OG IT CONSULTING

CAS CLIENT D'UN LEADER DU SECTEUR DE LA BANQUE AUX ETATS UNIS

EXERCICE DE SIMULATION D'ATTAQUES CYBER "PURPLE TEAM"
UTILISANT LE CADRE D'ATTAQUE MITRE

La protection de notre patrimoine digital relève de notre devoir. De ce fait, la sécurité au sein d'une entreprise ou institution n'est pas négociable.

Radiatou OURO-GBELE
President & Founder
Cybersecurity Project Manager

SOMMAIRE

WWW.OG-IT-CONSULTING.COM

QUI SOMMES NOUS?

OG IT CONSULTING est une société spécialisée dans le conseil et l'intégration de solutions de cybersécurité.

Nous accompagnons nos clients dans le conseil et la mise en oeuvre de solutions de sécurité de bout en bout. Nos consultants disposent de plusieurs années d'expérience dans le domaine de la cybersécurité.

Notre vision est de prévenir la cybercriminalité et les cyberattaques en accompagnant et en sensibilisant sur les bonnes pratiques de sécurité à adopter.

NOS SERVICES :

- **STRATEGY & RISKS:**
  - Cyber Business Intelligence
  - GRC (Gouvernance, Risque,Conformité)
    - Elaboration d'une PSSI
    - Protection des données
    - Mise en place d'un SMSI
    - Audit des SI et de la sécurité informatique
    - etc...
- **SECOPS** (Sécurité Opérationnelle)
  - Security Assessment
  - Test & Simulation Exercises (intrusion, etc...)
  - Identity (IAM, PAM, PKI)
- **CYBERDEFENSE**
  - Resilience (BIA, PCA et PRA)
  - Vulnerability Assessment
  - Application Security
- **Cyber Assurance & Legal Advisory**
  - Cyber assurance
  - Cyber Legal Advisory
  - On-demand Cyber Forensics & Legal Support
- **ACADEMY**
  - Security Awareness & Training

CAS CLIENT D'UN LEADER DU SECTEUR DE LA BANQUE AUX ETATS UNIS

Exercice de simulation d'attaques cyber "Purple Team" utilisant le cadre d'attaque MITRE

Enjeux:

Le secteur bancaire aux États-Unis et partout dans le monde est confronté à des enjeux majeurs en matière de cybersécurité. Les institutions financières sont de plus en plus ciblées par des attaques informatiques, notamment des ransomwares, en raison de la nature hautement confidentielle des données qu'elles traitent et de leurs nombreuses connexions avec des fournisseurs tiers. Les conséquences d'une cyberattaque peuvent être dévastatrices pour les banques, allant de la perte de données confidentielles à des pertes financières considérables, en passant par la dégradation de la confiance des clients. Ces risques soulignent l'importance cruciale de mettre en place des mesures solides de protection et de détection des cyberattaques.

Il est donc essentiel de maintenir une posture de cybersécurité à jour et adaptée aux dernières menaces...

Un autre enjeu majeur réside dans le fait que les contrôles de cybersécurité de l'entreprise cliente n'avaient pas été évalués depuis un certain temps. La cybersécurité est un domaine en constante évolution, avec de nouvelles techniques d'attaque qui émergent régulièrement. Il est donc essentiel de maintenir une posture de cybersécurité à jour et adaptée aux dernières menaces. L'absence d'évaluation régulière des contrôles de cybersécurité expose l'entreprise à un risque accru, car les vulnérabilités peuvent rester non détectées et non corrigées pendant une longue période.

De plus, la nature des activités bancaires implique une forte interconnexion avec des fournisseurs tiers, tels que les processeurs de paiement, les prestataires de services cloud et les agences de notation de crédit. Cette dépendance accrue vis-à-vis des tiers augmente également les risques de cyberattaques. Les attaquants peuvent exploiter les vulnérabilités présentes chez les fournisseurs tiers pour accéder aux systèmes de l'entreprise cliente. Par conséquent, il est essentiel de mettre en place des mesures de sécurité robustes pour protéger les connexions avec les fournisseurs tiers et s'assurer de leur conformité aux normes de cybersécurité.

Solutions apportées :

Pour répondre aux enjeux auxquels fait face notre client du secteur bancaire, une solution clé a été mise en place : des exercices de simulations d'attaques (Purple Team - «team violette») utilisant le cadre d'attaque MITRE. Ce processus impliquait la coordination les exercices de simulation d'attaques où l'entreprise cliente jouait le rôle de l'équipe bleue et l'expert externe spécialisé en cybersécurité dirigeait l'équipe rouge.

