5 أسباب تؤكد أهمية تبني الأتمتة من قبل مزودي الخدمات في الشرق الأوسط وشمال إفريقيا


لاكي لاريتشيا

أكد لاكي لاريتشيا، رئيس الخدمات الرقمية في إريكسون الشرق الأوسط وأفريقيا أن الرقمنة بدأت بالتأثير على مجموعة متنوعة من القطاعات على نحو ملاحظ، ويواجه مشغلو الهواتف المتنقلة تحدياً هائلاً يتمثل في رقمنة مؤسساتهم - ليتمكنوا بدورهم من تسريع عملية التحول الرقمي لعملائهم من المؤسسات، وسيؤدي تأخر المشغلين في تحويل أعمالهم إلى فقدان العديد من الفرص التي توفرها لهم التقنيات الجديدة كالجيل الخامس وإنترنت الأشياء.

شهد سوق الاتصالات في منطقة الشرق الأوسط وأفريقيا إقبالاً كبيراً على استخدام تقنية الجيل الرابع المطورLTE، إضافة إلى نسبة عالية لاختراق الهواتف الذكية (المزيد من التفاصيل، يرجى قراءة تقرير إريكسون الأخير للاتصالات المتنقلة). سيؤدي الارتفاع في استخدام الهواتف الذكية - إلى جانب الإزدياد في عدد أجهزة إنترنت الأشياء التي تستخدم تقنية الجيل الرابع المطورLTE إلى نمو كبير في استهلاك البيانات. وبينما يستعد مزودو الخدمات في الشرق الأوسط وشمال إفريقيا لتشغيل شبكة الجيل الخامس، فإنهم يحتاجون إلى زيادة استثماراتهم لتعزيز التغطية والموثوقية والسرعة لضمان توفير تجارب استثنائية للعملاء.

في إطار محادثاتي مع بعض المشغلين الرائدين لشبكات الهواتف المتنقلة في المنطقة، اكتشفت مدى إهتمامهم بأتمتة إدارة الشبكات وعملياتها، حيث يعتبرون ذلك بمثابة خطوة ضرورية لتحقيق استراتيجياتهم الخاصة بالتطوير. كما يعتبرون بأن أتمتة الشبكات أمر ضروري لإدارة تعقيدات شبكة الجيل الخامس / إنترنت الأشياء وتقديم خدمات الجيل الخامس بكفاءة للعملاء.

ومع استمرار مشغلي منطقة الشرق الأوسط وشمال إفريقيا في نقل وظائف الشبكة من الأجهزة ذات الملكية المسجلة إلى البرامج، إليكم بعض الأسئلة الرئيسية التي غالباً ما يتم طرحها في هذا الإطار مثال: كيف يمكنني استخدام الأتمتة لتخفيف النفقات؟ ما هي الأفضل طريقة لتقليل الوقت اللازم لتوفير الخدمة للعملاء؟ ما دور عملية تحليل البيانات في المساعدة على اكتساب رؤى جديدة لتقديم الخدمات التي يرغب العملاء بالحصول عليها في عالم الجيل الخامس / إنترنت الأشياء؟

ولتقديم أجوبة موثوقة عن هذه الأسئلة، كلفت إريكسون مجلة «إم آي تي تكنولوجي ريفيو» بإجراء مقابلات مع خبراء عاملين لدى مشغلي الاتصالات العالميين - نتج عنها تقرير بعنوان «أتمتة الشبكات: الكفاءة والمرونة والطريق إلى تقنية الجيل الخامس»، يتم في إطاره توضيح القيمة الناتجة عن أتمتة عمليات الشبكة ونقطة الإنطلاق للمشغلين الرائدين في هذا المجال.

من وجهة نظر كبار المسؤولين التنفيذيين في مجال التكنولوجيا العاملين لدى مشغلي الشبكات على مستوى العالم، يقدم التقرير الاستنتاجات التالية:

• مواجهة التغييرات: قد يرى كبار مسؤولي وحدات التكنولوجيا أنه من الخطورة إحداث تغييرات جذرية في شبكاتهم، لكن بعض «التغييرات الهيكلية ضرورية للإستفادة من المزايا التي توفرها الأتمتة». في الواقع تحتاج الشركات لإجراء تغييرات جذرية بهدف تعزيز ثقافة الموظفين في مجال تكنولوجيا المعلومات وتدريبهم لإكتساب مهارات البرمجة، والتي تعتبر ضرورية لتشغيل الشبكات.

