Comment concevoir la sécurité des environnements et réseaux OT

Prévenir, détecter et maîtriser les menaces avancées

Table des matières

Synthèse

Des cyberattaques sophistiquées mettent en danger les systèmes de contrôle industriel (ICS) et les systèmes de contrôle de surveillance et d'acquisition de données (SCADA). Alors que les réseaux industriels (OT - operational technology) convergent avec les technologies de l'information (IT), l'élargissement de la surface d'attaque permet aux cybermenaces avancées de cibler ces systèmes critiques. Les systèmes ICS et SCADA sur les réseaux OT présentent des exigences opérationnelles uniques qui peuvent les rendre plus difficiles à sécuriser que leurs homologues IT. Ainsi, les réseaux OT nécessitent des approches et des solutions de sécurité conçues spécialement pour eux.

L'utilisation de pratiques de sécurité automatisées et de technologies de leurre (technologies dites « deceptive ») aide à détecter les menaces avancées au sein des réseaux OT. Les solutions de sécurité au niveau du réseau identifient et contrôlent la propagation des cyberattaques provoquées par les pirates sur un réseau OT. Une veille sur les menaces spécifiques à l'OT est un élément central de cette stratégie, qui permet d'identifier rapidement les menaces visant plusieurs sites OT ou les menaces globales contre les environnements industriels, et d'y répondre.

64 % des décideurs en matière d'OT affirment que les cyberattaques sophistiquées constituent un défi majeur.[1]

Introduction

Les systèmes OT sont confrontés à de nouvelles cybermenaces. Par le passé, les réseaux OT étaient physiquement isolés des systèmes informatiques par un « air gap ». Cependant, de nombreuses entreprises éliminent ou minimisent ce cloisonnement, pour pouvoir apporter l'innovation digitale au sein de leurs environnements OT. En conséquence, les réseaux OT et IT sont de plus en plus connectés entre eux, tandis que les cybercriminels utilisent les réseaux IT comme passerelle vers le réseau OT.

Les systèmes OT ont souvent une durée de vie longue, intégrant des composants qui ont des cycles de vie sur le terrain de 20 ans ou plus dans certains cas. Il n'est pas rare que ces dispositifs contiennent de nombreuses vulnérabilités facilement exploitables, découvertes au fil des années (menaces anciennes). Aujourd'hui, de nouvelles menaces émergent dans l'écosystème criminel, le dark Web permettant des attaques nouvelles et sophistiquées sur plusieurs fronts et visant spécifiquement les opérateurs de réseaux OT.

Les exigences des infrastructures OT en matière de haute disponibilité signifient que les solutions de sécurité doivent être soigneusement conçues pour garantir un impact minimal sur l'opérationnel. De plus, les réseaux OT doivent atteindre et maintenir la conformité avec les directives réglementaires spécifiques à l'OT, telles que celles créées par le National Institute of Standards and Technology (NIST), la directive de la Commission européenne sur la sécurité des réseaux et des systèmes d'information (directive NIS) et la North American Electric Reliability Corporation (NERC).

La détection et la réponse automatisées aux menaces, une veille sur les menaces spécifiques à l'OT, des technologies de leurre et la segmentation des réseaux sont quatre éléments clés d'une approche de sécurité OT robuste qui protège contre les menaces avancées.

Près des trois quarts des industriels disposent de connexions entre leurs réseaux IT et OT.[2]

La détection et la réponse automatisées aux menaces améliorent la disponibilité des systèmes

Les auteurs des menaces avancées disposent des ressources et de la sophistication nécessaires pour concevoir des attaques qui échappent aux mécanismes de détection traditionnels. Les entreprises ont besoin d'une visibilité en profondeur sur le réseau et d'une bonne connaissance de la situation pour différencier les menaces réelles des faux-positifs et pour identifier le comportement des attaques et identifier les auteurs de la menace.

Pour atteindre le niveau de visibilité nécessaire à une réaction rapide en cas d'incident, il faut recourir à l'automatisation. La collecte, l'agrégation et l'analyse automatisées des données de sécurité permettent d'identifier les menaces réelles (et éviter les trop nombreux faux-positifs) et fournissent le contexte nécessaire à une réponse aux menaces et à la mise en œuvre de mesures correctives précises.

L'automatisation peut aussi permettre une réponse plus rapide à une menace identifiée. En créant des playbooks sur les menaces qui codifient les réponses aux menaces courantes, une entreprise peut automatiser certaines parties du processus de détection des menaces et de mesures de correction. Cela contribue à répondre aux besoins de haute disponibilité des systèmes OT puisque, une fois qu'un analyste a identifié une menace active, certaines mesures correctives, voire toutes, peuvent être prises instantanément, ce qui minimise l'impact de la menace sur les opérations.

La prise en compte contextuelle de la situation et une réponse automatisée aux incidents contribuent à garantir la sécurité et la disponibilité des systèmes OT. Des réponses ciblées, qui identifient les menaces et neutralisent leurs processus, minimisent l'impact de la réponse aux incidents sur la disponibilité du système.

