Veille Technologique

Sauvegarde et Plan de Reprise d'Activité (PRA)

BTS SIO 2ème année - SISR

Période : Janvier - Février 2025

Introduction

La veille technologique consiste à surveiller régulièrement l'actualité informatique. Pour un technicien SISR, c'est essentiel pour rester informé des nouvelles menaces et solutions.

Mon sujet porte sur la sauvegarde des données et le Plan de Reprise d'Activité (PRA). Le PRA est un ensemble de procédures pour redémarrer l'activité après un incident (cyberattaque, panne, incendie). Il repose sur deux indicateurs :

- RPO (Recovery Point Objective) = perte de données maximale acceptable
- RTO (Recovery Time Objective) = temps maximal pour redémarrer

En 2025, les ransomwares se multiplient. En France, 60% des PME victimes déposent le bilan. Les sauvegardes doivent suivre la règle 3-2-1 : 3 copies, sur 2 supports différents, dont 1 hors site.

Articles collectés

Date	Source	Résumé	Lien
07/01/2025	Arx One	Cyberattaque chez Kiabi : 20 000 comptes clients piratés avec vol d'IBAN. Montre l'importance d'une réaction rapide et d'un plan de sauvegarde.	www.arx-one.com/blog/cyberattaque-kiabi-2025
10/01/2025	Sophos	Enquête 2025 : le recours aux sauvegardes chute à 53% (vs 73% en 2024). Les entreprises font moins confiance à leurs backups, ce qui est alarmant.	www.sophos.com/fr-fr/content/state-of-ransomware
14/01/2025	Access Group	Différences entre sauvegarde, PRA et PCA. Le PRA organise la reprise avec RPO/RTO, le PCA garantit la continuité sans interruption.	www.access-group.com/fr/ressources/pra-pca-sauvegarde
18/01/2025	Fortinet	Statistiques 2025 : le coût des ransomwares atteindra 57 milliards de dollars par an, soit 156 millions par jour. Les PME sont les plus touchées.	www.fortinet.com/fr/resources/cyberglossary/ransomware-statistics
21/01/2025	Adista	PRA vs sauvegardes : les sauvegardes protègent les données mais ne suffisent pas. Le PRA inclut processus, outils et moyens humains pour reprendre l'activité.	www.adista.fr/blog/pra-vs-sauvegarde-differences
22/01/2025	Factoria	~75% des intrusions sont des ransomwares. Le facteur humain est impliqué dans ~60% des brèches. Les sauvegardes 3-2-1 testées sont prioritaires.	www.factoria.fr/blog/ransomware-facteur-humain-2025
25/01/2025	Mimecast	88% des violations de données ransomware concernent des PME. 64% des victimes ne paient pas la rançon et utilisent leurs sauvegardes pour récupérer.	www.mimecast.com/resources/research-reports/ransomware-readiness-2025
29/01/2025	Leviia	La sauvegarde cloud souveraine (ISO 27001, RGPD) devient un standard. Les tests réguliers de PRA sont indispensables pour vérifier la restauration.	www.leviia.com/blog/sauvegarde-cloud-souveraine-iso27001
01/02/2025	Hornetsecurity	Les attaques ransomware sont en hausse pour la première fois en 3 ans. Elles constituent l'une des menaces les plus persistantes pour les entreprises.	www.hornetsecurity.com/fr/resources/ransomware-report-2025