Dans un exercice Purple Team, le concept de la «team violette» fait référence à la collaboration entre le personnel de l'entreprise (l'équipe bleue) chargée de protéger les systèmes contre les attaques et les experts externes (l'équipe rouge) chargés de simuler des attaques. L'objectif est de tester et d'améliorer les capacités de détection, de prévention et de réponse aux

attaques de l'entreprise.
Dans ce cas, l'équipe bleue, composée de membres de l'équipe de cybersécurité de l'entreprise cliente, est chargée de maintenir et de défendre les systèmes de l'entreprise contre les attaques. Leur rôle consiste à mettre en place des mesures de protection et à surveiller les activités suspectes, en utilisant les connaissances et les outils de cybersécurité dont ils disposent. Ils sont responsables de la mise en œuvre des contrôles de sécurité et de la gestion des incidents.

D'un autre côté, l'équipe rouge, composée d'experts externes en cybersécurité qui nous ont accompagné, joue le rôle des attaquants dans l'exercice. Leur mission est de simuler des attaques réelles en utilisant différentes techniques et méthodes d'attaque. Ils explorent les vulnérabilités potentielles, tentent de contourner les contrôles de sécurité et évaluent la capacité de l'équipe bleue à détecter et à contrer ces attaques. Leur objectif n'est pas de nuire réellement à l'entreprise, mais plutôt de mettre en évidence les faiblesses et les lacunes du système afin d'apporter des améliorations et de renforcer la sécurité globale.

En utilisant le cadre d'attaque MITRE, qui fournit une méthodologie structurée pour évaluer les capacités de détection et de réponse aux attaques, l'exercice d'équipe violette offre à l'entreprise cliente une approche complète pour tester et améliorer sa résilience face aux cyberattaques. Les résultats et les recommandations de cet exercice permettent à l'équipe de cybersécurité de l'entreprise d'identifier les vulnérabilités, de renforcer les contrôles de sécurité et d'élaborer des stratégies de prévention et de réponse plus solides.

Résultats :

Ces exercices de simulations ont permis d'obtenir des résultats concrets et mesurables pour l'entreprise cliente dans le renforcement de sa cybersécurité. Voici quelques-uns des résultats clés obtenus :

1. Identification des vulnérabilités : L'exercice a permis d'identifier un certain nombre de vulnérabilités potentielles dans l'environnement de l'entreprise cliente. Par exemple, il a été révélé que certaines machines n'avaient pas les derniers correctifs de sécurité appliqués, exposant ainsi l'entreprise à des risques de cyberattaques. De plus, des configurations incorrectes ont été identifiées sur certains pare- feux, ce qui pouvait permettre aux attaquants de contourner les mesures de sécurité. Ces résultats ont fourni une base solide pour apporter des améliorations et renforcer la posture de cybersécurité de l'entreprise.

2. Recommandations pour les meilleures pratiques de protection : À la suite de l'exercice, des recommandations précieuses ont été formulées à la direction de l'entreprise cliente. Ces recommandations ont porté sur les meilleures pratiques à mettre en œuvre pour protéger l'environnement contre les cyberattaques. Par exemple, il a été suggéré de mettre en place une politique de gestion des correctifs régulière pour s'assurer que tous les systèmes disposent des derniers correctifs de sécurité. De plus, des recommandations ont été faites pour améliorer les configurations des pare-feux et renforcer l'authentification multifactorielle pour les accès sensibles. Ces recommandations ont fourni des orientations claires à l'entreprise cliente pour renforcer sa sécurité et atténuer les risques.

3. Renforcement de la confiance : L'exercice a également renforcé la confiance de l'équipe de cybersécurité de l'entreprise cliente en sa capacité à faire face aux menaces. Les membres de l'équipe ont pu mettre en pratique leurs compétences et tester les mesures de sécurité qu'ils avaient mises en place. En détectant et en contrant avec succès les attaques simulées, l'équipe a gagné en confiance en sa capacité à protéger les systèmes de l'entreprise contre les cyberattaques. Cela a également renforcé la confiance de la direction de l'entreprise dans les investissements réalisés en matière de cybersécurité, en démontrant l'efficacité des mesures prises pour protéger les actifs et les données de l'entreprise.

En conclusion, l'exercice Purple Team utilisant le cadre d'attaque MITRE a permis à notre client d'obtenir des résultats tangibles dans le renforcement de sa cybersécurité. L'identification des vulnérabilités, les recommandations pour les meilleures pratiques de protection et le renforcement de la confiance de l'équipe de cybersécurité ont tous contribué à améliorer la posture de sécurité de l'entreprise. Ces résultats ont permis à l'entreprise cliente de se prémunir contre les cyberattaques, de protéger ses actifs et de maintenir la confiance de ses clients.

OG IT CONSULTING

+33 6 69 50 78 02
contact@og-it-consulting.com
www.og-it-consulting.com
Paris, France