الأمن السيبراني للمؤسسات الأصغر حجمًا

قائمة التدقيق الخاصة بمدير أمن البيانات: حماية الاتصالات للجهات الخارجية

اختيار البائعين مع وضع الأمن السيبراني في الاعتبار

في كل مرة تقوم فيها بتقييم بائع محتمل، راجع الأسئلة التالية:

- ☐ ما هي الخبرة التي يمتلكها البائع في خدمة عملاء مشابهين لعملاء مؤسستك؟
- ☐ هل وثقوا امتثالهم لمعايير الأمن السيبراني المعروفة (مثل إطار عمل NIST أو معيار الأيزو 27001، أو هل يمكنهم تقديم تقرير SOC2)؟
- ☐ أي من بياناتك و/أو أصولك سيحتاجون إلى الوصول إليها لأداء خدماتهم، وهل يطلبون أي وصول غير ضروري ظاهريًا؟
- ☐ كيف يخططون لحماية أصول مؤسستك وبياناتها الموجودة في حوزتهم؟
- ☐ كيف يديرون المخاطر السيبرانية الخاصة بالجهة الخارجية، وهل يمكنهم تقديم معلومات عن أمن سلسلة التوريد الخاصة بهم؟
- ☐ ما خطتهم للتعافي من الكوارث واستمرارية الأعمال في حالة وقوع حادث يؤثر في مؤسستك؟
- ☐ كيف سيحافظون على تحديث مؤسستك من حيث التواصل، والتهديدات، والتغييرات داخل مؤسساتهم؟

تحديد المخاطر من خلال الجهات الخارجية

قم بإجراء تقييم للمخاطر السيبرانية للجهة الخارجية، بما في ذلك الخطوات التالية:

- ☐ قم بإنشاء قائمة بالعلاقات مع جميع البائعين، والأصول والبيانات المعروضة في كل منها، وحدثها باستمرار.
- ☐ قم بإجراء مراجعة للبيانات التي يمكن لكل بائع أو جهة خارجية الوصول إليها، مع ضمان التزام كل مستوى من مستويات الوصول بمبدأ "الامتياز الأقل".
- ☐ رتب علاقاتك مع البائع والجهات الخارجية (منخفضة، متوسطة، عالية) استنادًا إلى التأثير الذي قد يحدثه خرق أنظمتهم على مؤسستك.
- ☐ بدءًا من البائعين الأكثر عرضة للمخاطر، قم بتقييم إمكانات الأمن السيبراني لكل مزود والامتثال للمعايير ذات الصلة.
- ☐ قم بتطوير خطة للتقييم الأمني المنتظم، مع الأخذ في الاعتبار أنك قد ترغب أحيانًا في إجراء تقييمات في الموقع للبائعين الأكثر عرضة للمخاطر و/أو الذين لديهم إمكانية وصول أعلى إلى بيانات العميل.

إدارة أمن الجهة الخارجية

- ☐ قم بإجراء العناية الواجبة الشاملة. حدد توقعات الأمن السيبراني في جميع طلبات مؤسستك للمقترحات والعقود واستمرارية العمل والاستجابة للحوادث واتفاقات مستوى الخدمة مع البائعين. اتفق على المسؤوليات والالتزامات في حالة وقوع حادث سيبراني.
- ☐ استفسر عن ممارسات الأمن السيبراني للمؤسسات المالية والكيانات الأخرى التي تتعامل معها أو تشارك البيانات معها، مع الأخذ في الاعتبار أن البائعين والجهات الخارجية يجب أن يتبعوا أيضًا أي متطلبات أمن سيبراني يجب أن تلبيها مؤسستك.

- ☐ استخدم التدابير المحددة والمتفق عليها لمراقبة امتثال البائعين لمعايير الأمن السيبراني.
- ☐ تحقق مع البائعين الذين يتعاملون مع البيانات الحساسة لمعرفة ما إذا كانوا يقدمون المصادقة الثنائية العوامل أو التشفير أو إجراءات أمنية أخرى لأي حسابات لديك.
- ☐ تأكد من أن جميع برامج الجهة الخارجية والأجهزة التي تقوم بتثبيتها تحتوي على مصافحة أمان بحيث يتم تأمين عمليات التشغيل من خلال رموز المصادقة ولن يتم تنفيذها إذا لم يتم التعرف على الرموز.
- ☐ إذا صادفت منتجات بائع مزيفة أو غير مطابقة للمواصفات، فاعمل على التفاوض بشأن قرار أو أي استراتيجية للخروج من التعامل معه.
- ☐ قم سنويًا بتقييم عقود البائعين والتأكد من استمرارها في تلبية متطلباتك المتعلقة بالتوجيه الإستراتيجي وأمان البيانات التنظيمية. عند إنهاء العقد، قم بتضمين شروط حول استعادة الأصول أو البيانات الخاصة بالمؤسسة والتحقق من أن البائع يحذف الأصول أو البيانات بالكامل، وقم بمنع أي وصول إلى الأنظمة أو الخوادم الخاصة بالمؤسسة.

تبادل المعلومات

- ☐ تأكد من أن لديك قنوات اتصال ونقاط اتصال واضحة للتواصل بشأن المشكلات الأمنية مع بائعي مؤسستك ونظرائها.
- ☐ تحقق من أن لدى مؤسستك إجراءات لضمان تبادل معلومات الأمن السيبراني الموثوقة والقابلة للتنفيذ في الوقت المناسب مع أصحاب المصلحة الداخليين والخارجيين (بما في ذلك الكيانات والسلطات العامة داخل القطاع المالي وخارجه).
- ☐ تتبع التحديثات ذات الصلة بشأن ما تخوضه المؤسسات الأخرى مع الجهات الخارجية فيما يتعلق بالتهديدات، ونقاط الضعف، والحوادث، والاستجابات من خلال المشاركة في مؤسسات تبادل المعلومات مثل FS-ISAC والبحث عن مصادر معلومات تهديدات أخرى.