Secure by Design: Knowledge of threats and vulnerabilities

Contents

Historically, the design of IT infrastructure did not always account for the importance of security. System qualities such as "fast, cost-efficient or highly scalable" were prized ahead of "secure". However, as our world has become increasingly more instrumented and interconnected, the incidence of cyber crime and data theft have only increased. Now, customer trust has intangible business value, and as soon as an IT environment is exploited, or revealed to have problems protecting information, that trust can vanish. When customers begin to lose confidence in a business's ability to protect personal data, the speed, efficiency and scalability of a system no longer matters.

Businesses and governments need a smarter approach to IT security. The costs (both financially and otherwise) of trying to apply security as an afterthought are simply too great. For a more efficient, protected and streamlined IT environment, security needs to be an integral part of system design. That is why IBM Security Solutions are built on the philosophy of Secure by Design, a philosophy which states that IT infrastructure should be designed, created and operated with security constantly in mind. IBM cites three primary components to creating, and maintaining, a secure infrastructure:

- Knowledge of threats and vulnerabilities
- Structural elements
- Ongoing validation

The first of a three-part series, this executive summary whitepaper reveals how IBM helps clients understand threats and vulnerabilities so that they can more effectively apply the Secure by Design philosophy to their IT environments.

Understanding threats and vulnerabilities

For an organization to understand the level of risk that a system or component will face once it is deployed, that organization needs to first understand the threats that exist in the world the system or component is being deployed into. IT security risks are constantly evolving and maintaining a current understanding of their potential impact, likelihood and mitigation requires a significant level of both commitment and knowledge. IBM's understanding of threats and vulnerabilities is supported by a broad portfolio of offerings and this paper will look at the following three interconnected examples:

- IBM experience in computing and addressing security challenges for clients
- The IBM X-Force® security research and development team
- The IBM Rational® AppScan® product family for web application security testing

IBM experience in computing systems and security challenges

With more than a century of experience designing and implementing computing systems, IBM has helped shape the technological world. This experience translates to a deep knowledge of IT systems and the business processes they support—how they work, how they interact and where inherent weaknesses lie. In nearly every industry, IBM has experience working with the underlying technology systems that support business. Through the course of its history, IBM has worked through a wide variety of technology security challenges. As a result, when a business faces a new security concern, it is likely a concern that IBM has not only seen elsewhere but also already understands.

IBM's commitment to understanding threats and vulnerabilities is also reflected in the company's acquisition strategy. In 2007, IBM acquired Internet Security Systems (ISS), a company at the forefront of Internet security, cyber threats and vulnerability research. Just as IBM was involved in the origins of computing, ISS was a key player in the early years of Internet security, with a team of world-renowned security researchers called X-Force.

The IBM X-Force security research and development team

The IBM X-Force team is one of the best known, and most well-respected commercial security research groups in the world. X-Force security experts are dedicated to the ongoing research, documentation and evaluation of vulnerabilities and Internet security issues. Not only does the X-Force team discover and report vulnerabilities in software and systems, they also partner closely with development teams to ensure that security research becomes reliable security technology. With the rapid rate of new vulnerabilities and exploits, the X-Force team is an integral part of IBM's understanding of the security landscape. It is this knowledge that empowers IBM to educate clients, and the media, about the nature of security weaknesses in IT systems.

IBM X-Force maintains the most comprehensive threat and vulnerability database in the world—dating back to the early 1990s. It represents thousands of hours of research by the X-Force team, and much of the data is used to power preemptive protection delivered by IBM Security Solutions. The X-Force team regularly and automatically infuses new security intelligence into IBM security offerings—on average 341 days ahead of the latest threats. With X-Force security intelligence applied to its products, IBM clients are less likely to have their systems and services interrupted by malicious threats. To further educate clients, governments and the public at large, the X-Force team produces Internet security reports throughout the year.

IBM Rational AppScan solutions for web application security testing

As reported by the X-Force team, more than half of all new vulnerabilities occur in web applications, creating one of the largest attacks surfaces for cyber criminals. Many organizations depend on web-based software to run their business processes, conduct transactions and deliver increasingly sophisticated services to customers. Unfortunately,

in the race to meet deadlines and stay ahead of the competition, some businesses fail to perform adequate security testing.

As a result, companies unwittingly expose corporate or customer data to cyber criminals through existing vulnerabilities that could have been mitigated. And since many regulatory requirements mandate a degree of application security, these organizations risk non-compliance with audit requirements, which can result in fines and customer backlash. To help protect valuable information assets, it's important to test web applications throughout their entire life cycle—during development and once in production. Organizations should also encourage security awareness among development and testing teams. Identifying the privacy and security characteristics of the data/application and assessing the value of the data will drive the priorities for mitigating risk.

To be most effective, Rational AppScan should be used in the pre-production stage of application development. Numerous cases document companies spending millions of dollars to recover from a cyber-attack. Finding vulnerabilities in the production environment can cost 100 times more than fixing issues during development. By applying Rational AppScan web application security testing during the beginning stages of application development, clients can detect and correct vulnerabilities sooner than ever before.

Rational AppScan developers engage constantly with X-Force researchers to understand which web application security threats and vulnerabilities are most significant. As a result, Rational AppScan solutions enable IBM clients to take a smarter, more secure approach to application design and development.

Implementing knowledge of threats and vulnerabilities

IBM Managed Security Services (MSS) provides 24/7/365 monitoring and management of security technologies housed in the client's environment. While IBM MSS offers everything from device management to a web-based operation portal, this section will continue to focus on how IBM is helping our clients understand the evolving threat landscape.

By partnering with the X-Force team, MSS is able to take the most up-to-date information on the emerging threats and vulnerabilities and bring that content to clients in a way that is meaningful to them. MSS offers customized threat and vulnerability reporting based on individual client needs. Their daily assessment features a quick glance at what's going on in the world today along with information on the current alert level. When the alert level is at its lowest, it means that what MSS is monitoring (a combination of X-Force input and external resources) is showing everyday compromises. However, when the alert level rises, it signifies that something is happening that requires increased vigilance. MSS not only then reports these issues to clients, but works closely with them to say, "this is what is going on and here is how we can protect you."

Making IT infrastructure Secure by Design

The Secure by Design philosophy encompasses knowledge, tools and processes to generate components and systems that will perform reliably and securely throughout their life cycles. Secure by Design can also refer to a responsibility, or mindset, on the part of businesses and governments to make systems more inherently secure. Knowledge of threats and vulnerabilities is critical to both understandings of Secure by Design. IBM is committed to educating clients on the importance of security, and to delivering the cost savings and benefits of secure development. Through its nearly 100 years of computing and IT experience, its world renowned IT security research, and the collaboration between research, products and service delivery, IBM is helping to make "secure" as natural a characteristic of the Smarter Planet as "fast, stable or easy-to-use."

For more information

To learn more about Secure by Design: Knowledge of threats and vulnerabilities, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
September 2010

WGE03001-USEN-00