وكالة المخابرات المركزية هي المبدأ الأساسي وراء كل ما نقوم به في مجال الأمن السيبراني. ثالوث وكالة المخابرات المركزية والمعروفة أيضا باسم ثالوث وكالة المخابرات المركزية. الغرض من هذه المصطلحات هو وصف الأمن باستخدام كلمات ذات صلة وذات مغزى تجعل الأمن أكثر قابلية للفهم للإدارة والمستخدمين وتحديد الغرض منه. السريه : من الصعب تحقيق التوازن عندما يكون العديد من مستخدمي النظام ضيوفا أو عملاء، ومن غير المعروف ما إذا كانوا يصلون إلى النظام من جهاز معرض للخطر أو تطبيق هاتف محمول ضعيف. فإن التزام محترف الأمن هو تنظيم الوصول ـ حماية البيانات التي تحتاج إلى حماية، مع السماح بالوصول إلى الأفراد المصرح لهم. يتعلق الأمر بأي بيانات عن فرد يمكن استخدامها لتحديد هويته. وهي معلومات تتعلق بالحالة الصحية للفرد، وهو مقياس للأهمية المسندة للمعلومات من قبل مالكها، أو الغرض من الدلالة على حاجتها إلى الحماية. المعلومات الحساسة هي المعلومات التي إذا تم الكشف عنها بشكل غير صحيح (السرية) أو تعديلها (النزاهة) من شأنها أن تضر بمنظمة أو فرد. أي الأشخاص أو المنظمات التي قد لا تكون جزءا من المنظمة التي تعالج أو تستخدم المعلومات الناس وأفعالهم سلامة البيانات هي التأكيد على أن البيانات لم يتم تغييرها بطريقة غير مصرح بها. يتطلب ذلك حماية البيانات في الأنظمة وأثناء المعالجة لضمان خلوها من التعديل أو الأخطاء أو فقدان المعلومات بشكل غير صحيح وتسجيلها واستخدامها وصيانتها بطريقة تضمن اكتمالها. تغطي سلامة البيانات البيانات أثناء التخزين وأثناء المعالجة وأثناء النقل. يجب أن تكون المعلومات دقيقة ومتسقة داخليا ومفيدة لغرض معلن. كجزء من سلامة البيانات، أن تكون جميع حالات البيانات متطابقة في الشكل والمحتوى والمعنى. تشير سلامة النظام إلى الحفاظ على تكوين جيد معروف ووظيفة تشغيلية متوقعة حيث يعالج النظام المعلومات. على وجه التحديد، على سبيل المثال، للحفاظ على تلك الحالة، إذا تطابق الاثنان، وإذا لم يتطابق الاثنان، فإن سلامة البيانات أو النظام قد تعرضت للخطر. النزاهة هي عامل أساسي في موثوقية المعلومات والنظم. في كثير من الأحيان، تملي احتياجات المنظمة للوصول إلى معلومات موثوقة ودقيقة واستخدامها. و(2) للمستخدمين المصرح لهم، الوصول في الوقت المناسب وبموثوقية إلى خدمات البيانات والمعلومات. المفهوم الأساسي للتوافر هو أن البيانات متاحة للمستخدمين المصرح لهم متى وأينما كانت هناك حاجة إليها وفي الشكل والشكل المطلوبين. بدلا من ذلك، تفي النظم والبيانات بمتطلبات الأعمال التجارية للوصول في الوقت المناسب وبموثوقية. بعض الأنظمة والبيانات أكثر أهمية بكثير من غيرها، لذلك يجب على محترف الأمن ضمان توفير المستويات المناسبة من التوافر. غالبا ما يرتبط التوافر بمصطلح الأهمية الحرجة، من الضروري التحقق من أنهم المالكون الشرعيون لتلك الهوية. ببساطة، شيء تعرفه: كلمات المرور أو عبارات