78 % des entreprises n'ont qu'une visibilité partielle et centralisée sur leurs environnements OT.[3]

L’automatisation renforce la disponibilité des systèmes en permettant une réponse rapide et ciblée aux cybermenaces.

La veille sur les menaces spécifiques à l'OT identifie les menaces ciblant ces technologies

Les systèmes OT sont des cibles de choix. Les cybercriminels sont prêts à investir le temps et les ressources nécessaires pour identifier et exploiter les vulnérabilités de ces systèmes. Les cybercriminels effectuent généralement des reconnaissances contre des systèmes OT spécifiques et profitent du fait que l'OT utilise des protocoles réseau propriétaires qui, souvent, ne sont pas traités par les solutions de cybersécurité conçues pour les réseaux informatiques, pour dissimuler leurs activités.

La gestion des cybermenaces contre les réseaux OT requiert des connaissances spécifiques à l'OT et plusieurs années d'expérience dans la sécurisation des environnements OT. La sécurité des réseaux OT nécessite l'accès à une veille sur les menaces spécifiques à l'OT. Comme les organisations OT intègrent des équipements provenant de différents constructeurs, la visibilité sur les vulnérabilités au sein des produits de ces fournisseurs est essentielle pour la sécurité. Cela permet aux fournisseurs OT de renforcer les systèmes contre les exploits et de déployer des patchs virtuels pour protéger efficacement les systèmes vulnérables pendant le long intervalle entre deux opérations de maintenance.

Les entreprises doivent également être en mesure de partager ces renseignements sur les menaces à l'intérieur et à l'extérieur de l'organisation et de tirer parti des renseignements sur les menaces provenant de tiers. Cela permet d'identifier et de réagir rapidement à des campagnes d'attaques généralisées spécifiques à l'OT en utilisant l'intelligence artificielle (IA) et l'apprentissage automatique (ML).

85 % des menaces OT ciblent des machines fonctionnant avec les protocoles OPC Classic, BACnet et Modbus.[4]

Les solutions de cybersécurité pour les systèmes OT nécessitent de connaître les menaces et protocoles spécifiques à l’OT.

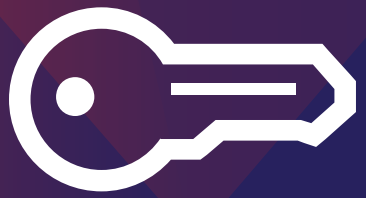
Les technologies de leurre permettent la détection des menaces avancées

Les acteurs des menaces avancées élaborent souvent des attaques « lentes et modérées » qui échappent aux défenses traditionnelles des réseaux : un assaillant peut ainsi être présent sur le réseau d'une organisation sans être détecté.

L'utilisation de technologies de leurre peut contribuer à identifier ces menaces furtives. Des « honeypots » peuvent être configurés à l'image de systèmes OT réalistes, ce qui augmente la probabilité d'attirer un cybercriminel ou une menace.

C'est ainsi qu'il devient possible d'identifier une menace furtive, puisque aucun processus légitime n'utilise ces honeypots. En outre, en examinant les détails l'activité d'un assaillant sur le système, il est possible d'obtenir des renseignements précieux sur ses outils, ses techniques et ses capacités. Ces informations de veille permettent une détection et une réponse plus efficaces à ces menaces sur d'autres systèmes du réseau OT et peuvent permettre à l'organisation d'identifier des attaques de type « zero-day » que les systèmes de détection traditionnels basés sur les signatures ne seraient pas capables d'identifier.

La sécurité de l'OT bénéficie également du déploiement de sandbox capables d'émuler des systèmes spécifiques à l'OT. Le machine learning automatisé permet de détecter des menaces inconnues en se basant sur la détection de comportements anormaux ou suspects lorsqu'ils sont exécutés au sein de ces environnements émulés.



« Un bon leurre doit être crédible. Il ne faut pas qu'il soit tellement protégé qu'il en devient impossible à le pirater, mais il ne faut pas non plus qu'il soit si vulnérable qu'il n'en est plus crédible. Si les assaillants reconnaissent le leurre, ils l'éviteront. Un leurre doit donc avoir l'air de se comporter comme les autres systèmes du réseau. »[5]

La segmentation du réseau cloisonne et maîtrise les menaces

Les environnements OT ont des exigences de disponibilité extrêmement élevées qui pèsent sur leur cybersécurité. En raison de délais serrés pour réaliser les opérations de maintenance et des exigences en matière de haute disponibilité, de nombreux appareils utilisent des systèmes d'exploitation et des logiciels en fin de vie. Les équipements obsolètes ne disposent pas des ressources nécessaires pour faire fonctionner un antivirus traditionnel. Enfin, si un incident se produit, il est souvent impossible de mettre à l'arrêt les systèmes OT infectés pour les restaurer.

Tous ces facteurs contribuent au fait que la sécurité de l'OT doit souvent être assurée au niveau du réseau plutôt qu'au niveau des terminaux. Grâce à la segmentation des réseaux et à l'application de patchs virtuels, il est possible de réduire le risque posé par les dispositifs non adaptés et vulnérables. Au lieu d'appliquer des mises à jour au dispositif, qui peuvent avoir un impact sur la disponibilité du système, le correctif virtuel garantit que le trafic qui tente d'exploiter une vulnérabilité connue est neutralisé en amont du dispositif vulnérable.

