أنه "بحلول عام ٢٠١٦ سيكون ٤٠٪ من العمالة يعملون فيمجال الأجهزة النقالة و ٦٧٪ من (Gartner) ٣٥٠وقد توقع جارتنر العمال يستخدمون الهواتف الذكية." "" (تم إضافة تأكيد). ولقد تطلبت الأنواع الجديدة من الأجهزة وبيئات التشغيل الجديدة مع ظهور مخاطر أمنية غير معروفة "، ولقد توصلت شبكة تحويل المعرفة إلى أنظمة Gسياسات جديدة لحوكمة المعلومات 1 رقمية (مركز أبحاث بالمملكة المتحدة) إلى "أن زيادة تدفق أجهزة الحوسبة النقالة داخل السوق سيكون أكبر التحديات الأمنية الحالية [المستمرة] " فمع الأجهزة النقالة المتصلة بشبكات الواي فاي أو البلوتوث ستتزايد الفرص أمام (قراصنة الإنترنت] للتسلل وسرقة المعلومات الشخصية. ويسبب ذلك التحول السريع تجاه الحوسبة النقالة ينبغي للشركات التي لديها أفراد يحملون الأجهزة النقالة مثل أفراد المبيعات وفنيو الخدمات توخي الحيطة والحذر تجاه التهديدات الأمنية المحتملة بشأن المعلومات السرية للشركة.٦٠٠ دولار أمريكي إلى أكثر من ٤٠٠،٠٠٠ دولار أمريكي. في الواقع معظم الأجهزة النقالة غير مصممة بمراعاة الهواتف الذكية من متابعة مجموعة متنوعة من os جوانب التأمين وفي الحقيقة أدخلت بعض التعديلات لتمكين أنظمة تشغيل آندرويد من جوجل ويشبه ذلك الخيارات التفصيلية التي أدخلتها مايكروسوفت عند تطوير نظام (OS) الأجهزة مثل، نظام تشغيل ويندوز لتعمل على مجموعة متنوعة من تصميمات الأجهزة الصادرة من جانب الشركات المصنعة للكمبيوتر OS تشغيل ويصعب اكتشاف الإصابات بفيروسات الهواتف الذكية على وجه الخصوص كما يصعب أيضاً إزالتها، فقد.(PC) الشخصي يكون معظم المستخدمين غير مدركين أن معظم بياناتهم تم السيطرة والاستيلاء عليها وأن قراصنة الإنترنت ينتظرون فقط الوقت المناسب لاستخدامها، وقد تعاني الشركات من خسائر اقتصادية وخسائر أخرى مثل انكشاف وإتلاف أصول معلوماتها أو الإساءة إلى سمعة الشركة جراء تضرر صورة الشركة. يشهد سوق الهواتف الذكية حالة توسع سريعة مع دخول تطورات يومية إلى ذلك السوق؛ تقدم فرصا جديدة للمجرمين. وقد أوضح تقرير مؤسسة بيانات دولية أن " مبيعات الهواتف الذكية تجاوزت مبيعات الكمبيوتر الشخصي لأول مرة في الربع الأول من عام ٢٠١٠ بواقع ١٠٠٩ مليون هاتف ذكي مقابل ١, ٩٢ مليون كمبيوتر ي" (تم إضافة تأكيد) وتعني وتيرة النمو المتزايدة في مبيعات الهواتف الذكية والخدمات الجديدة من البنوك مثل، إبداع الأموال عن بعد من خلال التقاط صورة شيك تزايد الفرص المتاحة للاحتيال وسرقة الهوية.٣٥١الوعي والتعليم هما المفتاح أو خط الدفاع الأول للمستخدمين هو فهم تقنيات الجرائمالإلكترونية بشكل أفضل والوعي والذكاء عند استخدام تقنيات الاتصالات والمعلومات. وسوف يجري كسب جزء كبير من المعركة عند تطوير ونضوج تقنيات توثيق القياسات الحيوية (التي تستخدم نظام التعرف على بصمات الأصابع والصوت وشبكية العين) بشكل كاف للتعرف على المستخدم وضمان وصول الشخص الصحيح إلى الحسابات المالية والسرية. فالاهتمام الأول لموردي التطبيقات هو الوظيفية والاستخدام واسع الانتشار ولا يكون الأمن هو الأولوية الأولي بالنسبة لهم، ويتعين أن يكون المستخدمون واعين ومتيقظين لحماية أنفسهم من السرقة والاحتيال وعلى مستوى المؤسسات، يتعين على كل شركة أن توفر كل الجهود التدريبية وإضافةطبقات من التقنيات الأمنية لحماية الوثائق والبيانات الإلكترونية المهمة وحماية أصول المعلومات. الهندسة الاجتماعية: استخدام الطرق المتنوعة لخداع المستخدم وإقناعه بإدخال البيانات الخاصة هو أكثر الطرق شيوعا، التي يستخدمها قراصنة الإنترنت والأمر في تزايد فالآلات تقوم بأداء مهامها وتؤدي البرامج أيضا الهدف من برمجتها بالضبط، ولكن العنصر البشري هو الحلقة الأضعف في سلسلة الأمن ونظرا للاتجاه المتزايد لاستخدام الأجهزة النقالة والقوى العاملة عن بعد، يجب أن يكون الناس مدربين على التهديدات القائمة ويكونوا على دراية باستمرار ومواكبين للطرق والبرامج الإجرامية الجديدة. ويعتبر هذا التدريب جزءًا من جهود إدارة المعلومات الكلية للتحكم فيمن يصل إلى المعلومات وإلى أي المعلومات ومتى وأين يصل إلى المعلومات.أصبحت عملية إدارة المعلومات أمرًا لازما وينبغي أن يتم تنفيذه باستمرار ومنتظم؛ جراء تزايد كمية المعلومات الحساسة المتعلقة بالأنشطة التجارية التي يتم الدفع بها على الأجهزة النقالة (أي برامج المحاسبة المالية والعقود التجارية والخطط الاستراتيجية وينبغي مراجعة السياسات عند استخدام جهاز محمول جديد وعند وجود تهديدات لم يتم الكشف عنها، حيث إن الموظفين يستخدمون شبكات واي فاي عامة غير مؤمنة والعمليات التجارية تتغير لتشمل المزيد ضمان أن تكون الأجهزة النقالة محمية ضد IT والمزيد من إستراتيجيات الأجهزة النقالة، ويتعين على أقسام تقنية المعلومات أحدث المخاطر الأمنية، وينبغي أن يطلع المستخدمون بانتظام على التهديدات الأمنية المتغيرة والطرق الإجرامية الجديدة المستخدمة من جانب قراصنة الإنترنت.٣٥٢الاتجاهات الراهنة في الحوسبة النقالةمع التغير السريع في الحوسبة النقالة من الأهمية بمكان تفهم اتجاهات ذلك التغير المعرفة التطورات التي ينبغي توقعها بشكل أفضل والتخطيط لها. ويتعين معرفة وفهم اتجاه ١. CIOZone.com وتطبيق استخدام الحوسبة النقالة لتخطيط وتطوير سياسات إدارة المعلومات لحماية أصول المعلومات.من

