TAG

ACRONIS, LEADER DE LA CYBERRÉSILIENCE DES TECHNOLOGIES OPÉRATIONNELLES (OT) : EXPLICATIONS

DR EDWARD AMOROSO,
PDG, TAG INFOSPHERE

Acronis

ACRONIS, LEADER DE LA CYBERRÉSILIENCE DES TECHNOLOGIES OPÉRATIONNELLES (OT) : EXPLICATIONS

EDWARD AMOROSO, PDG, TAG

INTRODUCTION :

Depuis des décennies, la cybersécurité est souvent associée à la protection des technologies de l'information (IT) contre les attaques malveillantes. C'est en tous cas la mission des responsables de la sécurité des systèmes d'information (RSSI). Depuis peu, la cybersécurité englobe aussi les systèmes d'exploitation, industriels, physiques et concrets. Il en résulte une nouvelle industrie, celle de la sécurité des technologies opérationnelles (OT).

La sécurité OT ayant vu le jour après la sécurité IT, les deux ont en commun nombre de contrôles. Gagner en visibilité et déployer des mesures d'atténuation sont par exemple au cœur des stratégies de sécurité à la fois IT et OT, ce qui s'avère utile tandis que la sécurité OT continue de s'imbriquer dans des initiatives IT plus larges. De nombreux responsables de la sécurité des systèmes d'information (RSSI) se voient d'ailleurs confier l'entière responsabilité de la sécurité OT.

Comme on pouvait s'y attendre, de nombreuses faiblesses qui caractérisent les schémas de sécurité informatique traditionnels se retrouvent dans les systèmes de protection industriels. La plus évidente concerne probablement la résilience souvent fragile des systèmes OT lorsqu'ils sont attaqués. Des ransomwares sont notamment parvenus à perturber de vastes environnements opérationnels, avec des conséquences graves pour les clients.

Mais les environnements de sécurité OT présentent aussi de multiples problèmes bien spécifiques. Ces problèmes sont généralement liés à l'absence dans la plupart des environnements OT de personnel en local formé à la sécurité, mais aussi à la multitude d'anciens systèmes propriétaires présents sur ces réseaux, et aux environnements opérationnels souvent complexes qui rendent particulièrement difficile l'exécution de mises à jour ou l'installation de correctifs sans perturber les opérations en cours (par exemple, une usine ou un site de production).

Ce rapport explique comment les équipes de sécurité des technologies OT, qui sont parfois désormais dirigées par des responsables de la sécurité des systèmes d'information (RSSI), peuvent améliorer leur résilience opérationnelle en privilégiant une seule fonction clé : la sauvegarde et la restauration. Cet aspect de la cyberprotection a toujours été un défi pour les équipes de sécurité informatique, car le déploiement de solutions efficaces suppose une connaissance approfondie de l'infrastructure, et dans ce domaine la plupart des fournisseurs sont traditionnellement plus axés sur les opérations informatiques que sur la sécurité.

Dans les environnements OT, nous pensons que la sauvegarde et la restauration sont les éléments les plus importants de toute initiative visant à améliorer la sécurité. Il est probablement nécessaire de fixer d'autres objectifs pour mieux former le personnel OT à la sécurité et réduire le nombre d'anciens systèmes toujours en place. Nous avons la conviction qu'il appartient aux ingénieurs spécialistes de la sécurité des systèmes OT de se concentrer sur cet élément clé de leur environnement.

Pour illustrer notre point de vue, nous prendrons pour exemple les solutions de cyberrésilience modernes de l'éditeur Acronis. Leur approche de la sauvegarde et de la restauration, quelle que soit la nature de l'infrastructure (IT ou OT), semble bien adaptée aux cybermenaces toujours plus nombreuses qui ciblent les activités industrielles des secteurs tels que la fabrication, les transports, l'énergie, la défense, etc., qui ne peuvent tolérer la moindre perturbation.[1]

SÉCURITÉ ACTUELLE DES SYSTÈMES OT

Comme nous l'avons indiqué précédemment, l'une des différences les plus marquées du manque de résilience entre les infrastructures IT et OT réside dans les conséquences potentiellement plus graves des problèmes de sécurité opérationnelle. La résilience insuffisante des contrôles industriels peut, par exemple, provoquer des défaillances des systèmes de sécurité, des arrêts de la chaîne de production ou des difficultés de fonctionnement des centrales nucléaires. L'on imagine alors aisément le risque pour les vies humaines.

