ABO Proxy Replacement Meeting

Date: 06/10/2015

Time: 2:00 PM

Location: Lewis-Edwards Conference Room

Present: Shane, Erik

# Agenda

1. Recommended/best practices security setup for web-facing servers (from a variety of sources, but most prominently (<http://social.technet.microsoft.com/wiki/contents/articles/13974.security-best-practices-to-protect-internet-facing-web-servers.aspx>)
   1. Firewall on the outside
   2. Reverse proxy
   3. IPS/IDS
   4. WAF
2. Erik to determine – Is it possible for us to implement a DIY solution on our own?
   1. Possible? Yes. But we just don’t have the experience, training or the ‘leeway’ if something goes wrong. I think implementing this ourselves would expose us to risk that we might not even be aware of. I think we should definitely have someone assist us with implementation.

I checked in some online forums (SpiceWorks, mostly) and they made the good point that if we do implement it ourselves, we are fully responsible for configuring it as well as maintaining it afterwards – host OS patches, IPS/WAF definitions and patches.

They also recommended we go to a hosted solution as soon as possible. I realize that’s probably not feasible.

We can usually configure the WAF/IPS to update its definitions automatically, but we would still need to manually perform updates on the apps themselves and the host OS.

1. So what next?
   1. Several folks recommended a UTM solution, specifically Sophos. Taking a look at this solution it is promising. It has ALL of the above – Firewall, Reverse Proxy, IPS and WAF.

Gartner lists their solutions as a leader (Checkpoint and Fortinet being the absolute best) for UTM.

* 1. I have been checking with “IT and Network Consulting” companies, and ones that target larger businesses. I am going to check out there for security consulting companies and talk to some of the consultants that I have yet to touch base with