٤٤ ٪ من الموظفين في مصر يخافون من فقدان وظائفهم بسبب الذكاء الاصطناعي

أظهرت دراسة استطلاعية أجرتها كاسبرسكي بين الموظفين في منطقة الشرق الأوسط وتركيا وإفريقيا، تتعلق بالروبوتات وأنظمة الأتمتة التي تستخدمها المؤسسات. فقد أبدى ما يقارب نصف الموظفين في مصر (٤٤٪) مخاوفهم من فقدان وظائفهم لصالح الروبوتات، وأفاد ٢٥٪ منهم بأنهم على دراية عن حوادث أمن رقمي ارتبطت بالروبوتات والأنظمة المؤتمتة في مؤسساتهم. وفي المقابل، يرى العديد من الموظفين المشاركين في الدراسة جوانب إيجابية تجلبها لهم الروبوتات.

ويرى الخبراء أن تزايد استخدام الذكاء الاصطناعي قد يشكل خطراً على وجود العديد من الوظائف البشرية. ويمكن للتطبيق الروبوتي ChatGPTالذي أتيح في الآونة الأخيرة للاستخدام العام، إجراء محادثة متماسكة، وشرح المفاهيم العلمية المعقدة، وترجمة النصوص بين اللغات بطريقة فنية، وإجراء غير ذلك من المهام. هذا بالطبع عدا عن الأنواع الأخرى من الروبوتات الموجودة بين الناس منذ سنوات، والتي تقوم بغسل السيارات وتوصيل الطلبات وفرز البضائع في المستودعات وتوصيل حبوب الدواء للمرضى وإنجاز عمليات التجميع في المصانع.

وأفاد المستطلعة آراؤهم في دراسة كاسبرسكي الحديثة، في أحيان كثيرة، بوجود مزايا نافعة لصحة الموظفين؛ إذ قال ٦٦٪إن الروبوتات تحرّر الموظفين من القيام بأعمال تتطلب مجهوداً بدنياً صعباً أو خطراً. وذكر ٥٢٪ أن الروبوتات زادت من كفاءة عمليات الإنتاج

وجلبت منافع اقتصادية للمؤسسات. وأعرب ٤٠٪عن اعتقادهم بأن الروبوتات أتاحت أمام الموظفين مزيداً من فرص التدريب على وظائف أهمّ وأعلى أجراً، فيما قال ٣٧٪ إنها قللت من احتمالية وقوع حوادث بسبب العامل البشري

قال عماد الحفار رئيس الخبراء التقنيين لمنطقة الشرق الأوسط وتركيا وإفريقيا لدى كاسبرسكي، إنه بينما يحذّر بعض الأفراد والمؤسسات من الأتمتة ويمتنعون عن استخدامها، يرى غيرهم أن من المهمّ تكييف عملياتهم لتحقيق أقصى استفادة ممكنة من أحدث التقنيات، مشيراً إلى أن باحثين هما بيلي ريوس وجوناثان بوتس، أوضحا في مؤتمر «بلاك هات» في عام ٢٠١٧، كيفية اختراق نظام آلي لغسل السيارات، وبيّنا التهديد الذي تمثله واقعة كهذه على البشر. وأضاف عماد: «درس الباحثان نظام غسل السيارات PDQ Laser Washالمتصل بالإنترنت، ووجدا طريقة لاختراقه، بل أظهرا أن بالإمكان إغلاق باب مرآب الغسل على السيارة أثناء وجودها داخله، الأمر الذي قد يعرّض حياة سائقها للخطر». ودعا الحفار مختلف المؤسسات حول العالم إلى التعرّف على السبل الكفيلة بجعل حلول الأتمتة أكثر أماناً وفاعلية لتلبية احتياجات الأعمال، نظراً لأن التوجه نحو المزيد من رقمنه الأعمال «أمر لا بدّ منه».

وتوصي كاسبرسكي المؤسسات باتباع التدابير التالية لحماية أنظمة الرقابة الصناعية من مختلف التهديدات:

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

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

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

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

• تعزيز قدرة الاستجابة للتقنيات الخبيثة الجديدة والمتقدمة من خلال تطوير القدرة على الوقاية من الحوادث واكتشافها ورفع مهارات الاستجابة لفرق الأمن الرقمي. ويُعدّ التدريب على أمن التقنيات التشغيلية المخصص لفرق أمن تقنية المعلومات والموظفين العاملين على هذه التقنيات، أحد التدابير الرئيسة التي تساعد في تحقيق هذا الهدف.

• إجراء تقييمات أمنية منتظمة لأنظمة التقنيات التشغيلية لتحديد مشكلات الأمن السيبراني المحتملة والقضاء عليها.

• إنشاء تقييم مستمر للضعف والفرز كأساس لعملية إدارة الضعف الفعالة. قد تصبح الحلول المخصصة