BOMGAR™ WHITE PAPER

Could Your IT Support be Compromising Your IT Security?

A BOMGAR WHITEPAPER

© 2003-2011 Bomgar Corporation. All Rights Reserved

Could Your IT Support be Compromising Your IT Security?

A BOMGAR WHITEPAPER

TABLE OF CONTENTS – A BOMGAR WHITE PAPER

© 2003-2011 Bomgar Corporation. All Rights Reserved

EXECUTIVE SUMMARY

Organizations are increasingly storing more and more critical information assets, such as intellectual property, proprietary corporate data, trade secrets and customer data records electronically. As a result, the risk and costs of a data breach are now higher than ever before. In fact, the Ponemon Institute's *2010 Annual Study: U.S. Cost of a Data Breach* report found that the average cost of an organizational data breach increased to $7.4 million and cost companies an average of $214 per data record. That's a significant increase from 2009, when the cost per compromised record was $204 and total organization cost per breach was $6.8 million.

How can companies protect themselves and their customers from security breaches? It is critical that organizations understand the attack vectors that malicious hackers use to gain access to computer systems. The Ponemon Institute's *Cost of a Data Breach* report indicates that 39 percent of data breaches involve third-party outsourcers, an especially troubling statistic as the trend towards SaaS and third-party hosted technology continues to grow. Much of the time, the breaches occur because the third-party isn't behaving or thinking like the company(s) for which they do business, especially those with strict regulatory or industry compliance standards.

> *The Ponemon Institute's Cost of a Data Breach report indicates that 39 percent of data breaches involve third-party outsourcers, an especially troubling statistic as the trend towards SaaS and third-party hosted technology continues to grow.*

One particular technology that is often a factor in these types of breaches is remote access or support technology. In fact, the *2011 Verizon Data Breach Investigations Report* found that for data breaches involving hacking, remote access and desktop support service solutions are the most commonly exploited attack vector, accounting for an astonishing 71 percent of all of the hacking attacks that Verizon assessed. Not surprisingly, most of the remote access solutions named by the report were point-to-point or SaaS solutions where the information is stored in data centers not under the company's direct control.

This paper will examine the data breaches caused by these remote access and support applications and include specific design and deployment techniques to minimize the associated risk. It will also discuss licensing models, data storage, credential authentication and client network connections. It will conclude with a case study of the security offered by the Bomgar solution.

ANATOMY OF A DATA BREACH

When they swipe their card at the check-out counter, consumers usually don't pause to consider what sensitive or personal information is associated with their cards. Nor do they ponder who might have access to such details. Customers are often unaware of the number of parties that have access to their data.

© 2003-2011 Bomgar Corporation. All Rights Reserved

When organizations need to access their company's computers — be it point of sale terminals, databases, Web servers, or personal computers — businesses frequently turn to remote administration applications as a cost effective way of managing and fixing their systems. With these types of remote access tools, users can essentially access any device, server or application within the organization, making them an obvious gateway for hackers. Unfortunately, many of these solutions were not designed with security as a first priority, leaving a number of vulnerabilities to be exploited.

First, a majority of remote access and support tools are offered as SaaS solutions, meaning that all of the data is passed through the vendor's off-premise servers. Most companies are very particular about which data they put in the cloud and which must be kept behind company firewalls. But by putting their remote support solution in the cloud, they've essentially opened the door for all data to exist in the cloud. Second, many solutions use a named-seat licensing model, which encourages the use of shared and generic credentials and reduces accountability for IT support technicians. Finally, many remote support products leverage inbound or peer-to-peer connections to access remote systems. In these cases, a port on the end-user's system must essentially be left "open" for whenever an IT rep wants to connect, which also opens an easy attack pathway for hackers.

Bomgar, an on-premise based remote support solution, was architected to be a secure, enterprise-class remote support solution. Its roots lie in the support of security-conscious enterprises, including government and financial institutions, as opposed to the consumer market, for which many of the other remote support solutions were designed. Because of the initial design objectives, Bomgar is significantly less subject to the security vulnerabilities inherent in other remote control solutions specifically identified in the *2011 Verizon Data Breach Investigations Report*.