• تسليط الضوء على الإرتباط بين مستقبل تقنيتي الجيل الخامس وإنترنت الأشياء: مع التبني المتزايد للتقنيات الذكية الجديدة كتقنية الجيل الخامس وإنترنت الأشياء، فإن تسليط الضوء على العلاقة بين التقنيتين بالنسبة لكبار المديرين التنفيذيين والمديرين الماليين يعزز حالات الأعمال المرتبطة بالأتمتة. ومع ارتفاع مستوى حركة البيانات، تصبح الحاجة إلى تعزيز الإستثمارات أمر لا بد منه.

• الثقة بالمعايير المفتوحة: تتطلب قدرات مزودي الخدمات في منطقة الشرق الأوسط وشمال إفريقيا على الاستفادة من الفرص الناشئة عن إنتشار التقنيات الجديدة، والعمل على الإقلال من التعقيدات القائمة في وحدات دعم العمليات المجزأة إلى أقصى حد ممكن.

• على المشغلين مواصلة تشجيع بائعيهم للقيام بالأمر ذاته»، إلى جانب تقديم الإلتزامات من جانبهم إلى إحدى المنصات مفتوحة المصدر. يمكن أن توفر أنظمة أتمتة الشبكات المفتوحة قيمة أكبر والإستفادة من إنشاء خدمات جديدة تدعم نماذج أعمال جديدة عبر مختلف القطاعات التي ستنشأ عن استخدام تقنية الجيل الخامس.

• تبني نظام DevOps: يعد نظام DevOps عنصر تمكين رئيسي لمجموعات الأعمال والشركات الناجحة التي تعتمد على البرامج. وقد يكون تزويد الموظفين المتخصصين في مجال الشبكة بالمهارات الجديدة غير كاف لمساعدتهم على تحقيق الإنجازات في البيئات السحابية سريعة التطور. وسواء تم إنشاء بنى جديدة أم لا، « قد يؤدي تعلم طرق العمل في نظام DevOps إلى تعزيز المزايا التي توفرها أتمتة الشبكة وتطوير العديد من الجوانب الأخرى».

• عدم التردد في دخول عالم الأتمتة: تعني «الأتمتة» استخدام البرمجيات للقيام بالمهام التي تؤديها عادة الإدارة والأجهزة إعتمادا على الأدوات المطوّرة التي تقوم بتوجيهها، «تحتاج الأتمتة واستخدام أدواتها إلى الثقة».

وقد يؤدي التأخر في تبنيها أو الحفاظ على الأدوات القديمة لأغراض متعلقة بتسريح الموظفين، إلى حرمان المؤسسة من الإستفادة من بعض المزايا التي يوفرها تبني الأتمتة».

وأنا على ثقة تامة بأن زيادة الإعتماد على الأتمتة، سيمكن مزودي الخدمة في الشرق الأوسط وإفريقيا من خفض تكاليف العمليات وتقديم الخدمات بسرعة أكبر، والاستعداد الكامل لإدارة التعقيدات وتجاوز توقعات العملاء في عصر التحول الرقمي - على الأرجح من خلال الخدمات التي لم يتم ابتكارها بعد!

لمراقبة وحماية الآلات في القطاع الصناعي

«بنتلي نيفادا» تطلق منصة Orbit 60 Series المتطورة

■ 80 قناة بيانات ديناميكية مع بنية هندسية متطورة توفر العديد من الإمكانات وتسمح بإدارة أكثر التطبيقات تعقيداً عبر نظام واحد

■ المنصة تتصل بجميع الآلات الصناعية الرئيسية وتتنوع استخداماتها بين قطاعات النفط والغاز والطاقة المتجددة


جهاز Orbit 60 Series

■ النظام الجديد يتصل ببرنامج إدارة الآلات لغرض المراقبة والتشخيص الاستباقي

أعلنت شركة «بيكر هيوز التابعة لجنرال إلكتريك» (المدرجة في بورصة نيويورك بالرمز BHGE)، اليوم عن قيام شركتها التابعة لها «بنتلي نيفادا» - الرائدة عالمياً في إنتاج أنظمة المراقبة لأكثر من ستين عاماً - بإطلاق منصتها الأحدث Orbit 60 Series.

وتعتبر Orbit 60 Series الجيل الأحدث من التقنيات المتخصصة بجمع ومعالجة البيانات، وتزويد المشغلين بالبيانات والتحليلات الصحيحة لتحديد سلامة أداء آلاتهم، وتشكّل المنصة الجديدة أول نظام آمن لمراقبة الآلات عبر الإنترنت مع تزويدها ببوابة اتصال إحادية الإتجاه تسمح بنقل البيانات من الجهاز إلى نظام إدارة الآلات في شركة «بنتلي نيفادا» (System 1) لأغراض المراقبة والتشخيص الإستباقي. وقد حصلت المنصة على شهادة مستوى السلامة (2 (SIL و3 . وكذلك شهادة معيار معهد البترول الأمريكي (API 670)، وهي بذلك تلبي معايير القطاع على صعيدي السلامة والأداء.

