif Continu :

Cette approche émergente implique des tests de sécurité réalisés de manière continue, intégrant les outils de gestion des surfaces d'attaque et les pratiques offensives dans les workflows DevSecOps. Cela permet de détecter et de remédier aux vulnérabilités de manière proactive, assurant une couverture de test plus complète et une intégration dans les cycles de développement.

Nicolas Kalmanovitz a réaffirmé que face à l'évolution rapide des menaces cybernétiques, les méthodes traditionnelles de sécurité, bien que nécessaires, sont insuffisantes pour protéger efficacement les organisations. Il a plaidé pour une intégration accrue des tests de sécurité offensifs, mais éthiques, tels que PTaaS et Bug Bounty, dans les stratégies de sécurité pour renforcer la robustesse et la résilience des systèmes d'information contre les attaques avancées.

IV. Programmes de bug bounty réussis

Nicolas Kalmanovitz, lors de sa présentation sur la sécurité offensive, a également mis en avant l'efficacité des programmes de Bug Bounty. Ces programmes invitent des hackers éthiques à identifier et à signaler des vulnérabilités en échange de récompenses et sont devenus un élément crucial pour améliorer la sécurité des systèmes informatiques des entreprises.

Un programme de Bug Bounty réussi dépend fortement de la qualité de la sélection et de la gestion des chercheurs en sécurité. Par exemple, les programmes privés permettent de contrôler qui teste le système, invitant des chercheurs ayant des compétences spécifiques et une bonne réputation dans la communauté. Cette approche garantit non seulement une expertise adaptée aux technologies utilisées mais aussi une gestion plus sûre des informations sensibles.

Définir clairement le périmètre du test est essentiel. Les règles doivent spécifier ce qui est autorisé à tester et ce qui ne l'est pas, pour éviter toute confusion et garantir que les efforts des chercheurs soient concentrés sur les zones critiques. La communication rapide et efficace avec les chercheurs est vitale. Reconnaître et répondre à leurs rapports rapidement non seulement maintient leur engagement mais renforce également la relation de confiance. Le tri rapide et précis des rapports aide à prioriser et à corriger les vulnérabilités pertinentes dans les meilleurs délais.

Le montant des récompenses doit être attrayant pour motiver les meilleurs talents. Les récompenses doivent être proportionnelles à la gravité des vulnérabilités découvertes, et des ajustements peuvent être nécessaires pour rester compétitifs sur le marché. Le programme doit être juste et transparent, avec des règles clairement définies pour la validation des soumissions et le paiement des récompenses. Les chercheurs doivent sentir que leur travail est valorisé équitablement, ce qui encourage une participation continue et de qualité.

Nicolas a souligné plusieurs exemples de programmes de Bug Bounty qui ont réussi à renforcer la sécurité des entreprises tout en engageant efficacement la communauté des chercheurs en sécurité. Ces programmes ont permis de découvrir des vulnérabilités critiques avant qu'elles ne puissent être exploitées malicieusement, protégeant ainsi les informations et les systèmes d'entreprise contre des attaques potentielles.

Ces initiatives montrent comment la mise en place de programmes de Bug Bounty bien structurés peut contribuer à créer une défense plus robuste contre les menaces de sécurité en constante évolution. En résumé, les programmes de Bug Bounty réussis ne se contentent pas de corriger des failles, ils transforment également la culture de la sécurité des organisations, en faisant de la détection proactive des vulnérabilités une partie intégrante de leur stratégie de sécurité.

V. Présentation de la plateforme 'Kids Can Hack'

La plateforme 'Kids Can Hack' a été conçue pour initier les enfants à la cybersécurité de manière ludique et éducative. Sara Sellos, ingénieur principal des études et techniques de l'armement à la Direction Générale de l'Armement (DGA), a partagé l'objectif de cette initiative lors de sa présentation. Co-créée avec Nicolas Fouville, cette plateforme vise à sensibiliser les enfants aux fondamentaux de la cyber à travers des jeux de hacking.

'Kids Can Hack' offre une expérience unique où les enfants dès 9 ans peuvent découvrir les rudiments du hacking éthique sans avoir besoin de compétences préalables en programmation ou en systèmes informatiques. La plateforme est accessible en ligne et propose 30 défis de hacking éthique, conçus pour être à la fois amusants et éducatifs. Chaque défi est accompagné d'une anecdote réelle, reliant la théorie à la pratique et montrant comment de véritables failles ont été exploitées dans le passé, ce qui renforce le réalisme et l'impact éducatif des activités.

Sara Sellos souligne que ces challenges ne requièrent que des compétences basiques en lecture, écriture et recherche sur Internet, en plus d'une logique et d'une curiosité naturelle. Cela rend la plateforme idéale pour les enfants, leur permettant de développer des compétences critiques tout en s'amusant. Les défis sont classés par niveau de difficulté : facile, moyen et difficile, permettant ainsi aux enfants de progresser à leur propre rythme.

L'importance de 'Kids Can Hack' ne réside pas seulement dans l'acquisition de connaissances techniques mais aussi dans la sensibilisation aux dangers d'Internet. En apprenant le hacking éthique, les enfants deviennent mieux préparés à naviguer en sécurité dans le cyberespace et à reconnaître les cybermenaces potentielles.