La sécurité des environnements OT doit donc être une priorité absolue. Ces environnements présentent toutefois des difficultés liées à l'utilisation de technologies hétérogènes et propriétaires, souvent avec des équipements et des systèmes d'exploitation obsolètes. Cela limite la possibilité d'appliquer des correctifs et des mises à jour, sans parler des fenêtres de sauvegarde très courtes dans des environnements qui sont souvent mal pourvus en personnel qualifié et en ressources informatiques adaptées.

Et les tentatives d'isoler les environnements OT des pirates en insérant une passerelle entre environnements IT et environnements OT ne donnent pas de résultats concluants. L'objectif initial, qui consiste à isoler les systèmes OT de l'Internet en créant un périmètre IT/OT, échoue comme c'est le cas pour tous les périmètres. Cette approche peine à identifier les menaces internes, manque les voies d'accès autour du périmètre, ignore la nature poreuse de tout périmètre, etc.

La stratégie de passerelle IT/OT ne résout pas non plus les problèmes de sécurité OT précités, liés aux systèmes propriétaires, à la difficulté d'application de correctifs, au manque de formation à la sécurité des équipes, etc. L'illustration ci-dessous montre en quoi une passerelle IT/OT ne permet pas de résoudre ces problèmes de sécurité. L'objectif principal n'est pas non plus traité, à savoir la résilience de la sécurité des systèmes OT via des capacités de sauvegarde et de restauration.

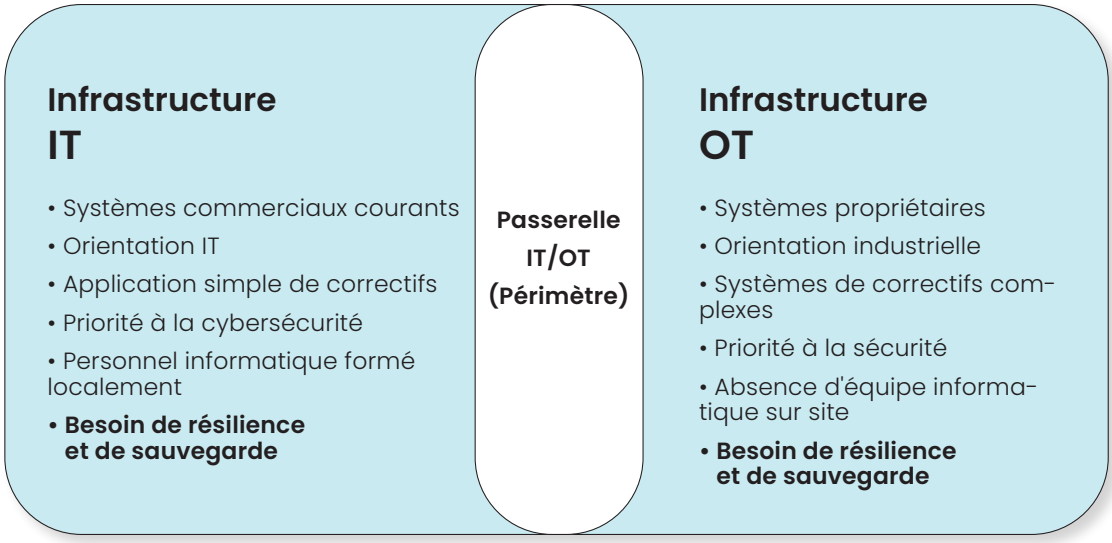

Figure 1. Défis liés à la sécurité des systèmes OT

Nous comprenons effectivement que la totale sécurité des systèmes OT nécessite des solutions en réponse à l'ensemble de ces problèmes. Mais nous pensons toutefois, et nous l'expliquerons ci-dessous, que la garantie de continuité des opérations face aux ransomwares, tentatives de sabotage et cyberattaques destructrices doit être l'objectif prioritaire des déploiements de sécurité OT modernes. Nous allons étudier ce cas dans le contexte de la plate-forme Acronis et de ses capacités de sécurité pour les systèmes OT.

