Stumbling through the Infosec forest

Some things I learned in the woods

Jim Klun/Microsolved

- 30+ years in IT (B.S. in Computer Science, 1979 Ohio State)
- 10+ in an increasingly global InfoSec organization (hello Bangalore!)
- Technician/Manager/Security “Architect”
- Now at Microsolved (doing unto others…)
- http://www.microsolved.com
- jklun@microsolved.com

MSI
MICROSOLVED,INC.

What I learned

- **Death by Silo**

*“*We have met the enemy and he is us” Pogo / Walt Kelly

- **The view from outside the bunker**

“And would some Power the small gift give us, to see ourselves as others see us!” To a Louse / Robert Burns

- **The dangers of third party infrastructure**

We’re here to help! Really!

- **So you say you’re patching?**

Really?

1. Death by Silo

Meaning: Bureaucracy + Human Nature = **Breach**

Bureaucracy essential – but dangerous

- Needed for repeatable business flows
- Dangerous in that they can slow recognition/adaption to new threat
- Silos of identity/communication form (“Those 3rd floor people!”)
- Events of real security significance go unreported
- Either out of ignorance or “not my job”
- So a breach goes undetected for months – or years.

  "On average, organizations take **229 days to detect a data breach**, according to a recent study from the cybersecurity firm FireEye."

  http://www.bankinfosecurity.com/speeding-up-breach-detection-a-7604/op-1

The best “Intrusion Detection System”?

Your own people!

- Engage them – across the silos
- Educate them to detect anomalies and not shrug them off
- Educate means more than a yearly “Acceptable Use Policy” signoff.
- More than just some yearly “click as fast as you can” web course
- Security awareness needs to be a constant theme
- Regular awareness emails relevant to your people
- Security website specific to your organization
- Create reporting mechanisms that go straight to your own security staff. (You have dedicated security staff, right?)

Past Life: What we did

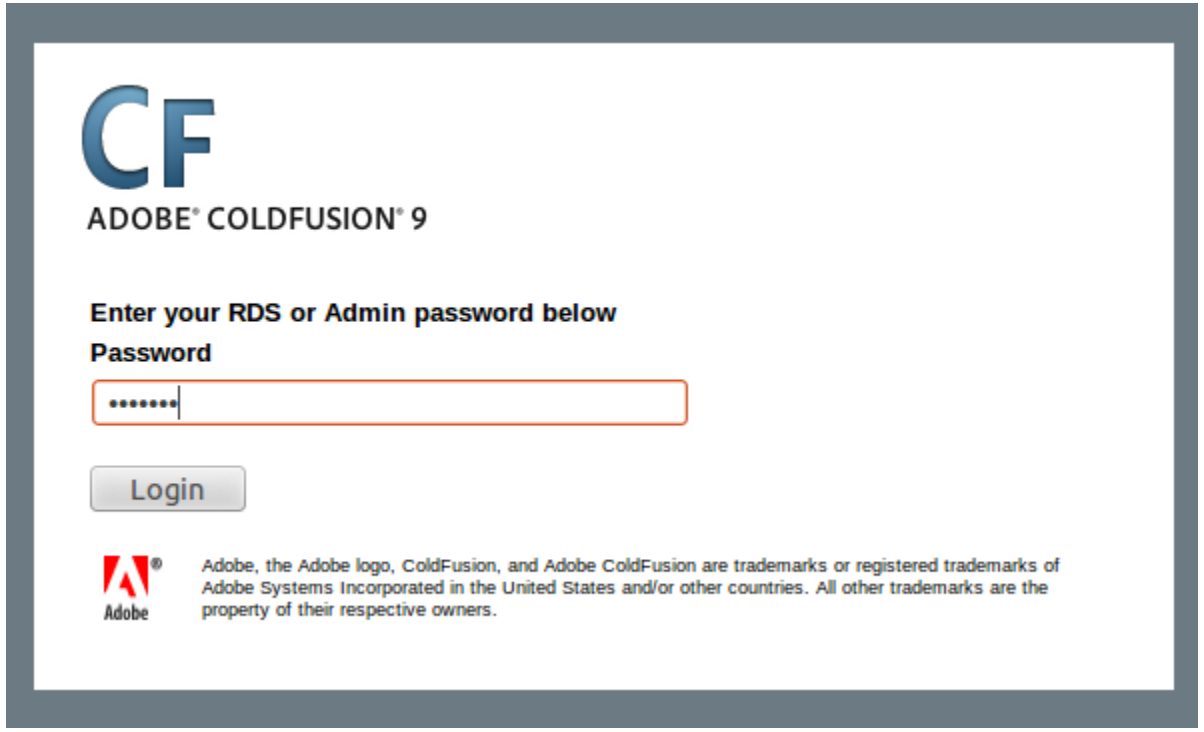
- Monthly security meeting – all invited
- Dedicated security website – stuff that applied to our organization
- Frequent – weekly – security awareness messages about current threats to end users. e.g. current phishing attacks, home router vulnerabilities, banking scams, etc. Stuff people care about.
- Reporting email address: security@our_organization.com
- We encouraged reporting and when good info came in we analyzed, summarized, and posted results on the website
- Publicly thanked the reporter on the site and in awareness emails
- It worked – we learned of things much earlier
- People felt they were an integral, helpful part of the effort – not its victims.

