



State and Local Governments: Get Serious About Web Abuse and Cyber Security Threats

By The Forsite Group

INTRODUCTION

When word surfaced in April 2008 that some workers in Tennessee had used their office computers and Internet connections to post more than 600 Wikipedia entries, it seemed like just another case of workplace Web abuse. What made it newsworthy? Those involved were state employees—whom taxpayers had every right to expect were spending time on important government matters, not wasting it on “Three Stooges” and “Star Trek” trivia.

Unfortunately, it was not an isolated case. It also underscores the unique challenges that state and local government agencies face when it comes to workplace Web use, abuse, and security. While government organizations require cutting-edge communications to achieve gains in efficiency, productivity, and cost-effectiveness, they also have a special covenant with their “customers”: Operate solely in the best interests of citizens while working continuously to preserve their trust.

Meeting that mission isn’t always easy. First, there are the realities of workplace Internet habits. The Ethics Resource Center’s National Government Ethics Survey (NGES) recently found that Internet abuse accounts for nearly 25% of the ethical misconduct observed within state and local agencies. Then there’s the growing sophistication (and increased incidents) of cyber security attacks. The state of Georgia says it beats back more than 10,000 attempts every day to break into state information systems. That kind of one-two punch raises the likelihood of sensitive data falling into the wrong hands, while potentially undermining compliance efforts, putting the network at risk, increasing exposure to liability, crippling productivity, and threatening legislative initiatives.

So how can state and local agencies mitigate against bad habits and today’s top threats? First, educate employees on what constitutes good online behavior—and on the dangers that lurk beyond the gateway. Visits to unauthorized sites or misuse of applications open the organization to a variety of vulnerabilities, from botnets to spyware and viruses. Second, take a fresh look at the acceptable use policy (AUP): Is there a clear one in place? Do employees know about it? And does your organization have a way to enforce the AUP effectively and proactively?

Finally, deploy technology that supports those efforts—which is where Web filtering can definitely help. State and local agencies should look for a Web filtering solution that:

- Features flexible, detailed, and real-time monitoring and reporting, which enables a proactive approach to protection and more effective enforcement of the AUP—while ensuring compliance efforts
- Deploys as an appliance rather than software, thus offering better performance, greater scalability, and lower total cost of ownership (TCO)
- Uses URL filtering supported by signature/pattern-based detection to preview access to unauthorized Web content and applications

THE SHIFTING MANDATE

These days, state and local agencies find themselves tasked with a lot more responsibility than they once were. It’s a fact buttressed by the findings of the U.S. Department of Labor’s Bureau of Labor Statistics: As population increases and the federal government offloads the handling of services it once provided, state and municipal governments are getting bigger—and busier.

- Consequently, they require broadband connections, communications applications, and the other tools that can help them accomplish a range of tasks, including but not limited to the following:
- Connecting with citizens to streamline tasks associated with documentation like driver’s licenses, vehicle registration, jury duty, and voting
- Disseminating information in the event of natural disaster or other event
- Researching news, records databases, and other online resources for information necessary to policymaking
- Completing clerical functions like arranging for staff travel or procuring supplies
- Recruiting and hiring employees through job sites or social networking sites

ON THE TAXPAYER'S DIME

But even as more government employees are using the Internet to do their jobs better, more are apparently abusing their Internet privileges. With 50 state governments and more than 87,000 municipal government entities across the U.S., comprehensive statistics are tough to come by. But anecdotal evidence suggests that misbehavior is widespread.

In a 2007 hearing before Virginia's Department of Employment Dispute Resolution, a former supervisor in the Virginia Department of Social Services testified that Internet abuse among employees was an "agency cultural problem"

In response to a public records request, the Massachusetts Turnpike Authority reported that employees made 6,864 Web visits to Amazon.com, Facebook.com and MySpace.com in 2007

A Department of Transportation official in Pennsylvania with a salary of \$84,000 was fired after distributing inappropriate content he downloaded from the Internet to other employees by e-mail. The story doesn't end there, though: Because the state's Civil Service Act makes such a firing difficult, the employee was reinstated at a lower salary. The employee fought on, eventually winning his old job and salary back—while the state footed the bill for the litigation

Governments are sure to face greater challenges on this front as the next generation of employees comes to work. Raised in the Internet age and accustomed to round-the-clock Web access, they're not likely to draw as stark a line between their personal and professional activities as their elders. At the same time, governments can't afford to alienate this pool of potential labor; rather, they need to entice new workers as their workloads increase. Consequently, they need the flexibility that will help them strike a balance between unfettered surfing and productive, job-related Internet use.

THE THREAT LANDSCAPE

State and local agencies also must deal with a range of evolving, sophisticated cyber security threats. The good news is that they are becoming more aware of—and getting more serious about—the dangers they face. Members of the National Association of State Chief Information Officers (NASCIO) now put security at or near the top of their lists of priorities; further, according to a survey by Government Technology, 60 percent of state and local respondents have established a chief information security officer (CISO) or similar position.

The bad news? State and local agencies seem lacking in knowledge about the types and severity of threats they face—which means they're at a disadvantage when it comes to defending against them. Following are some of the newest and most potentially damaging cyber security threats.

Bots and Botnets

What they are: Also known as Web robots, crawlers, or spiders, bots are simple software scripts used to run automated tasks over the Internet. These include searching for content, posting messages to multiple newsgroups, or

sifting through data to make online comparison-shopping possible. They serve numerous, legitimate commercial purposes—as well as nefarious ones.

