NOTE DE RETOUR D'EXPERIENCE

Incident ransomware PME industrielle -- Sous-traitance aeronautique

Chronologie, analyse post-mortem et lecons tirees -- Usage RSSI / Direction generale / Assureur

RÉFÉRENCE	L70C-REX-2026-04
DATE	Avril 2026
INCIDENT	Ransomware LockBit 3.0 (variante) -- Janvier 2026
ORGANISATION	PME industrielle anonymisee -- 180 salaries -- CA 28 M EUR
SECTEUR	Sous-traitance aeronautique -- Tier 2 Airbus / Safran
CLASSIFICATION	Confidentiel -- Diffusion restreinte

Avertissement. Ce document est un retour d'experience anonymise produit a des fins de demonstration commerciale. L'incident, l'organisation et les personnes cites sont fictifs. La methodologie et les observations refletent des situations reelles observees sur des incidents comparables. Toute ressemblance avec un incident reel est fortuite.

01 Contexte et profil de la cible

La structure affectee est une PME de 180 salaries specialisee dans l'usinage de precision et l'assemblage de composants aeronautiques. Fournisseur tier-2 d'Airbus et Safran, elle opere sur deux sites (Toulouse et Bordeaux) avec un parc informatique de 95 postes, un ERP metier (Sage X3) et des machines-outils a commande numerique (CNC) connectees au reseau de production.

Au moment de l'incident, la DSI se resumait a un responsable informatique unique, sans RSSI designe. Aucun plan de continuite operationnelle n'etait formellement etabli. La sauvegarde etait realisee sur un NAS local non isole du reseau principal. L'entreprise n'avait pas souscrit d'assurance cyber specifique.

02 Chronologie de l'incident

J-21 -- 06 jan. Vecteur d'entree : phishing RH

Un email de candidature spontanee contenant un CV piege (macro Excel) est ouvert par la responsable RH depuis son poste bureautique. L'ouverture declenche le telechargement silencieux d'un loader (Qakbot). Aucune alerte n'est generee -- l'antivirus endpoint ne detecte pas la menace.

J-21 a J-14 **Persistance et reconnaissance**	Le loader etablit une persistance via une tache planifiee Windows et commence une reconnaissance reseau silencieuse. L'attaquant cartographie les partages, l'AD, les sauvegardes. Aucune detection pendant 7 jours -- pas de SIEM, pas de supervision des evenements AD.
J-14 **Mouvement lateral -- compromission AD**	Exploitation d'un compte de service avec mot de passe faible (Hash NTLM capture via Responder). Elevation de privileges. L'attaquant obtient les droits Administrateur de domaine. A partir de ce moment, l'ensemble du SI est sous controle attaquant.
J-3 a J0 **Exfiltration de donnees**	Environ 18 Go de donnees sont exfiltrees via HTTPS vers une infrastructure externe (C2 masque derriere Cloudflare). Donnees concernees : plans techniques, contrats clients, fiches de paie, devis en cours. Le trafic sortant anormal n'est pas detecte -- pas de DLP ni de monitoring du trafic HTTPS sortant.
J0 -- 03h12 **Declenchement du ransomware**	LockBit 3.0 se deploie simultanement sur 87 postes et 12 serveurs. Chiffrement complet en 23 minutes. Les sauvegardes NAS sont chiffrees en meme temps que la production. Note de rancon : 380 000 EUR en BTC, double extorsion (paiement ou publication des donnees exfiltrees).
J+1 -- 06h45 **Decouverte par l'equipe de nuit**	Un operateur de production constate l'impossibilite d'acceder aux fichiers CNC. Alert donnee au responsable informatique a 07h15. Tentative de redemarrage infructueuse. Premier appel externe (prestataire informatique habituel) a 08h30.
J+1 apres-midi **Notification et activation de crise**	Notification a la direction generale a 10h. Decision de ne pas payer la rancon. Contact avec l'ANSSI (signalement sur cybermalveillance.gouv.fr). Cabinet de reponse a incident externe mandate a 14h. Notification CNIL effectuee le lendemain (J+2) dans le delai reglementaire de 72h.
J+3 a J+18 **Confinement et reprise partielle**	Isolation du reseau, reconstruction des serveurs critiques depuis des images saines (backup hors site partiel heureusement disponible pour 3 serveurs). Reprise de la messagerie a J+5, de l'ERP a J+12, des postes bureautiques a J+18. La production CNC reprend partiellement a J+10 depuis des fichiers recuperes sur des postes non chiffres (machines eteintes au moment de l'attaque).
J+47 **Reprise complete et bilan**	Reprise totale de l'activite. Perte de CA estimee a 1,2 M EUR (arret de production, penalites clients, couts de remediation). Donnees exfiltrees non publiees a ce jour (decision de non-paiement maintenue). Aucune poursuite penale n'a abouti.

03 Ce qui a tenu -- Ce qui a failli

CE QUI A TENU

TENU	La decision de ne pas payer la rancon a ete maintenue malgre la pression -- choix coherent avec l'absence de garantie de dechiffrement et le risque de recidive.
TENU	La notification CNIL a ete effectuee dans le delai reglementaire de 72h, evitant une sanction supplementaire sur un perimetre deja fragilise.

