Postcards From The States: Some Succinct Suggestions From A North American Cyber Security Consultant Sans Portfolio To His African Colleagues

Joseph St Sauver, Ph.D., University of Oregon and Internet2

Abstract—**This presentation will suggest a number of key steps you should be taking to improve the operational cyber security and the reputation and performance of your network, with each suggestion offered in the form of a "postcard." By employing a "postcard format," the key points are distilled into a set of succinctly described and readily tackled objectives.**

Index Terms—**Cybersecurity, Best Common Practices, Abuse, Deliverability, Domain Name System, Block Lists, Spam, Malware, Whois, Filtering, Monitoring, SPF, DKIM, IPv6.**

I. Introduction

African networks are rapidly assuming an increasingly prominent role in the global Internet community and the Internet is enabling key economic and social progress for all, but that progress may be hard to sustain given emerging operational cyber security-related concerns.

These cyber security concerns may be simple to articulate and easy (and cheap!) to fix if caught early-on, but if neglected, they can quickly result in difficult-to-diagnose-and-correct connectivity issues and even poor network performance as miscreants use up your network capacity and peer networks implement draconian self-defense measures against the abuse they may be experiencing.

This presentation will suggest a number of key steps which African network operators should be taking to improve the operational security, the reputation, and the performance of their networks, with each suggestion offered in the form of a "postcard." By employing a "postcard format," the key points will be (by sheer dint of space!) distilled into a set of succinctly described and readily tackled objectives.

Manuscript accepted October 7th, 2009.

Joe St Sauver, Ph.D., is Internet2's Security Program Manager (under contract through University of Oregon Information Services Division). Joe is also one of half a dozen senior technical advisors for the international carrier anti-spam forum, the Messaging Anti-Abuse Working Group (MAAWG). However, all opinions expressed in this paper do not necessarily represent those of Internet2, UO, MAAWG, or other organizations. The author's web site is http://www.uoregon.edu/~joe/

While these "postcards" are a literary device to help describe problems people may be seeing, the problems described are VERY real ones.

II. The Postcards

A. Postcard #1

I'm having trouble emailing you/getting email from you – are our emails getting blocked for some reason? Guess we'll just have to rely on snail mail postcards for now. Hope you're okay, my friend!

Anyone, anywhere can run into deliverability problems because of a "botted" system or because of a scammer/spammer customer. What matters is how you handle that problem if/when it occurs.

It may be tempting to try to just ignore these problems, but if you do, they're only going to get worse. If you have systems that get infected or you wind up with a bad customer using your service, clean them up, don't just try to ignore them.

Simple recommendation #1: Have at least one person dedicated to dealing with abuse issues, and give that person the authority to disconnect infected systems and the power to disable bad customers.

B. Postcard #2

Tried to find an email address for your postmaster, abuse guy, sysadmin, or network people to sort this out, but none of the addresses in whois worked. How frustrating!

When problems do arise communication can be key to getting those problems addressed. Unfortunately, all too often the communications channels that one would normally use to resolve particular issues may themselves not work. Examples of common problems include:

- Whois point of contact data may have grown inaccurate over time
- RFC2142-required abuse reporting addresses may be missing
- No one may be reading (and dealing with!) complaints sent to those addresses which do exist
- Mailboxes may be overflowing or misconfigured
- Spam or virus filtering may be getting applied to messages sent to those addresses, making it hard for people to report spam or viruses

At a minimum, make sure you have current domain whois contact information, current IP whois contact information, and current ASN (autonomous system number) whois contact information listed. Also be sure to check to make sure that the accounts required by RFC2142 are defined, work, and are read by someone. Particularly important accounts of this type are postmaster and abuse @<your domain>

Check www.rfc-ignorant.org for any listings for your domain, and make sure you've do have appropriate addresses listed at www.abuse.net, too.

If you're having widespread email deliverability issues, you may also want to think about offering a web-based contact form that people can use, too.

Simple recommendation #2: Make sure people can successfully communicate with your abuse staff!

