Advances in technology

Whitelisting is not a new concept. It was born in the days when servers sat surrounded by a perimeter of security defences. Computers and devices arrived with all features, services, and ports turned off by default – and that’s where they stayed until someone explicitly authorised and enabled (or whitelisted) them. IT managers found this approach too restrictive, too inflexible, and too difficult to manage within the modern enterprise. The good news is that the days of this static environment have passed. Whitelisting is dynamic and is being hailed as the solution that could help to protect organisations from dynamic and highly sophisticated targeted attacks.

About the author

Paul Zimski serves as Lumension’s vice-president of solution strategy. He has more than 12 years of experience in the IT security market and at Lumension he drives product strategy and positioning. Prior to Lumension, he served in various roles at Harris Corporation and Finjan Software.

References

3. Testimony by Paul Kurtz to the House Permanent Select Committee on Intelligence, 19 Sep 2008.
6. Cyber-Ark Software.

Social media strategies

Jim Mortleman, independent writer & consultant

Five years ago, the issue of social media was barely on any organisation’s radar. Most companies only started to take notice of the phenomenon around 2007–8, when they realised that a growing number of employees was spending a significant amount of time on a hitherto little-known site called Facebook. For some, it became such a problem in terms of eating up network bandwidth and employees’ time (not to mention opening up the organisation to security risks) that the most sensible solution seemed to be a blanket organisational ban on the use of the site and similar services.

Others, however, particularly in the business-to-consumer space, realised that if their employees were spending so much time on these sites, so were their customers. And that meant a social media ‘presence’ would be useful. In addition, there were forward-looking executives who suspected there might also be opportunities to use these technologies to improve internal communications, collaboration, corporate knowledge management and access to fresh ideas and talent both within and beyond the traditional organisational walls. Some even saw it as a way to help bring down those walls – dissolving silos and flattening management hierarchies in support of business transformation programmes.

Top of the agenda

Fast forward to today and social media has shot up the corporate agenda. According to a global study published in February 2011 by Burson-Marsteller, 84% of Fortune 100 firms are using at least one of the four most popular social media platforms – Twitter (77%), Facebook (61%), YouTube (57%) or a corporate blog (36%).1 However, the study also noted that too many firms are using these platforms more like traditional broadcast media, pushing out corporate news and campaigns rather than taking full advantage of the opportunity that social media gives them to engage...
more effectively with stakeholders – by listening, responding, conversing and learning. (A more comprehensive survey of the Fortune 500 conducted by the Center for Marketing Research at the University of Massachusetts, now in its third year, shows similar results, along with more detailed sector splits for social media use.)

“Even in organisations where social media use on corporate systems is prohibited, people still use social networking sites on their personal devices like laptops, smartphones and tablets”

As the pioneering Cluetrain Manifesto (which predicted the rise of social media back in 1999 and remains one the clearest guides on how organisations should approach it) notes: “Most corporations ... only know how to talk in the soothing, humourless monotone of the mission statement, marketing brochure and your-call-is-important-to-us busy signal. Same old tone, same old lies ... But learning to speak in a human voice is not some trick, nor will corporations convince us they are human with lip service about ‘listening to customers’. They will only sound human when they empower real human beings to speak on their behalf.”

Of course, many of those “real human beings” are speaking on your behalf (or, at least, about you) whether you’ve empowered them to do so or not. Even in organisations where social media use on corporate systems is prohibited, people still use social networking sites on their personal devices like laptops, smartphones and tablets, be it at work or in their own time. Not only can this lead to reputational damage for individuals and organisations, but it can also open up employees (quite possibly with sensitive corporate information sitting on their personal devices) to threats from malware, phishing scams or targeted social engineering attacks.

Double-edged sword

It’s clear, then, that social media can be a double-edged sword. How do you take advantage of the very real opportunities while minimising the risks? The first thing to say is that neither lockdown nor a laissez faire attitude is the answer. Being too prescriptive or Draconian not only cuts you off from potential opportunities to boost your social media savvy, become more innovative and improve your organisational agility, but the approach has been shown to drive social media use underground, leaving IT and business management powerless to monitor or control what’s going on. Similarly, allowing a social media free-for-all without working out clear policies as to how it should and should not be used (and effectively educating users about those policies) is a surefire recipe for disaster.

Having a clear vision of precisely what you’re trying to achieve with social media is important. Using it for ad hoc branding and marketing campaigns, for example, will require fewer resources than trying to use it to change business structure, culture and processes. The latter requires not only significant change management, but senior-level sponsorship and commitment to create the necessary buy-in and appropriate behaviours among users. Cisco, for example, has successfully adopted it for both internal and external use, and has produced a ‘Social Media Playbook’ which serves as a useful guide for others wishing to emulate its successes.

Those responsible for information security and corporate risk, though, need to focus on two key areas when they think about social media. First, they must ensure that sensitive organisational data is adequately protected. Second, they need to instil in users the dos and don’ts of social networking – both from the point of view of preventing information breaches and that of avoiding reputational damage. As a 2010 survey by security specialist McAfee points out: “Globally, leaders of organisations agree that security concerns and issues with
employee use of social media are the two major barriers for successful implementation of Web 2.0 in their organisations. In order to maximise the benefits from Web 2.0, organisations need to take measures to mitigate these risks."

