سياسة أمان الشبكة: تقرير رسمي عن أفضل الممارسات

المحتويات

المقدمة

في غياب سياسة أمان، يمكن أختراق توفر الشبكة. تبدأ هذه السياسة بتقييم الخطر على الشبكة وبناء فريق للاستجابة. ويتطلب إستمرار السياسة تنفيذ ممارسة إدارة التغيير الأمني ورصد الشبكة من أجل الانتهاكات الأمنية. وأخيرا، فإن عملية الاستعراض تعدل السياسة القائمة وتتكيف مع الدروس المستفادة.

وتنقسم هذه الوثيقة إلى ثلاثة مجالات: الإعداد، والوقاية، والاستجابة. لنلقي نظرة على كل خطوة من هذه الخطوات بالتفصيل.

تحضير

قبل تنفيذ سياسة أمان، يجب القيام بما يلي:

- قم بإنشاء عبارات نهج الاستخدام.
- قم بإجراء تحليل للخطر.
- إنشاء هيكله فرق الامن.

إنشاء كشوف نهج الاستخدام

نوصي بإنشاء عبارات سياسات الاستخدام التي تحدد أدوار المستخدمين ومسؤولياتهم فيما يتعلق بالأمان. يمكنك البدء بسياسة عامة تغطي جميع أنظمة الشبكة والبيانات داخل شركتك. وينبغي أن توفر هذه الوثيقة لأوساط المستعملين عموما فهما للسياسة الأمنية، والغرض منها، والمبادئ التوجيهية لتحسين ممارساتها الأمنية، وتعريفات لمسؤولياتها الأمنية. إذا كانت شركتك قد حددت إجراءات محددة يمكن أن تؤدي إلى إجراءات عقابية أو تأديبية ضد موظف، يجب

توضيح هذه الإجراءات وكيفية تجنبها في هذه الوثيقة بشكل واضح.

تتمثل الخطوة التالية في إنشاء بيان إستخدام مقبول للشركاء لتزويد الشركاء بفهم للمعلومات المتوفرة لهم، والتصرف المتوقع في هذه المعلومات، فضلا عن سلوك موظفي شركتك. يجب عليك أن توضح بشكل واضح أي تصرفات معينة تم تحديدها على أنها هجمات أمنية والإجراءات العقابية التي سيتم إتخاذها في حال تم الكشف عن هجوم أمني.

أخيرا، قم بإنشاء بيان إستخدام مقبول للمسؤول لشرح الإجراءات الخاصة بإدارة حساب المستخدم، وإنفاذ السياسة، ومراجعة الامتيازات. إذا كان لدى شركتك سياسات محددة تتعلق بكلمات مرور المستخدم أو المعالجة اللاحقة للبيانات، فقم بعرض هذه السياسات بشكل واضح أيضا. تحقق من السياسة مقابل الاستخدام المقبول من قبل الشريك وبيانات سياسات الاستخدام المقبولة من قبل المستخدم لضمان التوحيد. تأكد من أن متطلبات المسؤول المدرجة في سياسة الاستخدام المقبول تنعكس في خطط التدريب وتقييمات الأداء.

إجراء تحليل للخطر

يجب أن يحدد تحليل المخاطر المخاطر التي تهدد شبكتك وموارد الشبكة والبيانات الخاصة بك. هذا لا يعني أنه يجب عليك تحديد كل نقطة دخول ممكنة إلى الشبكة، ولا كل وسيلة هجوم ممكنة. إن الهدف من تحليل المخاطر هو تحديد أجزاء من شبكتك، وتعيين تصنيف التهديد لكل جزء، وتطبيق مستوى مناسب من الأمان. ويساعد هذا على الحفاظ على توازن عملي بين الأمان والوصول المطلوب إلى الشبكة.

قم بتعيين كل مورد شبكة واحد من مستويات المخاطر الثلاثة التالية:

- لن تؤدي الأنظمة أو البيانات **منخفضة المخاطر** التي إذا تم إختراقها (البيانات التي يتم عرضها بواسطة أفراد غير مصرح لهم أو البيانات التالفة أو فقدان البيانات) إلى تعطيل العمل أو التسبب في حدوث تداعيات قانونية أو مالية. يمكن إستعادة النظام أو البيانات المستهدفة بسهولة، ولا تسمح بمزيد من الوصول إلى الأنظمة الأخرى.
- أنظمة أو بيانات **متوسطة الخطورة** إذا تم الإخلال بها (بيانات تم عرضها بواسطة أفراد غير مصرح لهم، أو بيانات فاسدة، أو بيانات مفقودة) يمكن أن تتسبب في إعاقة متوسطة للأعمال، أو تشعبات قانونية أو مالية بسيطة، أو توفر إمكانية وصول أكبر إلى أنظمة أخرى. النظام أو البيانات المستهدفة تتطلب جهدا معتدلا لاستعادتها أو أن عملية الاستعادة تؤدي إلى تعطيل النظام.
- نظم أو بيانات **عالية الخطورة** إذا تم الإخلال بها (بيانات تم عرضها بواسطة أفراد غير مصرح لهم، أو بيانات فاسدة، أو بيانات مفقودة) فإنها ستسبب إرباكا شديدا في العمل، أو ستتسبب في تشعبات قانونية أو مالية كبيرة، أو ستهدد صحة وسلامة شخص ما. النظام أو البيانات المستهدفة تتطلب جهدا كبيرا للاستعادة أو أن عملية الاستعادة تؤدي إلى تعطيل الأعمال أو الأنظمة الأخرى.

تعيين مستوى مخاطرة لكل مما يلي: أجهزة الشبكة الأساسية وأجهزة شبكة التوزيع وأجهزة شبكة الوصول وأجهزة مراقبة الشبكة (شاشات SNMP ومستكشفات RMON) وأجهزة أمان الشبكة (RADIUS و TACACS) وأنظمة البريد الإلكتروني وخوادم ملفات الشبكة وخوادم طباعة الشبكة وخوادم تطبيقات الشبكة (DNS و DHCP) وخوادم تطبيقات البيانات (Oracle أو التطبيقات المستقلة الأخرى) وأجهزة الكمبيوتر المكتبية والأجهزة الأخرى (خوادم الطباعة المستقلة وأجهزة الفاكس الخاصة بالشبكة).

يمكن أن تسمح أجهزة الشبكة مثل المحولات والموجهات وخوادم DNS وخوادم DHCP بالمزيد من الوصول إلى الشبكة، وبالتالي فهي إما أجهزة متوسطة أو عالية المخاطر. كما يحتمل أن يؤدي تلف هذه المعدات إلى انهيار الشبكة نفسها. إن مثل هذا الفشل من الممكن أن يكون مزعجا للغاية للشركة.

بمجرد تعيين مستوى مخاطرة، من الضروري تحديد أنواع المستخدمين لهذا النظام. أكثر الأنواع الخمسة شيوعا هي:

- **المسؤولون** المستخدمون الداخليون المسؤولون عن موارد الشبكة.
- **المستخدمون** الداخليون **أصحاب الامتيازات** الذين يحتاجون إلى قدر أكبر من الوصول.
- **المستخدمون** الداخليون الذين لديهم حق الوصول العام.
- **الشركاء** المستخدمون الخارجيون الذين يحتاجون إلى الوصول إلى بعض الموارد.
- **مستخدمون** أو عملاء خارجيون **آخرون**.

يشكل تحديد مستوى المخاطر ونوع الوصول المطلوب لكل نظام شبكي الأساس للمصفوفة الأمنية التالية. توفر

المصفوفة الأمنية مرجعا سريعا لكل نظام ونقطة بداية لمزيد من التدابير الأمنية، مثل وضع إستراتيجية مناسبة لتقييد الوصول إلى موارد الشبكة.

النظام	الوصف	مستوى الخطر	أنواع المستخدمين
محولات ATM	جهاز الشبكة الأساسي	عالي	المسؤولون عن تهيئة الأجهزة (موظفو الدعم فقط)، بينما يتم إستخدام جميع البرامج الأخرى كوسيلة نقل
موجهات الشبكة	جهاز شبكة التوزيع	عالي	المسؤولون عن تهيئة الأجهزة (موظفو الدعم فقط)، بينما يتم إستخدام جميع البرامج الأخرى كوسيلة نقل
محولات الخزانة	جهاز شبكة الوصول	الوسيطة	المسؤولون عن تهيئة الأجهزة (موظفو الدعم فقط)، بينما يتم إستخدام جميع البرامج الأخرى كوسيلة نقل
خوادم ISDN أو الطلب الهاتفي	جهاز شبكة الوصول	الوسيطة	المسؤولون عن تكوين الأجهزة