ويُمكن المنصة الجديدة المشغلين من مراقبة المزيد من الآلات بجهد وتكلفة أقل، حيث توفر 80 قناة ديناميكية للبيانات بالمقارنة مع 50 قناة في المنصات القياسية المشابهة في القطاع، وتتمتع بقوة معالجة للإشارة أعلى بـ100 مرة من تلك المنصات، فضلاً عن كونها أصغر حجماً. ويمكن تركيب منصة Orbit 60 Series ضمن صندوق حامل أو توزيعها ونشرها عبر نظام إدخال وإخراج (I/O) معياري عن بعد. وتسمح بنيتها الهندسية القابلة للتطوير بالاتصال بمجموعة واسعة من الأصول تتنوع بين الآلات بالغة الأهمية والمعدات العامة عبر عدد من القطاعات، مثل النفط والغاز، وتوليد الطاقة، والطاقة المتجددة، والصلب، والورق، والصناعات العامة.

وبهذه المناسبة، قالت تيري نايت، رئيس مجلس إدارة «بنتلي نيفادا»: «ينشد العملاء دوماً مراقبة وحماية آلاتهم باستخدام حلول تنافسية لا تزودهم فقط بالبيانات والرؤى الصحيحة، وإنما تتمتع أيضا بالمرونة الكافية لمواكبة عمليات التوسع مستقبلاً. ومن هنا جاء تطوير Orbit 60 Series كمنصة مراقبة توفر تحليلات قوية للبيانات إلى جانب مرونتها وقابليتها للتوسع، وأيضاً تمتعها بميزة الاتصال الآمن عبر الإنترنت، الأمر الذي يقلل التكاليف الاستثمارية الإجمالية، ويتيح للمشغلين فرصة المراقبة الشاملة لآلات مصانعهم».

من جانبها، قالت باولا هولبوود، كبيرة محللي «مجموعة إي آر سي الاستشارية»: «يتعين على الجيل التالي من الأنظمة الصناعية أن تتخطى حدود الجمع بين التكنولوجيا التشغيلية وتكنولوجيا المعلومات لتشمل إدراج أنظمة قوية للأمن السيبراني. ومع Orbit 60 Series، كرّست "بنتلي نيفادا" إرثها العريق كشركة رائدة في مجال الابتكار التكنولوجي لتقوم بدمج العديد من المزايا الضرورية للارتقاء بالأنظمة الصناعية مستقبلاً. حيث تتمتع هذه المنصة بقدرتها على توفير اتصال آمن للأجهزة عبر الإنترنت مع نظام المراقبة، الأمر الذي يوفر مستوى إضافيا من الثقة بحماية الأصول المهمة وفقا لمتطلبات السلامة في القرن الحادي والعشرين».

وتأتي المنصة الجديدة استكمالاً لباقة عروض ومنتجات «بنتلي نيفادا» المخططة للنظم الصناعية، بما في ذلك منصة 3500 التي تم تركيب 85 ألف وحدة منها حول العالم، وستبقى متاحة كمنصة رائدة لمراقبة الأصول، وسيتم توفير خدمتها المخصصة لأجل طويل للعملاء على مستوى العالم.

لمعرفة المزيد عن منصة Orbit 60 Series، يمكن زيارة www.bently.com/Orbit60، أو حضور «منتدى الآلات التوربينية والمضخات» - الجناح رقم 2701، وكذلك مؤتمر الطاقة العالمي الرابع والعشرين في أبوظبي.

