TechTarget
Security Media

SearchSecurity.com SearchCloudSecurity.com SearchSecurity.co.UK SearchSecurity.in SearchFinancialSecurity.com
SearchMidmarketSecurity.com SearchSecurityChannel.com FINANCIAL INFORMATION SECURITY DECISIONS INFORMATION SECURITY

SearchSecurity.com

E-Guide

Expert guide to Web 2.0 threats: How to prevent an attack

A majority of today's organizations already leverage the benefits of Web 2.0 technologies, or at least wonder how they can take advantage of it. This expert e-guide provides an overview of what Web 2.0 really is and explains how to combat the myriad of threats that accompany this convenient technology.

Sponsored By: ArcSight™

TechTarget®
Where Serious Technology Buyers Decide

SearchSecurity.com

E-Guide

Expert guide to Web 2.0 threats: How to prevent an attack

Table of Contents

Web 2.0 security threats and how to defend against them

The threat landscape and Web 2.0 technologies

Resources from ArcSight

Web 2.0 security threats and how to defend against them

There is an old Chinese proverb that reads "may you live in interesting times." For security professionals, this does not ring hollow because a security career is always evolving and responding to emerging threats; "interesting" is our daily mission.

While our charge is broad, from architecture and policy, through awareness and compliance, much of what we do is defending against threats to the security of the information we protect. As the proverb tells us, this is where the interesting portion of our role gets defined. We have witnessed the evolution of threats migrate from attacking the vulnerabilities of the Web, through the weaknesses of messaging, on to data protection, and now into the realm of Web 2.0.

What exactly is Web 2.0? You would find a myriad of answers to this if you asked all of your security (and non-security) friends. It is now the Internet as we now know it, and is known as the second generation of the World Wide Web. Web 2.0 refers to Web design, development, and use that foster interactive information sharing, interoperability and collaboration on and via the Internet. Examples include Web-based communities, Web applications, social-networking sites, video-sharing sites, wikis, and blogs. A Web 2.0 site allows users to interact with other users, or even change website content, in contrast to non-interactive websites where users are limited to the passive viewing of information that is served to them.

Obviously, this is not the "push" Internet that we've sharpened our skills on, and with this next iteration come additional business opportunities, and security concerns. Chances are, your enterprise is either utilizing its power, or wondering how they can take advantage of it. Security needs to part of the conversation, no matter where you are in the process.

WEIGH BUSINESS NEED AGAINST WEB 2.0 RISKS

The collaborative, interactive nature of Web 2.0 has great appeal for business from a marketing and productivity point of view. Companies of all sizes and vertical markets are currently taking full advantage of social networking sites such as Facebook, Twitter and LinkedIn to connect with colleagues, peers and customers, or free online services such as webmail, Google Docs, and other collaborative platforms to share documents, best practices and message one another. "Ignore these technologies at possible business peril," says Diana Kelley, partner at Security Curve. "Not only are these technologies useful, but companies that don't adapt could well find themselves left behind the social revolution."

Companies are leveraging these sites for more than just communicating. Through Web 2.0 and social networking areas, enterprises are exchanging media, sharing documents, distributing and receiving resumes, developing and sharing custom applications, using social networks as a business strategy vehicle, leveraging open source solutions, and providing forums for customers and partners.

While all this interactivity is exciting and motivating, there is an enterprise triple threat found in Web 2.0: losses in productivity, vulnerabilities to data leaks, and inherent increased security risks.

I informally surveyed more than three dozen security colleagues across all verticals and found that 90 percent are concerned about these threats, and many have addressed (or are addressing) them through policy and technology. CISOs must find the delicate balance between security and the business need for these tools, and enable their use in such a way that reduces the risk for data loss or reputational harm to the corporate brand. While a sound security policy is a necessity in proactively responding to Web 2.0, policies must be enforced by technology.

The cost of dealing with a data breach continues to rise. In late January, the Ponemon Institute released its fifth annual study on the data breaches. The study reveals that the average cost to an enterprise from a data breach rose from $6.65 million in 2008 to $6.75 million in 2009. In addition, the average cost per compromised record also went up to $202, from $204 the previous year.

With the increasing value to data, and the numerous conduits that it can be breached, it's no wonder that increasing regulatory mandates and constraints have been enacted. Enterprises now have a list of laws to comply with, including Gramm-Leach-Bliley, the

Health Insurance Portability and Protection Act, Sarbanes Oxley, and the US Patriot Act to name just a few. Many states are also enacting stringent protection and encryption laws, such as California's SB 1386, and Massachusetts' 201 CMR 17.00, and businesses may be subject to these state-specific laws even if they are not based in either state.

The industry is starting to respond by developing and marketing standalone tools--or integrating protection into secure Web gateways, antimalware suites or UTMs--that filter for sensitive content and alert or block the action. Many have received excellent feedback, and industry analysts are quickly evaluating the tools and solutions available. One size does not fit all, however, and holistic thinking and documenting your expectations and success factors are critical.

NEW PARADIGM OF WEB 2.0 SECURITY THREATS

As with any evolution of a product or service, the old ways of performing a task or providing a solution simply may not work. This is also true in reducing and mitigating Web 2.0 threats. Time tested security solutions are no longer the key defense in guarding against attacks and data loss. Some characteristics of 2.0 securities that are being discussed are:

- Traditional Web filtering is no longer adequate
- New protocols of AJAX, SAML, XML create problems for detection
- RSS and rich Internet applications can enter directly into networks
- Non-static Web content makes identification difficult
- High bandwidth use can hinder availability
- User-generated content is difficult to contain

Security teams must be aware of the need to address Web 2.0 threat in their desktop clients, protocols and transmissions, information sources and structures, and server weaknesses. While none of these attack vectors are new, how we respond to them may be.

Very rarely does a week go by where we do not hear news of the negative aspects of social networking sites and collaborative platforms. Whether it is violence and lawlessness, cyber-bullying and harassment, or legitimate breaches of confidential data, it is apparent that this brave new world poses risks to companies. Many of the threats that lead to confidential data loss hijack employee credentials without their knowledge. While there are obvious threats that would not surprise even the most casual user of the Internet, others are more subtle and benign, and need to be addressed in our enterprises.

Direct posting of company data to Web 2.0 technologies and communities is the most common. No vulnerability need be exploited or malicious code injected when employees (whether as part of their responsibilities or not) simply post protected or restricted information on blogs, wikis, or social networking sites. According to many security companies, the attacks on these technologies are on the rise as well, knowing that their growth and fast maturation can be a jackpot for insider information. Many of these attacks also come via malicious payloads, which are downloaded when spam and phishing scams are utilized. According to Sophos, 57% percent (an increase of over 70% from the previous year) of people who use social networks report receiving spam and phishing messages. This number will surely continue to rise.

However, what about the risks posed by insiders who choose to utilize free webmail services, such as Gmail, Yahoo, Hotmail, and others? While allowing employees to access to these services during the workday most likely aligns with an acceptable use policy that allows "reasonable and limited personal use", the risk is what they are sending to these free mail services. They may be thinking that they are being good stewards of the company and sending data home to work on at night or over the weekend, but they are also placing the company at great risk. Not only are the transmission not encrypted, but the security of the servers may not be up to security requirements for the protection and value of the information. The data may be residing on several servers, and may not even reside in the country of origin or destination.

INCLUDE WEB 2.0 SECURITY IN ACCEPTABLE USE POLICY

Most enterprises already have a form of an acceptable use policy, which should govern the use of all resources in the enterprise computing environment. While it may be implicitly implied in your current policies that public 2.0 sites are covered (blogs, wikis, social networks), because of the nebulous nature of this technology, a more explicit rendering of the expectations and policies is necessary.

Critically read your current policy in a context of 2.0 technologies, and identify gaps that need to be addressed. For instance, because of the risks and inherent difficulty managing the use of social networking applications, many enterprises have made the decision to not allow access to social networking services and Web 2.0 powered sites from inside the corporate perimeter (often with the exception of human resources departments for recruiting purposes). This is an important decision because the information gained from these sites may be of corporate use. One security manager from a global manufacturer told me "there is no way we are going to design new ingredients for client products, and then prevent our employees from the public forums that enable us to gather the consumer experience."

Of greatest importance is a clear and unambiguous warning in the policy about sharing confidential corporate information. Enforcement of the policy can be made though analysis of Web logs for use during business time (if not allowed), or through automated searches of websites for corporate information. Many organizations have included Web 2.0 and data protection sections to their training on protecting corporate information. Ensure that the policy indicates the prohibitions against this, and clearly spells out the ramifications, including the levels of discipline that could occur. As always, when the acceptable use policy has been modified, ensure that all employees are made aware.

MAINTAIN YOUR TECHNICAL DEFENSES

Security success is all about combining the right combination of people, process, policy and technology. The same holds true when it comes to addressing Web 2.0 concerns. Utilizing this combination in a rapidly evolving area is difficult though. "This space is a reality and tough to fully monitor as there is a fine balance to levels of security rigidity and the inherent pervasive openness to Web 2.0", says Tim Young, vice president of information technology at Bright Horizons. Intrusion detection and intrusion prevention systems (IDS and IPS) need to be kept current to address the risks of this traffic, and bandwidth-shaping technology should be deployed in order to not only both maintain proper network speed, but also identify abuse or compromised machines.