المرور هناك نوعان من المصادقة. يعرف استخدام طريقة واحدة فقط من طرق المصادقة المذكورة سابقا باسم المصادقة أحادية العامل (SFA). يعرف منح المستخدمين حق الوصول فقط بعد إظهار أو عرض طريقتين أو أكثر من هذه الطرق بنجاح باسم المصادقة متعددة العوامل (MFA). قائم على الخصائص إذا اخترت رقم تعريف شخصي (PIN)، أو أنشأت كلمة مرور أو بعض القيم السرية الأخرى التي تعرفها أنت فقط، فقد واجهت مصادقة قائمة على المعرفة. على سبيل المثال، قد يتلقى مكتب المساعدة مكالمة لإعادة تعيين كلمة مرور المستخدم. للحصول على أمان أفضل، ستكون هناك حاجة إلى شكل ثان أو ثالث من المصادقة يعتمد على رمز مميز أو خاصية قبل إعادة تعيين كلمة المرور. يتكون الاستخدام المشترك لمعرف المستخدم وكلمة المرور من شيئين معروفين، فإنه لا يعتبر وزارة الخارجية. عدم التنصل: هو مصطلح قانوني ويعرف بأنه الحماية من الفرد الذي ينكر كذبا القيام بعمل معين. إنه يوفر القدرة على تحديد ما إذا كان فرد معين قد اتخذ إجراء معينا، في عالم التجارة الإلكترونية والمعاملات الإلكترونية اليوم، من المهم أن يثق جميع المشاركين في المعاملات عبر الإنترنت. الخصوصية :هي حق الفرد في التحكم في توزيع المعلومات عن نفسه. في حين أن كل من الأمن والخصوصية يركزان على حماية البيانات الشخصية والحساسة، إلا أن هناك فرقا بينهما. تعد الخصوصية العالمية قضية حاسمة بشكل خاص عند النظر في المتطلبات المتعلقة بجمع المعلومات الشخصية وأمنها. والتي تتغير بشكل دوري. إن ضمان وجود تدابير أمنية وقائية لا يكفي لتلبية لوائح الخصوصية أو لحماية الشركة من تكبد عقوبات أو غرامات من سوء التعامل مع المعلومات الشخصية أو الخاصة أو إساءة استخدامها أو حمايتها بشكل غير صحيح. التي تقوم بأعمال تجارية في الاتحاد الأوروبي أو أي أشخاص في الاتحاد الأوروبي. تملي هذه القوانين، بما في ذلك القوانين على المستوى الوطني وعلى مستوى الولاية، أن أي كيان في أي مكان في العالم يتعامل مع البيانات الخاصة للأشخاص في ولاية قضائية قانونية معينة يجب أن يلتزم بمتطلبات الخصوصية الخاصة به. بصفتك عضوا في فريق حماية البيانات التابع للمنظمة، لن يطلب منك تفسير هذه القوانين، ولكنك ستحتاج إلى فهم كيفية تطبيقها على مؤسستك. ولكن في كثير من الأحيان تفشل المنظمات في إدارة المخاطر بشكل استباقي. بصفتك عضوا في فريق الأمن في

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

المنظمة، ستعمل من خلال تقييم المخاطر والتحليل والتخفيف من حدتها ومعالجتها والتواصل. هناك العديد من النماذج المستخدمة لتسهيل عملية إدارة المخاطر، ومع ذلك، هذه الوحدة تجعلك تبدأ من خلال تقديم المصطلحات التأسيسية وتعريفك بعملية إدارة المخاطر. الآثار السلبية التي قد تنشأ إذا حدث الظرف أو الحدث، تعكس مخاطر أمن المعلومات الآثار الضارة المحتملة التي تنتج عن إمكانية الوصول غير المصرح به إلى المعلومات و/أو نظم المعلومات أو