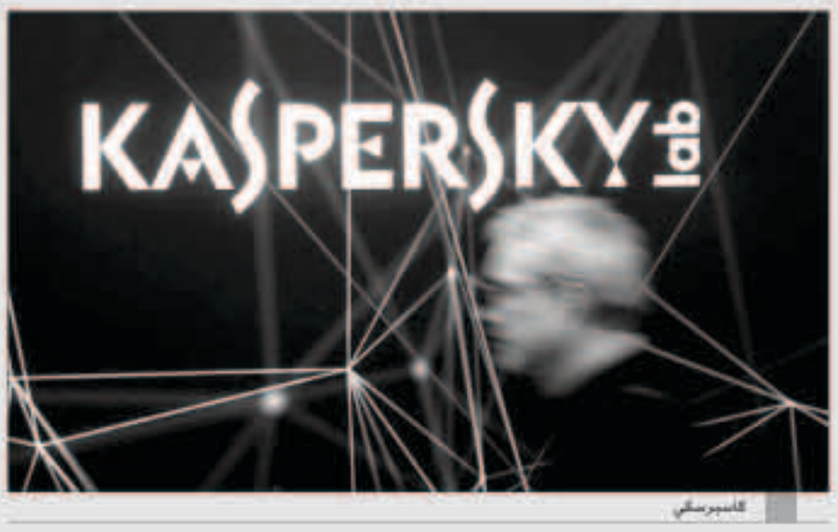
«إنفينيتي البابطين» تواصل حملة تأجير السيارات على «QX50 وQX80»

تعلن شركة عبد المحسن عبد العزيز البابطين، الوكيل الوحيد المعتمد لسيارات إنفينيتي في دولة الكويت، عن حملة تأجير السيارات والتي تتضمن عرضاً على سيارات إنفينيتي المفضلة QX50 وQX80 التي تتمتع بقوة الأداء والأناقة العالية.

صُنعت QX50 الجديدة كلياً لتلبي احتياجات عملاء السيارات المتميزين بشكل كامل حسب رغبتهم في امتلاك أحدث ما أبدعته التكنولوجيا في عالم اليوم. وتقدم QX50 ما يمكن وصفه بانه أكثر محركات الاحتراق الداخلي إبتكاراً في أسواق العالم حالياً. ويعتبر خبراء السيارات هذا المحرك قمة محركات الاحتراق الداخلي. وقد نجح مهندسو الشركة في تقديم ابتكار هو الأول من نوعه على مستوى العالم لصالح إنفينيتي متمثلاً في تقنية نسبة الضغط المتفاوت. يقدم محرك VC-تيربو أداءاً قوياً ومقنعاً لمحرك سداسي الأسطوانات والتوفير في استهلاك الوقود لمحرك الأربع أسطوانات، ليتحوّل عند الطلب وحسب مدخلات السائق. ومن خلال التكيّف مع احتياجات السائق فورياً.

بواقع 1.6 مليون هجوم في ستة أشهر

«كاسبرسكي»: 9 في المئة ارتفاعاً في عدد هجمات التصيّد الموجهة لمستخدمي أجهزة «أبل»



كاسبرسكي

وصل عدد هجمات التصيد الموجهة لمستخدمي حواسيب Mac، والأجهزة العاملة بنظام تشغيل iOS، ومنظومات الخدمة المتاحة لبيئات تشغيل أجهزة «أبل»، إلى 1.6 مليون هجوم في النصف الأول من العام 2019، وذلك بزيادة قدرها 9% مقارنة بعدد الهجمات المماثلة التي شنت خلال العام 2018 بأكمله. وتعدّ هذه إحدى النتائج التي أوردها تقرير كاسبرسكي بشأن «التهديدات الموجهة لمستخدمي ماك» للعام 2019.

وبينما يقل كثيرًا عدد البرمجيات الخبيثة التي تستهدف أجهزة «أبل» عن تلك التي تهدد مستخدمي الأجهزة العاملة بأنظمة التشغيل «ويندوز» و«أندرويد»، تجد الأمر مختلفًا قيما يخصّ بهجمات التصيّد، التي لا تميز بين نظم التشغيل، ولا تعتمد هجمات التصيد في الغالب على برمجيات معينة، كونها مبنية بالكامل على أساليب الخداع التي تستغل السمات البشرية، وهو ما يُعرف بالهندسة الاجتماعية، كالتلاعب والتأثير في الضحية المستهدفة.

وقد أظهرت دراسة كاسبرسكي البحثية الأخيرة أن عدد الحالات التي واجه فيها المستخدمون صفحات مزيفة تستغل هوية «أبل» التجارية ازداد ازديادًا ملحوظًا خلال النصف الأول من العام، ليصل 1.6 مليون حالة. ويشكل هذا الرقم زيادة قدرها تسعة بالمئة مقارنة بالحالات المشابهة التي اوقفتها حلول كاسبرسكي الأمنية في العام 2018، وبلغ عددها 1.49 مليون محاولة لزيارة صفحات مزيفة على شكل مواقع تابعة لعلامة «أبل».

وبنيت الدراسة على إحصاءات خاصة بالتهديدات الأمنية الواردة طوعًا من مستخدمي شبكة كاسبرسكي الأمنية Kaspersky Security Network، البنية التحتية السحابية العالمية المصممة للتعامل الفوري مع التهديدات الإلكترونية الجديدة.