Summarized by © lakhasly.com

قابلية التبادل البيني العالمي لمنافذ مايكروسوفت) وحيث إن شبكات) WiMax ٢. واي ماكس،(LTE) التطور طويل المدى الاتصالات وشبكات واي ماكس منتشرة ومستخدمة في الولايات المتحدة في خلال [٢٠١٣ وما بعدها فمن المتوقع أن نري نوت ودعم لاسلكي (واي ماكس بروتوكول للاتصالات يوفر ما (RFID) بوك وأجهزة لاب توب مزودة بتعريف ترددات لاسلكية داخلي لقد طورت سبرينت : Gو 4 Gيصل إلى ٤٠ ميجابايت / سرعات إضافية (أسرع بكثير من واي فاي)، . قابلية التبادل البيني 3 ومن المتوقع أن تتبع الشبكات الناقلة Gو 4 Gبطاقة نظام مزدوج تمكن مستخدمي الأجهزة النقالة من العمل على شبكات 3 الأخرى المجموعة. ٤. تطبيقات الهواتف الذكية: سوف يجعل بائعو برامج الأطراف الثالثة ـبشكل متزايد ـ تطبيقات الشركات سيستخدم GPS متاحة للهواتف الذكية بما في ذلك إدارة المخزون وإدارة السجلات الطبية ٥. نظام التموضع العالمي جي بي إس نظام التموضع العالمي بشكل متزايد ـ لتحديد أماكن المستخدمين النهائيين وتحليل الطرق المثالية لمسارات الطرق لعمال تسليم البضائع وفنبي الخدمات. ٦. الأمن: حيث إنه يجري تقديم أنواع جديدة ومختلفة من الهواتف الذكية، ستواجه إدارة تقنية صعوبة وتحديا في تحديد وتوثيق شخصية المستخدم النهائي وعلى المنوال نفسه،٣٥٣ مضاد الفيروسات ينبغي أن IT المعلومات على دراية بالفيروساتالمحتملة، تطبيقات الزر الضاغط دعنا نقول إن هناك شاحنة رمي (CIOs) يكون كبار موظفي المعلومات مخلفات وصلت إلى موقع صناعي، ولكنها غير قادرة على تفريغ المخلفات بسبب وجود مركبة تغلق الطريق أمامها. توجد تطبيقات مثبتة في الهواتف الذكية تمكن سائق الشاحنة من تصوير الشيء ء المسبب للعرقلة وإرسالالصورة إلى المرسل لتوثيق وشبكات واي ماكس LTE وتحديد زمن الإعاقة. ٩. النطاق العريض التكميلي ولأن الشركات الناقلة تستخدم التطور طويل المدى تنظر شركات مثل سبرينت وفيرزون في توفير إمكانيات النطاق العريض اللاسلكي الممتد المحتمل للشركات الصغيرة WiMax التي ليس لديها ألياف بصرية أو وصلات نحاسية على الأرض، وفي ظل هذا السيناريو قد تكون شركات حزم صغيرة في "نيو عالي السرعة) في مناطق الولايات المتحدة الأمريكية، حيث) T–جيرسي" بالفعل قادرة على استقبال إمكانيات النطاق العريض 1 ينبغي أن يتوقع عملاء :(SSD) يكون لديها مكاتب دون أن تمتلك وصلات نطاق عريض للكبل المعدني. ١٠. مشغل الحالة الصلبة الشركات مشاهدة تحسينات مستمرة في برامج التحكم،

Summarized by © lakhasly.com