Level 3, 66 King Street
Sydney NSW 2000 Australia
Telephone +61 2 9290 4444
or 1300 922 923

Enabling Business through Secure Web Based Applications

Web 2.0 technology and tools can be a path to a shiny new era of collaboration ... or to a viper's nest of vulnerabilities, breaches and consequences. Put the proper security protocols in place and you can conduct worry-free Web 2.0 business.

What is Web 2.0?

The second generation of web technologies – the 'participatory web' – isn't just ubiquitous, it's almost mandatory for doing business leading into the second decade of the 21st century. According to Wikipedia, "it is characterised as facilitating communication, information sharing, interoperability, user-centred design and collaboration."

It's consumer-driven and includes the broader development trends of Rich Internet Applications (RIA), feature-rich websites that mimic thick client applications; collaboration and participation, generating and sharing content in real time with wikis, extranets, blogs, online forums and social networking sites like Facebook and Twitter; and broadcasting of data - syndication with RSS or Atom feeds. The array is seemingly endless and growing – and changing - all the time.

It's behaviour and mindset as much as technology. We are now accustomed to accessing any information we want, instantly, at any time. And there is a lot of information out there – IDC says that the 487,000,000,000 (that's 487 billion) gigabytes of digital content available today is set to double every 18 months.

Web 2.0 statistics increase from moment to moment but according to thefuturebuzz.com, at the time of writing there were

- 133,000,000 blogs indexed by Technorati since 2002
- 900,000 blog posts every 24 hours
- 1,200,000,000 YouTube videos viewed every day
- 20 hours of video uploaded to YouTube every minute
- 65,000 iPhone apps online; 1,500,000,000 downloaded and over 100,000 developers

Applications that were once housed securely in an organisation's server room, accessed only by people within the physical bounds of the building, are now online, web-enabled to facilitate interactivity with suppliers and customers, putting them at the perimeter of the network. Some of those applications, of course, hold extremely valuable confidential information and making them so easily accessible by your employees can also make them much more vulnerable to attack.

Collaboration - between colleagues, between businesses and even between countries - is the norm today and Web 2.0 is what

"It's behaviour and mindset as much as technology."

facilitates it. Web 2.0 has enormous benefits – it provides practical and reliable access to shared information, it allows effective leverage of contacts and content, it increases productivity levels and it reduces operational costs. It provides excellent return on investment.

Thus, there are compelling business reasons to adopt Web 2.0.

But it's not all sweetness and light.

Why should I care about Web 2.0?

Web applications have become the Achilles heel of corporate IT security - they are heavily targeted by cyber criminals. Forrester Research says that 78 percent of IT organisations are concerned about the risks of employee-driven, unsanctioned use of Web 2.0 tools and technologies.

And so they should be. In fact, the other 22 percent have reason to be worried as well.

50 percent of respondents in a recent Gartner poll said they "customise their work environment moderately or aggressively" (including the use of unsanctioned tools) and will continue to do so. (Our italics).

For many, the instantaneous reaction on reading those statistics is to shut off employee access to Web 2.0, to close it down completely. The problem with this path is that whilst you're certainly limiting your vulnerability, you're also limiting your ability to maximise the very real advantages that Web 2.0 offers ... and that your competitors are almost certainly leveraging. The intention is protection, the result is stagnation.

Not only that, but as with all bans, the moment something is prohibited, a certain percentage of the population devotes itself to finding a way around the ban. So it's not about denying access, it's about allowing access securely.

Everyone is vulnerable. Even the tech-savvy aren't immune – the Twitter accounts of one of its founders and those of his wife and several employees have been hacked this year.

According to the Verizon 2009 Data Breach Investigations Report, in the twelve months covered by the report, 285 million records were compromised. Furthermore, 64 percent of data breaches resulted from hacking, 83 percent of attacks were not highly difficult, 87 percent were considered avoidable through simple or intermediate controls and 99.9 percent were compromised from servers and applications.

There's not much room for doubt, is there?

"The moment something is prohibited, a certain percentage of the population devotes itself to finding a way around the ban."

How could Web 2.0 hurt me?

Nearly 55 percent of all vulnerability disclosures in 2008 affected web applications.

Web applications have become the major hunting grounds for cyber criminals who quite rightly view them as low hanging fruit. Just as building new motorways improves access for traditional burglars and car thieves, web applications' internet accessibility literally delivers them to the hackers' doors.

For some time now, cyber crime has simply been another arm of organised crime. And organised crime is pouring a substantial portion of its vast resources into cyber crime ... because the return on investment is very high.

Organised crime goes to great lengths to get its hands on any information – and the more confidential it is, the better. Once they've hacked into an application, they can either make use of it themselves or sell it on to others. They can also take control of the various resources such as servers and databases that house that information and turn a profit from that as well.

Having gained control of your computing power by exploiting vulnerabilities and adding code to your application, they add your power to their existing haul and create bot nets – a global network of robots reporting to their master bot net – which can be directed to attack other organisations, or sold to other criminals who, once they hold enough power, can orchestrate denial of service attacks.

No longer is it enough for these criminals to boast of their hacking prowess; these days it's all about the money. Given that a properly engineered denial of service attack is powerful enough to bring down pretty much any global multi-national corporation or, in fact, any small country and take them off-line for the duration, this is not about bragging rights, it's extortion. It is money-motivated from start to finish.

Because all information and all computing power is grist to the mill for the criminals, no company is too small and certainly no company is too big to be targeted. And as the security in large enterprises is often no better than small entities, size is truly no barrier to the criminals.

And no business can afford the consequences of a security breach. At the very least, mismanaging confidential information almost always leads to reputational damage. Reputational damage leads to departure of existing clients as well as difficulty attracting new business – a situation that can go on for many years. There are obvious bottom line implications to those consequences; in the most extreme cases, businesses can go under.

"Web applications have become the major hunting grounds for cyber criminals who quite rightly view them as low hanging fruit. "

According to IBM's X-Force® 2009 Mid-Year Trend and Risk Report, the predominant risks to web applications are from cross-site scripting, SQL injection and file include vulnerabilities.

Cross-site scripting vulnerabilities occur when web applications do not properly validate user input, thus allowing criminals to embed their own script into a page the user is visiting. This script can steal confidential information or exploit existing vulnerabilities in the users web browser. Cross-site scripting vulnerabilities are typically exploited in phishing attacks by sending users a malicious link to a page in a legitimate domain name via email. The criminals get high returns because users trust the familiar domain name they are visiting and thus trust the links (created by the criminals) therein.

SQL injection vulnerabilities are also about improperly validated user input, but in this case that input includes SQL statements that are executed by a database, giving attackers access to that database to read, delete and modify sensitive information (like credit card data) as well as embedding code into the database allowing attacks against other visitors to the web site.

File-include vulnerabilities occur when the application is forced to execute code from a non-validated remote source, allowing criminals to take over the web application remotely. This category includes some denial-of-service attacks as well as techniques that allow criminals direct access to files, directories, user information and other components of the web application.

Facilitating all these kinds of attacks is the fact that many web sites contain some code to support various features and functions which inadvertently introduces vulnerabilities.

Russian roulette, anyone?

How can I use Web 2.0 securely?

The best way is to start as you mean to go on. Rather than testing a web application's information security immediately before go-live, which is better than not testing but can result in an urgent, reactive situation arising, it pays to consider secure practices as part of your lifecycle management.

Even before your developers code your application your business needs to be aware of how to make the application secure, needs to have some standards to comply with and needs to schedule regular testing after go-live to ensure vulnerabilities don't creep in over time.

Thanks to criminal multi-vectors, your operating system needs to be built to suitable standards as well. It's not just the application at the perimeter that's interacted with; it's the back-end database, the content management system and the underlying server

"Cross-site scripting vulnerabilities occur when web applications do not properly validate user input, thus allowing criminals to embed their own script into a page the user is visiting."

operating systems that all need to be protected. Sense of Security calls this our Defence and Depth approach - reviewing multiple layers.

This approach, of course, has some set up costs as there's more work involved than in a single application security review. What Defence and Depth achieves, though, is a truly significant narrowing of your organisation's risk. No system is perfect, but if you have enough protection around all the layers criminals pursue, your company becomes non-cost-effective for their efforts and they simply give up and move on to an easier target.

As well as our Defence and Depth approach, Sense of Security can take your organisation through security awareness training, providing you with secure coding guidelines so applications can be developed from the design stages with the appropriate rigour in mind followed up with governance by way of testing before and after those applications go live.

Why Sense of Security?

Sense of Security has been growing rapidly since its inception in 2002. A BRW Fast 100 winner in 2009 and a Deloitte Technology Fast 50 winner in 2008 and 2009, the company is now the foremost independent provider of IT security and risk management solutions to leading companies and government departments in Australia.

Our expertise in assessment and assurance as well as strategy and architecture through to deployment and ongoing management gives us the ability to provide our clients with solutions, not just identification of their problems.

Originally built around providing security testing and ethical hacking (penetration testing) services, Sense of Security has evolved into a provider of strategic security advice, implementing security frameworks and roadmaps and developing compliance programs. As the threat landscape has changed, our service offering has matured, now providing customers with continuous targeted vulnerability management and protection.

All our business functions are retained in-house, leaving our clients with no security grey areas. Sense of Security is regularly invited to present our findings and insight at Board level; we promote thought leadership at this level to raise awareness of IT security as a crucial business issue – not just an IT issue.

Understanding that secure web applications are critical to your business' wellbeing, the path forward is straightforward, starting with a discussion on where and how you intend to implement web applications in your environment.

"Even before your developers code your application your business needs to be aware of how to make the application secure"

Sense of Security consultants can add value to your business by providing specialist security expertise at any stage of the web application lifecycle however we encourage our clients to engage us early in the application design stages so we can ensure best practice security measures are adopted from day one.

Unlike other consultancies for whom security is an additional, rather than a core, service, Sense of Security has the capabilities to provide businesses with a program of services to address all their information security requirements.

Each client business has individual requirements – not all organisations need Department of Defence-level security. But to succeed in this new e-environment, all businesses will need to demonstrate an enterprise risk management strategy including protection of information assets.

Many of Australia's leading businesses entrust Sense of Security with their risk management. If you would like to speak to us about any aspect of web application security or your business' specific needs, please call **Neville Gollan** on **+ 61 2 9290 4453** or visit our website at www.senseofsecurity.com.au

"Understanding that secure web applications are critical to your business' wellbeing, the path forward is straightforward"

Level 3, 66 King Street
Sydney NSW 2000 Australia
Telephone +61 2 9290 4444
or 1300 922 923