SOLUTIONS DE SAUVEGARDE ET DE RESTAURATION ACRONIS POUR LES SYSTÈMES OT ET ICS

Notre expérience montre que les programmes de sécurité des systèmes OT doivent couvrir trois domaines complémentaires. Pour commencer, ils doivent assurer la visibilité de l'environnement OT, souvent au moyen de plates-formes commerciales comme Claroty et Dragos. La visibilité sur les menaces est essentielle et il convient de s'efforcer de l'améliorer systématiquement. Cela suppose une meilleure formation, et peut-être une plus grande importance accordée aux simulations de cyberattaques des réseaux OT.

Deuxièmement, nous pensons que les équipes de sécurité informatique doivent être incitées à créer des contrôles plus convergents alignés sur l'intégration des systèmes OT et IT. Il est par exemple recommandé de suivre les tendances Zero Trust OT, ce qui implique que de plus en plus de systèmes opérationnels se connectent au cloud et à d'autres systèmes informatiques traditionnels. Cela permet d'étendre les contrôles informatiques, tels que les plates-formes de protection des applications cloud natives (CNAPP), à l'infrastructure OT.

Mais surtout, nous recommandons aux équipes de sécurité des systèmes OT de se concentrer davantage sur la résilience opérationnelle. En pratique, cela implique la nécessité de garantir la continuité de l'activité grâce à des solutions de sauvegarde et restauration automatisées. Ceci vaut bien entendu pour les systèmes informatiques, mais comme nous l'avons déjà suggéré, toute perturbation d'un système OT peut avoir des conséquences bien plus graves, notamment pour la sécurité des personnes. Or la solution Acronis peut aider à éviter ces problèmes.

La plate-forme Acronis couvre parfaitement les exigences spécifiques de sécurité et de résilience des infrastructures OT. Il s'agit là d'une excellente nouvelle pour les équipes informatiques des entreprises qui n'ont ainsi pas à développer leur propre solution de sauvegarde et restauration, y compris si leurs équipements matériels et leurs logiciels sont obsolètes et propriétaires. Les principales fonctions de résilience des systèmes OT de la suite Acronis sont les suivantes :

1. **Restauration rapide des systèmes OT** – Acronis propose une protection hautes performances des ordinateurs OT, permettant de restaurer rapidement les opérations afin d'éviter les arrêts coûteux des chaînes de production. Cette fonctionnalité de restauration rapide est cruciale pour réduire au minimum les interruptions d'activité et maintenir la continuité opérationnelle.
2. **Restauration universelle des ordinateurs** – Acronis Cyber Protect garantit la restauration fiable et rapide de tout ordinateur, y compris des anciens systèmes datant de Windows XP, avec des options de restauration sur système nu. Cette fonctionnalité est essentielle pour la continuité d'activité des environnements OT qui tournent toujours sur d'anciens systèmes.
3. **Plans de sauvegarde personnalisables** – Acronis permet de créer des plans de sauvegarde personnalisables adaptés aux exigences spécifiques des environnements OT et ICS, pour une protection adéquate des données et systèmes critiques. Le besoin de personnalisation augmente à mesure que les infrastructures OT se modernisent grâce à l'intelligence artificielle et à des méthodes de distribution plus durables.
4. **Intégration avec des outils tiers** – Acronis propose une vue unifiée de la sauvegarde et de la restauration, avec un contrôle centralisé et des options d'intégration d'outils tiers, pour simplifier la gestion et améliorer l'efficacité opérationnelle. L'intégration d'outils de sécurité est particulièrement difficile dans les environnements OT ; cette fonctionnalité est donc particulièrement importante.
5. **Options de souveraineté des données** – Pour se conformer aux exigences de souveraineté des données, les entreprises ont le choix entre le stockage en interne ou dans les centres de données mondiaux d'Acronis, avec des options telles qu'Amazon S3 et Microsoft Azure. Acronis accompagne les clients dans le choix du mode d'hébergement le mieux adapté.

6. **Restauration en libre-service pour les télétravailleurs** – Acronis propose des options de restauration en libre-service pour les télétravailleurs. Ainsi, des utilisateurs sans compétences techniques peuvent lancer des processus de restauration, décentraliser efficacement les ressources informatiques et accélérer le retour à la normale suite à un incident.

