Cybersécurité : analyse des risques cyber pour le secteur de la chimie

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité et de cyberdéfense en France.

France Chimie est l'organisation professionnelle qui représente les entreprises de la Chimie en France. Elle est le porte-parole du secteur auprès des pouvoirs publics nationaux, européens et des instances internationales.

La démarche

L'ANSSI a conduit en collaboration avec France Chimie une analyse des risques cyber pesants sur le secteur de la Chimie. Cette démarche sectorielle a pour objectif **d'identifier les risques numériques qui pourraient porter préjudice à l'ensemble de la filière**. Dans cette optique, l'ANSSI et France Chimie ont étudié les enjeux et contraintes spécifiques du secteur, identifié des risques communs et évalué les impacts sectoriels de ces risques. La méthodologie utilisée est EBIOS *Risk Manager* de l'ANSSI.

Véritable boussole pour les organisations, **l'approche par les risques** EBIOS *Risk Manager* place les besoins métiers au centre de la réflexion avec une sécurisation des systèmes proportionnée à la menace, aux dépendances à l'écosystème et aux vulnérabilités de l'organisation. Chaque dirigeant d'entreprise élabore ainsi une posture équilibrée de sécurisation des activités de son organisation en appréciant ses risques cyber. Il se repose ensuite sur ses experts en cybersécurité afin de sécuriser ses actifs les plus critiques.

Les risques cyber identifiés pour le secteur Chimie

Plusieurs sources de risques numériques faisant peser des menaces importantes sur le secteur sont à relever : la menace étatique, cybercriminelle et interne. L'analyse identifie principalement des attaques ayant des objectifs lucratifs, de déstabilisation et d'espionnage économique et industriel.

1. **La diversité des chemins d'attaques pour atteindre la donnée, au cœur des préoccupations des industriels de la Chimie**

Les risques liés aux **données sont importants** pour tous les industriels du secteur. L'analyse identifie la protection des informations de R&D comme importante pour les entreprises réalisant cette activité. Dans un contexte de commerce international tendu, les données sensibles peuvent aussi être volées par des attaquants se cachant derrière des demandes légitimes.

L'un des principaux **chemins d'attaques est celui du rançongiciel**. Les PME/TPE/ETI constituent la catégorie d'entités la plus affectée par les compromissions par **rançongiciel**[1] et cette menace systémique n'épargne pas le secteur de la chimie. Les dirigeants de ces organisations sont de plus en plus sensibilisés à ce risque car le rançongiciel représente une perte financière directe conséquente à un arrêt prolongé de la production et au coût de la reconstruction pour l'industriel ciblé.

Dans le secteur de la chimie, le rançongiciel peut emprunter **des chemins d'attaques inédits**, résultant de **la porosité entre les systèmes informatiques classiques et les systèmes informatiques industriels**.

[1] 37% des victimes d'attaques par le biais de rançongiciels rapportées à l'ANSSI sont des TPE/PME/ETI en 2024. Source : panorama de la cybermenace 2024, page 33.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

ANSSI

FRANCE CHIMIE

Cette porosité est liée à **la numérisation des processus métier industriels** qui a lieu dans le secteur de la Chimie, au même titre que les autres secteurs.

2. L'écosystème des industriels : un risque cyber majeur

Un autre risque pour le secteur de la Chimie, par ailleurs observé par l'ANSSI dans d'autres secteurs, est celui des **attaques sur son écosystème**, dont ses chaines d'approvisionnement et de distribution.

La chaîne d'approvisionnement d'un SI offre des possibilités d'attaques variées et furtives. Les attaques par la chaîne d'approvisionnement permettent de compromettre par rebond les organisations clientes d'un prestataire commun ou utilisant un même logiciel ou équipement. En France, l'ANSSI observe que la majeure partie des attaques par la chaîne d'approvisionnement logiciel est réalisée en compromettant le SI d'un éditeur de logiciel.

D'autres axes de travail pour la filière chimie, non repris dans ce document, ont été identifiés. Pour aller plus loin et obtenir le document d'analyse de risques, les industriels sont invités à contacter le Comité Cyber de France Chimie qui a participé à son élaboration **: Chloé RETAILLEAU**

Ce Comité Cyber est aussi un cénacle de tout premier ordre permettant aux industriels de travailler sur les sujets de cybersécurité au travers d'échanges collectifs, de retour d'expérience, de mise en commun. Ce Comité sera le lieu d'animation privilégié pour engager une dynamique sectorielle de cybersécurité et de défense collective à la suite de l'analyse sectorielle.

Premières recommandations pour engager un projet de cybersécurité

En réponse à ces risques, l'étude propose des axes de travail à aborder en priorité pour engager la sécurisation de son entreprise. Ces axes visent à :

- Se préparer à l'arrivée des futures réglementations en rehaussant le niveau de sécurité par la mise en œuvre de mesures d'hygiène afin de limiter l'impact d'un incident de cybersécurité ;
- Mettre en place les dispositifs permettant de rétablir ses capacités de production en cas d'incident de cybersécurité paralysant l'activité via un plan de continuité et reprise d'activité intégrant la perte d'outils critiques ;
- Limiter les capacités de propagation d'une attaque sur les systèmes d'information ;
- Sécuriser les dépendances avec les fournisseurs de solutions bureautiques et industrielles afin de limiter le risque qu'ils soient un vecteur d'attaque.

Pour les entités les moins matures, le service « MonAideCyber » permet de réaliser gratuitement un diagnostic cyber avec un aidant. Cet outil est accessible sur le portail de services de l'ANSSI : « Le diagnostic cyberdépart | MesServicesCyber ».

Pour aller plus loin et accéder aux ressources

Ressources documentaires supplémentaire de l'ANSSI :

- Réaliser son diagnostic cyber Accueil | MesServicesCyber
- S'informer sur la directive NIS2
- La cybersécurité des TPE/PME
- Le guide d'hygiène informatique
- Les systèmes industriels
- Méthode EBIOS *Risk Manager* : La méthode EBIOS Risk Manager | ANSSI
- Homologation de sécurité des systèmes d'information : L'homologation de sécurité des systèmes d'information | ANSSI