greenPROFIT

Features

11/1/2017

Don’t Get Punked

Joe Dysart

Growing businesses uneasy about the increasing frequency of hacking on today’s business world can take heart: with a bit of planning, you can significantly reduce your vulnerability to a computer break-in via the Internet.

As many of us know all too well, some of the most notorious hacks have been, are—and most likely will continue to be—perpetrated by a shadowy group of computer wizards known as “Anonymous.”

“Anonymous is heroic to many people who are sick of government lies and weary of government intrusion—unwarranted and warrant-less—into the lives of U.S. citizens,” says Sharon D. Nelson, Esq., president of Sensei Enterprises, a computer security consulting firm. “They have become very much like—in ‘The Terminator’ movies—the Resistance fighting Skynet. Many are script kiddies or amateur hackers.

“But there is a core group of hackers who have extraordinary skills. They present one of the greatest security threats of recent years. And we have not, so far, done a lot to counter their intrusions.”

Perhaps even more sinister is the “professionalization” of hacking that’s emerged during the past years, in which hackers have become 9:00 to 5:00 workers with holidays, vacations and many of the other trappings associated with legitimate jobs.

Kevin Haley, Director of Symantec Security Response, says: “Advanced criminal attack groups now echo the skill sets of nation-state attackers. They have extensive resources and a highly-skilled technical staff that operate with such efficiency that they maintain normal business hours. We are even seeing low-level criminal attackers create call center operations to increase the impact of their scams.”

Beware Malware

One of the preferred ploys of these organized crime rings is ransomware: malware that downloads on your PC or business network, secretly encrypts all your business data and then demands a ransom for your files to be restored.

Rich Conklin, an IT security consultant and owner, Executive Computer Solutions, says one of his clients was recently hit with ransomware, which brought down 28 of its computers.

“Because they had a formal, data back-up program for their business, which I recommended and maintain, I was able to get most of their data restored later the same day,” Rich says.

All that remained encrypted was data tied up in software that was maintained by another, independent IT contractor for his client, who’d refused to allow his data to be backed-up by Rich’s overall back-up plan for the business. Ultimately, the ransomware victim was able to slowly re-enter some of that lost data by hand, he adds.

But understandably, the client was less-than-impressed with the contractor who'd refused to participate in its data back-up program. "Let's just say the day that ransomware hit the system—that was his last day," Rich says, referring to the independent IT contractor.

Ryan Naraine, a head of the global research and analysis at Kaspersky Lab, hears network take-over horror stories like Rich's every day.

"Right now, ransomware is an epidemic," he says. "Although it has been around for more than a decade, we have seen a recent explosion of new ransomware families that is cause for serious concern." Indeed, some of the newest variants of ransomware are even popping up on mobile technologies, according to recent a report released by Christian Fredrickson, CEO, F-Secure.

How to Protect Yourself

The security take-away? Businesses of all sizes need to make peace with the fact that hackers won't be neutralized any time soon. And they need to be honest with themselves that their current computer defenses are probably silly putty in the hands of experienced of hackers.

Caption: Good news: Sophisticated artificial intelligence systems, like IBM's Watson pictured here, are tooling up to combat hackers.

Job One: The best way to begin hardening the online digital perimeter of your business is to realize that the person or staff responsible for your web security is the over-arching factor in keeping your business safe—and not necessarily the security technology they administer and oversee.

"Fundamentally, good security really is just good systems administration," says Ira Winkler, founder of Internet Security Advisors Group, a computer security consulting firm. "And if you can't afford or can't get a good system administrator, I recommend outsourcing that."

In fact, Ira says the smallest of growing businesses will probably be best served by an out-sourced, third-party computing solution, given that the entire focus of a top-notch network systems provider is on configuring, maintaining and securing computer systems, 24/7. In other words: you may want to move the critical computer applications of your business to the cloud, so you can take advantage of the relatively sophisticated web security offered there, Ira says.

At minimum, Sharon at Sensei's recommends a quality Internet firewall that's properly configured and Internet security software that guards against viruses, malware and spyware. Both are available with software packages, like Symantec's Internet Security, Kapersky Security, Trend Micro Security and the like. And you'll also need to be sure your staff gets the message that your business security has to be taken very seriously.

"Education of your employees is key," Rich says.

Stay Vigilant

Staying a step ahead of hackers also means being careful with any custom-made software, Sharon adds, since these programs are rarely subjected to the rigorous security testing that popular, established software endures. Content Management Systems (CMS)—software designed to enable businesses to easily update their web sites—for example, are often custom-made. "A custom CMS is usually a bad idea," Sharon says.

Many employees also tend to get lazy about passwords. Surprisingly, one of the most commonly used password is P-A-S-S-W-O-R-D, a seemingly trivial oversight that has spelled the undoing of countless, otherwise stellar, computer security systems.

Sharon recommends complex alphanumeric passwords of more than 12 characters, which are tough to crack even by software specifically that's designed to crack passwords. And she reminds people to use different IDs and passwords to enter different gateways. Businesses looking to be especially vigilant about passwords can also use free, online password generators, like Secure Password Generator (passwordsgenerator.net), which will instantly generate long, complicated passwords for you.

Or they can purchase password management software that auto-generates complicated passwords, as well as centralizes all your IDs and passwords into a single, easy-to-use program. Top programs in this genre, according to PC Magazine, include Dashlane 4 (www.dashlane.com) and LastPass (lastpass.com).

Your business also need policies in place to establish lock-outs after a system user has entered a pre-determined number of incorrect IDs or passwords, Sharon adds. And the same lock-out fail-safe needs to activate the moment an employee departs or is terminated from your business.

For protection of especially critical data, Ira also advises multiple-authentication, such as the use of two or three passwords to access a web site maintenance account, rather than just one. And he says companies whose data privacy is especially critical should consider investing in data leakage prevention software.

Employees should also stay on the look-out for "social engineering" ploys, a fancy term for when a hacker forsakes the digital black arts and takes the easy route by tricking someone at your business into surrendering your crown jewels with a friendly phone call or a seemingly innocuous email. Regular meetings, e-newsletters or memos about security vigilance also offer an opportunity for you to update staff about the latest smoke-and-mirrors en vogue among hackers.

A popular hacker ploy lately, for example, is to regularly spam employees with marketing emails that seem to originate from a legitimate firm and include a handy "unsubscribe" link at the bottom. Unbeknownst to the recipient, clicking the link activates an invisible download of malware to their PC or other computer device—software that can be used to steal IDs, passwords, credit card numbers, client data and the like.

"Look at the link and see where it's coming from," Ira advises. If you don't recognize the company, or the link seems hinky, don't click it. There are, of course, other ways to further toughen your security. But at a certain point, you'll probably need to concede that your security will never be perfect; only hopefully, just good enough.

"Anybody who sells you 'perfect security' is a fool or a liar," Ira says. "What security is about is risk management. The more you elevate security, the more you're raising the bar, and the more exponentially you're decreasing your risk." **GP**

Joe Dysart is an Internet speaker and business consultant based in Manhattan. He can be reached at (646) 233-4089, by email at joe@joedysart.com or on the web at www.joedysart.com.