ARCHITECTURE DE LA PLATE-FORME ACRONIS

La plate-forme Acronis Cyber Protect repose sur un entrepôt de données où sont stockées et protégées les sources actuelles, historiques et autres des données OT des entreprises. Plusieurs instances de la console de la plate-forme Acronis Cyber Protect peuvent être installées dans l'environnement OT, assorties de plusieurs agents déployés dans l'environnement pour collecter et restaurer les données. Les métadonnées sont transmises des consoles à l'entrepôt.

Des tableaux de bord et des consoles de surveillance de tous les aspects du processus de sauvegarde et de restauration sont fournis pour chaque déploiement de Cyber Protect, ainsi que pour le Hub de surveillance centralisé d'Acronis. Ce hub fournit des vues historiques, avec reporting et surveillance personnalisables, en cours d'exécution de la procédure de sauvegarde et restauration. Bien entendu, l'objectif est de garantir la continuité de l'activité en cas d'incident, d'attaque ou de tout autre problème risquant d'affecter la résilience (voir la figure 2).

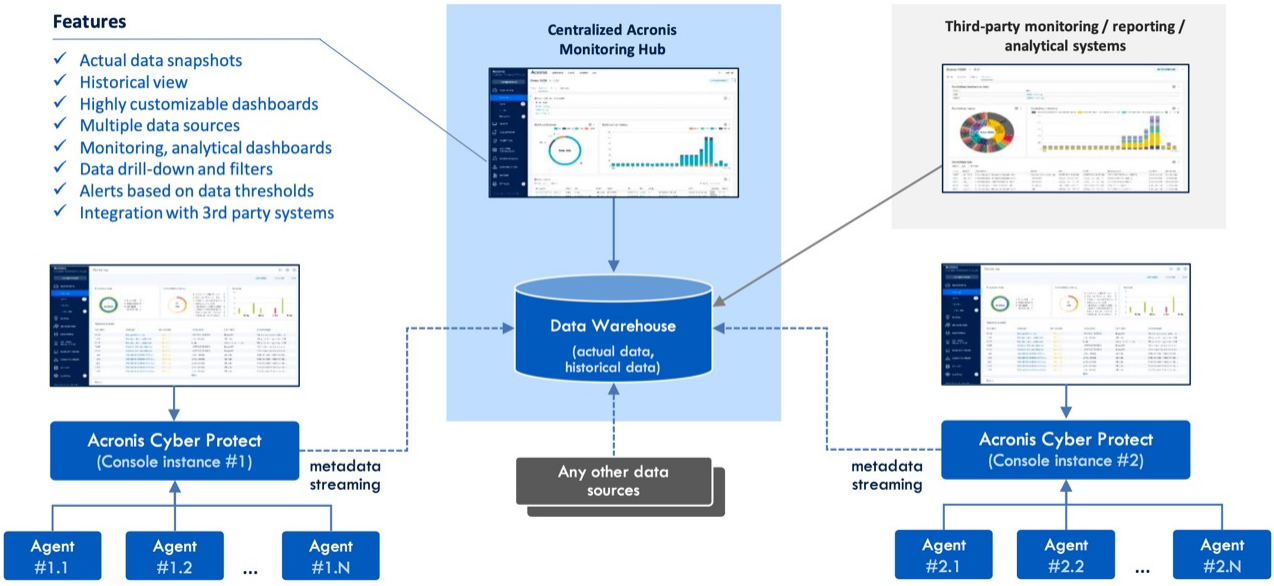

Figure 2. Architecture système Acronis

INTÉGRATIONS ACRONIS

Acronis Cyber Protect (notez les deux instances représentées dans le diagramme) unifie la sauvegarde, la reprise d'activité après sinistre, la protection contre les malwares basée sur l'intelligence artificielle, le support à distance et les outils de sécurité en intégrant l'ensemble dans une plate-forme unique pour l'équipe de sécurité, environnement OT compris. Cette consolidation permet à toute entreprise, y compris les équipes de sécurité OT, de gérer divers aspects de la cyberprotection via une seule interface, ce qui réduit la complexité et améliore l'efficacité.