C. Postcard #3

Tried visiting your ISP's web site today. Wow, it was really slow! Is it that slow for you all the time? I could hardly stand it! How do you and your family stand it every day? You should switch ISPs!

Transit bandwidth is obviously very expensive in Africa, so it is hardly surprising that many African ISPs purchase as little capacity as possible. What is surprising is that some ISPs do not carefully control how the bandwidth they do buy ends up getting used. For example, just to offer a few suggestions:

- Track usage of your connection's capacity with RRDtool so you'll be able to see if/when things "go crazy." You need an early warning system!
- Use deep packet inspection appliances (DPI) to analyze your traffic so you'll know how your bandwidth is being used -- is it going to flash video sites? Peer-to-peer applications? Porn web sites? Spam? DDoS traffic? Something else?
- Drop unwanted traffic before it can congest choke points on your infrastructure; often the same DPI appliances that can categorize traffic can also actively filter, limit or prioritize traffic.

If you let a few abusers use more than their fair share of your bandwidth, your good customers will take their business elsewhere to someone who can better meet their needs.

Simple recommendation #3: Take control of your network! Pay attention to what applications are in use, and use technical means to eliminate/control bandwidth abuse.

D. Postcard #4

Just had an idea. I wonder if a lot of your problems aren't related to the fact that your ISP's users are "anonymous?" If there was better accountability, maybe they could find and kick the bad guys out!

By implication, then:

- All access needs to be authenticated and controlled. There must be no network access by casual/unauthenticated ("walk-in") users.
- Online identities must be linked to real user identities as shown in national ID cards, passports, or similar documents, so that authorities can definitively identify abusers.
- All local email must be sent from the user's own account, via the provider's server, after authentication.
- The user's true identity should be included in message headers, X-Forwarded-For: headers, etc., to allow remote users to identify abuse sources.
- Because free web-based email services allow routine identity morphing and anonymization, access to free web-based email systems must be disallowed
- Use of abuseable anonymization facilities must be disallowed.

Simple recommendation #4: Identify your customers so you can hold them accountable for their online activities.

E. Postcard #5

Forgot to mention: once you know about customers causing problems, don't keep that info to yourself! Report those abusers to the authorities, and when you legally can, share that info with your peers.

Make sure your terms of service make it clear that:

- Abusers have no expectation of privacy,
- You will report abusers to authorities, and
- You will share information about them and their behavior with other ISPs.

Be sure to also provide some mechanism by which users can "appeal" being listing on a bad customer list.

Simple recommendation #5: Make sure your terms of

service allow you to share the identity of problematic customers with the authorities and other ISPs.

F. Postcard #6

Looks like some of our communication problems are purely mechanical. For example, I guess your IP addresses don't have "in-addrs," whatever those are. Maybe your ISP should try adding those?

We're all familiar with the use of DNS to translate domain names to IP addresses. For example, www.uoregon.edu translates to 128.223.142.89. This is done in the domain name system via an "A" record.

Many may not know, however, that you should also be able to do the reverse, converting IP addresses to fully qualified domain names via "inverse address" or "PTR" records. For example, there's a PTR record for 89.142.223.128.in-addr.arpa going to www.uoregon.edu

If you're an ISP and your IP addresses don't currently have inverse-address records, you should add them. Moreover, when you do add them, make it easy for people looking at them to tell if they're associated with dynamic DHCP pools, consumer broadband connections, wireless connections, etc., or a server.

Simple recommendation #6: Make sure you have forward and reverse DNS records for all your IP addresses, and use a meaningful naming convention.

G. Postcard #7

Another "mechanical thing" I just heard about: I guess your ISP isn't doing SPF or DKIM, either. Those are additional really good technologies that help control abuse and insure accountability.

Historically, mail from a particular domain could come from anywhere. Mail from a major credit card company could come from a cyber cafe in Eastern Europe (or Africa!) just as easily as it could come from the credit card company's real offices in California. SPF (see www.openspf.org) changes all that. Suddenly, a credit card company or bank or ISP can say, "Hey, the only IP addresses which should be originating mail as my domain are..." Once the credit card company, bank or ISP makes that sort of declaration, and ISPs begin to look for SPF records, mail for that domain can only come for authorized sources.