استخدامها أو الكشف عنها أو تعطيلها أو تعديلها أو تدميرها. ويشير أيضا إلى أن مخاطر تكنولوجيا المعلومات هي مجموعة فرعية من مخاطر الأعمال التجارية. مصطلحات إدارة المخاطر وتحديد كيفية استخدام بيانات المخاطر بفعالية، كجزء من تحقيق أو تعزيز هدفها أو أهدافها. الضعف هو ضعف أو عيب متأصل في نظام أو مكون، والذي، يمكن أن يتسبب في حدوث حدث خطر. لحماية نفسك من النشل، يمكنك حمل محفظتك في جيب داخلي بدلا من جيب البنطال الخلفي أو التصرف بحذر بدلا من تجاهل محيطك. احتمال: احتمال الحدوث هو عامل مرجح يعتمد على تحليل ذاتي لاحتمال أن يكون تهديدا معينا أو مجموعة من التهديدات قادرة على استغلال نقطة ضعف معينة أو مجموعة من نقاط الضعف. سينظر فريق الأمن في النتائج المحتملة إذا تحقق تهديد وحدث. تحديد المخاطر كيف تحدد المخاطر؟ هل تمشي في الشارع لمشاهدة حركة المرور وتبحث عن البرك على الأرض؟ ربما لاحظت أسلاكا فضفاضة في مكتبك أو ماء في طابق المكتب؟ إذا كنت تبحث بالفعل عن المخاطر، فستتناسب مع محترفي الأمن الآخرين الذين يعرفون أنه من الضروري البحث بشكل أعمق للعثور على المشاكل المحتملة. في عالم الإنترنت، إنه ينطوي على النظر إلى شركتك الفريدة وتحليل وضعها الفريد. حدد المخاطر لتوصيلها بوضوح. الموظفون على جميع مستويات المنظمة مسؤولون عن تحديد المخاطر. حدد المخاطر للحماية منها. بصفتك محترفا أمنيا، إذا كنت تعمل مع منظمة أصغر، أو منظمة تفتقر إلى أي نوع من خطة وبرنامج إدارة المخاطر والتخفيف، تقييم مخاطر يتم تعريف تقييم المخاطر على أنه عملية تحديد المخاطر وتقديرها وتحديد أولوياتها لعمليات المنظمة (بما في ذلك مهمتها ووظائفها وصورتها وسمعتها) والأصول والأفراد والمنظمات الأخرى وحتى الأمة. يجب أن يؤدي تقييم المخاطر إلى مواءمة (أو ربط) كل خطر محدد ناتج عن تشغيل نظام معلومات مع الأهداف أو الأهداف أو الأصول أو العمليات التي تستخدمها المنظمة، يحدد نشاط تقييم المخاطر المشترك خطر نشوب حريق في المبنى. فإن الهدف الأساسي من تقييم المخاطر هو التقدير وتحديد الأولويات. أجهزة إنذار الحريق هي الأقل تكلفة ويمكن أن تنبه الموظفين إلى الإخلاء وتقليل خطر الإصابة الشخصية، لكنها لن تمنع الحريق من الانتشار أو التسبب في المزيد من الضرر. لن تمنع أنظمة الرش الحريق ولكن يمكن أن تقلل من مقدار الضرر الناجم. في حين أن الرشاشات في مركز البيانات تحد من انتشار الحريق، فمن المحتمل أن تدمر جميع الأنظمة والبيانات الموجودة عليها. يمكن لتقييم المخاطر إعطاء الأولوية لهذه البنود للإدارة لتحديد طريقة التخفيف التي تناسب الأصول المحمية على أفضل وجه. يقدم هذا التقرير إلى الإدارة لمراجعته والموافقة عليه. في بعض الحالات، تعتمد القرارات المتخذة على موقف الإدارة تجاه المخاطر وتوافر ـ وتكلفة ـ التخفيف من المخاطر. الخيارات المستخدمة عادة للاستجابة للمخاطر هي:حدد كل نقطة ساخنة لعلامة زائد لمعرفة المزيد عن كل