

دليل على مستوى مدير أمن المعلومات: حماية الاتصالات للجهات الخارجية

تحديد المخاطر من خلال الجهات الخارجية

- قم بإنشاء قائمة محدثة بالعلاقات مع جميع البائعين، والأصول والبيانات المعروضة في كل منها، واحتفظ بها.
- راجع البيانات التي يستطيع كل بائع أو جهة خارجية الوصول إليها. تأكد من أن هذا المستوى من الوصول يلتزم بمبدأ «أقل الامتيازات».
- رتب علاقاتك مع البائع والجهات الخارجية (منخفضة، متوسطة، عالية) استنادًا إلى التأثير الذي قد يحدثه خرق أنظمتهم على مؤسستك.

إدارة أمن الجهة الخارجية

- قم بإجراء العناية الواجبة الشاملة. حدد توقعات الأمن السيبراني في طلبات مؤسستك للمقترحات والعقود واستمرارية العمل والاستجابة للحوادث واتفاقيات مستوى الخدمة مع البائعين. اتفق على المسؤوليات والالتزامات في حالة وقوع حادث سيبراني.
- استفسر عن ممارسات الأمن السيبراني الخاصة بجهات خارجية أخرى مثل، المؤسسات المالية التي تتعامل معها أو تشارك البيانات معها. يجب أيضًا على البائعين وأي منظمات أخرى، تشارك البيانات بها أو تعرض الأصول إليها، اتباع أي متطلبات أمن سيبراني على مؤسستك للالتزام بها.
- 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.

مشاركة المعلومات

- تأكد من أن لديك قنوات اتصال ونقاط اتصال واضحة للتواصل بشأن المشكلات الأمنية مع بائعي مؤسستك ونظرائها.
- شارك في مشاركة موثوقة في الوقت المناسب لمعلومات الأمن السيبراني القابلة للتنفيذ مع أصحاب المصلحة الداخليين والخارجيين (بما في ذلك الكيانات والسلطات العامة داخل القطاع المالي وخارجه).

كيفية اختيار البائعين مع وضع الأمن السيبراني في الاعتبار

اطرح الأسئلة التالية على البائعين المحتملين لقياس استعدادهم للأمن السيبراني والوعي به وبالتالي التأثير الذي سيدحدثونه على ملف المخاطر بمؤسستك:

1. ما الخبرة التي يمتلكونها؟ تعرف على تاريخ البائع في خدمة العملاء. هل قاموا بخدمة عملاء مشابهين لمؤسستك من قبل؟
2. هل وثقوا امتثالهم لمعايير الأمن السيبراني المعروفة مثل إطار عمل TSIN أو معيار الأيزو 27001، أو هل يمكنهم تقديم تقرير SOC2؟
3. أي من بياناتك و/أو أصولك سيحتاجون إلى الوصول إليها لأداء خدماتهم؟ هل يطلبون أي وصول غير ضروري على ما يبدو؟
4. كيف يخططون لحماية أصول مؤسستك وبياناتها الموجودة في حوزتهم؟
5. كيف يديرون المخاطر السيبرانية الخاصة بالجهة الخارجية؟ هل يمكنهم تقديم معلومات عن سلسلة التوريد الخاصة بهم؟
6. ما خططهم للتعافي من الكوارث واستمرارية الأعمال في حالة وقوع حادث يؤثر في أصول المؤسسة و/أو بياناتها؟
7. كيف سيحافظون على بقاء مؤسستك على اطلاع بأحدث التطورات؟ ما خططهم للتعريف بالاتجاهات والتهديدات والتغييرات داخل مؤسستهم؟