L'architecture flexible de la plate-forme, ainsi que ses interfaces de programmation d'applications et de ligne de commande, permettent à Acronis et à des tiers de développer et d'intégrer des applications tierces (notez les flux de données tiers représentés dans la figure 2, qui se connectent à l'entrepôt de données central). Cet écosystème dynamique permet d'intégrer ultérieurement des services de protection, de gestion et d'automatisation,

garantissant ainsi que la plate-forme s'adapte aux évolutions des paysages de cybersécurité. Les entreprises peuvent ainsi intégrer avec une totale flexibilité les solutions Acronis dans leurs infrastructures existantes, et renforcer la résilience et la sécurité de leurs activités, particulièrement dans les environnements OT.

SAUVEGARDE DES DONNÉES D'INVESTIGATION ACRONIS

Acronis Cyber Protect inclut une fonctionnalité de sauvegarde des données d'investigation afin de simplifier les analyses futures par la collecte de preuves numériques à partir de sauvegardes de disque. Cette fonctionnalité s'adresse tout particulièrement aux entreprises soumises à des exigences de conformité strictes et qui doivent mener des enquêtes internes efficaces. Elle est également cruciale pour les environnements OT, où de telles investigations numériques peuvent aider à identifier les attaques ciblant les infrastructures critiques et les services essentiels.

Le processus de sauvegarde des données d'investigation Acronis implique la création d'images de disque complètes, y compris des données actives, de l'espace libre et des vidages mémoire. Cette approche rigoureuse, qui devient un impératif de sécurité des systèmes OT, garantit que toutes les preuves numériques potentielles sont préservées correctement, ce qui facilite des analyses approfondies post-incident et le respect des obligations légales et réglementaires.

En intégrant la collecte de données d'investigation numérique aux processus de sauvegarde réguliers, Acronis permet aux entreprises fonctionnant avec des environnements informatiques et opérationnels de maintenir la continuité des opérations tout en garantissant la disponibilité immédiate des informations d'investigation numérique chaque fois que nécessaire. Cette intégration élimine la nécessité de disposer de processus distincts de collecte de données d'investigation numérique, ce qui rationalise les opérations et réduit le risque de perte de données en cas d'incidents.

ACRONIS INTEGRATED DISASTER RECOVERY

Acronis Cyber Protect intègre une solution de reprise d'activité après sinistre qui réduit la complexité et les coûts. En combinant les fonctionnalités de sauvegarde et de reprise d'activité après sinistre, la plate-forme garantit aux entreprises qu'elles pourront restaurer rapidement leurs ressources suite aux événements tels que les catastrophes naturelles, erreurs humaines, cyberattaques ou défaillances matérielles. Comme nous l'avons vu, de tels événements peuvent avoir des conséquences graves dans le contexte des systèmes OT.

Les fonctionnalités de reprise d'activité après sinistre incluent la possibilité de démarrer rapidement des ressources IT ou OT, des runbooks pour automatiser les processus de restauration, et des tests de basculement pour vérifier le bon fonctionnement des systèmes en cas de sinistre. Ces fonctionnalités sont essentielles pour assurer la continuité des activités et réduire au minimum les interruptions d'activité, en particulier pour les applications en temps réel, très répandues dans les environnements OT.

En intégrant reprise d'activité après sinistre, cybersécurité et gestion des terminaux, Acronis propose une approche globale de la cyberprotection. Tous les aspects de l'infrastructure informatique d'une entreprise sont ainsi protégés, pour une meilleure résilience face à un large éventail de perturbations potentielles. Cette intégration simplifie également la charge de travail des RSSI qui sont à la fois responsables des systèmes IT et OT de production.

ALIGNEMENT AVEC LES EXIGENCES RÉGLEMENTAIRES

En plus des impératifs opérationnels des sauvegardes et de la résilience, les équipes de sécurité des systèmes OT doivent de plus en plus tenir compte de nouveaux cadres de conformité et de réglementation externes. La conformité en matière de cybersécurité des systèmes OT devient bien plus difficile à gérer pour les entreprises, notamment en raison d'exigences convergentes qui évoluent avec l'augmentation des menaces.

Plus précisément, nous constatons que les instances de réglementation mondiales mettent l'accent sur la résilience opérationnelle, comme c'est le cas avec le règlement Digital Operational Resilience Act (DORA) de l'Union européenne et les recommandations du Comité de Bâle sur le contrôle bancaire, d'où la nécessité de

mesures de cybersécurité robustes dans les secteurs des infrastructures critiques. Les solutions Acronis aident à respecter ces exigences réglementaires au travers de fonctionnalités dans les domaines suivants :

1. **Cadres complets de gestion des risques** – Les solutions Acronis permettent aux équipes de sécurité des entreprises d'implémenter des cadres de gestion des risques adaptables, de tester la résilience régulièrement et de maintenir une communication ouverte avec les parties prenantes et les régulateurs, en total alignement avec l'ensemble des cadres de résilience opérationnelle applicables aux environnements informatiques et opérationnels.
2. **Plan d'intervention sur incidents** – Acronis aide ses clients à élaborer et rédiger des plans d'intervention sur incidents, individuels ou intégrés à un plan de continuité des activités, pour qu'ils soient prêts en cas de cybermenace. Il s'agit d'une nouvelle tâche pour de nombreuses équipes de sécurité OT, d'où l'importance d'être accompagnées par Acronis.
3. **Gestion des risques liés aux tiers** – Les capacités d'intégration d'Acronis incluent une surveillance robuste des tiers, un composant critique de la résilience opérationnelle selon les régulateurs. Comme nous l'avons vu plus tôt, l'intégration avec des tiers en matière de cybersécurité peut être difficile, car elle a été ignorée ou sous-estimée jusqu'à présent.

LES GRANDS FOURNISSEURS DE SOLUTIONS D'AUTOMATISATION OT ET ICS FONT CONFIANCE À ACRONIS

L'adoption des solutions Acronis de sauvegarde et de restauration par les plus grands fournisseurs au monde de plates-formes OT et ICS souligne leur capacité de résilience au sein des environnements OT et industriels. Des leaders du secteur, tels qu'ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation et Yokogawa, intègrent Acronis Cyber Protect dans leurs plates-formes, soit en marque blanche, soit en co-branding, pour assurer la résilience opérationnelle de leurs clients. Ceci témoigne de la fiabilité et de la flexibilité de la plate-forme, et de sa position de leader du marché en matière de sauvegarde et de restauration des systèmes OT.

CONCLUSION ET PLAN D'ACTION POUR LES ÉQUIPES DE SÉCURITÉ OT

Nous pensons que les solutions de sauvegarde et de restauration d'Acronis sont parfaitement adaptées aux clients qui souhaitent renforcer la résilience et la sécurité de leur infrastructure OT. En proposant des fonctionnalités de restauration rapide, le support des systèmes existants, des plans de sauvegarde personnalisables et la conformité aux exigences réglementaires, Acronis permet aux entreprises d'assurer la continuité de leur activité et de respecter les normes mondiales de résilience opérationnelle en constante évolution.

Nous conseillons aux RSSI concernés, ainsi qu'à toute autre équipe de direction ou de gestion cherchant à garantir la cyberrésilience des systèmes OT, de prendre immédiatement contact avec Acronis pour en savoir plus sur les capacités proposées. Les équipes TAG sont également disponibles à tout moment pour aider les lecteurs à approfondir leurs connaissances sur ce sujet et sur d'autres thèmes liés à la cybersécurité et à l'intelligence artificielle. Nous attendons de vos nouvelles avec impatience !

[1] Nous remercions tout particulièrement les équipes techniques et de direction d'Acronis de nous avoir aidés à comprendre les différents risques qu'elles observent dans les environnements OT de leurs clients. Elles nous ont donné accès à la documentation de leurs solutions et nous ont renseignés sur les feuilles de route de leurs solutions pour la sécurité des environnements informatiques et opérationnels.

À PROPOS DE TAG

TAG est une société réputée de recherche et de conseil qui fournit des informations et des recommandations en matière de cybersécurité, d'intelligence artificielle et de science du climat à des milliers de fournisseurs de solutions commerciales et à des entreprises du classement Fortune 500. Fondée en 2016 et basée à New York, TAG se démarque des cabinets de conseil classiques en proposant des conseils impartiaux et approfondis, des analyses de marché, du consulting de projet et des contenus personnalisés, le tout sous l'angle du praticien.