Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 13, Issue 8

An Advocate for Safer Things

By: Alan Zeichick

Stuff connected to our networks is vulnerable. Vulnerable to being hacked, with customer data stolen or corrupted. Vulnerable to being taken over and turned into bots that can launch Distributed Denial of Service (DDoS) attack. Vulnerable to serving as an attack vector into a business, school, hospital or government computer network. There's no doubt that there are vulnerabilities; we see reports of cyberattacks on the news every day. And like the tip of the iceberg, most of the attacks are never reported or seen.

Some might say that it's not our problem.

If you're a carrier, the argument goes, all you care about is the packets, and the reliability of your network. The service level agreement provided to consumers and enterprises talks about guaranteed bandwidth, up-time availability, and time to recover from failures; it certainly doesn't promise that devices connected to your service will be free of malware or safe from hacking. Let customers buy firewalls and endpoint protection – and hey, if we offer that as a service, that's a money-making opportunity.

If you're a security hardware, software, or service company, the problem of malicious bits traveling over broadband, wireless and the Internet backbone is also not your problem. Rather, it's an opportunity to sell products. Hurray for one-time sales, double hurray for recurring subscriptions.

Think about alarm systems in cars. By default, many automobiles don't come with an alarm system installed from the factory. That was for three main reasons: It lowered the base sticker price on the car; created a lucrative up-sell opportunity; and allowed for variations on alarms to suit local regulations.

My old 2004 BMW 3-series convertible (E46), for example, came pre-wired for an alarm — and all the dealer had to do, upon request (and payment of $$$) was install a couple of sensors and activate the alarm in the car's firmware. Voilà! Instant protection. Third-party auto supply houses and garages, too, were delighted that the car didn't include the alarm, since that made it easier to sell one to worried customers, along with a great deal on a color-changing stereo head unit, megawatt amplifier and earth-shattering sub-woofer.

But I digress. The dangers are real, and as an industry, it's in our best interest to solve this problem,

Not for distribution or reproduction.

not by sticking our head in the sand, not by selling aftermarket products, but by a two-fold approach: 1) encouraging companies to make more secure products; and 2) encouraging customers to upgrade or replace vulnerable products — even if there's not a dollar, pound, euro, yen or renminbi of profit in it for us.

Why bad things are a problem

There are many bad things connected to your network either directly or indirectly. My old Apple iPad 3, equipped with WiFi, can't upgrade to the latest version of iOS. While the tablet works great, it's getting older by the minute. How long will Apple patch vulnerabilities? Not forever. While iOS is inherently pretty secure, because of the sandbox model that Apple uses to lock apps out of the operating system kernel, it's not 100% bullet-proof. At some point, an iPad 3 user (maybe even me) might hit a malicious website that iOS 9.3.5 can't handle.

The problem is worse with Android, due to fragmentation. It's up to each device manufacturer to decide whether or not to push out a new version of Android to a WiFi-based device (i.e., like a tablet). If the device has a cellular modem (i.e., like a smartphone), the operating system upgrade might require the active participation of both the device maker and the provisioning carrier. What about the myriad Android-based Internet-of-Things devices, like cameras, stereos, smart watches? That's a gray area. There's no definitive word about who owns upgrades. If the product has been discontinued, nobody has much incentive. If the maker has gone bankrupt, nobody has any incentive.

According to Google, only about 31% of Android devices are running Marshmallow or Nougat, the latest versions of the platform. About 33% are running Lollipop, 23% are running KitKat, and a smattering are on even older, more vulnerable versions.

Obviously, this is not limited to just iOS and Android devices. Anything connected to the network can be subverted and attacked.

This is not hypothetical. The big Mirai-based malware attack in October 2016 was fueled, in part, by hacked IoT devices, including digital video recorders and Internet cameras that used components made by XiongMai Technologies. Those devices, which were made and sold by several companies under a variety of brand names, were then used to attack Dyn, a managed DNS service provider. Attacked! By DVRs and cameras!

