الخليج

اقتصاد, تقنية وسيارات

19 يناير 2023 20:17 مساء

عمليات الإنتاج الآلية قد تتعطل لأسابيع بسبب الهجمات الرقمية

«دبي: «الخليج

أظهرت دراسة استطلاعية أجرتها «كاسبرسكي» أن غالبية الموظفين العاملين في المؤسسات الصناعية في الإمارات العربية المتحدة (70%) يؤمنون بوجود أخطار كبيرة تتهدد عمليات الإنتاج الآلية التي تتحكم فيها الأنظمة الروبوتية، نظراً للهجمات الرقمية المحتملة التي تستهدف تلك الأنظمة.

تُستخدم الأنظمة الروبوتية مع نظم الرقابة الصناعية في عمليات الإنتاج لتحسّن كفاءة الإنتاج وتحل محل العمل اليدوي. ويرى 60% من الموظفين أيضاً أن عمليات الإنتاج التي تديرها الروبوتات قد تتعطل لعدة أسابيع أو أطول في حالة وقوع هجوم رقمي.

ولا يرى غالبية الموظفين أن بالإمكان إصلاح الروبوتات المعطلة على الفور في حالة وقوع هجوم رقمي؛ إذ قال بهذا الرأي 19% فقط من المستطلعة آراؤهم في دراسة «كاسبرسكي»، في حين رأى 17% أن إصلاح الأنظمة الروبوتية

المصابة سوف يستغرق بضعة أيام، فيما توقع أكثر من نصف الموظفين (60%) أن تستغرق عمليات التعافي وقتاً أطول بكثير؛ فذكر 54% مدة تتراوح بين بضعة أسابيع ونصف عام، وذكر 3% مدة تزيد على 7 أشهر وتصل إلى عام واحد، فيما رأى 3% أن انقطاع الإنتاج في حالة وقوع هجوم رقمي على الأنظمة الروبوتية سوف يستمر لأكثر من عام.

تقييم المستوى

لدى «كاسبرسكي»: «إن الدراسة طلبت من المشاركين KasperskyOS قال أندري سوفوروف، رئيس وحدة أعمال «تقييم مستوى الأنظمة الروبوتية في مؤسساتهم وقدرتها على مقاومة الأخطار الرقمية».

وأوضح أن الإجابات بيّنت وجود مشاعر مختلطة لدى العديد من الموظفين عند تقييم مدى حماية الأنظمة الروبوتية في مؤسساتهم، مشيراً إلى أنهم أظهروا ضرورة إيلاء أمن هذه الأنظمة مزيداً من الاهتمام مشككين في مدى سرعة تعافيها بعد وقوع حادث رقمي. وقال: «نواجه اليوم مخاوف بشأن أساليب العمل والحماية المناسبة لأنظمة إنترنت الأشياء الصناعية الحديثة، في ظل التنوّع الكبير في الأجهزة الذكية المعقدة التي تنطوي عليها».

وأضاف: «تقدم كاسبرسكي لأجل ذلك حلولاً أمنية قائمة على نموذج «المناعة الرقمية» لحماية وحدات مؤسسة معينة أو منظومة تقنية المعلومات بأكملها، ما يجعل الأنظمة الروبوتية الصناعية وأجهزة نظم الرقابة الصناعية والمركبات Kaspersky ذاتية القيادة محصّنة ضد معظم الهجمات الرقمية دون الحاجة إلى استخدام أدوات أمنية. فبإمكان الحل مثلاً، حماية نظام تقنية المعلومات وجمع البيانات الميدانية ونقلها إلى المنصات الرقمية IoT Secure Gateways بطريقة آمنة، ما يتيح صورة كاملة وواضحة للأجهزة ولعمليات الإنتاج».

تدابير الحماية

يوصي خبراء «كاسبرسكي» باتباع التدابير التالية لحماية أنظمة الحاسوب الصناعية من التهديدات المختلفة:

ـ إجراء عمليات تقييم أمني منتظمة لأنظمة التقنيات التشغيلية لتحديد مشكلات الأمن الرقمي المحتملة والقضاء عليها.

ـ وضع إجراءات تقييم وفرز مستمرة للثغرات وجعلها أساساً لعملية فعالة لإدارة الثغرات. قد تصبح الحلول أدوات مساعدة فعالة ومصدراً لمعلومات فريدة قابلة Kaspersky Industrial CyberSecurity المخصصة مثل للتنفيذ، غير متاحة بالكامل للجمهور.

ـ تنفيذ التحديثات البرمجية في الوقت المناسب للمكونات الرئيسية لشبكة التقنيات التشغيلية المؤسسية، وتطبيق التصحيحات الأمنية أو تنفيذ إجراءات للتعويض في أسرع ما يمكن من الناحية التقنية، وذلك لمنع وقوع حادث كبير يؤدي إلى خلل كبير في عمليات الإنتاج وقد يكلف خسائر بالملايين.

ـ الخاصة بالنظم الصناعية، (EDR) استخدام حلول الكشف عن التهديدات والاستجابة لها عند الأجهزة الطرفية لاكتشاف التهديدات المعقدة Kaspersky Industrial Cybersecurity for Nodes with EDR مثل الحل والتحقيق فيها ومعالجة الحوادث بطريقة فعّالة وفي الوقت المناسب.

ـ تعزيز قدرة الاستجابة للتقنيات الخبيثة الجديدة والمتقدمة من خلال تطوير القدرة على الوقاية من الحوادث واكتشافها ورفع مهارات الاستجابة لفرق الأمن الرقمي. ويُعد التدريب على أمن التقنيات التشغيلية المخصص لفرق

.أمن تقنية المعلومات والموظفين العاملين على هذه التقنيات، أحد التدابير الرئيسية التي تساعد في تحقيق هذا الهدف