SH05 - Note Personnelle

L’importance de la cybersécurité dans le monde de l’enterprise

Alexis LEBEL

A24

Table des Matières

Confidentialité

Restreint à l'utilisation par l'UTC dans le contexte de confidentialité du contrat d'apprentissage, à ne pas diffuser publiquement

Pour des raisons de confidentialité, certains noms d'enterprises sont omis, et certains détails sont volontairement vagues (ex: Méthodes de fabrication, etc.)

Introduction

Dans un monde où les données sont devenues un **actif stratégique** de premier ordre, la **cybersécurité** s'impose comme un enjeu crucial pour les entreprises. La protection des informations sensibles, qu'il s'agisse de secrets industriels, de données clients ou de stratégies commerciales, est au cœur des préoccupations des dirigeants. Les conséquences d'une fuite de données ou d'une cyberattaque peuvent être dévastatrices : perte de compétitivité, atteinte à la réputation, sanctions légales ou encore perturbations opérationnelles.

Au sein de **Poclain**, l'entreprise qui m'emploie en tant qu'Ingénieur R&D (par Alternance), la cybersécurité est un défi quotidien, en raison de la nature stratégique des données manipulées. Parmi les menaces les plus rencontrées, on observe une recrudescence des attaques par **phishing** et l'émergence de nouvelles techniques basées sur l'**intelligence artificielle**, notamment lors de visioconférences. Ces méthodes sophistiquées exploitent des failles principalement humaines[1] pour compromettre les systèmes de l'entreprise.

Ce document propose une synthèse des discussions menées avec des personnes du service informatique de l'enteprise. Il met en lumière les enjeux liés à la protection des données stratégiques, illustre les menaces auxquelles nous sommes confrontés et présente les mesures à adopter pour renforcer la sécurité de l'information. Au-delà d'une simple problématique technique, la cybersécurité est un levier stratégique indispensable pour préserver la compétitivité et la pérennité de l'entreprise dans un environnement économique marqué par une concurrence accrue.

[1] 85% des attaques d'enterprises utilisent le vecteur humain, source : Intervention DGSI 27/11/24

1 Importance de la protection des données stratégiques

1.1 Poclain : une ETI contre des grands groupes

Poclain est une entreprise industrielle spécialisée dans la conception et la fabrication de moteurs hydrauliques. Elle se positionne comme une ETI dans un secteur dominé par des grands groupes tels que Rexroth (Bosch) ou Danfoss. Malgré cette concurrence, Poclain se distingue par son expertise technique et son effort constant d'innovation. En 2023, elle a déposé 12 brevets, se plaçant parmi les premiers déposants dans les Hauts-de-France[2].

L'entreprise bénéficie d'une présence internationale grâce à un réseau de filiales et de partenaires répartis sur plusieurs continents. Cette exposition mondiale renforce son attractivité auprès des clients, mais augmente également sa vulnérabilité face aux menaces de cybersécurité, notamment le vol de données sensibles.

1.2 Des clients prestigieux et des relations de confiance à préserver

Les clients de Poclain incluent des acteurs majeurs de l'industrie mécanique et hydraulique, répartis sur différents marchés internationaux. Ces collaborations stratégiques reposent sur des échanges réguliers de données confidentielles, telles que les spécifications techniques de machines ou les conditions commerciales.

Toute fuite ou divulgation d'informations confidentielles pourrait affaiblir la relation de confiance avec ces clients, menaçant à la fois des contrats en cours et de potentielles opportunités commerciales.

D'autres données à risque sont les stratégies commerciales de Poclain, incluant des négociations contractuelles et des analyses de marché par exemple. Ces informations sont essentielles pour maintenir la compétitivité de l'entreprise face à des concurrents mieux dotés financièrement ou technologiquement.

Une divulgation non autorisée de ces données pourrait permettre à des concurrents d'adapter leurs propres offres pour évincer Poclain sur des appels d'offres ou des marchés stratégiques. Les impacts financiers et commerciaux d'une telle fuite pourraient être significatifs.

1.3 Des secrets industriels essentiels à la compétitivité

Les produits de Poclain, bien que perçus comme simples dans leur conception, reposent sur des processus de fabrication complexes et optimisés. Ces processus incluent :
- la sélection et le traitement de matériaux spécifiques,
- des procédés avancés de traitement thermique,
- des méthodes d'assemblage brevetées.

Ces processus sont au cœur de l'avantage compétitif de Poclain, garantissant à la fois la qualité de ses produits et le contrôle de ses coûts de fabrication. Une fuite de ces informations techniques pourrait permettre à un concurrent de reproduire ces méthodes, réduisant ainsi la compétitivité de Poclain.

[2] https://www.inpi.fr/sites/default/files/PalmaresRegions2023.pdf

Les projets de R&D en cours, incluant des prototypes et des brevets non encore publiés, représentent également un enjeu critique. Ces travaux, souvent à l'origine d'innovations différenciantes, sont exposés à des risques accrus de cyberespionnage. La perte de ces données avant leur protection juridique pourrait compromettre la stratégie d'innovation de l'entreprise et son positionnement sur le marché.

1.4 Des concurrents en quête d'informations sensibles

Les concurrents de Poclain, notamment de grands groupes disposant de ressources significatives, cherchent souvent à accéder à ces informations, par tous moyens légaux à leur disposition, parmis lesquels on trouve :

- Une veille sur la propriété intellectuelle de Poclain : Tous les brevets déposés par Poclain sont publics et peuvent être consultés par des tiers. Les concurrents peuvent ainsi :
  - Identifier les axes d'innovation de Poclain,
  - Repérer des opportunités pour contrer l'avanatge compétitif apporté par le brevet (contre-brevet bloquant l'utilisation de la technologie),[3]
- Une veille sur l'actualité de Poclain : Les informations publiques sur l'entreprise (communiqués de presse, rapports financiers, etc.) peuvent donner des indications sur sa santé financière, ses projets en cours, ses partenariats, etc.

Ces solutions répandues peuvent être complétées par des actions moins assumées, mais néanmoins très présentes, comme l'utilisation des informations des réseaux sociaux des employés. En effet, parfois sans intention malveillante, les employés peuvent divulguer des informations sensibles sur leur entreprise, apportant des informations précieuses aux concurrents.[4]

[3] Informations tirées de la formation interne sur la propriété intellectuelle
[4] source : Intervention DGSI 27/11/24

2 Des tentatives d'attaques sophistiquées

2.1 Des attaques qui exploitent le vecteur humain

L'un des principaux points d'entrée pour les cyberattaques reste le facteur humain. Malgré les protections technologiques mises en place, des méthodes d'ingénierie sociale, telles que le phishing, ciblent directement les collaborateurs pour contourner les défenses de l'entreprise.

2.1.1 Les attaques par phishing

Les attaques par phishing représentent la menace la plus fréquente pour Poclain. Ces attaques, souvent réalisées via des emails frauduleux, visent à récupérer les identifiants des collaborateurs. Une fois ces informations obtenues, les conséquences peuvent inclure :

- **Compromission de données** : des informations stratégiques ou sensibles peuvent être volées.
- **Compromission de boîtes mail** : un attaquant qui accède à une boîte mail interne peut l'utiliser comme vecteur de confiance pour tromper d'autres collaborateurs ou partenaires.
- **Propagation de ransomwares** : après avoir obtenu un accès, un attaquant peut déployer un ransomware, entraînant :
  - le vol ou la destruction de données,
  - un blocage des systèmes critiques de l'entreprise,
  - des demandes de rançon sous forme de chantage, menaçant de divulguer des données sensibles ou de maintenir les systèmes inaccessibles.

2.1.2 Les attaques par IA en visioconférence

En 2024, une tentative d'attaque par intelligence artificielle a été identifiée au sein de Poclain. Cette méthode sophistiquée consistait à imiter la voix et les comportements d'un interlocuteur de confiance lors d'une visioconférence. Bien que cette tentative ait été déjouée grâce aux bons réflexes des collaborateurs, acquis lors des formations de sensibilisation, cette attaque illustre l'évolution rapide des menaces.

Les experts en cybersécurité s'accordent à dire que ces attaques basées sur l'IA deviendront plus fréquentes et difficiles à détecter. Elles posent un risque particulier dans les entreprises où la communication interne et externe repose de plus en plus sur des plateformes numériques.

2.2 La sécurité : une responsabilité collective

La défense contre ces menaces repose sur l'implication de tous les collaborateurs. Poclain adopte une approche proactive en matière de sensibilisation et de formation à la cybersécurité :

- **Formations à l'arrivée** : chaque nouvel employé reçoit une formation spécifique pour reconnaître les risques courants tels que le phishing.

- **Campagnes de sensibilisation régulières** : des simulations d'attaques par phishing sont organisées pour évaluer et renforcer les réflexes des collaborateurs face à ces menaces.

En complément des initiatives humaines, des mesures techniques strictes garantissent une sécurité accrue :

- **Séparation des droits d'accès** : les collaborateurs n'ont accès qu'aux données nécessaires à leur rôle, limitant les impacts d'une éventuelle compromission.

- **Contrôle des interactions externes** : les échanges de données sensibles avec des tiers font l'objet d'une vérification rigoureuse.

- **Politique d'exposition minimale des infrastructures** :
  - Les services internes sont uniquement accessibles depuis le réseau sécurisé de l'entreprise, soit sur site, soit via un VPN.

  - Les solutions Cloud utilisées par Poclain sont rigoureusement évaluées pour garantir leur sécurité et leur conformité aux standards de l'entreprise.

Ces actions coordonnées entre les équipes techniques et les collaborateurs permettent à Poclain de limiter l'exposition aux menaces tout en renforçant sa résilience face aux attaques.

Conclusion générale

Dans un environnement où la donnée est un atout stratégique, la cybersécurité se positionne comme un enjeu majeur pour les entreprises industrielles telles que Poclain. Protéger les informations sensibles, qu'il s'agisse de secrets industriels, de données clients ou de stratégies commerciales, est essentiel pour maintenir la compétitivité et assurer la pérennité de l'entreprise face à des concurrents mieux armés ou à des menaces externes.

Les cyberattaques, qu'elles exploitent des failles humaines comme le phishing ou des technologies avancées telles que l'intelligence artificielle, illustrent la nécessité d'une vigilance constante. La mise en œuvre d'une politique de sécurité globale, intégrant des formations pour les collaborateurs, des contrôles d'accès stricts et des infrastructures sécurisées, permet à Poclain de minimiser les risques tout en répondant aux exigences de son environnement économique et industriel.

Conclusion sur le rapport à l'intelligence économique et stratégique

La cybersécurité est un pilier fondamental de l'intelligence économique et stratégique. Protéger les informations critiques revient à préserver les capacités d'innovation, les parts de marché et la confiance des partenaires. Dans le cas de Poclain, où l'innovation et la R&D sont au cœur de la stratégie, la maîtrise des risques cyber est une condition sine qua non pour rester compétitif face aux grands acteurs du secteur.

En intégrant les enjeux de cybersécurité dans une démarche d'intelligence économique, l'entreprise peut anticiper les menaces, surveiller les pratiques de ses concurrents et protéger efficacement son patrimoine informationnel. Cette approche proactive et stratégique renforce non seulement la résilience de Poclain, mais lui donne également les moyens d'exploiter son potentiel de manière optimale sur le long terme.