Minutes SIGS 2nd Zero Trust Forum - Breakout Session 2:

Rafik Chaabouni, Head IT Security at Rothschild & Co. Bank AG - Navigating the Zero Trust Journey: Challenges and Insights

Notes and take aways from round 1:

Status on the ZT journey:
Most of the Attendees reached some maturity on ZT already and defined a sort of Baseline, some are using NIST for the maturity evaluation, some did other assessments, few have a road map to follow. Nobody has reached the stage: Automation yet. Some are still at the beginning of the ZT Journey, doing discoveries, though.

What are some of the mechanisms/current methods on moving forward on the ZT journey mentioned:
Defining how to do micro segmentation, moving away or reducing VPNs, do not talk about ZT: show me the next step

Biggest challenges:

1. Asset Management, also combined within the next step of the maturity: data classification
2. Proper Identity Management, Access Management, proper source of truth
3. Shared responsibility, also in combination with SaaS
4. Data, data classification and management
5. Enabling usability when dealing with issues
6. Where to start, management buy-in, convince others to join the journey

Key take aways:

- Do the basics!
- Align Infosec and IT-Sec in your organization and find the same language
- Use frameworks to help you

Major questions:

- Where to start on the ZT journey?
  There were several different answers to this.... A good start would be in the international standard frameworks.
- Do we need data classification first or other mechanisms instead, for example proper rules?
  No final answer was given...but all agreed that this topic is very relevant to be clear on in the individual set up

Notes and take aways from round 2:

Status on the ZT journey:
Most of the attendees just started on the ZT journey, defining how to move forward with management buy-in or how to consult clients, some are doing assessments, ZT is in the beginning, and some are here to be inspired, one already moved quite a bit on the journey

What are some of the mechanisms/current methods on moving forward on the ZT journey mentioned:
Inform management about what you are doing, do not necessarily mention ZT, integrate architectural program and define a structured yearly plan to receive management acceptance, implementations based on ZT are a success, but not mention the name ZT!
Isolate your crown jewels

Biggest challenges:
1. Asset management
2. Working in silos
3. Shared responsibility
4. Awareness about data classification
5. Lacking understanding own business model
6. Cultural challenges, CH is not USA

Key take aways:
- Define ZT mindset, take others on your journey with you, share your experiences
- Align Infosec and IT-Sec and define realistic goal in order to integrate it in your program successfully
- Use frameworks in order to evaluate where you are and what are the quick wins
- Define ZT principles and implement partially based on risk and value of your assets/data

Some questions asked:
How far do you want to go on your ZT journey? All the way, if possible, mostly partial implementation intended, all in would be also too expensive
How do you establish continuous authentication/authorization – is it not a huge step?
Implement risk based and prioritize high-risk apps first