The R in SSR

ICANN Security Team | Riga, Latvia 2015

Resiliency

- What is Resiliency:
  - Resiliency is the ability to react to “Stress” without breaking.

- There are many different ways to be “Resilient”

Several frameworks exist to help guide your resiliency activities

ISO20072 : NIST SP 800-53 :
SANS / CSC Top 20 : ASD Mitigation Strategies

Resiliency Frameworks

- NIST SP 800-53 & ISO 27002 –hundreds of security controls grouped into families
  - Access Control, ConfigManagement, IR, etc
  - Very large, all encompassing, and ***intimidating*** for small organizations

Use this if you have the resources to devote to a comprehensive approach to resiliency

Resiliency Frameworks

- CSC (SANS) Top 20
  - 20 things you can do “today”, includes guidance, recommended tools, implementation ideas
  - Consensus of community experts
- ASD Mitigation Strategies
  - 35 things you can do to increase resiliency
  - Based on things that would have stopped 85% of the attacks that ASD responded to
  - Use these if you have limited resources and need to know where to get started

ASD - Examples

Top 4

–Application whitelisting

–Patch application

–Patch OS

–Restrict administrative privileges

ASD - Examples

Others

–Application hardening
–Host-Based IDS
–Disable local administrator accounts
–Network segmentation
–Multi-factor authentication
–Application firewalls
–Web filtering
–Strong passwords
–Network traffic capture
–Event logging

CSC (SANS) - Examples

First 5 Quick Wins

–Application whitelisting

–Standard secure configurations

–Patch applications software within 48 hours

–Patch system software within 48 hours

–Reduced number of users with administrative privileges

CSC (SANS) - Examples

Others

–Hardware inventory
–Software inventory
–Vulnerability assessment
–Wireless access controls
–Control ports/protocols
–Boundary defense
–Account monitoring
–Incident response
–Network engineering

Resiliency in Practice

Backups

–Backup everything!

Not just data.. Think about configurations, credentials etc.

Locate it locally for speed of recovery and offsite for resilience

Restore!! Test your backups an untested backup is worthless!

Resiliency in Practice

Remove all Single Points of Failure in critical systems!!

This is a standard of designing infrastructure that people forget.

If it is a SPF then look to solutions such as replication of services, adding secondary ISPs, Cross training staff…

Solutions that require time to bring up are cheaper than live systems .. .. Time costs money

Final thought

Resiliency must be something you plan for.

There are plenty of standards out there, find one that suits your situation

Some basic design principles will go a long way.

Engage with ICANN

Update email address

Thank You and Questions

Reach us at:
Email: security@icann.org
Website: http://www.icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations

References

- ISO20072 http://www.iso20072.org/iso-20072.htm
- NIST SP 800-53 https://web.nvd.nist.gov/view/800-53/home
- SANS / CSC Top 20