إطار حماية لبيئة السحابة والأجهزة الخاصة

اسم الطالب
خالد علي المرحبي

بحث مقدم لنيل درجة الدكتوراه في تخصص علوم الحاسبات

المشرفون

أ.د. كمال منصور جمبي
د. عمر عبدالله باطرفي

المستخلص

فكرة إحضار أو استخدام أجهزة الموظفين الشخصية في العمل بدلا من تقديم أجهزة لهم مفهوم جديد بدأ في الانتشار بشكل متزايد. تكمن فوائد هذه الفكرة في العمل من أي مكان من خلال الإتصال بالإنترنت، وتقليل نفقات شراء وصيانة أجهزة الشركة، وزيادة كفاءة ومخرجات العمل ورضا الموظفين أيضا. وفي المقابل فإن هذا الإتجاه الذي لا مفر منه في الغالب يشكل خطراً وتحدياً أمنياً كبيراً على بيانات الموظفين وبيانات الشركة والشبكة عامة لأن هذه الأجهزة قد تكون مصابة بفايروسات أو برامج تجسس أو برامج خبيثة وقد تحصل على صلاحيات للوصول غير المصرح به إلى بعض المعلومات الحساسة. هذا الوصول غير المرغوب فيه يؤدي إلى مجموعة من التأثيرات السلبية منها: نشر البيانات المهمة بشكل غير رسمي وتعديل في بعض الصلاحيات وتوقف بعض الخدمات الإلكترونية و فقدان الإنتاجية وتبعات مالية وقانونية وغيرها. سنركز في هذا البحث على إيجاد حلول للقضايا المتعلقة بصلاحيات الوصول والتي يمكن إجمالها في أربع قضايا رئيسة. أولا: فرض وتعزيز سياسات الوصول والصلاحيات بشكل متوافق مع مفهوم أحضر جهازك الخاص. ثانيا: حماية البيانات وسياسات الوصول أثناء تخزينها وانتقالها ومعالجتها. ثالثا: تقديم حلول تدعم مختلف أنظمة التشغيل ولا تتقيد ببيئة محددة. رابعا: التأكد من موثوقية أجهزة الموظفين وقابليتها للعمل مع هذه الفكرة الجديدة قبل اتصالها بالسحابة.

الحلول الحالية المقترحة لبيئة احضر جهازك الخاص تواجه مجموعة من التحديات أولها وضع قوانين صارمة لاختيار الجهاز الخاص من مجموعة محددة من الأجهزة وبالتالي فإن بعض إيجابيات مفهوم أحضر جهازك الخاص سوف يفقد. ثانيها هو عدم وجود منصة موحدة للتحكم في الوصول للأجهزة المختلفة في أنظمة التشغيل. آخر التحديات هو المطالبة بتغيير نظام التشغيل ليكون معتمدا على التحكم الإلزامي في الوصول والذي سيكون مكلفا ومجهدا على المؤسسات بسبب الصعوبة الموجودة في تلك الآلية. لذلك فإن الحاجة لإيجاد حل مقترح بعيدا عن هذه التحديات والأطر أمر مطلوب.

هذا البحث قدم إطار حماية مبتكر باستخدام تقنيات جديدة وأخرى متجانسة لفرض سياسات التحكم في الوصول إلى الموارد للسيطرة عليها وحفظها في بيئة السحابة والأجهزة الخاصة. تم بناء نموذج للتأكد من موثوقية الأجهزة كما تم تأمين البيانات وسياسات الوصول أثناء انتقالها ومعالجتها وتخزينها بشكل توافقي مع أي جهاز يمكن أن يتلاءم مع متطلبات وسياسات الشركة. اعتمد في هذا البحث استخدام الوكيل المعتمد مع الاستفادة من بعض الأنظمة الموثوقة المتبِعة لآلية التحكم الإلزامي في الوصول. تم بناء الإطار عمليا واختباره وأظهر نتائجا إيجابية من خلال فرض سياسات الوصول بشكل فعال وقادر على اكتشاف الهجمات التي تستهدف ملفات سياسات الوصول بتكلفة أقل وزيادة في السرعة. في نهاية المطاف فإن هذا البحث قدم إطار حماية وحلول لمزودي الخدمة السحابية وللشركات التي ترغب في تبني فكرة إحضار الجهاز الخاص.

SECURITY FRAMEWORK FOR THE CLOUD AND BYOD ENVIRONMENT

By Khalid Ali Almarhabi

A thesis submitted for the requirements of the degree
of Doctor of Philosophy in Computer Science

Supervised by

Prof. Kamal Mansor Jambi
Dr. Omar Abdullah Batarfi

Abstract

Bring Your Own Device (BYOD) is growing in popularity. The benefits of BYOD are virtually limitless, and they include financial gain, greater employee satisfaction levels, elevated morale, increased job efficiency, and improved flexibility. However, this inevitable and unstoppable trend poses new security risks and challenges in controlling and managing corporate networks and data. BYOD may be infected by viruses, spyware, or malware that can gain access to sensitive data, leading to the disclosure of information, modified access policies, disruption of service, loss of productivity, financial issues, and legal implications. This research focuses on access control issues and attempts to address the following problems: lack of access control enforcement, untrusted BYOD devices, lack of data and policy protection, platform dependency, and lack of respect for users' privacy.

Existing access control solutions in BYOD and cloud environments face several challenges, including restrictions on choosing BYOD devices, platform dependency, and modifying operating systems of servers. Therefore, understanding the BYOD environment and building new suitable access control mechanisms will be a key component to achieving a high level of authorization. Thus, new approaches are needed.

The research introduces a new security framework using new and integrated techniques to implement access control policies in the cloud and BYOD environment. This solution is derived from large volumes of research into information privacy and security to manage and control access to enterprise networks by BYODs. This research has been achieved via loosely coupled integration of Mandatory Access Control (MAC) and Discretionary Access Control (DAC) mechanisms in the BYOD environment. With the proposed techniques, software agents are used to enforce access control policies and to prevent untrusted devices from accessing sensitive corporate data. In order to enhance the access control mechanism, we secured access control policies during the transfer, process, and storage phases. The experiment part of this research shows positive results. It has reduced restrictions and enforced access control policies in the cloud and BYOD environment in a soft and secure manner with an independent platform. The research provides solutions and a framework for cloud providers and those who implement the BYOD trend in their enterprises.