Making the Business Case for Email Authentication

Introduction to DMARC.org

DMARC.org is an initiative of the non-profit Trusted Domain Project (TDP).

The mission of DMARC.org is to promote the use of DMARC and related email authentication technologies to reduce fraudulent email, in a way that can be sustained at Internet scale. This overall goal is met by educating individuals and organizations through a combination of articles, tutorials, presentations, and webinars.

For more information, please visit https://dmarc.org

For more about TDP, please visit http://trusteddomain.org

Introduction to DMARC.org

The work of DMARC.org is made possible through the generous support of these sponsors:

Overview

- Prerequisites for Success
- Making the Business Case for Email Authentication
- Implementation
- Why You Want Others to Succeed Too
- *Never Give Up, Never Surrender!*

Prerequisites for Success

Prerequisites for Success - Scope

- This is not a once-and-done project
  - If so you'll have to repeat it
  - Would you be able to line up the same support again?
- Don't limit it to one domain, or customer-facing domains
  - Make it about how you use/protect email company-wide
- Emphasize that at the end you will have new processes and better controls around email
  - Risk Management
  - Control of Domain Assets
  - Governance and Compliance
  - Efficient Processes (lower on-going costs)
  - More KPIs and metrics that can be tracked

Prerequisites for Success - BAU

- Your project will create established, continuing processes around the provisioning and use of email/domains
- For the initial efforts, find a way to work within whatever project framework is already accepted
- The more this looks like “just another project,” the less likely you’ll encounter resistance because you’re “special”
- Maybe less likely to be treated as a “one off” project
- The more your processes fit within established practices, the more likely they’ll endure

Prerequisites for Success - Authority

- You need the authority to establish policies & processes
  - If you have it, or can assert it: *Bravo*!
  - Otherwise an executive sponsor may be required
  - Somebody who understands and can accept the risks
- What kinds of risks need to be accepted?
  - Might block legitimate email to customers temporarily
    - Is 200 okay? 2,000? 20,000? Is there a limit?
  - It may take a few hours to a few days before a report uncovers a problem
  - Do you have groups that assert such outages cause the loss of millions of dollars?

Building Strategic Support

- In large, balkanized organizations the support of other teams can be invaluable
  - Customer-facing business units
  - Information Security
  - Compliance and Audit
  - Beware of *Unstated Expectations*…
    - "This guarantees reaching the inbox, right?"
- What are the success metrics or goals for these groups?
  - Figure out how Email Authentication meets them
  - Broad metrics and trends
  - If you don't have a good measure of fraud losses tied to phishing, it can be tough to build across organization

Who Are Your Partners?

- Do you depend on other internal or external teams to execute day-to-day?
  - Do you know who all these players are?
  - Who maintains DNS, for example?
  - Is there a devops or SRE group that would consume the stats from DMARC reporting?
- Will you have to (re-)negotiate contracts if you change procedures?
  - Usually found in cases where functions have been outsourced
  - Have you built a base of support that will allow for any increased costs – or fight the vendor over such increases?

Vendor Support

- You may have many vendors to consider too
  - How many already support the protocols and policies you need to implement?
  - Will any of them require negotiations or payments?
  - Check `https://dmarc.org/resources/`

Making the Business Case for Email Authentication

Explaining the Risks in Business Terms

Phishing increased 700% from 2008-2012, and 67% of those attacks targeted financial and payment services companies. Total cost, nearly US$8 billion.

-- Gartner Group

A successful attack on 500 customers can cost up to US$1.4MM

-- cisco Systems

There are many ways that having criminals impersonating your brand, sending fraudulent email to customers and partners, can hurt your business…

Financial and Payment Services companies targeted in over 61% of phishing attacks.

-- APWG Reports, 1Q-3Q2014

Consumers are 42% less likely to do business with a brand for which they receive phishing messages.

-- Cloudmark

Direct Connections and Don't Over Promise

- A major bank loses millions each year to "routine" phishing that targets their consumers – direct losses, increased customer support, stalls "paperless" initiatives uptake, more
- The most effective phishing uses your own domains
- Email authentication can prevent this, forces attackers into more detectable methods like "display name" manipulation

```
From: Bank Of America Alerts <onlinesecure@ealertonlineboa.com>
Return-Path: <ogrodosf@ogrodosfera.pl>
```

- Proceed with DMARC to eliminate most blatant threats, get reporting data, and prepare for the next protection measure
- Email authentication is a critical part of customer protection

More Business Case Drivers

- Limit or lower your fraud losses
- Preserve email as a viable, low-cost channel
- Customer loyalty
  - “Hey, they’ve got my back! Maybe I don’t mind that they charge me X% interest so much…”
- Protect brand/reputation
  - “I get so much spam from you guys!”
- Avoid negative publicity
  - “I don’t ever want our company on the front page of the Wall Street Journal because we didn’t do this.”

Implementation - Execution

Success is All About Execution

- To do it right, you must have your house in order:
  - Inventory of domains (in production, parked, whatever)
  - … and vendors/partners sending on your behalf
  - Processes and policies around domain registration, contracting for services that send email, etc
  - Control of corporate gateways (especially the ones you don't know about - or acquire)
  - Procedures to respond to alerts generated from DMARC reporting data

Getting Started

- Where will you keep the information you gather?
  - Easy to access, easy to update, appropriate controls
  - A wiki, Sharepoint site, a database…
- Do you know what domains you're using?
  - Is there an inventory being kept, or are you creating it?
  - When and how are new domains or sub-domains brought into service?
  - Can you change that process so new domains are added?
- Who are the owners or primary users of each domain?
  - Record points of contact and keep up to date
  - Can you make this group or manager an ally?

Getting Started – Collecting Data

- Establish a mailbox to collect reports
  - Could be many dozens per day for aggregates
  - Hold off on failure reports until you have a picture of volume
- Consider engaging a report processor vs. coding
  - See `https://dmarc.org/resources` for options
  - Could start with a free trial and then decide later
- Publish a "`p=none`" policy for each domain
  - Start familiarizing yourself with what's actually happening
  - Establish baselines or characterizations of each domain
  - See if you do in fact have a problem, and if so what's your best candidate domain for testing a solution?

Getting Started - Socialization

- Socialize the problem(s) you've decided to try to address
  - Pick one or a few domains that clearly have problems
  - Inform those impacted, and/or who you think will need to sign-off of larger parts of the project down the road
  - Describe what results you expect, and why you think that's an accurate assessment
- If you need to establish change controls, do that
  - Many organizations already have it and don't need more
  - But if not, remember you want to establish procedures for this
- Make a deployment plan and share that with your stakeholders and interested parties
  - Set your dates and stick to them, or explain why not

Getting Started – Deployment

- Deploy your “blocking policy”
  - Doesn’t matter if it’s `p=quarantine` or `p=reject`
  - Remember to keep your stakeholders informed as you go
  - That definitely includes any executive sponsors
- Monitor very closely over ~48 hours
  - Aggregate reports will trickle in from Receivers over this period
  - Try to make sure you catch problems before customers do
- Make sure your procedures for alerts are working
  - If the reports do indicate something’s up, this is the “live test” of both your alerts and response procedures

Getting Started - Measurement

- Compare a few weeks of traffic before and after
  - Did you get the results you expected?
  - If not, any indication why not?
- Present results internally
  - Doesn't have to be anything too formal
  - Think about who you want to work with on the next deployment
  - Make sure the benefits you talked about are clear
- Remember to keep it simple – don't over-promise
  - You'll never block every bad message
  - Make sure nobody sells it that way, internally or externally

Getting Started – Rinse, Repeat

- Run down the list of candidate domains and schedule a deployment date for each
  - As your team gains confidence in procedures, consider your tolerance for overlapped deployments of multiple domains
- Deployment for each domain should follow this model
- Remember to keep the reporting going
  - And provide results to the stakeholders!

Why You Want Others To Succeed Too

You Don't Operate In a Vacuum

- Your customers are our customers, and vice versa
- If they're *pwned* due to phishing of your company, or their city government, or the local supermarket chain, we still get hit with fraud losses
- Your ability to protect your brand is my concern too
- This justified:
  - Speaking at conferences
  - Working on open standards vs. proprietary stuff

Never Give Up, Never Surrender!

Never Give Up, Never Surrender!

- Depending on your organization, or your partners and vendors, you may encounter resistance. Perhaps a lot of resistance
- Institutions and the people in them resist change
- The business reasons for deploying email authentication are on your side
- Every headline-grabbing data breach shows how much your customers are at risk
- Be patient, build your case logically, and be persistent

Questions?