February 6th-7th

NIC 20/20 VISION

Oslo Spektrum

Assume breach. Notes from the field.


NIC

Michael Simon Arntzen

blinQ

Twitter: @msarntzen

60 minutes

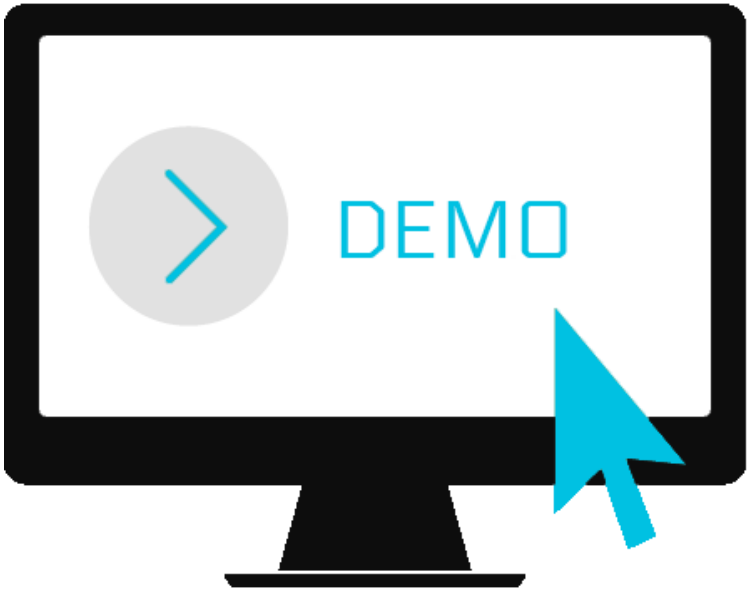
- When the s..t hits the fan, what then?
- Assume breach…
- Spear-phishing. Two attacks in one month

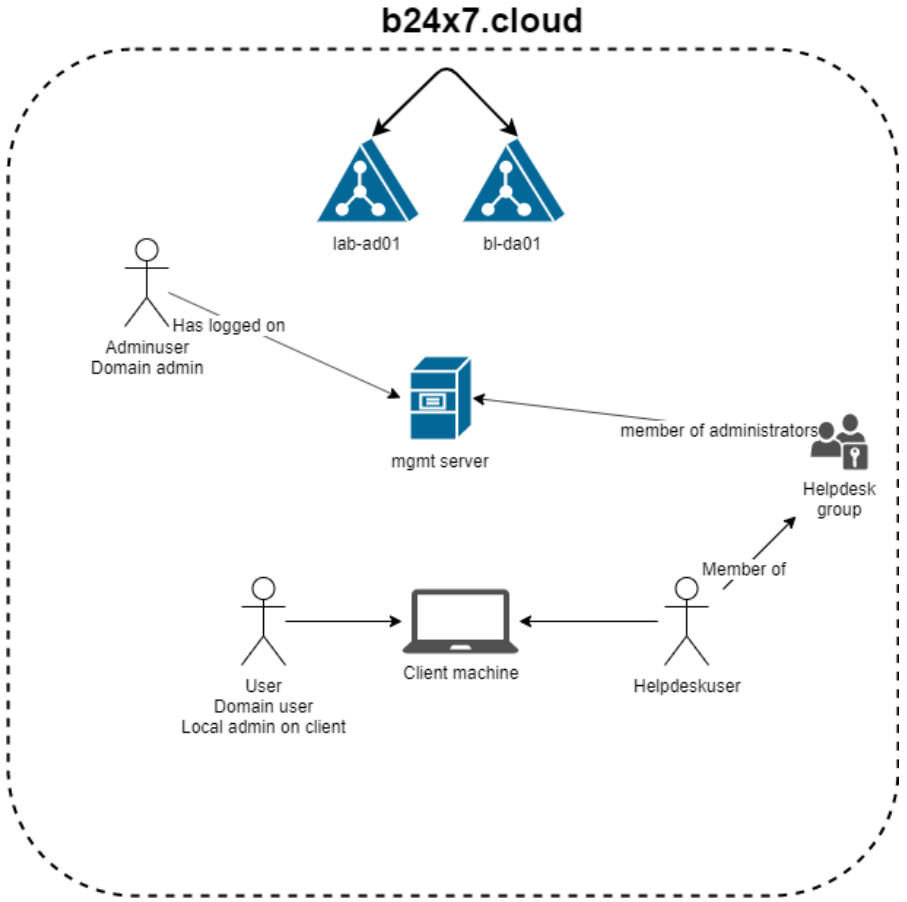
When the s..t hits the fan, what then?

Hopefully, the following is in place

- Azure Sentinel (SIEM. Security Information and Event Management)
  - Forensics (e.g when, where, account/s)
- Business continuity plan. Must include Cyber incident response
- Documentation
- System recovery procedures.
  - Forest recovery
  - Common scenarios recovery
- Already know how high impact you can handle before….

