ان ما يحدث في أي جزء من العالم قد يكون له تأثير بسيط أو كبير على البيئة الاقتصادية المحلية. يتعين على أي شركة بغض النظر عن عملياتها وحجمها ومنطقة عملياتها أن تثبت قدرتها على أدى تطور أحدث تكنولوجيا المعلومات والاتصالات إلى بناء أنظمة متكاملة للشركة تجعل تخزين المعلومات مرنة للمعلومات والتي تكون قابلة للتكيف بسهولة مع التغيرات في بيئتها التشغيلية، يكون قادرًا على التكيف بسرعة حيث تشهد بيئة الأعمال العالمية الجديدة تغييرًا وتحولا مستمرًا وسيكون هذا التعديل مستحيلاً دون مساعدة تكنولوجيا المعلومات الجديدة والبنية التحتية للكمبيوتر التي تدور حول شبكة قد يكون استخدام شبكات وأنظمة الاتصالات خطيرًا لأنه قد يواجه أحداثا غير متوقعة مثل تعطل وإذا نظرنا إلى الشركة من هذا المنظور فإن النظام المحاسبي يعتبر أهم عنصر في نظام معلومات الشركة 1. يعتبر نظام المعلومات المحاسبية هو النظام الوحيد الذي يسمح للإدارة والمستخدمين الخارجيين بالحصول 2 يربط نظام المعلومات المحاسبية أنظمة المعلومات الفرعية الرئيسية الأخرى مثل التسويق والموارد البشرية والبحث والتطوير والإنتاج وما إلى ذلك، إلى الحد الذي يمكن فيه التعبير عن جميع المعلومات 3. يتم دمج المعلومات غير المالية في مجالات مثل المسؤولية الاجتماعية والموارد البشرية مع المعلومات 4. تكامل المحاسبة مع الأنظمة الفرعية الأخرى يؤدي إلى تقديم معلومات أكثر دقة للمستخدمين وبسرعة تشير عبارة البنية التحتية للمعلومات إلى موارد المعلومات بما في ذلك أنظمة الاتصالات والكيانات فضلاً عن البنية التحتية العالمية للمعلومات. المهاجمين المحتملين المصادر الرئيسية للمخاطر التي قد تواجهها أنظمة المعلومات المحاسبية هي الأشخاص داخل الشركة علاوة على :Attackers ذلك يمثل الأشخاص خارج الشركة مصدرًا مهما للخطر في بعض الحالات لأنهم أكثر تحفيزا ويصعب اكتشافهم والتحقيق معهم من الأشخاص داخل الشركة من المحتمل أن يتسبب "الوكلاء" التاليون في حدوث مشكلات متعلقة بالأمان لنظام المعلومات المحاسبية: أفضل بنقاط ضعف النظام، ويمكنهم إجراء عمليات تضر بالشركة وقد يقومون بحذف السجلات الرقمية الاستشاريون موظفو خدمة النظام ويتمتع هؤلاء الأشخاص بإمكانية الوصول بشكل متكرر إلى المناطق الموردون الزبائن: لا تتوافق أسبابهم الاقتصادية دائما مع أسباب الزبون المورد, وفي بعض الأحيان قد يتخذون إجراءات من المحتمل أن تشكل مخاطر متعلقة بالأمن. مرتزقة تكنولوجيا المعلومات / المجرمين المحترفين (الهاكرز): الأشخاص الذين يخترقون أنظمة الأشخاص بخبرة تقنية عالية إنهم مدربون جيدا ويمكنهم في أغلب الأحيان متابعة اهتماماتهم دون أن يتم اكتشافهم الحوادث الكوارث الطبيعية: يمكن أن تتسبب في فقدان المعلومات المهمة أو قد تجعلها غير متاحة. 