FROST & SULLIVAN

IBM Podcast: Security: Internal and External Strategies

Pod Cast

"We Accelerate Growth"

Introduction

Security is one of the most talked about issues in business today. It is a broad term and encompasses the security of internal confidential information, as well as external customer data and use of web pages and applications. As businesses have grown increasingly dependent upon the web to provide services to customers, employees and partners, these complex applications have become more difficult to secure; the potential for breaches is high along the information chain. Moreover, regulatory compliance has relatively recently put an unprecedented focus on the necessity of sound security controls. In just one example of several where a company failed to secure its date with damaging consequences, un February of 2005, Bank of America disclosed that it had lost the credit card information for 1.2 million clients.

In today's podcast we will focus on strategies and solutions for comprehensive and effective security both inside and outside an organization.

The Complexity of Security

The issue of security can be a complex one for a company. Indeed, external regulatory compliance is only one element within it. An organization must be certain it is providing secure data and avenues for its customers. This is a key part in ensuring customer satisfaction and, ultimately, a healthy bottom line. A proactive approach is necessary to address regulations and standards including Sarbanes-Oxley Act, Basel II, the Gramm-Leach Bliley Act, or the USA Patriot Act. Businesses must ensure that financial systems are ready for audits at any time by establishing and enforcing business controls across the enterprise.

An organization must be aware of threats from everywhere, at all points in the network. Data privacy and protection is crucial, whether it is within a company file, or a customer's personal information on a public site. Confidential information must be protected at the source and wherever it ends up and in travel – in a database, across a network or the web, and ultimately when stored. In the financial services industry for instance, the internet and online banking is a key part of growth for companies. However, one of the major restraints of online systems for financial services companies continues to be the customer's security concerns. Particularly in banking and insurance companies, the provision of a secure online system is fundamental in cultivating long-term customer loyalty and retention. In addition, there are now global standards to which businesses must adhere, such as the Payment Card Industry Data Security Standard (PCI DSS). Merchants and service providers must validate compliance.

Conduct Thorough Security Assessment

Before creating policy and implementing strategy, an organization should conduct a thorough security assessment. First, determine the specific challenges for its business as different businesses will have different security needs. As discussed, financial services companies are heavily regulated, but another type of organization may not have to comply with such strict standards, but must focus on securing its mobile devices thoroughly. Whatever the industry, breakdown each component and apply a security strategy that addresses all of them. The web application lifecycle includes four stages: inception, elaboration, construction and transition, and security must be addressed throughout. The pressures of competition in the marketplace will often motivate organizations to push web applications through these phases without adequate testing, which can lead to serious vulnerabilities and place the business at risk. To mitigate the risk, development and delivery teams must address the security of their websites throughout the lifecycle by taking the next step, and addressing the many layers.

Employ a Comprehensive Approach to Security

Employing a comprehensive approach to security will ultimately simplify the process for an organization. An end-to-end security and compliance solution with integrated products and services can ensure proper management and reporting. There are several layers of security to peel away and examine, confirming encryption and authentication where needed. Since a breach can come from anywhere with the proliferation of wireless devices which employees may use for mixed purposes – personal and professional – the potential for negative effects on a company's network is significant. In today's environment, such a violation can impact the bottom line, as well as its reputation.

Integrate security management across multiple and varied systems. This is where the methodical, layer by layer approach is vital. In addition, regular testing is necessary going forward. Companies must also support ongoing compliance efforts with strategic and scalable solutions. A service that is flexible and can grow with a company can provide a competitive edge.

Conclusion

In summary, key takeaways from this podcast are: The complexities of security can be navigated with an automated, yet flexible, service. Software and systems delivery teams need to think defensively – focus on the protection of proprietary information, data and trade secrets, in addition to ease of use for the customer. An eagle's view at the outset when creating policy is helpful. Finally, no web application can be truly secure unless the elements within its operating environment are secure as well.