2. The view of your “bunker”

Here is what your people see when they drive to work:

Here’s what attackers (that’s me) see:

And one of my favorites:



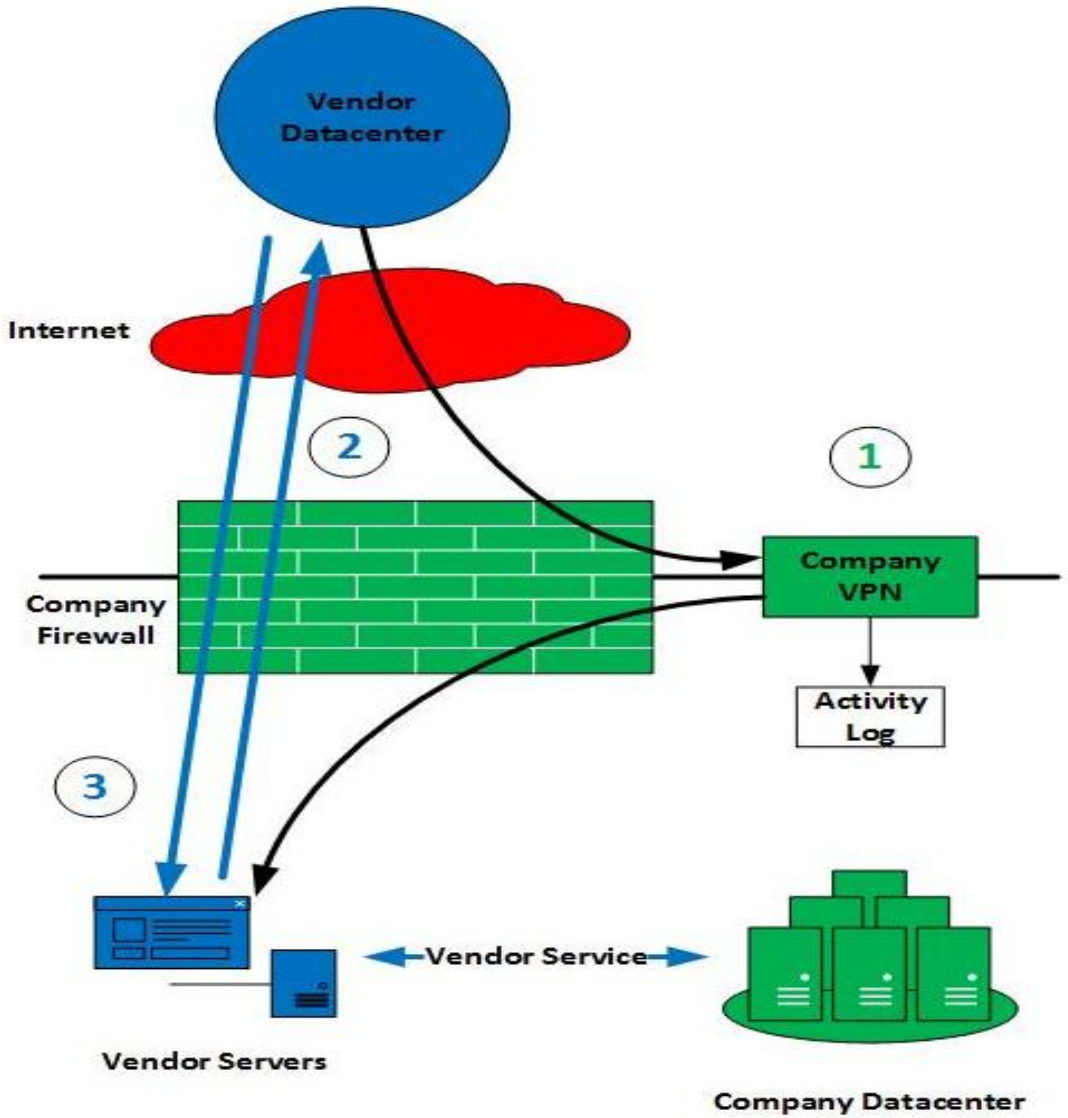
The point: organizations do not know what their Internet “face” looks like.