The problem is deeper than operating systems. Users and devices are especially vulnerable to attacks if they are running old versions of Web browsers, or have old versions of plug-ins, add-ons and applications. Sure, zero-day exploits are a challenge, but unpatched known vulnerabilities are even worse because they are easily exploited – it's not hard to scan for them across the network or by reading Internet headers. Once they see that someone has an out-of-date mail server, browser, or other application, hackers know exactly what to do.

That doesn't explain why that's our problem, though. If some VP gets his email hacked and loses some corporate financial statements, that's his bad luck. Right? If a hospital administrator messes up with ransomware and ends up with an encrypted server that can't be salvaged, and that loses six months' of test results, it sucks to be a patient, but you can't blame the ISP. Right?

I am not a lawyer, but I think this is exactly our problem to solve. Not only because we have a moral responsibility to our customers, but also because in many cases, we are the only ones who might be able to detect the problem in advance of an attack. And, of course, if there's a major DDoS attack that hits one of our customers, or originates on our network, our throughput and performance and SLAs will be affected too. So, let us push for less insecure products, and encourage our customers to upgrade or replace vulnerable hardware and software.

Push for less vulnerable products

Depending on your company, you may have more or less influence across the agency. Certainly

Not for distribution or reproduction.

Verizon and Vodafone have more pull than, say, regional or specialized carriers. If you have pull… use it. If you resell products to your customers, don't resell them if they are not safe. If that means testing, then test. If that means partnering with independent labs, then do so.

Now go beyond that and publicize what you find. If products or services (and this includes cloud platforms) are not secure, publish that on your website, and in notices to your customers. Withhold your recommendation. Urge customers not to use those products due to the lack of security, or because the vendors do not adequately maintain them. Will this hurt? Yes. Might this cost you some partnerships? Yes. However, if you do not advocate for your customers' privacy, security and safety, who will? And after all, if those devices end up becoming corrupted and host bots that are used in a cyberattack, your network may be affected… and your business too, by bad publicity and possible lawsuits. Do what you can to keep your vendors from selling bad stuff, and to encourage them to fix vulnerabilities as quickly as possible – by any means possible.

Encourage customers to be safe and to upgrade

A few months ago, the doorbell rang. It was a representative from our city's water department. They noticed that our water usage had suddenly spiked. Was something wrong? There was indeed a leak in a pipe, and thanks to them, not only did we avoid paying for excess usage for more than a few days, but we also saved precious water (we live in Phoenix, which is in the middle of the Sonoran desert). Who better than our water company to know that we have a water problem?

In the same vein, every month I receive an email from APS, our local electric utility. They tell us how much power we have used, and also how that compares to our neighbors. They, too, are in the best position to see how my household is doing.

Imagine, if in every month, you sent your customers an email that indicated that you detected traffic originating on an insecure, unsafe IoT device, whether it's an industrial sensor, smartphone, smart cities camera, HVAC controller, or other devices with out-of-date operating systems – and include a link to a page about how to update that specific device. Or that if you saw they were using old browsers, old versions of Microsoft Exchange Server, an unsecured dbMongo server, or an orphaned and unprotected web camera. They may not know about the vulnerability. But you can detect this, and help them remediate the problem. If you want to.

That's a start. You can also provide real-time push alerts when the user attempts to use your SMTP server to send to a known phishing site, or attempts to download malware. Or, if you detect an unknown service trying to access a customer's home security system, or worse yet, modify its firmware.

Can you do that? Technologically, yes. How about the fact that you're a common carrier, aren't you imperiling your status if you look at customers' traffic metadata and took actions based on it? IANAL, but my own sense is that as long as you aren't giving preferences to partners, or penalizing non-partners, you may be fine. If there are regulatory roadblocks to protecting your customers, sunlight is the best disinfectant – and use industry groups to lobby to overturn them.

You can do this

Credit card companies can temporarily block transactions if they believe those transactions are fraudulent. That's to protect their own interests, of course, but in that case, their interests and those of their customers are in alignment.

I believe that everyone involved in carrying traffic has the responsibility to help protect consumers and business customers from malware, from being hacked, and from being hijacked. All of our customers are vulnerable, and we are in a unique position to take action. Will it be easy? No. But advocating, with and on behalf of our customers, for safer things is the right thing to do.

Not for distribution or reproduction.