ABO Proxy Review - 6/4/2014 10:00 AM

1. Present
   1. Shane
   2. Erik
2. What’s been done
   1. Research. Lots of research.
   2. Spoken with 7 consulting companies
3. What’s left to do
   1. Finish getting recommendations on solutions / confirm things work “the way we think they work” with consultants
      1. This has been tough. I haven’t been able to find a vendor that will take a look at our setup without some kind of “I WANT TO SELL YOU THIS PRODUCT” angle.
   2. Decide on a paradigm/scheme
      1. Once this is done, flesh out project plan
4. What we know
   1. The majority of information security threats currently come from 2 places:
      1. Employees
      2. Web protocol (application-level) threats
   2. The oldest (but still relevant) infrastructure/network security technologies are:
      1. Firewalls - Filter packets based on IP/Mac/Port rules
      2. Proxy Servers - Obscure identity of host server
   3. The previous (but still relevant) infrastructure/network security technologies are:
      1. IPS/IDPS - Intrusion prevention system - rule-based low-layer packet inspection and analysis that blocks attacks based on signatures
   4. The current infrastructure/network security technologies are:
      1. UTM - Unified Threat Management - May combine Firewall, IPS, gateway antivirus, gateway anti-spam, VPN, content filtering, load balancing, data leak prevention, and on-applicance reporting.
      2. NGFW - Next Generation Firewall - Firewall with integrated IPSs (and sometimes WAFs) that work together to prevent attacks and unauthorized traffic. Ex: Can identify BitTorrent traffic being tunneled through HTTP.
      3. NGIPS - Next Generation IPS - IPS that inspects low-layer as well as upper layer (application) traffic. Can do things like block access to known malware sites and update definitions on the fly. Can do some HTTP inspection but generally not as focused as a WAF.
      4. WAF - Web Application Firewall - Rules-based security technology that performs inspection of HTTP traffic and identifies attack patterns and common exploits (SQL injects, XSS attacks)
5. What our options are for ABO proxy replacement:
   1. From least expensive, to most expensive:
      1. Repurpose existing computer to use identical modproxy setup in case of failure, test periodically. Have identical machine on hand with identical setup.
      2. CloudFlare Free (no WAF) - Reverse Proxy & CDN
         1. Requires that we change DNS for avantipress.com to CF nameservers (or use independent domain)
      3. CloudFlare Pro (basic WAF, $20/mo) - Reverse Proxy & CDN
         1. Requires that we change DNS for avantipress.com to CF nameservers (or use independent domain)
      4. ASA w/ NGIPS - (Approx. $800 quote for HW from Logicalis)
         1. Sit between preexisting ASA and Sweetpea (or replace preexisting ASA)
      5. WAF ($7.5K - $50K)
         1. Sit between NGIPS/ASAs and Sweetpea
      6. Employee Training - Variable cost, have not priced this out so putting last.
         1. Training employees about information security
6. What I’m looking at based on the information so far:
   1. Use CloudFlare - We should have a reverse proxy in place. Putting a server out there directly on the internet is not a good idea. CloudFlare does this (my personal website hostname based on pinging the domain www.distractal.com):

PING www.distractal.com.cdn.cloudflare.net (104.31.73.48): 56 data bytes

64 bytes from 104.31.73.48: icmp\_seq=0 ttl=56 time=10.894 ms

64 bytes from 104.31.73.48: icmp\_seq=1 ttl=56 time=23.361 ms

64 bytes from 104.31.73.48: icmp\_seq=2 ttl=56 time=26.239 ms

^C

--- www.distractal.com.cdn.cloudflare.net ping statistics ---

3 packets transmitted, 3 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 10.894/20.165/26.239/6.660 ms

Actual IP address:

173.236.174.242

We should use CloudFlare, and configure the firewall (or other intermediary device) to only accept port 80 traffic on that IP, and only respond to traffic from CloudFlare’s IPs.

We will need to set up and test CloudFlare ourselves. I have not found any consultants that perform CloudFlare implementations, and CloudFlare themselves said they do not current know of any nor offer any.

To do this we will either need to reconfigure avantipress.com to use CloudFlare, and turn off CloudFlare proxying for all subdomains except abo.avantipress.com, or utilize a separate domain name for ABO.

* 1. Use WAF or ASA w/ NGIPS (or both)

This cuts both ways. We already have an IPS, but it doesn’t perform upper layer inspection.

With CloudFlare we already have a basic WAF, but a dedicated WAF is substantially more robust.

I intend to speak with our consultants and determine which solution fits better (obviously the ideal would be to do both).

* 1. Train employees

I think we may have had one or two (maybe you or Tai?) security trainings in the past but I think another one might be beneficial. Especially when I overhear stuff like “I got a suspicious email and I wasn’t sure if I should open it but I did anyways” and when people are forwarding us mail they are unsure about (possibly allowing threat propagation).

1. Summary
   1. As you mentioned, our current ABO setup utilizes security through obscurity. We hide the ABO IP behind a username and password on our Joomla site and hope nobody figures out how to find it.

But that’s easily bypassed:

(from searching Google for Avanti Back Office):

<http://www.avantipress.com/cards/70-reps/abo> (link to ABO right in middle of page)

<http://www.avantipress.com/cards/82-reps> (link to ABO at bottom of page)

My recommendations are based on putting up adequate defenses for today’s attacks, for our web-facing systems.

If the ABO Proxy replacement goes well (and depending on what we end up doing) we may want to consider doing something similar for our other subdomains and web-facing systems.