Cour des comptes
République et canton de Genève

Réalisation de tests de pénétration informatique dans les organisations publiques

Rapport n°206

4 septembre 2026

SYNTHÈSE

AUDIT DE PERFORMANCE

Au service d'une action publique performante

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

La Cour des comptes est chargée du contrôle indépendant et autonome des services et départements de l'administration cantonale, du pouvoir judiciaire, des institutions cantonales de droit public, des organismes subventionnés ainsi que des institutions communales. Elle a également pour tâche l'évaluation des politiques publiques et assure la révision des comptes de l'État.

La Cour des comptes vérifie d'office et selon son libre choix la légalité des activités et la régularité des recettes et des dépenses décrites dans les comptes, et s'assure du bon emploi des crédits, fonds et valeurs gérés par les entités visées par ses missions. La Cour des comptes peut également évaluer la pertinence, l'efficacité et l'efficience de l'action de l'État. Elle organise librement son travail et dispose de larges moyens d'investigation. Elle peut notamment requérir la production de documents, procéder à des auditions, à des expertises, se rendre dans les locaux des entités concernées.

Le champ d'application des missions de la Cour des comptes s'étend aux entités suivantes :

- l'administration cantonale comprenant les départements, la chancellerie d'État et leurs services ainsi que les organismes qui leur sont rattachés ou placés sous leur surveillance ;
- les institutions cantonales de droit public ;
- les entités subventionnées ;
- les entités de droit public ou privé dans lesquelles l'État possède une participation majoritaire, à l'exception des entités cotées en bourse ;
- le secrétariat général du Grand Conseil ;
- l'administration du pouvoir judiciaire ;
- les autorités communales, les services et les institutions qui en dépendent, ainsi que les entités intercommunales.

Les rapports de la Cour des comptes sont rendus publics : ils consignent ses observations, les conclusions de ses investigations, les enseignements qu'il faut en tirer et les recommandations conséquentes. La Cour des comptes prévoit en outre de signaler dans ses rapports les cas de réticence et les refus de collaborer survenus au cours de ses missions.

La Cour des comptes publie également un rapport annuel comportant la liste des objets traités, celle de ceux qu'elle a écartés, celle des rapports rendus avec leurs conclusions et recommandations et les suites qui y ont été données. Les rapports restés sans effet ni suite sont également signalés.

Vous pouvez participer à l'amélioration de la gestion de l'État en prenant contact avec la Cour des comptes. Toute personne, de même que les entités comprises dans son périmètre d'action, peuvent communiquer à la Cour des comptes des faits ou des pratiques qui pourraient être utiles à l'accomplissement des tâches de cette autorité.

Prenez contact avec la Cour par téléphone, courrier postal ou électronique.

Cour des comptes
Route de Chêne 54, 1208 Genève | 022 388 77 90 | info@cdc-ge.ch | www.cdc-ge.ch

Table des matières

1. Cadre et contexte de la publication

La Cour a réalisé un audit de performance sur la cybersécurité d'une entité entrant dans son périmètre de contrôle.

Selon l'article 43 de la loi sur la surveillance de l'État, du 13 mars 2014, (LSurv, rs/GE D 1 09), si la Cour des comptes rend publics ses rapports (al. 1), elle détermine l'étendue des informations contenues dans lesdits rapports, en tenant compte des intérêts publics et privés susceptibles de s'opposer à la divulgation de certaines informations (al. 4).

En matière de cybersécurité, la publicité liée à d'éventuelles vulnérabilités ou faiblesses présente un risque de sécurité très important pour l'entité concernée. De surcroît, un éventuel constat positif quant aux dispositifs de sécurité en place pourrait être considéré comme un défi pour des pirates informatiques voulant se mettre en avant.

Considérant ce qui précède, la Cour n'est donc pas en mesure de rendre public le rapport considéré, à plus forte raison de publier des informations relatives à l'entité auditée, aux constats et aux recommandations du cas d'espèce, ainsi qu'aux mesures mises en place pour assurer sa sécurité informatique. Cependant, certaines observations ressorties de ces travaux peuvent être utiles à l'ensemble des organisations publiques. Elles sont présentées ci-dessous, après une présentation succincte des travaux réalisés.

