Assurer la continuité des services publics

Protégez les infrastructures électriques, hydrauliques, de gaz naturel et d'énergie revouvelable.

Les enjeux

Les services publics ne se résument pas à l'éclairage. Ils permettent aux hôpitaux de fonctionner grâce à l'alimentation de secours, ils fournissent de l'eau potable sans danger, acheminent le gaz vers les foyers en hiver et permettent aux services d'urgence d'intervenir. Lorsqu'un service public n'est plus assuré, il entraîne d'autres défaillances, d'autres secteurs.

Des groupes liés à des États ont démontré que l'objectif vise davantage la perturbation que le vol de données. Volt Typhoon est resté 300 jours non détecté au sein d'un service public américain d'électricité et d'eau, cartographiant les procédures d'exploitation OT et la topologie du réseau.[1] Le FBI et la CISA ont confirmé que le modèle n'est pas isolé : les services publics sont devenus une cible principale pour les attaquants liés à des États, les groupes de ransomware et les attaques destructrices.

Cette perturbation a de fortes chances de frapper un poste de transformation distant, une station de pompage d'eau ou un site de production rural, où aucun professionnel IT n'est sur site et où le spécialiste le plus proche peut se trouver à plusieurs heures de route. La fenêtre pour rétablir l'électricité, la pression de l'eau ou le débit de gaz vers une communauté se mesure en minutes, et non en jours ouvrables.

L'enseignement des réseaux d'eau américains

En 2024, le plus grand service public d'eau des États-Unis a subi une cyberattaque qui n'a pas touché les systèmes opérationnels, mais a contraint à suspendre la facturation et à fermer le portail. Les systèmes IT dont dépendent les OT, notamment Active Directory, les historiques, les SIG, les systèmes de gestion des coupures et la facturation, entrent également dans le champ d'application.[2]

[1] https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days

[2] https://www.amwater.com/press-room/press-releases/corporate/american-water-reactivating-systems-after-cyber-event-10102024

Contexte de menace

Un quart des organisations ICS / OT ont subi un incident de cybersécurité confirmé au cours de l'année écoulée. Pas des alertes. Les incidents confirmés ont touché des systèmes opérationnels, 40 % provoquant une perturbation opérationnelle directe et près d'un sur cinq nécessitant plus d'un mois pour être résolu. Pour les services publics, ce délai de restauration n'est pas une statistique. Cela signifie des jours sans électricité, eau ou gaz fiables pour les communautés qui en dépendent.

1 sur cinq

organisations ICS / OT ont subi un incident de cybersécurité au cours de l'année écoulée.

SANS State of ICS/OT Security 2025

40 %

de ces incidents ont causé une perturbation sur le plan opérationnel de la production, de la fourniture de services ou des opérations publiques. 37,9 % provenaient d'un ransomware.

SANS State of ICS/OT Security 2025

19 %

des incidents OT ont mis plus d'un mois à être restaurés en 2025. La détection s'est améliorée. La restauration reste le point critique.

SANS State of ICS/OT Security 2025

Les services publics de taille petite et moyenne sont des cibles privilégiées pauvres en cybersécurité : des cibles à forte valeur ajoutée sans équipes de cybersécurité dédiées et avec des ressources de restauration limitées.

La solution : une restauration efficace là où votre équipe ne peut pas intervenir

Acronis Cyber Protect for OT offre une cyberrésilience de niveau IT aux environnements OT des services publics sans perturber les opérations en direct. La solution répond à une réalité opérationnelle essentielle : lorsqu'un incident se produit dans un poste électrique distant, une station de pompage ou un site énergétique, la personne la plus proche du système peut très bien être un ingénieur en automatisation ou un chef d'équipe, et non un spécialiste de la cybersécurité. Les workflows de restauration sont conçus pour fonctionner localement, avec une dépendance minimale à la connectivité externe ou à l'intervention de spécialistes.

Sauvegarde sans perturbation
Sauvegarde d'image ou de fichiers sans redémarrage ni interruption d'activité. Le mode secteur par secteur s'active automatiquement pour les systèmes de fichiers OT propriétaires. Instantanés VSS cohérents sur des configurations SCADA historiques.

Restauration en un clic pour les opérateurs
Le personnel local autorisé, y compris les ingénieurs de sous-station, les responsables des opérations liées à l'eau et les superviseurs, peut suivre un workflow de restauration guidé pour restaurer un système en panne à son dernier état opérationnel connu, ce qui permet de réduire le temps de restauration de plusieurs heures ou jours à quelques minutes, selon les conditions du site.

Sur système nu et Universal Restore
Restaurer automatiquement sur un matériel différent ou de remplacement. Universal Restore injecte les pilotes appropriés sans reconfiguration manuelle, ce qui est critique lorsque le PC industriel d'origine est obsolète ou indisponible.