- You must know what your Internet perimeter really is
- Do NOT assume someone knows and is taking care of it
- Make sure it is well-defined and regularly assessed
- Remove all unneeded exposures
- Do **NOT** allow administrative interfaces to be exposed to outside
- One mistake on the inside – default password re-instated – and you are toast.
- http://stateofsecurity.com/?p=3341 - discovery “how to”
- http://stateofsecurity.com/?p=3216 - datacenter “attack surfaces”

3. Third Party Infrastructure Risks

- Following example is a recent discovery of mine
- Organization was public sector
- You?
- See: http://stateofsecurity.com/?p=3605

Third party monitoring service



Unplanned Vendor Connectivity

Vendor contracted to perform administration services for company datacenter

1. Vendor was provided company VPN access with expectation that it would be used for access to vendor's on-premise equipment.

2. Instead, vendor established outbound site-to-site VPN from their equipment, through company firewall, to their datacenter.

3. Vendor routinely accessed their equipment across the site-to-site VPN they controlled. Company had no record of vendor access or activity.

Vendor and company infrastructure are now joined, without the company's awareness.

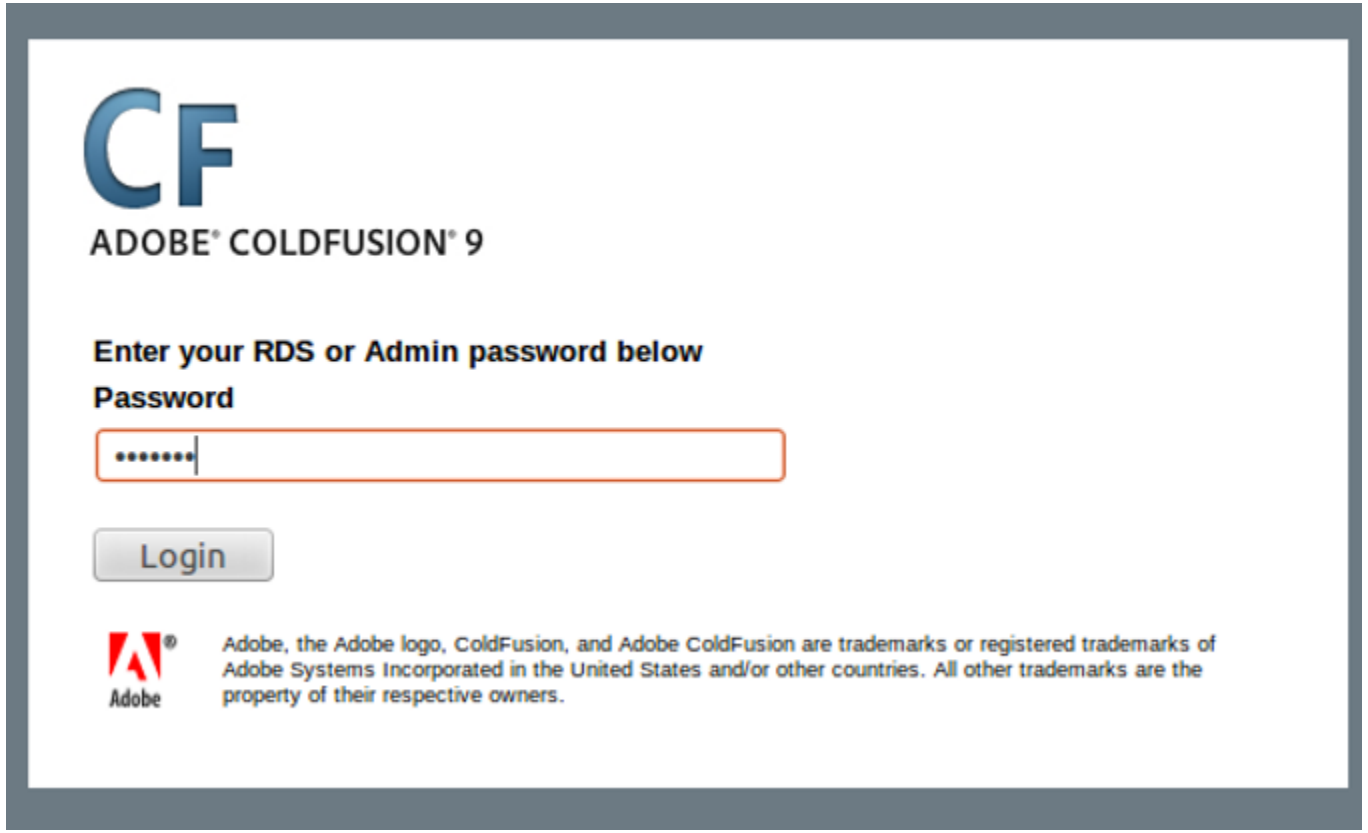
You cannot blindly trust vendors

- In the illustration, vendor techs were just doing their job
- But what they created was not what the customer staff expected
- It was a management decision, not aggressively vetted by staff
- As a result, an unmonitored path into the organization was created.
- Another one: Got security cameras?
- "*doveryai no proveryai*" It's an old saw at this point, but always true. **"Trust, but verify"** https://www.youtube.com/watch?v=As6y5eI01XE (Reagan/Gorbachev)
