المركز الوطني
للأمن السيبراني
National Cyber
Security Center

تصنيف وحماية الأصول

المحـاور

- مفهوم الأصول وأهميتها
- أنواع الأصول وفئاتها ومميزاتها
- مبادئ تصنيف الأصول
- الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

مفهوم الأصـول وأهميتها

ما هي الأصول؟

- الأصل هو كل ما يملك قيمة للجهة ويدعم أهدافها.
- يمكن أن تكون الأصول ملموسة أو غير ملموسة.
- من الأمثلة على الأصول: البيانات، والمعلومات، والأنظمة، والأجهزة، والشبكات، والأفراد، والعمليات، والسمعة.

مفهوم الأصـول وأهميتها

لماذا تعتبر تصنيف الأصول وحمايتها مهمة؟

تعتبر تصنيف الأصول وحمايتها مهمة لأنها تساعدك على:

- فهم قيمة وحساسية أصولك والمخاطر التي تواجهها.
- تحديد أولويات مواردك وجهودك لحماية الأصول الأكثر أهمية وعرضة للخطر.
- الامتثال للمتطلبات القانونية والتنظيمية والمعايير المتعلقة بأمن الأصول.
- تعزيز الثقة لدى العملاء والشركاء وأصحاب المصلحة.

أنواع الأصول وفئاتها ومميزاتها

- يمكن تصنيف الأصول إلى أنواع وفئات مختلفة استنادًا إلى خصائصها وسماتها.
- بعض الأنواع الشائعة للأصول هي:

البيانات:

هي الحقائق والأرقام الخام التي تُجمع وتُخزن وتُعالج وتُرسل من قبل المؤسسة أو الجهة.

المعلومات:

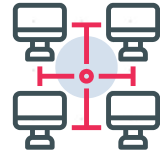
هي البيانات المعالجة ذات القيمة والمعنى للمؤسسة أو الجهة.

الأنظمة:

هي الأجهزة الأساسية والبرمجيات والبرامج الثابتة التي تمكننا من إنشاء البيانات وتخزينها ومعالجتها وإرسالها.

أنواع الأصول وفئاتها ومميزاتها

أنواع وفئات الأصول:



الأجهزة:
هي المعدات الفعلية والمكونات التي تدعم عمل الأنظمة والشبكات.

الشبكات:
هي البنية التحتية والبروتوكولات التي تربط الأجهزة والأنظمة وتمكننا من التواصل وتبادل البيانات.

الأفراد:
هم الموارد البشرية والشخصيات المشاركة في إنشاء وإدارة واستخدام الأصول.

العمليات:
هي إجراءات وخطوات سير العمل التي تحدد كيفية إنشاء وإدارة واستخدام الأصول.

السمعة:
هي الصورة والانطباع الخاص بالمؤسسة أو الجهة لدى العملاء و الشركاء وأصحاب المصلحة.

مبـادئ تصنيف الأصـول

تصنيف الأصول هو عملية تعيين مستوى الحساسية والأهمية للأصول استنادًا إلى قيمتها وتأثيرها على المؤسسة أو الجهة لتحديد المستوى المناسب من الحماية والضوابط الأمنية التي يجب اتباعها لحماية تلك الأصول.

لماذا تعتبر تصنيف الأصول وحمايتها مهمة؟

- **السرية:** هي الدرجة التي يجب أن تحمى فيها أصولك من الوصول غير المصرح به أو الكشف أو الاستخدام.
- **النزاهة:** هي الدرجة التي يجب أن تحمى فيها أصولك من التعديل غير المصرح به أو التغيير أو الحذف.
- **التوفر:** هو الدرجة التي تحتاج فيها أصولك إلى أن تكون متاحة وقابلة للاستخدام من قبل المستخدمين المصرح لهم عند الحاجة.