DKIM (see dkim.org) is another critical technology, allowing ISPs to cryptographically sign email messages as having come from one of their customers.

Simple recommendation #7: Begin doing SPF and DKIM, both for the traffic you send outbound and for the traffic you receive inbound.

H. Postcard #8

Also tell your ISP: they should get signed up for these things called "feedback loops." Feedback loops give your ISP copies of messages from them that are being reported as "spam."

To understand how feedback loops work, you should know that most web email interfaces have a "Report as spam" or "This is spam" button that users can push while looking at a message. When they push that button, a copy of the message with full headers is provided to the operator of the web email service so they can tweak their filters or take other steps.

One thing that many web email providers have begun to do is to share (sanitized) copies of those complaints with their apparent source, if you've signed up to receive them. A list of feedback loop signup websites can be found at the Spamhaus FAQ page. [1]

Simple recommendation #8: Sign up to receive feedback looks from all providers that offer them.

I. Postcard #9

Looks like your ISP has some entries on the Spamhaus Block List. Urge your ISP to get those problems fixed and those SBL entries removed! It would really help your email deliverability I think!

More than any other block list, people listen to the Spamhaus block lists (see www.spamhaus.org). If you've got entries on the SBL or XBL, you really want to get those problems fixed and those entries removed.

Simple recommendation #9: Check the Spamhaus SBL and XBL, and get any listings shown there cleared up. Consider listing dynamic ranges that shouldn't be directly emitting email on the Spamhaus PBL (Policy Block List), too.

J. Postcard #10

While I was talking with some network engineers, they mentioned that we're going to RUN OUT of IPv4 addresses in just a couple of years. Did you know this? Are you beginning to deploy IPv6 now?

Best estimates are that the regional Internet registries will run out of IPv4 addresses to allocate to ISPs on July 2nd, 2012 (see ipv4.potaroo.net). The bad news is that's less than three years from now. The good news is that IPv6 addresses are readily available now, and are well supported in modern routing hardware and in modern computer systems.

Any ISP that's NOT actively aware of this issue, and which

is NOT working hard to deploy IPv6 alongside IPv4 on their networks, will likely NOT be ready when IPv4 address exhaustion occurs.

Some ISPs have been pushing ahead with IPv6 thinking that it will improve their overall security; other ISPs have been holding back on deploying IPv6, worrying that it will undercut their current security. In reality, neither is true. To see the author's thoughts on IPv6 security-related issues, see "IPv6 and the Security of Your Systems and Networks." [2]

Some parts of the developing world may face special challenges when it comes to deploying IPv6, and that's because budgets may not allow wholesale replacement of non-IPv6 hardware with new IPv6-capable kit.

Use of open source operating systems and applications may help address parts of this challenge, but the developing world should also insure that IPv6-related needs are made known to international assistance organizations as soon as possible so as to allow time for the international community to provide necessary assistance for situations where only hardware upgrades will make IPv6 possible.

African ISPs should also be reviewing their current IPv4 usage plans, insuring that their current and foreseeable needs for IPv4 address space are up to date.

Simple recommendation #10: Review your current IPv4 address allocations, and begin thinking about/planning for deployment of IPv6 now.

III. The Email Messages

A. Email Message #1

It was great to just get your email, and to hear that you've been out of touch because of a camping vacation with your family! Sorry to have been worrying so much when it was just a power surge that took down your own system while you were on the road! I hate it when that happens to me!

Now that you're back home and on line again, what do you think of some of those ideas I sent along? Regards, Joe.

References

[1] http://www.spamhaus.org/faq/answers.lasso?section=ISP%20Spam%20Issues#119 (or http://tinyurl.com/y8u5z6s)
[2] http://www.uoregon.edu/~joe/i2mm-spring2009/i2mm-spring2009.pdf