2. La réalisation de tests de pénétration par la Cour

2.1. Une approche concrète et utile pour les audités

2.1.1 Pourquoi faire un test de pénétration ?

Un test de pénétration ou test d'intrusion, appelé communément « *pentest*[1] », consiste à évaluer la sécurité d'un système d'information en reproduisant les actions d'un pirate informatique afin d'identifier des vulnérabilités et essayer de les exploiter. Contrairement à un audit classique, qui repose principalement sur des entretiens, une revue documentaire et l'analyse des contrôles en place, le test de pénétration se concentre uniquement sur le résultat final : l'efficacité des mesures défensives en place. Il permet ainsi de valider en pratique la robustesse des dispositifs de sécurité et de mesurer leur capacité à résister à des attaques réelles.

Souvent réalisés en collaboration directe avec les équipes de sécurité informatique, les *pentests* favorisent également le dialogue entre les principales équipes concernées : sécurité informatique, gestion de la production et de l'infrastructure informatique et direction.
Cette approche est complémentaire à d'autres mécanismes souvent mis en place par les institutions afin de garantir la bonne sécurité du système d'information (SI), tels que des évaluations du contrôle interne ou la mise en conformité avec la norme ISO 27'001. Cette dernière évalue principalement la gouvernance de la cybersécurité et la mise en place d'un système de gestion adapté. Elle ne se prononce en revanche pas sur l'efficacité des mécanismes, l'absence de vulnérabilités techniques ni la capacité réelle des dispositifs en place à résister à une attaque.

2.1.2 Une approche technique et concrète

<u>Des compétences spécifiques</u>

Pour mettre en œuvre cette approche d'audit innovante, la Cour a profité du renforcement, ces dernières années, de ses équipes d'audit informatique, lesquelles bénéficient de plusieurs certifications en sécurité des systèmes d'information. En complément, et afin de disposer d'une expertise opérationnelle à jour sur les différentes techniques de piratage informatique, la Cour a fait appel à une entreprise spécialisée, après une mise en concurrence de plusieurs acteurs de la cybersécurité en Suisse romande. Considérant la sensibilité des travaux demandés, des mesures particulières de sécurité ont été prises par la Cour (clause de confidentialité[2], protocole strict d'échange d'informations, etc.).

Le recours à des spécialistes a permis de bénéficier d'une expertise technique approfondie grâce à des personnes qui se consacrent exclusivement à ce type d'exercices, ce qui leur permet de maintenir un haut niveau de compétence, de rester à jour face à l'évolution des menaces et d'utiliser des outils actuels et performants.

[1] En référence à l'anglais « *penetration testing* ».
[2] Outre la soumission, de par la loi (art. 41 LSurv), au secret professionnel en tant que mandataire extérieur.

Des scénarios portant sur plusieurs aspects du système d'information

La Cour a choisi de découper ses tests en trois phases ou trois scénarios, afin de couvrir des périmètres différents de la sécurité informatique :

- Le périmètre exposé à internet,
- La robustesse des postes informatiques à disposition du personnel,
- Le réseau informatique interne.

Les scénarios sont détaillés en annexe (voir chapitre 4 de cette synthèse).

2.1.3 L'identification de vulnérabilités réelles

Les tests d'intrusion permettent d'identifier et de démontrer l'existence de vulnérabilités réelles et d'évaluer s'il est possible pour un pirate informatique de les exploiter. Les résultats des tests peuvent facilement être analysés par l'organisation publique concernée qui sait précisément où se situent les faiblesses et peut ainsi apprécier leurs impacts. En plus d'être très concrètes, ces observations correspondent souvent aux attaques les plus fréquentes et donc les plus probables. La priorisation des mesures correctives est également facilitée.

Dans le cadre de la mission de la Cour, les résultats des tests réalisés ont permis de mettre en évidence un niveau de sécurité globalement suffisant, même si plusieurs pistes d'amélioration ont pu être mises en œuvre rapidement afin de renforcer ce niveau de sécurité. Certaines vulnérabilités ont pu être corrigées dans les jours suivant leur identification, réduisant ainsi de manière presque immédiate la surface d'attaque possible. Au-delà des corrections ponctuelles, les enseignements tirés de ces travaux contribuent à renforcer durablement les pratiques de sécurité et la résilience de l'organisation face aux cybermenaces.

3. Plusieurs observations d'ordre général

Comme évoqué en introduction de ce document, la Cour ne peut pas détailler les observations concrètes faites durant cet audit, pour ne pas communiquer des informations susceptibles d'exposer l'entité concernée à des attaques informatiques et, finalement, de mettre en péril sa sécurité informatique. Cependant, en se basant sur cet exercice ainsi que sur des interventions précédentes dans diverses institutions publiques genevoises, la Cour souhaite partager ici quelques observations d'ordre général.