Restauration sûre et vérifiée
Les images de sauvegarde sont analysées à la recherche de malware et validées avant la restauration, ce qui contribue à réduire le risque de réinfection d'un système SCADA ou IHM restauré. Les menaces détectées sont signalées et peuvent être supprimées dans le cadre du workflow de restauration.

Fonctionnement hors ligne et en environnement isolé
Tous les composants sont déployés sur site.
Le serveur de gestion fonctionne hors ligne.
Les définitions antimalware se mettent à jour sans accès Internet, et les agents continuent d'assurer la protection pendant 30 jours si le serveur de gestion est inaccessible.

Stockage de sauvegarde immuable
Les archives de sauvegarde ne peuvent pas être supprimées, modifiées ou chiffrées par un ransomware, même si les identifiants sont compromis. Modes Gouvernance et Conformité avec des périodes de rétention jusqu'à 10 ans pour répondre aux obligations réglementaires.

Systèmes traditionnels : protéger ce que d'autres ont abandonné

Les ressources OT des services publics peuvent fonctionnent pendant plus de 30 ans. Les systèmes informatisés qui les gèrent, notamment les IHM, les serveurs SCADA et les postes de travail d'ingénierie, exécutent souvent des systèmes d'exploitation que les fournisseurs grand public ont cessé de prendre en charge il y a des années.

Windows 10 pour OT : gérer le risque lié au cycle de vie[3]

De nombreux postes de travail OT des services publics exécutent encore des éditions de Windows 10 avec différentes échéances de support. Certains ne sont déjà plus pris en charge, tandis que d'autres ont un cycle de vie allant jusqu'à 2027, 2029 ou plus tard encore. Mettre à niveau ou appliquer un correctif à ces systèmes n'est souvent pas une simple actualisation ; cela peut déclencher une nouvelle validation coûteuse, impacter des logiciels SCADA / IHM sous licence ou annuler les contrats de support OEM. Acronis agit comme un contrôle compensatoire, en associant la sauvegarde d'image à la liste d'autorisation des applications pour aider à exploiter plus sûrement les systèmes traditionnels lorsqu'une migration immédiate du système d'exploitation n'est pas réalisable.

Acronis offre un support complet de sauvegarde et de restauration depuis Windows XP SP1 / SP2 / SP3 jusqu'à Windows Server 2025, du noyau Linux 2.6.9 à 5.19 et de tous les principaux hyperviseurs, couvrant chaque génération de systèmes OT.

Restauration et recovery : il y a une distinction à faire

Dans les environnements des services publics, confondre ces deux termes porte préjudice à la continuité de service et, dans les pires cas, à la sécurité publique.

Le recovery consiste à rétablir le contrôle de fréquence ou à reprendre la pression de l'eau rapidement, à partir de tout état validé disponible. Les opérations partielles qui maintiennent un hôpital sous tension ne constituent pas un état de défaillance. C'est la mission prioritaire.

La restauration consiste à ramener en toute sécurité l'ensemble de la pile de systèmes certifiés à une base de référence connue et saine, sans réintroduire de malware ni de corruption.

Acronis prend tout en charge. One-Click Recovery aide à assurer une continuité opérationnelle rapide, en permettant au personnel autorisé d'initier la restauration localement sans l'intervention de spécialistes. La sauvegarde d'investigation validée assure une restauration complète et vérifiée, y compris l'analyse des images de sauvegarde à la recherche de malware en amont et la fourniture de chaînes de preuves notarisées sur blockchain pour l'investigation numérique post-incident et l'audit.

Selon le rapport SANS State of ICS/OT Security 2025, alors que près de la moitié des incidents OT sont détectés dans les 24 heures, 19 % nécessitent plus d'un mois pour être pleinement restaurés. La détection s'est améliorée. La restauration reste le point critique.

