Is Twitter the newest data security threat?

Lori MacVittie, 2008-16-10

One of the most dangerous threats to data security is also one of the least talked about: employees. Are Twitter and other microblogging sites yet another avenue through which sensitive data can leak out of the corporate database and into the hands of ... anyone? Perhaps more worrisome, what information are you giving away simply by being a part of the community?

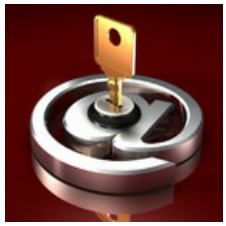
Of course Twitter is a potential threat. Like personal e-mail accounts and instant messaging, Twitter and sites of its ilk are primarily messaging mechanisms, which translates into personal channels for exporting sensitive data outside the enterprise. If you aren't familiar with Twitter, its messaging mechanisms allow several "modes" of communication: a blast to the general twitterverse, a public reply to a specific twitter user, and a direct (private) message to another twitter user. The direct messages aren't displayed in your public timeline, only the intended recipient can see them, so they're perfect for sneaking out tidbits like customer information or competitive information like upcoming product features/launches.

Despite the good intentions of compliance initiatives like HIPAA and PCI DSS, implementation of security measures designed to comply with these standards tend to focus mainly on the easiest and most obvious ways in which sensitive personal information can be lost, stolen, or shared: web applications.

But Twitter *is* a web application, you say, so shouldn't it be covered?

Perhaps, but it likely isn't. Current regulations tend to concentrate on preventing data from being taken out of the enterprise database, not cut-and-pasted into a tweet or e-mail or instant message. While monitoring and even filtering of web applications is commonplace today, it's almost universally focused on filtering of inbound web content, not *outbound* except at the URI or domain level. Content filtering solutions can stop inbound web content containing naughty words and those naked pictures of Bea Arthur the transfer of which no one can explain. But they don't generally focus on filtering *outbound* requests and POST data, despite the inherent risk in allowing unfettered communication with the outside world.

There have been solutions offered to prevent this exact scenario from happening via e-mail, but monitoring around web and even instant messaging continues to primarily focus on inbound content rather than outbound content. This makes microblogging sites like Twitter a potential security risk when attempting to secure all the possible avenues through which sensitive corporate data may be leaked.



What's necessary to block these holes is a two-pronged attack posture:

1. Reiterate to employees the ramifications of exporting sensitive data, including recognition of having read and agreed to organizational policies regarding how the organization will deal with proven breaches involving data security. Hint: A slap on the hand may not be harsh enough, though getting medieval on them may be too much. Maybe.
2. Consider the implementation of a forward proxy security solution capable of at the very least monitoring outbound web content (over HTTP) and optimally blocking anything that appears to be a credit card or social security number or anything else that might be considered sensitive personal information.

Proactive information security (sometimes also known as 'due diligence' in legal speak) requires recognizing both possible holes and acting to block them.

CAN YOU SHARE TOO MUCH INFORMATION?

And even if you aren't concerned about Twitter as a possible data security threat, you might consider the number of brands that are using Twitter to communicate with customers. That means the folks following a particular brand (company) could be viewed as a very public customer list. In the past, vendors - especially startups, for whom Twitter is particularly attractive - have aggressively guarded their customer lists so that competitors can't swoop in and convince them to "change sides". Twitter offers a public view of customers - and potential customers - that could be easily used in sales strategies to obtain new customers.

Conversely, some companies have always been reluctant to admit whose solutions they use for security and software because they are juicy targets for bad guys. Letting the bad guys know which solutions might be securing or serving up their corporate data gives them an edge, and if employees are following a "brand" it might be a hat tip to those intent on harm or theft as to how to target their attacks.

Whether it's direct leaks of information coming from employees or inadvertently allowing too much information about customers or your own infrastructure to leak out publicly through deductive reasoning based on who you're following, the use of Twitter should be viewed as both a possible business benefit and a potential security threat.

Twitter and sites of its ilk are definitely a possible hole in your security strategy (isn't everything in the eyes of information security folks?) and should be evaluated and if necessary addressed sooner rather than later.

Related Links

The Unpossible Task of Eliminating Risk

What IT Security can learn from a restroom sign

PCI DSS Requirements 6.6: A best practice for the rest of us

New TCP vulnerability about trust, not technology

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com