Date	Source	Résumé	Lien
03/02/2025	Semperis	83% des ransomwares compromettent l'Active Directory. 76% des victimes mettent plus d'un jour à reprendre leur activité normale.	www.semperis.com/resources/ransomware-active-directory-2025
04/02/2025	GlobalSP	Face aux ransomwares qui ciblent les sauvegardes locales, le cloud externalisé devient obligatoire. La règle 3-2-1 est le minimum.	www.globalsp.com/fr/blog/cloud-externalise-ransomware
08/02/2025	SentinelOne	Les ransomwares attaquent aussi le cloud. Il faut des plans de sauvegarde robustes avec MFA et contrôles d'accès stricts.	www.sentinelone.com/blog/cloud-ransomware-backup-mfa-2025
11/02/2025	Wikipedia	76% des collectivités françaises n'ont ni PCA ni PRA. 64% n'ont pas de RSSI. Un retard alarmant face aux cyberattaques.	fr.wikipedia.org/wiki/Plan_de_reprise_d%27activit%C3%A9
15/02/2025	Adista	En 2025, seulement 12% des entreprises françaises refusent de payer la rançon. Il faut externaliser et répliquer les sauvegardes.	www.adista.fr/blog/ransomware-paiement-ranccon-france-2025
18/02/2025	LeMagIT	Février 2025 : 547 cyberattaques mondiales. En France, +121% de demandes d'assistance ransomware vs 2024. Le PRA devient obligatoire pour les OIV.	www.lemagit.fr/actualites/ransomware-france-2025-hausse
20/02/2025	Gridinsoft	Triple extorsion dans 87% des attaques : chiffrement + vol de données + DDoS. Les ransomwares chiffrent 220 000 fichiers en 4,5 minutes.	gridinsoft.com/blog/triple-extortion-ransomware-2025
23/02/2025	Veeam	La règle 3-2-1 évolue en 3-2-1-1-0 : ajouter une copie immuable et vérifier qu'il n'y a aucune erreur de restauration.	www.veeam.com/blog/3-2-1-1-0-backup-rule.html
25/02/2025	Fidens	Le PRA/PCA doit être testé régulièrement. Un PRA non testé reste théorique. La gouvernance doit impliquer les directions métiers.	www.fidens.fr/blog/tester-son-pra-pca-bonnes-pratiques
27/02/2025	GoodTech	50% des entreprises victimes paient la rançon en 2025. 71% tentent de négocier. Le montant moyen payé est 1 million d'euros.	www.goodtech.fr/blog/ransomware-paiement-statistiques-2025
05/03/2025	ANSSI	Publication du guide ANSSI 2025 sur la sécurisation des sauvegardes en entreprise. Recommandation d'adopter le chiffrement de bout en bout pour toutes les copies hors site.	www.ssi.gouv.fr/guide/securisation-sauvegardes-2025
11/03/2025	CyberMalveillance	Hausse de 34% des signalements de ransomwares en France depuis début 2025. Les TPE/PME représentent 68% des victimes enregistrées sur la plateforme.	www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/ransomware-bilan-2025
18/03/2025	Coveware	Rapport Q1 2025 : le temps de chiffrement moyen avant détection passe à 2h30. Les sauvegardes immuables ont permis à 41% des victimes d'éviter le paiement.	www.coveware.com/blog/q1-2025-ransomware-marketplace-report
22/03/2025	Cloudflare Blog	Présentation d'une nouvelle approche Zero Trust appliquée aux accès de sauvegarde : chaque restauration est authentifiée via MFA + vérification d'intégrité automatique.	blog.cloudflare.com/zero-trust-backup-access-2025
08/01/2026	LeMagIT	Bilan 2025 : les ransomwares ont coûté plus de 60 milliards d'euros aux entreprises européennes. En France, le nombre d'attaques a doublé en un an. La NIS2 impose désormais un PRA documenté aux ETI.	www.lemagit.fr/actualites/ransomware-bilan-europe-2025-nis2
14/02/2026	Veeam	Veeam Data Protection Report 2026 : 74% des entreprises ayant subi une attaque ransomware ont pu restaurer leurs données grâce à des sauvegardes immuables. Le RTO moyen est passé de 28h à 6h en deux ans.	www.veeam.com/resources/vc/data-protection-report-2026.html
05/03/2026	ANSSI	L'ANSSI publie une mise à jour de son référentiel PRA/PCA intégrant les environnements hybrides (cloud + on-premise). Les entreprises soumises à NIS2 ont jusqu'au 01/07/2026 pour se conformer.	www.ssi.gouv.fr/guide/referentiel-pra-pca-nis2-2026

Ce que j'ai retenu

- La règle 3-2-1 est la base : 3 copies, 2 supports, 1 hors site
- Les sauvegardes doivent être immuables (impossibles à modifier) pour résister aux ransomwares
- Un PRA doit être testé régulièrement sinon il ne sert à rien
- Le cloud devient obligatoire pour externaliser et sécuriser les sauvegardes
- 60% des PME victimes de ransomware déposent le bilan
- 76% des collectivités françaises n'ont ni PRA ni PCA
- Le facteur humain = 60% des failles (erreur, phishing)
- Triple extorsion : chiffrement + vol + DDoS pour faire pression

Conclusion

Cette veille montre que la sauvegarde et le PRA sont indispensables face aux ransomwares. Les attaques de 2025 sont violentes et professionnalisées. Tout technicien SISR doit maîtriser ces concepts pour protéger les données et assurer la continuité d'activité en cas d'incident.