

صناعة الأمن السيبراني

في هذه المقالة، سنفصل المجالات الشائعة في الأمن السيبراني.

يصبح الأمن السيبراني مجالاً أوسع مع انتقال المزيد من الصناعات إلى الإنترنت وأصبحت جزءاً من المشهد الرقمي. هذا يعني أن هناك احتياجات للأمن السيبراني في كل صناعة تقريباً بالإضافة إلى كون الأمن السيبراني صناعة بحد ذاته. لم تعد الأدوار الأمنية مجرد الصورة النمطية للهاكرز الذين يخترقون الأنظمة ويكتبون الأكواد طوال الوقت؛ الأمن السيبراني ككل يشمل العديد من المهارات التي تعمل معاً.

في هذه المقالة، سنفصل بعض المجالات الكبيرة في صناعة الأمن السيبراني. هناك الكثير من التداخل بين المجالات المختلفة ومهن الأمن السيبراني، لذا ضع في اعتباك أن المجالات ليست مرسومة بخطوط صارمة، خاصة أنها تستمر في التطور!



الهندسة الأمنية

تشير هذه الفقرة إلى التنفيذ الفني لأشكال مختلفة من الأمان.

- **أمن المعلومات (InfoSec)** يحمي البيانات بأي شكل من الوصول غير المصرح به، التعديل، المشاركة، أو الحذف من قبل الأشخاص الخطأ.
- **أمن الشبكات** يهتم ببنية الشبكة الخاصة بالمؤسسة التي تحمي ضد الوصول غير المصرح به أو اعتراض البيانات.
- **أمن التطبيقات** يشير إلى تنفيذ التدابير التي تدافع عن التطبيقات (المحمولة، المكتبية، أو الويب) من الهجوم، بما في ذلك الحلول البرمجية والعتادية. أمثلة على أمن التطبيقات تشمل الترميز الآمن، استخدام برامج مكافحة الفيروسات، الجدران النارية، والتشفير.
- **أمن السحابة** يشير إلى المجال الجديد لضمان أمان الموارد التي يتم تحميلها إلى السحابة. الشركات والمستخدمون ينقلون باستمرار المزيد من الموارد إلى السحابة، ويجب على المحترفين في هذا المجال أن يكونوا على دراية بتنفيذ الأمان في هذا البيئة.
- **التشفير** يركز على الطرق لإخفاء وكشف المعلومات بحيث تكون البيانات قابلة للقراءة أو الاستخدام فقط من قبل الأشخاص المصرح لهم. يتطلب ذلك الإلمام بجميع أنواع خوارزميات التشفير والتجزئة.

- **أمن البنية التحتية الحيوية** هو الدفاع عن الأنظمة الفيزيائية التي تصبح أكثر رقمية/مرتبطة بالشبكات، مثل شبكات الطاقة، المستشفيات، أنظمة المياه والصرف، وحتى المدارس. من بين القضايا التي تظهر هي الكوارث الطبيعية والانقطاعات.

الحوكمة والامتثال

من الضروري فهم القوانين واللوائح الدولية والفدرالية والمحلية للأمان. لهذا تأثير في عمليات الأمان لجميع المنظمات. الامتثال يشير إلى التأكد من أن المؤسسة تنفذ سياسات معينة، وتدقيقها بشكل مستمر أيضاً.

هذا يصبح مجال عمل متزايد الأهمية. على الرغم من أن هذه الأدوار قد لا تتطلب معرفة بالبرمجة، إلا أنها تتطلب معرفة أساسية بالأمن السيبراني وكذلك جميع القوانين واللوائح التي تؤثر في صناعة معينة.

إدارة المخاطر ومخبرات التهديدات

لن يكون أي نظام مثاليًا أبدًا، وسيكون هناك دائمًا مخاطر، لذا فإن هذا المجال من العمل يتعلق بإدارة تلك المخاطر.

كيف تتم إدارة المخاطر؟ من خلال تحديد المخاطر، تقييم احتمال وتهديد نقاط الضعف الأمنية، وإيجاد التدابير الأمنية الأكثر فعالية من حيث التكلفة والكفاءة.

مخبرات التهديدات هي جمع مستمر للمعرفة بالهجمات المحتملة. قد تبدو المخبرات كمعرفة الدوافع وراء الهجمات، وما هو حجم الهجمات الممكنة، وما هي النواقل التي قد تستخدمها. غالبًا ما تتقاطع هذه الأدوار مع علم البيانات والتعلم الآلي بسبب الحاجة إلى معالجة كل هذه المعلومات.

عمليات الأمان

الأشخاص الذين يعملون في هذا المجال مسؤولون عن تنفيذ مبادئ الأمان، مراقبة الحوادث، والتعافي من الكوارث. يعملون عن كثب مع الجميع تحت مظلة الأمان:-

- اكتشاف متى يحدث شيء خطأ.
- تنفيذ تدابير وقائية ضد الهجمات السيبرانية.
- التأكد من وجود نسخ احتياطية في حالة تم اختراق النظام وفقدان البيانات.
- تتبع التغييرات في النظام.
- وضع خطط التعافي من الكوارث مقدماً.
- إنشاء الوثائق وسياسات المنظمة لكل ما سبق.

التعليم

تعليم الأمان هو مجال متنامٍ بحد ذاته! يعترف هذا المجال بأن التقنيات المصممة بشكل آمن هي فقط بقوة الأشخاص الذين يستخدمونها. تعليم المستخدم يعلم أفضل الممارسات للأشخاص لحماية أنفسهم ضد التهديدات السيبرانية. يحدث التدريب على الأمان أيضًا في المنظمات الكبيرة، حيث يتم تثقيف الموظفين وتحديثهم على سياسات وممارسات الأمان الخاصة بالمنظمة.

يمكن أن يشمل هذا المجال أيضًا تطوير وتدريب المهنيين الجدد في مجال الأمان.

الخاتمة

هناك مجموعة واسعة من الأدوار في الأمن السيبراني التي تختلف في الخبرة الفنية والتدريب المطلوب. هناك أدوار تتقاطع مع الهندسة، أدوار تتقاطع مع التعليم، وأدوار تتقاطع مع الإدارة.

نشجعك على القيام ببحثك بعقل مفتوح.