White Paper Executive Summary

Top Security Rules for Cloud Systems

Safeguarding Cloud Applications and Data

Early high-profile cybercrimes were typically perpetrated via Denial of Service (DOS) attacks, where the attackers would render a service unavailable by simply overwhelming it with queries, or by Distributed Denial of Service (DDOS), where perpetrators would hijack PCs and use them to flood a service with more queries than they can handle, thus taking the service offline. Frequently, while victims were focused on countering the attacks, the perpetrator used the distraction they caused to access other systems in the network or unleash another exploit.

With the advent of the millions of Internet-connected devices that comprise the IoT, cybercriminals now have a target far larger than ever before. Well-publicized cyber-attacks on key infrastructures, like power grids, nuclear power plants, and transportation systems, are becoming more common.

This white paper outlines the most common cyber-attack methods – social engineering, viruses, and exploits – and describes 12 security rules to protect against these methods.

Furthermore, recent threats against cloud applications are exposing vulnerabilities that enable the theft of private data, as has been seen in many recent attacks to major retailers and institutions. Most cloud applications run on webservers like Apache httpd or IIS or application servers like Tomcat/TomEE, Glassfish, JBoss, or Websphere. If there is an exploit for one of these servers or even for the underlying operating system, a hacker would have an opportunity to attack all cloud applications using that technology.

While cloud-based applications will never completely replace on-premise solutions, they do create new challenges for providers trying to operate their cloud services safely and securely. One key question exists: Who operates the cloud? Do independent software vendors themselves need to have the solution ready, or can they cooperate with a trustworthy partner? The next priority is to safeguard availability and protect against attacks. When third parties, like clients or remote partners, are entrusted with running your application, the means to fight back against piracy also come into the equation.

As a provider of security technologies and a dedicated cloud solution for the creation and distribution of licenses, Wibu-Systems is an experienced and reliable partner for every step of the journey from the first design to the implementation and safe operation of your licensing needs.

5062-011-02/20190821

sales@wibu.com | www.wibu.com

WIBU SYSTEMS