أتيفو نتوركس تتحدث عن اكتشاف ومنع التهديدات الإلكترونية

الأربعاء 23 أغسطس 2017 06:08 م

عندما نتحدث عن التهديدات الأمنية، سرعان ما يتبادر إلى الذهن القراصنة الخارجيون الذين يقومون بشن مجموعة من الهجمات مثل أحصنة طروادة أو هجمات التصيد الإلكتروني أو هجمات APTs، وغيرها

ومع ذلك، فإن الوقت قد حان لكي تتوقف الشركات عن الاكتفاء بالبحث عن مصادر التهديد الخارجية وحدها، والتفكير مليًا بعوامل التهديد الداخلية التي قد تكون كامنة في شبكاتها فقد خلص استطلاع أجرته "آي دي سي" IDC أن التهديد الأكبر الذي تواجهه الشركات في الشرق الأوسط ناشئ من الداخل وتشكل جرائم سرقة البيانات وإصابة الأجهزة وهجمات APTs القوة الدافعة للتطور المتسارع في مشهد التهديدات

فيما يتعلق بالتهديدات الداخلية، فهي تتوزع عادة إلى ثلاثة أنواع:

الموظفون المطلعون أصحاب النوايا الخبيثة: ينطوي سلوك الموظف المطلع صاحب النوايا الخبيثة على دافع لإلحاق الضرر مصحوب بقرار نهائي للتصرف بشكل غير مناسب من ضمن ذلك على سبيل المثال، حفظ وتسليم المعلومات الحيوية إلى منافس بعد إنهاء خدماته أو تحقيق مكاسب مالية أو غيرها من المنافع الشخصية
الإهمال: يمكن أن يحدث الإهمال في حال كان الموظف يبحث عن طرق لتجنب التقيد بالسياسات التي يرى بأنها تعيق عمله وفي حين أن معظم الموظفين على دراية تامة بالمخاطر الأمنية ويقدرون أهمية الامتثال، فمن الممكن أن تكون حلولهم الوقتية محفوفة بالمخاطر
التصرف المتهور: قد يحدث التصرف المتهور نتيجة الإهمال غير المقصود لأحد الموظفين، مما قد يتسبب في حدوث الاختراقات الأمنية ومن الممكن أن يحدث ذلك عادة عندما يتوانى الموظفون عن تصحيح أنظمتهم، واتباع سياسة أحضر جهازك الشخصي للعمل أو التعرض عن طريق الخطأ لإحدى هجمات الاختراق الأمني أو هجوم الوسيط أثناء الاتصال بشبكات الإنترنت المجانية Wi-Fi.
وبالإجمال، عند التفكير في التهديدات الناشئة من الداخل، سرعان ما يتبادر إلى الذهن الموظفين المطلعين ذوي النوايا الخبيثة الذين يبحثون عن مكاسب خاصة بهم ومع ذلك، نلاحظ حدوث قدر هائل من الانتهاكات لأن العديد من الموظفين يفشلون في فهم المخاطر الأمنية وعدم الالتزام بالسياسات وعندما يتعلق الأمر بتعريض البيانات المهمة للخطر، غالبا ما يشير هؤلاء المذنبون بأصابع الاتهام إلى الموظفين والمقاولين وموردي الطرف الثالث وتورطهم في البيانات المسروقة والتي عادة ما تكون مستندات مكتبية مخزنة على وسائط متعددة مثل وسائط التخزين القابلة للإزالة USB وأجهزة الكمبيوتر المحمول

لقد أدى الاعتماد الجماعي على تكنولوجيا الحوسبة السحابية و سياسة أحضر جهازك الشخصي للعمل إلى زيادة احتمالات التهديدات الداخلية ويتيح هذا الاتجاه للموظفين فرصة أكبر للوصول إلى الشبكة – مما يساعد الموظفين المطلعين ذوي النوايا الخبيثة على التهرب من الأنظمة الأمنية المقيدة بمعايير قياسية

وعلى الرغم من تزايد تكرار ظهور هذه الأنواع من الاختراقات، إلا أن العديد من الشركات تتجاهل كليًا هذه المسألة ونجدها تلجأ لاستخدام أنظمة الدفاع التقليدية التي صممت فقط لمنع هجمات القرصنة الإلكترونية من خلال جدار الحماية ومكافحة الفيروسات أو حلول النطاقات الأمنية الأخرى وكشف استطلاع أجرته مؤسسة جارتنر أن هذا الإنفاق من المتوقع أن يصل إلى ملياري دولار بحلول عام 2020 في منطقة الشرق الأوسط وشمال أفريقيا