In addition, many popular Web-based social network services have an increasing number of applications available to download locally. While many are benign, a significant number of these small apps carry malicious payloads, hacking tools or marketing software. This can be combated by having a standard desktop image that does not allow local installation of applications, or changes to the registry keys or operating systems. Lastly, firewall rule sets can be granularly defined to monitor, catch or block social network traffic, and of course, always ensure that antivirus products are up to date as a last line of defense.

Finally, even with all of these controls in place, data and information will inevitably find its way to the Internet. Enterprises should remain vigilant in scouring the Internet regularly for any information that may be sensitive in nature. Using third-party reputation protection services, internal monitoring programs, or simply performing Web searches for keywords and phrases can be essential in identifying and addressing instances when company information is made available via social communities, either inadvertently or intentionally.

DATA PROTECTION THROUGH OUTBOUND CONTENT MANAGEMENT

There are many vendors and solutions that promise to mitigate and solve the threat of data loss in Web 2.0 environment. While this technology area has shown great promise, and continues to deliver, it is oftentimes misunderstood as a CISO reviews the morass of materials and reviews available.

Data loss prevention, for example, is a solution, as well as a generic term that is an umbrella for many different technologies and strategies. Data loss can be prevented by encryption. It can also be mitigated or prevented by port blocking or content filtering. And there are software suites and appliances that can help in this area. Every security vendor of any size or maturity will gladly let you know of their DLP solution, and will use the term to cover just about all of their products. This doesn't make it any clearer.

A clearer definition can be simply stated as implementing an outbound content management program that reduces, mitigates, and eliminates data loss. The trick is how a company deploys systems capable of successfully detecting your highly sensitive information in the outbound mail system.

Also be aware of the types of DLP solutions, which fall into three broad categories: network based, host-based, and data identification. All three have their positives and negatives, and a CISO must remember that a performance hit will be observed on the network when a company runs any such solution inline. As with all security solutions, you need to strike a balance between speed, accuracy, and adequate coverage.

DLP solutions must be made aware of what a company lists as sensitive content if they are to be successful. Upon the sensitivity being listed, there are several ways in which the content can be identified, but first the solution must be able to open and understand numerous file types, and be able to detect content in nested and zipped documents as well. Once the files are opened and reviewed by the solution, content analysis is begun to identify any sensitive data. Content analysis techniques include:

- Pattern-based searches using regular expressions
- Fingerprinting by searching elements of actual databases
- Exact file matching
- Statistical analysis to search for content that may resemble sensitive data, or contain pieces of it
- Document matching for complete files
- Analysis of lexicons (ex. employment opportunities, insider trading, harassment)
- Solution supplied categories, to address regulatory mandates such as HIPAA and GLBA

WEB 2.0 SECURITY STRATEGY MUST MIX TECHNOLOGY, POLICY

Security teams must be aware of the need to address Web 2.0 threats in their desktop clients, protocols and transmissions, information sources and structures, and server weaknesses. While none of these attack vectors are new, how we respond to them may be. Our enterprises ask us to eliminate malware and protect our company's data, all while allowing productivity, improving IT efficiency, and proving compliance. We should be encrypting our data and protecting our endpoints, but not hinder the process of how we do business. Add in the realities of an evolving Web and its use, and our task is a large one. The good news is, with preparation and process, we can be successful.

The first step is to embrace Web 2.0 and create a strategy and toolset to maximize its benefits. A CISO must proactively identify the risks, but use this information to increase awareness and inform the business of their possibility. Gone are the days of "fear, uncertainly, and doubt" because board level management now looks to security for business success.

Next, document a strategy that is based upon business objectives, and clearly indicate what to allow, what to block, and who should have access and when. New policy should be developed, or a current policy set be updated, and they should be clear and enforceable. Ensure that your policies address Web 2.0 technologies, and consider subjective policy setting, group level access, and productivity based sections to give your policy strength. Revisit your acceptable use policy, and look at it from a Web 2.0 lens, and be sure to cover new technologies such as anonymizing proxies. Include other groups for support such as HR, legal and audit.

After the policy set is in place, focus on data loss protection, and stopping any information from exiting your network before it happens. You need to protect and comply with regulatory mandates, all without disrupting the business processes. A solution that monitors, prevents, alerts, and encrypts, and quarantines as needed is necessary. Deploy a solution that is capable of stopping sensitive data from leaving via your outbound mail system. Your filtering system should analyze and act on outgoing email in real time, in order to not impact productivity, and be able to perform searches in nested and zipped files and attachments.