مبـادئ تصنيف الأصـول

أساليب تصنيف الأصول:

- تعتمد على نوع وفئة أصولك والمعايير والإطارات التي تتبعها.
- بعض الأساليب الشائعة هي:

تصنيف البيانات:
عملية تعيين حساسية بياناتك استنادًا إلى نوعها ومحتواها وسياقها والتأثير المحتمل لفقدانها أو اختراقها.

تصنيف المعلومات:
عملية تعيين حساسية معلوماتك استنادًا إلى هدفها واستخدامها والجمهور المستهدف والتأثير المحتمل لفقدانها أو اختراقها.

مبـادئ تصنيف الأصـول

أساليب تصنيف الأصول:

تصنيف الأنظمة:
عملية تعيين الأهمية لأنظمتك استنادًا إلى وظيفتها وأدائها واعتمادها والتأثير المحتمل لفشلها أو اضطرابها.

تصنيف الأجهزة:
عملية تعيين الأهمية لأجهزتك استنادًا إلى موقعها وملكيتها وتكوينها والتأثير المحتمل لفقدانها أو تلفها.

تصنيف الشبكات:
عملية تعيين الأهمية لشبكاتك استنادًا إلى توبولوجيا الشبكة وهندستها واتصالاتها والتأثير المحتمل لفشلها أو اضطرابها.

مبـادئ تصنيف الأصـول

مستويات تصنيف الأصول:

- تعتبـر مسـتويات تصـنيف الأصـول علامـات تشـير إلـى مسـتوى الحساسية والأهمية لأصولك.
- تساعدك في فرض متطلبات وضوابط لتأمين أصولك.
- تختلف حسب نوع وفئة أصولك والمعايير والأطر التي تتبعها.

مبـادئ تصنيف الأصـول

مستويات تصنيف الأصول:

بعض مستويات تصنيف الأصول الشائعة هي:

عام: أدنى مستوى من الحساسية أو الأهمية، مما يشير إلى أن الأصل مخصص للوصول العام وليس له تأثير أو له تأثير ضئيل على مؤسستك في حالة الفقدان أو الاختراق.

سري: مستوى عالٍ من الحساسية أو الأهمية و يشير إلى أن الأصل مخصص للوصول المحدود ويؤثر بشكل كبير على مؤسستك في حالة الفقدان أو الاختراق.

داخلي: مستوى متوسط من الحساسية أو الأهمية و يشير إلى أن الأصل مخصص للاستخدام الداخلي فقط وله بعض التأثير على مؤسستك في حالة الفقدان أو الاختراق.

سري جدًا: أعلى مستوى من الحساسية أو الأهمية و يشير إلى أن الأصل مخصص للوصول القليل جدًا ويؤثر بشكل كبير على مؤسستك في حالة الفقدان أو الاختراق.

مبـادئ تصنيف الأصـول

عملية تصنيف الأصول:

- تعتبر عملية تصنيف الأصول عملية مستمرة تتطلب مراجعة وتحديثات منتظمة لضمان تحديد الأصول وحمايتها بشكل صحيح.
- تشمل عملية تصنيف الأصول عادة الخطوات التالية:

تحديد الأصول:
الخطوة الأولى هي تحديد وجرد جميع الأصول التي تمتلكها مؤسستك أو تستخدمها وجميع خصائصها وسماتها.

تقدير قيمة الأصول:
الخطوة الثانية هي تقييم وتحديد قيمة الأصول وتأثيرها على مؤسستك وعلى أهدافها.

مبـادئ تصنيف الأصـول

عملية تصنيف الأصول:

تصنيف الأصول:

الخطوة الثالثة هي تعيين الحساسية والأهمية لأصولك استنادًا إلى قيمتها وتأثيرها ومبادئ السرية والنزاهة والتوفر.

تسمية الأصول:

الخطوة الرابعة هي تسمية أو وضع علامات على أصولك بالمستوى المناسب للتصنيف واعلام أصحاب المصلحة ذوي الصلة بهذه العلامات.