[3] https://learn.microsoft.com/en-us/windows/release-health/release-information

La protection Acronis des services publics

Environnement des services publics	Systèmes et données protégés par Acronis
Électricité : production, transmission et distribution	Serveurs SCADA / EMS, PC de contrôle de sous-station, postes de travail IHM, contrôleurs DER / micro-réseau, contrôleurs de site BESS, serveurs d'historique. Les données protégées comprennent les images du système d'exploitation, les configurations SCADA / IHM, la logique d'alarme, les bases de données historiques et les fichiers de projet d'ingénierie.
Systèmes d'eau et d'eaux usées	Systèmes SCADA de traitement de l'eau, postes de travail IHM, PC de contrôle de pompes et de stations de relevage, systèmes de surveillance de réservoirs. Les données protégées comprennent les images du système d'exploitation, les configurations des processus de traitement, la logique de contrôle des pompes et les données de reporting réglementaire.
Distribution de gaz naturel	Serveurs de surveillance de pipelines, PC de stations de compression, PC de stations de régulation, serveurs SCADA, systèmes de transfert de garde. Les données protégées comprennent les configurations de processus, les données de surveillance, les fichiers d'étalonnage et les enregistrements opérationnels des pipelines.
Énergie renouvelable : éolien, solaire, biomasse et hydrogène vert	PC de contrôleur de turbine / onduleur, serveurs de gestion d'usine, systèmes de gestion BESS, surveillance environnementale. Les données protégées comprennent les logiciels de contrôle, les configurations du site et les jeux de données opérationnels.
Systèmes IT dont dépendent les OT	Active Directory / DNS, hôtes de rebond, historiques (côté IT), SIG, OMS, AMI / MDMS, facturation et portails clients. Les données protégées comprennent les images système, les données de configuration, les dossiers clients et opérationnels.

Intégration SIEM : l'intégration SIEM sur site d'Acronis transmet les alertes de sauvegarde, de sécurité et de gestion RMM aux outils SIEM tiers via syslog, aidant les équipes OT et de sécurité à centraliser la visibilité des incidents dans tous les environnements protégés.

Conformité et assurance

Acronis aide les services publics à générer des preuves de plan de restauration et des enregistrements de validation des sauvegardes, des résultats de test de restauration et des contrôles de rétention, ainsi qu'une documentation d'assurance fournisseur sécurisée pouvant soutenir la préparation aux audits au regard des principaux cadres. Acronis est certifiée IEC 62443-4-1.

NERC CIP (Amérique du Nord)

Peut aider à fournir des preuves pour la documentation du plan de restauration CIP-009 grâce aux enregistrements de validation des sauvegardes et aux données d'investigation. Conçu pour fonctionner dans des réseaux totalement isolés, sans dépendance au cloud.

Directive NIS 2 (Europe)

Peut contribuer aux attentes de l'article 21 en matière de continuité des activités et de gestion des sauvegardes. Les sauvegardes immuables et les périodes de rétention configurables sont alignées sur l'intention de protection des données et de préparation à la restauration de NIS 2.

IEC 62443 (global)

Certification IEC 62443-4-1 SSDLC. Les sauvegardes en temps réel, non perturbatrices, et la vérification de l'intégrité s'alignent sur les attentes de disponibilité des ressources et de continuité au regard du cadre IEC 62443.

Loi européenne sur la cyberrésilience

La certification du cycle de développement sécurisé peut soutenir les évaluations d'assurance des fournisseurs OEM qui sont de plus en plus exigées dans les achats des services publics au regard du CRA de l'UE.

Remarque : Acronis prend en charge les preuves de plan de restauration et la préparation aux audits. Le respect de tout cadre réglementaire reste de la responsabilité de l'exploitant.

Partenaires OEM et intégrateurs

Acronis Cyber Protect for OT est disponible en marque blanche, co-labellisée ou vendue comme solution de référence, permettant aux partenaires OEM et aux intégrateurs de systèmes de contrôle d'intégrer directement la cyberrésilience OT dans leur offre de systèmes des services publics.

Acronis travaille à l'échelle mondiale avec des OEM et des partenaires de technologies industrielles dans des environnements OT, notamment ABB, Emerson, GE Vernova, Honeywell, Rockwell Automation, Schneider Electric et Yokogawa.

Pour les partenaires OEM

- Intégrez One-Click Recovery nativement. Devenez un partenaire de résilience, et non seulement un fournisseur de matériel.
- Aidez à réduire le volume des appels réactifs et les coûts de déplacement des ingénieurs pour les scénarios de restauration courants.
- Développez des services de résilience récurrents et managés et augmentez vos revenus contractuels.
- Certifié IEC 62443-4-1, ce qui devient de plus en plus déterminant dans les achats de services publics et la conformité au règlement européen CRA.

Pour les intégrateurs de systèmes de contrôle

- Intégrez la restauration dans la livraison des serveurs SCADA / IHM / OT.
- Standardisez les procédures de restauration sur l'ensemble des systèmes de services publics livrés.
- Réduisez la charge de support après déploiement et les risques liés à l'accord de niveau de service (SLA).
- Ajoutez des services de résilience récurrents aux portefeuilles de projets et de services managés.
- Proposez en marque blanche ou co-labellisez avec votre activité d'intégration.

Prêt à protéger les infrastructures dont les communautés dépendent ?

Contactez un spécialiste Acronis OT ou votre partenaire OEM pour organiser une démonstration en direct.

CONTACTER UN EXPERT OT

Acronis

Pour en savoir plus : acronis.com