PEN TESTS ET AUDIT DE CYBERSÉCURITÉ EXEMPLE DE RÉUSSITE

Tests d'intrusion et audit de cybersécurité

SURVOL

Le client voulait évaluer la robustesse de son infrastructure technologique et la maturité de sa sécurité organisationnelle en tenant compte du nouveau cadre établi par le ministère de la Santé et des Services sociaux.

ESI a évalué la posture de l'organisation en matière de sécurité informatique, les opérations de sécurité de l'information et a également effectué divers tests d'intrusion.

L'objectif général de ce mandat étaitd'offrir l'accompagnement et les conseils nécessaires afin d'assurer au client une visibilité sur ses réseaux locaux qui repose sur les meilleures pratiques en cybersécurité.

Le mandat comportait la mise à l'épreuve des réseaux informatiques par des tests d'intrusion, la rédaction et la mise à jour de politiques de sécurité,l'accompagnement pour la mise en œuvre de correctifs et la sensibilisation du personnel afin de mieux prévenir les risques.

DÉFIS

1. Criticité des résultats et valeur du rapport – niveau exécutif, fonctionnel et technique
2. Complexité technologique et exigences des méthodes utilisées
3. Nécessité de travailler avec des équipes diversifiées à tous les niveaux de l'organisation, des décideurs aux équipes techniques
4. Nécessité de fournir une vue d'ensemble la plus exacte possible pour un réseau étendu de sites

Tests d'intrusion et audit de cybersécurité

Histoire d'une réussite

GARDIEN VIRTUEL

RÉSULTATS

- ESI a réalisé un rapport technique détaillé destiné aux experts en sécurité ainsi qu'une version stratégique pour la haute direction qui a été incorporée au rapport d'audit général.

- L'implication d'ESI dans le projet a permis de dresser une feuille de route efficace et intelligente afin de limiter les vulnérabilités de cybersécurité.

Analyse stratégique

Feuille de route intelligente

NOTRE CONTRIBUTION

Notre équipe s'est appuyée sur une méthodologie en deux étapes menées en parallèle : audit par ateliers et tests d'intrusion. Tout d'abord, dès que le protocole d'intervention a été approuvé par le client, nous avons mené une série d'entretiens avec les équipes responsables des différents services. Ces ateliers nous ont permis de recueillir les données nécessaires sur la cybersécurité en tenant un registre complet des preuves fournies et en les classant.Pour compléter cette phase d'information, nous avons effectué des tests de défaillance afin de détecter les vulnérabilités susceptibles d'être attaquées. L'un des défis majeurs de ce mandat était l'importance de la confidentialité totale des données.

Nous avons évalué la posture de sécurité du client selon trois grands axes d'intervention. D'abord, par des rencontres avec les équipes opérationnelles pour analyser le déroulement de leurs activités quotidiennes. Ensuite, des rencontres avec les gestionnaires de services pour obtenir un portrait de la situation qui prévalait. Finalement, suite à différents incidents reliés à la cybersécurité, une compilation des résultats pour fournir au client un portrait des aspects positifs et des éléments à corriger pour améliorer la posture en cybersécurité de l'organisation et de ses nombreux réseaux régionaux.

Le rapport produit incluait un plan de remédiation, des indicateurs mesurables et des conseils pour l'optimisation de la structure opérationnelle. Les résultats ont été présentés à huis clos aux directeurs informatiques concernés, dont le dirigeant responsable.

En raison de l'étendue du réseau et de l'importance de préserver la confidentialité des informations du client, nos spécialistes ont obtenu des sauf-conduit en cas de problèmes avec les responsables de la sécurité physique des différents établissements.

Les tests d'intrusion ont été effectués en mode « boîte noire », notamment par l'installation de sondes sur des postes de travail laissés sans surveillance ou encore des accès à des salles de raccordement. Une fois l'accès au réseau obtenu, le conseiller a procédé aux balayages ainsi qu'à l'évaluation des failles de sécurité.

Par la suite, la gravité des failles détectées a été évaluée selon les indices des référentiels CVSS et de l'OWASP.

L'exercice a été répété pour l'ensemble des réseaux internes et externes. Les équipements médicaux, pour des raisons évidentes de protection du public, ont été exclus de la portée.