دليل على مستوى مدير أمن المعلومات: حماية الاتصالات للجهات الخارجية

كيفية اختيار البائعين مع وضع الأمن السيبراني في الاعتبار

اطرح الأسئلة التالية على البائعين المحتملين لقياس استعدادهم للأمن السيبراني والوعي به وبالتالي التأثير الذي سيحدثونه 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 NIST 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 خطتهم 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 خطتهم للتعريف بالاتجاهات والتهديدات والتغييرات داخل مؤسستهم؟

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.
⇒ بدءًا من أكبر البائعين المعرضين للمخاطر، قم بتقييم إمكانات الأمن السيبراني لكل مزود. يُعد الالتزام بالمعايير ذات الصلة نقطة بداية جيدة. ضع خطة للتقييم الأمني المنتظم. قد تحتاج أحيانًا إلى إجراء تقييمات في الموقع للبائعين ذوي أعلى المخاطر و/أو الوصول الأكبر لبيانات العملاء.

إدارة أمن الجهة الخارجية

⇒ قم بإجراء العناية الواجبة الشاملة. حدد توقعات الأمن السيبراني في 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 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 الالتزام 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.
⇒ 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.

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).
⇒ تتبع التحديثات ذات الصلة حول ما تواجهه المنظمات الأخرى مع أطرافها الثالثة فيما يتعلق بالتهديدات ونقاط الضعف والحوادث والاستجابات لتعزيز دفاعات مؤسستك، وزيادة الوعي بالموقف، وتوسيع نطاق التعلم. كونك جزءًا من مؤسسات مشاركة المعلومات، على سبيل المثال، FS-ISAC، سوف يسهل التحديث.