1) الدافع الاجتماعي: يحاول المهاجمون في هذه الفئة اكتساب شعور بالتفوق أو السيطرة أو الاندماج النظام، 3) الدافع السياسي: يحاول المهاجمون في هذه الفئة الحصول على الاهتمام السياسي من أجل الترويج لقضية معينة. مرتزقة تكنولوجيا المعلومات أو الشركات المختلفة أو حتى الأشخاص الذين يتعاملون مع الأمور السرية للمعلومات وما الى ذلك. قد يكون للهجمات على البنية التحتية لنظام المعلومات المحاسبية أشكال مختلفة يمكننا التمييز بين نوعين من الهجمات: في الموقع أو عن بعد). ثانيا: يمكن إجراء تصنيف ثان وفقا للطريقة التي يتفاعل بها المهاجم مع المعلومات بعد الهجوم الناجح. في معظم الحالات يجب أن يكون الشخص قادرًا على التعامل مع الأنواع التالية من الهجمات: ومفرقعات كلمات المرور، فيجب على المرء أن يأخذ في الاعتبار الفئات المختلفة من "البرامج الضارة، على 3:33 the هو برنامج يمكنه كسر كلمات المرور أو تجاوز الماسح الضوئي : Apassword cracker برنامج كسر كلمة المرور هو تطبيق مفيد يستخدم للكشف تلقائيا عن نقاط الضعف في أمان من نقاط الدخول لاختراق النظام ثم تغطية هذه : scanner الثغرات الأمنية لاحقا. في البداية لتعزيز هذا الحاجز إلا أن وصولها إلى الجانب الآخر من الحاجز قد يسبب مشاكل خطيرة في وهو عبارة عن مكون برمجي او جهاز مصمم للتنصت" و"النقاط" المعلومات المنقولة عبر الشبكة. ومن : A sniffer المتشمم أجل التعرف على حركة المرور, هناك شروط معينة مطلوبة : يجب أن تسمح بنية الشبكة أو تكوين لوحة الشبكة بحدوث ذلك لا يمكن وضع أداة الشم داخل الشبكة إلا إذا وجد المهاجم ثغرة في نظام الأمان أو كان هو أو هي موظفا في الشركة التي ترغب في تستخدم الطبيعة البشرية لتأمين الوصول إلى المعلومات : social engineering جمع معلومات سرية. الهندسة الاجتماعية السرية غالبا ما تستهدف مثل هذه الهجمات الأشخاص السذج من بين موظفي المنظمة. الشركة وهي أن قواعد البيانات تمثل أكبر قدر من المعلومات التي تعمل بها الشركة, يمكن لقواعد البيانات الكشف عن التفاصيل الشخصية من خلال معالجة المعلومات العامة الأنواع الرئيسية للهجمات على قواعد البيانات هي المباشرة وغير المباشرة وعن طريق المراقبة. الهجمات من أجل منعها أو الحد من آثارها مثل برامج مكافحة الفيروسات وجدران الحماية، وتعليم المستخدم. تمثل التهديدات التي تؤثر على البنية التحتية لنظام المعلومات المحاسبية سواء كانت محتملة أو متخذة والتي ومتعمدة تلك المتعمدة هي الأكثر شيوعا وهي تنقسم إلى فئتين

داخلية وخارجية تأتي التهديدات الداخلية من داخل الشركة حيث يمكن عليها بالإضافة إلى ذلك فهم على دراية بسياسة أمن الشركة . مثل وكالات الاستخبارات الأجنبية والإرهابيين والمنظمات الإرهابية والمجرمين والمتسللين . التهديدات التي تواجه البنية التحتية لنظام المعلومات المحاسبية على النحو التالي: التهديدات الأساسية والتهديدات غير المباشرة تمثل التهديدات الأساسية ما يريد المهاجم القيام به وتتمثل تمثل التهديدات الميسرة تلك التهديدات التي تسمح بالوصول إلى التهديدات الأساسية. في حد ذاته فالأمن كهدف يمكن تفسيره كدولة ولن يكون مثاليا أبدًا بغض النظر عن التدابير المتخذة لهذا وما إلى ذلك. وهي مصممة للحد من الوصول برنامج مكافحة الفيروسات هو أداة مساعدة تكتشف عمل البرنامج الضار وتقضي عليه سيكتشف برنامج مكافحة الفيروسات روتينا فرعيا وهو اللقاح الذي سيقضي على عمل الفيروس عند اختيار برنامج مكافحة