Comment élaborer un programme de sécurité informatique

Par Vasiliki Tafili et Trent Nelson

Les installations qui manipulent des matières nucléaires ou d'autres matières radioactives, et qui mènent des activités connexes, sont des infrastructures essentielles qui exigent des niveaux élevés de sûreté et de sécurité. En adoptant une stratégie de sécurité informatique globale et préventive, les organismes peuvent protéger les informations sensibles et systèmes informatiques de ces installations pour éviter qu'ils ne soient compromis. La stratégie que recommande d'adopter l'AIEA suppose que les États établissent des prescriptions pour les stratégies ou politiques nationales, et qu'ils aident à assurer la confidentialité et la protection des informations et des systèmes informatiques sensibles liés à la protection physique, à la sûreté nucléaire ainsi qu'à la comptabilité et au contrôle des matières nucléaires. Ces prescriptions peuvent également prendre la forme de réglementations nationales prévoyant l'élaboration et la mise en œuvre d'un programme de sécurité informatique (PSI)*.

Un PSI est un cadre général qui comprend des éléments clés pour établir un plan efficace de mise en œuvre des politiques et procédures de sécurité informatique qui seront utilisées pendant toute la durée de vie d'une installation nucléaire ou d'une installation contenant des sources radioactives. Il vise à protéger les informations sensibles et les systèmes informatiques indispensables au maintien des fonctions de sûreté et de sécurité contre les cyberattaques afin d'atténuer leurs conséquences.

Stratégie nationale

Toute stratégie de sécurité informatique globale et efficace doit être systématique et intégrer divers éléments, notamment des réglementations, des programmes, des mesures de protection de la sécurité et des capacités de réaction à l'appui des régimes nationaux de sécurité nucléaire.

Réglementation

Une réglementation efficace fournit un cadre juridique pour la protection des systèmes informatiques sensibles et oblige les organismes à mettre en place des PSI et des contrôles appropriés.

Éléments clés du PSI :

Rôles et responsabilités

La définition des rôles et responsabilités des organismes, et l'obligation de rendre compte, sont essentielles pour une gestion efficace, en particulier dans le cas des infrastructures critiques. Il est indispensable de connaître la hiérarchie de l'organisme et de disposer de lignes d'autorité et d'une structure hiérarchique claires pour pouvoir assurer une collaboration et une synergie efficaces et efficientes dans le cadre des PSI.

Gestion des risques, des failles et du respect des règles

La gestion des risques de sécurité informatique consiste à évaluer les failles et effets potentiels des ressources numériques et systèmes informatiques sensibles afin de mettre en place des contrôles de sécurité informatique en suivant une approche graduée pour se défendre contre les cyberattaques. Le niveau des mesures de sécurité appliquées devrait être proportionnel au niveau de risque associé aux informations ou aux systèmes informatiques protégés. En tenant compte des conséquences de la faille ou de la menace, les organismes peuvent déterminer le niveau des mesures de sécurité nécessaires pour atténuer le risque.

Conception et gestion de la sécurité

La conception de la sécurité informatique est un aspect essentiel de la protection contre les cybermenaces. Parmi les grands principes de conception figure l'adoption d'une approche graduée et d'une défense en profondeur, où plusieurs couches de contrôles de sécurité par zone sont appliquées pour prévenir et atténuer les attaques. Les exigences en matière de sécurité doivent également être respectées tout au long du cycle de développement du système, et les organismes tiers doivent suivre des politiques et accords clairs afin de garantir la cohérence et l'efficacité des mesures de sécurité.

Gestion des ressources numériques

Pour que la stratégie de sécurité informatique soit efficace, il convient de suivre une approche systématique, en dressant une liste exhaustive de toutes les fonctions, ressources et de tous les systèmes de l'installation, y compris les ressources numériques sensibles qui sont essentielles à la protection des opérations nucléaires ou à l'utilisation sûre et sécurisée des matières nucléaires et autres matières radioactives. Cette liste doit également couvrir les flux de données et interdépendances importantes pour l'organisation, car ils jouent un rôle dans le contrôle des accès, les sauvegardes et les autres mesures de sécurité visant à protéger ces ressources contre le sabotage ou le vol.

Procédures de sécurité

Les politiques et procédures opérationnelles de sécurité nucléaire permettent à la direction de définir les responsabilités de chacun pour prévenir le vol, le sabotage ou l'utilisation non autorisée de matières et d'installations nucléaires. Avec de telles politiques, l'accès aux informations et aux ressources sensibles est contrôlé de près, et les personnes qui y ont accès sont sélectionnées et formées de manière appropriée.

Gestion du personnel

La fiabilité, la sensibilisation et la formation sont autant de points clés pour la gestion du personnel dans l'industrie nucléaire. Des évaluations de la fiabilité doivent être effectuées pour s'assurer que le personnel est fiable, compétent et n'est pas en situation de conflit d'intérêts qui pourrait compromettre la sûreté ou la sécurité. Il est primordial de toujours disposer d'un personnel qualifié et digne de confiance pour garantir la sûreté et la sécurité nucléaires.

*Pour plus d'informations, voir le document *IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities*.