3.1. La réalisation de tests de pénétration par les entités elles-mêmes : une pratique à renforcer

3.1.1 Des tests qui se limitent souvent à certains actifs clés, notamment ceux exposés à internet

Les institutions publiques genevoises ont commencé à intégrer les tests de pénétration parmi les mesures visant à évaluer et renforcer la sécurité de leurs systèmes d'information. Cette pratique constitue aujourd'hui un élément important des dispositifs de cybersécurité et témoigne d'une prise de conscience croissante des risques numériques.

Il peut cependant exister un risque que les tests réalisés ne couvrent pas tous les périmètres et se limitent par exemple aux principales applications métiers et aux services exposés sur internet.

Si cette approche est cohérente puisqu'elle vise à couvrir en priorité les risques les plus immédiats (les vulnérabilités exploitables depuis l'extérieur), il est nécessaire qu'elle soit enrichie, pour permettre de couvrir une large partie, voire la totalité, des scénarios d'attaque auxquels les organisations publiques sont confrontées.

En effet, l'évolution rapide de la menace cyber invite désormais à adopter une vision plus large. Les attaques sont de plus en plus fréquentes, sophistiquées et diversifiées. Elles exploitent non seulement les systèmes accessibles depuis internet, mais également les faiblesses internes, les erreurs de configuration, les comptes compromis ou encore les interactions entre différents composants du système d'information. Par exemple, le fait que des identifiants et mots de passe de comptes administrateurs puissent être trouvés sur le réseau interne ne permet pas une attaque directement depuis internet mais ils pourraient être facilement utilisés dans un second temps, si les pirates informatiques arrivent à pénétrer le premier rideau de défense et à accéder au réseau interne.

Dans ce contexte, les organisations doivent veiller à ce que leurs programmes de tests de pénétration couvrent l'ensemble du système d'information. Les infrastructures internes, les réseaux, les environnements bureautiques, les systèmes d'administration ainsi que les processus liés à la gestion des identités et des accès devraient faire l'objet d'évaluations régulières, selon des priorités à définir en fonction des risques et des moyens à disposition. Une telle approche permettrait d'obtenir une vision plus complète du niveau de sécurité réel de l'organisation et de sa capacité à résister à différents types d'attaques.

3.1.2 L'émergence de l'intelligence artificielle au service des pirates informatiques

Depuis plusieurs années, un phénomène nouveau rend le travail des équipes de sécurité de plus en plus compliqué. L'intelligence artificielle (IA) est de plus en plus utilisée par des personnes ou groupes à des fins malveillantes. L'IA offensive, comme elle est appelée, renforce le besoin de réaliser des tests de pénétration de plus en plus poussés. En effet, les attaquants utilisent désormais l'IA pour automatiser la découverte de failles, personnaliser les attaques d'hameçonnage à grande échelle et accélérer la vitesse d'exécution de leurs attaques. Pour y faire face, la stratégie de test des organisations doit dorénavant réduire l'espace de temps entre deux *pentests*.

Ainsi, les organisations devraient envisager de passer progressivement d'une logique de tests ponctuels à une logique de validation en continu de l'efficacité des mesures en place. Il s'agirait concrètement d'utiliser des outils automatisés testant en permanence différents périmètres du système d'information[3].

3.2. Les pirates informatiques ne prennent pas de vacances

3.2.1 Des cyberattaques permanentes

Les périodes en dehors des heures ouvrées sont souvent choisies par les *hackers* pour réaliser leurs attaques. Ils profitent ainsi de créneaux durant lesquels les moyens de défense de leurs cibles sont plus limités en ressources. Plusieurs études issues d'acteurs reconnus de la cybersécurité montrent qu'au niveau mondial, environ 50 % des cyberattaques sont menées en dehors des horaires de bureau, notamment durant les nuits, les week-ends ou les jours fériés.

À titre d'exemple, une étude publiée par Semperis indique que plus de la moitié des attaques par rançongiciel surviennent durant les fins de semaines ou les vacances (*Semperis*, 2025, *« Ransomware Holiday Risk Report »*[4]). De même, une analyse des activités de plusieurs centres opérationnels de sécurité réalisée par *Arctic Wolf*[5] confirme cette tendance et met en évidence qu'environ 51 % des alertes de sécurité sont générées en dehors des heures ouvrées.