			(فريق الدعم فقط) والشركاء والمستخدمين المتميزين للوصول الخاص
جدار الحماية	جهاز شبكة الوصول	عالي	المسؤولون عن تهيئة الأجهزة (موظفو الدعم فقط)، بينما يتم إستخدام جميع البرامج الأخرى كوسيلة نقل
خوادم DNS و DHCP	تطبيقات الشبكة	الوسيطة	المسؤولون عن التكوين، المستخدمون العامون والمتمتعون بامتيازات الاستخدام
خادم البريد الإلكتروني الخارجي	تطبيق الشبكة	منخفض	المسؤولون عن التكوين، وجميعهم لنقل البريد بين الإنترنت وخادم البريد الداخلي
خادم البريد الإلكتروني الداخلي	تطبيق الشبكة	الوسيطة	المسؤولون عن التكوين، جميع المستخد

			مين الداخليين الآخرين للاستخدام
قاعدة بيانات Oracle	تطبيق الشبكة	متوسطة أو عالية	المسؤولون عن إدارة النظام، المستخدمون المتميزون لتحديثات البيانات، المستخدمون العامون للوصول إلى البيانات، جميع الآخرين للوصول الجزئي للبيانات

إنشاء هيكله فرق الامن

أنشئ فريق أمان متعدد الوظائف بقيادة مدير أمن مع مشاركين من كل منطقة عملياتية لشركتك. ينبغي أن يكون الممثلون في الفريق على دراية بالسياسة الأمنية والجوانب التقنية لتصميم الأمن وتنفيذه. وغالبا ما يتطلب ذلك تدريبا إضافيا لأعضاء الفريق. ويتولى فريق الأمن ثلاثة مجالات من المسؤوليات: وضع السياسات، والممارسة، والاستجابة.

ويركز وضع السياسات على وضع ومراجعة السياسات الأمنية للشركة. على أقل تقدير، قم بمراجعة كل من تحليل المخاطر والسياسة الأمنية على أساس سنوي.

إن مرحلة الممارسة هي المرحلة التي يجري خلالها فريق الأمن تحليل المخاطر، والموافقة على طلبات تغيير الأمن، ومراجعة التنبيهات الأمنية من كلا الموردين وقائمة CERT البريدية، وتحويل متطلبات سياسة الأمن باللغات العادية إلى تطبيقات تقنية محددة.

آخر مجال للمسؤولية هو الإستجابة. بينما تحدد مراقبة الشبكة عادة انتهاك أمان، فإن أعضاء فريق الأمان هم الذين يقومون باستكشاف الأخطاء وإصلاحها وإصلاحها بشكل فعلي وتثبيت هذا الانتهاك. يتعين على كل عضو من أعضاء فريق الأمن أن يعرف بشكل مفصل الخصائص الأمنية التي توفرها المعدات في منطقته العملياتية.

في حين أننا حددنا مسؤوليات الفريق ككل، يجب عليك تحديد الأدوار والمسؤوليات الفردية لأعضاء فريق الأمن في سياستك الأمنية.

منع

يمكن تقسيم عملية الوقاية إلى قسمين: الموافقة على تغييرات الأمان ومراقبة أمان الشبكة.

الموافقة على التغييرات الأمنية

يتم تعريف التغييرات الأمنية على أنها تغييرات على أجهزة الشبكة التي يمكن أن يكون لها تأثير على الأمان الإجمالي للشبكة. يجب أن تحدد سياسة الأمان الخاصة بك متطلبات تكوين الأمان المحددة بعبارات غير فنية. بمعنى آخر، بدلا من تعريف متطلب على أنه "لن يتم السماح باتصالات FTP لمصادر خارجية من خلال جدار الحماية"، قم بتعريف المتطلب على أنه "يجب ألا تكون الاتصالات الخارجية قادرة على إسترداد الملفات من الشبكة الداخلية". ستحتاج إلى تحديد مجموعة فريدة من المتطلبات لمؤسستك.

يجب أن يراجع فريق الأمان قائمة متطلبات اللغة العادية لتحديد تكوين شبكة معينة أو مشاكل تصميم تلبي المتطلبات. بمجرد أن يقوم الفريق بإنشاء تغييرات تكوين الشبكة المطلوبة لتنفيذ سياسة الأمان، يمكنك تطبيق هذه التغييرات على أي تغييرات تكوين مستقبلية. في حين أنه من الممكن أن يراجع فريق الأمن جميع التغييرات، إلا أن هذه العملية تسمح لهم فقط بمراجعة التغييرات التي تشكل خطرا كافيا لتبرير المعاملة الخاصة.

نوصي بأن يقوم فريق الأمان بمراجعة أنواع التغييرات التالية:

- أي تغيير على تكوين جدار الحماية.
- أي تغيير على قوائم التحكم في الوصول (ACL).
- أي تغيير على تكوين بروتوكول إدارة الشبكات البسيط (SNMP).
- أي تغيير أو تحديث في البرامج يختلف عن قائمة مستوى مراجعة البرامج المعتمدة.

