وزارة الاتصالات وتقنية المعلومات

السياسات العامة لأمن المعلومات

في الجهات الحكومية

إعداد:
م/ صـــادق الصوفي

8

سياسة إدارة التحكم بالنفاذ والدخول

سياسة إدارة التحكم بالنفاذ والدخول

سياسة إدارة التحكم بالنفاذ والدخول

بنود السياسة

يجب أن تتضمن خطة أمن المعلومات لجهة حكومية ما يلي:

- تحديد حقوق الوصول إلى البيانات تحديداً واضحاً ويتم مراجعتها بشكل دوري.
- آليات واضحة للتحكم في النفاذ إلى أنظمة المعلومات وأصول المعلومات.
- التحقق من هوية المصرح لهم بالنفاذ إلى أنظمة المعلومات أو المرافق المستخدمة في معالجة المعلومات بما يتوافق مع متطلبات العمل.
- يجب مراقبة محاولات الدخول المتتابعة وغير الناجحة.
- المراجعة الدورية لملفات النفاذ إلى أنظمة المعلومات والمرافق وإلغاء الصلاحيات التي لم تعد لازمة لمتطلبات العمل، مع ضرورة إبلاغ المستخدمين بالتزاماتهم ومسؤولياتهم تجاه أمن المعلومات.

سياسة إدارة التحكم بالنفاذ والدخول

بنود السياسة

- التأكد من وضع وتنفيذ سياسات تتعلق بالنفاذ والدخول لمعلومات وخدمات الجهة الحكومية من خارج أماكن العمل الرسمية.
- التأكد من وضع وتنفيذ سياسات تتعلق بضوابط وأمن النفاذ من خلال الأجهزة الإلكترونية المحمولة) أجهزة اللابتوب المحمولة، هواتف ذكية، وغيرها).
- التأكد من وضع ضوابط فنية لمنع وتقييد ربط وتوصيل أي طرفيات أو أقراص صلبة قابلة للإزالة أو نحوها من وسائل تخزين محمولة ومتنقلة مالم تكن تلك الطرفيات أو الوسائل مسموحة من قبل إدارة / قسم أمن المعلومات بالجهة مع وجود القدرة للأنظمة على تسجل الأحداث مع هوية الطرفية ونوع العملية التي تمت منها واليها ووقتها .
- تحتفظ الجهة الحكومية بحقها بفحص جميع المعلومات المخزنة أو المرسلة عبر أنظمة المعلومات الحكومية مع مراعاة قوانين الخصوصية .

