منصة جديدة لمساعدة الشركات على مواجهة الأنشطة الاحتيالية عبر الإنترنت

الأربعاء 24 مايو 2017 07:05 م

طرحت كاسبرسكي لاب حديثًا حل Kaspersky Fraud Prevention Cloud الجديد المصمم لمساعدة الشركات في مواجهة المخاطر الناشئة عن الأنشطة الاحتيالية عبر خدمات الإنترنت سريعة النمو.

وإلى جانب احتوائه على حلول مكافحة الاحتيال لنقاط النهاية والأجهزة المتنقلة ضمن منصة Kaspersky Fraud Prevention، قالت كاسبرسكي لاب إن المنتج الجديد جُهّز بمجموعة من التقنيات القائمة على السحابة والمصممة لحماية البنوك والمؤسسات المالية وموردي برامج الولاء والهيئات الحكومية من الهجمات الاحتيالية.

وأضافت الشركة أن ذلك يشمل قاعدة بيانات عالمية إحصائية تتبّع موثوقية وتحليل أداء الجهاز وتحليل بيئة التشغيل والتحليل السلوكي ومعلومات التعريف البيومترية Biometric واكتشاف البرامج الخبيثة الصامتة Clientless.

وأشارت كاسبرسكي لاب إلى أنه ومع تنامي الخدمات المصرفية عبر الإنترنت وعبر الهواتف المتنقلة، أصبحت المؤسسات بحاجة ماسة لمكافحة الاحتيال وغسيل الأموال مع ضمان الحماية لعملائها. على سبيل المثال، وفقًا لاستطلاع مخاطر المؤسسات المالية 2016، الذي أجرته B2B International وكاسبرسكي لاب، تبيّن أن واحدًا من بين كل أربعة عملاء من البنوك وقعوا ضحية الاحتيال المالي في العام الماضي. ويوفر حل مكافحة الاحتيال الجديد من كاسبرسكي لاب حماية متعددة القنوات لكل من الشركات والمستخدمين، مما سيساهم في تقليل وطأة الخسائر الناشئة عن الاحتيال وتكاليف الوقاية الخاضعة للتحكم.

وذكرت كاسبرسكي لاب أن الحل يشتمل على تقنيات متقدمة لتحسين الرؤية والكشف عن النشاط المشبوه دون التأثير على تجربة المستخدم. ويساعد التحليل السلوكي ومعلومات التعريف البيومترية Biometric في التعرف على ما إذا كان الشخص حقيقيًا أم خلاف ذلك، وذلك من دون الحاجة إلى اتخاذ أي إجراءات أو تدابير إضافية من قبل المستخدم. ويتم تحليل السلوك من خلال حركات الماوس والنقرات والتمريرات وضربات لوحة المفاتيح على أجهزة الكمبيوتر ومقياس التسارع وحالة الجيروسكوب وحركات اليد (كاللمس والتمريرات وغير ذلك) على الأجهزة المتنقلة.

ويقوم حل Kaspersky Fraud Prevention Cloud بجمع معلومات عن سلوك المستخدم والجهاز والبيئة وفترة الاستخدام وتحليلها كبيانات كبيرة في السحابة على أساس أنها مجهولة المصدر وليس لها أي صفة شخصية، مما يجعلها متاحة لخبراء الفحص الجنائي والتحليل التلقائي دون الاتصال بالإنترنت. وتتم إضافة هذه المعلومات الجديدة إلى نظام إدارة مكافحة الاحتيال الداخلي في الشركات الذي يتيح إمكانية الكشف الاستباقي عن الاحتيال في الوقت الحقيقي، حتى قبل البدء بتنفيذ المعاملة. ويستند هذا السيناريو على نهج استخبارات HuMachine من كاسبرسكي لاب الذي يدمج بين البيانات الكبيرة وتحليل أبحاث التهديدات مع خوارزميات التعلم الآلي والخبرة المقدمة من نخبة الفرق الأمنية في الشركة.

وتعمل خاصية المصادقة القائمة على المخاطر Risk Based Authentication على تقييم المخاطر قبل قيام المستخدم بتسجيل الدخول إلى القناة الرقمية، وتوفير القرارات للنظم الداخلية الداخلية حول ما إذا كان ينبغي المتابعة، أو طلب معلومات إضافية حول المصادقة أو حظر الدخول لحين إجراء المزيد من التحقق. وتساهم هذه الميزة في تحسين مرونة الاستخدام بالنسبة للمستخدمين النظاميين، وذلك عن طريق خفض عدد مراحل المصادقة، في حين يتم الكشف عن المستخدمين غير المصرح لهم قبل ارتكاب أي نشاط احتيالي.

كما تساعد خاصية Continuous Session Anomaly Detection على توسيع نطاق الكشف عن الاحتيال، وذلك من خلال تحديد الحساب المخترق وعمليات الاحتيال الجديدة على الحسابات وحالات غسيل الأموال والأدوات المؤتمتة أو أي عمليات مشبوهة تحدث خلال فترة

الاستخدام. وعلى هذا النحو، يتم تفعيل منصة Kaspersky Fraud Prevention Cloud خلال عملية تسجيل الدخول بالإضافة إلى فترة الاستخدام بأكملها، ويتيح إنشاء نماذج إحصائية قائمة على الأنماط السلوكية المختلفة بمساعدة تقنيات التعلم الآلي.

وتشمل مهام الكشف عن البرامج الخبيثة الصامتة Clientless المتاحة من خلال منصة Kaspersky Fraud Prevention Cloud الجمع بين تقنيات الكشف المباشر والكشف الاستباقي. يحدد الكشف المباشر ما إذا كان جهاز العميل يستخدم كوسيط لشن هجوم مباشر على الخدمات الرقمية لمؤسسة معينة. في حين أن الكشف الاستباقي يساعد في التعرف على البرمجيات الخبيثة التي لا تؤثر على المؤسسة بشكل مباشر، بل يحتمل أن يتم تطويرها لهذا الغرض مستقبلًا. وهذا يساعد الشركة في تقليل المخاطر وتجنب الخسائر الناشئة عن أي هجوم فعلي عند حدوثه.

وقال الكسندر ارماكوفيتش، رئيس مكافحة الاحتيال في كاسبرسكي لاب. يضم فريق مكافحة الاحتيال لدينا مجموعة من الخبراء المختصين الذين يشكّلون معًا فريق الأبحاث والتحليلات ذات الصلة بالاحتيال. ويقوم هذا الفريق بتقديم الدعم للعملاء من حيث التقليل والتخفيف من تداعيات وأضرار مخاطر الاحتيال وجمع الأدلة الجنائية لحالات الاحتيال وضبط تكاليف مكافحة الاحتيال. ومن خلال الاعتماد على خبرتنا، نتمكن من توفير الاستشارات وخدمات الاستجابة للحوادث الأمنية الناشئة عن هجمات الاحتيال فائقة التطور. ويتم دمج هذه الخبرة المهنية في منصتنا القائمة على السحابة، مما يساهم في تحسينها ويضمن جاهزيتها وقدرتها على مساعدة عملائنا في التصدي للتهديدات دائمة التطور والتغير وكافة تكتيكات الاحتيال.