Assume breach…


DEMO


b24x7.cloud
lab-ad01
bl-da01
Has logged on
Adminuser
Domain admin
mgmt server
member of administrators
Helpdesk
group
Member of
User
Domain user
Local admin on client
Client machine
Helpdeskuser

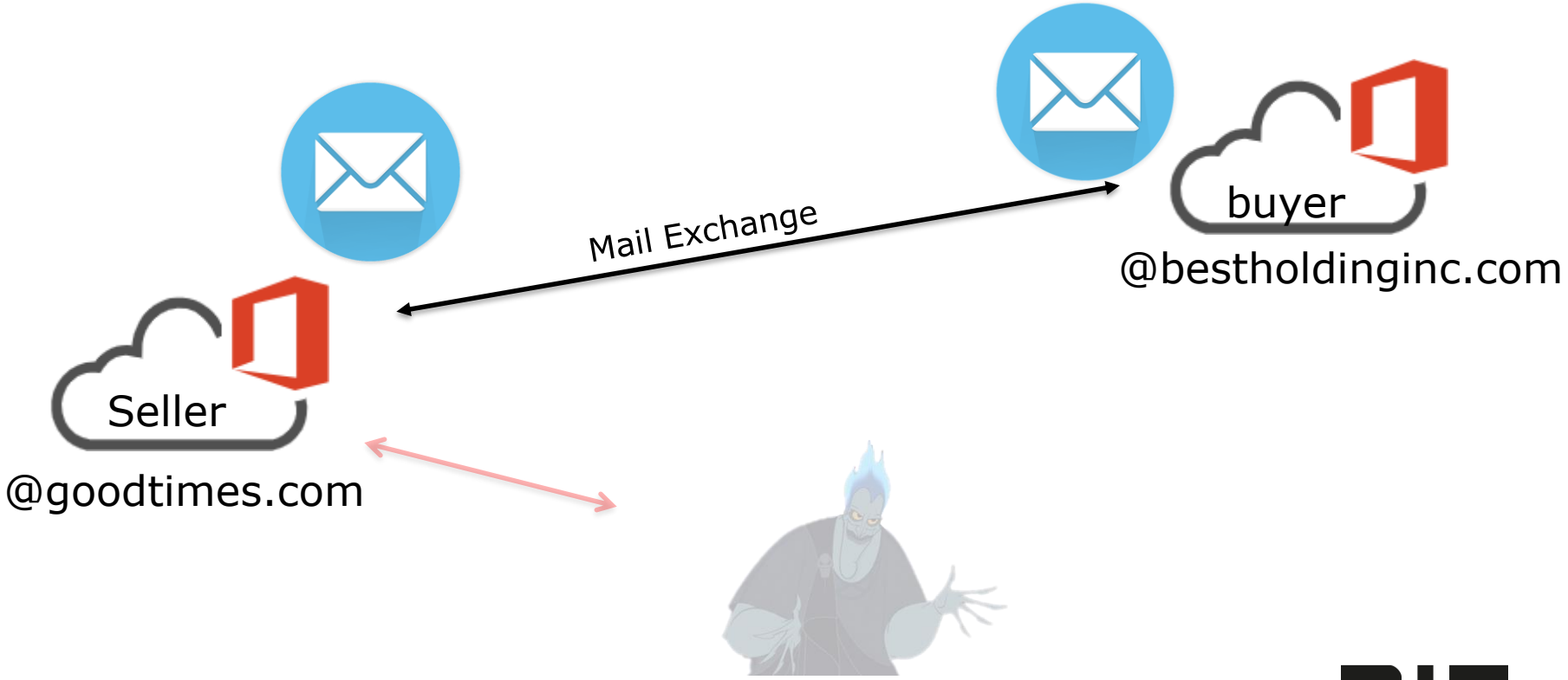
I didn’t know what to do!

What you should do

- Azure Advanced Threat Detection
- Administrative Tier model.
- Keep members of privileged groups to a minimum
- Delegate permissions.
- Enforce secure workstation
- Store Active Directory backups securely
- Monitor all, both on-prem and off-prem with Azure Sentinel or 3.party solutions
- Force password change on KRBTGT and AZUREADSSOACC at a regular basis
- Do not use synced accounts for privilege use in Office 365
- Implement Multifactor Authentication for access to cloud solutions for admins
- Plausible last resort… Big bitcoin account

Spear-phishing. Two attacks in one month
That succeeded

Spear-phishing



Spear-phishing

buyer

@bestholdinginc.com

Mail Exchange

Hades communicates with seller & buyer

Seller

@goodtimes.com

@besthodinglnc.com

Spear-phishing

buyer

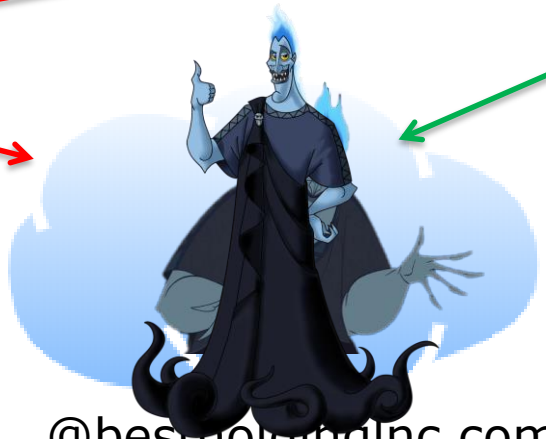
@bestholdinginc.com

Mail Exchange

Hades communicates with seller & buyer

Seller

@goodtimes.com



@bestholdinginc.com

Spear-phishing

buyer

@bestholdinginc.com

Mail Exchange

Hades communicates with seller & buyer

Seller

@goodtimes.com

I didn’t know what to do!

What you should do

- Implement multifactor authentication(MFA)
- Users training / Simulate phishing attacks
  - Company focus on cybersecurity
- Ensure systems and devices are well managed and patched
- Encrypt sensitive company information
- Sender Policy Framework record (SPF)
- Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- DomainKeys Identified Mail (DKIM)

"My message for companies that think they haven't been attacked is: You're not looking hard enough."

- James Snook, Deputy Director, UK Office for Cyber Security

Thanks for attending my session!

Assume breach. Notes from the field.

Michael Simon Arntzen

Twitter: @msarntzen

LinkedIn: https://www.linkedin.com/in/michaelarntzen

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2020