A DLP solution should be part of an overall, integrated security architecture that includes a vigilant anti-virus program, a robust anti-malware protection program, and the capabilities of an AJAX-aware analysis platform. In addition, make sure your browsers (and their plug-ins) are patched, and do not simply focus on the critical patches, because all vulnerabilities are targets in Web 2.0.

WEB 2.0: WITH PROGRESS COME RISKS

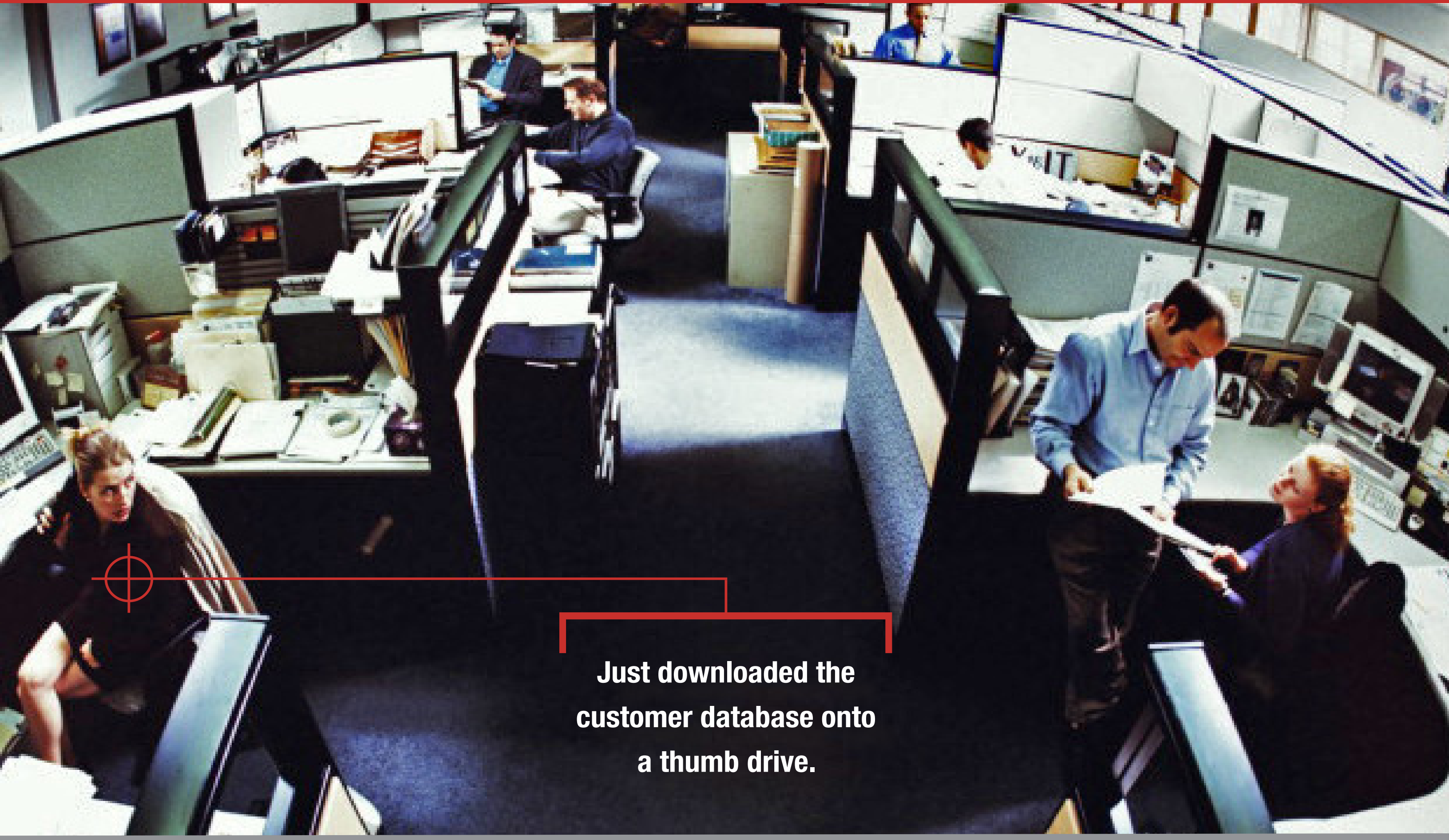
As with all emerging technologies, Web 2.0 and its related components are advancing rapidly, and security professionals need to remain aware of the risks and defenses associated with it. There is a generation entering the workforce ("digital natives") that assumes this technology will not only be available for their use, but is also essential to the way they communicate with colleagues and business partners. In addition, businesses are realizing the reach and depth they can achieve with a social media marketing strategy.