واسم منتج البرنامج، برامج مكافحة الفيروسات على سبيل المثال من الصعب إجراء فحص الفيروسات من كل محطة عمل محطة عمل. وحدة تحكم واحدة، الشركات سوف يحمي جهاز الكمبيوتر أو الشبكة من الوصول غير المصرح به عند اختيار جدار الحماية كاشف التسلل هو عملية تكتشف الاستخدام السيء لمكونات البنية التحتية لمعلومات المحاسبة وتستجيب له. سيؤدي استخدام كاشف التسلل إلى تحقيق فوائد للشركة فيما يتعلق باكتشاف الهجمات وحظرها والرد عليها ودعم تقييم الأضرار المتكبدة بالإضافة إلى الأدلة المقبولة في المحكمة ضد الأشخاص المتهمين بالاستخدام كشف التسلل في المؤسسات الصغيرة يتم تضمين أجهزة كشف التسلل هذه في جدار الحماية المثبت. التشغيل تسهيل اكتشاف الاختراقات. حدث متوقع لمنع وقوع حدث من المحتمل أن يؤثر على أمن نظام المعلومات يجب اتخاذ تدابير محددة يتضمن تحليل المخاطر عملية تحديد المخاطر الأمنية وتحديد مدى هذه المخاطر وتحديد المناطق عالية المخاطر التي تحتاج إلى التأمين تحليل المخاطر هو جزء من مجموعة تقييم المخاطر هو نتيجة لتحليل المخاطر يمكن تعريف إدارة المخاطر شاملة من التدابير تسمى إدارة المخاطر, تقييم المخاطر هو نتيجة لتحليل المخاطر يمكن تعريف إدارة المخاطر ومن الحقائق المعروفة أن مديري الشركات يترددون في الاستثمار وعندما يقتنعون بضرورة تخصيص المبالغ المطلوبة لضمان الحماية تكون هذه وفي ظل هذه الظروف تحتاج المنشأة الى ضمان وجود نظام أمني لا تتجاوز نفقاته المبلغ المخصص, هناك حلان بديلان لهذه الحالة أي وتقليل تكاليف إجراءات التحقق الأول يسمح بأقصى درجة من الحماية ضد بعض التهديدات لكنه قد يترك أو منخفض، ومع ذلك يمكن قياس مستوى الأمان على الأقل من وجهة نظر وتحديد مراحل تنفيذ الأمن، وتحديد متطلبات الارتقاء بالأمن، وإبلاغ الموظفين بالإجراءات الأمنية المطلوبة، ويمكنهم إجراء كل من أنها توفر كل من الخدمات الأمنية وإدارتها مستمرة. مع تزايد (SMS) الدراسة والتنفيذ، فإننا نشير إلى مورد إدارة خدمات الأمان اعتماد الشركات والمؤسسات على التشغيل الموثوق لأنظمة المعلومات المحاسبية أصبحت مسألة أمن النظام ذات أهمية قصوى وتعتمد البنية التحتية لأمن المعلومات المحاسبية في الشركات الحديثة على شبكات الاتصالات, وبالتالي يمكن ان تحدث ثغرة أمنية مزدوجة محتملة في البنية التحتية التلاعب بالمعلومات والاستخدام غير فإن تنفيذ بعض الآليات المحددة له أهمية قصوى يبدأ هذا التنفيذ من المستوى المادي الحماية المادية لخطوط النقل وإجراءات منع الوصول إلى وتطبيق تقنيات تشفير البيانات (التشفير) طريقة محددة لحماية الاتصال والتكوين غير المناسب لعناصر الأجهزة والبرامج ونقص الدعم من الشركات المصنعة، وضعف المعرفة أو المشكلات الأمنية أو الجهل بها النقاط الواردة في يتطلب الواقع من حولنا اتباع نهج ثلاثي الأبعاد للمخاطر التي تواجهها البنية التحتية للمعلومات المحاسبية, التهديدات التي تعتبر أحداثًا أو أنشطة (عمومًا) من خارج النظام الذي تم تقييمه والتي تؤثر على نقاط الضعف مما يسبب التأثير الذي يُفهم على أنه خسارة أو نتيجة للشركة أو المؤسسة قد يعاني على