> *But by putting their remote support solution in the cloud, they've essentially opened the door for all data to exist in the cloud.*

DATA CONTROL: ON-PREMISE VS. CLOUD COMPUTING

Several issues need to be taken into account when selecting a remote support solution, one of them being who controls the data. It is important that the data accessed via remote support is always under the control of the company that owns that data. Unlike other remote support solutions mentioned in the *2011 Verizon Data Breach Investigations Report*, Bomgar is appliance-based, so all data remains under the control of the customer. This is a significant benefit for companies that must, for example, conform to the requirements of the Payment Card Industry (PCI) Data Security Standard (DSS), which holds the customer responsible for payment card data even when third-party outsourced solutions are used. The customer is liable for any data breach even if the breach occurs at the outsourcer. If the data is stolen via the remote support application, the customer remains liable for the theft, not the remote support software provider.

© 2003-2011 Bomgar Corporation. All Rights Reserved

One advantage to appliance ownership is that enterprise directory integration is possible without requiring a company to open outside access to their domain controllers. This integration permits the service desk technicians to authenticate to the remote access solution using their tightly controlled enterprise credentials, not arbitrary login credentials assigned by a SaaS vendor. Along with the centralized authentication, the remote access privileges are also managed through the directory. Such enterprise directory credential management is not usually available with outsourced solutions because of the risk in allowing outside connections into the enterprise directory. When the remote administration appliance resides within an enterprise's own network infrastructure the risk associated with opening ports to outside vendors is removed. The huge benefit with Bomgar's owned-appliance approach is that the organization does not have to expose its enterprise directories to outside entities.

> *When the remote administration appliance resides within an enterprise's own network infrastructure the risk associated with opening ports to outside vendors is removed.*

LICENSING MODELS

The licensing model used by most software vendors presents an inadvertent threat to data security. A commonly used method is the named-seat model, employed by a number of popular remote support vendors. The named-seat model forces the customer to purchase a set number of licenses, regardless of how many will be used simultaneously. In order to reduce costs, the named-seat model encourages the use of shared credentials, making it very common to see generic remote control login identities such as "Tech001," "Tech002" and so on. When a service technician needs remote control/ access, that technician simply uses an available credential. This leads to two liabilities. First, accountability is lost between the actions undertaken in the support session and the specific individual technician. Second, passwords associated with the shared credentials are rarely updated, which introduces an enormous vulnerability as individuals change responsibilities within an organization or leave the company.

In contrast, Bomgar's concurrent licensing model is based on the number of service desk technicians active at any one time. It doesn't matter how many service desk technicians are *authorized* to use the software; if only 100 technicians log in at any given time then the customer needs to purchase only 100 licenses. Beyond having significant cost savings for customers delivering 24/7 service, the concurrent model has an additional security aspect that isn't necessarily obvious.

CREDENTIAL AUTHENTICATION WITH CONCURRENT LICENSING

The concurrent licensing model is an even stronger bulwark against data breaches when coupled with technician credential authentication through an enterprise directory such as Microsoft Active Directory. Enterprise directory authentication provides two main benefits. First, the technicians authenticate to the remote support solution using the same credential they use to login to their workstations, thus eliminating the requirement to remember a separate credential, as well as credential sharing between technicians. Second, with enterprise directory authentication there is no added burden of credential management as the authentication to the support software is managed as a by-product of normal enterprise directory activities.

© 2003-2011 Bomgar Corporation. All Rights Reserved

The customer can also seamlessly manage technical privileges through group membership within the enterprise directory. So, for example, if a service desk technician is promoted from first-tier support to second-tier support, the change in the directory security group would automatically change their privileges within the administration software. Similarly, if the technician leaves the support team altogether the change in security group would automatically remove their ability to access. Finally, and most importantly, when an individual leaves a company his or her enterprise directory credential would be disabled as part of the exit process. Disabling the credential immediately removes his or her ability to access remote systems and potentially cause damage.

The named-seat model, on the other hand, has manual administrative overhead associated with technician credential management. Failure to remove named-seat access for former employees can be a major attack risk, especially among former employees who are disgruntled.