موضوع. أولويات المخاطر عندما يتم تحديد المخاطر، هذا ضروري لتحديد السبب الجذري وتضييق المخاطر الظاهرة والمخاطر الأساسية. يعمل محترفو الأمن مع فرقهم لإجراء كل من التحليل النوعي والكمي. يساعد فهم المهمة العامة للمنظمة والوظائف التي تدعم البعثة على وضع المخاطر في سياقها وتحديد الأسباب الجذرية وتحديد أولويات تقييم هذه العناصر وتحليلها. في معظم الحالات، اتخاذ القرار بناء على أولويات المخاطر يجب على المنظمات تقييم احتمالية المخاطر وتأثيرها وكذلك تسامحها مع أنواع مختلفة من المخاطر. ولكن سيتعين على شركة شيكاغو التخطيط للعواصف الثلجية. مما يعرض العمال للأسبستوس، على سبيل المثال، تحمل المخاطر غالبا ما يتم تشبيه إدارة التصور نحو المخاطرة بشهية الكيان للمخاطر. ما مقدار المخاطرة التي هم على استعداد لتحملها؟ هل ترحب الإدارة بالمخاطر أم تريد تجنبها؟ يختلف مستوى تحمل المخاطر عبر المنظمات، يهدف المتخصصون في مجال الأمن إلى الحفاظ على مستويات المخاطر ضمن حدود الإدارة لتحمل المخاطر. على سبيل المثال، تخطط الشركات في أيسلندا للمخاطر التي تفرضها البراكين القريبة على أعمالها. ستكون الشركات التي هي خارج المسار المتوقع لتدفق الحمم البركانية أقل عرضة للخطر من تلك الموجودة مباشرة في تدفق المسار. فإن احتمال انقطاع التيار الكهربائي الذي يؤثر على مركز البيانات يشكل تهديدا حقيقيا في جميع مناطق العالم. في المناطق التي تكون فيها العواصف الرعدية شائعة، قد يحدث انقطاع التيار الكهربائي أكثر من مرة في الشهر، في حين قد تشهد مناطق أخرى انقطاعا واحدا أو اثنين فقط سنويا. إذا كان لدى الشركة تحمل منخفض لخطر التوقف عن العمل، فمن المرجح أن تستثمر في مولد لتشغيل الأنظمة الحيوية. ستستثمر الشركة التي لديها تسامح أقل مع وقت التوقف عن

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

العمل في مولدات متعددة ذات مصادر وقود متعددة لتوفير مستوى أعلى من الضمان بأن الطاقة لن تفشل. سواء كان ذلك لتوفير المواد الخام لصناعة ما، أو تصنيع المعدات لبناء أجهزة الكمبيوتر، أو توفير السلع والخدمات. عندما ينفذ القادة والإدارة الأنظمة والهياكل التي ستستخدمها المنظمة لتحقيق أهدافها، مما يؤدي إلى إجراءات. مدونة قواعد السلوك المهنية والواجب تجاه مديرينا، أن نلتزم، بأعلى المعايير الأخلاقية للسلوك. غطينا المبادئ الأمنية، لقد سلطنا الضوء على ثالوث وكالة المخابرات المركزية باعتباره المكونات الأساسية لضمان المعلومات. تمثل "I" النزاهة؛ يجب أن نضمن عدم تغيير البيانات بطريقة غير مصرح بها. يجب أن نتأكد من أن البيانات في متناول المستخدمين المصرح لهم متى وأينما كانت هناك حاجة إليها، وفي الشكل والتنسيق المطلوبين. كما ناقشنا أهمية الخصوصية والمصادقة وعدم التنصل والتفويض. لقد استكشفت الضمانات والتدابير المضادة المنصوص عليها لنظام المعلومات لحماية سرية وسلامة وتوافر النظام ومعلوماته. من خلال