PHYS.ORG

Social-network use leads companies to boost security

March 2 2012, By Byron Acohido

When Randy Kortering decided to upgrade computer network defenses at Haworth, a $1 billion-a-year office fixtures manufacturer, his chief of security warned him about social-networking use.

"He laid out what was coming through a Facebook connection and how it could very quickly spread a virus that we weren't prepared to block," recalled Kortering, vice president of global information services for the Holland, Mich., company.

Kortering began reviewing new security systems designed to closely monitor or restrict, as needed, employee use of Facebook, Twitter, Google, LinkedIn and other popular online services. Because of a surge of headline-grabbing database breaches, many companies attending the massive RSA security conference here this week are following suit.

"The problem is pervasive," said Jeff Wilson, principal security analyst at Infonetics Research. "Companies of all sizes are definitely re-evaluating what they have installed for IT security."

Verizon's annual Data Breach Investigations Report supplies a benchmark. Its 2011 study examined patterns in 800 corporate intrusions, up from 761 in 2010. By contrast, Verizon's forensic experts were called in to solve 900 database break-ins in the previous six years combined, 2004 through 2009.

This is new terrain. The tech industry's marquee players are intensifying the collection and sharing of personal information in order to sell more advertising. Yet the implications of companies acquiring beefier security systems to restrict employee access to popular services are difficult to discern.

Security analysts and criminologists say this much is clear: "Spear-phishing" attacks, crafted to get unsuspecting employees to inadvertently seed computer viruses and infections at targeted organizations, are jumping. And the surge of attacks on corporations correlates to the rise in unfettered use of social networks, search engines and Web apps on company networks, analysts say.

These popular free online services have turned out to be a boon for spear phishers, who prowl social networks and use search engines to gather intelligence. "Just like online marketers and advertisers, criminals see a tremendous value in knowing more about their targets," said Rob D'Ovidio, a criminology professor at Drexel University.

Spear phishers are adept at inhabiting social networks to troll for victims. And they have proved endlessly inventive at crafting emails and social-network postings that appear to arrive from a trusted source, while stealthily delivering a malicious payload to gain them access deep inside company networks. The desired booty: customer lists, design documents, patents, financial statements - anything that can be sold in the cyberunderground.

"In most of the high-profile breaches we've seen in the past 12 months, hackers used social engineering to get an initial foothold inside the company," said Hugh Thompson, RSA conference program committee chair. "It isn't a generic stranger trying to deceive your employees; it's someone who knows them through online reconnaissance."

Recent studies illustrate this dark side of social networking. Firewall maker Barracuda Networks analyzed Web traffic of 5,500 PC users in 20 nations and found one in 60 Facebook postings, and one in 100 Twitter tweets, carried malicious code.

"The dangers associated with social networking have climbed exponentially," said Barracuda chief research officer Paul Judge.

Meanwhile, an analysis of Web traffic at 1,636 companies by firewall supplier Palo Alto Networks found a marked increase in employees' use of Facebook to run Web apps and games, not just read wall postings. In December 2011, employees used Facebook apps three times as often than they did in October 2010; and they used Twitter seven times as often.

Those increases tracked with an uptick in corporate use of Facebook and Twitter for marketing and recruiting, said Palo Alto senior security analyst Wade Williamson.

But new Web apps are being pumped out so swiftly that many organizations aren't able to fully grasp the security risks introduced by their employees trying out every cool new app that comes along, Williamson said.

What's more, companies now routinely permit employees to connect their personally owned smartphones and tablet PCs into company systems, creating myriad fresh pathways into corporate networks.

Apple recently had to quell a furor over disclosures that social network Path and several other makers of apps for iPads and iPhones routinely collected and stored the contents of users' address books - without asking permission.

The Path revelation underscored how intrinsically porous services delivered to PCs and mobile devices from the Internet cloud can be. Cybercriminals, of course, long ago realized this and continue to take full advantage.

A recent Juniper Networks survey of applications available for all mobile device operating systems, except Apple's iOS, tallied 28,472 malicious mobile apps in 2011, a 155 percent increase from the 11,138 malicious apps that existed in 2010. (Apple does not make iOS apps available for independent inspection.)

"Companies are going to have to learn exactly which applications are on their networks, who is using them, why they're being used and make sure they are being used securely," Williamson said.

Some companies have already begun doing just that. Haworth's Kortering was persuaded to upgrade to a next-generation firewall that can distinguish traffic going to and from specific applications, and block very specific types of traffic deemed non-productive or too risky.

"The easiest thing would be to block everything," said Kortering. But "we block what we feel is outside of our policies and values."

Waqas Akkawi, director of information security at global moving company SIRVA, is keeping much closer watch on his company's network, too. Last fall, SIRVA purchased cutting-edge network access control, or NAC, technology to meticulously manage who gets to log into its networks and to block any malicious programs trying to load from specific devices.

Many of SIRVA's 3,000 employees, and most of its customers, log in to the company's network remotely. "I could not say no to anybody because they'd say, 'Hey, you're limiting revenue generation,' " Akkawi said. "So I said, 'No problem; you can bring it in.' "

Sales of next-generation firewalls and NAC systems are expected to grow robustly over the next five years as more companies come to grips with rising security threats. Many will discover that limiting employee access to social networks and Web apps can also directly help the bottom line, said Chris Rodriguez, network security analyst at Frost & Sullivan.

Haworth, for instance, has used its new firewall to restrict employees from watching streamed videos in the lunchroom because that activity was consuming bandwidth needed on the production side at the fixtures manufacturer. "There's a lot to be said for the value security tools offer operational-wise, such as the ability to automate tasks and reduce lost productivity," Rodriguez said.

Even so, it is the capacity for new tools to help corporations protect against as yet unforeseen threats likely to arise from employees' escalating use of social networks, Web apps and mobile devices that's generating buzz at the RSA conference.

Some security experts worry about the chronological nature of Facebook's new Timeline interface, which went live for most users this month.

No evidence has surfaced that spear phishers have begun mining Timeline. And Facebook spokeswoman Meredith Chin says that Facebook essentially works the way it always has and that Timeline surfaces no new information, nor does it change any privacy settings.

But a cottage industry appears to be taking shape to more systematically broker stolen Facebook account logons. Aviv Raff, chief technology officer at threat alert service Seculert, tracked down a criminal server set up to continually harvest data from tens of thousands of infected PCs. Raff found an unusual program running in the background.

"They created specific code to extract just the Facebook credentials," Raff said. "We found logon credentials for over 45,000 different Facebook accounts."

Criminals use stolen logons to pose as a trusted source in attempts to dupe employees into clicking a poisoned link or opening an infected document, said Anup Ghosh, chief scientist at browser security firm Invincea. "With Timeline," he said, "literally years worth of status updates, photo uploads and links can be pored through to create convincing personalized messages."

(c)2012 USA Today
Distributed by MCT Information Services

Citation: Social-network use leads companies to boost security (2012, March 2) retrieved 27 April 2024 from https://phys.org/news/2012-03-social-network-companies-boost.html