CLIENT NETWORK CONNECTIONS

There are multiple ways to initiate sessions with the connections to remote appliances – *inbound to* the client or *outbound from* the client. If the connection is an inbound connection to the client, the client must constantly have an open listening port on the computer. The ideal method is to have the remote support client initiate an outbound connection *from the client to the appliance*. Open listening services on Internet-connected computers are a major source of compromise. Additional security can be added by encrypting the connection using the public key portion of the SSL certificate of the Bomgar appliance. This means that *only* the Bomgar appliance can decrypt the data. Thus, the Bomgar client connection is essentially immune to any type of man-in-the-middle (MITM) attack.

Additionally, all client connections, whether that of the remote computer receiving support or from the service technician providing the support, terminate at the Bomgar appliance. There is no peer-to-peer connection exposure to allow the service technician to establish a direct unsupervised, unaudited connection to a remote customer.

BOMGAR SOLUTIONS AND RESULTS

As previously mentioned, because the Bomgar solution sits behind a company's firewall, it gives complete control and ownership of all data to its customers. With the appliance-based approach, sensitive data never passes through a third-party server. The Bomgar remote support solution centralizes all data and audit logs on-premise, avoiding the security risks inherent to SaaS-based alternatives.

> *Because the Bomgar solution sits behind a company's firewall, it gives complete control and ownership of all data to its customers.*

© 2003-2011 Bomgar Corporation. All Rights Reserved

In fact, Bomgar is the industry's only remote support provider to achieve FIPS 140-2 Level 2 compliance for its complete solution. This means the Bomgar solution meets stringent requirements set by the National Institute of Standards and Technology for both hardware and software, demonstrating Bomgar's extensive commitment to security. As a result of this certification, Bomgar can offer government agencies and heavily regulated industries the most secure remote support solution on the market.

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

CASE STUDY: THE JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LAB

The Johns Hopkins University Applied Physics Laboratory (APL), a not-for-profit center for engineering, research, and development, solves complex research, engineering, and analytical problems that present critical challenges to the United States.

After careful evaluation of its support services, the Information Technology Support Department, or ITSD, learned that their IT remote support solutions were substandard in terms of security and reliability. As a federally funded research site, the Lab often works with sensitive and classified information from various government agencies, including the Department of Defense and NASA. Therefore, security is critical and ITSD discovered some security concerns related to their existing remote support solution.

The ITSD team performed analysis on several remote support solutions, testing them for reliability, security and functionality. As a result of APL's rigorous security standards, no third-party applications could be involved with the remote support solution. Bomgar met these security standards because it retains all support session data onsite, requires session permission from the user and enables ITSD to maintain a complete audit trail through session recording. In addition, Bomgar provided the ITSD team a remote support solution for the various platforms required.

© 2003-2011 Bomgar Corporation. All Rights Reserved

ABOUT BOMGAR

Bomgar is a worldwide leader in secure, appliance-based remote support solutions. The company's award-winning solutions enable organizations to improve IT support efficiency by securely accessing and managing virtually any system – Windows, Mac, Linux, BlackBerry, the iPhone, iPad and most versions of Windows Mobile, regardless of their location. More than 5,500 companies around the world have deployed Bomgar's enterprise-class solutions to rapidly transform their IT support functions and significantly improve operational efficiency and customer satisfaction while dramatically reducing costs. Bomgar is privately-held with offices in Jackson, Atlanta, San Francisco, Washington D.C., Paris and London. In 2010, Bomgar was named one of the fastest-growing technology companies in America by Deloitte.

CONTACT BOMGAR | www.bomgar.com | info@bomgar.com

BOMGAR CORPORATION

Corporate Headquarters
578 Highland Colony Parkway
Paragon Centre, Suite 300
Ridgeland, Mississippi 39157
1-601-519-0123

Atlanta
11695 Johns Creek Parkway
Suite 200
Johns Creek, GA 30097
1-770-407-1800

San Francisco
1686 Union Street
Suite 212
San Francisco, CA 94123
1-415-800-8032

Washington D.C.
11921 Freedom Drive
Two Fountain Square, Suite 588
Reston, VA 20190
1-703-736-8361

Paris
54-56 Avenue Hoche
75008 Paris
France
33.(0) 1 .56.60.50.88

EMEA Headquarters
Oakridge House
Wellington Road
High Wycombe
HP12 3PR
United Kingdom
44 (0) 1 494.557.350

© 2003-2011 Bomgar Corporation. All Rights Reserved