Why they're a problem: Bots infect computers surreptitiously. They land on user systems through visits to unauthorized sites, by clicking on links in suspicious e-mail messages, or even by mousing over compromised banner advertising. Bots are built to elude detection, morphing as they travel so that most anti-spyware, -spam, and -virus packages can't catch them.

The real trouble begins when a bot's creator ropes individual infected computers into pools known as botnets. The combined computing power of these "zombie" machines is then harnessed to blast spam, launch denial of service (DoS) attacks, and mine vast stores of confidential data that can be stolen and sold to the highest bidder. Botnets are difficult to locate and disable because their operators constantly register and de-register the DNS addresses of individual nodes within the botnet.

The danger to government organizations: The big danger with bots and botnets is liability: As of now, the rules aren't clear on the responsibility of organizations whose computers have been used for blasting spam, launching attacks, or stealing data. Data leakage is another concern.

Proxy anonymizers

What they are: Simple scripts that allow users to bypass traditional Web filters and access sites that are officially off-limits. Also known as Web proxies, they're written in open source, allowing just about anyone to create them and making them more numerous than ever.

Why they're a problem: A proxy anonymizer masks the IP address of the user's machine, essentially becoming the "system" that actually requests the Web page. Because that masked system isn't visible to the network, the Web filter can't flag any of the requests made from it.

While proxy anonymizers help users gain access to any site they want, they're typically associated with efforts to reach social networking sites like MySpace and Facebook. In fact, many anonymizers were originally intended for just this purpose, aimed at students seeking to bypass the filters in their school libraries and classrooms. These students have become adept at using anonymizers, and they are now beginning to show up in the workforce.

The danger to government organizations: Abuse and productivity issues are major concerns when it comes to proxy anonymizers. Of course, if employees use them to access inappropriate content that is then distributed in the workplace, liability issues also arise. And unauthorized sites are also likely repositories for the kind of malware that can land on a user's machine and put sensitive data at risk.

State and local agencies must also contend with the continued threat of spyware—malicious programs that install themselves on computers to record interactions and intercept communications—that can put sensitive data at risk.

Phishing—an e-mail exploit that fools users into parting with valuable data by directing them to spoofed sites that look legitimate—also remains a potent risk. Instant messaging (IM) and peer-to-peer (P2P) communications introduce other vulnerabilities; since they function outside the traditional medium of secured e-mail, they raise the chances of data leakage, and thus the likelihood of regulatory violations and exposure to liability. And P2P poses particular problems in terms of bandwidth consumption and employee productivity.

ADDRESSING THE ISSUES

Clearly, state and local agencies face no shortage of challenges when it comes to Web use by their employees. Fortunately, there is a way to address them.

Begin by educating (and re-educating) workers on the dangers that lie beyond the gateway—and on the good habits that can help in avoiding those dangers. They shouldn't click on suspicious links. They shouldn't respond to e-mail come-ons. They should limit their IM chats to topics related only to work. When employees are aware of these and other best practices for communicating online, they're better equipped to protect both themselves and the organization they work for.

Also keep AUPs clear and up to date. As new threats emerge or new applications become the norm, governments should be able to revise their policies accordingly. Keep in mind that enforcement plays a major role: Employees should know that violating the policy will have consequences.

Finally, support these efforts with security Web filtering technology that delivers comprehensive functionality for fighting today's top threats. A good Web filtering solution should provide the following capabilities:

- Utilizes a comprehensive and up-to-date URL database
- Filters the Internet, including URLs and/or IP addresses, file types (like MP3, MPEG, .zip), HTTP, HTTPS, FTP, newsgroups, and TCP ports
- Provides activity overview and historical trending of Web traffic, as well as detailed forensic reporting that pinpoints policy violations and gauges user intent
- Blocks Internet threats, including spyware, malicious code, phishing sites, and botnets—proactively and in real time
- Blocks anonymous proxies, IM/P2P, streaming media, remote access applications and network games by using signature/pattern-based detection
- Permits customizable levels of restriction, from category lockout to complete quarantine prohibiting network access
- Retains archived records to satisfy legal requirements and aid in compliance with regulatory measures like CIPA, HIPAA, and Sarbanes-Oxley
- Helps optimize network bandwidth for mission-critical functions

With such technology in place, state and local agencies can improve productivity by eliminating visits to unauthorized Web sites. They can secure confidential information against threats like botnets. They can maintain network performance by managing access to bandwidth-intensive sites. And they can reduce the liability and legal costs associated with exposure to and dissemination of inappropriate or offensive content.

Most importantly, by addressing all of these issues together, governments can also accomplish their biggest goal: Strengthening the bond of trust they have with their citizens, and continuing in their mission to serve the taxpayer efficiently, economically, and ethically.

CONCLUSION

Expanding populations and added responsibilities are forcing state and local agencies to run themselves more like a business. This means implementing cutting-edge communication tools to streamline operations, increase productivity, and improve interactions with their “customers”—the citizens they're supposed to serve.

But governments are finding they face the same challenges as corporate organizations when it comes to preventing employee Web abuse and defending against emerging Internet threats. When workers are wasting time on unauthorized sites or when threats like spyware and botnets are compromising confidential data, elected officials risk losing the trust they've worked to establish with the voters who put them in office.

Fortunately, through a combination of employee education and enforcement of AUPs, state and local agencies can begin to address these issues. And when they supplement these efforts with the appropriate Web filtering technology, they can strengthen their defense against dangerous cyber security threats, help raise employee productivity, reduce bandwidth consumption, and improve regulatory compliance efforts while lowering exposure to liability.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters

828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific

Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Auckland, New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 09.01.09