Cour des comptes
République et canton de Genève

RÉALISATION DE TESTS DE PÉNÉTRATION INFORMATIQUE DANS LES ORGANISATIONS PUBLIQUES

Expertise

La Cour des comptes s'attache à moderniser ses pratiques pour répondre aux enjeux actuels des institutions publiques. Dans le cadre d'une récente mission d'audit de performance sur la cybersécurité d'une institution genevoise, la Cour a réalisé des tests de pénétration informatique (« *pentests* »). Elle partage ici quelques observations générales.

Conformément au cadre légal (art. 43 Lsurv) et face aux évidents risques pour l'institution et ses usagères et usagers, la Cour a fait le choix de ne pas publier d'information sur l'entité auditée ni aucun détail sur les résultats de l'audit.

Une approche technique et des résultats concrets

Un test de pénétration ou test d'intrusion consiste à évaluer la sécurité d'un système d'information (SI) en reproduisant les actions d'un attaquant réel afin d'identifier des vulnérabilités et essayer de les exploiter. Contrairement à un audit classique, qui repose sur des entretiens et une revue documentaire, le *pentest* se concentre uniquement sur le résultat final : l'efficacité des mesures défensives en place.

Pour cet audit, les tests ont été découpés en trois phases visant à couvrir des périmètres différents :

- Le périmètre exposé à internet et donc aux menaces venant du monde entier ;
- La robustesse des postes informatiques des collaborateurs et ;
- Le réseau informatique interne.

Des vulnérabilités identifiées et rapidement corrigées

Ce type d'exercice est particulièrement utile pour les audités puisqu'il permet d'identifier et de démontrer l'existence de vulnérabilités réelles. Les résultats des tests peuvent facilement être analysés par l'institution concernée qui sait précisément où se situent les faiblesses et peut ainsi apprécier leurs impacts. Souvent réalisés en collaboration directe avec les audités, les *pentests* favorisent également le dialogue entre les principales équipes concernées : sécurité informatique, gestion la production et de l'infrastructure informatique et direction. C'est exactement ce qui s'est passé dans le cadre de l'audit.

Les pirates informatiques ne prennent pas de vacances

Les périodes en dehors des heures ouvrées sont souvent choisies par les *hackers*. Environ 50 % des cyberattaques ont lieu en dehors des heures de bureau (nuits, fins de semaine ou jours fériés). Or, les institutions n'ont pas toujours les moyens d'assurer des services permanents, il serait pourtant primordial qu'elles puissent disposer de capacités de détection et de réponse 24/7.

Face aux contraintes budgétaires et à la rareté des ressources humaines spécialisées, il existe un défi important. Des solutions hybrides peuvent toutefois être envisagées : renforcement des équipes internes, mise en place d'un piquet et recours à des prestataires externes spécialisés pour assurer la surveillance et la capacité de réponse.

Le facteur humain et l'importance de la formation

Quelles que soient les mesures techniques mises en œuvre, un usage inapproprié des outils informatiques par une utilisatrice ou un utilisateur qui se ferait piéger par exemple, peut suffire à rendre possible une cyberattaque.

Antivirus, pare-feu, systèmes de détection d'intrusion, authentification renforcée, outils de surveillance constituent aujourd'hui des composantes essentielles des dispositifs de cybersécurité. Ces protections peuvent être contournées lorsqu'une personne dument habilitée est amenée, volontairement ou non, à effectuer une action inappropriée : en cliquant sur un lien hypertexte malveillant reçu par courriel, un membre du personnel peut involontairement rendre possible la compromission de l'ensemble de l'infrastructure informatique.

Ainsi, il est nécessaire de rappeler l'importance que toutes les utilisatrices et tous les utilisateurs des systèmes d'information (personnels internes ou prestataires) disposant d'un accès aux ressources informatiques de l'organisation, soient régulièrement sensibilisés aux principaux risques et aux comportements attendus et ceux à proscrire.

Le risque cyber doit être traité au bon niveau de l'organisation

La gestion des risques cyber constitue un exercice d'équilibre permanent entre les coûts et les bénéfices. Chercher à éliminer l'ensemble des risques n'est ni réaliste ni économiquement justifié. Toutefois, il arrive que les instances dirigeantes ne disposent pas toujours d'une vision claire du niveau de protection réellement atteint par l'organisation. Au-delà de la connaissance des mesures mises en œuvre, il est essentiel de comprendre les limites de ces dispositifs, les vulnérabilités non couvertes et les conséquences potentielles des scénarios les plus critiques. Cette visibilité permet aux responsables de prendre des décisions éclairées concernant l'allocation des ressources, les priorités d'investissement et le niveau de risque que l'institution est prête à accepter.

Clément REMARS, Responsable d'audit informatique