Enhancing Cloud Security
Trends from the Cloud Security Alliance

Eric A. Hibbard

OVERVIEW: Security continues to be one of the top concerns for many organizations when considering a move to cloud computing. The issues frequently include a lack of understanding of the threats and risks, inadequate methods of determining the trustworthiness of internal and external cloud service providers, a poorly trained workforce in the areas of cloud and virtualization security, and limited insight into the security controls frequently employed to guard against attacks and data breaches in the cloud. With its best practices, the Cloud Security Alliance (CSA) has emerged as a dominant player in the cloud security space and it is positioned to play an even more important role with some of its new initiatives.

INTRODUCTION

In 2008, the information security community started to take notice of the issues and opportunities of cloud computing. By early 2009, these initial interests and concerns served as a catalyst to form the Cloud Security Alliance (CSA) as a not-for-profit organization. The CSA was chartered with a mission to promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing. It continues to be led by a broad coalition of industry practitioners, corporations, associations, and other key stakeholders.

While it is probably best known for its cloud security guidance, the CSA has numerous other publications that cover a broad range of cloud security and related issues. In addition, the CSA has undertaken several new endeavors that are likely to expand the CSA's influence in the cloud security space. This article highlights some of these emerging activities and trends.

SECURITY GUIDANCE AND CONTROL OBJECTIVES

In the second half of 2011, the CSA published a major update to the Security Guidance for Critical Areas of Focus in Cloud Computing (Version 3) as well as a minor update to the Cloud Controls Matrix (Version 2.1). Both of these documents are key elements of the CSA materials and represent some of the best materials available to help secure cloud computing.

Over the next few months, a major rewrite of the Cloud Controls Matrix (Version 2) is anticipated, and the resulting document will improve alignment with both the CSA "security guidance" as well as the new U.S. Government Federal Risk and Authorization Management Program (FedRAMP), which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services sold to the Government.

Other notable activities include the CSA CloudTrust Protocol (CTP) with its CTP Reference Architecture Model, updates to the CSA Top Threats to Cloud Computing (Version 2), and Big Data Working Group (BDWG) will be identifying scalable techniques for data-centric security and privacy problems.

CSA CERTIFICATIONS

The CSA has recently unveiled certification programs for cloud computing users and professionals as well as

cloud computing providers.

Cloud Provider Security Certification

In May 2012, the CSA announced the CSA Open Certification Framework, which is an industry initiative to allow global, trusted certification of cloud providers. This program is intended to be a flexible, incremental, and multi-layered cloud provider certification that is aligned to the CSA's security guidance and control objectives. The program is intended to support popular third-party assessment and attestation statements developed within the public accounting community. Initial partners for the CSA Open Certification Framework will be announced this fall and a detailed timeline of deliverables will provided at that time as well.

Cloud Security Professional Certification

In a first of its kind, the CSA has established a user certification program for secure cloud computing. This professional certification, known as the Certificate of Cloud Security Knowledge (CCSK), is designed to ensure that a broad range of professionals with a responsibility related to cloud computing have a demonstrated awareness of the security threats and best practices for securing the cloud. The body of knowledge for the CCSK certification is based on the CSA guidance as well as materials from the European Network and Information Security Agency (ENISA).

This professional certification is influencing the minimum security expectations of organizations hiring cloud computing professionals, which in turn is causing professionals in the field to pay more attention to cloud security. The long-term impact of the program is unclear because only a few employers have made the certification a mandatory element of their hiring practices thus far.

FORMAL STANDARDIZATION

The CSA guidelines are currently recognized as industry best practices, which can limit their adoption and effectiveness within organizations around the world. This is a recognized issue and something the CSA has begun to address.

As a first step, the CSA has undertaken efforts to establish formal liaisons with standards development organizations (SDOs) like ISO/IEC JTC 1, which deals with international information technology standards, and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), which deals with standards covering all fields of telecommunications on a worldwide basis. Within ISO/IEC JTC 1, two subcommittees, SC 27 (IT security techniques) and SC 38 (Distributed application platforms and services), have active cloud computing and cloud security standardization projects. Likewise, the ITU-T has multiple cloud computing and cloud security projects underway. The CSA is actively participating in the meetings as well as contributing materials from its research and guidance projects.

To ensure that the CSA puts forward a consistent position, it has also established an internal International Standardization Council (ISC). The CSA ISC handles all communication to and from the SDOs as well as other organizations like industry trade associations. Although it is relatively new, the CSA ISC has already had success in getting materials from the CSA Cloud Controls Matrix adopted by ISO/IEC.

CONCLUSIONS

The CSA is expected to continue to be a recognized leader and trusted advocate on matters related to cloud security. However, its new cloud provider certification program could shift the focus of the CSA from education and awareness concepts to detailed requirements that serve as the basis for certification. Within a few years, the CSA may take on a role similar to the Payment Card Industry (PCI) Security Standards Council, which also focuses on technical requirements for data security compliance programs.

REFERENCE

(1) Official Cloud Security Alliance web site, http://www.cloudsecurityalliance.org

ABOUT THE AUTHOR

Eric A. Hibbard, CISSP, CISA
Joined Hitachi Data Systems in 2004, where he continues to work as the CTO Security & Privacy. He is currently engaged in wide range of product-oriented security activities. Mr. Hibbard serves as the International Representative for INCITS Technical Committee CS1 Cyber Security, Co-Chair of the American Bar Association's Electronic Discovery and Digital Evidence Committee, Co-Chair of the Cloud Security Alliance International Standardization Council, Chair of the IEEE Information Assurance Standards Committee, Chair of the SNIA Security Technical Work Group, and the Editor of ISO/IEC 27040 (Storage security) and ISO/IEC CD 17788 (Cloud computing - Vocabulary).