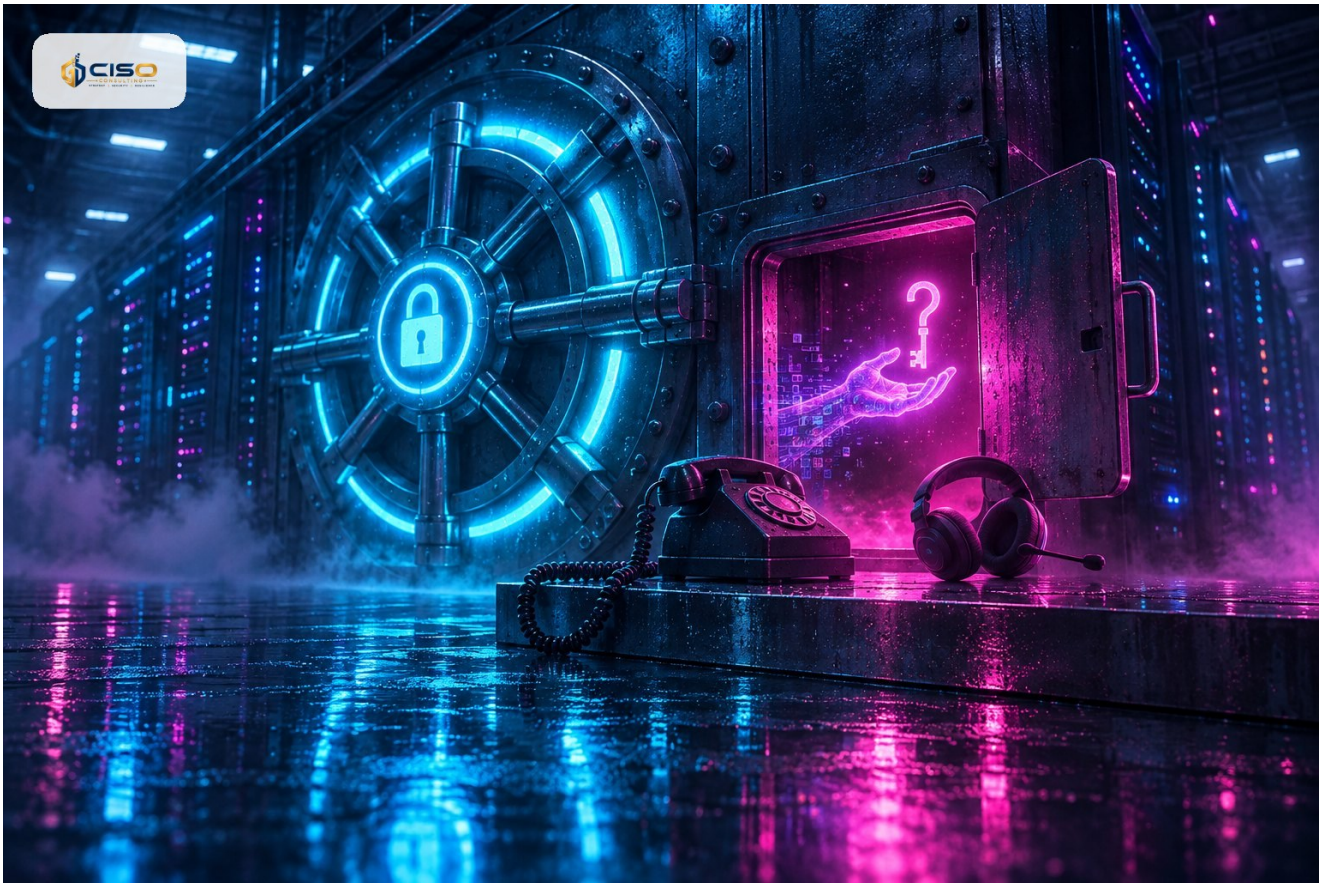
إعادة تعيين كلمات المرور عبر مكتب الخدمة: سدّ الثغرة التي تتجاوز المصادقة متعددة العوامل



يرى مقال برعاية جهة تجارية أن أسئلة التحقق المعرفية في مكتب الخدمة تُضعف ضوابط الدخول القوية، وأن الهندسة الاجتماعية والذكاء الاصطناعي يجعلان استعادة الحسابات هدفاً رئيسياً، ويدعو إلى تحقق موحّد.