حماية الأصول:

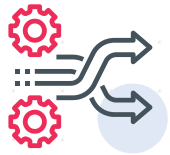
الخطوة الخامسة هي تنفيذ وفرض الضوابط والتدابير الأمنية المناسبة لأصولك استنادًا إلى مستوى التصنيف ومتطلبات الأمان والمعايير التي تتبعها.

مبادئ تصنيف الأصول

تحديات تصنيف الأصول:

التعقيد:

تعقيد الأصول والبيئة التي تعمل فيها قد يجعل من الصعب تحديدها وتصنيفها بدقة واستمرارية.



التغيير:

التغيير في الأصول والبيئة التي تعمل فيها قد يجعل من الصعب الحفاظ على تحديث وتصنيف الأصول وجعلها ذات صلة.

الاتساق:

انتشار تصنيف الأصول بين مختلف أنواع الأصول والفئات الأخرى والكيانات وأصحاب المصلحة قد يجعل من الصعب ضمان فهم مشترك واتفاق حول مستويات تصنيف الأصول وآثارها.

الامتثال:

الامتثال لمتطلبات القوانين واللوائح والمعايير لأمان الأصول قد يجعل من الصعب تحقيق التوازن بين احتياجات الأمن للمؤسسة واحتياجات الأعمال.

الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

مبادئ حماية الأصول:

- **حماية الأصول** هي تنفيذ وفرض الضوابط والتدابير الأمنية المناسبة لأصولك استنادًا إلى مستوى التصنيف ومتطلبات الأمان والمعايير التي تتبعها.
- تساعد حماية الأصول على تقليل مخاطر فقدان أو تعرض أصولك للسرقة أو الاختراق وتضمن سرية ونزاهة وتوفرها.

الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

مبادئ حماية الأصول:

الوقاية:
مبدأ منع أو ردع التهديدات المحتملة من الوصول إلى أصولك أو إلحاق الضرر بها.

الكشف:
مبدأ الكشف أو التعرف على التهديدات المحتملة التي وصلت إلى أصولك أو ألحقت بها الضرر.

الاستجابة:
مبدأ الاستجابة أو التفاعل مع التهديدات المحتملة التي وصلت إلى أصولك أو ألحقت بها الضرر.

الاستعادة:
مبدأ استعادة أصولك إلى حالتها الطبيعية بعد حدوث حادث أمني.

الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

أساليب حماية الأصول:

- التشفير: تحويل بياناتك ومعلوماتك إلى شكل غير قابل للقراءة حيث يمكن فقط للأطراف المصرح بهم الوصول إليه أو فك تشفيره.
- المصادقة: طريقة التحقق من هوية مستخدم يحاول الوصول إلى أصولك أو استخدامها.
- التفويض: طريقة منح أو رفض حقوق الوصول أو الاستخدام لأصولك استنادًا إلى هوية المستخدم أو النظام والدور.
- جدار الحماية: طريقة تصفية أو حجب حركة مرور البيانات عبر الشبكة و التي تحاول الدخول إلى شبكتك أو مغادرتها استنادًا إلى قواعد وسياسات محددة مسبقًا.
- برنامج مكافحة الفيروسات: فحص وإزالة البرمجيات الخبيثة أو الكود الضار الذي قد يصيب أو يتلف نظامك أو جهازك.
- النسخ الاحتياطي: إنشاء نسخ احتياطية وتخزينها من أصولك في موقع أو وسيلة منفصلة يمكن استخدامها لاستعادتها في حالة الفقدان أو التلف.

الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

مستويات حماية الأصول:

- مستويات حماية الأصول هي التدابير الأمنية التي يتم تنفيذها وفرضها على أصولك استنادًا إلى مستوى تصنيفها ومتطلبات الأمان والمعايير التي تتبعها.
- تساعد مستويات حماية الأصول على ضمان حماية أصولك بشكل كافٍ وضمان أن التدابير الأمنية متناسبة مع المخاطر والتأثيرات المرتبطة بالأصول.
- قد تختلف مستويات حماية الأصول اعتمادًا على نوع وفئة الأصول الخاصة بك والمعايير والأطر التي تتبعها.

الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

مستويات حماية الأصول:

- **الأساسية:** أدنى مستوى من الحماية، مشيرًا إلى أن الأصل لديه قيمة أو تأثير أدنى ويواجه خطرًا منخفضًا من الفقدان أو التعرض. قد تتضمن التدابير الأمنية الأدنى تدابير بسيطة كحماية كلمة المرور، و تفعيل جدار الحماية.

- **المتوسطة:** مستوى متوسط من الحماية، مشيرًا إلى أن الأصل لديه بعض القيمة أو التأثير ويواجه خطرًا معقولًا من الفقدان أو التعرض. قد تتضمن التدابير الأمنية مستوى حماية أقوى، مثل استخدام مصادقة متعددة العوامل، وتقسيم الشبكة.

- **المتقدمة:** أعلى مستوى من الحماية، مشيرًا إلى أن الأصل لديه قيمة أو تأثير عالي ويواجه خطرًا متزايدًا من الفقدان أو التعرض. قد تشمل التدابير الأمنية الشاملة تدابير مُحكمة لحماية الأصول، مثل المصادقة الحيوية (بصمة الاصبع, بصمة العين ... الخ)، وأنظمة كشف ومنع الاختراق.

الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

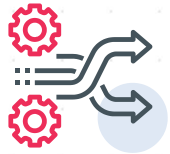
عملية حماية الأصول:

- تقييم المخاطر: الخطوة الأولى هي تحديد وتقييم المخاطر التي تواجه أصولك والتأثير المحتمل لهذه المخاطر على مؤسستك.
- التخطيط: الخطوة الثانية هي وضع وتنفيذ خطة أمنية توضح التدابير الأمنية لأصولك استنادًا إلى مستوى تصنيفها ونتائج تقييم المخاطر.
- التنفيذ: الخطوة الثالثة هي تثبيت و تطبيق التدابير الأمنية لأصولك وفقًا للخطة الأمنية.
- المراقبة: الخطوة الرابعة هي مراقبة وتحليل حالة أمان أصولك لاكتشاف التهديدات أو الحوادث المحتملة.
- الاستجابة: الخطوة الخامسة هي الاستجابة والاستعادة من أي حوادث أمنية تؤثر على أصولك والتعلم والتحسين من هذه الحوادث.

الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

تحديات حماية الأصول:

التعقيد:
تعقيد الأصول والبيئة التي تعمل فيها قد يجعل من الصعب حمايتها بشكل فعال وفعّال.



التغيير:
التغيير في الأصول والبيئة التي تعمل فيها قد يجعل من الصعب الحفاظ على حماية الأصول محدثة وملائمة.

الاتساق:
انعدام الاتساق في حماية الأصول عبر مختلف أنواع الأصول والفئات المختلفة والكيانات وأصحاب المصلحة قد يجعل من الصعب ضمان فهم مشترك واتفاق حول مستوبات حماية الأصول وتداعياتها.

الامتثال:
الامتثال للمتطلبات والمعايير القانونية والتنظيمية لأمان الأصول قد يجعل من الصعب تحقيق التوازن بين احتياجات الأمان للمؤسسة واحتياجات الأعمال.

الضوابط الأمنية والإجراءات المناسبة لحماية الأصول

معايير تصنيف وحماية الأصول:

- ISO/IEC 27001 : هو معيار دولي يوفر إطارًا لإنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمان المعلومات (ISMS)
- NIST SP 800-53 : هو معيار فدرالي أمريكي يوفر فهرسًا لضوابط الأمان والخصوصية لجميع أنظمة المعلومات الفيدرالية الأمريكية باستثناء تلك المتعلقة بالأمن القومي.
- CIS Controls : مجموعة من 20 من الضوابط الأمنية الحرجة التي توفر خارطة طريق لتحسين موقف الأمن السيبراني وتقليل مخاطر التهديدات السيبرانية.

نتمنى لكم السلامة في

العالم الرقمي.