- Oh – and watch your logs! Example discoverable in network logs.

4. So you say you’re patching?

- You probably are
- You subscribe to Microsoft security announcements
- You have a regular window for the application of maintenance
- All good!

Or maybe not……


CF
ADOBE® COLDFUSION® 9
Enter your RDS or Admin password below
Password
Login
Adobe
Adobe, the Adobe logo, ColdFusion, and Adobe ColdFusion are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

Third party software patching critical!

- Such software is often more important to security than the OS.
- It’s part of the periscope sticking out of the water
- It’s what attackers see and what they go after
- ColdFusion, Apache, PHP, Oracle Web Apps, Java, etc…
- All such delivery software must be part of coherent, mandatory patching
- Often service delivery organizations resist that
- Delivery of service is what they are measured on – not security
- See that earlier discussion about “Silos”.
- http://blog.securestate.com/third-party-web-applications/

What to do?

- Knowledge of your Internet face plays a role
- Know it – and all supporting software used to deliver service
- Make sure every component that is part of service delivery is also part of a patching program
- Subscribe to vendor alerts
- Talk with one another!
- **Management must ensure no communication barriers exist**
- Fight the Silo effect
- Perform regular (monthly?) security assessments - at least from Internet
- Things degrade quickly – be prepared to catch those mistakes

Thanks!

Discussion

- What is your world like?
- Do people talk?
- Is there an organized security communication effort?
- Is it real – or just another Silo?

- jklun@microsolved.com