كما نوصي بالالتزام بالمبادئ التوجيهية التالية:

- قم بتغيير كلمات المرور إلى أجهزة الشبكة على أساس روتيني.
- تقييد الوصول إلى أجهزة الشبكة بقائمة معتمدة من الموظفين.
- تأكد من أن مستويات مراجعة البرامج الحالية لمعدات الشبكة وبيئات الخادم تتوافق مع متطلبات تكوين الأمان.

إضافة إلى هذه المبادئ التوجيهية للموافقة، إجعل ممثلا من فريق الأمن يجلس في مجلس إدارة الموافقة على التغيير، من أجل مراقبة جميع التغييرات التي يستعرضها المجلس. يمكن لممثل فريق الأمن أن ينكر أي تغيير يعتبر تغييرا أمنيا إلى أن يوافق عليه فريق الأمن.

مراقبة أمان الشبكة

تعد مراقبة الأمان مماثلة لمراقبة الشبكة، باستثناء أنها تركز على اكتشاف التغييرات في الشبكة التي تشير إلى انتهاك أمان. وتتمثل نقطة البداية لرصد الأمن في تحديد ما هو الانتهاك. وفي إجراء تحليل للمخاطر، حددنا مستوى الرصد المطلوب استنادا إلى التهديد الذي يتعرض له النظام. عند الموافقة على التغييرات الأمنية، حددنا تهديدات محددة للشبكة. من خلال النظر إلى هذين المعيارين، سنطور صورة واضحة لما تحتاج إلى مراقبته وعدد المرات التي تحتاج فيها.

في مصفوفة تحليل المخاطر، يعتبر جدار الحماية جهاز شبكة عالي الخطورة، مما يشير إلى أنه يجب عليك مراقبته في الوقت الفعلي. من قسم الموافقة على تغييرات الأمان، ترى أنه يجب عليك المراقبة لأي تغييرات تطرأ على جدار الحماية. هذا يعني أنه يجب على وكيل اقتراع SNMP مراقبة أشياء مثل محاولات تسجيل الدخول الفاشلة، حركة المرور غير العادية، التغييرات في جدار الحماية، الوصول الممنوح لجدار الحماية، وإعداد الاتصالات من خلال جدار الحماية.

وباتباع هذا المثال، قم بإنشاء سياسة مراقبة لكل مجال تم تحديده في تحليل المخاطر الخاص بك. نوصي بمراقبة المعدات ذات الخطورة المنخفضة كل أسبوع، والمعدات ذات الخطورة المتوسطة يوميا، والمعدات ذات الخطورة العالية كل ساعة. إذا كنت بحاجة إلى اكتشاف أكثر سرعة، فعليك المراقبة على إطار زمني أقل.

وأخيرا، يجب أن تتطرق سياسة الأمان الخاصة بك إلى كيفية إعلام فريق الأمان بالانتهاكات الأمنية. وغالبا ما يكون برنامج مراقبة الشبكة هو أول من يكتشف الانتهاك. يجب أن تقوم بتشغيل إخطار لمركز العمليات، والذي بدوره يجب أن يقوم بإبلاغ فريق الأمن، باستخدام جهاز النداء إذا لزم الأمر.

إستجابة

يمكن تقسيم الاستجابة إلى ثلاثة أجزاء: الانتهاكات الأمنية، والترميم، والمراجعة.

المخالفات الامنيه

وعندما يتم اكتشاف انتهاك، فإن القدرة على حماية معدات الشبكة وتحديد مدى التطفل واستعادة العمليات العادية تعتمد على قرارات سريعة. إن إتخاذ هذه القرارات قبل أوانها يجعل الاستجابة لأي تطفل أمرا أكثر سهولة.

والإجراء الأول الذي يلي اكتشاف إقتحام هو إخطار فريق الأمن. وبدون وجود إجراء، سيكون هناك تأخير كبير في جعل الأشخاص الصحيحين يطبقون الاستجابة الصحيحة. حدد أحد الإجراءات في سياسة الأمان المتوفرة على مدار 24 ساعة طوال أيام الأسبوع.

بعد ذلك يجب عليك تحديد مستوى السلطة الممنوحة لفريق الأمان لإجراء التغييرات وبأي ترتيب يجب إجراء التغييرات. الإجراءات التصحيحية المحتملة هي:

- تنفيذ التغييرات لمنع المزيد من الوصول إلى الانتهاك.
- عزل الأنظمة التي تم إنتهاكها.
- الاتصال بالناقل أو مزود خدمة الإنترنت (ISP) في محاولة لتعقب الهجوم.
- إستعمال أجهزه التسجيل لجمع الادله.
- قطع اتصال الأنظمة المخالفة أو مصدر الانتهاك.
- الإتصال بالشرطة، أو الوكالات الحكومية الأخرى.
- إغلاق الأنظمة المخالفة.
- إستعادة الأنظمة وفقا لقائمة ذات أولوية.
- أخطار الموظفين الاداريين والقانونيين الداخليين.