ومع ذلك، فإن الشركات تنفق مبالغ أكبر على التكنولوجيا القديمة المعقدة، غير القادرة أو المؤهلة لدرء التكتيكات والأدوات المتطورة التي يستخدمها مجرمو الإنترنت خلسة وهذا النقص في التركيز على أهمية تأمين البيانات الهامة يدل على الحاجة إلى اتباع نهج جديد لمنع تلك التهديدات من الداخل نهج يوفر إمكانية الكشف عن حالات الاستطلاع المريبة لتتبع الوصول غير المصرح به إلى الأصول، ومعرفة المخاطر الطارئة المرتبطة بعمليات التعريف الخاطئة وسوء استخدام بيانات التعريف الشخصي

عندما يتعلق الأمر بالتخفيف من وطأة التهديدات الداخلية، فإن الإقرار بوجود تلك المخاطر سيساعد الشركات في اتخاذ خطوات مضمونة لمنع هذه الهجمات. ولمواجهة هذه التهديدات على النحو الأمثل، تحتاج الشركات إلى تطبيق استراتيجيات وحلول وقائية بإمكانها التقليل من حجم الهجمات الداخلية المدمرة، ولكنها تحتاج أيضا إلى امتلاك القدرة على الكشف عن التهديدات التي تتهرب من أنظمة الرقابة والتتبع المتطورة بسرعة وبدقة عالية.

وبالتالي، يقترح الخبراء تطبيق تقنيات الخداع التي تتيح الرؤية المبكرة واستجابة أسرع للحالات الأمنية المكتشفة، وتزيد بشكل كبير في السرعة التي يتم خلالها الكشف عن التهديدات داخل الشبكة وإطلاق تنبيهات عالية الدقة وتبسيط الارتباط بين البيانات، وتسريع إجراءات الاستجابة للحوادث لغرض أتمتة عملية منع وحجب الهجمات. تم تصميم تقنية الخداع وفق أعلى مستوى من الأصالة والمصداقية، وهي تتميز بقدرتها على التعلم الذاتي والتأقلم مع البيئة المحيطة، والقيام بالتحديث التلقائي لوسائل الخداع، وكذلك التخفي لتجنب أخذ بصمات المهاجمين بعد شن الهجوم.

ومن شأن هذا، إلى جانب قدرات الشراك الخداعية التفاعلية عالية المستوى التي يتم تصميمها لتتماشى مع طبيعة بيئات الشركات 100%، سيجعل من الصعب على جهات التهديد الخارجية والداخلية تمييز تلك البيئة نظرًا لما تتسم به من دقة في التخفي والتمويه. إن تطبيق تقنية الخداع على جهات التهديد الداخلي لا يضيف عبئا على فرق الأمن، وذلك لأن التصميم لا يتطلب بالضرورة مبدأ الحاجة للتعلم لنكون بمستوى جيد أو توقيعات أو مطابقة الأنماط أو تحليلات البيانات الكبيرة.

وباعتبار أن التنبيهات تستند إلى مبدأ المشاركة وتشمل أنشطة هجوم مدعمة، لايوجد هناك نتائج إيجابية كاذبة، وبالتالي، يمكن التعرف على الأنظمة المصابة بسهولة من أجل العمل على حجبها وتصحيحها مباشرة. ونتيجة لفاعليتها العالية، تشهد تقنيات الخداع انتشارًا متسارعًا، نظرًا لقدرتها على الكشف عن التهديدات الداخلية والتهديدات الناشئة عن الموردين والتي تستهدف بروتوكول الإنترنت في الشركة وسجلات الموظفين المالية وغيرها من المعلومات الحيوية المخزنة في مراكز البيانات أو التي يتم تبادلها فيما بين أطراف ثالثة.

وفي حين أن الهجمات الخارجية ستواصل غزوها المحموم للشركات، سيكون من الخطأ التغاضي عن التهديدات التي يحدثها موظفوكم والموردون الذين تتعاملون معهم. إن حلول الرؤية والكشف المبكر عن التهديدات مثل تقنية الخداع، إلى جانب برامج تدريب الموظفين من شأنها أن تتيح لكم منصة دفاعية قوية ضد هذه التهديدات الداخلية وتعزز حماية أصولكم الحيوية.