وكانت من أكثر عمليات الاحتيال شيوعًا تلك التي تخفت بواجهة تشبه واجهة خدمة iCloud، في محاولة من القائمين عليها لسرقة بيانات اعتماد الدخول إلى حسابات «أبل». وعادة ما تأتي الروابط المؤدية إلى مثل هذه الخدمات الاحتيالية عن طريق البريد الإلكتروني على شكل رسائل تدّعي أنها من فرق الدعم الفني وغالبًا ما تهدّد بتجميد حساب المستخدم في حال لم يتبع الرابط المرفق.

وتشمل حيل التصيد الأخرى المنتشرة محاولات لإقناع المستخدم بأن حاسوبه تحت تهديد أمني خطر يمكن حله ببساطة بعد عدّة نقرات على روابط مختلفة وبدفع مبلغ قليل من المال.

ورأت تاتيانا سيدورينا، الباحثة الأمنية في كاسبرسكي، أن محاولات التصيد تنطوي على تهديد أكبر لمستخدمي «أبل» مقارنة بغيرهم مثل مستخدمي «ويندوز» أو «أندرويد»، على الرغم من أنها ليست محاولات جديدة، حسبما أشارت. وعزت الخبيرة الأمنية هذا الأمر إلى شعور بالاطمئنان بين مستخدمي أجهزة «أبل» سببه الإعتقاد السائد بكون بيئة عمل هذه الأجهزة «أكثر أمنًا» من غيرها، الأمر الذي يؤدي إلى تساهل البعض في احتمال مواجهة صفحات مزيفة أثناء تصفح الإنترنت.

وقالت: «قد تؤدي سرقة بيانات حسابات iCloud إلى عواقب وخيمة، مثل قفل جهاز «آي فون» أو «آي باد» أو محو محتوياته عن بعد، لذلك نحثّ مستخدمي أجهزة «أبل» على توخي الحذر من أية رسائل واردة تدعي أنها من فريق دعم فني ما، طالبة الحصول على بيانات معينة، أو تحويل المتلقي إلى روابط خارجية».

من جهة أخرى، كشف التقرير عن أشكال أخرى من التهديدات التي تواجه مستخدمي أجهزة «ماك»، بإظهار النتائج بعض الأنماط الإيجابية؛ إذ كانت أكثر التهديدات انتشارًا بين مستخدمي «ماك» لا تنطوي على قدر خطر من التهديد، كالتروجانات المصرفية، وإنما برمجيات إعلانية تظهر إعلانات مزعجة للمستخدم، غالبًا ما تصنف تحت بند البرمجيات غير المرغوب بها، فهي تكتفي بملء أجهزة المستخدمين بالإعلانات، التي قد يكون بعضها يُخفي تهديدات أخطر أثرًا.

وتشمل بعض النتائج الأخرى الواردة في التقرير ما يلي:

• قارب إجمالي عدد هجمات التصيد في النصف الأول من العام 2019 والتي تستهدف أجهزة «ماك» المحمية بحلول كاسبرسكي، 6 ملايين هجمة، بينما شهد العام 2018 بأكمله 7.3 ملايين حالة.

• حاول نسبة قدرها 39.95% من هذه الهجمات سرقة بيانات المستخدمين المالية، بزيادة قدرها 10% مقارنة بالنصف الأول من العام 2018.

• شهدت بعض المناطق هجمات تصيد موجهة لمستخدمي «ماك» أكثر من غيرها. ففي المملكة العربية السعودية، تعرض 20.8% من المستخدمين لهجمات، تبعتها الكويت بنسبة 18.3% من المستخدمين.و الإمارات العربية المتحدة بنسبة 15.6%.

• كانت أكثر البرمجيات الخبيثة نشاطًا على أجهزة «ماك» إصدارات من عائلة Shlayer، التي تتنكر على هيئة تحديثات لبرنامج Adobe Flash Player.

وتوصي كاسبرسكي المستخدمين باتباع الخطوات التالية لتأمين أجهزتهم:

• الحفاظ دائمًا على تحديث نظام التشغيل macOS وجميع البرمجيات على الجهاز.

• استخدام البرمجيات الرسمية للحملة من صفحات للطورين مباشرة أو عن طريق متجر التطبيقات App Store فقط.

• المباشرة باستخدام حل أمني معتمد يتيح الحماية على أجهزة «ماك» وعلى الحواسيب والأجهزة المحمولة من «أبل»، مثل الحل Kaspersky Internet Security.