Digital Risk: Remote-Monitoring, IoT Sensors and Data Integrity Fatality File – French



Un pirate informatique a réussi à accéder à distance à une usine de traitement d'eau en Floride et a tenté d'empoisonner l'approvisionnement en eau de 15 000 résidents en manipulant les systèmes de contrôle des produits chimiques.

Ce qui s'est passé

Le 5 février 2021, un pirate informatique non autorisé a obtenu un accès à distance à l'usine de traitement de l'eau Bruce T. Haddock à Oldsmar, en Floride, à l'aide de TeamViewer – une application de bureau à distance partagée par tous les employés de l'usine sous un mot de passe unique, sans pare-feu en place. L'attaquant a accédé au système SCADA de l'installation et a modifié la concentration d'hydroxyde de sodium, la faisant passer de 100 parties par million à 11 100 parties par million – un niveau susceptible de causer de graves brûlures chimiques, voire la mort, s'il atteignait les consommateurs. Un opérateur de l'usine, vigilant, a remarqué que le curseur bougeait sur son écran, a observé l'attaquant naviguer dans le système en temps réel et a immédiatement annulé la modification avant qu'elle ne puisse prendre effet.

Ce qui a mal tourné

L'enquête a révélé que les employés utilisaient une version non prise en charge de Windows, dépourvue de pare-feu, et partageaient un seul mot de passe TeamViewer entre tous les membres du personnel – ce qui donnait à tout acteur externe ayant obtenu ce mot de passe un contrôle total et en temps réel sur un procédé chimique critique pour la sécurité. Aucune authentification à facteurs multiples n'était en place. Aucun système de détection d'anomalies n'a signalé cet accès non autorisé. La seule barrière entre un déversement de produit chimique mortel et 15 000 résidents était un employé qui surveillait son écran au bon moment.

Conclusion

Cet incident a été évité grâce à la vigilance humaine – et non grâce aux systèmes conçus pour surveiller et contrôler l'usine. La sécurité de tout système de sécurité connecté dépend de la sécurité de son point d'accès le plus faible, et la fiabilité de toute lecture de capteur dépend de celle du système qui la transmet. Les travailleurs doivent savoir ce que leurs systèmes numériques ne peuvent pas détecter – et être prêts à vérifier les conditions de manière indépendante.

Source: https://www.securitymagazine.com