10 توجهات ترسم ملامح أمن البنى التحتية الرقمية

إعداد: بشار باغ - غرافيك: أسيل الخليلي

تُستهدف الشركات ومزودو الخدمات والحكومات يومياً بهجمات حجب الخدمة الموزعة المعروفة بـ «DDoS» إضافة إلى تهديدات متطورة في جميع أنحاء المنطقة. ومع تزايد اتجاه إنترنت الأشياء في منطقة الشرق الأوسط، أضحت هذه الهجمات تشكل التهديد الأكبر لجميع أنواع الشبكات مما يرفع الطلب على خدمات أمن البنى التحتية بحسب تقرير شركة آربور نتوركس، الشركة المتخصصة في أمن المعلومات.

1 500

غيغابايت في الثانية حجم أكبر هجوم مسجل خلال العام الماضي مع تسجيل هجمات أخرى 450 غيغابايت في الثانية، و425 غيغابايت في الثانية و 337 غيغابايت في الثانية. أي إن حجم الهجمات قد تنامى خلال 11 عاماً بما هو أكثر من 60 ضعفاً.

2 56 %

من المستطلعين في الدراسة قالوا إنهم تعرضوا لهجمات متعددة النواقل تستهدف البنية التحتية والتطبيقات والخدمات في آن واحد، بارتفاع قدره 42 % مقارنة بالعام الماضي. بينما ذكر 93 % تعرضهم لهجمات حجب الخدمة الموزعة DDoS. أما أكثر الخدمات المستهدفة شيوعاً والتي تستهدفها هجمات التطبيقات فهي DNS (وليس HTTP).

3 السحابة الإلكترونية تتعرض للهجوم

قبل عامين، شهد 19 % من المستطلعين هجمات تستهدف الخدمات القائمة على السحابة الإلكترونية. ونمت هذه النسبة إلى 29 % في العام الماضي، وأصبحت الآن 33 % هذا العام - وهو اتجاه متصاعد واضح. وفي الواقع، تعرض 51 في المئة من مشغلي مركز البيانات لهجمات DDoS على اتصالات الإنترنت الخاصة بهم. وكانت هناك أيضاً زيادة حادة في عدد مراكز البيانات التي تعرضت لهجمات من ملقمات ضمن شبكاتهم، حيث ارتفعت النسبة إلى 34 في المئة مقارنة بـ 24 في المئة العام الماضي.

4 التركيز على الحالات الداخلية:

ارتفعت نسبة المستطلعين الذين تعرضوا لهجمات من الداخل إلى 17 في المئة هذا العام (كانت 12 % في العام الماضي). ولا يمتلك ما يقرب من 40 في المئة من المشاركين حتى الآن أي تطبيق لمراقبة الأجهزة الشخصية للأفراد الذين يعملون عليها BYOD عبر الشبكة. وتضاعف عدد الحوادث الأمنية المتعلقة بـ BYOD إلى 13 في المئة مقارنة بستة في المئة العام الماضي.

5 مشكلة التوظيف:

هناك انخفاض كبير في عدد الذين يسعون لزيادة مواردهم الداخلية لتحسين الاستعداد والاستجابة للحالات، بانخفاض من 46 إلى 38 %.

6 تهاوي جدران الحماية الرقمية

أفاد أكثر من نصف عدد الشركات المستطلعة بفشل جدار الحماية أمام هجوم DDoS، بينما كان العدد هو الثلث في العام السابق. وتتمثل نقاط الضعف في جدران الحماية firewalls في كونها أول ضحايا تلك النوعية من الهجمات بسبب القضاء على قدرتها على تتبع الاتصالات. ولأنها مضمنة في الشبكة، فإنها تضعف أداءها خلال الهجمات.

7 تخطيط أفضل

شهد العام 2015 زيادة في نسبة المستطلعين الذين وضعوا خطط استجابة للحوادث، وخصصوا على الأقل بعض الموارد للرد على مثل هذه الحالات، بارتفاع قدره حوالي الثلثين عن العام الماضي، حيث وصلت النسبة إلى 75 % هذا العام.

8 تسرع الاستجابة

ذكر 57 % من الشركات أنها تتطلع إلى استخدام حلول لتسريع عمليات الاستجابة أمام الهجمات. ومن بين مقدمي الخدمات، نجح قرابة الثلث في تقليل الوقت المطلوب لاكتشاف التهديد المستمر المتقدم (APT) في شبكة الاتصال الخاصة بهم إلى أقل من أسبوع واحد، وذكر 52 % أن الوقت اللازم بداية من الاكتشاف وحتى الاحتواء انخفض إلى أقل من شهر واحد.

9 ابتزاز

لم يكن الدافع الرئيس هذا العام هو «النضال البرمجي» أو التخريب ولكنه تمثل في «قدرات هجومية اعتراضية إجرامية»، وهو شيء يرتبط عادة بمحاولات الابتزاز عبر الإنترنت.

10 اعتماد متزايد على الدعم الخارجي

أدى نقص الموارد الداخلية إلى زيادة الاستعانة بالخدمات المدارة والدعم الخارجي، حيث تعاقد 50 في المئة من الشركات مع شركات خارجية للاستجابة للحوادث. وهذا ارتفاع قدره 10 % ضمن مقدمي الخدمات. ومن بين مقدمي الخدمات، ذكر 74 في المئة وجود طلب متزايد من العملاء على الخدمات المدارة.

البيان