AUDIT

Protection des infrastructures critiques – Rapport de synthèse des audits précédents axés sur la cyberrésilience

Office fédéral de la protection de la population, Office fédéral de la cybersécurité, Secrétariat d'État à la politique de sécurité

L'ESSENTIEL EN BREF

Les infrastructures critiques telles que l'approvisionnement en électricité, les soins médicaux ou les télécommunications sont essentielles au fonctionnement de l'économie et à la subsistance de la population. La protection des infrastructures critiques (PIC) revêt une grande importance.

Aujourd'hui, il n'est plus possible d'exploiter des infrastructures critiques sans recourir aux technologies numériques connectées. Cela accroît aussi la probabilité de cyberattaques et la cybersécurité joue un rôle clé dans la PIC. Dans ce contexte, le Contrôle fédéral des finances (CDF) a analysé un échantillon de neuf audits antérieurs (voir annexes 4 et 5) portant sur la PIC et axés sur la cyberrésilience. Le CDF en a déduit sept facteurs de réussite pour une cybersécurité et une surveillance efficaces :

Facteurs de réussite en matière de cybersécurité	Facteurs de réussite en matière de surveillance
Définir clairement les rôles et les responsabilités	Élaborer des directives contraignantes avec la participation des secteurs et des échelons fédéraux
Ancrer et mettre en œuvre les mises à jour des systèmes et les cycles de vie dans les contrats de maintenance	Assurer la communication et la diffusion des informations en cas d'incidents
Protéger les composants critiques de manière appropriée contre les accès virtuels et physiques	Surveiller et contrôler de près les mesures de résilience
S'exercer à mettre en œuvre les plans et les organisations d'intervention d'urgence	

La cybersécurité peut déjà être améliorée avec des mesures « simples »

Souvent, des mesures simples peuvent déjà contribuer de manière significative à une meilleure cyberrésilience. Ainsi, une organisation bien structurée avec des rôles et des responsabilités clairement définis peut avoir un effet positif sur la mise en œuvre des processus liés à la sécurité. Une protection adéquate contre l'accès non autorisé aux systèmes et/ou aux composants critiques améliore considérablement la sécurité. En fin de compte, la préparation à une éventuelle attaque constitue une « bouée de sauvetage » qui peut aider à la reprise rapide de l'exploitation des infrastructures critiques. Les plans d'intervention et les exercices contribuent à la préparation de cette reprise.

Les projets et les durées d'exploitation qui se prolongent ainsi que les technologies obsolètes menacent la cybersécurité

Les projets et l'exploitation des installations d'infrastructures critiques qui se prolongent constituent des défis pour la cyberrésilience. En effet, les systèmes qui sont à la pointe de la technologie pendant la phase de planification sont déjà obsolètes au moment de leur mise en service. Tandis que les installations d'infrastructures critiques sont exploitées pendant plusieurs dizaines d'années, les composants informatiques devraient être remplacés tous les trois à quatre ans. Les composants logiciels devraient faire l'objet d'une maintenance continue et être actualisés au moyen de correctifs de sécurité. Cependant, un renouvellement permanent peut être très coûteux et complexe, raison pour laquelle il n'est souvent pas effectué. Par conséquent, il est fréquent de trouver des composants obsolètes dans les infrastructures critiques, le logiciel n'est pas à jour et présente des vulnérabilités connues. De tels systèmes constituent des cibles faciles pour les cyberattaques.

Les exploitants sont tenus de maintenir à jour les installations d'infrastructures critiques et leurs composants TIC grâce à des architectures faciles à entretenir, des planifications systématiques et une mise en œuvre conséquente des mesures.

La PIC constitue une tâche commune et permanente, les directives nécessaires ne sont pas assez contraignantes

Les infrastructures critiques sont classées par secteurs et sous-secteurs. Selon les secteurs, les responsabilités en matière de surveillance et de réglementation incombent soit à la Confédération, soit aux cantons. En outre, de nombreuses infrastructures critiques sont exploitées par des entreprises privées. Tous ces éléments compliquent la surveillance des exploitants par les autorités fédérales. La diffusion des informations, la communication et une réaction ciblée et rapide en cas d'incident sont ainsi entravées.

Les technologies numériques employées évoluent rapidement. La mise en place et la garantie d'une cybersécurité robuste sont une tâche permanente. Elle ne peut être accomplie que si toutes les parties impliquées dans la PIC travaillent main dans la main. Les directives existantes pour la réglementation de la PCI sont aujourd'hui incomplètes et, pour certaines, trop peu contraignantes. Les autorités sectorielles de surveillance et de réglementation sont donc chargées de préciser les directives afin que la mise en œuvre des mesures de cyberrésilience puisse être exigée des exploitants d'infrastructures critiques. Au moment de la rédaction du rapport de synthèse, la Confédération s'efforce en outre d'examiner les bases légales relatives à la PIC.