Sécuriser un unité ou une plateforme scientifique

Pour Qui ? Pourquoi ? Comment ?

➢ Pour Qui ?

« Si vous pensez que seule la technologie peut résoudre vos problèmes de sécurité, alors vous n'avez rien compris à la technologie, ni à vos problèmes »

Bruce Schneier (cryptologue, spécialiste en sécurité informatique)

De quoi parle -t- on ?

D'organisation, d'aspects juridiques (lois et règlements), d'usages (ergonomiques, psychologiques …), de moyens (financiers et humains) ET de technique…

Ce n'est donc pas qu'un problème d'informaticiens mais avant tout un sujet pour les décideurs et porteurs d'enjeux.

Pourquoi ?

Attaques en constante augmentation : 15 % des attaques ciblent les établissements d'enseignement supérieur et de recherche selon l'ANSSI.

Confiance des partenaires : demande d'engagement sur notre niveau de sécurité (audits, certifications…)

Le cadre réglementaire se durcit : RGPD, RGS, II901, décret 2022-513 du 8 avril 2022 , instruction générale interministérielle IGI-1337 du 26 octobre 2022, directive européenne NIS sur la sécurité informatique.

Utopie : Vouloir tout sécuriser et partout

Réalité : Il faut prioriser les mesures de sécurité

L'Analyse de Risques en Cybersécurité permet d'identifier les risques inacceptables afin de s'en prémunir

Comment ?

Nature des risques : « CIA » (en), « CID » (fr)

La **confidentialité** ou le risque d'accès illégitime à des données est la propriété selon laquelle l'information n'est pas rendue disponible ni divulguée à des personnes, des entités ou des processus non autorisés (ISO 27000).

L'**intégrité** ou le risque de modification non désirées de données est la propriété d'exactitude et de complétude (ISO 27000). Voir l'annexe sur l'intégrité pour plus de détail.

La **disponibilité** ou le risque de disparition de données est la propriété d'être accessible et utilisable à la demande par une entité autorisée (ISO 27000). Voir l'annexe sur l'intégrité pour plus de détail.

Comment ?

Les 10 étapes concrètes

1. Définir les responsabilités, l'organisation et le processus permettant de planifier et de suivre les étapes suivantes.

À noter : Le DU est responsable de la sécurité des systèmes d'information de son unité. La nomination d'un référent cybersécurité au sein de l'unité fortement encouragée à INRAE. Sont particulièrement bien placés pour ce rôle : Les qualiticiens, référents données opérationnels, informaticiens, référents sécurité…

2. Identifier les typologies d'informations sensibles, notamment les informations à régime restrictif, les données de recherche impliquant la sécurité biologique, en santé, médicales, personnelles ou contractuelles.

3. Analyser les risques portant sur les informations sensibles et les conséquences en cas d'incident.

4. Décider d'une échelle de sensibilité avec la nomenclature associée et définir les processus de marquage des informations, données, documents, fichiers, mails... En cas d'échange avec d'autres entités, l'échelle de sensibilité doit aussi être transmise et les échanges doivent être chiffrés.

5. Localiser les données les plus sensibles. L'objectif est d'identifier les entités qui produisent ou manipulent des informations sensibles.

Comment ?

Les 10 étapes concrètes

6. Cartographier et faire homologuer les SI supports actuels. L'objectif est d'identifier et de sécuriser les moyens utilisés pour stocker, exploiter, véhiculer ou échanger les informations sensibles.

7. Identifier et mettre en place des mesures de sécurité limitant les accès des données sensibles aux personnes autorisées et les protégeant en terme de Confidentialité, Intégrité et Disponibilité.

8. Formaliser une politique SSI. Utiliser la POSSI INRAE et l'appliquer au contexte de l'unité.

9. Contrôler le processus de marquage des données sensibles et leur bonne protection.

10. Réévaluer la politique de sécurité des SI périodiquement ou en cas de changement majeurs des activités. Contrôler périodiquement la conformité à la POSSI.

INRAE

SSI

FIN