"An organisation needs to set clear policies about such things as secure passwords and what users can and cannot say in public or semi-public forums”

Classifying data types
In terms of protecting sensitive data, most security analysts are in agreement. Given today’s multiplicity of entry and exit points for information, old-style perimeter security is no longer effective. The focus must shift to protecting the sensitive data itself – and to do that effectively, without constraining the necessary flow of information, means you need to ensure that different data types are properly classified. Adrian Davis, principal research analyst at the Information Security Forum (ISF), says: “That can be as simple as embargoing certain information until a specific date, or as complex as having multiple layers of classification. But you’ve got to work with the business to get that right.”

You might, for example, tag any piece of information red, amber or green according to its level of sensitivity and build controls into systems to limit access or prevent users from passing on anything sensitive across particular networks. “Another approach is to try to upscale DLP [Data Loss Prevention] and DLM [Document Lifecycle Management],” says Davis. “We may even go back to the old world of having different networks for different levels of information. Organisations will adopt different approaches.”

But technical controls are only a small part of the solution. The key consideration is how you successfully manage the way people use social media in both a business and personal context, and that’s a lot trickier. Again thinking about the potential for data breaches, an organisation needs to set clear policies about such things as setting secure passwords (and frequently changing them) and what users can and cannot say in public or semi-public forums. More importantly, they must ensure that their users understand those policies and any personal and organisational consequences that might ensue if they break them.

They also need to ensure that users are kept abreast of the latest technical threats and social engineering scams in order to minimise the chances of them falling foul of these, which (given the rate at which such threats emerge, change and evolve) implies they need to implement not just a static usage policy but an ongoing mechanism for threat analysis and communication (quite possibly taking advantage of social media to do so).

They must also monitor the changing privacy and usage policies of any third-party networks their employees use and make sure people are clear about how much of what they post will, for example, be visible not only to their mutual contacts on these networks, but also to unknown ‘contacts of contacts’, commercial partners of the social networking sites in question such as advertisers, or indeed to anyone, through public search engines and aggregators. When privacy policies change, as they frequently do, organisations should notify users with clear instructions of how to amend their privacy settings.

Reputational risks
The hardest challenge, though, is mitigating the reputational risks of social media. First, your reputation can be damaged if you are seen to be technically inept – for example, if social networking or corporate blog accounts are hijacked by malware which then spreads to customers, partners and other contacts. On social networks like Facebook and Twitter, a common form of attack is to entice users to authorise some third-party application which is then given permission to access the user’s data and post information on his or her behalf, or to click on a link that invisibly installs some malware.

“If you’re not routinely monitoring the web and social networks for conversations taking place about you then these conversations can quickly escalate and cause severe reputational damage”

But equally, your people are key to your reputation – and if they post inappropriate, defamatory or inaccurate comments (or indeed, comments which contradict a corporate message), this can have disastrous consequences. You need
to set out and explain clearly what they can and cannot say – and clearly outline any disciplinary consequences of failing to adhere to these policies. “People need to be much more aware of the consequences of their actions and statements,” says the ISF’s Davis.

Finally, it’s vital to remember that social media can damage your reputation whether you use it or not. People talk about companies online all the time. If you’re not routinely monitoring the web and social networks for conversations taking place about you (and routinely responding quickly and openly) then these conversations can quickly escalate and cause severe reputational damage, as companies like BP have found to their cost.

Users of these networks increasingly expect companies to engage with them on a level playing field, so organisations without a presence – or which attempt to silence critics, or push out messages without actually joining in the conversation – could be doing themselves the most harm of all.

About the author

Jim Mortleman is editor of the Infosecurity Network <http://www.infosec.co.uk>, and an independent business and technology commentator, consultant and writer with 20 years’ experience researching and covering IT developments and their implications for business and society. He has written for numerous titles and online services including The Guardian, Silicon.com, Computer Weekly and Computing, as well as writing and consulting for private clients and speaking at business and technology leadership events.

References


Identity and Access Management: the second wave

Cath Everett, freelance journalist

Many regulated organisations are now starting to activate a second wave of Identity and Access Management (IAM) initiatives as they attempt to rectify the mistakes made in the first attempt.

The primary wave began as much seven years ago among large enterprises, particularly in the financial services sector. Deployments were typically led by IT or security professionals and therefore focused on fixing administrative rather than business problems. To make matters worse, a lot of vendors aggressively sold their products as a silver bullet for tackling compliance issues. In fact, all that many of them could do was handle basic tasks, such as automating user provisioning in order to make it quicker to add or remove staff from the system when they joined or left the organisation. Although such activity led to a nice fat tick in one audit box, it failed to deal with recurring problems such as too many orphan accounts, account-copying or how to control access rights among staff as they moved around the company, which were just as much cause for concern.

As Martijn Verbree, senior manager of KPMG’s risk and compliance team, points out: “You don’t manage IAM because it’s fun – you need control because you don’t want people accessing systems inappropriately. The focus on the real issues was lost in the first wave so now it’s almost about getting back to basics.”

One of the key problems in the past was that, because IAM was seen as a technology rather than a business project, many organisations did not treat it as a change management programme and so neglected to deal with matters ranging from processes and governance to policies and people. But the problem