سياسة إدارة التحكم بالنفاذ والدخول

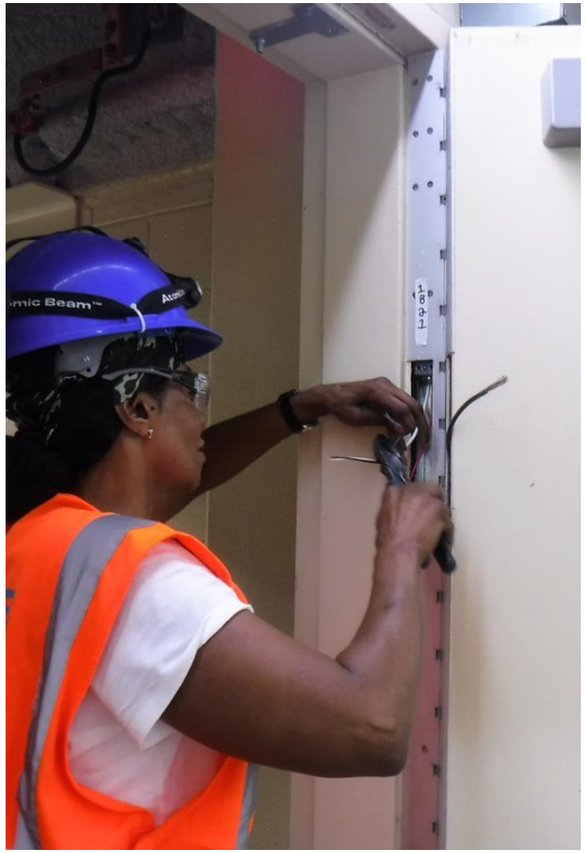
بنود السياسة

- يجب على الجهة الحكومية تحديد سياسات صارمة لكلمة المرور كتحديد الحد الأدنى لطول هذه الكلمة، طبيعة اختيار الكلمات، مدة استخدام الكلمة، بالإضافة إلى وجود إرشادات توضح كيفية اختيارها، وكذلك منع مشاركة كلمات المرور بين الموظفين أو إفشاء سريتها إلا عند الضرورة القصوى وبشكل موثق .
- عند تخزين كلمات المرور يجب حمايتها ويجب تشفير كلمات المرور عند انتقالها خلال وسائل اتصال غير موثوقة.
- يجب تغيير جميع كلمات المرور الافتراضية لأي نظام من نظم المعلومات عند تشغيله واستخدامه بشكل رسمي ومن اللحظات الأولى.
- يجب تغير كلمات المرور بصورة دورية تفادياً لأي اختراق قد يحدث وحفاظاً على سرية المعلومات أو عند الاشتباه بأنها مخترقة أو عند الكشف عنها للفنيين من أجل الصيانة والدعم الفني.

بنود السياسة

- يمنع إضافة أي قسم أو شخص لأي نظام معلومات إلا بموافقة مسبقة من إدارة الجهة الحكومية وإدارة نظم/تقنية المعلومات فيها مع مراعاة المحافظة على مستوى مناسب من أمن المعلومات.
- يجب وضع آلية وإجراءات لتوثيق وتسجيل أنشطة نظم المعلومات التابع للجهة الحكومية وفقاً لاحتياجات العمل وتصنيف البيانات، وأن يتم الاحتفاظ بسجلات التوثيق وسجلات الاحداث والانشطة لفترة تتناسب مع استعمالها كأداة لمراجعة الأحداث.
- يجب وضع سياسات للتعامل مع السجلات تضمن الاحتفاظ بكافة سجلات الأحداث سليمة ومكتملة بكافة تصنيفاتها وعلى كافة المستويات ولكافة العمليات ولمدة زمنية مناسبة.

مقدمة :



- تعتبر سياسة التحكم بالنفاذ والدخول (Access Control Policy) أحد أهم الأساسيات في أي نظام معلوماتي. حيث انها هي مجموعة من القواعد والإجراءات التي تحدد كيفية الوصول إلى الموارد المعلوماتية شاملاً جميع المعلومات والأنظمة والشبكات والأجهزة في الجهة ومن يمكنه الوصول إليها ، وكيف يتم ذلك، ومتى يتم ذلك.
- وتهدف هذه السياسة إلى حماية الموارد المعلوماتية من الوصول غير المصرح به، ومنع الاستخدام غير المصرح به للموارد المعلوماتية.
- كما تهدف هذه السياسة إلى ضمان أن يتم منح الوصول إلى الموارد المعلوماتية فقط للأشخاص المصرح لهم وفقًا للاحتياجات الوظيفية وتقديم الحماية اللازمة لها. على أن يتم تسجيل جميع عمليات الوصول إلى الموارد المعلوماتية في الجهة.

سياسة إدارة التحكم بالنفاذ والدخول

النطاق:

- تنطبق هذه السياسة على جميع المعلومات والأنظمة والشبكات والأجهزة التابعة للجهة.
- تنطبق هذه السياسة على جميع الموظفين والمستخدمين الخارجيين الذين لديهم وصول إلى المعلومات والأنظمة والشبكات التابعة للجهة.

الأهداف

1 تعزيز الأمان

- زيادة مستوى الأمان في الجهة وتقليل مخاطر الاختراق والتلاعب.