While there are many benefits that come with this new Web internally and externally, the policy, technology, people, and architecture to defend against the risks must be addressed proactively and not taken lightly. CISO's are the vanguard of their organizations in this regard, and through this effort, further solidify their value to the business.

Interesting times, indeed.

Find the cybercriminal.

(Never mind. ArcSight Logger already did.)



Stop cybercriminals, enforce compliance and protect your company's data with ArcSight Logger 4.

Learn more at www.arcsight.com/logger.

ArcSight™

The threat landscape and Web 2.0 technologies

There's been a lot of talk lately about Web. 2.0 --Web applications that facilitate sharing, collaboration and user-managed design, such as social media, blogs and wikis -- greatly expanding the threat landscape. The first time I heard this, I didn't take it seriously because it was made by someone outside of information security. However, as of late, fellow information security professionals have begun to make the same or similar assertions. Frankly, the threat landscape has not expanded because of Web 2.0.

Threat Considerations

Web 2.0 may represent another attack vector, but the same old threat landscape exists. Even without Web 2.0, technology still is highly vulnerable to threats and attack. Humans make technology. As much as we want to be perfect, we are not. Sure, companies can embed quality checks into technology; however, the dynamic life of technology makes it hard to match quality 100 percent of the time.

Case in point, the non-profit Open Web Application Security Project (OWASP) is doing a fantastic job of evangelizing secure coding. It's working to a degree for those organizations willing to invest in training their developers, but such organizations are rare. Secure coding as a core competency is absent in the developer community. If developers are in a hot industry such as banking, working in an organization that must meet PCI requirements or that's suffered a security breach and privacy sanctions, then secure coding may be a part of the software development lifecycle. But even if the developers code securely, consider the upstream chance that someone will not patch a server the application is hosted on or has added the dreaded "any any" rule to your firewall. The weakest link has always been humans.

Consider the fact that attackers typically take the surest path of exploit. If Web 2.0 did not exist, attackers would target the vector offering the greatest critical mass. For example, appliance-based technology (e.g. SSL VPNs or application delivery controllers) is ripe for exploitation when we consider it is built on open source technology and freely available to anyone who wants to use it. However, it takes a bit more effort and expertise to abuse the access gained once an exploit has succeeded. There will always be new attack vectors; information security professionals should expect it.

Technology Considerations

Looking at the threat landscape from a service-oriented architecture (SOA) perspective, attackers build on the existing threat landscape by reusing Web 2.0 as an additional attack vector. Attacks over port 25, 80 and 443 are commonplace in Web 1.0 technologies. Attackers reap the benefits of attacking traditional Web services and have taken that knowledge to use against Web 2.0: iFrame, code injection and cross-site scripting (XSS) attacks.. The black hat community draws from lessons learned in writing exploits against Web 2.0 technology. One of the biggest lessons is exploitation is possible when defense in depth is rote as opposed to rational. Rational defense in depth will consider layering defenses from at least two perspectives, thereby creating a mesh of defenses that are difficult to defeat. Rote defense in depth is a checklist you can show your auditors; a look beneath the hood will reveal the absence of technology tuning and in some cases, disabling of features that are integral to a strong defense posture.

An example of rote defense in depth is the now infamous Google hack where criminals launched whaling attacks to gain access. The attack is labeled "sophisticated" because it used encrypted channels to hide its presence. Since at least 1999, firewall technology has provided protocol inspection to defeat tunneling of protocols, but some networking and information security professionals have been led to believe protocol inspection either breaks applications or slows down network traffic. Networks that have been sized correctly with data flow analysis will rarely run into problems leveraging protocol inspection.

Ultimately, Web 2.0 is here to stay, but it hasn't radically changed the threat landscape. We're still dealing with the same fundamental threats – fallible humans and old flawed technologies. Rational analysis is best to determine the right defenses.

Resources from ArcSight

Annual Cost of Cyber Crime Study

ArcSight IdentityView: Detecting Role Violations

Advanced Persistent Threat: Cross Domains

About ArcSight

ArcSight (NASDAQ: ARST) is a leading global provider of cybersecurity and compliance solutions that protect organizations from enterprise threats and risks. Based on the market-leading SIEM offering, the ArcSight Enterprise Threat and Risk Management (ETRM) platform enables businesses and government agencies to proactively safeguard digital assets, comply with corporate and regulatory policy and control the internal and external risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage.