أدوات التصيّد ذات معدلات الاختراق المرتفعة: ما يجب أن يعرفه فريق الأمن



تقيس Push Security «معدل الاختراق» لأدوات التصيّد، أي نسبة الهجمات التي تتجاوز أمن البريد وبوابات الويب والتصفح الآمن وتصل إلى المستخدم. وتتفاوت الأدوات في ذلك تفاوتًا كبيرًا.

- يجب أن يتجاوز كل هجوم تصيّد أمن البريد وتصفية الويب والتصفح الآمن قبل أن يصل إلى الموظف.
- تعرّف Push Security معدل الاختراق بأنه نسبة الهجمات التي تتجاوز هذه الطبقات وتصل إلى المستخدم.
- تنجح بعض أدوات التصيّد في ذلك أكثر بكثير من غيرها.
- ينبغي أن تركّز فرق الأمن على الأدوات الأكثر نجاحًا في الاختراق.

تتناول مادة جديدة من Push Security التصيّد من زاوية عملية: لا يهم عدد الهجمات المرسلة بقدر ما يهم عدد ما

يتجاوز منها الضوابط القائمة في المنشأة.

المقياس

تستخدم الشركة مصطلح **معدل الاختراق** للدلالة على نسبة الهجمات التي تتجاوز أمن البريد الإلكتروني وبوابات الويب والتصفح الآمن وتصل إلى المستخدم. والفكرة بسيطة: يجب أن يمر كل هجوم تصيّد بهذه الطبقات أولاً، وبعض الأدوات تتجاوزها أكثر من غيرها بكثير.

لا يذكر المقتطف الذي اطلعنا عليه أسماء الأدوات أو أساليبها أو النسب، ولذلك لا نوردها هنا. ويُستحسن الرجوع إلى المقال الأصلي كاملاً قبل استخلاص نتائج بشأن أدوات بعينها.

أهمية الموضوع

بالنسبة إلى الجهات الخاضعة للتنظيم، الفائدة الأبرز تتعلق بترتيب الأولويات. فمحتوى التوعية وقواعد الكشف وخطط الاستجابة ينبغي أن تُبنى على الأدوات والأساليب التي تصل فعلاً إلى الموظفين، لا على حجم بلاغات التصيّد الإجمالي.

كما يؤكد ذلك أن ضوابط البريد والويب طبقة واحدة وليست ضمانًا كاملاً. وما يحدث بعد وصول الرسالة، كإبلاغ المستخدمين وحماية الهوية وسرعة الاستجابة، يستحق الاهتمام نفسه.

نهج مقترح

راجعوا المادة الأصلية، وقارنوها ببيانات التصيّد لديكم، وقرروا ما إذا كانت اختباراتكم تعكس الأدوات الأكثر قدرة على تجاوز منظومتكم.

ما يجب فعله الآن

1. اقرؤوا مقال Push Security كاملاً ودوّنوا الأدوات والأساليب ذات الصلة ببيئتكم.
2. قارنوا ما ورد فيه ببيانات التصيّد وبلاغات المستخدمين لديكم لمعرفة ما يصل فعليًا إلى صناديق البريد.
3. نفّذوا محاكاة تصيّد تعكس أساليب التهرّب، لا الطُعوم البسيطة فقط.
4. تأكدوا من وجود قناة إبلاغ سهلة للمستخدمين ومن سرعة فرز البلاغات في مركز العمليات الأمنية.
5. راجعوا ضوابط حماية الهوية حتى لا يؤدي نجاح رسالة تصيّد إلى استيلاء مباشر على الحساب.