Ainsi, il apparaît primordial pour les organisations de disposer de capacités de détection et de réponse aux cyberattaques en dehors des heures de travail afin de maintenir l'exposition à un niveau de risque qu'elle accepte. Un manque de ressources sur certaines périodes peut entraîner des délais de détection prolongés, laissant aux attaquants d'avantage de temps pour compromettre des systèmes, exfiltrer des données ou établir des mécanismes plus élaborés.

---

[3] Les outils automatisés de pénétrations informatiques reprennent la même logique que des tests traditionnels sauf qu'ils s'exécutent en quelques heures et peuvent être rejoués régulièrement. Ils scannent d'abord les réseaux ou les applications pour détecter les failles de sécurité connues. Ensuite, ils comparent ces failles à une base de données de codes malveillants pour simuler des attaques informatiques. Enfin, ils génèrent un rapport détaillé qui liste les failles trouvées et propose des solutions pour les corriger.

[4] Disponible à l'adresse - https://www.semperis.com/wp-content/uploads/resources-pdfs/reports/resources-semperis-ransomware-holiday-risk-report.pdf.

[5] *Arctic Wolf*, *2025*, *« Security Operations Report »* disponible à l'adresse https://arcticwolf.com/resource/aw/security-operations-report-2025.

3.2.2 Une capacité de réponse 24/7 difficile à mettre en œuvre

Face à ces attaques permanentes, les entités doivent trouver des moyens techniques et organisationnels appropriés pour garantir, en tout temps, la sécurité de leurs systèmes d'information et, *in fine*, assurer la délivrance des prestations publiques.

Dans un contexte budgétaire limité, il n'est pas toujours aisé d'obtenir le financement nécessaire pour mettre en place une organisation suffisante et recruter du personnel. Au-delà des coûts, les ressources humaines spécialisées en sécurité des SI sont rares et les entités publiques sont, dans ce domaine, en concurrence directe avec le secteur privé pour attirer les talents.

Ainsi, les organisations publiques doivent souvent composer avec leurs contraintes budgétaires, la rareté des ressources humaines et la difficulté d'attirer les talents qui pourraient être amenés à travailler les soirs, les nuits ou les fins de semaine. Dans ce contexte, des solutions hybrides peuvent être envisagées : renforcement des équipes internes, mise en place d'un piquet et recours à des prestataires externes spécialisés pour assurer la surveillance sur certaines tranches horaires par exemple. Il peut également être envisagé que la prestation externe ne se limite pas à la surveillance mais qu'elle s'étende à une capacité de réponse, par exemple en intervenant directement sur le système d'information pour désactiver un accès. Cette configuration induit cependant de nouveaux risques, puisque l'on donne des droits étendus ou d'administration à une entreprise externe, qu'il s'agit d'analyser au regard des bénéfices espérés.

3.3. 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. Compte tenu de la complexité des systèmes d'information, de l'évolution constante des menaces et des ressources des organisations qui ne sont pas illimitées, il n'est ni réaliste ni économiquement justifié de chercher à éliminer l'ensemble des risques ou à couvrir l'ensemble des menaces. Toute organisation est amenée à effectuer des arbitrages entre les coûts, les contraintes opérationnelles et le niveau de sécurité recherché. La question n'est donc pas de savoir si un risque existe, mais plutôt de déterminer quels risques doivent être réduits, lesquels doivent être surveillés et lesquels sont acceptés en connaissance de cause.
Dans le cadre de ses divers travaux, la Cour a pu observer que certaines vulnérabilités identifiées étaient déjà connues des équipes techniques. Dans plusieurs cas, leur correction nécessitait des investissements importants et des modifications complexes des systèmes existants ou présentait des contraintes opérationnelles significatives. Les équipes concernées avaient alors fait le choix de ne pas traiter immédiatement ces vulnérabilités, considérant que les efforts requis étaient disproportionnés au regard des bénéfices attendus ou que d'autres priorités devaient être traitées en premier lieu.

Il ne revient pas à la Cour de remettre en cause la pertinence de ces décisions, qui relèvent de la gestion courante des systèmes d'information. Elle constate toutefois que ces situations traduisent *de facto* une acceptation du risque, laquelle n'est pas toujours portée à la connaissance des niveaux décisionnels appropriés, voire pas formalisée.

Or, une gouvernance efficace de la cybersécurité suppose que les instances dirigeantes et de surveillance disposent d'une vision claire du niveau de protection souhaité et 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'organisation est prête à accepter.

Dans cette perspective, les risques résiduels devraient faire l'objet d'un suivi structuré et être régulièrement présentés aux différentes instances de gouvernance. Les risques les plus significatifs, notamment ceux susceptibles d'avoir un impact important sur l'atteinte des objectifs de l'organisation, la confidentialité des données ou la continuité des activités et prestations publiques, devraient être explicitement portés à la connaissance des organes compétents. Une telle démarche permet de s'assurer que l'acceptation d'un risque résulte d'une décision consciente et documentée, prise au niveau approprié de l'organisation. Elle contribue également à renforcer la transparence, la responsabilité et la maîtrise globale du risque cyber au sein des entités publiques.

3.4. L'importance de la formation et de la sensibilisation de l'ensemble des membres du personnel

On dit souvent que la cybersécurité est l'affaire de tout le monde au sein d'une organisation. En effet, 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 et outils de surveillance constituent aujourd'hui des composantes essentielles des dispositifs de cybersécurité. Toutefois, les tests réalisés par la Cour ont montré que ces protections peuvent être contournées lorsqu'une personne dûment habilitée est amenée, volontairement ou non, à effectuer une action qui se révèlerait malveillante. Lors du test d'un scénario d'hameçonnage, il a été démontré qu'en cliquant sur un lien hypertexte reçu par courriel, un membre du personnel pourrait involontairement rendre possible la compromission de la majeure partie, voire de l'ensemble, de l'infrastructure informatique.

Aussi est-il nécessaire de rappeler l'importance que toutes les utilisatrices et tous les utilisateurs des systèmes d'information (personnel interne ou prestataires) disposant d'un accès aux ressources informatiques de l'organisation, soient sensibilisés et formés aux principaux risques, aux comportements attendus et ceux à proscrire. Ces sensibilisations et formations doivent être régulières afin de tenir compte de l'évolution des menaces et des techniques employées par les pirates. Elles doivent également être adaptées aux différents profils d'utilisatrices et d'utilisateurs afin de garantir une compréhension concrète des risques auxquels elles et ils sont exposés dans leurs activités quotidiennes.

Enfin, des campagnes simulées d'hameçonnage permettent d'évaluer périodiquement la vigilance des utilisatrices et des utilisateurs dans des conditions proches de la réalité. Elles offrent l'opportunité d'identifier les secteurs pour lesquels un renforcement de la sensibilisation est nécessaire et permettent de mesurer l'efficacité des actions menées au fil du temps. Utilisées dans une logique d'amélioration continue, ces simulations contribuent à développer une véritable culture de cybersécurité au sein des organisations et à renforcer leur capacité à faire face aux menaces actuelles.

3.5. Quasi-absence de mesure technique visant à mitiger le risque de perte de données

La LIPAD et le RIPAD

À Genève, les institutions publiques cantonales, communales et intercommunales sont soumises à la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) du 5 octobre 2001[6] et au règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD) du 21 décembre 2011[7]. Ces deux textes sont largement inspirés des règles fédérales en la matière[8].

Concernant la sécurité des données, la LIPAD vise à poser des principes généraux : « *Les données personnelles* ***doivent être protégées*** *contre tout traitement* ***illicite par des mesures organisationnelles et techniques appropriées*** »[9].

Les évolutions du cadre juridique international et national[10] ont conduit à une révision importante de la LIPAD, adoptée le 3 mai 2024 par le Grand Conseil (L 13347). La date d'entrée en vigueur de cette nouvelle loi doit encore être fixée par le Conseil d'État et une adaptation du RIPAD est en cours. Cette révision de la LIPAD ne prévoit pas de changements fondamentaux en ce qui concerne les mesures techniques et organisationnelles nécessaires à la sécurité des données personnelles. Cependant, la modification du RIPAD en cours de consultation précise plusieurs exigences, notamment la possibilité de détecter rapidement les violations de la sécurité des données.

Quasi-absence de mesures techniques quant à la fuite ou la perte de données

Au travers de l'analyse du poste utilisateur (ordinateur portable) réalisée dans le cadre d'un test d'intrusion, la Cour note que, de manière générale, peu de dispositifs techniques sont en place visant à (1) prévenir ou (2) identifier d'éventuelles pertes ou fuites de données. Plus spécifiquement, les éléments suivants ont retenu l'attention de la Cour :

- La quasi-absence de blocages techniques ou d'alertes lors du transfert de documents, quels que soient leur niveau de sensibilité et le média utilisé (ports USB, courriel, impression, transferts vers des solutions de stockage en ligne, etc.) ;
- Le nombre insuffisant de scénarios visant à détecter d'éventuels exports en masse ;
- L'absence d'outil de classification des documents selon la criticité des informations qu'ils contiennent.

