Edition <kes>

Editor
Peter Hohl, Ingelheim, Germany

With modern computer technology everywhere, the importance of data integrity and the security of IT systems has increased immensely. Given the complexity and rapid progress of information technology, IT professionals need in-depth knowledge in this field.

The series Edition <kes> provides the required know-how, promoting risk awareness and helping in the development and implementation of security solutions of IT systems and their environment.

Editor of the series is Peter Hohl. He is also editor of <kes> – Journal of Information Security (see www.kes.info), which has been published in SecuMedia Verlag since 1985. <kes> covers all subjects from audits and security policies to encryption and access control. It also provides information about new security hard- and software as well as the relevant legislation for multimedia and data security.

Eberhard von Faber · Wolfgang Behnsen

Secure ICT Service Provisioning for Cloud, Mobile and Beyond

A Workable Architectural Approach Balancing Between Buyers and Providers

Springer Vieweg

Prof. Dr. Eberhard von Faber
Dipl.-Math. Wolfgang Behnsen
T-Systems
Germany

ISBN 978-3-658-00068-4 ISBN 978-3-658-00069-1 (eBook)
DOI 10.1007/978-3-658-00069-1

Library of Congress Control Number: 2012952618

Springer Vieweg

Printed on acid-free paper

Springer Vieweg is a brand of Springer
Springer is a part of Springer Science+Business Media (www.springer.com).

In diesem Buch wird eine Referenzarchitektur für die Absicherung marktgängiger ICT-Services vorgestellt (ICT: Informations- und Kommunikationstechnologie). Anwenderunternehmen werden in die Lage versetzt, Angebote zu vergleichen und die Risiken zu bewerten, die mit der Nutzung von Cloud-Computing, mobilen Anwendungen und anderen ICT-Services verbunden sind. ICT-Dienstleister erhalten eine umfassende Vorlage zur Implementierung und Pflege von Sicherheitsmaßnahmen, die neben dem Service Portfolio Management alle Vertriebsphasen und Realisierungsprojekte sowie das Service Delivery Management abdeckt. Die Architektur ist vollständig modular und hierarchisch aufgebaut. Sie enthält eine Security-Taxonomy, die alle Aspekte moderner, industrialisierter ICT-Produktion enthält und strukturiert. Das Buch beschreibt darüber hinaus eine Fülle konkreter Sicherheitsmaßnahmen. Sie werden aus den Herausforderungen abgeleitet, denen sich ICT-Produktion und Service Management in der Praxis gegenübergestellt sehen.

Ce livre présente une architecture de référence qui améliore la sécurité des services proposés sur le marché des technologies de l'information et de la communication (TIC). Il permet aux clients de comparer les offres et d'évaluer les risques liés à l'utilisation de services de TIC fournis par des tiers, y compris les services informatiques hébergés (cloud computing) et mobiles. Les prestataires de services reçoivent un plan détaillé pour la mise en œuvre et le maintien de la sécurité qui couvre la gestion du portefeuille de services, les phases de soumission et les projets de réalisation, ainsi que la gestion de la prestation des services. L'architecture est entièrement modulaire et hiérarchique. Elle comprend une classification relative à la sécurité qui organise tous les aspects de la production industrialisée de TIC moderne. Le livre décrit également toute une série de mesures de sécurité s'inspirant de problèmes réels en matière de gestion des services et de production de TIC.

Este libro presenta a una arquitectura de referencia que mejora la seguridad de los servicios que se ofrecen en el mercado de las tecnologías de la información y la comunicación (TIC). Permite a los clientes comparar las ofertas y valorar los riesgos a la hora de utilizar servicios TIC de terceros, incluidos servicios informáticos de la nube y móviles. Los proveedores de servicios disponen de un plan de acción integral para la implantación y mantenimiento de la seguridad que cubre la gestión de la cartera de servicios, las fases asociadas con la presentación de ofertas y la realización de proyectos, al igual que la gestión de la prestación de servicios. La arquitectura es completamente modular y jerárquica. Contiene una taxonomía de seguridad que organiza todos los aspectos de la producción de la TIC industrializada moderna. El libro también describe una buena cantidad de medidas de seguridad que se basan en los retos del mundo real relativos a la producción de TIC y la gestión de servicios.

Foreword

Following a series of high-profile incidents involving big-name and international players, the issues of information security and data protection are making their way into the public eye, and the threats are entering a whole new dimension. In the past, the tools available were used to attack systems that appeared to be vulnerable in order to gather information or gain money. Today, the goal and targets are often determined in advance. The attacks are increasingly targeting specific businesses and value chains. For example, we are encountering a whole new generation of malware specifically designed for industrial espionage and sabotage. Obstruction, espionage and cyber crime seem to have become a specific commercial sector. Millions of credit card numbers are stolen and sold. Private account and digital identity theft is common. Huge amounts of data are lost and cannot be restored. The list of such incidents can be extended and filled with specific names of attacked parties and more and more new examples of scenarios. The newspapers are providing material on this on an almost daily basis.

Regardless of whether they are actually observed or merely assumed, the dramatic increase in such major incidents both in number and in degree is often attributed to the rise in vulnerabilities associated with information and telecommunication technology (ICT). But this is less than half of the truth. Intruders need to have an opportunity to break in and technology has become more complex and innovative, resulting in more gaps. But this does not explain what we are seeing today. The reason for the increase in anticipated risk is associated with the enormous success of using ICT. Nowadays, ICT is used in almost all businesses in order to automate and increase speed and quality. This has two major consequences. Firstly, enterprises and authorities are much more dependent on ICT. At the same time, the value of the data being processed is going up and up. Today, even highly confidential data and highly priced intellectual property are processed electronically. Thus our adversaries, which include individual hackers, organized crime and authorities, are unfortunately highly motivated. Secondly, ICT is now a ubiquitous part of everyday life, i.e. by being mobile and using networks around the globe. This increases the main attack surfaces that can adversely be used.