- قد تتجاوز عملية استعادة الحساب في مكتب الخدمة المصادقة متعددة العوامل والوصول المشروط إذا اعتمدت على أسئلة مثل اسم المدير أو القسم.
- يستطيع المهاجمون جمع الإجابات من لينكدإن ومواقع الشركات ووسائل التواصل والبيانات المسرّبة.
- تنتحل مجموعات مثل Scattered Spider صفة الموظفين للحصول على إعادة تعيين كلمات المرور أو تسجيل أجهزة مصادقة جديدة.
- يستشهد المقال باستطلاع Gartner لعام 2025 (62% من المنظمات تعرضت لهجوم هندسة

اجتماعية بتقنية التزييف العميق) وبتقرير Verizon DBIR لعام 2026 (نجاح الهندسة الاجتماعية عبر المكالمات والرسائل أعلى بنسبة 40% من التصيّد البريدي).

- يوصي بتحقق إلزامي قبل التغييرات الحساسة وتدريب الموظفين واستعادة ذاتية آمنة. والمقال برعاية Specops Software.

الثغرة

عزّزت مؤسسات كثيرة تسجيل دخول موظفيها بالمصادقة متعددة العوامل (MFA) والوصول المشروط. ويشير مقال برعاية Specops Software إلى أن قيمة هذه الضوابط تتراجع إذا كان مسار استعادة الوصول أضعف من تسجيل الدخول نفسه. فما زال كثير من مكاتب الخدمة يتحقق من الهوية بأسئلة معرفية، مثل اسم مدير الموظف أو قسمه.

ويبيّن المقال أن هذه المعلومات يسهل جمعها من الملفات المهنية ومواقع الشركات ووسائل التواصل والبيانات المسرّبة، ويذكر أن إرشادات الهوية الرقمية الصادرة عن NIST لم تعد تعدّ أسئلة الأمان وسيلة مصادقة مقبولة.

لماذا تتفاقم المشكلة

يذكر المقال أن مجموعات مثل Scattered Spider تستهدف مكتب الخدمة، فتنتحل صفة الموظفين للحصول على إعادة تعيين كلمات المرور أو تسجيل أجهزة MFA جديدة. ويجعل الذكاء الاصطناعي التوليدي الروايات المقنعة أسهل، بل يمكنه محاكاة الأصوات. ويورد المقال استطلاع Gartner لعام 2025 الذي أفاد بأن 62% من المنظمات تعرضت لهجوم تزييف عميق يتضمن هندسة اجتماعية أو عمليات آلية، وتقرير Verizon DBIR لعام 2026 الذي وجد أن الرسائل والمكالمات الصوتية أكثر نجاحاً بنسبة 40% من التصيّد عبر البريد.

وخلاصته ألا يُطلب من الموظف الحكم على مدى إقناع المتصل، بل أن يكون التحقق خطوة إلزامية في سير العمل، مع التدريب وإتاحة الرفض أو التصعيد.

قراءة المصدر

يروّج المقال لمنتج الجهة الراعية، لذا ينبغي تقدير ادعاءاته بحذر. غير أن المبدأ الرقابي سليم ولا يرتبط بمنتج بعينه: يجب أن تكون الاستعادة بقوة المصادقة نفسها.

ما يجب فعله الآن

1. راجعوا طريقة تحقق مكتب الخدمة من المتصلين قبل إعادة تعيين كلمات المرور وتسجيل أجهزة MFA، وأوقفوا اعتماد أسئلة المدير أو القسم دليلًا على الهوية.
2. اجعلوا التحقق خطوة إلزامية موثّقة في سير العمل عبر قناة يصعب على المهاجم الوصول إليها، لا اجتهاداً من الموظف.
3. اشترطوا موافقة إضافية أو تصعيداً للحسابات ذات الصلاحيات العالية ولأي طلب تسجيل جهاز MFA جديد.
4. درّبوا موظفي مكتب الخدمة على انتحال الأصوات والهندسة الاجتماعية المدعومة بالذكاء الاصطناعي،

وامنحوهم صلاحية الرفض أو التصعيد.

5. فكّروا في الاستعادة الذاتية الآمنة لتقليل الطلبات، واختبروا إجراءات الاستعادة بتمارين هندسة اجتماعية داخلية.