Jacobs Douwe Egberts : atténuer les risques grâce aux renseignements sur la cybersécurité des TO

Un aperçu complet des risques potentiels de cybersécurité dans l'ensemble de ses usines a aidé Jacobs Douwe Egberts à mettre en œuvre des mesures d'atténuation adaptées pour éliminer les vulnérabilités, améliorer sa posture de cybersécurité et exercer ses activités en toute confiance.

Jacobs Douwe Egberts (JDE) est une entreprise mondiale spécialisée dans le café et le thé qui a vu le jour à la suite d'une fusion entre la division du café de Mondelez International et Douwe Egberts. En 2017, un incident lié à un logiciel malveillant a provoqué une panne informatique dans l'ensemble du réseau mondial de Mondelez. L'incident a causé des retards de livraison et de facturation pendant plusieurs jours, entraînant des pertes de 100 millions d'euros. Cette brèche a été le catalyseur de la mise en œuvre par JDE d'un programme de cybersécurité visant les technologies opérationnelles (TO), y compris l'environnement du système de contrôle industriel (SCI) dans l'ensemble de ses usines dans le monde.

Le défi

L'industrie 4.0 favorise une interconnectivité sans égal dans les environnements de production. De plus, en raison de la criticité des opérations, le secteur manufacturier est fortement ciblé par les pirates informatiques. La sécurité informatique traditionnelle ne suffit plus à protéger les entreprises manufacturières contre les cyberattaques. Qui plus est, la plupart des fabricants ne disposent pas des connaissances et des capacités spécialisées requises pour faire face aux menaces croissantes de cybersécurité.

JDE cherchait un partenaire expert pour lui fournir une vue d'ensemble de tous les risques et vulnérabilités liés à la cybersécurité dans ses usines. Il fallait donc tenir compte de tous les systèmes informatiques TO utilisés pour gérer l'ensemble des activités industrielles.

Voici ce que comprend notre analyse de cybersécurité des TO et des SCI

- Évaluation de la maturité
- Évaluation en fonction des normes IEC62443/NIST800
- Phase de validation en usine
- Phase de découverte en usine, y compris un examen de la sécurité physique et logique des TO et des SCI et des conclusions documentées
- Analyse et balayage du réseau de TO de SCI (découverte automatisée des actifs, anti-logiciels malveillants, gestion des identités et des accès, pare-feu, accès à distance, etc.)

Un partenaire fiable en sécurité des TI et des SCI

JDE nous a choisis pour nos solutions et services complets et intégrés de cybersécurité en technologie de l'information (TI) et en TO, appuyés par notre capacité à adopter une approche uniforme pour évaluer dans les délais prescrits ses usines réparties dans le monde entier.

Pour évaluer les environnements de TO et de SCI dans l'ensemble des usines, nous avons donc mis à la disposition de JDE une équipe de spécialistes chevronnés ayant une connaissance approfondie du contrôle des processus. Nos experts ont utilisé la méthodologie éprouvée d'évaluation de la sécurité des TO de CGI pour mieux comprendre la maturité de la politique existante à ce sujet et en examiner la mise en œuvre. L'évaluation comprenait des visites sur place, des entrevues structurées avec des employés, un examen de l'usine en fonction de la norme de cybersécurité industrielle IEC62443 et un balayage topologique du réseau de TO et de SCI.

Une évaluation des risques pour les personnes, les machines, les processus et la technologie

Nos experts ont connecté du matériel spécialisé au réseau de TO et de SCI pour effectuer une découverte automatisée des actifs et générer une carte topologique présentant tous les actifs pertinents dans l'environnement du client et la façon dont ils sont interconnectés. Les données des systèmes de supervision, de contrôle direct et sur le terrain ont été évaluées en vue de cibler les aspects particulièrement vulnérables à la cybercriminalité.

Nos évaluations de la sécurité des TO s'appuient sur les normes internationales de conformité en matière de SCI pertinentes (p. ex. NIST et ISO/ISA/IEC). Nos équipes d'évaluateurs (chacune composée de deux spécialistes en sécurité des TO) ont réalisé de multiples évaluations sur place et ont adopté une approche uniforme leur permettant de produire des rapports cohérents. La préparation à l'évaluation, l'analyse du réseau et du pare-feu ainsi que l'évaluation de l'architecture de TO et de SCI ont été effectuées de manière centralisée depuis notre centre d'excellence en sécurité des TO.

Le rapport d'évaluation comprenait un inventaire des risques avec une carte de densité, des recommandations en matière d'atténuation des risques ainsi que des indications quant au budget pour chaque mesure d'atténuation suggérée. Il présentait les risques, leur probabilité et leur incidence, ainsi que les mesures d'atténuation recommandées en ordre de priorité, aidant ainsi JDE à définir sa stratégie en matière de cybersécurité des TO et des SCI.

Des mesures d'atténuation des risques et de sensibilisation

À la suite des évaluations et du rapport, nous avions aussi le mandat de mettre en œuvre des mesures d'atténuation. À la lumière des conclusions tirées de notre programme d'évaluation, nous avons conçu une vidéo de sensibilisation à la cybersécurité des TO et des

SCI à l'intention des employés, qui peuvent désormais prendre connaissance des meilleures pratiques en matière de cybersécurité de TO et des STI et ainsi minimiser le risque d'atteintes internes.

La cybersécurité est intégrée à tout ce que nous faisons

Depuis 45 ans, CGI aide ses clients à transformer et à sécuriser leur entreprise en offrant des services de cybersécurité novateurs au sein d'environnements complexes partout dans le monde, y compris dans les secteurs de la défense et du renseignement. Nous avons considérablement investi dans le développement de nos compétences en collaborant avec des associations internationales de sécurité et des organismes de normalisation.

Bien que les cybermenaces soient mondiales, nous savons que les exigences varient selon les régions et que les défis sont uniques à chaque organisation. En tirant parti de notre expertise sectorielle, de nos connaissances techniques et commerciales approfondies, de nos meilleures pratiques et de nos cadres de gestion, nous offrons des services-conseils stratégiques, des résultats sécurisés et des services de sécurité en mode délégué. Nous travaillons en étroite collaboration avec vous pour nous assurer que les contrôles de sécurité sont intégrés dès le départ, et non de façon réactive.

À propos de CGI

Allier savoir et faire

Fondée en 1976, CGI figure parmi les plus importantes entreprises de services-conseils en TI et en management au monde.

Nous sommes guidés par les faits et axés sur les résultats afin d'accélérer le rendement de vos investissements. À partir de centaines de bureaux à l'échelle mondiale, nous offrons des services-conseils complets, adaptables et durables en TI et en management. Ces services s'appuient sur des analyses mondiales et sont mis en œuvre à l'échelle locale.

Pour en savoir plus

Visitez cgi.com/secteur-manufacturier
Écrivez-nous à manufacturing@cgi.com.