deliver it to you more or less out of the box. Make sure:

- The solution fits into your network infrastructure
- The interface provides the views and capabilities required by your users-searches can be automated
- You consider segregation of duties.

The more complex the requirements for real-time analysis and reporting, the more important it is that the solution be configured according to the business needs of the customer. Typical questions should be:

- How much out-of-the-box content exists?
- Does it meet my needs?
- Is the solution flexible and extensible?
- Does the vendor have the ability and experience to implement the solution?

Failures can be prevented by defining the use cases of each project and deciding on a solution that meets current and future needs. These solutions are not easily and quickly replaced.

About the author

Fabian Libeau is the EMEA marketing director at ArcSight. He has more than 12 years of IT security experience, and has spent the past eight years in the security information and event managementspace. Fabian joined the EMEA headquarters of ArcSight in April 2005. Prior to that, he worked at CA as a principal architect and VP for SIM solutions in EMEA. Fabian is a recognised expert in the field of IT Security and he is a frequent speaker at security conferences. He has managed major security solution roll-outs at various global IT companies. He holds a CISSP certification, and has a Masters in Physics.

Danger in the clouds

Steve Mansfield-Devine


Steve Mansfield-Devine

Cloud computing is hot, but are we running ahead of our ability to ensure a secure environment? If you are smart, you have invested significant resources in securing the perimeter of your organisation. You feel safe behind the firewalls, DMZs, VPNs and fiercely enforced policies. Then along comes cloud computing and suddenly your users are keeping valuable and even business-critical data outside the perimeter, beyond your control. Scary, is it not?

Cloud computing is hip, technologically elegant, and so conceptually simple even a CEO can grasp it. You can lump most of the benefits into one category – cost. But there are other advantages, such as ease of rolling out new capabilities, scalability, and automatic rightsizing. Cloud computing – or software as a service (SaaS) – is attractive from technological, practical, and financial perspectives. That makes it inevitable.

More and more services are being offered this way. They range from security services that vet your email and web traffic, through external data storage (such as Amazon's S3), to personal productivity applications like those offered by Google. These all raise security issues, but none more so than those services that provide a major business IT function – such as Salesforce.com, which gives small and medium-size companies the CRM functionality they could not afford to install and run themselves.

While risks may be acceptable if all you are doing is using Gmail for messaging, it is a different story when you are using similar technologies for your organisation's crown jewels. Alas, the cloud picture is getting more, not less, complex. With Microsoft's new Azure offering, for example, the processing is split between the local machine and Microsoft's servers. What is handled where depends to a large extent on the application programmer. Azure includes mesh networking capabilities as well, effectively making each user's computer a router. All this makes for a variable and highly convoluted security environment where current practices and concepts may not apply.

Large target

There are important differences between cloud services and, say, an outsourced data centre, which will be in a readily identifiable location, on dedicated servers that are integrated into your own network.

"Traditional systems are masked behind firewalls, NATs, and other gateway boundaries, so attackers must do intensive intelligence gathering to know that they exist," explains Greg Day, security analyst at McAfee. Cloud services, on the other hand, are highly visible and are designed to be accessible from anywhere by anyone. As far as malicious hackers are concerned, that is like painting a large target on them. This is especially true as cloud services place a lot of valuable data from thousands of users in a single place – a juicy target indeed.

"Last year, Monster was hacked and millions of contact details stolen which unleashed a phishing attack," says Day. "When it comes to business services in the cloud, the cyber criminal only needs to hack one site to get access to multiple companies."

So what is the problem?

Gartner recently outlined seven security issues – privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability.[1] Some of these concerns could be applied to any outsourced service, but there are cloud-specific security threats.

"The majority of the threats are going to come from conventional sources," says Ken Munro, director of penetration and security testing company SecureTest. "You need to be able to log into the

service, you need to give people a route to access it, you need protocols to send traffic to it." These raise classic issues, Munro suggests, and the problems are likely to be the standard ones of poorly implemented protocols, authentication processes and so on.