TENU	Un backup hors site partiel (3 serveurs sur 12) existait chez le prestataire cloud -- il a permis d'accelerer significativement la reprise. Sans lui, le delai aurait ete double.
TENU	La communication externe a ete maitrisee : aucune fuite presse, clients informes directement et individuellement par la direction, sans declaration publique precipitee.

CE QUI A FAILLI

FAILLI	Absence totale de supervision reseau (pas de SIEM, pas de NDR) : l'attaquant a opere 21 jours sans etre detecte. La fenetre de detection existait -- elle n'a pas ete utilisee.
FAILLI	Les sauvegardes NAS etaient connectees en permanence au reseau de production et ont ete chiffrees en meme temps que les serveurs. La regle des 3-2-1 n'etait pas appliquee.
FAILLI	Le compte de service compromis disposait d'un mot de passe de 8 caracteres inchange depuis 4 ans. Aucun MFA n'etait deploye sur les acces privilegies.
FAILLI	Aucun plan de crise n'existait : les premieres heures ont ete chaotiques, les decisions prises sans cadre, les prestataires contactes dans le desordre. La cellule de crise n'a ete activee qu'a J+1 apres-midi.
FAILLI	Les machines CNC etaient sur le meme segment reseau que les postes bureautiques. L'absence de segmentation a permis une propagation totale en 23 minutes.
FAILLI	Aucune assurance cyber n'avait ete souscrite. La totalite des couts (1,2 M EUR) a ete absorbee par la tresorerie de l'entreprise.

04 Lecons tirées -- Recommandations post-mortem

L1 — Superviser ou subir

L'absence de supervision reseau est le facteur determinant qui a transforme une intrusion controlable en catastrophe operationnelle. Un SIEM leger (Wazuh, Elastic) avec alertes sur les evenements AD critiques aurait signale la compromission des J-14. Cout d'un SIEM basique : 5 000 a 15 000 EUR/an. Cout de l'incident : 1,2 M EUR.

L2 — La regle 3-2-1 n'est pas optionnelle

3 copies, 2 supports differents, 1 hors site et hors reseau. La sauvegarde connectee en permanence n'est pas une sauvegarde : c'est une copie supplementaire de ce que l'attaquant va chiffrer. Le backup hors site partiel a sauve la reprise -- il aurait du couvrir 100% des systemes critiques.

L3 **Les comptes a privileges sont la cible numero un**

Le mouvement lateral n'a ete possible que grace a un compte de service avec un mot de passe faible et aucun MFA. LAPS pour les administrateurs locaux, MFA sur tous les acces privilegies, rotation des mots de passe de service : ce sont des mesures a cout marginal pour un gain de resilience majeur.

L4 **Un plan de crise teste vaut dix fois un plan non teste**

Les premieres heures d'un incident sont les plus couteuses en erreurs. Sans plan pre-etabli, chaque decision est prise sous stress, sans cadre, souvent dans le mauvais ordre. Un exercice de simulation annuel -- meme leger -- cree les reflexes qui font la difference entre 18 jours et 47 jours de reprise.

L5 **La segmentation reseau est le filet de securite de dernier recours**

Si les CNC avaient ete sur un segment isole, le ransomware n'aurait probablement pas atteint la production. La segmentation ne previent pas l'intrusion -- elle limite la propagation. C'est la difference entre un incident contenu et une catastrophe totale.

L6 **Souscrire une assurance cyber avant l'incident**

Une assurance cyber adaptee (couverture rancon, frais de remediation, pertes d'exploitation) aurait absorbe une large part des 1,2 M EUR. Les primes pour une PME de ce profil se situent entre 8 000 et 25 000 EUR/an selon le niveau de maturite cyber. Le ROI est immediat des le premier incident evite ou absorbe.

05 Synthese pour l'assureur

Critere	Etat au moment de l'incident	Impact sur sinistralite
Supervision reseau	Absente	Duree de presence attaquant : 21 jours -- aggravant majeur
Sauvegardes	Partiellement hors site	Duree de reprise reduite -- attenuant partiel
MFA comptes privilegies	Absent	Compromission AD facilitee -- aggravant majeur
Plan de continuite	Absent	Couts de crise amplifies -- aggravant
Segmentation reseau	Absente	Propagation totale en 23 min -- aggravant majeur
Notification reglementaire	Effectuee dans les delais	Absence de sanction CNIL -- attenuant
Assurance cyber	Non souscrite	Totalite du sinistre en charge propre -- 1,2 M EUR

CONCLUSION

Cet incident illustre le profil de sinistre le plus frequent en 2025-2026 pour les PME industrielles : un attaquant patient, une intrusion par phishing non detectee, une propagation rendue possible par l'absence de mesures basiques, et un impact operationnel et financier disproportionne par rapport aux investissements de prevention qui auraient pu l'eviter ou le contenir. Les six lecons tirees de cet incident sont directement actionnables et constituent la base d'un plan de remediation prioritaire pour toute structure de profil equivalent.

L. Bonjean
Capitaine de fregate (h) -- Gerant Louis70 Conseil SAS -- SIREN 989 600 481