Small IT Shop Challenges

BAD THINGS DON'T CARE ABOUT SIZE

Nico Stein – AVP of IT at a medium sized Financial Institution

VMUG
VMWARE USER GROUP

Originally started at IBM Germany

DC-VMUG Co-Leader

Connect with me on Twitter: @NicoAStein

LinkedIn: linkedin.com/in/nico-stein-3404171

Or at my blog: https://nicostein.com

SCAN
ME

Challenges:

- ❑Audits
- ❑Penetration Testing
- ❑Security as a whole
- ❑Automation
- ❑Continuous learning
- ❑Team Building

Audits:

Financial Institutions get Government audited once a year with heavy focus on IT

❑ Audits are stressful and add a load of workload. Depending on the auditors there can be valuable lessons for improvement though

Penetrations Tests:

From my experience one of the most valuable investments

- ❑ More affordable than one might assume
- ❑ High probability of massively increasing your security posture
- ❑ If budget concern arise, point out the cost for announcing a breach of your customers data. There is such a thing as bad PR.

You can't fix what you don't know is broken

❑ In 2020, the average business cost of a cyberattack is $3.86 million and it takes over 200 days to detect the breach. (IBM)

❑ Cyberattacks projected to hit $6 trillion in annual loss in 2021 which has doubled since 2015. (Cybersecurity Ventures)

❑ Cybersecurity spending estimated to exceed $1 trillion in 2021. (Cybersecurity Ventures)

❑ There will be nearly 3.5 million open cybersecurity jobs waiting to be filled this year, with over 500,000 open positions in the United States alone. (Net Sparker)

❑ 68% of business leaders felt the risk of a cyberattack increasing. (Accenture)

❑ A majority of cyberattacks are motivated by financial gain, nearly 86%. The second leading motivator of a cyberattack includes state espionage. (Verizon)

Source: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

Security:

How can we protect our system with a limited amount of staff?

- ❑ Leverage the power from the big shops without all the implementation headaches
  - ❑ Cisco Umbrella is a great tool to get all the security feeds from huge shops, while it still can fit smaller budgets.
- ❑ Security logs; They are important, but usually not enough manpower in house – This can be outsourced
- ❑ Make sure your users don’t reuse passwords. Connect your ActiveDirectory with have I been pwned?

Like any shop we need to have lines of defenses

Automation:

One of the biggest struggles – How do I find the time to learn/implement automation when doing it manually would take a fraction of time per task?

- ❑ A good example is verification of backups. Can it be automated? Can I prove my backups work?
  - ❑ Veeam SureBackup can help with this

Continuous learning:

Like any other shop, dedicating time is difficult.

- ❑ If budgets allows, have some seats for Pluralsight, CBT Nuggets….
- ❑ Invaluable resources are user groups and conferences. (Like this one!)
    - ❑ You get to benefit from talking and learning from peers that might run much bigger installations and bigger challenges.
    - ❑ You might be able to "test-drive" solutions that are not applicable to you, yet!

Team Building

None of it matters if you can't rely on each other

- ❑ Especially in smaller shops we wear many hats
- ❑ Welcome to the "hyperconverged" administrator
- ❑ Have team events, but don't make them just another forced task
  - ❑ Try to vary it. If someone doesn't attend, no judgement
- ❑ IT is stressful, especially when things break. But during the hardest times teams are build that will last.
- ❑ Everyone makes mistake. Don't make your team members afraid to fail.
- ❑ Lead by example.

Q&A

Thank you for attending this session!

Last year we did a podcast on this subject. You can check it out at ITR (IT Reality, Episode 32) with Vince Wood, Jim Jones and me.

SCAN ME