تأكد من تفصيل أي تغييرات يمكن إجراؤها دون موافقة الإدارة في نهج الأمان.

وأخيرا، هناك سببان لجمع المعلومات والاحتفاظ بها أثناء هجوم أمني: تحديد مدى إخلال هجوم أمني بالنظم، ومقاضاة مرتكبي انتهاكات خارجية. يختلف نوع المعلومات وطريقة جمعها وفقا لهدفك.

تحدد مدي المخالفه والقيام بما يلي:

- قم بتسجيل الحدث عن طريق الحصول على آثار sniffer للشبكة ونسخ من ملفات السجل وحسابات المستخدم النشطة واتصالات الشبكة.
- الحد من الاختراق الإضافي من خلال تعطيل الحسابات وفصل أجهزة الشبكة عن الشبكة وفصل الاتصال عن الإنترنت.
- قم بإجراء نسخ إحتياطي للنظام المتضرر للمساعدة في تحليل مفصل للأضرار وطريقة الهجوم.
- ابحث عن علامات أخرى للتسوية. عادة ما يكون هناك أنظمة أو حسابات أخرى معنية عند تعرض نظام ما للخطر.
- الاحتفاظ بملفات سجل أجهزة الأمان وملفات سجل مراقبة الشبكة ومراجعتها، لأنها غالبا ما توفر أدلة لطريقة الهجوم.

إذا كنت مهتما باتخاذ إجراءات قانونية، اطلب من القسم القانوني مراجعة إجراءات جمع الأدلة ومشاركة السلطات. ويزيد هذا الاستعراض من فعالية الأدلة في الإجراءات القانونية. إذا كان الانتهاك داخليا في طبيعته، فاتصل بقسم الموارد البشرية.

ترميم

إستعادة عمليات الشبكة العادية هو الهدف النهائي لأي إستجابة لانتهاك الأمان. حدد في نهج الأمان كيفية إجراء النسخ الاحتياطية العادية وتأمينها وتوفيرها. وبما أن لكل نظام وسائله وإجراءاته الخاصة للنسخ الاحتياطي، ينبغي أن تكون السياسة الأمنية بمثابة سياسة شاملة، تفصل لكل نظام الشروط الأمنية التي تتطلب الاستعادة من النسخ الاحتياطي. إذا

كانت الموافقة مطلوبة قبل تنفيذ الاستعادة، فقم بتضمين عملية الحصول على الموافقة أيضا.

مراجعة

إن عملية المراجعة هي المجهود الأخير في إنشاء وصيانة سياسة أمنية. هناك ثلاثة أمور ستحتاج لمراجعتها: السياسة والوضع والممارسة.

وينبغي أن تكون سياسة الأمن وثيقة حية تتكيف مع بيئة دائمة التغير. يؤدي إستعراض السياسة الحالية مقابل أفضل الممارسات المعروفة إلى تحديث الشبكة باستمرار. وأيضا، راجع موقع CERT على الويب للحصول على نصائح مفيدة وممارسات وتحسينات أمنية وتنبيهات يمكن تضمينها في سياسة الأمان الخاصة بك.

يجب عليك أيضا مراجعة وضع الشبكة مقارنة بوضع الأمان المطلوب. يمكن للشركة الخارجية المتخصصة في الأمان أن تحاول أختراق الشبكة واختبار ليس فقط وضع الشبكة، ولكن أيضا الاستجابة الأمنية لمؤسستك. بالنسبة للشبكات عالية التوفر، نوصي بإجراء مثل هذا الاختبار سنويا.

وأخيرا، تعرف الممارسة بأنها إختبار أو تمرين لموظفي الدعم للتأكد من أنهم يتمتعون بفهم واضح لما ينبغي القيام به أثناء وقوع انتهاك أمني. عادة، لا يتم الإعلان عن هذا التدريب من قبل الإدارة ويتم تنفيذه بالاقتران مع إختبار وضعية الشبكة. ويحدد هذا الاستعراض الثغرات في الإجراءات وتدريب الموظفين بحيث يمكن إتخاذ إجراءات تصحيحية.

معلومات ذات صلة

- المزيد من التقارير الرسمية حول أفضل الممارسات
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).