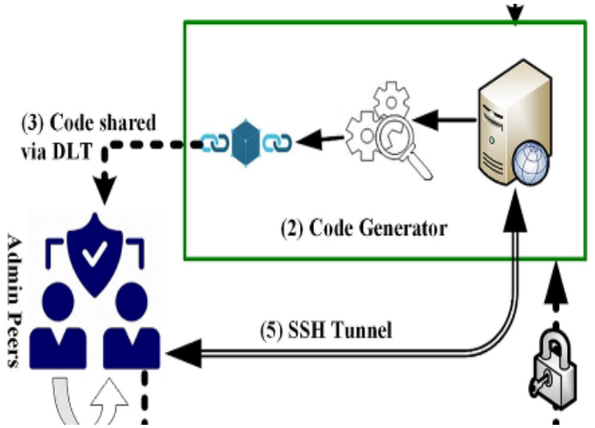
2 حماية المعلومات الحساسة

- ضمان سلامة المعلومات الحساسة والحفاظ على خصوصيتها من الوصول غير المصرح به.

3 ضبط الوصول

- تحديد الصلاحيات المناسبة لكل مستخدم وفقًا لدوره ومسؤولياته.

اهم إجراءات منع الوصول غير المصرح به

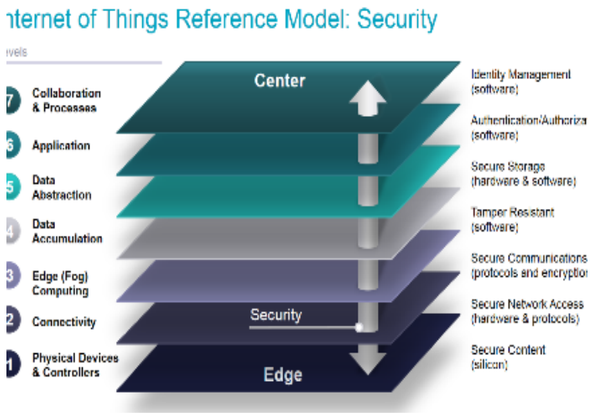


تطبيق طرق المصادقة

تطبيق أساليب موثوقة للمصادقة مثل تعقيد كلمات المرور والمصادقة متعددة العوامل (MFA) والبصمة وبطاقات الوصول للتحقق من هوية المستخدمين.
ضبط وإعداد كلمات مرور التشغيل لنظام BIOS.

التحكم في الوصول الفعلي

تنفيذ نظام يضمن أن الأشخاص فقط الذين لديهم الصلاحية يمكنهم الوصول إلى المناطق المحمية.



حماية الشبكة

تأكيد حماية الشبكة والأنظمة من الوصول غير المصرح به.

سياسة إدارة التحكم بالنفاذ والدخول

ضوابط إدارة التحكم بالنفاذ والدخول

حماية المعلومات

- تشفير الملفات الحساسة.
- إعداد وتنفيذ أنظمة جدار الحماية وأنظمة كشف ومنع التسلل IPS/IDS
- تثبيت برامج مكافحة الفيروسات.
- تحديث بشكل منتظم الأنظمة الأمنية
- إلغاء أو إعادة تسمية الحسابات الإفتراضية أو غير التفاعلية أو غير اللازمة.
- تطبيق مبدأ الحد الأدنى من الصلاحيات والإمتيازات

المراقبة

- تثبيت أنظمة المراقبة عبر الفيديو
- تحليل سجلات النشاط.
- إعداد تقارير أمان دورية.
- الإبلاغ عن الحوادث الأمنية