[6] rs/GE A 2 08. Entrée en vigueur le 1er mars 2002 en ce qui concerne l'aspect transparence. La réforme des règles sur la protection des données a été introduite par la loi 9870 du 9 octobre 2008, entrée en vigueur le 1er janvier 2010.
[7] rs/GEA 2 08.01. Entré en vigueur le 29 décembre 2011.
[8] Principalement composé des dispositions de la loi fédérale sur la protection des données (LPD, RS 235.1) et de son ordonnance (OPDo, RS 235.11).
[9] Art. 37, al. 1 LIPAD.
[10] En particulier le protocole d'amendement de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel. Sur ces questions, voir l'exposé des motifs du projet de loi 13347, p. 25-30, https://ge.ch/grandconseil/data/texte/PL13347.pdf.

Cette observation fait écho à un précédent constat de la Cour dans son rapport sur « La sécurité des données personnelles sensibles en Ville de Genève » (Rapport n°198, 14 octobre 2025)[11].

En vue du renforcement des exigences légales et réglementaires, la Cour encourage les organisations publiques à évaluer l'opportunité de renforcer les mesures techniques de prévention et de détection de perte et de fuite de données et de s'assurer que les mesures décidées soient cohérentes avec l'appétence au risque (défini ou à définir).

[11] Disponible à l'adresse : https://cdc-ge.ch/publications/n-198-audit-de-conformite-relatif-a-la-securite-des-donnees-personnelles-sensibles-en-ville-de-geneve/.

4. Annexe

4.1. Présentation des trois phases de tests réalisés par la Cour

Phase 1 : le périmètre extérieur

Le premier scénario vise à simuler une attaque depuis l'extérieur du système d'information et de communication (SIC). Le pirate ne dispose d'aucune information autre que celles disponibles publiquement et doit tenter d'attaquer le SIC depuis internet. Il s'agit de la partie la plus exposée d'un système d'information.

La première étape, appelée *footprinting*, consiste à essayer de recueillir des informations techniques sur l'organisation (domaine, adresses IP, systèmes d'exploitation, etc.) afin de cartographier l'environnement informatique et les systèmes existants. Ensuite, l'ensemble des ports informatiques sont scannés par des outils dédiés afin de déterminer s'il existe des services ou des protocoles non sécurisés qui peuvent être exploités. Enfin, pour chaque vulnérabilité identifiée, une analyse manuelle est réalisée afin de déterminer la possibilité réelle d'exploitation de cette faille et, le cas échéant, son impact potentiel.

Phase 2 : la configuration des ordinateurs des membres du personnel

Cette phase consiste à apprécier le niveau de sécurité des postes de travail fournis par l'organisation aux membres du personnel (ordinateur portable).

Le scénario vise à simuler une utilisatrice ou un utilisateur qui se serait fait compromettre par l'ouverture d'un programme informatique malveillant reçu au travers d'un courriel piégé. Les deux principaux objectifs sont (1) de voir dans quelle mesure il était techniquement possible de corrompre le poste ou les identifiants de l'utilisatrice ou de l'utilisateur et (2) d'apprécier plus globalement la configuration et les outils de sécurisation installés sur le PC.

Phase 3 : le réseau informatique interne

Ce dernier scénario vise à apprécier le niveau de sécurité et d'étanchéité du réseau interne. À partir du PC et des identifiants de tests obtenus lors de la phase précédente, l'objectif est de déterminer s'il est possible d'atteindre d'autres composants du réseau informatique (serveur, machine, dossier partagé, etc.) et de les corrompre ou d'en devenir administrateur.

Cour des comptes
République et canton de Genève

Vous pouvez participer à l'amélioration de la gestion de l'État en prenant contact avec la Cour des comptes.

Toute personne, de même que les entités comprises dans son périmètre d'action, peuvent communiquer à la Cour des comptes des faits ou des pratiques qui pourraient être utiles à l'accomplissement des tâches de cette autorité.

La Cour des comptes garantit l'anonymat des personnes qui lui transmettent des informations.

Vous pouvez prendre contact avec la Cour des comptes par téléphone, courrier postal ou électronique.

Cour des comptes
Route de Chêne 54, 1208 Genève | 022 388 77 90
info@cdc-ge.ch | www.cdc-ge.ch

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX