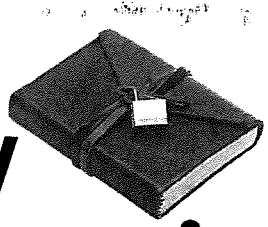


Security Manager's Journal

MATHIAS THURMAN

Vendors Can Make Us a Target

The data breach suffered by Target could make it easier to make some needed changes at our manager's company.

THANK YOU, Target! It's a pity that security managers have to capitalize on other organizations' misfortunes to broker change within their own enterprises, but the notorious Target breach of late last year just might get me some things I think my company has needed.

The breach may have occurred due to a gap in Target's vendor management program. Although the incident is still under investigation, it is suspected that an outside service provider that managed some of Target's heating and ventilation systems fell victim to a phishing attack that let the hackers gain access to Target's internal infrastructure and exploit resources containing customer data. I feel for Target, but this was the perfect scenario to accelerate action on findings that revealed shortcomings in the security of our company's vendor management program.

Last year, my security department approved more than 600 tickets for what we call "Vendor/Partner/Distributor," or VPD, requests. Typically, a VPD is a company or person who performs work based upon a statement of work. Since we don't have any fancy onboarding automation tools, managers simply use an online form to request access for a VPD.

Such requests trigger several email workflows. An email is sent to our procurement team to ensure that the vendor is valid and authorized to do work for our company and that the proper services and nondisclosure agreements are in place. Another email comes to my team, and we review the access request from a security perspective. A third email asks the help desk to provision an Active Directory account, an email address if needed, and an RSA software token for two-factor authentication to our partner VPN portal. Finally, the network team receives an email asking to add the user to one of our defined VPN profiles, which are configured to restrict general access to various applications.

About six months ago, we identified several weaknesses in this process. In some cases, vendors that no longer needed access still had valid accounts in our Active Directory server because the manager forgot to terminate the vendor's access at the end of a contract. To address this, we will create an automated process for terminating a vendor's access after a set period of time unless the manager requests an extension.

Another problem was that the network team too often failed to restrict access to the lowest level of privileges needed. For example, a vendor hired to modify some marketing material should have been granted access to a single document contained within a Microsoft SharePoint site, but its VPN profile let it access SharePoint, our financial servers, our HR systems and our source code repositories.

Join in the discussions about security! **computerworld.com/blogs/security**

> **The Target breach is the perfect scenario to accelerate action on some security lapses.**

Trouble Ticket

At issue: Gaps in the vendor management program could leave the company vulnerable.

Action plan: Use Target as an example to procure real change.

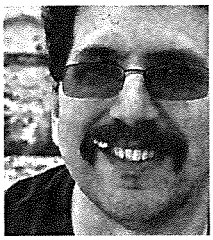
Even Worse

Both of those issues need to be addressed, but what really concerns me is that vendors have been allowed to download the VPN client and use it to connect to our network. Vendors are supposed to be restricted to a clientless VPN portal with links to needed applications. That keeps vendors' PCs off our network — PCs whose integrity we can't vouch for. But any PC using the VPN client is configured as a node on our network, just as if it were plugged into an Ethernet port in our office. That, of course, ups the chances that hackers can propagate malware or take advantage of an exploit and gain unauthorized access to our network.

To mitigate this issue, I've been pushing for the deployment of machine certificates to all company-owned PCs. No certificate, no remote access to our network.

There is some work to be done to tighten this process, but now, thanks to Target's pain, I have the perfect war story to gain traction for my plans. ◆

This week's journal is written by a real security manager, **"Mathias Thurman,"** *whose name and employer have been disguised for obvious reasons. Contact him at mathias_thurman@yahoo.com.*



OPINION

RON MILLER

When Will We Start Taking Security Seriously?

We must set the smartest minds to coming up with newer, safer and less complicated security methods.

A FEW WEEKS AGO, I was happy to hear that Target CIO Beth Jacobs had resigned. This wasn't only because falling on her sword was the right thing to do after her company's massive data breach. The fact that just days earlier I had realized that I was caught up in this mess had something to do with it.

My credit card was used several dozen times at a Mumbai shopping site, and I am convinced that it was compromised in the Target breach. But why didn't my credit card issuer's security algorithms pick up this obvious anomaly? Because I am a frequent traveler, I was told, the charges didn't seem out of the ordinary.

Really? Forty purchases from the same online shopping site didn't seem just a bit suspicious — even though, in all my travels, I've never been to India?

All of this has been smoothed over. Jacobs is out, I have a new card, and the bank will absorb all those bad charges. Still, I can't help but wonder whether there isn't a better way to do security.

As it turns out, I did do some foreign travel around the time that I discovered those Indian charges. I went to Barcelona for the Mobile World Congress. And while I was there, I peppered Gary Davis, a vice president in consumer global marketing at McAfee, with questions about the state of Internet security. He told me we should be seeing some real improvements shortly.

Today, most of us protect our accounts with a simple password. Many of those passwords are laughably easy to crack, as the list of last year's 25 worst passwords illustrates. Some sites try to remedy that by forcing users to create ridiculously complex passwords, but that just causes users to write the passwords down and leave them where anyone can see them.

And password complexity is a moot point when a database gets hacked and passwords are among the prizes. The same is true if someone installs a keystroke logger on your machine.

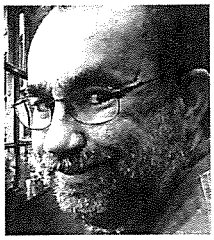
So how do we improve security? There are a lot of things we can do, Davis told me. For starters, he said, companies over the next five years are going to get better at detecting behavioral anomalies by building more detailed security profiles based on typical behaviors.

That could help, but making devices themselves more secure would help more. For too long, we've had nothing but password protection on mobile devices. Apple's and Samsung's moves to let you unlock your phone with a fingerprint are feints in the right direction, but not enough. How about a combination of face and voice recognition? Davis said those two things together would make devices very difficult to hack. And we have most of what we need to implement it. Nearly everyone today carries a phone equipped with a microphone and a camera. We just need some cheap recognition software to complete the picture.

We have other unique identifiers we can leverage, he noted, such as our retinas, our heartbeats and even the cadence of our typing. We already have the technology to wrangle all of those.

What's holding us back? It's clear that our credit cards, our personal devices and our networks are porous to anyone with a modicum of technological savvy. What's going to have to happen before we see that we must set the smartest minds to the task of coming up with newer, safer and less complicated security methods? For once, let's not wait for the worst. ◆

Ron Miller is a freelance technology journalist and blogger. He is an editor at FierceContentManagement and a contributing editor at *EContent Magazine*.



OPINION

S.J. VAUGHAN-NICHOLS

Who Needs Operating Systems? Not You.

Cloud-based apps have a lot to do with the end of the OS's dominance.

I WRITE A LOT ABOUT OPERATING SYSTEMS: Android, Linux, Windows, Mac OS and anything else you can think of. That's because I've always been fascinated by them.

I started working with technology in the late 1970s. Along the way, I've worked with IBM's mainframe OS/360, Unix on DEC PDP-11, and that ancestor of all PC operating systems, CP/M-80. Operating systems ruled your user experience; you had to care about which one you used.

But more and more, we aren't going to care.

Oh, if you're an engineer, programmer or techie you're still going to care. And I'm in no danger of running out of OSs to write about in my lifetime. But I can foresee a time when they will matter very little to users.

I'm not just talking about clueless users — "lusers," as disgusted techies dubbed them long ago. They will always be with us, if we're to believe the results of a recent Vouchercloud survey, in which 11% of the U.S. respondents said HTML is a sexually transmitted disease, 27% thought a gigabyte was a South American insect, and 23% identified an MP3 as a *Star Wars* robot.

No, even users who are aware that a motherboard isn't the deck of a cruise ship are going to stop thinking much about the operating systems their devices run.

If you want to see how little an OS can matter to the user experience, check out Google's Chromebook. It runs a Linux variation, but most of its users probably don't give that a thought. That's because the experience is ruled, not by the OS, but by the Chrome Web browser and all the software-as-a-service programs you're likely to run on a Chromebook, such as Gmail, Google Apps, Google Drive, Google Music and Google+ Hangouts, a de facto videoconferencing system.

Chromebooks were a niche product not so long ago, but market analyst firm NPD reported in December that they held more than 20% of the U.S. commercial PC market by the end of 2013. My view is that Chromebooks are going to challenge Windows PCs for desktop dominance as the decade continues.

Cloud-based applications like Google Docs have a lot to do with the end of the OS's dominance. It may be that even Microsoft, the king of the OS world, is preparing for this. Microsoft now offers the cloud-based Office 365. And plenty of other companies are following suit. Intuit's QuickBooks Online, for example, runs on all the major Web browsers, regardless of platform, as well as Apple iOS and Google's Android.

So companies are letting end users run the programs they want on any platform. They're doing this by moving applications to the cloud. Even when there is a local client, major business software vendors such as SAP are betting on Web-based HTML5 apps rather than operating system-specific clients.

Sure, there will still be some programs that demand powerful local resources, such as Adobe Photoshop, Apple Final Cut Pro and massively multiplayer online role-playing games that require a PC. But for most users (I'm going to put the figure at 95%), nearly all of their applications (99% doesn't seem unreasonable) will run off the cloud, and that is where users will store their data as well. What OS will they use to get to the cloud? Whatever.

As long as they can get to the apps they want, users couldn't care less. ◆

Steven J. Vaughan-Nichols has been writing about technology and the business of technology since CP/M-80 was cutting-edge and 300bps was a fast Internet connection — and we liked it! He can be reached at sjvn@vna1.com.