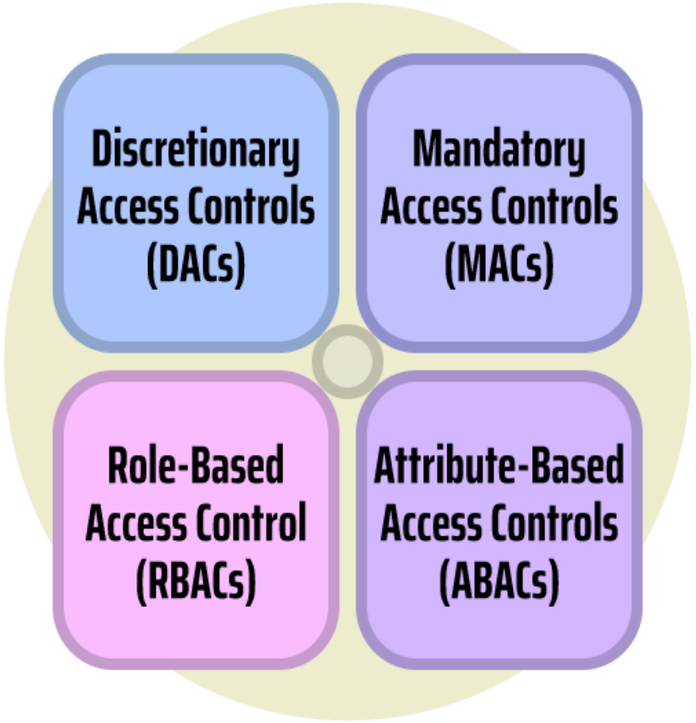
التوعية

- تقديم تدريبات أمن المعلومات للموظفين.
- توزيع مواد توعية بالأمان.
- إعداد سياسات وإرشادات واضحة.

تطبيق إجراءات متعددة لتحقيق اهداف الامان CIA

سياسة إدارة التحكم بالنفاذ والدخول

نماذج التحكم في النفاذ الأربعة :



- تقييد الوصول إلى أجهزة المستخدمين وحصره على حساب المستخدم فقط.
- تطبيق مبدأ الحد الأدنى من الصلاحيات والإمتيازات للمستخدمين فقط.
- التحكم بالوصول التقديري Discretionary Access Control (DAC)
- التحكم بالوصول الإلزامي Mandatory Access Control (MAC)
- التحكم في الوصول استناداً إلى الدور Role-Based Access Control (RBAC)
- التحكم في الوصول القائم على الخصائص attribute-based access control (ABAC)

تنقسم طرق التحكم بالنفاذ الى فئتين رئيسيتين :

1- طرق التحكم بالنفاذ المادية physical access control

2- طرق التحكم بالنفاذ المنطقية logical access control

تشمل طرق التحكم بالنفاذ المنطقية :

- 1- قوائم التحكم بالنفاذ Access Control Lists (ACLs)
- سياسات المجموعة Group Policies
- قيود الحساب Account Restrictions
- كلمات المرور Passwords

تشمل طرق التحكم بالنفاذ المادية :

- بوابات الوصول (Access Gates)
- بطاقات الوصول (Access Cards)
- أنظمة الكشف عن الحركة (Motion Detection)
- أنظمة الإنذار (Alarm Systems)
- كاميرات المراقبة (Cameras Surveillance)

الأدوار والمسئوليات

❖ مسئوليات مهندسي الشبكات والسيرفرات:

- حماية السيرفرات والمعدات الإلكترونية من الهجمات المادية
- إدارة صلاحيات الوصول
- استخدام تقنيات الأمان، مثل جدار الحماية ومكافحة الفيروسات، لحماية الأنظمة والشبكات.
- ضرورة تسجيل الأحداث وتحليلها لاكتشاف ومنع الهجمات.

❖ مسئوليات إدارة أمن المعلومات:

- إدارة المستخدمين و حماية معلومات المصادقة
- مراجعة الصلاحيات الافتراضية وضمان توفر التحكم في الوصول.
- مراجعة حماية معلومات المصادقة السرية، مثل كلمات المرور وأرقام PIN.

❖ مسئوليات المطورين:

- إدارة صلاحيات الوصول البرمجية وتصميم البرامج بطريقة آمنة.
- اختبار البرامج بحثًا عن الثغرات الأمنية

انتهى