تطبيق إدارة المخاطر، تمكنا من تقييم المخاطر وتحديد أولوياتها (نقاط الضعف في الأصول التي يمكن استغلالها من قبل التهديدات) للمنظمة. يمكن للمنظمة أن تقرر ما إذا كانت ستقبل المخاطر (تجاهل المخاطر ومواصلة الأنشطة المحفوفة بالمخاطر)، أو تجنب المخاطر (وقف النشاط المحفوف بالمخاطر لإزالة احتمال حدوث حدث ما)، أو التخفيف من المخاطر (اتخاذ إجراءات لمنع أو تقليل تأثير الحدث)، أو نقل المخاطر (نقل المخاطر إلى طرف ثالث). ثم تعلمت عن ثلاثة أنواع من الضوابط الأمنية: المادية والتقنية والإدارية. ينبغي أن يقلل تنفيذ الضوابط الأمنية من المخاطر، والسمات المعمارية للمباني والمرافق، والإجراءات الأمنية المحددة التي يتخذها الناس. نستمد عادة الإجراءات من السياسات، والسياسات من المعايير، والمعايير من اللوائح. غالبا ما تستخدم فرق الحوكمة المعايير لتوفير إطار لإدخال السياسات والإجراءات لدعم اللوائح. لتوفير التوجيه في جميع الأنشطة لضمان دعم المنظمة لمعايير ولوائح الصناعة. وأخيرا، التي يلتزم أعضاء المنظمة بدعمها الكامل. يجب أن نتصرف بشكل قانوني وأخلاقي في مجال الأمن السيبراني. A-C: الأمن الكافي ـ الأمن الكافي بما يتناسب مع خطر وحجم الضرر الناجم عن فقدان المعلومات أو إساءة استخدامها أو الوصول غير المصرح به إليها أو تعديلها. المصدر: OMB Circular A-130 ومن الأمثلة على ذلك عمليات التحكم في الوصول ومطالبة العديد من الموظفين بإجراء عملية محددة. غالبا ما يتم إنفاذ الضوابط الإدارية في البيئات الحديثة بالاقتران مع الضوابط المادية و/أو التقنية، مثل سياسة منح الوصول للمستخدمين الجدد التي تتطلب تسجيل الدخول والموافقة من قبل مدير التوظيف. الأصول ـ أي شيء ذي قيمة تملكه منظمة. تشمل الأصول كلا من العناصر الملموسة مثل نظم المعلومات والممتلكات المادية والأصول غير الملموسة مثل الملكية الفكرية. عادة، إجراء مصمم للحماية من عمليات الإرسال الاحتيالية من خلال إثبات صحة الإرسال أو الرسالة أو المحطة أو المنشئ. الترخيص ـ الحق أو الإذن الممنوح لكيان النظام للوصول إلى مورد النظام. نيست 800-82 التنقيح 2 التوافر ـ ضمان الوصول إلى المعلومات واستخدامها في الوقت المناسب وبموثوقية من قبل المستخدمين المصرح لهم. خط الأساس ـ أدنى مستوى موثق من التكوين الأمني يسمح به معيار أو منظمة. مع قدرات أخرى على طروادة والدودة. السرية ـ خاصية البيانات أو المعلومات عندما لا يتم إتاحتها أو الكشف عنها للأشخاص أو العمليات غير المصرح لهم. نيست 800-66 A-D: سلامة البيانات ـ الخاصية التي لم يتم تغيير البيانات بطريقة غير مصرح بها. المصدر: NIST SP 800-27 Rev A يستخدم المصطلحان أحيانا بالتبادل في الأدب ولهما معان متشابهة. اللائحة العامة لحماية البيانات (GDPR) – في عام 2016، أصدر الاتحاد الأوروبي تشريعا شاملا يتناول الخصوصية الشخصية، معتبرا أنها حق فردي من حقوق الإنسان. الحوكمة ـ عملية كيفية إدارة المنظمة؛ عادة ما تشمل جميع جوانب كيفية اتخاذ القرارات لتلك المنظمة، إنه يوجه اعتماد المعايير الوطنية لمعاملات الرعاية الصحية الإلكترونية مع حماية خصوصية المعلومات الصحية الفردية. والأصول، والأفراد، وحتى الأمة، معهد مهندسي الكهرباء والإلكترونيات ـ IEEE هي منظمة مهنية تضع معايير الاتصالات السلكية واللاسلكية وهندسة الكمبيوتر والتخصصات المماثلة. النزاهة ـ ملكية المعلومات التي يتم من خلالها تسجيلها واستخدامها وصيانتها بطريقة تضمن اكتمالها ودقتها واتساقها الداخلي وفائدتها لغرض معلن. التوحيد القياسي الدولي، فرقة العمل المعنية بهندسة الإنترنت (IETF) – منظمة معايير الإنترنت، التي تحدد معايير البروتوكول (على سبيل المثال، TCP ،IP، احتمال الحدوث ـ عامل مرجح يعتمد على تحليل ذاتي لاحتمال أن يكون تهديدا معينا قادرا على استغلال نقطة ضعف معينة أو مجموعة من نقاط الضعف. شيء أنت عليه) للتحقق من الهوية. بما في ذلك أمن المعلومات داخل مركز موارد أمن الحاسوب التابع لشعبة أمن الحاسوب. عدم التنصل ـ عدم القدرة على رفض اتخاذ إجراء مثل إنشاء المعلومات والموافقة على المعلومات وإرسال رسالة أو تلقيها. بما في ذلك (1) أي معلومات يمكن استخدامها لتمييز أو تتبع هوية الفرد، و(2) أي معلومات أخرى مرتبطة أو قابلة للربط بالفرد، مثل المعلومات

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي

الطبية والتعليمية والمالية والتوظيف". الاحتمال ـ الفرص، أن يكون تهديدا معينا قادرا على استغلال نقطة ضعف معينة أو مجموعة من نقاط الضعف. 1 والمساءلة). Q-R: التحليل النوعي للمخاطر ـ طريقة لتحليل المخاطر تستند إلى تعيين واصف مثل منخفض أو متوسط أو مرتفع. المصدر: NISTIR 8286 التحليل الكمي للمخاطر ـ طريقة لتحليل المخاطر حيث يتم تعيين القيم العددية لكل من التأثير والاحتمال استنادا إلى الاحتمالات الإحصائية والتقييم النقدي للخسارة أو الربح. المصدر: NISTIR 8286 المخاطر ـ مقياس لمدى تهديد الكيان بظرف أو حدث محتمل. تجنب المخاطر ـ تحديد أن تأثير و/أو احتمال حدوث خطر معين أكبر من أن تقابله الفوائد المحتملة وعدم أداء وظيفة تجارية معينة بسبب هذا القرار. بما في ذلك جميع مراحل سياق (أو إطار المخاطر)، وتقييم المخاطر، ورصد المخاطر. إطار إدارة المخاطر ـ نهج منظم يستخدم للإشراف على المخاطر وإدارتها للمؤسسة. المصدر: CNSSI 4009 تحمل المخاطر ـ مستوى المخاطر الذي يرغب الكيان في تحمله من أجل تحقيق النتيجة المرجوة المحتملة. عتبة المخاطرة ورغبة المخاطرة والمخاطر المقبولة هي أيضا مصطلحات تستخدم بشكل مرادف مع تحمل المخاطر. نقل المخاطر ـ دفع طرف خارجي لقبول التأثير المالي لمخاطر معينة. Z-S: المصدر: FIPS PUB 199 الحساسية ـ مقياس للأهمية المعطاة للمعلومات من قبل مالكها، لغرض الدلالة على حاجتها إلى الحماية. المصدر: NIST SP 800-60 المجلد 1 1 Rev

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي