كاسبرسكاي تعزز حماية الشركات من تهديدات البريد الإلكتروني

الأحد 2 يونيو 2024 12:30 م

علنت شركة كاسبرسكي طرح تحديث مهم لحل (Kaspersky Security for Mail Server)، المصمم لتقوية مناعة الأنظمة ضد تهديدات البريد الإلكتروني الناشئة. ويتميز هذا الإصدار الأحدث من هذا الحل بوظائف متقدمة لفلترة المحتوى، وإدارة العزل، وتحسين الشفافية لمراكز العمليات الأمنية (SOC).

وقد كشفت دراسة حديثة أجرتها كاسبرسكي أن نسبة تبلغ 77% من الشركات حول العالم، ونحو 78% في منطقة الشرق الأوسط وتركيا وأفريقيا، قد تعرضت لحادث سيبراني واحد على الأقل في العامين الماضيين. وعلى وجه التحديد، كانت نسبة قدرها 21% من هذه الحوادث عالميًا – في حين بلغت 29% في منطقة الشرق الأوسط وتركيا وأفريقيا – ناتجة عن وقوع الموظفين ضحايا لهجمات التصيد الاحتيالي.

وأشارت كاسبرسكي إلى أنه من المرجح أن يكون العدد الفعلي لهجمات البريد الإلكتروني الخارجية على الشركات أعلى بكثير، حيث لا تتضمن هذه الإحصائيات سوى الحوادث التي أُبلغ فيها عن محاولات التصيد الاحتيالي. لذلك تؤكد هذه الإحصائيات ضرورة وجود حلول أمان قوية لحماية البريد الإلكتروني من التهديدات المتزايدة.

استجابة كاسبرسكي:

لمواجهة التهديدات المتزايدة عبر البريد الإلكتروني، أعادت كاسبرسكي تصميم حل (Kaspersky Security for Mail Servers) بشكل جذري، مع التركيز في تحسين قدرات فلترة المحتوى وإدارة العزل.

أهم مزايا حل **(Kaspersky Security for Mail Server)** المُعاد تصميمه:

1- فلترة متقدمة للمحتوى:

يُقدم التحديث الأخير لحل (Kaspersky Security for Mail Servers) قدرات فلترة للمحتوى متقدمة لمحاربة التهديدات المتطورة بنحو فعال، إذ تتيح للمسؤولين القيام بما يلي:
إنشاء قواعد فلترة معقدة تعتمد على الكلمات المفتاحية الموجودة في سطور رسائل البريد الإلكتروني، ونصوصها الرئيسية، وكذلك اسم المرسل والمرفقات.
دعم الفلترة حسب الترويسات المخفية في النص العادي لرسائل البريد الإلكتروني.
إنشاء قواميس للكلمات المفتاحية المسموحة والمحظورة، وذلك لتحسين قواعد الفلترة لمجموعات المستخدمين المختلفة. ثم تطبيق التغييرات التي أُجريت على هذه القواميس على كافة قواعد الفلترة المرتبطة بها بشكل مركزي، مما يضمن الاتساق والكفاءة في إدارة أمان البريد الإلكتروني.
2- حماية فعالة من تسريب البيانات**:**
دعمت كاسبرسكي حلها (Kaspersky Security for Mail Server) أيضًا بمزايا قوية للحماية من تسريب البيانات (DLP)، ومنها:
مراقبة رسائل البريد الإلكتروني الصادرة بحثًا عن البيانات الحساسة.
إنشاء تعابير عادية للكشف عن أنماط وتنسيقات البيانات الحساسة مثل أرقام بطاقات الائتمان.
منع إرسال البيانات الحساسة خارج المؤسسة أو بين أقسام معينة داخلها.
3- تعزيز الشفافية لمراكز العمليات الأمنية**:**

يوفر أحدث إصدار من (Kaspersky Security for Mail Server) معلومات شاملة حول الوقائع المحظورة لفرق مراكز العمليات الأمنية، ويتضمن ذلك تفاصيل المرفقات، ونتائج عمليات الفحص، والأحكام الخاصة بالروابط المحظورة.
وتتيح هذه الشفافية المحسنة لمحللي مراكز العمليات الأمنية ربط الأحداث بشكل أفضل وتعزيز إستراتيجيات الاستجابة للحوادث.
4- الإدارة المتقدمة للعزل**:**
يمكن للمسؤولين الآن الاستفادة من وظيفة العزل المتقدمة، مما يسمح لهم بعرض رسائل البريد الإلكتروني المعزولة بتنسيقها الأصلي مباشرةً من وحدة التحكم. إذ تعمل هذه المزية على تبسيط عملية إدارة العزل، مما يوفر للمسؤولين قدرًا أكبر من الشفافية والتحكم في تهديدات البريد المحتملة.
وتعليقًا على هذا التحديث المهم، قال تيموفي تيتكوف، رئيس قسم الحلول السحابية وأمن الشبكات في كاسبرسكي: "نحن فخورون بإعلان آخر تحديث لمنتجنا للدفاع عن البريد الإلكتروني، فهو قناة الاتصال الرئيسية في جميع الشركات. وبفضل آليات الدفاع المتعددة الطبقات المدعومة بخوارزميات التعلم الآلي وأنظمة الدفاع الشاملة، لا يكتفي حل (Kaspersky Security for Mail Server) بتوفير حماية قوية ضد مجموعة واسعة من التهديدات فحسب، بل يوفر راحة البال لعملائنا في مواجهة المخاطر السيبرانية المتطورة أيضًا. ومن خلال هذا التحديث، نحن نعزز التزامنا بتقديم حلول متطورة تمكّن المؤسسات من الدفاع ضد برمجيات حصان طروادة غير المألوفة، وهجمات برامج الفدية الموجهة، والتهديدات الناشئة الأخرى في مشهد التهديدات الديناميكي اليوم".