Having the service go down or disappear is clearly a worry. Both Amazon S3 and Flexiscale have suffered significant outages – the latter caused by an engineer's error.[2] More worrying is denial of service (DoS). With internally hosted systems, what you lose is your internet-based systems – web and email. That can be very serious. Nevertheless, internal systems will remain largely unaffected, allowing some business processes to continue. With a web-based model, these business-critical processes are vulnerable to DoS attacks. That makes you a potential target for the same kind of extortion racket we have seen in the online gambling world.

Design flaws

You have to place a great deal of trust in the design of the system – not least in the access and authentication capabilities. This was highlighted when a flaw in a new indexing system at Zoho resulted in one user being able to read other users' documents. Zoho says it fixed the issue within hours and only one user was affected. How many others found it, though, and failed to report it or even took advantage of it?

"You have to place a great deal of trust in the design of the system – not least in the access and authentication capabilities"

Numerous issues have been reported with Google's services including a cross-site scripting (XSS) attack on Blogspot Polls that revealed the blogger's contacts and incoming Gmail, a combined XSS and cross-site request forgery (CSRF) and malformed URI attack on Picasa to steal images from the Picasa user's hard disk, and several Gmail issues, including one CSRF exploit that was able to insert filters into a victim's Gmail account, automatically forwarding emails to an arbitrary address.

Cloud applications are, by nature, browser-based. This is an interface whose weaknesses are well known, so many of the attacks on cloud-based services and data will be of a conventional kind.

"Criminals no longer have to go for a complete compromise of the system because a compromise of the browser alone achieves a lot," says Ivan Ristic of Breach Security. "In practice this means, while previously the focus was on vulnerabilities such as buffer overflows, we are now seeing more interest in web-related vulnerabilities such as cross-site scripting (XSS) and cross-site request forgery (CSRF)."

To complicate matters, many cloud services – Salesforce.com being a leading example – are positioning themselves not so much as SaaS but as 'platform as a service' by offering function-rich APIs. This allows third-party service suppliers to extend and build on Salesforce's own capabilities. Hundreds of third parties are developing code for Salesforce.com, which has more than 800 applications installed across 40 000 customers. Who is checking the code?

Services are springing up that add functionality to existing cloud applications. For example, Appirio, which offers a single route into both Salesforce.com and a storage service – which is provided by another SaaS vendor, Amazon S3. Appirio's take is that this is all made possible by the mature APIs being offered by cloud service suppliers. Technologically, that may be true. In terms of auditing the security, it sounds like a nightmare. It means you are further abstracted from the organisations hosting the service and holding your data.

Authentication and access

Typically, communication between users and cloud services is secured using SSL. It is a familiar technology – too familiar. Certificate warnings are treated by most users as a nuisance and they ignore them. They might not notice if they are logging on to a spoof site as the result of, say, a DNS poisoning exploit. Of course, the rogues who created the spoof site could also disable SSL to avoid the possibility of warnings.

Google has demonstrated the kind of authentication vulnerability that might be exploited in cloud-based services. This was the result of Google's implementation of the OASIS Security Assertion Markup Language (SAML) for single sign-on. SAML uses XML-based authentication data to be shared by a number of domains. Once you have signed in to, say, Google AdSense, you could then switch to Google Docs without signing in again, even though you have moved to another server. The flaw meant that someone could set up a server that allows you to log in to Google, and could then use the SAML authentication data to impersonate you on Google, and get access to all your data and files. Google has closed this loophole.[3]

Data governance

Given that cloud services are shared by many customers, you also need to worry about data segregation. In this kind of multi-tenancy arrangement, how certain are you that other customers cannot get at your information? It may be an unlikely scenario but what about who else has access to that data? Presumably, system administrators at the cloud vendor need access in order to run the system. As the Gartner report points out, these are "people who do not have a long-term commitment to your organisation."

Nor can you ever be entirely sure where your data is held. A cloud supplier might itself outsource data storage, or it might use data centres liberally distributed around the globe.

There are compliance issues here, for example, can you be sure you are complying with the data protection regulations of wherever your data happens to be? And can you provide adequate access to the data for investigative purposes? These are not security issues, but they may become so if something goes wrong and you need to recover the data or at least ensure that it is secured. You will not always get adequate notice when a cloud vendor goes down. It is essential, therefore, to have a contingency plan and to have means for getting your data back built into your agreement.

Taking control

Underlying all this is the issue of who has control. Who has the responsibility for

security and the ability to take action? Without clarifying this it is impossible to ensure adequate data governance.

If you run your own systems you can implement, test, and verify security measures to your own satisfaction. With a cloud service you are dependent on the service supplier to implement strong security and take appropriate and timely action when a problem occurs.

A cloud service provider will argue that worries about control are answered by its service level agreements (SLAs) and compliance with 'industry best practice'. But try asking them to indemnify you against any financial or business losses and you may see the confidence level slip.

What do you do?

There are no security standards specific to cloud computing. Worse, security is often addressed as an afterthought in the rush to adopt these technologies. Nevertheless, you can usefully apply conventional security concepts.

"This is a displacement of risk rather than additional risk," says Gunter Ollmann, chief security strategist for IBM Internet Security Systems. "From my own professional penetration testing experiences, these larger applications tend to be orders of magnitude more secure than what most organisations have the capability to develop and deploy themselves."

The key here is transparency. And this needs to be spelled out in the SLAs. In addition to assurances about business continuity and disaster recovery, you need specific details about security policies and implementations. Gartner's report stated the problem as, "You can't see into the cloud – you just assume that it works." But seeing into the cloud is precisely what you need to do.

"Complete infrastructure information must be available on request, equally at the negotiation phase and at any point in the service lifetime," argues Ristic. "Ask vendors to show you their software development procedures and policies, security testing policies, and vulnerability disclosure policies. Ensure the SaaS vendor employs the state-of-the-art security measures. And require better security measures from SaaS vendors than you could ever provide internally. There is no reason to outsource yet get inferior quality."

Testing is very important, preferably carried out by third parties. "I would recommend verifying that the provider is undertaking regular application penetration tests," says Ollman. "For the larger application platforms, or services deemed to be critical from a confidentiality perspective, I would recommend that daily automated vulnerability scans are run against the application/site, with monthly consultant penetration tests, and that the results of these tests be available on demand."

Lee Lawson, lead penetration tester for DNS, also raises the issue of who has access to the system. "How does the cloud application handle user account creation, deletion, and management? How does it manage the access and permissions granted to user accounts?" He stresses the need to ensure, "that an organisation has mature processes for identity management – for example, what happens when someone leaves."

How many cloud vendors will be prepared to provide this degree of transparency is another matter. And having high security standards may prevent you from adopting otherwise beneficial services. But that has always been the dilemma we face.

References

1. J. Heiser and Mark Nicolett: "Assessing the security risks of cloud computing." Gartner, 3 June 2008 <www.gartner.com/DisplayDocument?id=685308>
2. C. Metz: "Engineer accidentally deletes cloud." *The Register*, 9 October 2008 <www.theregister.co.uk/2008/08/28/flexiscale_outage/>
3. "Google SAML Single Sign on vulnerability." US-CERT, 9 October 2008 <www.kb.cert.org/vuls/id/612636>

False positive response

Siraj A. Shaikh, research officer, Department of Informatics and Sensors, Cranfield University, UK
Howard Chivers, professor, Department of Informatics and Sensors, Cranfield University, UK
Philip Nobles, lecturer, Department of Informatics and Sensors, Cranfield University, UK
John A. Clark, professor, Department of Computer Science, University of York, UK
Hao Chen, research associate, Department of Computer Science, University of York, UK

In an earlier article we examined reconnaissance activity over networks and discussed some of the challenges in detecting such behaviour.[1] One approach to dealing with such activity is false positive response.[2] The purpose of false positive response is to make it difficult for an intruder to distinguish between the operational active address space and the inactive one, and between genuine and decoy hosts. Such an approach is designed to render any reconnaissance information useless and make it difficult to obtain accurate information about a potential target network.

We survey a range of options available for deploying a false response. There are two main aspects of this: first, the simulation of a network of hosts that are potential targets for an intruder and are therefore accessible through the network and second, the means to generate traffic as a