In the same era, user organizations are increasingly using ICT services from ICT service providers instead of producing these ICT services “in-house” by themselves. Reasons for this include wanting to reduce costs and increase flexibility and quality. Having started with “outsourcing”, over the years the trend has

accelerated and intensified to be described as "cloud computing". Application and data have become mobile and collaboration between enterprises, public authorities and different types of users has become more important than ever. So, it's now up to the ICT service providers not only to support the businesses as required, but to integrate security measures in order to reduce associated risks to an acceptable level, at affordable costs. Customers are demanding reliability and seeking trustworthy dependable suppliers offering secure ICT services.

The task of securing ICT services is not an easy one. Technology is complex; requirements vary considerably, and industrial and competitive production results in constraints. For a long time now, T-Systems has made data protection a top priority. However, enforcing this in production and service delivery is far from easy, not only in large-scale ICT production. T-Systems therefore started to develop a systematic holistic approach and continued to add all the necessary ingredients to the architecture to make ICT services really secure. The key results are presented in this book. The book is intended to help implement security measures throughout a complex ICT delivery infrastructure in organization, processes and technology, from design to service management, while taking into consideration effectiveness as regards customer requirements and efficiency relating to costs. The book should also help user organizations to understand the security aspects of ICT production and to select the correct provider and the correct services in terms of information security. In this way, the workable architecture presented here aims at finding a balance between buyers and providers: requirements and deliverables must correspond. "Secure ICT Service Provisioning for Cloud, Mobile and Beyond" is of utmost concern to both partners.

Reinhard Clemens

Member of the Board of Management at Deutsche Telekom

CEO of T-Systems

Preface

The management of information security in a large organization is not a task that can be described simply as the implementation of individual security measures or the definition of security policies. The first steps in a large enterprise are the set-up and maintenance of what is known as an Information Security Management System (ISMS) as specified in ISO/IEC 27001. Major elements include the definition of scope, setting up risk management, raising awareness for security, monitoring and effectiveness control, auditing, as well as the clarification of management responsibilities and roles.

Corporate security management has to coordinate different areas including production security, privacy, audit management, risk management, and business continuity management. Specific programs need to be planned, executed and continuously improved for these different topics. The coordination and interconnection of these programs is fundamental. The execution of a security awareness campaign may be seen as an example. This needs to be coordinated with the line management concerned with this campaign and with Human Resources at least. The training itself is often performed globally and in various languages, preferably reaching all employees and managers of the enterprise.

The scope of information security management is explicitly not limited to the ICT services that may be produced for the market. The ISMS covers all business processes of the corporation and all its departments, including all employees. Corporate security management is a huge task in a globally active corporation. The tasks are characterized using terms such as coordination, support, definition of criteria, set-up of processes, provision of tools, planning and documentation, as well as control of performance, effectiveness, quality, adherence and compliance. Such corporate security management and its ISMS have a primarily enabling function. Accordingly, they work on a rather high process level and do not control all the specific security measures that are implemented in ICT production.

However, the task of making ICT services secure is important and mission critical for any ICT service provider paid to deliver secure ICT services for cloud, mobile and beyond. Such providers are challenged to use the above ISMS framework to turn requirements into real material security in a way verifiable for customers. This puts leading ICT service providers in a very specific and (does it surprise anyone?) very complicated and truly complex situation. The reasons are easy to see. The provider is facing an almost unmanageable multitude of different sets of requirements that are all to be met by its single ICT service delivery infrastructure.

The provider usually operates within various layers of security requirements – those set out by the service company itself and those required by its customer. The security requirements are of various origins. Some customers use their own best practices or risk management approaches, others implement industry security standards, such as Basel II, SAS70 Type II/SSAE16 and SOX, ISO/IEC 27002 and PCI DSS control sets, NIST standards and other requirements and recommendations of federal authorities that vary from one country to another as well as regulations for privacy, accounting and taxation. The provider has to implement them all and write reports demonstrating compliance according to ISAE3402 and various other directives.

In the past, this was managed in "customer silos". But security requirements have dramatically increased in number, coverage and depth in recent years. At the same time, the customers of the ICT Service Provider demand a significant cost reduction while retaining or even enhancing performance and flexibility and at the same time being provided with more security transparency and assurance. The solution to this situation can only be a fundamental modernization of ICT and the transfer of the customer silos to multi-customer platforms.

This situation was the starting point some time ago when some security managers from T-Systems sat down together sat down together with the authors of this book to discuss precisely the issues described above. We decided to take a big step forward. We invented the idea of "industrializing security" or adapting ICT security to an industrialized ICT production method. That was the birth of ESARIS, the subject of this book. That approach and its realization have proven to be very successful. We decided to publish large parts of the work in order to contribute to "Secure ICT Service Provisioning for Cloud, Mobile and Beyond". At the same time, we want to encourage customers and a wider audience to discuss the concepts and to adapt useful ideas. In this way, the industry should be able to progress in balancing the requirements of user organizations and the measures that are provided by ICT service providers.

Sebastian Winterstein
Chief Security Officer
T-Systems

Thomas Speichert
Head of IT Production Security Management
T-Systems, Computing Services and Solutions

Table of Contents