La segmentation du réseau peut également contribuer à réduire l'impact d'un incident de cybersécurité en limitant le mouvement latéral d'un adversaire à l'intérieur du réseau. La segmentation garantit que toutes les communications entre les appareils sont analysées à la recherche de contenus malveillants ou anormaux et que l'authentification forte des utilisateurs et le contrôle d'accès sont appliqués sur l'ensemble du réseau.

Les grandes entreprises OT sont 51 % plus susceptibles de segmenter leur réseau que les petites entreprises.[6]

La segmentation des réseaux est nécessaire pour empêcher la propagation en interne des menaces sur les réseaux OT.

Conclusion

Les réseaux OT sont de plus en plus la cible de cybermenaces avancées. Ces assaillants connaissent bien les systèmes OT et développent des logiciels malveillants personnalisés, conçus pour exploiter les vulnérabilités des systèmes couramment utilisés dans les environnements OT.

Les responsables de l'exploitation réseau doivent comprendre l'impact d'une surface d'attaque qui s'élargit et envisager de tirer parti de l'automatisation de la sécurité, des technologies de leurre, d'une veille sur les menaces spécifiques à l'OT et de la segmentation du réseau, pour ainsi optimiser la lutte contre les menaces avancées.

Voici quelques questions que les responsables de l'exploitation de réseaux doivent se poser sur le sujet :

- Avons-nous mis en place des processus automatisés de réponse aux incidents et de gestion des événements afin de neutraliser les intrusions avant qu'elles ne se propagent et n'aient un impact majeur ?
- Notre infrastructure de sécurité est-elle suffisamment intégrée pour pouvoir partager en temps réel la veille sur les menaces entre tous les systèmes de sécurité ?
- Disposons-nous de capacités avancées de détection des menaces et des intrusions, à l'image du sandboxing et des technologies de leurre ?
- Avons-nous mis en place des mesures pour réduire la fenêtre d'attaque et bloquer l'accès aux ressources du réseau après intrusion ?

[1] « Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat? », Siemens and Ponemon Institute, 2019.

[2] « Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks », Fortinet, 28 juin 2019.

[3] « 2020 State of Operational Technology and Cybersecurity Report », Fortinet, 30 juin 2020.

[4] « Fortinet 2019 Operational Technology Security Trends Report », Fortinet, 8 mai 2019.

[5] Kevin Townsend, « How Deception Technology Can Defend Networks and Disrupt Attackers », SecurityWeek, 5 juin 2019.

[6] « 2020 State of Operational Technology and Cybersecurity Report », Fortinet, 30 juin 2020.

www.fortinet.fr

Copyright © 2020 Fortinet, Inc. Tous droits réservés. Fortinet®, FortiGate®, FortiCare®, FortiGuard® et certaines autres marques sont des marques déposées de Fortinet, Inc., et les autres noms Fortinet mentionnés dans le présent document peuvent également être des marques déposées et/ou des marques de droit commun de Fortinet. Tous les autres noms de produit ou d'entreprise peuvent être des marques commerciales de leurs détenteurs respectifs. Les données de performances et autres indicateurs de mesure figurant dans le présent document ont été obtenus au cours de tests de laboratoire internes réalisés dans des conditions idéales, et les performances et autres résultats réels peuvent donc varier. Les variables de réseau, les différents environnements réseau et d'autres conditions peuvent affecter les performances. Aucun énoncé du présent document ne constitue un quelconque engagement contraignant de la part de Fortinet, et Fortinet exclut toute garantie, expresse ou implicite, sauf dans la mesure où Fortinet conclut avec un acheteur un contrat écrit exécutoire, signé par le directeur des affaires juridiques de Fortinet, qui garantit explicitement que les performances du produit identifié seront conformes à des niveaux de performances donnés expressément énoncés et, dans un tel cas, seuls les niveaux de performances spécifiques expressément énoncés dans ledit contrat écrit exécutoire ont un caractère obligatoire pour Fortinet. Dans un souci de clarté, une telle garantie sera limitée aux performances obtenues dans les mêmes conditions idéales que celles des tests de laboratoire internes de Fortinet. Fortinet rejette intégralement toute convention, déclaration ou garantie en vertu des présentes, qu'elle soit expresse ou implicite. Fortinet se réserve le droit de changer, de modifier, de transférer ou de réviser par ailleurs la présente publication sans préavis, et c'est la version la plus à jour de la publication qui est applicable. Fortinet rejette intégralement toute convention, déclaration ou garantie en vertu des présentes, qu'elle soit expresse ou implicite. Fortinet se réserve le droit de changer, de modifier, de transférer ou de réviser par ailleurs la présente publication sans préavis, et c'est la version la plus à jour de la publication qui est applicable.

726519-0-0-FR

décembre 7, 2020 11:55 AM

eb-how-to-design-security-for-ot-network-environments_FR