Ce projet éducatif reflète également une ambition de diversification et de démocratisation de la cybersécurité. En rendant la cyber plus accessible, Sellos et Fouville espèrent inspirer une future génération de cyberprofessionnels, prêts à relever les défis de demain. C'est une initiative qui non seulement éduque mais encourage également une plus grande inclusion dans le domaine traditionnellement dominé par les hommes, en promouvant la mixité et en brisant les stéréotypes dans les métiers techniques.

Sara Sellos va sortir un cahier de jeux, aux éditions Dunod, pour sensibiliser les enfants et les aider à résoudre les défits de la plateforme Kids can Hack.

VI. Session questions / réponses

Durant cette session, Nicolas Kalmanovitz a répondu à diverses questions concernant les pratiques de bug bounty et de tests d'intrusion. Voici un résumé de ses réponses :

Question 1 : Rétribution des chercheurs en cas de découverte simultanée d'une faille

Généralement, la prime est attribuée au premier rapport validé. Cependant, il existe des cas où des groupes de chercheurs travaillent collectivement et partagent les primes. Ce processus met en avant un écosystème collaboratif et auto-organisé où le partage des connaissances est encouragé.

Question 2 : Objectif des pentests pour durcir les produits

Les tests d'intrusion visent à améliorer la maturité de sécurité des produits. Ils encouragent une amélioration continue au sein des organisations, exigeant des hackers une motivation et une technicité accrues pour compromettre des produits de mieux en mieux sécurisés. L'approche vise à démontrer les vulnérabilités avant qu'un acteur malveillant ne le fasse.

Question 3 : Gestion des connaissances des failles détectées

Les informations sur les failles sont conservées dans des bases de données normalisées, utilisant des référentiels comme les CVE. Cela permet une meilleure communication au sein du système d'information et aide à guider les futurs tests dans d'autres entreprises.

Question 4 : Impact des bug bounties sur la fréquence des incidents de sécurité

Il est difficile de prouver statistiquement que les entreprises pratiquant les bug bounties subissent moins d'incidents de sécurité que celles qui n'en font pas. Cependant, l'engagement des hackers éthiques dans les tests continus est considéré comme crucial pour prévenir les problèmes avant la mise en production.

Question 5 : Position légale sur le pentesting et les risques pour les acteurs éthiques

Le pentesting, souvent réglementé, est encouragé par la loi, surtout lorsqu'il est réalisé par des entités qualifiées. La loi Lemaire de 2016 a amélioré la protection des hackers éthiques, démontrant que leurs actions, si elles sont menées dans un but éthique et rapportées aux autorités compétentes, peuvent les protéger légalement. Toutefois, l'évaluation se fait au cas par cas, rendant parfois difficile la démonstration d'une conduite éthique.

Ces réponses soulignent l'importance d'une gestion rigoureuse et éthique des tests d'intrusion, ainsi que le rôle des législations dans la protection des bonnes pratiques dans ce domaine.

Conclusions et recommandations

Cette session du "Lundi de la Cybersécurité" a offert une perspective approfondie sur les pratiques actuelles et les innovations dans le domaine de la cybersécurité, mettant en avant l'importance des programmes de bug bounty et les initiatives éducatives telles que 'Kids Can Hack'. Ce rassemblement a souligné l'urgence des défis et des opportunités émergentes tout en renforçant l'idée que la sécurité informatique doit être une priorité partagée entre divers acteurs de la société.

La collaboration s'est imposée comme un leitmotiv, où la synergie entre hackers éthiques et entreprises révèle son potentiel pour renforcer significativement la sécurité des systèmes et des produits informatiques. Par ailleurs, l'initiative 'Kids Can Hack' de Sara Sellos illustre parfaitement comment l'éducation précoce peut armer les futures générations contre les risques du numérique, en cultivant dès le plus jeune âge les compétences et la sensibilisation nécessaires.

Au terme de cette session, plusieurs recommandations émergent clairement : il est crucial d'intensifier les efforts de collaboration en encourageant les organisations à adopter et à soutenir des programmes de bug bounty et de tests d’intrusion. Ces programmes doivent être intégrés comme composante essentielle des stratégies de sécurité des entreprises et soutenus par des plateformes offrant des mécanismes équitables pour la reconnaissance et la récompense des découvertes de vulnérabilités.

En parallèle, il convient d'élargir le champ des initiatives éducatives en intégrant la cybersécurité dans les programmes scolaires à différents niveaux éducatifs. Adopter des approches pédagogiques engageantes et interactives permettra de sensibiliser et de former efficacement les jeunes esprits.

Enfin, un renforcement des cadres législatifs et un meilleur soutien aux tests éthiques sont nécessaires pour protéger les droits des chercheurs en cybersécurité tout en sanctionnant les pratiques malveillantes. Il est également impératif de promouvoir une culture où la sécurité est une préoccupation intégrée dès la conception des produits et où la détection continue des vulnérabilités est couramment pratiquée.

Cette session a renforcé la nécessité d'une approche proactive pour assurer la sécurité dans le cyberespace, une tâche qui doit être portée collectivement pour préparer un avenir numérique aussi sûr que possible pour tous.